باسمه تعالی

عنوان

بررسی تهدیدات مانای پیشرفته (APT) و حملات مربوط به آن در ایران

فهرست مطالب

۱ مقدمه

در اواسط سال ۲۰۰۰، جامعه ای از هکرهای "کلاه سیاه" نوجوان متهم به خرابکاری در شبکه های جرایم سازمان یافته، طرحی سودمند برای سرقت هویت و اطلاعات شخصی تعداد انبوهی از کاربران شبکه های دولتی را به اجرا گذاشتند.

امروزه شاهد حمله های هدفمند سایبری به سازمان ها هستیم که به تدریج پیچیده تر، جدی و گسترده تر می شوند. به تازگی، تغییرات در زیرساخت های فناوری اطلاعات و مدل های استفاده شده، از جمله پویایی، رایانه های ابری و مجازی سازی، فضاهای امنیتی سازمانی سنتی را با ایجاد محیطی "هدفمند" برای هکرها تبدیل کرده اند. اما شاید مهمترین عنصر جدید در دورنمای تهدید، ظهور مبارزات جاسوسی و خرابکارانه بسیار هدفمند، درازمدت و بین المللی توسط بازیگران دولتی مخفی است.

این مبارزات بلند مدت و حمایت شده از سوی دولت گاهی اوقات به عنوان تهدید های پایدار پیشرفته (APTs) شناخته می شوند. این اصطلاح به رمز واژه مورد استفاده و سوء استفاده رسانه ها، و برخی از فروشندگان فن آوری تبدیل شده است. در حالی که APT ها در دنیای امروز نشانگر یک خطر واقعی هستند، مهم است که بدانیم چگونه آنها در یک چارچوب بزرگتر شکل می گیرند. تنها با جداسازی واقعیت از دروغ و دیدن نحوه ارتباط APT ها با حوزه وسیع تر روش ها و تکنیک های هدفمند حمله، سازمان ها قادر خواهند بود اطلاعات و عملیات خود را در دهه آینده حفظ کنند.

۲ APT چیست؟

APT یک نوع حمله هدفمند است. حملات هدفمند از تکنیک های متنوع و متعددی از جمله دانلودهای ناخواسته، تزریق SQL، بدافزار، نرم افزارهای جاسوسی، فیشینگ و هرزنامه ها، استفاده می کنند. APT ها اغلب می توانند از بسیاری از این تکنیک ها استفاده کنند. یک APT همیشه یک حمله هدفمند است، اما حمله هدفمند لزوما APT نیست.

اخیرا تعداد زیادی آسیب پذیری های امنیتی موجب برجسته شدن یک دسته جدید از تهدیدات برای شبکه ها شده و باعث شده که APT ها با تبدیل به یک موضوع جهانی سبب نگرانی بسیاری از شرکت ها شوند. این تهدیدات به عنوان فعالیت های حمایت شده از سوی دولت های ملی با هدف آسیب رسانی به شبکه های دولتی درنظر گرفته شده و هم چنین برای سازمان ها مشکلاتی ایجاد کرده اند.

RSA, NASA, Google و دولت ایران تجربه های زیادی از نقص امنیتی توسط APT ها داشتند و شواهد نشان می دهد که APT ها شبکه های سازمانی و دولتی را مورد هدف قرار داده اند.

APT ها به طور قابل توجهی متفاوت با تهدیدات سنتی بوده اما با این وجود بسیاری از حملات بردارهای حمله را تحت تاثیر خود قرار می دهند. از انجا که دیدگاه های متفاوتی در مورد اینکه حمله APT از چه چیزی تشکیل شده وجود دارد لازم است که مطالعاتی در این زمینه صورت گیرد.

APT ها اغلب هدفشان سرقت مالکیت معنوی (جاسوسی) بود اما در دراز مدت به حملات مخفیانه خود ادامه می دهند. مطابق با تعریف موسسه استاندارد و فناوری ملی امریکا (NIST[1]) در حمله های APT مهاجم که دارای تخصص زیاد و منابع قابل توجهی است هنگامی که فرصتی به وجود آید با استفاده از چند بردار حمله (cyber, physical, and deception,…) می تواند به اهداف خود دست پیدا کند.

این اهداف به طور معمول عبارتند از: ایجاد و گسترش پایانه هایی در زیرساخت فناوری اطلاعات سازمان های مورد هدف به منظور انتقال غیرمجاز اطلاعات حساس[2] و تضعیف یا جلوگیری از جنبه های بحرانی ماموریت، برنامه، سازمان و هم چنین خود را در اینده به سوی این اهداف سوق می دهد.

۳ ویژگی های تهدیدات پیشرفته پایدار (APT)

- اهداف خود را بارها و بارها در مدت زمان طولانی دنبال می کنند
- سازگار با تلاش های محافظت کننده برای مقاومت در برابر آنها

و هم چنین مصمم است تا سطح تعامل مورد نیاز برای اجرای اهداف خود را حفظ کند.

این تعریف یک مبنای خوب برای درک تفاوت بین تهدیدات سنتی و APT را فراهم می کند. ویژگی هایی نظیر: پیگیری مکرر اهداف، سازگاری با محافظت کننده ها و ماندگاری سبب می شود APT ها را از یک حمله معمول جدا کند. در ابتدا هدف اکثر APT ها استخراج اطلاعاتی (نظیر پژوهش های مهم، مالکیت معنوی و یا اطلاعات دولت) از سیستم است.

APT به گونه ای پیشرفته و به صورت مخفیانه عمل می کند و این توانایی را دارد که خود را در میان ترافیک شبکه سازمان پنهان کند و فقط به اندازه ای ارتباط برقرار کند تا بتواند کارهایی را که نیاز دارد انجام دهد. این توانایی جهت پنهان کردن خود سبب می شود که متخصصان امنیتی جهت شناسایی و یا متوقف کردن حمله APT تلاش بیشتری کنند. استمرار APT در دستیابی به هدف و تکرار تلاش خود جهت تکمیل کار

[1] US National Institute of Standards and Technology
[2] exfiltrating

بدین معنی است که پس از یک تلاش ناموفق دست نخواهید کشید و تا زمانی که به هدف خود نرسد به طور مداوم تلاش می کند تا به سیستم مورد نظر نفوذ کند.

ویژگی های این دسته از حملات عبارت اند از: به صورت مخفیانه عمل کردن، سازگاری و پایداری

به طور مثال حملات سنتی اغلب سعی می کنند از یک آسیب پذیری بهره برداری کرده اما اگر با هدف اولیه خود نتوانند نفوذ کنند به سمت چیزی که از امنیت کمتری برخوردار بوده حرکت می کنند اما در حالی که APT ها متوقف نمی شوند.

افراد و گروه هایی که پشت حملات APT هستند قادر و مصمم بوده تا با در اختیار داشتن منابع، حملات روز صفر را به شرکت و سازمان ها آغاز کنند و این باعث می شود که سخت تر بتوان در برابر آنها مقاومت نمود.

کسانی که قصد دارند حملات APT را به سوی یک سازمان روانه کنند از حملات هک Spear Phishing[۳] به عنوان یک درگاه ورود به سازمان ها استفاده می کنند و اغلب فیلترهایی که بر روی ایمیل ها انجام می شود به اندازه کافی در جهت شناسایی حملات Spear phishing ها موثر نبوده و هنگامی که کاربر بر روی لینک کلیک کرده و ضمائم ایمیل را باز می کند حمله APT شروع به اجرا شدن می کند که این اولین مرحله حمله بوده و هم چنین اضافه کردن فاکتور انسانی به کلاس تهدیدی که آسیب پذیری های شناخته شده را شناسایی نمی کند دفاع و پیشگیری را سخت تر می کند.

حملات APT از دیگر حملات هدفمند به شیوه های زیر متفاوت است:

حملات سفارشی – علاوه بر روش های معمول حمله، APTها اغلب از ابزارهای بسیار سفارشی و تکنیک های نفوذ استفاده می کنند که به طور خاص برای مبارزات گسترش یافته است. این ابزارها عبارتند از سوء استفاده از آسیب پذیری روز صفر، ویروس ها، کرم ها و روت کیت ها. علاوه بر این، APTها اغلب چندین تهدید یا زنجیره کشتار[۴]" را به طور همزمان برای نقض اهداف خود و اطمینان از دسترسی مداوم به سیستم های هدفمند انجام می دهند.

کم و آهسته– حملات APT در طی مدت زمانی اتفاق می افتد که طی آن مهاجمان به آهستگی و آرامی حرکت می کنند تا از شناسایی جلوگیری کنند. برخلاف تاکتیک های "پر سروصدا و با شتاب" بسیاری از حملات هدفمند که توسط جنایتکاران معمولی سایبری راه اندازی شده است، هدف از APT این است که با

---

[۳] spear phishing به معنای جمع آوری مشخصات شخصی افراد ، شامل نام ، سال تولد و سایر اطلاعات مشابه ، قبل از انجام حمله ی اصلی فیشینگ است. در واقع spear phishing ، فراهم کردن مقدمات حمله ی اصلی فیشینگ است.

[۴] The Kill Chainیک چارچوب کاری منحصر به فردی می باشد و عملیات هکری را که قصد نفوذ به شرکت را دارد سازماندهی میکند. هکر برای نفوذ نیاز به انجام برخی امور به صورت سلسله مراتبی می باشد که در صورت از کار انداختن یکی از این زنجیره کشتار متصل به هم منجر به خنثی سازی حمله هکر می شود که بسته به هر مرحله اطلاعات و اقدامات مختلفی وجود دارد که در صورت داشتن اطلاعات لازم میتوان این زنجیره را از عمل باز نگهداشت.

حرکت "کم و آهسته" با نظارت و تعامل مداوم تا زمانی که مهاجمان به اهداف تعیین شده خود دست یابند، شناسایی نشوند.

آرمان های بالاتر – بر خلاف طرح های سریع پولی که معمولا برای حملات هدفمند رایج تر هستند، APT ها برای تحقق نیازهای جاسوسی و یا خرابکاری بین المللی طراحی شده اند که معمولا شامل بازیگران دولتی مخفی می باشند. هدف APT ممکن است شامل جمع آوری اطلاعات نظامی، سیاسی یا اقتصادی، اطلاعات محرمانه یا تهدید تجاری محرمانه، اختلال در عملیات، یا حتی تخریب تجهیزات باشد. گروه هایی که پشت APTها هستند، به خوبی تامین مالی و پرسنل می شوند؛ آنها ممکن است با حمایت اطلاعات نظامی یا دولتی عمل کنند.

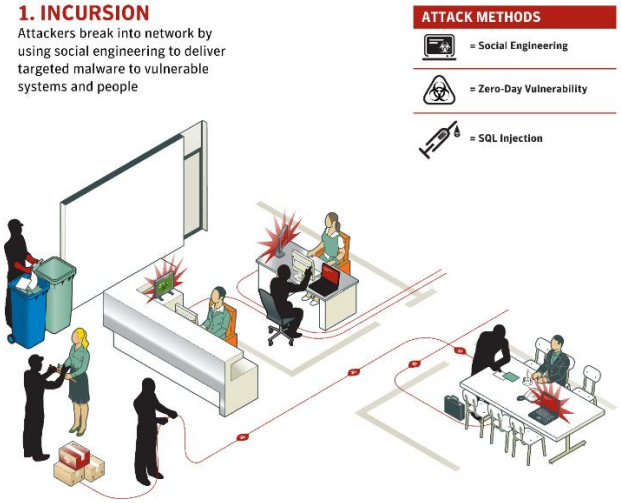
اهداف خاص – در حالیکه تقریبا هر سازمان بزرگ دارای مالکیت معنوی یا اطلاعات مشتری با ارزش در معرض حملات هدفمند است، APTها در مقیاس بسیار کوچکتری از اهداف مدنظر قرار می گیرند. حملات APT که به طور گسترده گزارش شده اند، در سازمان ها و تأسیسات دولتی، پیمانکاران دفاعی و تولید کنندگان محصولات که در بازارهای جهانی بسیار رقابتی هستند، راه اندازی شده اند. علاوه بر این، APTها ممکن است به فروشندگان یا سازمان های شریک که تجارت با اهداف اصلیشان را انجام می دهند، حمله کنند. اما سازمان های مربوط به دولت و تولید کنندگان تنها اهداف نیستند. شرکت های معمولی با تکنولوژی با ارزش یا دارایی های معنوی در حال حاضر توسط دولت های ملی هدف قرار می گیرند. با جهانی شدن اقتصاد دنیا، امنیت ملی و امنیت اقتصادی همگرا شده است. علاوه بر این، سازمان هایی که زیرساخت های ضروری ملی را حفظ و اداره می کنند نیز محتملا هدف هستند. امنیت™ Symantec.cloud ، که به ادغام داده های حمله هدفمند در چندین سازمان اجازه می دهد، گزارش می دهد که تنها ۱ در ۲۵ مورد از سازمان های مشتری آن هدف قرار گرفته است. بیشترین صنایع مورد هدف، مواد معدنی و سوخت هستند (۱ در ۸)، سپس حمل و نقل و آب و برق، ارتباطات راه دور و مهندسی.

۴ APTها چقدر مناسب هستند؟

اکنون باید آشکار شود که اگرچه هر سازمان یک هدف احتمالی یک APT نیست، اما آنها به عنوان یک تهدید واقعی و جدی برای برخی از سازمانها هستند. علاوه بر این، هر سازمان می تواند از درک بهتر APT ها بهره‌مند شود، زیرا تکنیک های APT احتمالا در طول زمان توسط هکرها و مجرمان سایبری اتخاذ می شود. در نهایت، از آنجا که هر کسی می تواند هدف حمله هدفمند باشد، و APT ها مثال هایی از حملات هدفمند بسیار پیشرفته، دراز مدت و در مقیاس بزرگ هستند - اگر شما درک بهتری از APT ها داشته باشید، می توانید بهتر از سازمان خود در مقابل تهدیدات هدفمند از هر نوعی دفاع کنید.

۵ چگونه حمله APT کار می کند؟

حملات APT به دقت برنامه ریزی شده و دقیق اجرا می شود. آنها معمولا به چهار مرحله تقسیم می شوند: نفوذ، کشف، ضبط و انتقال غیرمجاز اطلاعات حساس. در هر مرحله ممکن است از تکنیک های مختلف استفاده شود.



۵-۱ مرحله ۱: هجوم

در حملات هدفمند، هکرها به طور معمول در شبکه سازمان با استفاده از مهندسی اجتماعی، آسیب پذیری روز صفر، تزریقSQL، نرم افزارهای مخرب هدفمند و یا سایر روش ها، به شبکه نفوذ می کنند. تفاوت اصلی این است که در حالی که حملات هدفمند از روش های کوتاه مدت، "پر سروصدا و با شتاب" استفاده می کنند، تهاجم های APT برای راه اندازی عملیات مخفی در طی مدت زمان طولانی طراحی شده اند. ویژگی های دیگر تهاجم APT عبارتند از:

شناسایی[۵] – حملات APT اغلب تعداد زیادی از محققان را که ممکن است ماه ها را صرف مطالعه اهداف خود و آشنا ساختن خود با سیستم های هدف، فرایندها و افراد، از جمله شرکا و فروشندگان می کنند، بکار می گیرد. اطلاعات ممکن است به صورت آنلاین و با استفاده از روش های نظارت معمولی جمع آوری شوند. در مورد حمله Stuxnet به سازمان هایی که تصور می‌شود که کارخانه های هسته ای ایران را اداره می کنند، تیم حمله، متخصص در طراحی کنترل کننده‌های منطقی قابل برنامه ریزی (PLC ها) مورد استفاده در غنی سازی اورانیوم، که در این حمله مورد هدف قرار گرفته بود، بودند.

[۵] Reconnaissance

مهندسی اجتماعی – تهاجم اغلب از طریق استفاده از تکنیک های مهندسی اجتماعی انجام می شود، مانند فریب دادن کارکنان ناآگاه به کلیک بر روی لینک یا باز کردن پیوست هایی که به نظر می رسد از شرکا یا همکاران مورد اعتماد، فرستاده شده است. بر خلاف حمله فیشینگ معمولی، این تکنیک ها اغلب با تحقیقات عمیق در مورد سازمان هدف، تغذیه می شوند. در یک مورد، تعداد کمی از کارکنان منابع انسانی با استفاده از یک پیوست ظاهرا بی ضرر، یک صفحه گسترده در مورد نیازهای استخدام که ظاهرا از یک وب سایت شغلی ارائه شده بود، مورد هدف قرار گرفتند. در مورد حمله Hydraq، کاربران مورد هدف به یک وب سایت میزبانی عکس هدایت می شدند که در آن از طریق یک دانلود ناخواسته توسط ویروس آلوده می شدند.

آسیب پذیری های روز صفر – آسیب پذیری های روز صفر ،نقاط ضعف امنیتی هستند که برای توسعه دهندگان ناشناخته است و بنابراین ممکن است قبل از اینکه توسعه دهنده بتواند یک وصله فراهم کند یا آن را تعمیر کند توسط مهاجمان مورد سوء استفاده قرار بگیرند. در نتیجه، سازمان هدف دارای آسیب پذیری روز صفر هیچ فرصتی برای آماده سازی خود و اقدامات لازم جهت مواجه شدن با این آسیب پذیری ها ندارد. از آنجایی که زمان و تلاش زیادی برای شناسایی آسیب پذیری های روز صفر لازم است، تنها پیشرفته ترین سازمان های مهاجم احتمالا از آنها استفاده می کنند. APT ها اغلب از یک آسیب پذیری روز صفر برای شکستن هدف استفاده می کنند، به دومین و سپس سومین نقطه حمله تغییر می دهند تا بالاخره هر نقطه حمله در نهایت ثابت شود. در مورد حمله Hydraq اینگونه بود. حمله Stuxnet استثنایی بود بطوریکه در آن چهار آسیب پذیری روز صفر جداگانه به طور همزمان مورد سوء استفاده قرار گرفتند.

عملیات دستی – حملات رایج یا بزرگ از اتوماسیون به منظور به حداکثر رساندن دسترسی استفاده می کنند. کلاهبرداریهای فیشینگ روش spray and pray (اول شلیک کن بعد دعا) از هرزنامه اتوماتیک استفاده می کنند تا هزاران کاربر را هدف قرار دهند به این امید که درصد مشخصی از آنها روی یک لینک یا پیوست کلیک خواهند کرد و سبب حمله شود.

از سوی دیگر، در حالی که APT ها ممکن است هرزنامه ها را گسترش دهند، اغلب آنها سیستم های فردی مشخصی را هدف قرار می دهند و روند حمله به شدت متمرکز است.

