مرکز تخصصی آپا
دانشگاه صنعتی اصفهان

امنیت فضای سایبری

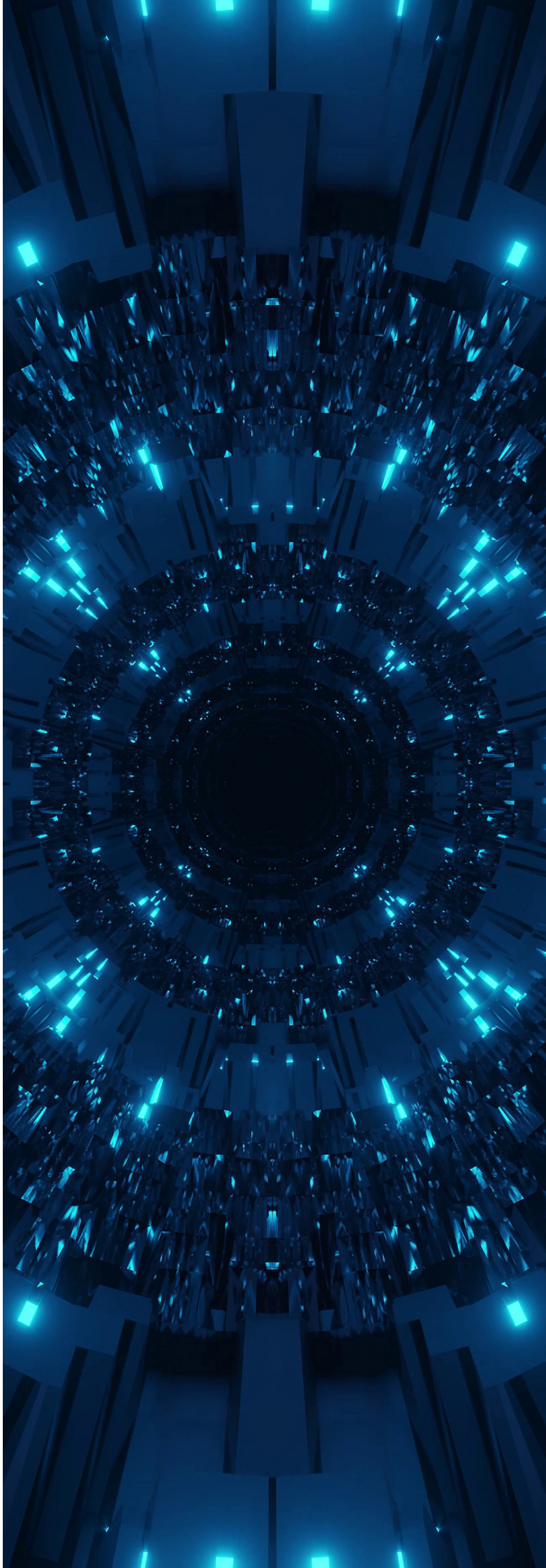
مروری بر وضعیت امنیت سایبری ایران و جهان
در سال ۱۳۹۹

گزارش سالانه

مروری بر وضعیت امنیت سایبری ایران و جهان سال ۱۳۹۹

مرکز تخصصی آپا دانشگاه صنعتی اصفهان

تابستان ۱۴۰۰



حق مالکیت معنوی و سلب مسئولیت

۱ مقدمه

اگرچه به‌دلیل شیوع کرونا و شرایط دورکاری انتظار می‌رفت که سال ۹۹ سالی پرهیاهو در حوزه فناوری اطلاعات باشد، اما شاید کمتری کسی حدس می‌زد که این سال حتی در نخستین روزهای خود در حوزه امنیت سایبری غوغا به پا کند. جالب این که در اولین روزهای فروردین ۹۹، نه اخبار مربوط به کرونا، بلکه خبر نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام فضای مجازی کشور را تکان داد. اما این تنها روزهای ابتدایی سال بود. با نگاهی به اخبار و رخدادهای سال ۹۹ می‌توان دریافت که این سال یکی از پرهیجان‌ترین و پرالتهاب‌ترین سال‌ها از دید امنیت سایبری چه برای مردم ایران و چه برای مردم جهان بوده است. حملات سولاروبندز، Zerologon، نشت‌های اطلاعاتی گسترده و پیشرفت پروژه‌های کلان کشوری در حوزه فناوری اطلاعات تنها بخشی از اخبار داغ سال ۹۹ بودند.

در این گزارش سعی نموده‌ایم با مروری بر رخدادهای مهم امنیت سایبری در سال گذشته و بررسی آماری آنها، تصویری جامع و تا جای امکان نزدیک به واقعیت از فضای سایبری ایران و جهان در سال ۹۹ بسازیم. امیدواریم این سال‌نامه بتواند توجه علاقه‌مندان، کارشناسان و مدیران این حوزه را جلب نموده و در تصمیم‌گیری‌های آینده آن‌ها مفید باشد. این سال‌نامه در پنج فصل تهیه شده است. در فصل دوم این گزارش به حمله وسیع سولاروبندز تحت عنوان داستان سال می‌پردازیم که اگر آن را داستان سایبری قرن هم خطاب کنیم چندان بیراه نگفته‌ایم. در فصل سوم، آسیب‌پذیری‌های سال گذشته و آمار آن‌ها را بر اساس سطح خطر، محصولات آسیب‌پذیر و بسیاری از ویژگی‌های دیگر بررسی نموده‌ایم. فصل چهارم به تشریح وضعیت امنیت سایبری ایران در سال ۹۹ و ماه‌های ابتدایی سال ۱۴۰۰ اختصاص دارد. در ابتدای این فصل، داده‌های سامانه ملی مقابله با بات و آسیب‌پذیری را تحلیل کردیم و سپس به برخی رخدادهای مهم و پروژه‌های ملی بزرگ در حوزه فضای مجازی کشور پرداختیم و از دید امنیت، ابعاد مختلف آن‌ها بیان کردیم. در فصل پنجم و انتهایی این سال‌نامه به بزرگترین حملات سایبری جهان در سال ۹۹، نشت‌های اطلاعاتی سازمان و شرکت‌های جهانی، تأثیرات جهانی دورکاری و کرونا و همچنین به بررسی مهم‌ترین بدافزارهای سیستم عامل‌های ویندوز، مک و موبایل پرداختیم.