۵-۲ مرحله ۲: کشف

به محض ورود، مهاجم سیستم های سازمان را بررسی می کند و به طور خودکار برای اطلاعات محرمانه یا، در مورد برخی از APT ها، دستورالعمل های عملیاتی و کاربرد های آن را اسکن می کند. کشف ممکن است شامل داده های محافظت نشده شبکه ها و همچنین آسیب پذیری های نرم افزاری و سخت افزاری، گواهینامه های لورفته و مسیرهایی به منابع اضافی یا نقاط دسترسی[۶] باشد.

در اینجا دوباره، در حالی که بیشتر حملات هدفمند فرصت طلبانه هستند، حملات APT اکثرا روشمند هستند و برای جلوگیری از تشخیص در مدت زمان طولانی تری انجام می پذیرند.

چندین بردار – همراه با حمله، APTها تمایل دارند از تکنیک های کشف متعدد بصورت ترکیبی استفاده کنند. هنگامی که بدافزار در سیستم میزبان حضور دارد، ابزارهای اضافی را می توان در صورت نیاز برای جستجوی نرم افزار، سخت افزار و آسیب پذیری های شبکه دانلود کرد.

اجرای بیصدا، اجرا عمیق- از آنجا که هدف APT ماندن در داخل سازمان و برداشت اطلاعات در طولانی مدت می باشد، فرایندهای کشف طوری طراحی شده اند که به هر قیمتی از شناسایی شدن جلوگیری شود. Hydraq(همچنین به عنوان Aurora یا حملات گوگل شناخته می شود) از تکنیک های مبهم برای پنهان

[۶] access point

ماندن در سازمان های قربانی استفاده کرد. به خصوص، از spaghetti code استفاده کرد، یک تکنیک که سبب می شود تجزیه و تحلیل و تشخیص بدافزار سخت تر شود.

تحقیق و تحلیل- تلاش های کشف با تحقیق و تحلیل بر روی سیستم ها و داده های یافت شده، از جمله توپولوژی شبکه، شناسه های کاربری، رمز عبور و غیره همراه است.

هنگامی که یک APT شناسایی می شود، اولین سؤالی که پرسیده می شود این است: چه مدت آنجا بوده است؟ در مورد حمله هدفمند معمولی چنین نیست؛ اگر شماره حساب ها به سرقت رفته باشد، محاسبه زمان نفوذ و ارزیابی آسیب خیلی سخت نیست. با این حال، با استفاده از APT ها ممکن است تقریبا غیرممکن باشد که مشخص شود حمله چه زمانی رخ داده است. قربانیان ممکن است نیاز به بررسی فایل های ورود به سیستم و یا تنظیم تجهیزات شوند، چرا که مراحل حمله و کشف به خوبی پنهان شده است.

در برخی موارد، Kill Chain حمله APT ممکن است بسیار آسان پیدا شود. اما ظاهر می تواند فریبنده باشد. Kill Chain آشکار ممکن است عمدا راه اندازی شود تا قربانی را منحرف سازد، در حالی که مجرمان بطور پنهانی در جهت اهداف واقعی خود پیش می روند.

۵-۳ مرحله ۳: ضبط

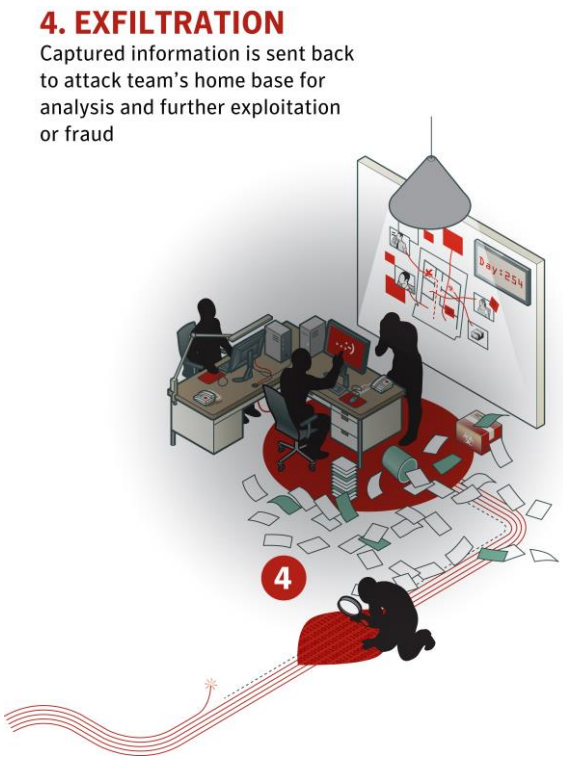
در مرحله ضبط، داده های ذخیره شده در سیستم های محافظت نشده بلافاصله در دسترس قرار می گیرند. علاوه بر این، ممکن است در سیستم های هدفمند و نقاط دسترسی شبکه روت کیت ها به صورت مخفی نصب شوند تا اطلاعات و دستورالعمل ها را همانطور که در سازمان جریان دارند، ضبط کنند. در مورد Duqu، که به نظر می رسد مقدمه ای برای آینده باشد، حمله مانند Stuxnet، تنها هدف آن جمع آوری اطلاعات است، که می تواند برای دادن بینشی که برای حملات آینده نیاز دارند، به مهاجمین داده شود. در حالی که Duquبه طور گسترده ای مورد استفاده قرار نگرفته بود، بسیار هدفمند است و اهداف آن شامل تامین کنندگان تجهیزات صنعتی می باشد.

اشغال طولانی مدت- APT طراحی شده است تا اطلاعات را در مدت زمان طولانی ضبط کند. به عنوان مثال، یک عملیات جاسوسی گسترده به نام GhostNet ، که در مارس ۲۰۰۹ کشف شد، قادر به نفوذ به سیستم های کامپیوتری در ۱۰۳ کشور از جمله سفارتخانه ها، وزارتخانه های خارجی و دیگر ادارات دولتی و مراکز تبعید تبتی دالایی لاما در هند، لندن، و نیویورک شد.

بر اساس یک گزارش توسط Information Warfare Monitor ، GhostNet شروع به ضبط اطلاعات در ۲۲ ماه مه ۲۰۰۷ کرد و حداقل تا ۱۲ مارس ۲۰۰۹ ادامه داد. به طور متوسط، زمانیکه یک میزبان به طور فعال توسط یک APT آلوده شد ۱۴۵ روز بود، طولانی ترین دوره آلوده بودن سیستم ۶۶۰ روز است.

کنترل: در بعضی موارد، APTها باعث سوئیچ از راه دور یا خاموش کردن سیستم های نرم افزاری و سخت افزاری اتوماتیک می شوند. همانطور که دستگاه های فیزیکی بیشتر و بیشتر با میکروپروسسورهای جاسازی شده کنترل می شوند، احتمال وقوع این اتفاقات زیاد است. در حقیقت، Stuxnet فراتر از سرقت اطلاعات پیش رفت. هدف آن تجدید برنامه های سیستم های کنترل صنعتی - برنامه های کامپیوتری برای مدیریت محیط های صنعتی مانند نیروگاه ها، پالایشگاه های نفت و خطوط لوله گاز بود. به طور خاص، هدف آن دستکاری تجهیزات فیزیکی متصل به سیستم های کنترل صنعتی خاص بود تا تجهیزات بر خلاف هدف مورد نظر خود، به نحوی که توسط مهاجم برنامه ریزی شده عمل کنند. سرورهای فرماندهی و کنترل ممکن است، مخفیانه کنترل سیستم های هدف را بگیرند و حتی بسته به برنامه APT آنها را از بین ببرند.

۵-۴ فاز ۴: انتقال غیرمجاز اطلاعات حساس[۷]



هنگامی که مهاجمان کنترل سیستم های هدف را به دست آوردند، ممکن است با سرقت مالکیت معنوی یا سایر اطلاعات محرمانه ادامه دهند.

[۷] Exfiltration

انتقال داده ها – پس از سیگنال های فرمان و کنترل، داده های برداشت شده ممکن است به پایگاه تیم حمله کننده به صورت کامل (از طریق پست الکترونیکی، بطور مثال) یا بسته بندی شده در بسته های رمزگذاری شده یا فایل های زیپ با حفاظت رمز عبور فرستاده شود. Hydraq از تعدادی تکنیک جدید برای ارسال اطلاعات سرقت شده به پایگاه اصلی استفاده کرد. یکی از این ها، استفاده از پورت ۴۴۳ به عنوان یک کانال اصلی برای بارگیری اطلاعات دزدیده شده بود. همچنین ارتباطاتی را ایجاد کرد که یک کلید SSL تبادلی را شبیه سازی می کرد، اما در یک کانال SSL کاملا مذاکره شده نتیجه نداد. در نهایت، از رمزهای خصوصی برای رمزگذاری محتوا استفاده کرد تا اینکه سازمان های قربانی را ترک کرد.

تجزیه و تحلیل در حال انجام – در حالی که شماره کارت اعتباری ربوده شده از یک حمله هدفمند به سرعت برای فروش بسته بندی می شود، اطلاعاتی که توسط APT ها ضبط شده است، اغلب برای سرنخ هایی برای فرصت های استراتژیک مورد مطالعه قرار می گیرد. چنین داده هایی ممکن است به منظور تحلیل دستی توسط متخصصان در این زمینه برای استخراج اسرار تجاری، پیش بینی حرکت های رقابتی و برنامه ریزی مانورهای متضاد مورد استفاده قرار گیرد.

۶ اقدامات در برابر حملات APT

کلاهبرداری در اطراف APT ها یک حقیقت اساسی را پنهان می کند؛ این تهدیدات، در واقع، یک مورد خاص در دسته بسیار گسترده تری از حملات هدفمند در سازمان های خاصی از هر نوع است. همانطور که APT ها همچنان در چشم انداز تهدید ظاهر می شوند - و هیچ دلیلی وجود ندارد که فکر کنیم که آنها نخواهند بود - انتظار می رود تکنیک های مشابهی را که توسط دیگر مجرمان سایبری به کار گرفته می شوند، مشاهده شود. علاوه بر این، این واقعیت است که APT ها اغلب به سرقت مالکیت معنوی منجر می شوند، نقش های جدیدی برای مجرمان سایبری به عنوان دلالان اطلاعات در طرح های جاسوسی صنعتی پیشنهاد می شود.

بهترین راه برای آماده سازی در مقابل یک APT این است که اطمینان حاصل شود که به طور کلی در برابر حملات هدفمند دفاع می کنید. در واقع، در حالی که شانس یک APT که بر سازمان شما تاثیر می گذارد، ممکن است نسبتا کم باشد، احتمال این که شما قربانی یک حمله هدفمند باشید، متاسفانه بسیار زیاد است.

Symantec ارزیابی امنیتی دقیقی ارائه می دهد که می تواند به شناسایی خطرات احتمالی حملات هدفمند کمک کند.

ارزیابی حمله هدفمند

- آیا شما نگران هستید که کارکنان و مدیران کلیدی شما ممکن است یک هدف سرقت IP باشند؟
- آیا شما تعجب می کنید اگر هر یک از سیستم های کلیدی شما توسط نرم افزارهای مخرب به خطر افتاده باشد؟

ارزیابی فعالیت مخرب

- آیا شما درباره آلودگی های پنهانی نگران هستید؟
- برای اطمینان از اینکه سازمان شما آلوده نیست، چه کاری انجام می دهید؟
- آیا میخواهید از نظارت مداوم خود بهتر استفاده کنید؟

ارزیابی خطر از دست دادن داده ها

- آیا نگران هستید که داده های حساس از طریق حساب های ایمیل شخصی و شرکتی از شبکه شما خارج می شوند؟
- آیا می خواهید بدانید که کدام فایل های حساس آسیب پذیر هستند زیرا آنها برای همه قابل دسترسی هستند؟
- آیا شما یک پیروی از قوانین اولیه دارید که حفاظت از اطلاعات حساس کارت پرداخت یا اطلاعات شخصی را اجبار کرده است؟

ارزیابی آسیب پذیری

- آیا می دانید که کدام پایگاه های داده، سرورها و دستگاه های شبکه برای حملات هکرها آسیب پذیر هستند؟
- آیا می دانید که کدام دستگاه های مدیریت نشده یک خطر امنیتی برای سیستم های بحرانی شما مطرح می کند؟
- آیا می دانید کدام آسیب پذیری ها باید بیشترین اولویت را برای تلاش های درمانی دریافت کنند؟

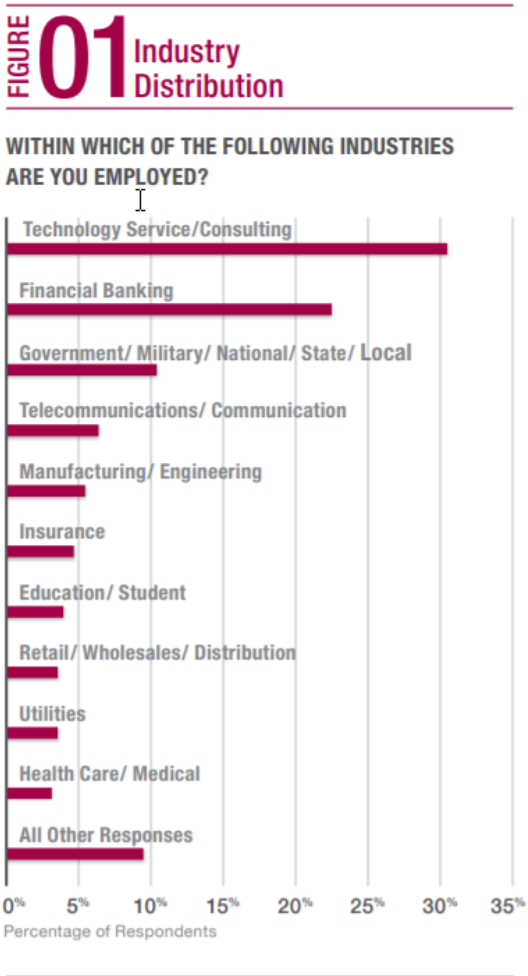
۷ مطالعات انجام شده بر روی APT ها

بر روی APT ها یک مطالعه تحقیقی در اواخر سال ۲۰۱۲ صورت گرفت. در چند سال اخیر سرفصل هایی برای APT ها جهت نفوذ به شبکه های سازمانی شناخته شده تهیه شد. هنگامی که تصور می شد APT ها فقط محدود به حملات شبکه های دولتی می باشند حمله Google Aurora در سال ۲۰۱۰ نشان داد که APT ها فقط محدود به حملات دولتی نمی باشند بلکه طیف عظیمی از حملات را در برمی گیرد و سبب شد که تبدیل به یک موضوع بین المللی شود به طور مثال نفوذ به RSA در سال ۲۰۱۱ جز نفوذ هایی است که در طبقه بندی APT قرار گرفته است اگرچه سطح آگاهی در موردAPT درحملات Stuxnet و Flame بیشتر شد. به همین خاطر تیم مشاوره ISACA و Practices Committee تشکیل شد تا یک سری مطالعات

تحقیقی بر روی حملات APT انجام دهند. این تیم جهت درک بهتر اینکه چگونه متخصصان امنیتی APT ها را درک کنند و همچنین اقدامات پیش گیرانه ایی در برابر انها انجام دهند تشکیل شد.

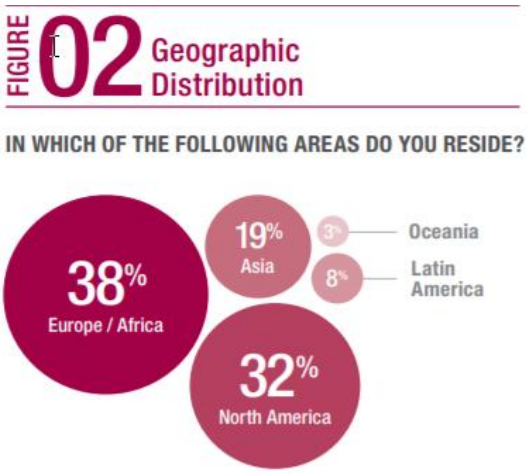
نظرسنجی توسط LinkedIn با دعوت از CISMs و متخصصان امنیت اطلاعات برای افراد عضو ISACA و هم چنین افرادی که کارشناس امنیتی نبودند راه اندازی شد و منجر به تعریف یک نمونه که شامل مدیران امنیت اطلاعات در صنایع و سازمان های مختلف در سراسر دنیا شد. لازم به ذکر است که این نظر سنجی در ۵ بخش اصلی برگذار و از مقیاس های multiple-choice و Likert در آن استفاده شد.

لازم به ذکر است این مطالعه بر روی افرادی مانند متخصصان امنیت اطلاعات و افرادی که روزانه با این مسائل سروکار دارند انجام شد.



نمونه این مطالعه جهانی بوده و شامل افرادی است که دارای مدرک ISACA وCISM بوده و هم چنین متخصصان امنیت اطلاعات که در قالب گروه هایی بر روی امنیت و APT ها در LinkedIn فعالیت دارند.

هم چنین لازم به ذکر است که Survey Monkey[۸] از ۱۵۵۱ فرد در جهان که حدود ۹۳.۱٪ انها عضو ISACA بوده اطلاعاتی را جمع آوری نمود. همچنین در این مطالعه از بیش از ۲۰ صنایع استفاده شده و اکثر پاسخ دهندگان (۳۰.۹ ٪) جز حوزه خدمات فناوری و مشاوره بوده و همچنین اکثر پاسخ دهندگان ساکن اروپا و افریقا با (۳۸.۳٪) و پس از ان امریکای شمالی با(۳۲٪) بوده اند.



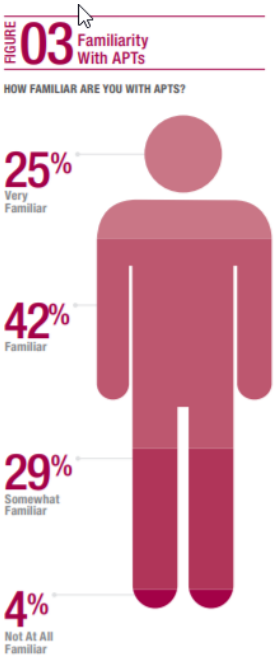
۷-۱ دیدگاه ها در مورد APT ها

بسیاری از شاخص های مثبت در طول مطالعه مشخص شدند اما لازم به ذکر است که به نظر می رسد پاسخ ها مغایرت داشته باشند با انالیزهایی بعدی که مکمل انها خواهد بود.

این مقیاس های مثبت (شامل: افزایش توجه مدیریت، بودجه های امنیتی و اجرای سیاست ها) با نشانه های پاسخ دهندگان مغایر بوده و نشان می دهد که ان ها تمایلی به افزایش آگاهی های امنیتی و نحوه برخورد با اشخاص ثالث ندارند.