فهرست

۲

داستان سال

حملات سولارویندز

پس از ده سال محاصره شهر تروا توسط لشکریان یونانی و پس از کشته شدن آشیل، روحیه لشکریان یونان تضعیف شده بود و آن‌ها آماده برگشت به یونان بودند که آتنا یکی از خدایان یونان، حیله‌ای برای فتح تروا پیشنهاد می‌دهد؛

اسب تروجان!


solarwinds

۲ داستان سال: حملات سولارویندز

پس از ده سال محاصره شهر تروا توسط لشکریان یونانی و پس از کشته شدن آشیل، روحیه لشکریان یونان تضعیف شده بود و آن‌ها آماده برگشت به یونان بودند که آتنا یکی از خدایان یونان، حیله‌ای برای فتح تروا پیشنهاد می‌دهد؛ اسب تروجان!

داستان نبرد تروا و داستان حمله زنجیره تأمین سولارویندز (SolarWinds) اشتراکات بسیاری دارد؛ از جمله وجود اسب پیشکشی که به سادگی از دیوارهای امنیتی شهر عبور کرده و به قلب هدف نفوذ می‌کند. در داستان نبرد تروا پس از فریب اهالی تروا و استقرار پیکره‌ای عظیم‌الجثه اسب تروا در معبد شهر، شب‌هنگام سپاهیان یونانی از پیکره اسب بیرون آمده، دروازه‌های شهر را برای یاران خود گشوده و پس از غارت، تجاوز و تسخیر شهر به نبرد پایان دادند. لیکن لشکریان سایبری داستان سولارویندز صبورانه و هوشمندانه و برای ماه‌ها بدون آن که کسی متوجه حضورشان شود؛ از شهری به شهر دیگر رفته، در هر شهر خود را به سلاحی جدید آراسته‌اند و هنوز کسی نمی‌داند چه چیزهایی دقیقاً غارت شده است؟ با سلاح‌های جدید، چه نبرد جدیدی در انتظار است؟ و مهاجمین چه قابلیت‌های جدیدی دارند و تا چه اندازه کنترل شهرهای تسخیرشده را بدست گرفته‌اند؟

در این بخش به حمله زنجیره تأمین سولارویندز پرداخته شده است که برخی می‌گویند نه فقط داستان سال که داستان قرن ماست.

۲-۱- شروع داستان

هجدهم آذرماه ۱۳۹۹، شرکت FireEye اعلام کرد که مورد هجوم حملات گسترده‌ای واقع شده است که طی این حملات، بسیاری از ابزارها و اطلاعات حساس این شرکت به سرقت رفته است. پنج روز بعد، کریس بینگ (Chris Bing) از رویترز از نفوذ به وزارت خزانه‌داری ایالات متحده آمریکا پرده برداشت. اِلن ناکاشیما (Ellen Nakashima) تحلیل‌گر امنیت اطلاعات واشنگتن‌پُست با ارائه مدارکی، دو حمله فوق‌الذکر را به هم مرتبط دانست و مدعی شد که هر دو توسط یک گروه تهدید روسی به نام APT29 پیاده شده‌اند و در هر دو حمله از پلتفرم SolarWinds Orion سوءاستفاده شده است.

محصول Orion شرکت سولارویندز، یک سیستم مدیریت شبکه (Network Management System) یا NMS است که قابلیت‌های بسیاری برای نظارت و مدیریت سیستم‌های شبکه از سرورها و ایستگاه‌های کاری، تا تجهیزات شبکه مانند مسیریاب‌ها، دیوار آتش و ... دارد.

> SANS: «SolarWinds Orion is to NMS what Kleenex is to tissues»

برای مهاجمین، NMSها اهداف بسیار

مهمی هستند؛ چرا که:
سیستم NMS بایستی با تمامی دستگاه‌های شبکه در ارتباط باشد و از این حیث مکانیزم‌های لیست دسترسی یا ACLs بر آن اثر ندارد.
به‌علاوه، NMSها اغلب به‌گونه‌ای پیکربندی می‌شوند که بتوانند شبکه را نظارت کنند و به رویدادهای آن پاسخ دهند. در صورت نفوذ به NMS این امکان، قابلیت‌های بسیاری را در اختیار مهاجم قرار خواهد داد.
حتی اگر NMS فقط برای نظارت شبکه پیکربندی شده باشد؛ با به‌دست آوردن اعتبارنامه‌ها، مهاجم سطح دسترسی خوبی در شبکه هدف خواهد داشت.

« در صورت نفوذ، هر کاری که NMS قادر به انجام آن است؛ مهاجم نیز می‌تواند انجام دهد ».

۲-۲- حمله زنجیره تأمین سولارویندز

حمله زنجیره تأمین، حمله‌ای است که برای نفوذ به یک نهاد/سازمان/شرکت از ضعیف‌ترین عنصر (ضعیف‌ترین حلقه) در زنجیره هدف سوءاستفاده می‌شود. در حمله زنجیره تأمین سولارویندز نیز از سولارویندز به‌عنوان حلقه ضعیف برای نفوذ به بزرگ‌ترین شرکت‌ها، نهادها و سازمان‌ها مانند پنتاگون ایالات متحده آمریکا، ناتو، اتحادیه اروپا، چندین وزارت‌خانه ایالات متحده آمریکا، چندین شرکت دارویی فعال در تولید واکسن کووید-۱۹ وخوش‌نام‌ترین شرکت‌ها مانند مایکروسافت، VMware، سیسکو، اینتل، FireEye و ... استفاده شد.
در مقایسه با نبرد تروا، کد دلخواه مهاجم همان لشکریان یونانی و اسب تروای سولارویندز، DLL به‌روزرسانی نرم‌افزار SolarWinds Orion است که کد مهاجم به آن تزریق شده است.

سرورهای سولارویندز نیز همان معبد تروا است که نرم‌افزار آلوده از آنجا به کلیه شرکت‌ها و سازمان‌هایی که به‌روزرسانی‌ها را دریافت می‌کردند، راه یافته است.
برای تزریق کد بایستی مکان مناسبی در DLL انتخاب می‌شد. جایی که به‌صورت دوره‌ای فراخوانی و اجرا شود و بدافزار را در سیستم قربانی، مانا یا Persistent کند. بدین منظور تابع RefreshInternal برای آغاز اجرای بدافزار انتخاب و کد سبکی به آن تزریق شد تا به‌صورت موازی thread اجرا کند و روند اجرای تابع RefreshInternal را مختل نسازد.
تابع RefreshInternal از این رو انتخاب خوبی بود که بخشی از کلاس SolarWinds.Orion.Core.BusinessLayer.BackgroundInventory.InventoryManager است که به‌دنبال کلاس CoreBusinessLayerPlugin فراخوانی می‌شود. هدف از این کلاس آغاز سایر مؤلفه‌ها و زمان‌بندی وظایف است. بدین‌ترتیب مهاجمین با تزریق کد در این نقطه آغازین از مانایی و اجرای همیشگی بدافزار مطمئن خواهند بود. ولیکن بدافزار پیش از فاز اجرا، محیطی که در آن اجرا می‌شود را بررسی می‌کند تا مطمئن شود در محیط ارزیابی و تحلیل بدافزار و/یا Sandbox اجرا نخواهد شد:

- نام دامنه محیط میزبان را بازیابی کرده و آن را بررسی می‌کند که آیا دامنه سیستم Joined است؟
- فرآیندها و درایوهای در حال اجرا را بررسی می‌کند که آیا مرتبط با نرم‌افزارهای امنیتی یا تحلیلی مثل Wireshark هستند؟
- درخواست ترجمه دامنه داده و بررسی می‌کند که آیا پاسخ آدرس IP مربوط به همان محیط است؟ چرا که محیط‌های تحلیلی و Sandbox ترافیک نرم‌افزار

موردبررسی را به خود برمی‌گردانند تا آن را نظارت و تحلیل کنند.
در تمامی این موارد در صورت مطلوب نبودن محیط اجرایی، بدافزار اجرا نخواهد شد و اگر همه شرایط موردبررسی مناسب بود؛ بدافزار وارد فاز اجرایی می‌شود. بیشتر آن‌که اجرای بدافزار به‌صورت رندوم از ۱۲ تا ۱۴ روز تأخیر خواهد داشت.
اسب تروای داستان سولاروینڈز در حقیقت یک در پشتی است که FireEye آن را Sunburst یا آفتاب‌سوختگی نامیده است (وجه تسمیه آن اشاره به نام شرکت سولاروینڈز یا بادهای خورشیدی است). درب پشتی Sunburst نیز مانند سایر درهای پشتی به‌محض اجرا، درصدد ارتباط با سرور فرمان و کنترل یا C2 برمی‌آید. برای این‌کار اطلاعات اولیه‌ای از سیستم تسخیرشده جمع‌آوری و برای دامنه C2 ارسال می‌کند. این دامنه با استفاده از مکانیزم‌های DGA تولید می‌شود و برای هر قربانی منحصربه‌فرد است. بدین ترتیب تشخیص و فیلتر آن دشوار خواهد بود.
در صورت برقراری ارتباط با سرور C2 دستورات اولیه برای Sunburst ارسال می‌شود. ممکن است اطلاعات سرور C2 دیگری برای ارسال گزارشات و اطلاعات جمع‌آوری‌شده برای در پشتی فرستاده شود. این دستورات، کنترل کامل سیستم قربانی را برای مهاجمین فراهم می‌سازد.

نهایتاً بدافزار، پیلودهای بدخواه دیگری همچون Rundll32، PowrShell و ... را در سیستم هدف بارگذاری می‌کند تا در صورت بسته شدن درب پشتی Sunburst، هنوز راهی برای نفوذ به سیستم وجود داشته باشد. همچنین وجود بدافزارهای دیگری از جمله SuperNova، SunSpot، Teardrop و RainDrop در میزبان‌های آلوده به Sunburst تأیید شده است. تمامی این بدافزارها، ابزارهایی هستند که به مهاجم برای مانایی بیشتر در سیستم هدف کمک می‌کنند.

چنانچه گفته شد روایت حمله سولاروینڈز برای اولین بار در آذرماه ۱۳۹۹ گفته شد؛ ولی در حقیقت زمان این حمله به ماه‌ها قبل‌تر یعنی اواخر ۱۳۹۸ باز می‌گردد. مایکروسافت لیستی از ۱۹ DLL آلوده سولاروینڈز را در گزارشی منتشر کرد که زمان دیده شدن این فایل‌ها بهمن و اسفند ۱۳۹۸ است. متأسفانه هنوز نمی‌دانیم در این بازه زمانی، مهاجمین چه اطلاعاتی را به سرقت برده‌اند؟ تا چه اندازه کنترل شبکه‌های تسخیرشده را بدست گرفته‌اند و در آینده با توجه به قابلیت‌های جدید چه می‌کنند؟
نیمه پر این داستان این است که بسیاری از شرکت‌های مطرح حوزه امنیت اطلاعات برای شناسایی بدافزارهای مرتبط با این حملات روش‌ها و دستورالعمل‌هایی را صادر کرده‌اند. همچنین شرکت سولاروینڈز وصله‌هایی را برای رفع آسیب‌پذیری‌های مورد سوءاستفاده در این حملات منتشر کرد. اما نیمه خالی لیوان آن است که هنوز بسیاری از سازمان‌ها اقدام به به‌روزرسانی سیستم‌های خود نکرده‌اند. برای مثال با گذشت چندین ماه از انتشار اخبار مرتبط با این حملات پیچیده و گسترده، هنوز نسخه آسیب‌پذیر Solarwinds Orion بر ۳۰ آدرس IP ایرانی نصب است!

۲-۳- نتیجه‌گیری و پیشنهاد

حملاتی مانند زنجیره تأمین سولاروینڈز درس‌هایی زیادی برای مدیران امنیت و ناظران شبکه دارند:

• حتی بهترین‌ها، کامل نیستند. محصول Solarwinds Orion از مهم‌ترین و محبوب‌ترین محصولات NMS است که در سراسر جهان استفاده می‌شود. ولیکن این بدین معنی نیست که از همه نظر - از جمله از نظر امنیتی - بی‌نقص باشد. در نتیجه برای استفاده از چنین محصولاتی با استفاده از رویکردهای اعتماد صفر یا Zero Trust، بایستی ورودی و خروجی‌هایشان کاملاً کنترل و نظارت شود.

• گزارش وقوع حمله، کمک به خود و سایر قربانیان است. اگر چه هنوز ابعاد دقیق این حمله کاملاً روشن نیست؛ ولیکن چراغ اول شناخت حمله را FireEye با انتشار وقوع حملات به زیرساخت‌هایش روشن کرد. اگر شرکت‌ها و سازمان‌های قربانی حملات سایبری به جای توضیح و تشریح حمله، وقوع آن را کتمان کنند نه تنها به جای سایر قربانیان به مهاجم کمک می‌کنند؛ بلکه کمک دیگران را از خود دریغ کرده‌اند. برای مثال در حمله سولاروینڈز، بدافزار Sunburst توسط FireEye شناسایی و معرفی شد. پس از آن CrowdStrike بدافزار SunSpot را شناسایی کرد؛ شرکت‌هایی مانند مایکروسافت آن‌ها را تحلیل و روش‌هایی برای شناسایی‌شان ارائه کردند و این روند هم‌افزایی همچنان ادامه دارد.