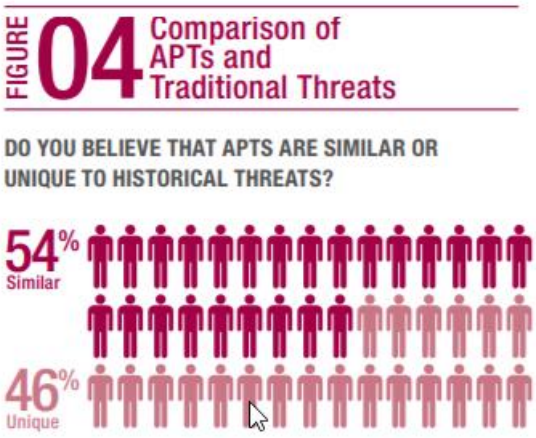
۵۳.۴ درصد از پاسخ ها نشان می دهد که آن ها اعتقاد دارند که APT ها با تهدیدات سنتی متفاوت بوده. همچنین نتایج نظر سنجی نشان می دهد که ۲۵.۱ درصد از پاسخ دهندگان اعتقاد دارند با APT اشنایی کافی دارند و در مجموع ۹۶.۲ درصد بیان می کنند که حداقل تا حدودی با APT آشنایی دارند.

[۸] :www.surveymonkey.com



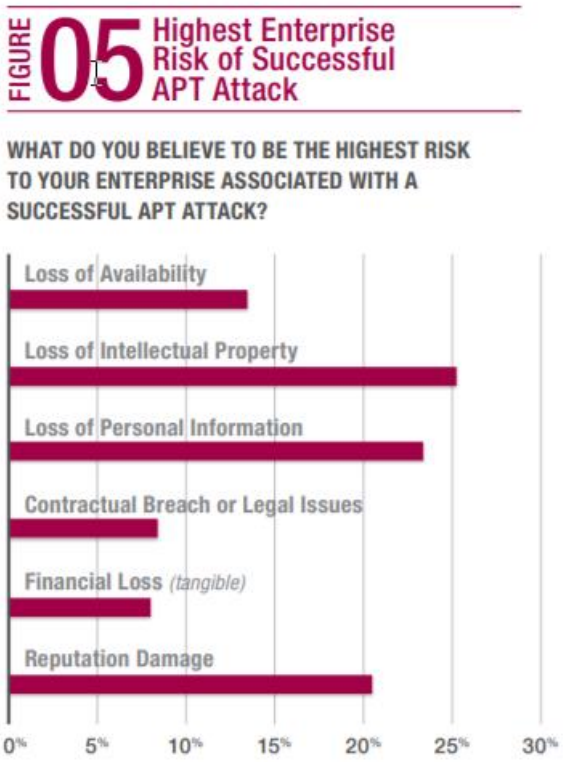
در حالی که این سطح اشنایی با APT ها یک امتیاز مثبت است به نظر می رسد که ۵۳.۴ درصد پاسخ ها نشان می دهد که شرکت کنندگان در نظرسنجی معتقدند که APT ها با تهدیدات سنتی متفاوت بوده اما این یافته ها مشکل زا بوده چرا که به این معنی است که یک سردرگمی در مورد ماهیت APT ها و تفاوت آن ها با تهدیدات سنتی وجود دارد. و اگر متخصصان امنیتی تفاوت بین کلاس های تهدید را درک نکنند قادر به شناسایی روش درست دفاع در برابر APT ها و پاسخ درست به آن ها نخواهند بود.

۹۳.۹ درصد بازخورد گزارش ها نشان می دهد که پاسخ دهندگان معتقدند که APT ها یک تهدید اصلی برای امنیت ملی و ثبات اقتصادی بوده و لازم است به درک روشنی از آنچه که هست نمایان شود.



هم چنین ۸۹.۷ درصد از پاسخ دهندگان بر این باورند که استفاده از سایت های شبکه اجتماعی احتمال حمله موفق APT را افزایش می دهد و نیز ۸۳.۷ درصد پاسخ دهندگان بر این باورند که هنگامی که دستگاه خود را به محل کار خود می آورند ممکن است این دستگاه قبلا توسط صاحب دستگاه به منظور افزایش سطح دسترسی سیستم عامل و عملکرد بهتر سخت افزار و یا برای فرار از محدودیت های فروشندگان دستکاری شده باشد که این امر سبب می شود احتمال حمله موفق APT را افزایش می دهد.

در حالی که اکثر پاسخ دهندگان معتقدند که APT مسئله ایی است که موجب نگرانی آنها شده و عده ایی اندک معتقدند در صورتی که حمله APT به صورت موفقیت آمیز انجام می شود می تواند بزرگ ترین خطر برای شرکت ها باشد. همچنین از دست دادن مالکیت معنوی شرکت ها با ۲۵.۵ درصد و از دست رفتن اطلاعات شخصی کارمندان و مشتریان با ۲۳.۶ درصد به ترتیب جز بزرگ ترین خطراتی است که سازمان ها را تهدید می کند.



۲-۷ تجربه مستقیم APT

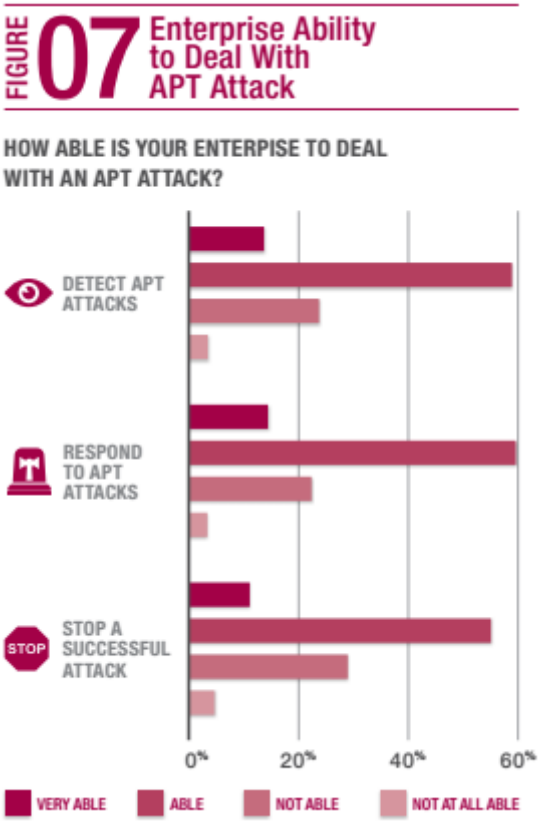
در حالی که پاسخ دهندگان سناریوهای خطر یک حمله APT را شناسایی می‌کردند بیشتر آن‌ها هنوز با یک حمله واقعی سر و کار نداشته‌اند. تنها ۲۱/۶ ٪ از پاسخ دهندگان گزارش داده‌اند که مورد حمله APT قرار گرفته‌اند. از این تعداد ۲۶/۲ ٪ در زمینه خدمات تکنولوژی و مشاوره‌ای مشغول به کار بودند و ۲۲/۷ ٪ در خدمات مالی کار می‌کردند. به علاوه از افرادی مورد حمله قرار گرفته بودند، پرسیده شد که آیا قادر به شناسایی منبع حمله هستند؛ ۶۵/۴ ٪ پاسخ مثبت دادند.

در حالی که تنها ۲۱/۶ ٪ از پاسخ دهندگان گزارش دادند که شرکتشان قبلاً تحت APT قرار گرفته است، حدوداً سه برابر این تعداد -۶۳ ٪- بر این باور بودند که شرکتشان دیر یا زود هدف قرار خواهد گرفت. (شکل ۶)

۶۳ ٪ از پاسخ دهندگان فکر می‌کنند که دیر یا زود شرکتشان توسط APT هدف قرار خواهد گرفت.

از همه پاسخ دهندگان سوال شد که آیا فکر می‌کنند شرکتشان برای مقابله با تهدید APTها آماده است؟ اکثریت باور داشتند که توانایی تشخیص، واکنش و توقف یک حمله موفقیت آمیز APT را دارند. (شکل ۷)

به طور کلی، حدود ۶۰ ٪ از پاسخ دهندگان باور داشتند که آمادگی واکنش به حملات APT را دارند.



۳-۷ کنترل‌های امنیت، فرایندها و واکنش‌ها

همانطور که قبلاً اشاره شد، اکثر پاسخ دهندگان بر این باور بودند که برای شناسایی، واکنش و توقف یک حمله APT در موقعیت خوبی قرار دارند. چه کنترل‌ها و اقدامات متقابلی نیاز است تا اطمینان حاصل شود که این درست است؟

در طول این بررسی، الگوها نشان می دهد که گرچه در مورد اینکه APT چیست سردرگمی وجود دارد، به نظر می‌رسد شرکت‌ها در راستای برنامه ریزی برای APTها یک رویکرد بر پایه ریسک دارند. کنترل‌ها در شرکت‌هایی که احساس می‌کنند می‌توانند هدف حمله یک APT قرار گیرند، نسبت به شرکت‌هایی که احساس می‌کنند مورد حمله قرار نمی‌گیرند رایج‌تر است.

۴-۷ طرح‌های مدیریت حادثه

به طور کلی، نزدیک به ۶۰ ٪ پاسخ دهندگان باور دارند که برای واکنش به حملات APT آمادگی دارند. هنگامی که از میزان آمادگی شرکت‌ها برای مقابله با حمله APT پرسیده شد، ۱۴ ٪ پاسخ دادند که "کاملاً آماده هستند" ، که این نشان می‌دهد آن‌ها یک طرح آزمایش شده و ثبت شده برای APT در شرکت دارند. ۴۹/۶ ٪ دیگر پاسخ دادند "آماده هستند"، که این نشان دهنده داشتن یک طرح مدیریت حادثه است گرچه نتواند به طور خاص APT را پوشش دهد. ۳۷/۴ ٪ از پاسخ دهندگان مطمئن نبودند که برای مقابله با رویدادی که از طریق این دسته از تهدیدها ایجاد می‌شود آمادگی داشته باشند.

با ارزیابی بیشتر نتایج، می‌توان یک رابطه بین درک احتمال هدف حمله APT قرار گرفتن شرکت‌های پاسخ دهندگانو سطح آمادگی آن‌ها برای مقابله با چنین حادثه‌ای مشاهده کرد.ظاهراً درک بیشتر از احتمال اینکه هدف قرار گیرند منجر به آمادگی بیشتر شرکت می‌شود.

از میان ۱۷/۹ ٪ از پاسخ دهندگانی که احساس می‌کردند "بسیار محتمل" است که سازمانشان هدف یک حمله APT قرار گیرد، ۳۱/۱ ٪ خود را در گروه "بسیار آماده" و ۴۹/۵ ٪ در گروه "آماده" قرار دادند. این نشان می‌دهد که ۸۰/۶ ٪ از کسانی که احتمال هدف قرار گرفتن شرکتشان را بالا می‌دانند، برای مقابله با آن آماده‌اند.به همین ترتیب کسانی که شرکت خود را به عنوان هدف "احتمالی" می‌شناختند (۴۵/۱ ٪)، اظهار داشتند که آن‌ها نیز برای مقابله با حمله آماده هستندکه ۱۴ ٪ خود را "بسیار آماده"می‌دانند و ۵۳/۲ ٪ ادعا می‌کنند "آماده" هستند (جمعاً ۶۷/۲ ٪). در حالی که کل درصد "آماده" برای این گروه به اندازه گروه "بسیار محتمل" نیست،این جمعیت انتظار احتمال کمتری را نیز دارند.

ارتباط بین احتمال و آمادگی در دسته‌های پایین‌تر همچنان ادامه دارد. از میانکسانی در گروه که پاسخ "زیاد محتمل نیست" که شرکتشان توسط یک APT هدف قرار گیرد را می‌دهند، ۵۱/۵ ٪ گزارش دادند که حداقل برای یک حمله آماده‌اند و در میان گروه "اصلاً محتمل نیست" تنها نیمی خود را آماده می‌دانستند. (شکل ۸).

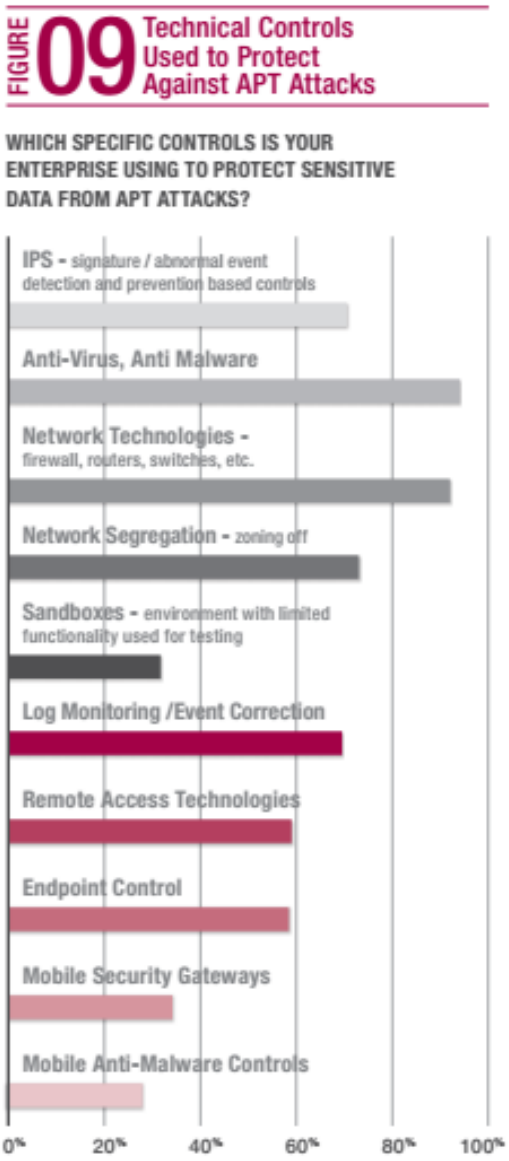
FIGURE 08 Correlation Between Likelihood of and Preparedness for an APT Attack

CORRELATION BETWEEN LIKELIHOOD OF AND PREPAREDNESS FOR AN APT ATTACK.

	How likely do you feel that your organization will be the target of an APT?			
	Very Likely	Likely	Not Very Likely	Not at all Likely
Very prepared We have a documented and tested plan in place for APT	31.1% (69)	14% (90)	4.8% (21)	23.1% (6)
Prepared But incident management does not specifically cover APT	49.5% (110)	53.2% (303)	46.7% (205)	26.9% (7)
Not very prepared	15.8% (35)	30.2% (172)	42.1% (185)	34.6% (9)
Not prepared at all	3.6% (8)	2.6% (15)	6.4% (28)	15.4% (4)

۷-۵ تکنولوژی

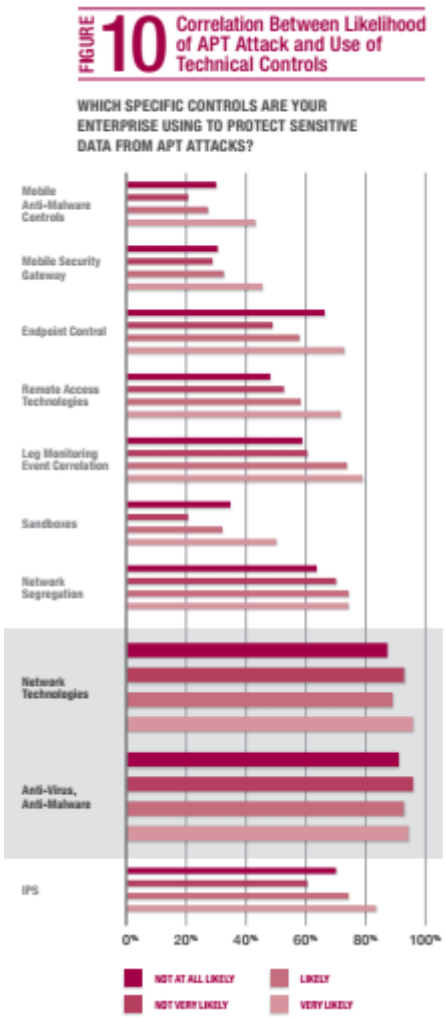
پاسخ دهندگان تنوعی از کنترل‌های تخصصی آشکار کننده و بازدارنده و نیز تحصیل، آموزش و سیاست را برای کمک به کاهش احتمال یک حمله به کار می‌برند. درصد بسیار بالایی از کسانی که مورد بررسی قرار گرفتند، بیان کردند که از ضد ویروس، ضد بدافزار و یا تکنولوژی‌های محیط شبکه سنتی برای خنثی کردن APT ها استفاده می‌کنند، اما امتیازهای بسیار کمتری برای کنترل‌های حیاتی برای دستگاه‌های تلفن همراه، تکنولوژی‌های دسترسی از راه دور (RATها) و رابطه ورود/واقعه (logging/eventcorrelation)دیده شد. (شکل ۹).



علاوه بر این کنترل‌های تخصصی، ۷۰/۶ ٪ از افراد مورد بررسی پاسخ دادند که از آموزش و یادگیری برای کمک به جلوگیری از حملاتی از قبیل spear phishing و مهندسی اجتماعی (social engineering) استفاده می‌کنند،که این روش‌ها به طور خاص تلاش می‌کنند تا از فاکتور انسانی بهره برند.

درصد بسیار بالایی از کسانی که مورد بررسی قرار گرفتند، بیان کردند که از ضد ویروس و ضد بدافزار و یا تکنولوژی‌های محیط شبکه سنتی برای خنثی کردن APT ها استفاده می‌کنند.

در بخش مدیریت حادثه، یک رابطه بین درک احتمال حمله APT و میزان آمادگی برای مقابله با حمله بیان شد. یک ارتباط مشابه در اینجا نشان داده شده است که در آن به نظر می‌رسد شرکت‌هایی که درک کرده‌اند احتمال دارد یا بسیار احتمال دارد که هدف APT قرار گیرند، از کنترل‌های تخصصی بیشتری نسبت به کسانی که خود را اهداف احتمالی این تهدیدات نمی‌دانند، استفاده می‌کنند. (شکل ۱۰)



تمرینات آموزشی نیز به عنوان یک دفاع برای شرکت‌هایی که احساس می‌کنند به احتمال زیاد (۸۲ ٪) یا احتمالاً (۷۴/۱ ٪) هدف قرار می‌گیرند متداول‌تر است.

در حالی که این مورد که میزان بالاتر درک احتمال حمله APT با افزایش استفاده از کنترل-های تخصصی و آموزشی در ارتباط است نشانه مثبتی است، نگران کننده است که تکنولوژی-های محیط شبکه و ضد ویروس و ضد بدافزار در بالای لیست کنترل‌های مورد استفاده قرار دارند.

در حالی که این مورد که میزان بالاتر احتمال حمله APT با افزایش استفاده از کنترل‌های تخصصی و آموزشی در ارتباط استنشانه مثبتی است، نگران کننده است که تکنولوژی‌های محیط شبکه و ضد ویروس و ضد بدافزار در بالای لیست کنترل‌های مورد استفاده قرار دارند. APTها بسیار پیشرفته‌اند و برای دوری کردن از روش‌هایی که معمولاً توسط این کنترل‌ها جلوگیری می‌شوند، شناخته شده هستند. به عنوان مثال،

APTها تمایل به هدف قرار دادن آسیب‌پذیری‌های شناخته شده‌ای که پچ شده‌اند ندارند و از امضاهای قابل تشخیص که ممکن است برای سیستم‌های پیشگیری و تشخیص نفوذ مورد نیاز باشند استفاده نمی‌کنند.

امنیت تلفن همراه برای کمک به دفاع در برابر APTها استفاده بسیار کمی را نشان می‌دهد علیرغم این واقعیت که ۸۷/۳ ٪ پاسخ دهندگان BYOD با rooting و jailbreakingرا در احتمال یک حمله کافی شناختند.

۷-۶ تاثیر APT بر سیاست ها و تمرینات

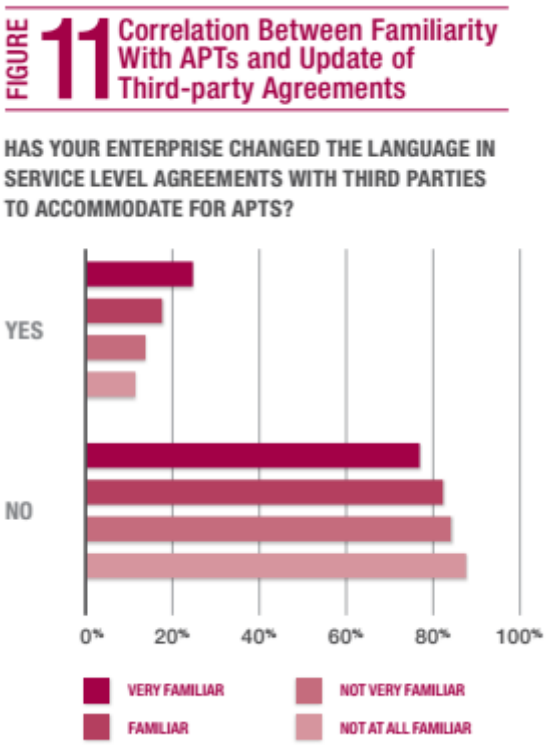
تهدید حمله APT بسیاری رویکردهای دفاعی از جمله کنترل‌های تخصصی، تغییرات در آموزش آگاهی منابع انسانی و به روز رسانی‌های توافقات شخص ثالث را فرا می‌خواند. یکی دیگر از مسائلی که در این ارزیابی بررسی شد، تاثیر تهدیدات APT بر سیاست‌های شرکت و آموزش‌ها و روش‌های مدیریت اجرایی برای استراتژی‌های امنیت سایبری است.

۷-۶-۱ مدیریت فروشنده

مدیریت فروشنده یک عامل مهم برای محافظت از داده‌هایی با منبع خارجی است. بنابراین این ارزیابی، روابط موجود با اشخاص ثالث را بررسی کرد تا تعیین کند که آیا شرکت‌ها زبان قرارداد یا توافقات سطح خدمات (service level agreements) (SLAs) را تنظیم می‌کنند تا اطمینان حاصل کنند که اشخاص ثالث برای تلاش مداوم به منظور محافظت از خود در برابر APTها و در صورت نیاز به جبران مالی در شرایطی که علیرغم کنترل‌ها مورد حمله قرار گرفته‌اند و منجر به آسیب به مشتری شده است، آموزش دیده‌اند.

به طور کلی ۸۱/۸ ٪ از پاسخ دهندگان توافقات با اشخاص ثالث را برای محافظت در برابر APTبه روز رسانی نکرده‌اند، درصدی که به ویژه در حالی که بیش از دو سوم پاسخ دهندگان (۶۷/۶ ٪) آشنایی باAPTها را اذعان کرده‌اند شگفت انگیز است. شکل ۱۱ چگونگی وضعیت آگاهی از APTها و به روز رسانی توافقات اشخاص ثالث را نشان می‌دهد.

۸۲ ٪ پاسخ دهندگان توافقات با اشخاص ثالث را برای محافظت در برابر APTها به روز رسانی نکرده‌اند.



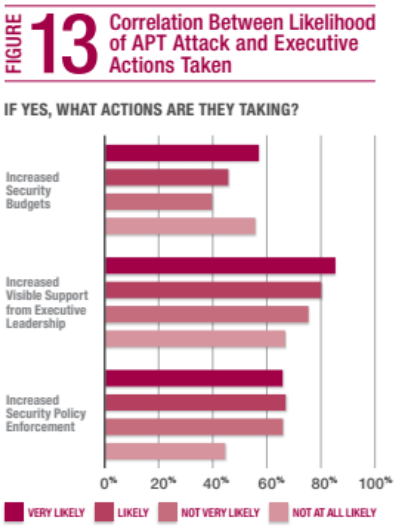
۷-۶-۲ مشارکت مدیران

با توجه افزایش توجه به APTها در سال‌های اخیر، انتظار می رود که مدیران در فعالیت‌های امنیت سایبری بیشتر مشارکت کنند. از پاسخ دهندگان به این پرسشنامه خواسته شد تا مشخص کنند که متوجه تغییری در فعالیت مدیر در شرکت شده‌اند. به طور مشابه با سایر یافته‌هادر این تحقیق، یک رابطه بین درک احتمال هدف قرار گرفتن شرکت و میزان مشارکت مدیر وجود داشت، به گونه‌ای که احتمال بیشتر هدف قرار گرفتن شرکت، افزایش مشارکت مدیر و احتمال کمتر،کاهش مشارکت مدیر را درپی داشت (شکل ۱۲).

از کسانی که افزایش مشارکت مدیر را در استراتژی‌های امنیتی مشاهده کردند درباره انواع فعالیت‌های خاصی که مدیران در آن مشارکت داشتند پرسیده شد. با توجه به لیستی از فعالیت‌های ممکن که شامل افزایش بودجه‌های امنیتی، افزایش حمایت واضح از مدیران ارشد، و افزایش اجرای سیاست‌ها بود، اکثریت (۷۹/۸ ٪) شاهد افزایش حمایت از مدیران ارشد بودند، در حالی که ۶۶ ٪ شاهد افزایش اجرای سیاست‌ها بودند. کمتر از نیمی (۴۶/۹ ٪) افزایش در بودجه امنیتی را تجربه کرده بودند.

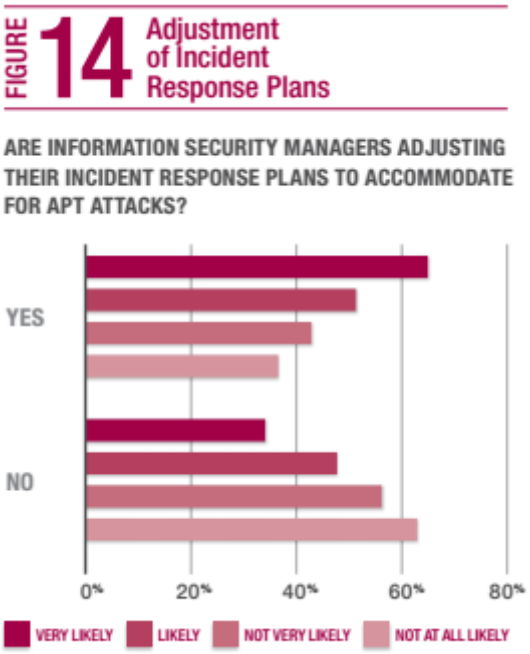
با این حال هنگامی که پاسخ‌ها با توجه به احتمال اینکه شرکت هدف APT قرار گیرد فیلتر شوند، اعداد تغییر می‌کنند(شکل ۱۳).

جالب است که بیشترین وقوع افزایش بودجه‌های امنیتی نه تنها در شرکت‌هایی که احتمال بالایی برای این که هدف APTها قرار گیرند می‌دهند، بلکه در شرکت‌هایی که اصلا این احتمال را نمی‌دهند نیز رخ می‌دهد. به همین ترتیب، افزایش اجرای سیاست در شرکت‌هایی که زیاد محتمل حمله نیستند (۶۵/۹ ٪) با نرخ‌های مشابه شرکت‌های با احتمال بالای حمله (۶۵/۸ ٪) رخ می‌دهد.



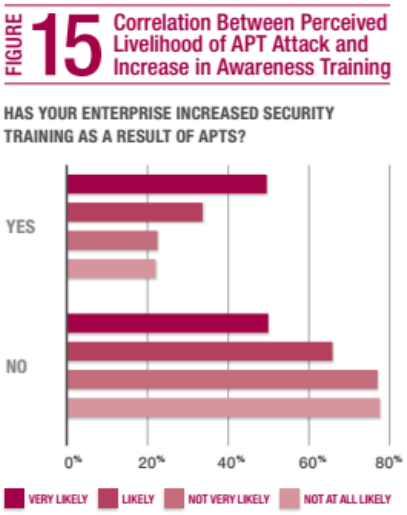
۷-۶-۳ مدیریت حادثه و آموزش آگاهی

مدیریت یک حمله APT همیشه به سادگی حذف تهدید نیست. بسیاری از APTها قابل انطباق هستند و قادر به تغییر برای تطابق با موقعیت هستند. طرح های واکنش به حادثه معمول که برای متوقف و اصلاح کردن طراحی شده‌اند ممکن است برای یکAPT مناسب نباشند. این طرح‌ها باید مورد بررسی قرار گیرند و الحاق مقررات خاصی برای APTها در نظر گرفته شود. این پرسشنامه نشان می‌دهد که بسیاری از پاسخ دهندگان شروعی در این زمینه داشته‌اند: بیش از نیمی از پاسخ دهندگانی که اعتقاد داشتند شرکتشان هدف احتمالی APT است، بر این باور بودند که طرح‌های مدیریت حادثه موجود ممکن است نیاز به اصلاح داشته باشند (شکل ۱۴).



متاسفانه، چنین باوری برای آموزش آگاهی کاربر وجود ندارد. به طور کلی، ۶۷/۳ ٪ از پاسخ دهندگان گزارش کردند که آموزش آگاهی نسبت به APT را افزایش نداده‌اند. درصدها برای شرکت‌هایی که خود را برای حمله APT "بسیار محتمل" یا "محتمل" می‌دانستند کمیافزایش می‌یابد، اما حتی دراین موارد، کمتر از نیمی آموزش آگاهی را افزایش دادند (شکل ۱۵).

۶۷ ٪ از پاسخ دهندگان گزارش کردند که آموزش آگاهی نسبت به APT را افزایش نداده‌اند.



این نظرسنجی نتایج مثبت بسیاری را نشان داد. به نظر می‌رسد متخصصان زمینه امنیت شرکت کننده، مدیریت امنیت خوبی را با استفاده از یک رویکرد بر پایه ریسک برای مدیریت APTها در شرکتشان تمرین می‌کنند.

در طول این تحقیق نشان داده شد که شرکت‌هایی که خود را با احتمال بیشتری در معرض تجربه APT می‌دانند، برای مدیریت امنیت شرکتشان یک رویکرد لایه‌ای اتخاذ کرده‌اند. تقریباً در همه موارد، هر چه درک احتمال هدف قرار گرفتن بیشتر باشد، توجه بیشتری به APTها از طرف مدیران و از لحاظ تکنولوژی، آموزش آگاهی، مدیریت فروشنده و مدیریت حادثه می‌شود. این فعالیت و تلاش مرتبط با آن برای حفاظت از اطلاعات عالی هستند.

با این حال APTها در بازار جدید هستند. آن‌ها با تهدیدهای سنتی متفاوت هستند و باید به عنوان یک دسته متفاوت از تهدید در نظر گرفته شوند. هنوز بین فهم اینکه APTها چه هستند و چگونه باید در مقابل آن‌ها دفاع کرد یک شکاف وجود دارد. این مورد توسط تعدادی از پاسخ دهندگان که با APTها حداقل آشنایی دارند (۶۷/۶ ٪) در مقایسه با کسانی که احساس می‌کنند APTها به تهدیدهای سنتی شبیه هستند (۵۳/۴ ٪) نشان داده شده است.

داده‌های بیشتر نشان می‌دهد که بازار روش‌های محافظت در برابر APTها را واقعاً تغییر نداده است. کنترل-های تخصصی که بیشتر برای استفاده به منظور حفاظت در مقابل APTها شناخته می‌شوند، تکنولوژی‌های محیط شبکه از قبیل فایروال‌ها و لیست‌های دسترسی در routerها و همچنین ضد بدافزارها و ضد ویروس‌ها می‌باشند.

در حالی که این کنترل‌ها برای دفاع در برابر حمله‌های سنتی کارآمد هستند، احتمالاً برای جلوگیری از APTها مناسب نیستند. این به دلایلی درست می‌باشد: APTها از تهدیدات zero-day که اغلب آسیب-پذیری‌های ناشناخته‌ای هستند بهره می‌برند و بسیاری از APTها از طریق حملات spear phishing که به

خوبی طراحی شده‌اند وارد شرکت می‌شوند. این نشان می‌دهد که کنترل‌های اضافی از قبیل تقسیم بندی شبکه و افزایش تمرکز بر امنیت ایمیل و آموزش کاربران می‌تواند مفید باشد. علاوه بر این، کمبود توجه به اشخاص ثالث نگران کننده است. شرکت‌ها باید اطمینان داشته باشند که داده‌های با منبع خارجیشان محافظت می‌شود حتی اگر خود تامین کننده یک حمله را تجربه کند.

در نهایت ۷۹/۱ ٪ از پاسخ دهندگان خاطر نشان کردند که در بازار متمرکز بر APT کمبود راهنمایی وجود دارد. ISACA به عنوان بخشی از تلاش مستمر خود برای خدمت به اعضای خود و دیگر مشتریان، مجموعه‌ای از محصولات را برای نشان دادن چالش‌های امنیت سایبری ایجاد کرده است، که یکی از مولفه‌های آن بر APTها تمرکز خواهد داشت.

۸ سابقه حملات APT در ایران

۸–۱ حمله BlackOasis

در تاریخ ۱۰ اکتبر ۲۰۱۷، سیستم های پیشگیری آزمایشگاه کسپرسکی آسیب‌پذیری روز صفر جدیدی در نرم‌افزار Adobe Flash که بر علیه کاربران استفاده می شد را شناسایی کرد. این حمله از طریق فایل‌های مایکروسافت منتشر شده و در نهایت حامل آخرین نمونه بدافزار FinSpy می باشد. پس از شناسایی و ارائه شناسه CVE-۲۰۱۷-۱۱۲۹۲ به آسیب‌پذیری مذکور، شرکت Adobe وصله امنیتی برای این نقص فنی ارائه کرد.

فعالیت های BlackOasis برای اولین بار در می ۲۰۱۶، در حین تحقیق در مورد آسیب‌پذیری روز صفر دیگری در نرم‌افزار Adobe Flash مشاهده شد. در تاریخ دهم می ۲۰۱۶، Adobe در مورد آسیب پذیری (CVE-۲۰۱۶-۴۱۱۷) که Flash Player ۲۱.۰.۰.۲۲۶ و ورژن های قبلی Windows، Macintosh، Linux و Chrome OS را تحت تاثیر قرار میدهد هشدار داد.

پس از بررسی‌های صورت گرفته مشخص شد که این آسیب‌پذیری توسط مهاجمی به نام BlackOasis توسعه داده‌شده است. بررسی‌ها نشان می‌دهد مهاجم پس از بهره‌برداری از این آسیب‌پذیری فعالیت مخرب خود را اجرا می کند. مهاجم با استفاده از بدافزار FinSpy در حملات خود فعالیت سرور را تحت نظر قرار می‌دهد.

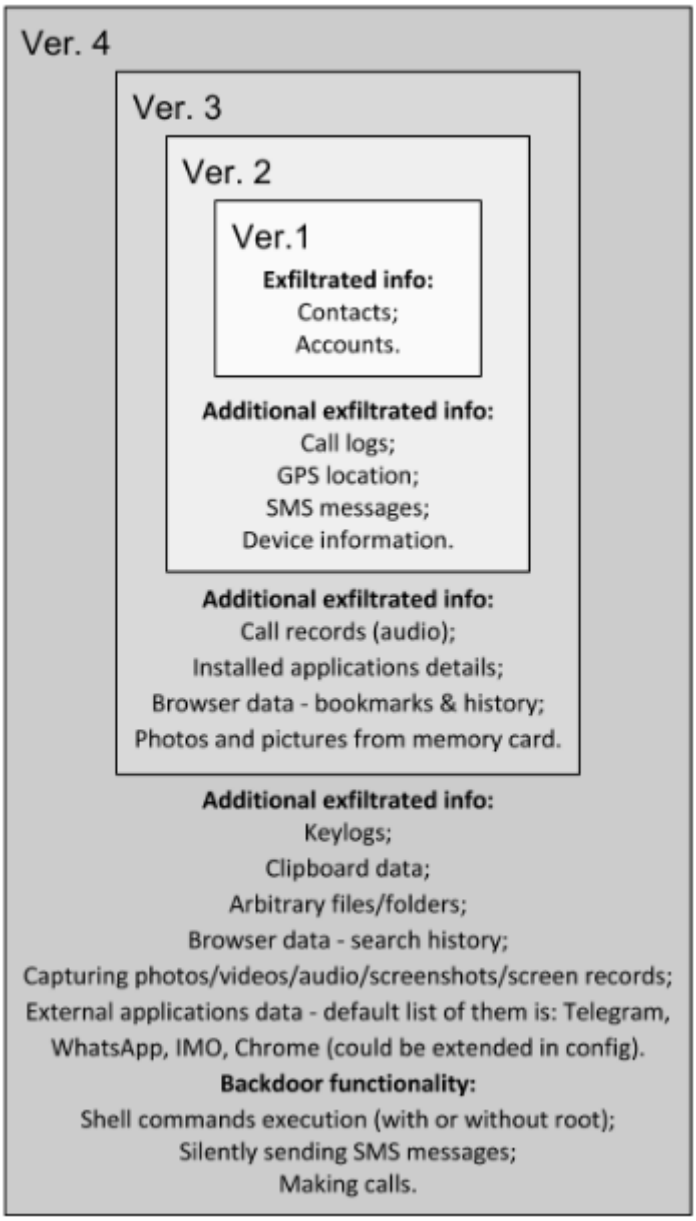
بهره‌برداری از این قابلیت فقط با استفاده از آسیب‌پذیری موجود در حافظه صورت می‌گیرد که در کلاس com.adobe.tvsdk.mediacore.BufferControlParameters قرار دارد این در حالتی است که در صورت

موفقیت‌آمیز بودن بهره‌برداری توسط مهاجم، عملیات خواندن و نوشتن اجرا می‌شود و در مرحله دوم مهاجم به اجرای یک shellcode برای پیش برد اهداف خود استفاده می‌کند.