• از آنجا که کد بدخواهانه در این حمله به فایل به‌روزرسانی محصول Solarwinds Orion تزریق شده بود؛ سؤال معمول آن است که آیا به‌روزرسانی‌ها نباید نصب و اعمال شوند؟! در پاسخ باید گفت حتماً باید به‌روزرسانی‌ها اعمال شوند ولی نه بصورت خودکار و بدون تحلیل. در رویکرد اعتماد صفر، شما نباید هر وصله، فایل و ... را بدون تحلیل بارگذاری و نصب کنید. علاوه بر این بدافزار Sunburst با دوره خاموشی ۱۴ روزه‌اش نشان داده است که تحلیل و بررسی کوتاه‌مدت ابداً کافی نیست.

• مهم‌تر از همه آن که امنیت شرکت/سازمان خود و شرکت‌ها/سازمان‌های وابسته‌تان را جدی بگیرید. به زنجیره تأمین شرکت/سازمان خود توجه کنید و هر گونه ارتباط با حلقه‌های ضعیف‌تر این زنجیره را رصد کنید. توجه کنید که اگر به زیرساخت‌های پیچیده شرکت‌های مطرح و مهمی مانند سولاروینڈز، FireEye، مایکروسافت، سیسکو و سازمان‌هایی مانند پنتاگون، وزارت‌خانه‌های ایالات متحده، ناتو حمله شده است؛ حمله به شرکت/سازمان شما نیز ممکن است.

۳

آسیب‌پذیری‌های امنیتی در سال ۹۹

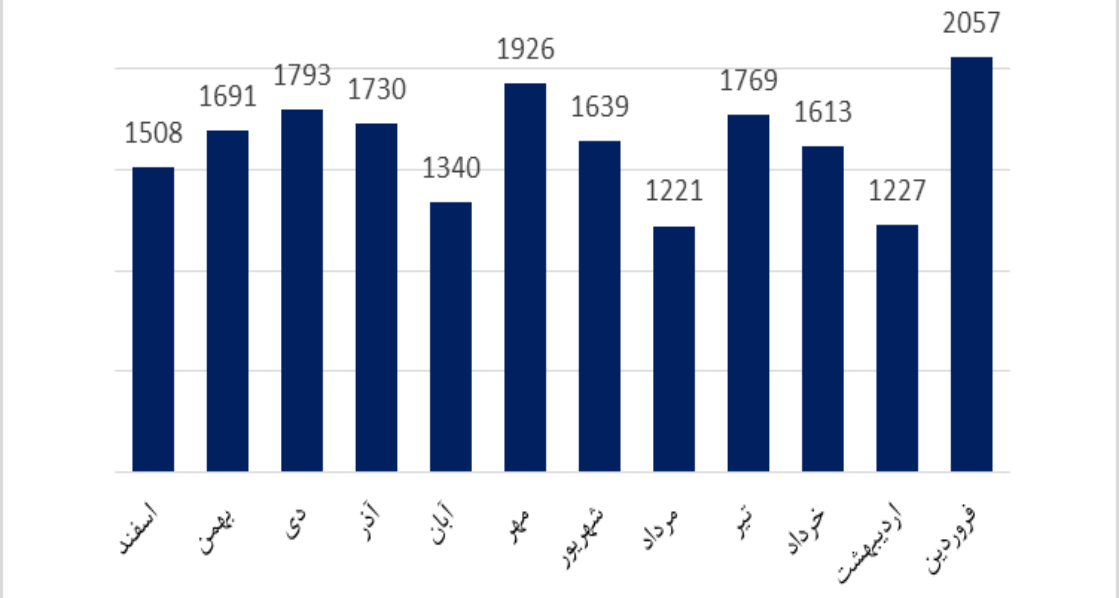
آسیب‌پذیری راه نفوذ مهاجم به سیستم است و از این رو شناسایی و رفع به‌موقع آن می‌تواند در بهترین حالت از وقوع بسیاری از حملات امنیتی پیشگیری کند و در صورت وقوع حمله به تشخیص و مقابله با آن کمک کند.

۳ آسیب‌پذیری‌های امنیتی در سال ۹۹

۱.۳ مقدمه

آسیب‌پذیری، ضعف یا عیبی است که با یک اشتباه در طراحی، توسعه یا پیکربندی سیستم بوجود می‌آید و سوءاستفاده از آن می‌تواند سیاست‌های صریح یا ضمنی امنیتی را خدشه‌دار کند. می‌توان گفت آسیب‌پذیری راه نفوذ مهاجم به سیستم است و از این رو شناسایی و رفع به‌موقع آن می‌تواند در بهترین حالت از وقوع بسیاری از حملات امنیتی پیشگیری کند و در صورت وقوع حمله به تشخیص و مقابله با آن کمک کند.

این بخش، آمار و ارقام مرتبط با آسیب‌پذیری‌های اعلانی سال ۱۳۹۹ را ارائه می‌کند. سال ۱۳۹۹، در پایگاه ثبت آسیب‌پذیری VulDB جمعاً ۱۹۵۱۴۵ آسیب‌پذیری ثبت شده است. نمودار ۳-۱ تعداد این آسیب‌پذیری‌ها را به تفکیک ماه نشان می‌دهد. فروردین‌ماه سال ۱۳۹۹ با ۲۰۵۷ آسیب‌پذیری، بیش‌ترین و مردادماه با ۱۲۲۱ آسیب‌پذیری کم‌ترین آسیب‌پذیری را داشته‌اند.



نمودار ۳-۱ تعداد آسیب‌پذیری‌ها به تفکیک ماه

در ادامه، در زیربخش ۳-۱ ابتدا تعریفی از سطح خطر آسیب‌پذیری‌ها و نحوه تعیین آن آمده است.
سطح خطر آسیب‌پذیری از آن جهت مهم است که بدون در نظر گرفتن شرایط محیطی، نشان می‌دهد هر آسیب‌پذیری چرا و چه اندازه می‌تواند خطرآفرین باشد. پس از تعریف سطح خطر در ادامه همان زیربخش، آمار تعدد آسیب‌پذیری‌های سال ۱۳۹۹ به تفکیک ماه و با توجه به سطح خطرشان ارائه شده است.
درپایان زیربخش ۳-۱ به ویژگی‌های مرتبط با نحوه سوءاستفاده از آسیب‌پذیری‌های سال ۱۳۹۹ پرداخته شده است. این ویژگی‌ها عبارتند از: بردار حمله، پیچیدگی حمله، امتیاز موردنیاز برای سوءاستفاده از آسیب‌پذیری و ... . زیربخش ۳-۲ به ارزش فعلی و روز صفر آسیب‌پذیری‌های سال ۱۳۹۹ پرداخته است.