۸-۲ حمله ZooPark

گروه جاسوسی سایبری APT با نام ZooPark از سال ۲۰۱۵ فعالیت خود را آغاز کرده و در طی سال ها به پیچیدگی خود افزوده است.

محققان عملیات های گذشته ی این گروه را بر اساس بدافزاری که در حملات خود استفاده کرده اند به چهار دوره تقسیم کرده اند.



- **فاز اول(۲۰۱۵)**

مهاجمان از بدافزار بسیار ساده ای استفاده کرده اند که فقط قادر به انجام دو کار بود: سرقت جزئیات حسابی که در دستگاه قربانی ذخیره شده است و سرقت آدرس ها و اطلاعات مخاطبین. در این مرحله مهاجمین اپلیکشن خود را به عنوان اپلیکیشن رسمی تلگرام مخفی می کردند.

- **فاز دوم(۲۰۱۶)**

بدافزار مورد استفاده پیشرفت می کند، قابلیت های جدید آن نشان می دهد که این بدافزار برای جاسوسی بوده است.

- **فاز سوم(۲۰۱۶)**

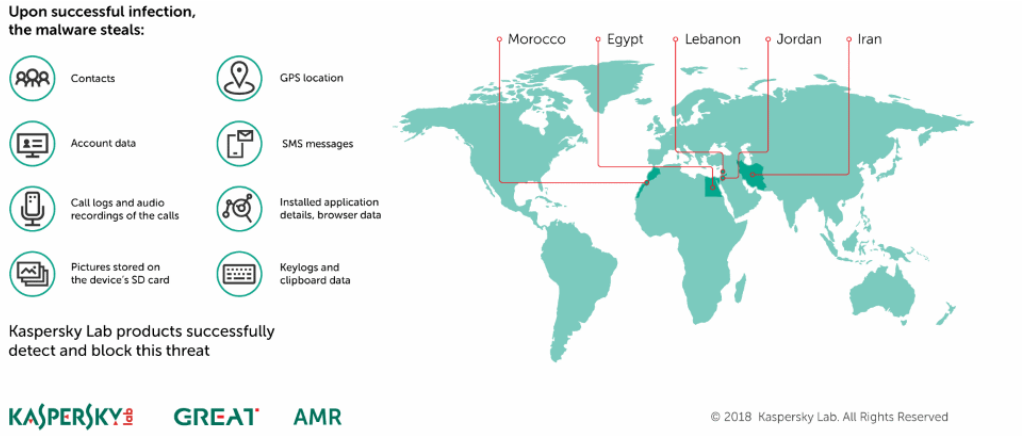
این گروه متوجه می شود که با وجود تلاش های فراوان، بدافزار همچنان توسعه ی چندانی نداشته است. آن‌ها از نمونه ای از اپلیکیشن بدافزار جاسوسی تجاری Spymaster Pro استفاده می کنند تا آن را با بدافزار خود ترکیب کنند.

- **فاز چهارم(۲۰۱۷)**

در این فاز بدافزار ZooPark تغییرات زیادی می کند. تغییرات اضافه شده در فاز سوم حذف می شوند و قابلیت ها و مولفه های جدیدی بر پایه کد فاز دوم، اضافه می شود.

دررابطه با روش انتشار، ZooPark از روش های ساده ای استفاده می کند. یکی از روش ها ساختن کانال های تلگرامی است که لینک اپلیکیشن بدافزار را به اشتراک می گذارد. راه دیگر آن آلوده کردن سایت های معتبر است به گونه این که افرادی که قصد ورود به سایت را دارند را به صفحات دیگری هدایت میکند که اپلیکیشن های آلوده را برای دانلود پیشنهاد می دهد.

این حمله در کشور های مراکش، مصر، لبنان، اردن و ایران انتشار یافته است.



۳-۸ حمله Satellite Turla

گروهی از نفوذگران توانستند با سوءاستفاده از ارتباطات ماهواره‌ای موقعیت مکانی و فعالیت‌های خود را از دید سایرین مخفی کنند. یک گروه جاسوسی سایبری روسی‌زبان، که از بدافزار Turla سوءاستفاده می‌کند، از ماهواره‌ها برای رسیدن به سطح بالاتری از ناشناس‌ماندن استفاده می‌نماید. این گروه از ضعف‌های امنیتی موجود در شبکه‌های ماهواره‌ای جهانی سود می‌برد.

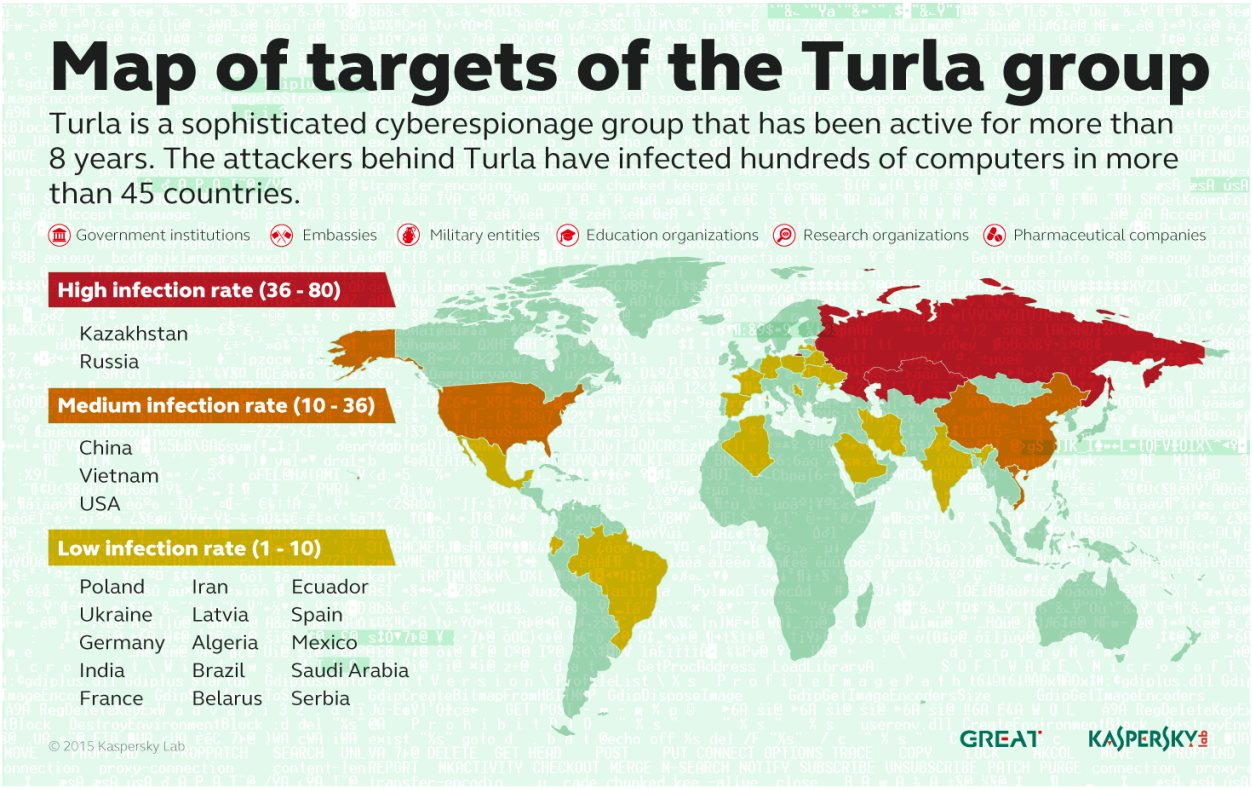
Turla یکی از گروه‌های جاسوسی سایبری پیچیده است که بیش از ۱۰ سال از فعالیت آن می‌گذرد، این بدافزار صدها رایانه را در بیش از ۴۵ کشور اعم از قزاقستان، روسیه، چین، ویتنام، و آمریکا آلوده کرده است. مؤسسات دولتی و سفارت‌خانه‌ها، و نیز شرکت‌های نظامی، آموزشی، پژوهشی و دارویی دست کم یک بار مورد اصابت حملات گروه پیشرفته‌ی Turla قرار گرفته‌اند.

علت خاص بودن Trula فقط پیچیدگی ابزارهای آن که شامل Oroburos rootkit یا "Snake" می شود، یا مکانیزم های طراحی شده برای کنار گذاشتن air gap[۹] ها شبکه های چند مرحله ای proxy در LAN ها نیست، بلکه مکانیزم دقیق و بدیع C&C بر اساس ماهواره ای است که در مراحل بعدی حمله استفاده می شود.

مکانیزم های C&C مبنی بر ماهواره ای که گروه های APT مانند Turla\Snake برای کنترل مهم ترین قربانیان خود استفاده می کنند باید به صورت دقیق تری مورد بررسی قرار گیرد. همان گونه که استفاده از این مکانیزم ها روز به روز محبوب تر می شود، مهم است که استراتژی دفاعی صحیحی برای مقابله با این حملات به کار گرفته شود.

---

[۹] Air gap: لایه ای از امنیت شبکه ای است بر روی یک یا بیش از یک کامپیوتر که آن ها را از کامپیوتر های غیر امن مانند اینترنت عمومی به صورت فیزیکی دور می کند.



۴-۸ حمله Penquin Turla: بدافزار Turla\Snake\Oroburos برای Linux

این بدافزار نمونه ی مخرب جالبی بود که بر روی یک سرویس چند اسکنر آپلود شد. این موضوع مورد توجه قرار گرفت زیرا نشان دهنده ی قسمتی از یک پازل بزرگ تر بود. این پازل همان Turla یکی از بزرگترین APT ها در جهان است.

تمام نمونه های مشاهده شده Turla برای سیستم عامل های ۳۲ و ۶۴ بیتی خانواده Microsoft Windows طراحی شده بودند ولی این نمونه ی اولین نمونه ی Turla ی کشف شده بود که سیستم عامل Linux را مورد هدف قرار می داد.

مولفه ی جدید Turla برای پشتیبانی سیستم گسترده تر به منظور حمله به سامانه‌های لینوکسی استفاده می‌شود. ماژول لینوکس Turla یک ماژول اجرایی C\C++ است که به صورت استاتیک با چند library لینک شده است، این اتصال باعث افزایش زیاد حجم فایل شده است. مانند دیگر نسخه‌های Turla، تابع‌های Penquin Turla، شامل ارتباط‌های شبکه‌ای مخفیانه، دسترسی از راه دور و اجرای کد از راه دور می‌شود. از ویژگی مهم Penquin عدم نیاز به سطح دسترسی بالا برای اجرای کدها است. هم‌چنین شناسایی این بدافزار دشوار است.

۸-۵ حمله Lazarus

آغاز فعالیت گروه Lazarus در سال ۲۰۱۱ بوده و فعالیت های آن حتی بعد از انتشار گزارشاتی مانند Operation Blockbuster توسط Novetta متوقف نشد. حملات Lazarus محدود به یک منطقه نیست بلکه عملیات های این گروه در سرتاسر جهان اتفاق می افتد. فعالیت های Lazarus اصولا به صورت جاسوسی و خرابکاری سایبری می باشد. مانند حمله بر Sony Pictures Entertainment که در نتیجه ی آن مقدار زیادی از اطلاعات داخلی آن به بیرون درز کرد و تعدادی از هارددیسک های سیستم های آن پاک شد. اما علاقه ی آن ها به سود مالی و اقتصادی امری است که نسبت به سن این گروه تازگی دارد.

صد ها نمونه ی جمع آوری شده نشان می دهد که Lazarus به کارخانه ای از بدافزار شباهت دارد که بر روی نوار نقاله های جداگانه نمونه های جدید تولید می کند.

سطح پیچیدگی این گروه در دنیای مجرمان سایبری منحصربفرد است. زیرا نیازمند سازمان دهی سخت گیرانه و کنترل بر تمامی مراحل عملیات است. البته این پروسه نیازمند سرمایه زیادی است، که می تواند دلیل ظهور زیرگروه Bluenorof در گروه Lazarus شود.

حمله ی Watering Hole بر علیه بانک های لهستانی نمونه ای از فعالیت های Bluenorof است که تنها مورد، میان تعداد زیادی موارد مشابه است که توسط رسانه ها پوشش داده شد. این حمله ی Watering Hole[۱۰] در سال ۲۰۱۶ بعد از اختلال در عملیات آن ها در جنوب شرقی آسیا آغاز شد. Lazarus/Bluenorof با همکاری هم به سراغ کشور های فقیرتر و کمتر توسعه یافته و بانک های کوچک تر رفتند.

تا به امروز حملات Bluenorof بر علیه چهار نوع اصلی از هدف ها بوده است:

- موسسه های مالی و اقتصادی
- کازینو ها
- کمپانی هایی که به توسعه ی نرم افزار های تجارت مالی می پردازند
- تجارت های crypto-currency

موج حمله گروه Lazarus به چندین آلودگی در سراسر جهان از جمله ایران انجامید.

---

[۱۰]: Watering Hole Attack استراتژی حمله ی کامپیوتری که در آن سایت هایی که مکررا توسط گروه قربانی استفاده می شوند توسط بدافزار آلوده می شوند، تا در نهایت بعضی از اعضای این گروه آلوده شوند.

بیشتر ابزار های استفاده شده توسط گروه Lazarus، در صورت از دست رفتن و غیر قابل استفاده بودن می توانند به راحتی توسط نسل جدیدی از ابزار ها جایگزین شوند. Lazarus از استفاده دوباره از ابزار ها، کد ها، و الگوریتم های مشابه به حملات گذشته خودداری می کنند و همواره در حال تغییر هستند، و اگر در دو مورد جداگانه از یک ابزار استفاده شود به دلیل وسعت این گروه است؛ قسمت های جداگانه و دور از هم از فعالیت های یک دیگر مطلع نیستند.

Bluenorof که یک زیرگروه از Lazarus است فقط بر روی حملات با سودآوری مالی تمرکز می کند. این گروه دارای مهارت های مهندسی معکوس است. برای سرقت مقادیر زیاد پول آن ها اول نرم افزار های معتبر را تکه تکه کرده وpatch ای از نرم افزار اتحاد SWIFT[۱۱] در آن اعمال می کنند.

[۱۱] SWIFT Alliance Software

یکی از استراتژی های معمول Bluenorof ادغام شدن در پروسه های در حال اجرا بدون متوقف کردن آن هاست. هدف آن ها سرقت پول بدون کشف شدن و به جا گذاشتن رد است.

حملات بر اساس آسیب پذیری نرم افزار SWIFT نبوده بلکه بر زیرساخت و کارکنان بانک ها تمرکز کرده و از آسیب پذیری نرم افزار ها و وب سایت هایی که مکررا مورد استفاده بوده اند استفاده کرده است.

۸-۶ حمله DuQu

DuQu که یک بدافزار پیچیده است که سازندگان ابزار های صنعتی را مورد هدف قرار می دهد. این بدافزار توسط همان افرادی نوشته شده که کرم بدنام Stuxnet را نوشتند. هدف اصلی آن این است که به عنوان یک درب پشتی در سیستم عمل کند و اطلاعاتی را از آن جمع آوری کند، در حالی که Stuxnet برای خرابکاری صنعتی طراحی شده بود. همچنین برخلاف Stuxnet، DuQu قابلیت انتقال خود به کامپیوتر های دیگر را ندارد.

وجه اشتراک DuQu و Stuxnet در کلید های رمزگذاری استفاده شده در آن است که شامل کلید هایی نیز می باشد که در دسترس عموم قرار داده نشد.

برای اولین بار این بدافزار در اوایل آوریل ۲۰۱۱ دیده شد و تا هجدهم اکتبر که اخبار مربوط به آن برای عموم منتشر شد به حملات خود ادامه داد.

حداقل هفت نمونه مختلف آن وجود دارد که با نام های متفاوت توسط شرکت های آنتی ویروس مختلف ردیابی شده اند. تا به حال دو مولفه برای سرقت اطلاعات و هفت درایور مشاهده شده است.

DuQu با استفاده از یک سند آفیس که از آسیب پذیری CVE-۲۰۱۱-۳۴۰۲ استفاده می کند کامپیوتر کاربران را آلوده می کرد.

بدافزار Duqu سیستم‌های مدیریت صنعتی را هدف قرار نداده و به آنها حمله نمی‌کند. بلکه فقط اقدام به جمع‌آوری اطلاعات از شرکت‌های سازنده این سیستم‌های مدیریت صنعتی می‌کند. هدف از جمع‌آوری و سرقت این اطلاعات نیز احتمالاً ساخت یک ویروس براساس اطلاعات و دانش به دست آمده است.

این بدافزار ابتدا اقدام به آلوده کردن کامپیوتر می‌کند. نحوه این آلودگی به روش‌های مختلف از جمله حافظه‌های USB و فریب از طریق مهندسی اجتماعی، گزارش شده است.

پس از آلوده کردن کامپیوتر، بدافزار با یک مرکز فرماندهی که در کشور هند است، تماس برقرار می‌کند. (در حال حاضر، این ارتباط قطع شده است.) از طریق این مرکز، دستورات جدید و انواع برنامه‌های مخرب دریافت شده و بر روی کامپیوتر قربانی به اجرا در می‌آید. همچنین اگر کامپیوتر آلوده، به شبکه وصل باشد، کل

شبکه توسط بدافزار برای شناسایی نقاط ضعف احتمالی، کنترل و بررسی شده و نتیجه به دست آمده به مرکز فرماندهی ارسال می‌شود.

در حال حاضر اهداف خاص بدافزار Duqu مشخص نیست. احتمال داده می‌شود که بدافزار در حال ایجاد بسترهای لازم برای انجام یک حمله خاص است. ساختار فعلی بدافزار Duqu هیچگونه امکانات حمله و تخریب ندارد ولی در هر لحظه می‌تواند از طریق ارتباط با مرکز فرماندهی، این نوع قابلیت‌ها را به دست آورد.

درباره قربانیان اصلی بدافزار Duqu اختلاف نظر وجود دارد. برخی معتقدند که این بدافزار برای حمله به مراکز صدور گواهینامه‌های دیجیتالی (Certificate Authority) طراحی شده و برخی دیگر، سیستم‌های مدیریت صنعتی خاصی را قربانی و هدف اصلی بدافزار Duqu می‌دانند.