نهایتاً این بخش با زیربخش ۳-۳ که آمار و ارقام نوع محصولات آسیب‌پذیری سال ۱۳۹۹ را ارائه می‌کند، پایان می‌یابد.

۲.۳ میزان اهمیت آسیب‌پذیری‌ها

سطح خطر و میزان اهمیت آسیب‌پذیری‌ها متفاوت است. با توجه به تعداد بالای آسیب‌پذیری‌های منتشرشده در هر روز و عدم امکان رسیدگی موازی به تمامی آن‌ها، تعیین سطح خطر و اولویت‌بندی آن‌ها ضروری است.

بدین منظور با در نظر گرفتن ویژگی‌های مبنای آسیب‌پذیری که به محیط سیستم و کاربر بستگی ندارد، امتیازی به هر آسیب‌پذیری اختصاص داده می‌شود. برای تعیین امتیاز آسیب‌پذیری‌ها، سیستم امتیازدهی استانداردی به نام CVSS وجود دارد.

ویژگی‌های مبنای آسیب‌پذیری که در سیستم CVSS از آن‌ها استفاده می‌شود، عبارتند از:

- بردار حمله آسیب‌پذیری (نحوه دسترسی و سوءاستفاده از آسیب‌پذیری)؛
- پیچیدگی حمله یا سوءاستفاده از آسیب‌پذیری؛
- امتیاز موردنیاز برای سوءاستفاده از آسیب‌پذیری؛
- نیاز به تعامل با کاربر در حمله؛
- حوزه تأثیرگذاری آسیب‌پذیری (آیا آسیب‌پذیری تنها بر محصولات آسیب‌پذیر اثر دارد یا بر سایر محصولات مقیم در سیستم/شبکه هدف نیز اثر خواهد داشت)؛
- تأثیر حمله موفق بر سه رکن اصلی امنیت: محرمانگی، صحت و دسترس‌پذیری.

این ویژگی‌ها در کنار یکدیگر دو کمیت با نام «قابلیت سوءاستفاده»، «تأثیر» و نهایتاً کمیت امتیاز مبنا را می‌سازند که با استفاده از روابط زیر محاسبه می‌شوند:

اگر کمیت تأثیر یا $Impact$ کمتر از صفر باشد؛ سطح خطر برابر صفر خواهد بود:

Base Score = 0.0

در غیر این صورت:

اگر حوزه تأثیر بدون تغییر باشد؛ سطح خطر برابر است با:

Base Score = $Roundup(Minimum[(Impact + Exploitability), 10])$

در غیر این صورت:

Base Score = $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

کمیت تأثیر یا $Impact$ بصورت زیر تعریف می‌شود:

اگر حوزه تأثیر بدون تغییر باشد:

$Impact$ = 6.42 × ISCBase

در غیر این صورت:

$Impact$ = 7.52 × $[ISCBase - 3.25 - [0.029 \times [ISCBase - 15\text{^}[0.02$

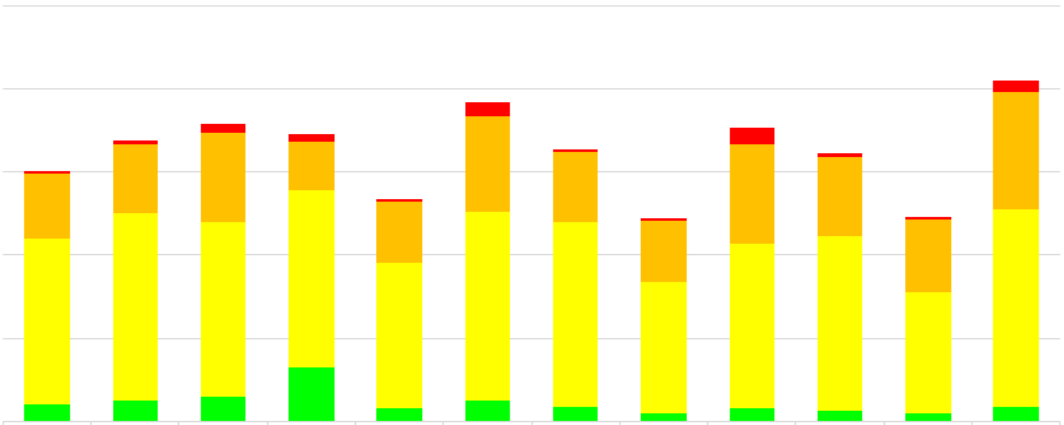
که در آن:

$ISCBase$ = $1)] - 1 - ImpactConf) \times (1 - ImpactInteg) \times (1 - ImpactAvail)]$

و کمیت قابلیت سوءاستفاده یا $Exploitability$ از رابطه زیر حاصل می‌شود:

$Exploitability$ = 8.22 × $AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$

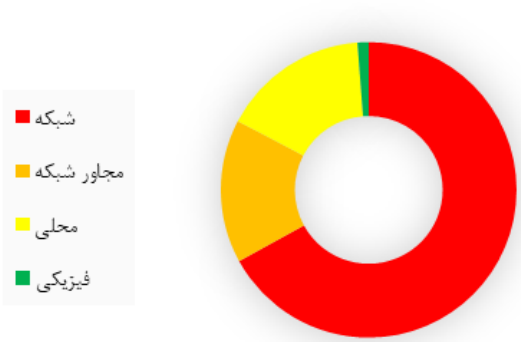
بدین‌ترتیب هر آسیب‌پذیری امتیازی بین صفر و ده را دریافت می‌کند که نشان‌دهنده سطح خطر آسیب‌پذیری است. با توجه به این امتیازات، آسیب‌پذیری‌ها به چهار دسته کم‌خطر (امتیاز ۰ تا ۴)، خطرناک (امتیاز ۴ تا ۷)، پرخطر (امتیاز ۷ تا ۹) و بحرانی (امتیاز ۹ تا ۱۰) تقسیم می‌شوند. نمودار ۳-۲ سطح خطر آسیب‌پذیری‌های سال ۱۳۹۹ را به تفکیک ماه نشان می‌دهد (مبتنی بر اطلاعات پایگاه آسیب‌پذیری VulDB).