۸-۷ حمله Wiper

در سال ۲۰۱۲ چندین داستان در رابطه با یک حمله ی بدافزار مرموز که سیستم های کامپیوتر را در تجارت ایران خاموش کرد منتشر شد. اما نمونه ای از این بدافزار پیدا نشد. به دنبال این اتفاقات به درخواست ITU[۱۲]، آزمایشگاه کسپرسکی به بررسی این واقعه پرداخت.

بعد از تحقیقات با تحلیل چند مورد که توسط Wiper به آن ها حمله شده بود مشخص شد که این بدافزار در آوریل ۲۰۱۲ وجود داشته است. موارد مشابه با آن نیز قبلاً در دسامبر ۲۰۱۱ مشاهده شده بود.

بدافزار مخرب Wiper(پاک کننده) قادر به نابود کردن داده‌ها از روی کامپیوتر قربانیان می باشد. همچنین با پاک کردن تمام اثرات مخرب و حمله خود را از صحنه پاک کرده و چیزی از خود بر جای نمی گذارد. تمامی دیتای قابل استفاده برای ردیابی بدافزار به دقت پاک می شود. در تمامی موارد تحلیل شده "تقریبا هیچ ردی" از آن به جا نمانده بود. پاک کردن دیسکی که صدها گیگابایت حجم دارد کار زمانبری است. سازندگان این بدافزار از الگوریتم های پاک کردنی استفاده کرده اند که بیشترین بازده را دارد. از آن جایی که هدف مهاجمان این بوده که این بدافزار کشف و ردیابی نشود، اولین فایل ها برای پاک شدن مولفه های بدافزار بودند، بعد از پاک شدن این فایل ها نوبت به فایل هایی می رسید که باعث در هم شکستن سیستم می شدند.

[۱۲] International Telecommunications Union

این بدافزار به قدری حرفه ای و با مهارت نوشته شده بود که هیچ دیتایی باقی نماند. حتی با وجود این که آثار وجود آلودگی مشاهده شد، این بدافزار همچنان ناشناخته است زیرا هیچ مورد دیگری که با Wiper خصوصیات مشترک داشته باشد دیده نشده است و هیچ ردی از آن در مولفه های ردیابی فعال راه حل های امنیتی یافت نشده است.

این بدافزار در انجام عملیات خود بسیار موثر بوده و باعث به وجود آمدن نمونه های تقلیدی مانند Shamoon شد. همچنین این نکته قابل توجه است که استفاده از Wiper برای پاک کردن چند سیستم معدود باعث ردیابی و کشف کمپین جاسوسی سایبری چهار تا پنج ساله ی Flame شد.

۸-۸ حمله Regin

Regin نام حملهی بدافزاری است که در یکی از ارائه های آزمایشگاه کسپرسکی در رابطه با DuQu توسط شخص سومی به دلیل شباهت آن با برخی از جنبه های بدافزار DuQu به آن اشاره شد. Regin نامی است که در بسیاری از آژانس های مدیریت امنیت در سرتاسر دنیا باعث ترس و وحشت می شود. حدود دو سال است که به ردیابی این بدافزار پرداخته شده است. هر چند وقت یک بار نمونه هایی از آن در سرویس های چند اسکنر یافت می شوند. اما هیچ ارتباطی بین آن ها پیدا نشده است. نمی توان مشخص کرد که اولین نمونه ی Regin مربوط به چه زمانی بوده است اما اولین تاریخ کشف شده به سال ۲۰۰۳ باز می گردد.

قربانی های Regin به صورت زیر طبقه بندی می شوند:

- اپراتورهای مخابراتی
- نهادهای سیاسی چند ملیتی
- موسسات مالی و اقتصادی
- موسسات تحقیقاتی
- افراد درگیر در تحقیقات پیشرفته ریاضی / رمزنگاری

تا به حال دو هدف اصلی این مهاجمین مشخص شده است:

- جمع آوری اطلاعات
- تسهیل کردن انواع دیگر حملات

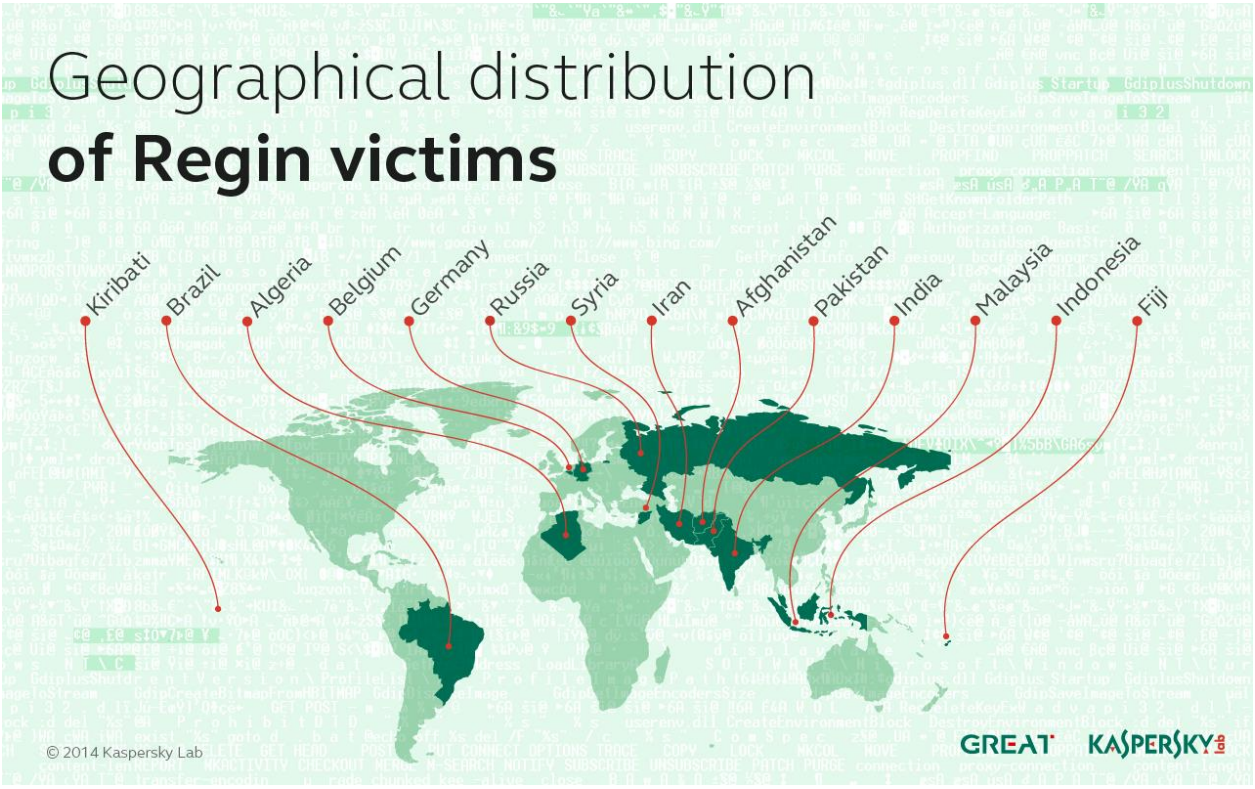
در حالی که در اغلب موارد مهاجمان بر روی استخراج اطلاعات حساس مانند ایمیل و اسناد متمرکز شده اند، مواردی مشاهده شده است که مهاجمان از اپراتورهای مخابراتی آلوده شده استفاده کرده اند تا امکان حملات پیچیده اضافه تری را فراهم کنند. قربانی قابل توجه Regin کامپیوتری به نام "آهن ربای تهدیدات[۱۳]" است. این سیستم متعلق به یک موسسه ی تحقیقاتی است و توسط Turla, Mask/Careto, Regin, Itaduke, Animal Farm و چند تهدید پیشرفته ی دیگر که نام عمومی ندارند مورد حمله قرار گرفته است. همه ی این ها در نقطه ای از زمان بر روی همین کامپیوتر هم زیستی داشته اند.

به طور خلاصه، Regin یک پلتفرم حمله سایبری است که مهاجمان در شبکه های قربانی برای بیشترین کنترل از راه دور، در تمام سطوح ممکن استفاده می کنند.

در طول دو سال گذشته، آمار مربوط به حملات و قربانیان Regin جمع آوری شده است. تا کنون قربانیان Regin در چهارده کشور شناسایی شده اند:

- الجزایر
- افغانستان
- بلژیک
- برزیل
- فیجی
- آلمان
- ایران
- هندوستان
- اندونزی
- کیریباتی
- مالزی
- پاکستان
- روسیه
- سوریه

[۱۳] The Magnet of Threats



در مجموع، بیست و هفت قربانی مختلف شناسایی شده است، اگر چه باید اشاره کرد که تعریف قربانی در اینجا به یک نهاد کامل، از جمله کل شبکه آن اشاره دارد. تعدادی از PC های منحصر به فرد آلوده به Regin بسیار، بسیار بالاتر است.

نام Regin معکوس شده عبارت "Reg In" به معنای "Registry" است زیرا این بدافزار می تواند ماژول های خود را در رجیستری ذخیره کند.

از برخی نظر ها، این پلتفرم به یادآوری بدافزار پیشرفته ی دیگری می انجامد: Turla. بعضی از شباهت ها شامل استفاده از سیستم های فایل مجازی و استفاده از drone های ارتباطی می باشد تا شبکه ها را به هم متصل کنند. با این وجود از طریق اعمال آنها، روش های کدگذاری، پلاگین ها، تکنیک های پنهان نگاری و انعطاف پذیری، Regin از Turla به عنوان یکی از پیچیده ترین پلتفرم های حمله ای که تا کنون تحلیل کرده است، پیشی می گیرد.

توانایی این گروه برای نفوذ و نظارت بر شبکه های GSM شاید جنبه غیر معمول و جالب این عملیات باشد. در دنیای امروز، ما بیش از پیش وابسته به شبکه های تلفن همراه شده ایم که به پروتکل های ارتباطی بسیار قدیمی پایبند هستند که در نتیجه ی آن امنیت بسیار کمی برای کاربر نهایی وجود دارد.

۸-۹ حمله BlackEnergy

موجی از حملات سایبری به چندین بخش بحرانی و حساس در اوکراین ضربه زد. این حملات به طور گسترده در رسانه ها مورد بحث قرار گرفت، حملات با استفاده از تروجان شناخته شده BlackEnergy و همچنین چندین ماژول جدید بود. اقدامات مخرب در دستور کار اصلی BlackEnergy قرار دارد، به علاوه ی فعالیت های جاسوسی و تحت خطر قرار دادن تاسیسات کنترل صنعتی.

BlackEnergy یک بدافزار است که توسط یک هکر به نام Cr۴sh ایجاد شده است. در سال ۲۰۰۷، او کار بر روی آن را متوقف کرده و کد منبع را به مبلغ ۷۰۰ دلار فروخت. به نظر می رسد کد منبع توسط یکی از بازیگران تهدید انتخاب شده است و برای انجام حملات DDoS علیه گرجستان در سال ۲۰۰۸ مورد استفاده قرار گرفت.

از سال ۲۰۱۱ میلادی، بسیاری از شرکت هایی که از سامانه های کنترل صنعتی استفاده می کنند و به اینترنت متصل هستند، مورد حمله بدافزاری به نام BlackEnergy قرار گرفته اند که با ایجاد یک درب پشتی دسترسی غیرمجاز به سیستم ها و ماشین های صنعتی داشته است.

چندین شرکت صنعتی که همکاری نزدیکی با گروه واکنش رخدادهای رایانه های آمریکا (US-CERT) دارند، بدافزار BlackEnergy را بر روی نرم افزار کاربردی HMI یا Human-Machine Interface در سامانه های کنترل صنعتی متصل به اینترنت خود یافته و شناسایی کرده اند.

HMI نوعی نرم افزار کاربردی است که یک صفحه رابط گرافیکی برای مدیریت و کنترل ماشین های صنعتی در اختیار کاربر می گذارد. این نوع نرم افزارها بخشی از سامانه SCADA یا Supervisory Control & Data Acquisition هستند که در محیط های صنعتی بکار می روند.

در حدود سال ۲۰۱۴، یک گروه خاص از مهاجمان BlackEnergy هنگامی که شروع به استفاده از پلاگین های وابسته به SCADA به قربانیان در بخش های ICS و انرژی در سراسر جهان کردند، توجه محققان را جلب کرد.

از اواسط سال ۲۰۱۵، یکی از بردار های حملات محبوب BlackEnergy در اوکراین، اسناد Excel با ماکروهایی است که اگر کاربر تصمیم بگیرد اسکریپت را در سند اجرا کند، تروجان را در دیسک قرار می دهد.

یک سند جدید را کشف شده است که به نظر می رسد بخشی از حملات گروه BlackEnergy APT در برابر اوکراین است. بر خلاف فایل های قبلی Office که در حملات قبلی استفاده می شود، این یک فایل Excel نیست، بلکه یک سند Microsoft Word است.

اسناد Office با ماکروها در اوائل دهه‌ی ۲۰۰۰، زمانی که Word و Excel از ماکروهای Autorun پشتیبانی می کردند، مشکل بزرگی بود. یعنی یک ویروس یا تروجان می توانست بر روی بارگذاری سند اجرا شود و به طور خودکار یک سیستم را آلوده کند. Microsoft بعدا این قابلیت را غیر فعال کرد و نسخه های فعلی Office به کاربر اجازه می دهد تا به طور خاص ماکروها را در سند فعال کند تا آنها را اجرا کنند. برای جلوگیری از این مانع، مهاجمان معمولا به مهندسی اجتماعی تکیه می کنند و از کاربر می خواهند که ماکرو را فعال کنند تا محتوای "افزایش یافته" را مشاهده کنند.

تجزیه و تحلیل نشان می دهد که بخش های زیر در سال های اخیر به طور فعال مورد هدف قرار گرفته اند:

ICS، انرژی، دولت و رسانه ها در اوکراین

- شرکت های ICS / SCADA در سراسر جهان
- شرکت های انرژی در سراسر جهان

۸-۱۰ حمله THE MASK

گروه PUNTA CANA-A که به احتمال زیاد توسط یک دولت ناشناخته ملی حمایت می شود، بیش از پنج سال است که نمایندگان دولتی، سفارتخانه ها، دفاتر های دیپلماتیک و شرکت های انرژی را هدف قرار داده اند و محققان کسپرسکی آن را پیشرفته ترین APT که تاکنون دیده اند می نامند.

این تهدید Careto یا MASK نامیده می شود که ظاهرا ترجمه ی آن از زبان اسپانیایی "صورت زشت" یا "ماسک" است.

این کمپین نگران کننده است زیرا به وضوح نشان می دهد که مهاجمان فوق العاده ماهرانه در حال یادگیری هستند، تجارتشان را اصلاح می کنند و به طور کلی در آلودگی، جاسوسی و سرقت از اهداف خاص مهارت و توانایی هایشان را افزایش می دهند. دلیل دیگر این نگرانی این است که حمله MASK بدون کشف شدن و جلب توجه از سال ۲۰۰۷ وجود داشته است و بی سر و صدا اطلاعات حساس را به دست می آورده است. این حمله زمانی کشف شد که مهاجمان سعی کردند از آسیب پذیری های یکی از محصولات قدیمی کسپرسکی استفاده کنند.

Costin Raiu، مدیر گروه تحقیقات و تحلیل جهانی این شرکت می گوید که استفاده از آسیب پذیری های محصولات کسپرسکی بسیار غیر عاقلانه است.

با این حال، کمپین های بسیار پیشرفته APT مانند The Mask، عموما طراحی شده اند تا سیستم های افرادی را که به شبکه های بسیار خاص دسترسی دارند، آلوده کنند، که در بیشتر موارد از سازمان های دولتی و شرکت های انرژی است. به عبارت دیگر، مهاجمان به اکثریت افراد نسبتا عادی علاقه مند نیستند.

یک نگرانی دیگر این است که هر کسی که مسئول این کمپین است، تنها چند ساعت پس از آنکه گروه تحقیقات و تحلیل جهانی کسپرسکی پیش نمایشی از کمپین APT را منتشر کرد، آن را تعطیل کرد. با این حال، اگر مهاجمان بخواهند می توانند عملیات را دوباره و به سرعت راه اندازی و اجرا کنند.

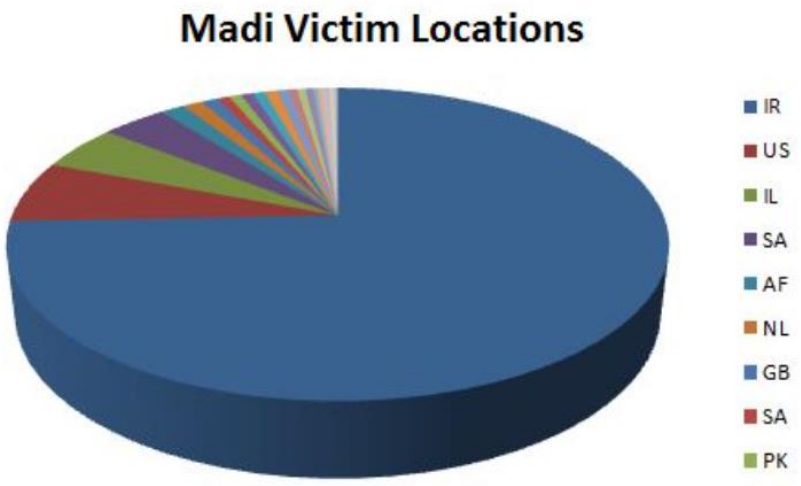
The Mask به دلایل مختلف قابل توجه است. اولا، به نظر نمی رسد که هیچ ارتباطی با چین داشته باشد، جایی که ادعا می شود بسیاری از این نوع حملات در آن به وجود آمده است. این نیز جالب است که افرادی که این کمپین را هدایت می کنند، به نظر می رسد اسپانیایی زبان هستند، که مطمئنا اتفاق تازه ای است، اما کاملا تعجب آور نیست، زیرا ۴۰۰ میلیون فرد اسپانیایی زبان در جهان وجود دارد. اهداف حملات The Mask نیز عمدتا اسپانیایی هستند اما در بیش از ۳۰ کشور گسترش یافته اند.

گفته شده است که این گروه حداقل یک آسیب پذیری روز صفر و نسخه های بدافزار Mask برای هدف قرار دادن ماشین هایی تحتMac OS X، لینوکس و شاید حتی دستگاه های تلفن همراه iOS و Android را در انبار مهمات خود دارد.

همانطور که در اغلب موارد مشاهده می شود، مهاجمان مخرب قربانیان خود را با ایمیل های spear-phishin مورد هدف قرار دادند که به وب سایت های مخرب که در آن exploit ها میزبانی شده بود هدایت می شود. این سایت ها در واقع پر شده از exploit ها است و فقط از طریق لینک مستقیم که مهاجمان به قربانیان ارسال می کنند، قابل دسترسی هستند.