	اسفند	بهمن	دی	آذر	آبان	مهر	شهریور	مرداد	تیر	خرداد	اردیبهشت	فروردین
بحرانی	13	21	56	49	14	85	17	14	101	19	10	75
پرخطر	393	413	538	289	371	578	421	371	602	476	438	703
خطرناک	999	1134	1051	1070	876	1138	1114	793	990	1054	732	1193
کم‌خطر	103	123	148	322	79	125	87	43	76	64	47	86

نمودار ۳-۲ سطح خطر آسیب‌پذیری‌ها به تفکیک ماه

چنانچه گفته شد، از ویژگی‌های تعیین‌کننده سطح خطر آسیب‌پذیری، بردار حمله است که نشان می‌دهد آسیب‌پذیری با چه میزان دسترسی به سیستم هدف مورد سوءاستفاده قرار می‌گیرد. این ویژگی می‌تواند مقادیر کیفی «شبکه»، «مجاور شبکه»، «محلی» و «فیزیکی» را به خود بگیرد. ترتیب مذکور از بهترین حالت برای مهاجم یعنی «شبکه» به بدترین حالت برای وی یعنی «فیزیکی» است. به عبارت دیگر، زمانی که بردار حمله برابر «شبکه» باشد؛ مهاجم می‌تواند از راه دور از آسیب‌پذیری سوءاستفاده کند و اگر بردار حمله «فیزیکی» باشد؛ مهاجم برای حمله نیاز به دسترسی فیزیکی به سیستم هدف دارد.



نمودار ۳-۳- بردار دسترسی سوءاستفاده از آسیب‌پذیری

نمودار ۳-۳ بردار حمله آسیب‌پذیری‌های سال ۱۳۹۹ را نشان می‌دهد. توجه شود که ۶۷٪ آسیب‌پذیری‌ها از طریق شبکه قابل سوءاستفاده هستند. برای سوءاستفاده از ۱۶٪ آسیب‌پذیری‌ها مهاجم بایستی اصطلاحاً مجاور شبکه هدف باشد. همچنین بطور مشابه برای ۱۶٪ آسیب‌پذیری‌ها مهاجم بایستی دسترسی محلی به شبکه هدف داشته باشد یا بعبارت دیگر، از طریق لینک لایه دو شبکه به سیستم هدف متصل باشد و نهایتاً برای ۱ درصد آسیب‌پذیری‌ها مهاجم بایستی دسترسی فیزیکی به سیستم هدف داشته باشد.

ویژگی دیگر یک آسیب‌پذیری نیاز به احراز اصالت است. آیا مهاجم پیش از سوءاستفاده از آسیب‌پذیری لازم است در سیستم هدف احراز اصالت شود؟ برای برخی آسیب‌پذیری‌ها پاسخ «خیر» است و مهاجم بدون نیاز به هیچ اعتبارنامه‌ای می‌تواند از طریق آسیب‌پذیری به سیستم نفوذ کند. نمودار ۳-۴ نشان می‌دهد که مهاجم برای سوءاستفاده از ۴۵٪ آسیب‌پذیری‌های سال ۱۳۹۹ نیازی به احراز اصالت ندارد. برای ۴۹٪ آسیب‌پذیری‌ها سطح احراز اصالت لازم «کم» و تنها برای ۶٪ سطح احراز اصالت «بالا» است.

نمودار ۳-۴- نیاز به احراز اصالت

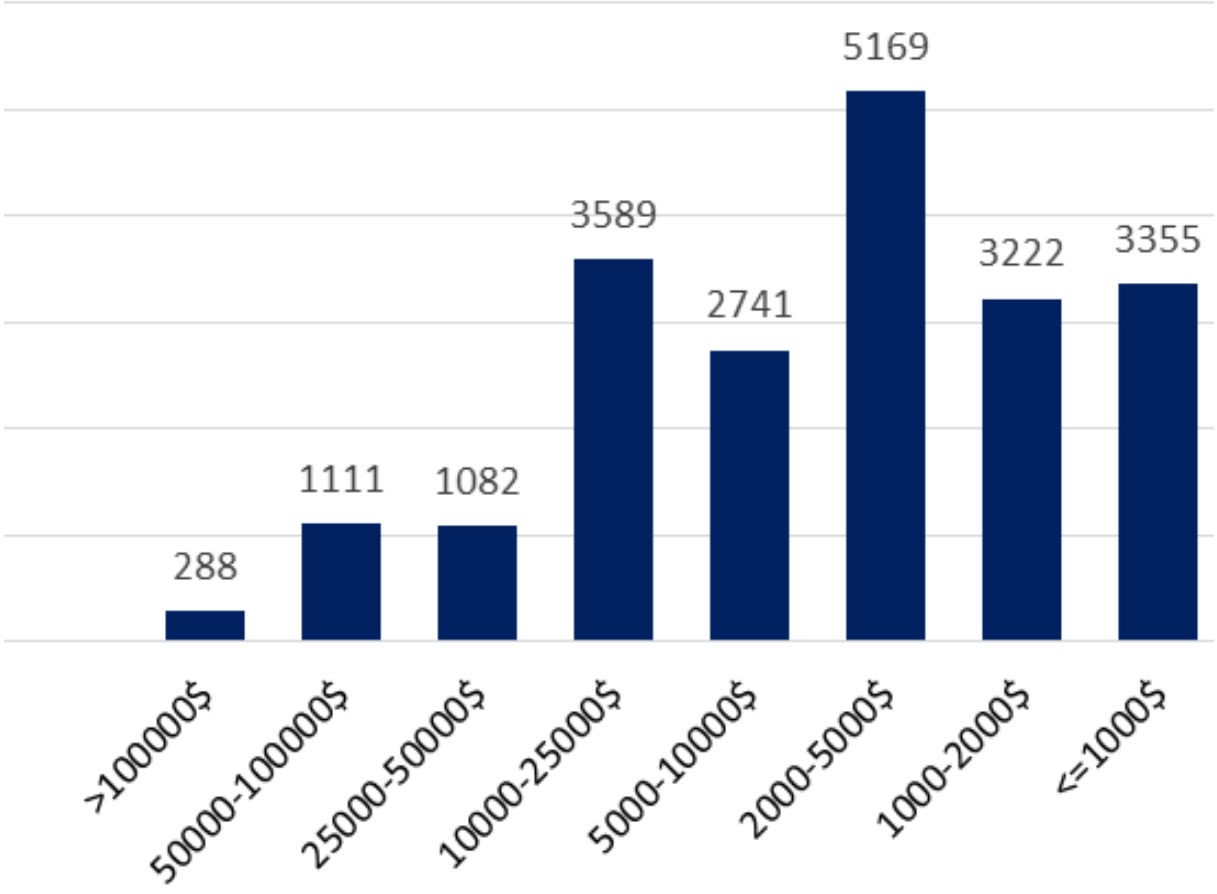
ویژگی حائز اهمیت دیگر که در قابلیت سوءاستفاده از آسیب‌پذیری تعیین‌کننده است؛ نیاز به تعامل با کاربر است. چنانچه به منظور سوءاستفاده از آسیب‌پذیری نیاز به تعامل با کاربر باشد؛ مهاجم بایستی پیش از حمله زمینه فریب کاربر را فراهم کند. در نتیجه سوءاستفاده از آسیب‌پذیری پیچیده‌تر بوده و سطح خطر آن کم‌تر است. نمودار ۳-۵ نسبت نیاز/عدم نیاز به تعامل با کاربر آسیب‌پذیری‌های سال

۱۳۹۹ را نشان می‌دهد.با توجه به این نمودار، مهاجم برای سوءاستفاده از ۷۴٪ آسیب‌پذیری‌ها نیازی به تعامل با کاربر ندارد.