۸-۱۱ حمله MADI

حدود یک سال است که یک کمپین در حال پیشرفت برای نفوذ به سیستم های کامپیوتری در خاورمیانه، افرادی را در ایران، اسرائیل، افغانستان و هم چنین در نقاط دیگر در سراسر جهان را مورد هدف قرار داده است.



بعد از تحقیقات کامل در مورد این عملیات و با توجه به رشته حروف استفاده شده توسط مهاجمین آن را MADI نام گذاری کرده اند.

این کمپین از چند روش شناخته شده و ساده تر برای حمله استفاده کرده است، که اطلاعات کمی راجب آگاهی اینترنتی قربانیان نشان می دهد. حجم زیاد داده های جمع آوری نشان می دهد که تمرکز کمپین بر شرکت های مهندسی زیرساخت های بحرانی ، سازمان های دولتی، خانه های مالی و دانشگاه ها در خاورمیانه است.

مهاجمان مادی بیشتر به تکنیک های مهندسی اجتماعی برای توزیع نرم افزارهای جاسوسی خود متکی هستند.

اولین طرح از دو طرح مهندسی اجتماعی که گسترش فعالیت را برای این کمپین نظارتی امکان پذیر می کنند، استفاده از تصاویر جذاب و مضمون های گیج کننده است که در اسلاید های پاورپوینت نشان داده شده است که حاوی دانلودرهای تدوین شده تروجان Madi است.

یکی دیگر از اسلاید های پاورپوینت به نام Moses_pic۱.pps بیننده را از طریق یک سری از تصاویر آرامش بخش، با مضمون مذهبی، بیابان بی سر و صدا و تصاویر استوایی، کاربر را تشویق می کند تا payload را در سیستم خود اجرا کند.

برخی از دانلودر ها نیز اسناد را با محتوای اخبار خاورمیانه و موضوعات مذهبی باز می کنند.

درپشتی هایی که حدود ۸۰۰ سیستم قربانی را آلوده کرد، همه به زبان Delphi کدگذاری شده اند. این انتخاب بیشتر از برنامه نویسان تازه کار انتظار می رود یا توسعه دهندگان در برای انجام پروژه تحت دچار کمبود وقت هستند.

عملکرد درپشتی مشابه گزینه های موجود در ابزار configuration است:

- ثبت استفاده از کلید های کیبورد
- ضبط عکس در فواصل مشخص شده
  - ضبط تصاویر در فواصل مشخص شده، به طور انحصاری توسط یک رویداد مربوط به ارتباطات اتفاق می افتد. این رویداد ممکن است این باشد که قربانی با وب میل، یک مشتری IM یا سایت شبکه اجتماعی ارتباط برقرار می کند. این سایت های محرک ضبط تصویر عبارتند از: Gmail، Hotmail، ایمیل !Yahoo، ICQ، Skype، Google+، Facebook و غیره.
- به روز رسانی این در پشتی
- ضبط صدا به عنوان فایل .WAV و ذخیره برای آپلود
- بازیابی هر ترکیبی از ۲۷ نوع مختلف فایل های داده
- بازیابی ساختارهای دیسک
- حذف و اتصال

۸-۱۲ حمله EPIC TURLA

مهاجمان Epic Turla چند صد کامپیوتر را در بیش از ۴۵ کشور آلوده کرده اند. از جمله اهداف آن ها نهادهای دولتی، سفارتخانه ها، ارتش، آموزش و پرورش، تحقیقات و شرکت های دارویی می باشد. گفته می شود که حملات حداقل دو مورد سوء استفاده از آسیب پذیری روز صفر را انجام داده اند.

همچنین سوء استفاده از آسیب پذیری های قدیمی، تکنیک های مهندسی اجتماعی و استراتژی هایwatering hole در این حملات مشاهده شده است. درهای پشتی اولیه ای که در حملات Epic Turla استفاده می شود نیز به عناوین "WorldCupSec"، "TadjMakhal"، "Wipbot"یا " "Tavdig"شناخته می شوند.

تحلیل ها نشان می دهد که قربانیان از طریق یک حمله چند مرحله ای پیچیده، که با Epic Turla آغاز می شود، آلوده می شوند. با گذشت زمان، بعد از این که مهاجمان اطمینان بیشتری به دست آورند، این به درپشتی پیشرفته تر، مانند سیستم Carbon\Cobra ارتقا می یابد. گاهی اوقات هر دو درپشتی در کنار هم اجرا می شوند و در صورت قطع ارتباط با یکی از آن ها، یکدیگر را نجات می دهند.

هنگامی که مهاجمان مدارک لازم را بدون این که قربانی متوجه شود، بدست آوردند، آنها rootkit۱۴ و دیگر مکانیزم های تداوم و ماندگاری شدید را اعمال می کنند.

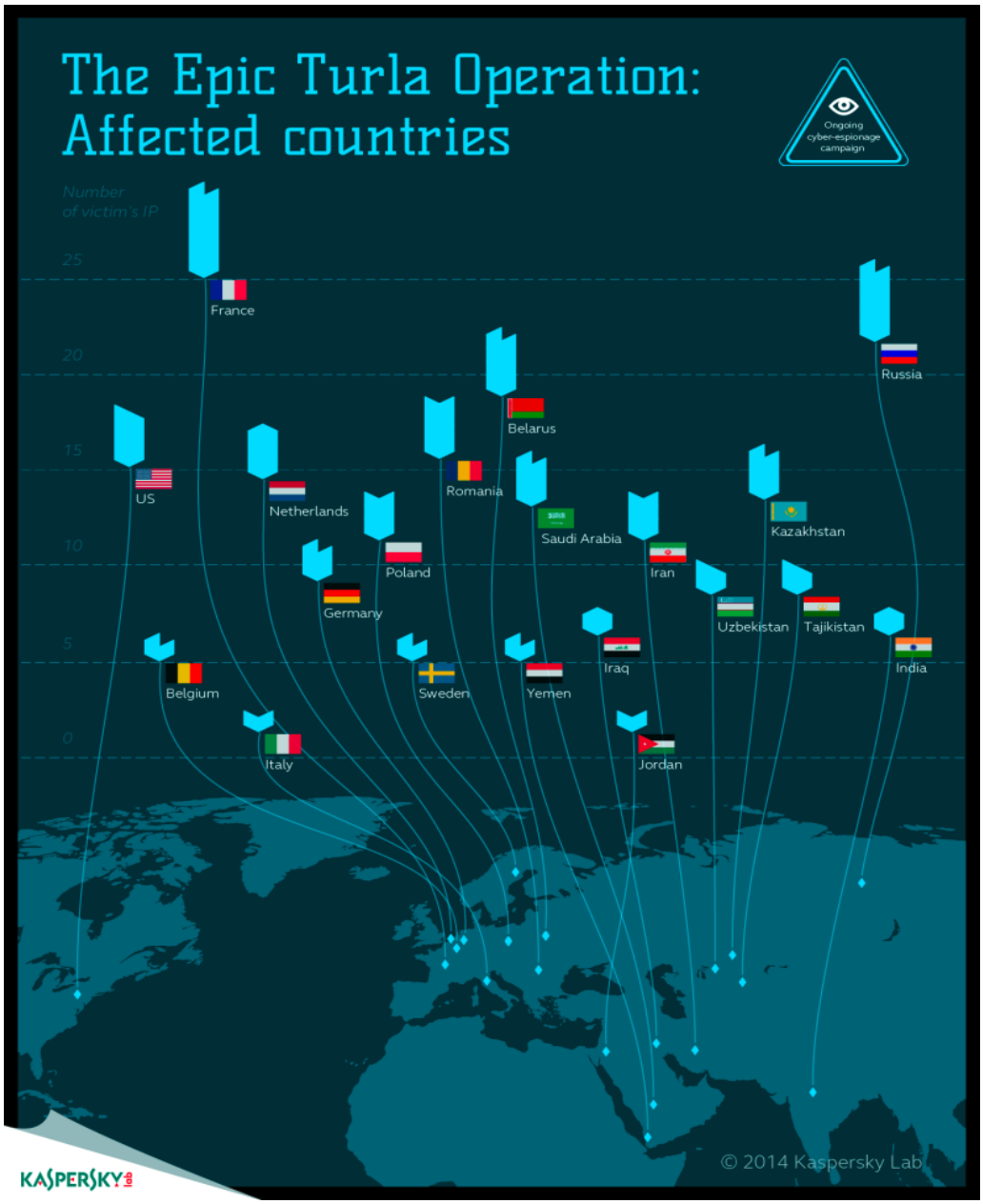
حملات همچنان ادامه دارد و فعالانه کاربران را در اروپا و خاورمیانه مورد هدف قرار می دهند.

بسته به بردار مورد استفاده در آسیب رسانی اولیه حملات در این کمپین به چند دسته تقسیم می شوند:

- ایمیل Spearphishing با استفاده از آسیب پذیری Adobe PDF
- مهندسی اجتماعی برای فریب دادن کاربر در جهت نصب بدافزار با پسوند "SCR." ، گاهی اوقات با "RAR"
- حملات watering hole با سوء استفاده از آسیب پذیری های Java، Flash یا Internet Explorer ۶،۷،۸
- حملات watering hole که به مهندسی اجتماعی متکی هستند تا کاربر را به اجرای نصب کننده های بدافزار های با قالب تقلبی "Flash Player" هدایت می کند

[۱۴] Rootkit: مجموعه ای از نرم افزار معمولا مضربرای فراهم کردن دسترسی به یک کامپیوتر یا قسمت هایی از آن، که خود را با پوشیدن ماسک نرم افزار های قابل اعتماد مخفی می کند.

در حال حاضر، مهاجمان Epic Turla یک شبکه وسیع از watering hole ها را که بازدید کنندگان را با دقت بسیار زیاد مورد هدف قرار می دهند، مدیریت و اجرا می کنند. در برخی از سرورهای C&C مورد استفاده در حملات حماسی، آمار دقیق قربانیان شناسایی شده است که توسط مهاجمین برای اهداف اشکال زدایی[۱۵] ذخیره شده است. تصویر زیر نشان دهنده ی توزیع کشور های آسیب دیده با استفاده از IP قربانیان است:



با توجه به اطلاعات عمومی موجود برای IP های قربانیان، اهداف Epic Turla متعلق به دسته های زیر است:

[۱۵] Debugging

- دولت
- وزارت کشور (کشور اتحادیه اروپا)
- وزارت تجارت و بازرگانی (کشور اتحادیه اروپا)
- وزارت امور خارجه / امور خارجی (کشور آسیایی، کشور اتحادیه اروپا)
- اطلاعات[۱۶] (خاورمیانه، کشور اتحادیه اروپا)
- سفارتخانه ها
- نظامی (کشور اتحادیه اروپا)
- تحصیلات
- تحقیقات (خاورمیانه)
- شرکتهای دارویی
- ناشناخته (غیر قابل تعیین بر اساس داده ها یا IP موجود)

۸-۱۳ حمله MiniFlame یا SPE

در ماه می ۲۰۱۲، تحقیقات آزمایشگاه کسپرسکی یک بدافزار جاسوسی سایبری جدید را شناسایی کرد، که به نام "Flame" شناخته می شود. تحقیقات همچنین ویژگی های مشخصی از ماژول های Flame را شناسایی کرده است. بر اساس این ویژگی ها، مشخص شده است که در سال ۲۰۰۹، اولین گونه ی جدید کرم Stuxnet شامل یک ماژول است که براساس پلتفرم Flame ایجاد شده است. این تأیید کرد که نوعی همکاری بین گروه هایی که پلتفرم های Flame و(Stuxnet / Duqu) Tilded را توسعه داده بودند وجود دارد.

تحقیقی جامع تر در ژوئن ۲۰۱۲، منجر به کشف بدافزار دیگری به نام Gauss که توسط دولت ملت دیگری حمایت شده بودند، شد. Gauss از یک ساختار ماژولار شبیه Flame استفاده کرد، با پایه کد و سیستم مشابه برای برقراری ارتباط با سرورهای فرمان و کنترل۱۷ (C&C)، به علاوه شباهت های متعدد دیگری نیز با Flame وجود داشت.

تحلیل سرور C&C نشان داد که کد می تواند چندین پروتکل ارتباطی با client های مختلف یا بدافزار های مختلف را تشخیص دهد:

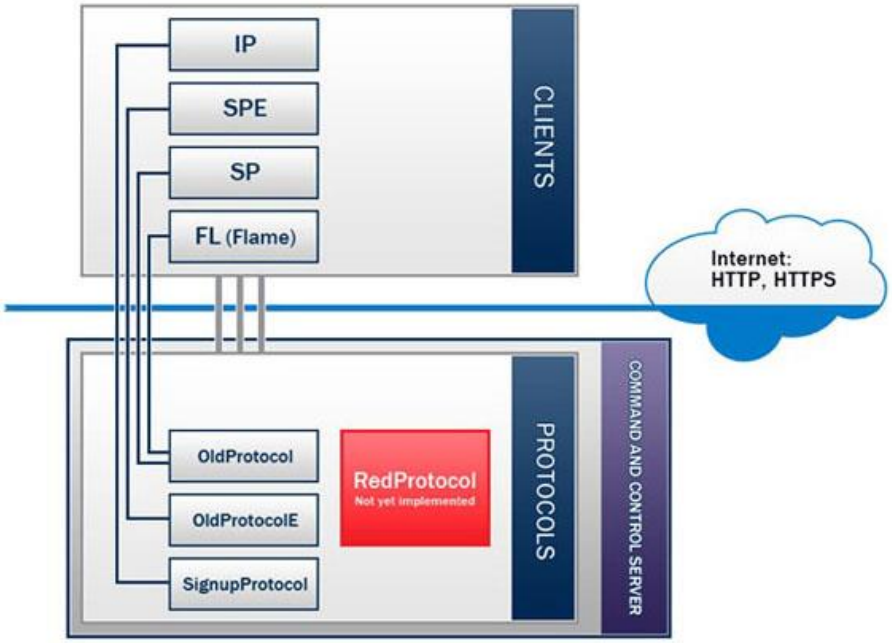
- OldProtocol

[۱۶] Intelligence

[۱۷] Command and control(C&C): سرور استفاده شده توسط مجرمین برای ارسال دستورات از راه دور به سیستم آلوده شده

- OldProtocolE
- SignupProtocol
- RedProtocol (نام برده شده اما اعمال نشده)

نگاهی نزدیک به handler های این پروتکل ها، چهار نوع مختلف از client ها (بدافزارها) را نشان داده و به صورت SP، SPE، FL و IP نامگذاری کرد.



بر اساس منطق کد، می توان تأیید کرد که بدافزار Flame به عنوان client FL شناسایی شده است. بدیهی است که این به این معنی بود که حداقل سه بدافزار کشف نشده ی خرابکاری سایبری یا جاسوسی سایبری ساخته شده توسط همین نویسندگان وجود داشت: SP، SPE و IP.

۸-۱۳-۱ بدافزار SPE

پس از تجزیه و تحلیل سرور C&C بدافزار Flame، تعجب برانگیز بود که این ماژول جدید به نظر می رسید از OldProtocolE برای ارتباطات استفاده کند، که توسط بدافزار اسرار آمیز SPE استفاده می شود. پلاگین Flame در حقیقت یک بدافزار منحصر به فرد و مستقل است و توسط سرور C&C ی Flame با نام SPE شناخته می شود. بر اساس تحلیل های موجود، چندین نکته اصلی درباره SPE که همان "miniFlame"یا "John"(توسط Gauss configuration) نامگذاری شده، وجود دارد:

- بدافزار miniFlame در میان عموم گسترده نیست. احتمالا تنها در موارد بسیار کمی برای قربانیان "مهم[۱۸]" مورد استفاده قرار می گیرد.
- بر خلاف Gauss، SPE/miniFlame یک client/server backdoor کامل را اجرا می کند که اجازه می دهد اپراتور دسترسی مستقیمی به سیستم آلوده داشته باشد.
- به نظر می رسد کدهای Flame C&C برای کنترل مشتریان SPE ماژول خاصی ندارند. دیگر سرورهای اختصاصی SPE C۲ با کدبندی خاص خود می توانند وجود داشته باشند.
- توسعه SPE به صورت موازی با Flame و Gauss طی سالهای ۲۰۱۰-۲۰۱۱ انجام شد.
- Flame و Gauss از miniFlame/SPE به عنوان ماژول استفاده می کنند.
- بردار آلودگی دقیق SPE ناشناخته است؛ اعتقاد بر این است که بدافزار از طریق سرور C&C درآلودگی های Flame یا Gauss اعزام می شوند.

اگرFlame و Gauss عملیات های جاسوسی عظیمی بودند و هزاران نفر را آلوده می کردند، SPE/miniFlame یک ابزار جاسوسی با دقت بالا است. تعداد قربانیان آن با Duqu قابل مقایسه است.

می توانیم فرض کنیم این بدافزار بخشی از عملیات Flame و Gauss است که در چندین موج رخ داده است. موج اول: آلوده کردن تعداد زیادی از قربانیان که پتانسیل جالب بودن و سودآوری دارند. موج دوم: اطلاعات از قربانیان جمع آوری شده به مهاجمان اجازه می دهد تا آنها را شناسایی کرده و جالب ترین اهداف را از میان آن ها بیابند. نهایتا، برای این اهداف "منتخب"، یک ابزار جاسوسی تخصصی مانند SPE/miniFlame برای نظارت/کنترل نصب شده است.

در کد Flame C&C، به دو فایل بدافزار دیگر اشاره شده است: SP و SP .IP به احتمال زیاد به یک مدل قدیمی تر از بدافزار اشاره دارد و احتمالا IP متفاوت است و همچنان ناشناخته باقی می ماند. با توجه به کد اصلی C&C، IP آخرین بدافزار از بسته است.

با بررسی Flame، Gauss و miniFlame، احتمالا فقط سطح رویی عملیات های جاسوسی گسترده در خاورمیانه را خراشیده ایم. هدف واقعی آنها هنوز نامشخص است و هویت قربانیان و مهاجمان ناشناخته.

[۱۸] High profile

۸-۱۴ حمله Flame

پس از اینکه اتحادیه بین المللی مخابرات سازمان ملل متحد برای کمک در پیدا کردن یک قطعه ناشناخته از بدافزار که اطلاعات حساس در خاورمیانه را حذف می کرده است از آزمایشگاه کسپرسکی درخواست کمک کرد، کرم جاسوسی سایبری"Flame" توجه محققان را جلب کرد. در حال جستجو برای آن کد (با نام مستعار Wiper) یک تروجان جدید به نام Worm.Win۳۲.Flame شناسایی شد.