نمودار ۳-۵- نیاز به تعامل با کاربر

۳.۳ ارزش روز صفر آسیب‌پذیری‌ها

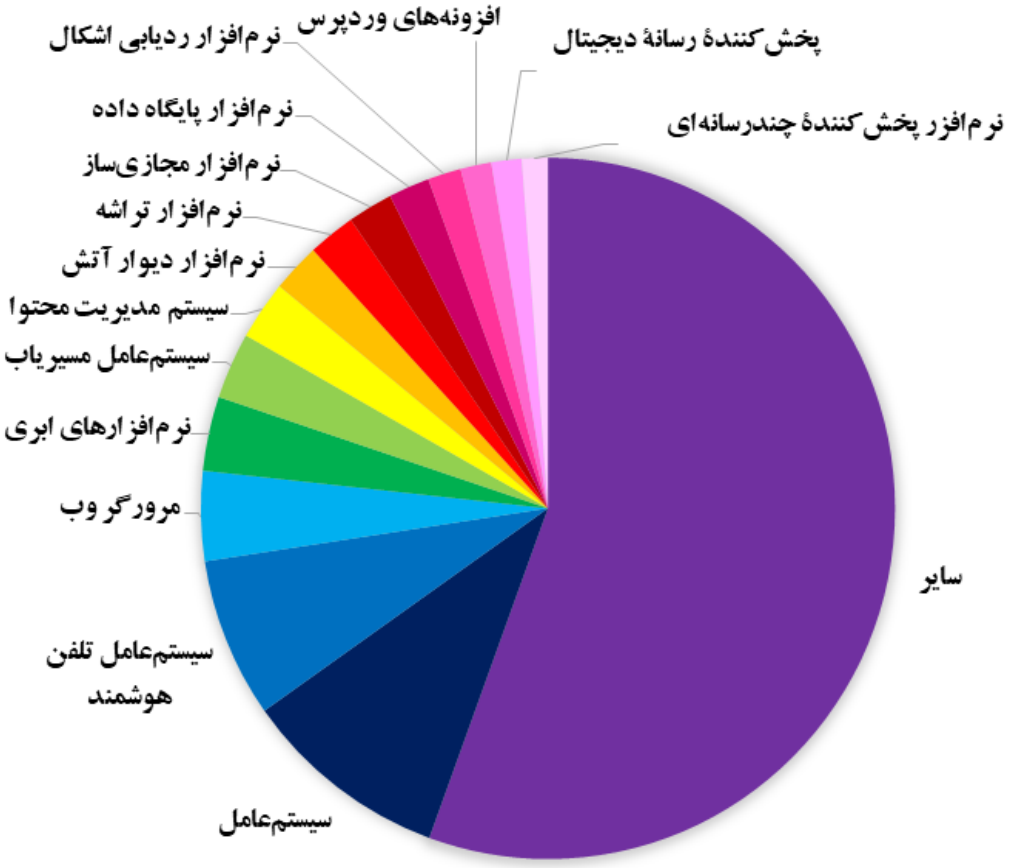
ارزش روز صفر یک آسیب‌پذیری، ارزشی است که آسیب‌پذیری قبل از اعلان عمومی و افشا دارد.استاندارد خاصی برای تعیین ارزش روز صفر آسیب‌پذیری وجود دارد. مقدار محاسبه‌شده عموماً با قیمت آسیب‌پذیری در بازار اکسپلویت مطابقت دارد. نمودار ۳-۶ ارزش روز صفر آسیب‌پذیری‌های سال ۱۳۹۹ در پایگاه آسیب‌پذیری VulDB را نشان می‌دهد.



نمودار ۳-۶ ارزش روز صفر آسیب‌پذیری‌های سال ۱۳۹۹

۴.۳ نوع محصولات آسیب‌پذیر

نمودار ۳-۷ نسبت انواع محصولات آسیب‌پذیر را نشان می‌دهد. بیشترین آسیب‌پذیری‌ها به سیستم‌های عامل مربوط می‌شوند. پس از آن سیستم‌های عامل هوشمند، مرورگرهای وب، نرم‌افزارهای ابری و سیستم‌های عامل مسیریاب‌ها قرار دارند. همچنین به دلیل تنوع زیاد محصولات، دسته‌ای با عنوان «سایر» در نمودار وجود دارد.



نمودار ۳-۷ انواع محصولات آسیب‌پذیر

تعداد زیاد آسیب‌پذیری‌ها و رشد آن‌ها نسبت به سال گذشته، لزوم توجه جدّی به بحث مدیریت آسیب‌پذیری در سازمان‌ها را روشن‌تر می‌نماید. بدین منظور لازم است تیم امنیت شبکه هر سازمان به طور پیوسته اخبار آسیب‌پذیری‌های مختلف و به خصوص آسیب‌پذیری‌هایی که در ارتباط با تجهیزات و یا نرم‌افزارهای مورد استفاده در آن سازمان را رصد کرده و با به‌روزرسانی نرم‌افزارها و اعمال وصله‌های امنیتی منتشر شده، اقدام به امن‌سازی شبکه کنند. تیم کارشناسی مرکز تخصصی آپا دانشگاه صنعتی اصفهان، مهم‌ترین آسیب‌پذیری‌ها را به صورت هفتگی در وب‌سایت خود به نشانی www.nsec.ir منتشر می‌کند.

۴

وضعیت امنیت سایبری ایران و رخدادهای آن در سال ۹۹

مروری بر رخدادهای مهم امنیتی کشور در سال ۹۹

به همراه بررسی آماری آلودگی‌ها و آسیب‌پذیری‌های کشور در سال گذشته

۴ وضعیت امنیت سایبری ایران و رخدادهای آن در سال ۹۹

۱.۴ مقدمه

برخلاف همیشه که روزهای نخستین سال حداقل از لحاظ اخبار داخلی امنیتی سایبری، روزهای آرامی بودند، سال ۹۹ پر هیاهو آغاز شد. خبر نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام در بستر اینترنت، خبر تکان‌دهنده‌ای بود که نه‌تنها در ایران بلکه در خبرگذاری‌های خارجی بازتاب گسترده‌ای داشت. در این بخش ابتدا، داده‌های سامانه ملی مقابله با بات و آسیب‌پذیری را تحلیل می‌کنیم و سپس به برخی رخدادهای مهم و پروژه‌های ملی بزرگ در حوزه فضای مجازی کشور می‌پردازیم و با دیدگاه امنیت سایبری، نتایج هر یک را بررسی می‌کنیم.