یکی از ماژول های اصلی بدافزار Flame نامگذاری شده است. این ماژول مسئول حمله و آلوده کردن ماشین های اضافی است. نام نرم افزار از این ماژول گرفته شده است.

Flame دارای ویژگی های مشترک بسیاری با سلاح های سرسخت سایبری Duqu و Stuxnet است. این بدافزار به راحتی می تواند به عنوان یکی از پیچیده ترین تهدیدات شناخته شود. Flame فوق العاده بزرگ و پیچیده است و می تواند مفهوم جنگ سایبری و جاسوسی سایبری را بازنویسی کند.

Flame یک toolkit پیچیده حمله است، که بسیار پیچیده تر از Duqu است. Flame یک تروجان و همچنین یک backdoor است، و دارای یک مولفه ی کرم مانند است، که به آن اجازه می دهد اگر توسط صاحبش به آن فرمان داده شود، خود را در یک شبکه محلی یا در رسانه های قابل جابجایی تکثیر کند.

نقطه اولیه وارد شدن Flame ناشناخته است. محققان معتقد هستند که از طریق حملات هدفمند مستقر شده است؛ با این حال، بردار اصلی آن دیده نشده است.

هنگامی که یک سیستم آلوده می شود، Flame یک مجموعه پیچیده از عملیات را آغاز می کند، از جمله خراب کردن ترافیک شبکه، گرفتن تصاویر، ضبط مکالمات صوتی، رهگیری صفحه کلید و غیره. همه این داده ها برای اپراتورها از طریق لینک به سرورهای Flame C&C در دسترس است.

بعدها، اپراتورها می توانند ماژول های بیشتری را آپلود کنند که قابلیت Flame را گسترش می دهند. در مجموع حدود ۲۰ ماژول وجود دارد و هدف بسیاری از آنها هنوز در حال بررسی است.

اول از همه، استفاده از زبان برنامه نویسی Lua و اندازه ی بسیار بزرگ toolkit در بدافزار ها غیر معمول است. به طور کلی، بدافزار های مدرن کوچک هستند و با زبان های برنامه نویسی جمع و جور نوشته میشوند که پنهان کردن آن آسان است. پنهان کاری با استفاده از مقدار زیادی کد یکی از ویژگی های جدید در Flame است.

ضبط اطلاعات صوتی از میکروفون داخلی نیز نسبتا جدید است. البته، دیگر بدافزار هایی وجود دارد که می توانند صدا را ضبط کنند، اما نکته ی کلیدی در اینجا کامل بودن Flame است، که یعنی توانایی سرقت اطلاعات با استفاده از بسیاری از روش های مختلف.

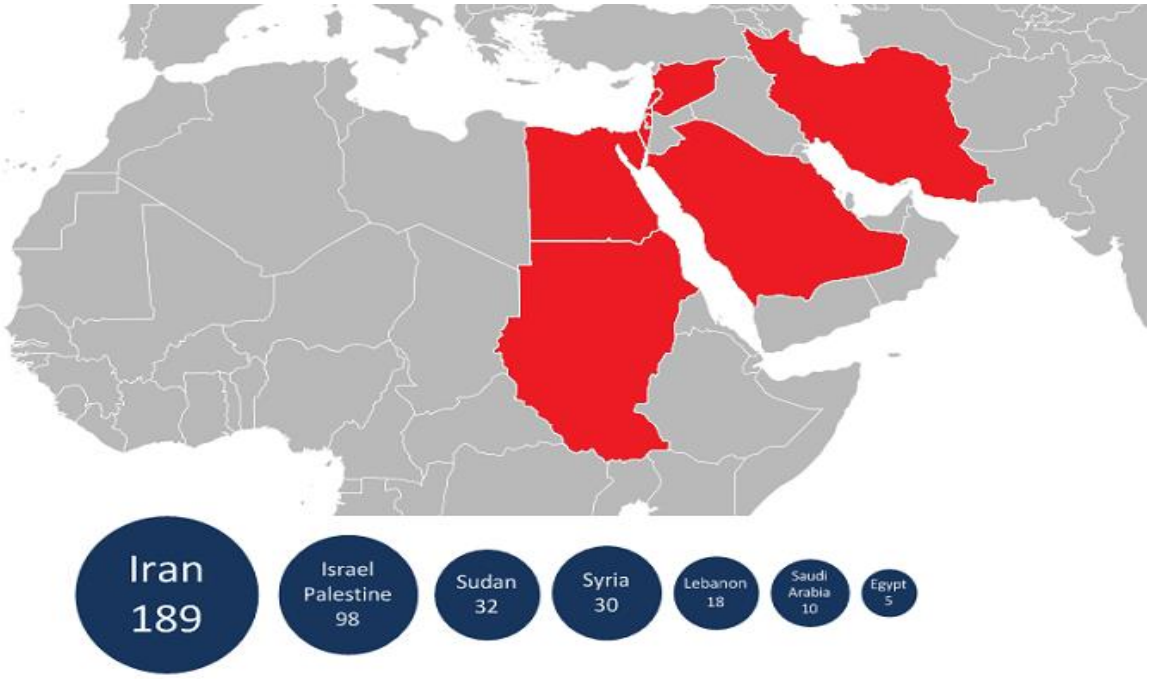
یکی دیگر از ویژگی های شگفت انگیز Flame استفاده از دستگاه های بلوتوث است. هنگامی که بلوتوث در دسترس است و گزینه مربوطه در بلوک configuration روشن شده است، اطلاعات در مورد دستگاه های قابل کشف در نزدیکی دستگاه آلوده را جمع آوری می کند. همچنین می تواند دستگاه آلوده را به یک فرستنده تبدیل کند و آن را از طریق بلوتوث قابل کشف کند و اطلاعات عمومی در مورد وضعیت بدافزار کدگذاری شده دستگاه را ارائه دهد.

بدافزار توانایی گرفتن تصاویر را دارد؛ علاوه بر این، زمانیکه برخی برنامه های کاربردی اجرا می شوند، تصاویر گرفته می شود.

در حال حاضر سه کلاس شناخته شده از بازیکنان که بدافزار های جاسوسی را توسعه می دهند وجود دارد: hacktivist ها، مجرمان سایبری و کشورهای ملی[۱۹]. Flame طراحی نشده است که پول را از حساب های بانکی سرقت کند. همچنین متفاوت از ابزارهای هک ساده و بدافزارهایی است که توسط hacktivist ها استفاده می شود. بنابراین با حذف مجرمان سایبری و hacktivist ها، می توان نتیجه گرفت که احتمالا متعلق به گروه سوم است. علاوه بر این، جغرافیای اهداف (برخی کشورهای خاورمیانه) و نیز پیچیدگی تهدید، هیچ شک و تردیدی باقی نمی گذارد که Flame مطعلق به یک کشور ملی است.

هدف Flame جمع آوری اطلاعات به طور سیستماتیک در مورد عملیات کشورهای خاصی در خاورمیانه، از جمله ایران، لبنان، سوریه، اسرائیل و غیره. در اینجا یک نقشه از ۷ کشور آسیب دیده وجود دارد:

[۱۹] Nation states



Flame حدودا ۲۰ برابر بزرگتر از Stuxnet است، و شامل بسیاری از مولفه های مختلف حمله و جاسوسی سایبری می شود. و به صورت کلی شباهتی با Stuxnet / Duqu ندارد. با این حال برخی از نشانه ها می توانند به این اشاره کنند که سازندگان Flame به تکنولوژی مورد استفاده در پروژه Stuxnet دسترسی داشته اند.

به طور خلاصه، Flame و Stuxnet/Duqu احتمالا توسط دو گروه جداگانه توسعه یافتند. Flame به عنوان یک پروژه در موازات Stuxnet و Duqu در نظر گرفته می شود.

۸-۱۵ حمله Equation

نمونه ای از روش پخش این بدافزار از طریق CD ی است که از طرف برگذار کنندگان یک همایش و دورهمایی علمی برای شرکت کنندگان فرستاده می شود، که معمولا حاوی تصاویری از همایش و شرکت کنندگان آن به همراه خلاصه ای از مطالب ارائه شده است.

مشخص نشده است که گروه Equation در چه زمانی شروع به صعود خود کردند. برخی از اولین نمونه های مخرب دیده شده در سال ۲۰۰۲ جمع آوری شد؛ با این حال، C&C آنها در ماه اوت سال ۲۰۰۱ ثبت شده است.

به نظر می رسد که سایر C&C هایی که توسط گروه Equaiton استفاده می شود در اوایل سال ۱۹۹۶ ثبت شده اند، که می تواند نشان دهد این گروه حدود دو دهه فعال بوده است. این گروه سالهاست که با دیگر گروههای قدرتمند مانند گروههای Stuxnet و Flame تعامل داشته اند، اما همیشه از یک موقعیت برتر برخوردار بود، زیرا به expliot ها زودتر از دیگران دسترسی داشته اند.

از سال ۲۰۰۱، گروه Equation مشغول آلوده کردن هزاران نفر یا حتی ده ها هزار قربانی در سراسر جهان در بخش های زیر است:

- دولت و نهادهای دیپلماتیک
- مخابرات
- هوافضا
- انرژی
- تحقیقات هسته ای
- نفت و گاز
- نظامی
- فناوری نانو
- فعالان و محققان اسلامی
- رسانه های جمعی
- حمل و نقل
- موسسات مالی
- شرکت های توسعه فن آوری های رمزگذاری

گروه Equation از یک انبار مهمات قدرتمند از "ایمپلنت" (آنها تروجان ها خود را ایمپلنت می نامند) استفاده می کنند. از جمله مواردی که برایشان نام انتخاب شده است: EQUATIONLASER، EQUATIONDRUG، DOUBLEFANTASY، TRIPLEFANTASY، FANNY و GRAYFISH می باشند. بدون شک "ایمپلنت" هایی وجود دارد که هنوز باید شناسایی و نامگذاری شود.

خود گروه دارای نامهای بسیاری برای ابزارها و ایمپلنتهای خود است، از جمله SKYHOOKCHOW، UR، KS، SF، STEALTHFIGHTER، DRINKPARSLEY، STRAITACID، LUTEUSOBSTOS، STRAITSHOOTER، DESERTWINTER و GROK.

شاید قوی ترین ابزار در انبار مهمات گروه Equation یک ماژول مرموز است که تنها با یک نام رمزآلود شناخته می شود:"nls_۹۳۳w.dll". این ماژول اجازه می دهد تا آنها سیستم عامل هارد دیسک بیش از دوازده برند مختلف، از جمله Seagate، Western Digital، Toshiba، Maxtor و IBM را مجددا برنامه ریزی کنند. این یک پیشرفت فنی شگفت آور است و نشان دهنده توانایی گروه است.

در طول سال های گذشته، گروه Equation حملات مختلفی را انجام داده است. یکی از موارد برجسته کرم Fanny است. احتمالا در جولای ۲۰۰۸ گردآوری شده بود، و اولین بار توسط سیستم های ما در دسامبر

۲۰۰۸ مشاهده و مسدود شد. Fanny از دو آسیب پذیری روز صفر سوء استفاده کرد که بعدا در طی کشف Stuxnet مشاهده شد.

۸-۱۶ حمله Animals Farm

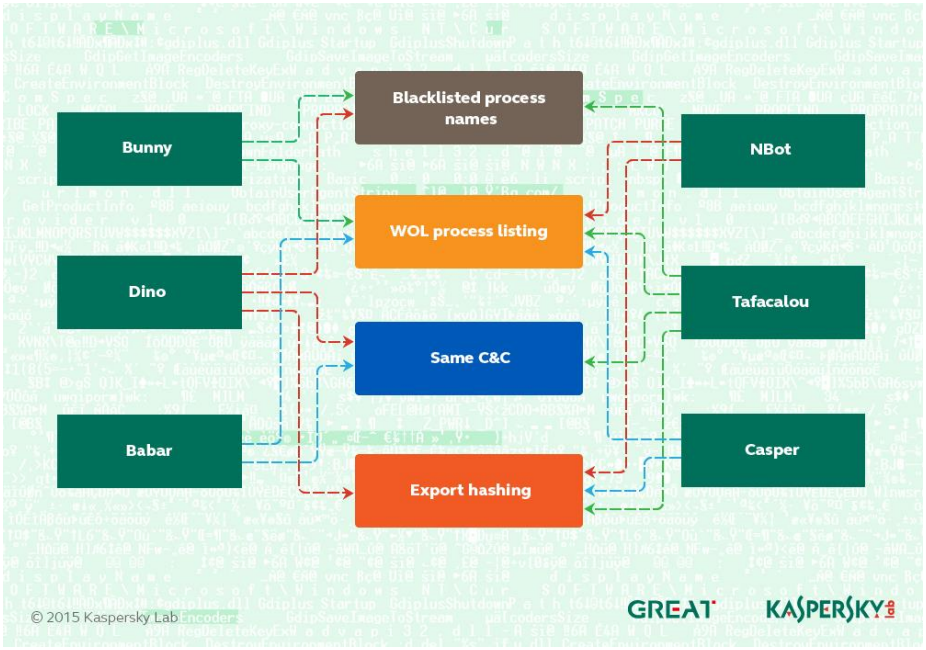
در سال ۲۰۱۴، محققان آزمایشگاه کسپرسکی سه آسیب پذیری روز صفر را کشف کرد و گزارش دادند که در حملات سایبری مورد استفاده قرار گرفتند.

دو مورد از این آسیب پذیری های روز صفر با یک بازیگر تهدید پیشرفته به نام Animals Farm مرتبط است. طی چند سال گذشته، Animals Farm طیف گسترده ای از سازمان های جهانی را هدف قرار داده است. قربانیان عبارتند از:

- سازمان های دولتی
- پیمانکاران نظامی
- سازمان های کمک بشردوستانه
- شرکت های خصوصی
- روزنامه نگاران و سازمان های رسانه ای
- فعالان[۲۰]

Bunny، Casper و Babar نام برخی از تروجان هایی است که توسط Animals Farm مورد استفاده قرار می گیرد.Animals Farm شامل چندین تروجان است که به شش خانواده اصلی تقسیم شده است:

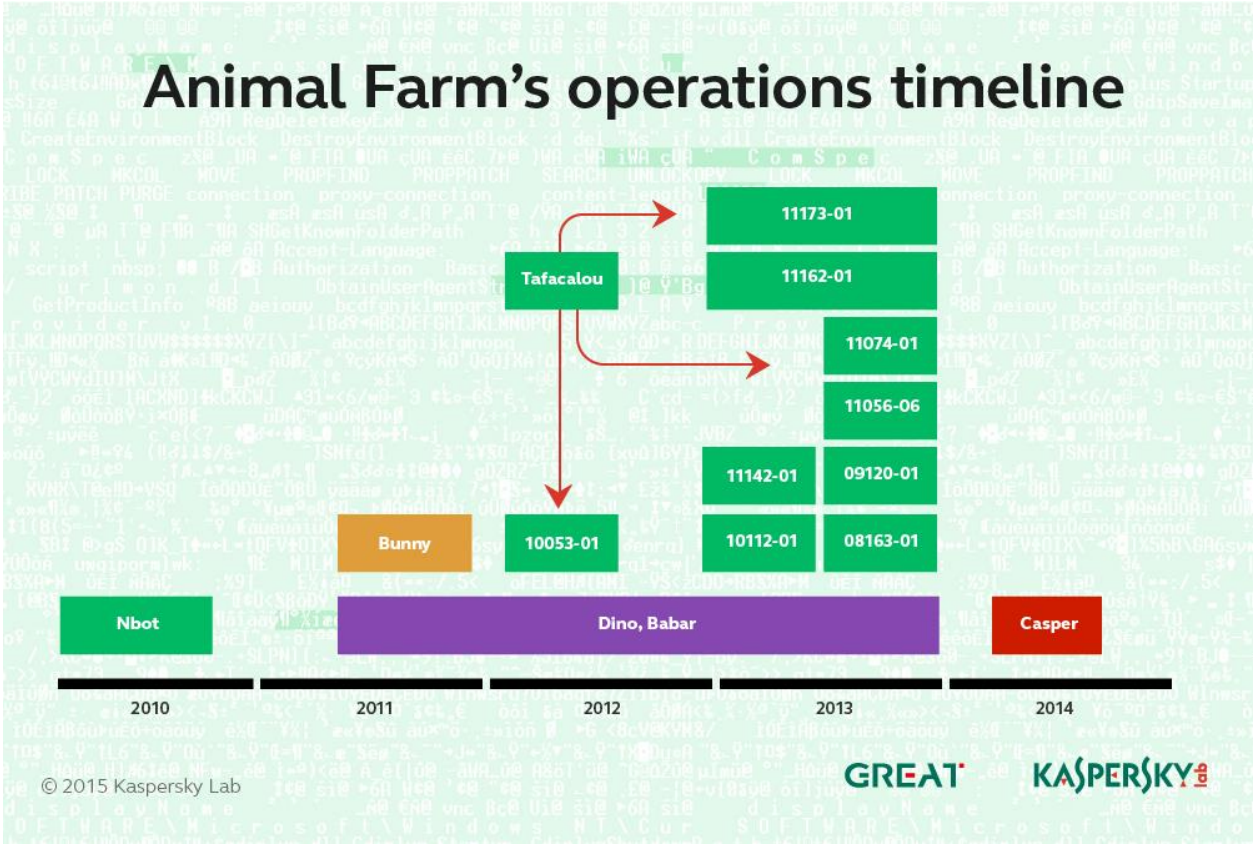
[۲۰] Activists



- Bunny - تروجان قدیمی "اعتبار سنج۲۱" با یک حمله ی PDF با آسیب پذیری روز صفر در سال ۲۰۱۱ استفاده شد.
- Dino - یک پلت فرم جاسوسی کامل است.
- Babar - پیچیده ترین پلت فرم جاسوسی از گروه Animals Farm.
- NBot– بدافزار که توسط گروه در یک عملیات botnet استفاده شد و قابلیت DDoS دارد.
- Tafacalou- یک تروجان به سبک اعتبار سنج است که توسط مهاجمان در سال های اخیر مورد استفاده قرار گرفته است. قربانیان تایید شده به Dino یا Babar ارتقا می یابند.
- Casper - جدیدترین ایمپلنت "اعتبار سنج" از گروه Animals Farm است.

این گروه حداقل از سال ۲۰۰۹ فعال بوده و نشانه هایی وجود دارد که نسخه های قبلی بدافزار از سال ۲۰۰۷ توسعه یافته اند.

[۲۱] Validator



بیشتر قربانیان مربوط به کشورهای زیر هستند:

سوریه، ایران، مالزی، ایالات متحده آمریکا، چین، ترکیه، هلند، آلمان، بریتانیا، روسیه، سوئد، اتریش، الجزایر، اسرائیل، عراق، مراکش، نیوزیلند، اوکراین .