حمله منع خدمت انعکاسی/تقویتی

یکی از متداول‌ترین حملات منع خدمت توزیع شده، حمله منع خدمت از نوع انعکاسی/تقویتی (Amplification DDoS) است. در این نوع حمله مهاجم درخواست‌هایی ارسال می‌کند که اندازه آن‌ها از اندازه پاسخ دریافتی بسیار کوچک‌تر است. در صورتی که مهاجم بتواند تعداد زیادی از این درخواست‌ها را به قربانی هدایت کند، قربانی برای پاسخ‌دهی به این درخواست‌ها با کمبود منابع مواجه می‌شود. پروتکل‌های مختلفی هستند که نسبت به این حمله آسیب‌پذیر هستند و مهاجمین می‌توانند از آنها برای اجرای حمله منع خدمت توزیع شده سوءاستفاده نمایند. بر اساس داده‌های حاصل از سامانه ملی مقابله با بات و آسیب‌پذیری، بیشترین سرویس‌های آسیب‌پذیر نسبت به حمله منع خدمت تقویتی در سال ۱۳۹۹ در ایران بر اساس بیشترین تعداد تکرار در جدول شماره ۴-۱ نمایش داده شده است. یکی از مورد توجه‌ترین پروتکل‌ها که نرخ تقویت زیادی نیز دارد، پروتکل همگام‌سازی زمانی NTP است. توصیه می‌شود در صورتی که نیازی به همگام‌سازی زمانی ندارید این سرویس را غیرفعال نمایید. برای سایر پروتکل‌ها نیز توصیه می‌شود در صورت امکان دسترسی به پورت مذکور از طریق اینترنت را مسدود کنید و از پورت‌های غیر استاندارد برای این پروتکل‌ها استفاده کنید.

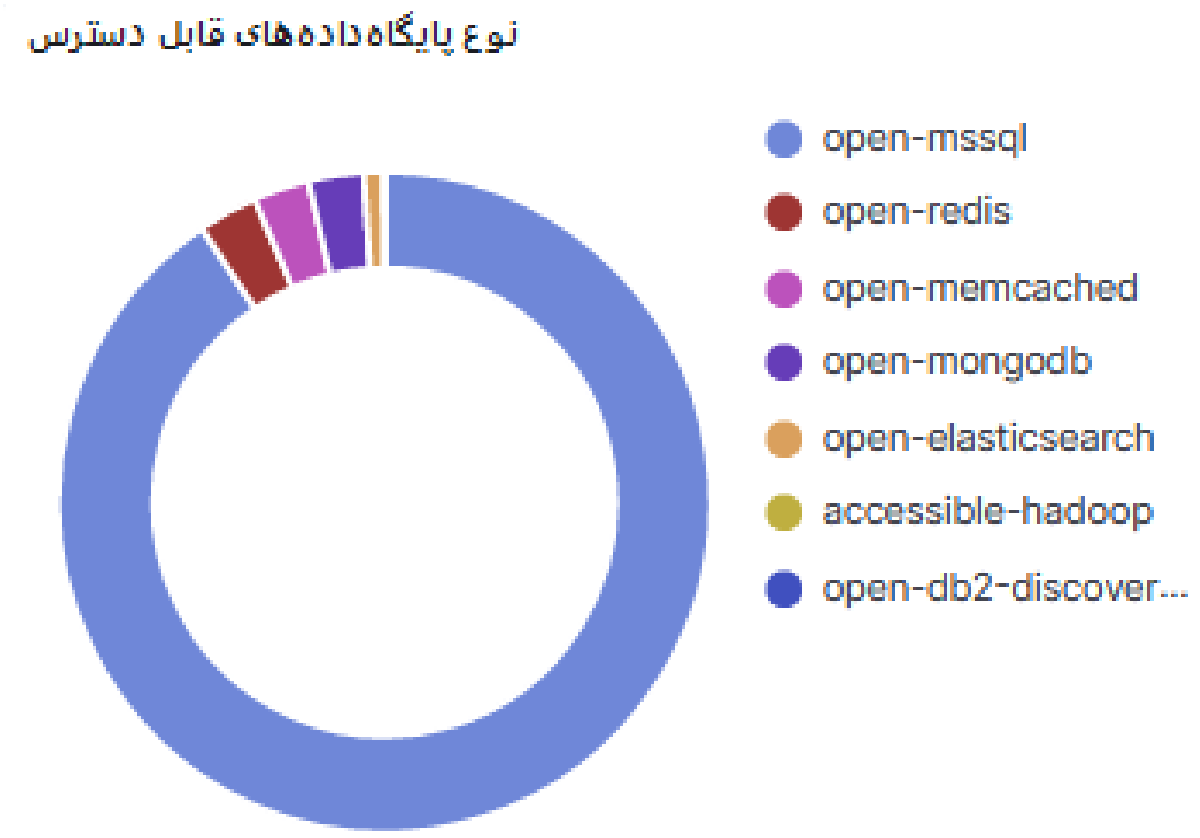
دسترسی به پورت مذکور از طریق اینترنت را مسدود کنید و از پورت‌های غیر استاندارد برای این پروتکل‌ها استفاده کنید.

نام سرویس	تعداد تکرار	شماره پورت
NTP	۴۸۹۴	۱۲۳
LDAP	۲۹۶۵	۳۸۹
CHARGEN	۱۴۲۱	۱۹
SSDP	۹۴۴	۱۹۰۰
TFTP	۶۷۶	۶۹
rpcbind	۶۶۴	۱۱۱
Memcached	۲۱۶	۱۱۲۱۱

جدول شماره ۴-۱، بیشترین سرویس‌های آسیب‌پذیر نسبت به حمله منع خدمت تقویتی در سال ۹۹ در ایران بر اساس بیشترین تعداد تکرار

پایگاه داده‌های قابل دسترس از طریق اینترنت

پایگاه داده‌های قابل دسترس از طریق اینترنت در ایران ۱۳۹۹ به صورت شکل ۴-۱ هستند. در صورت در دسترس بودن پایگاه داده از طریق اینترنت، امکان اجرای حمله بروت‌فرس برای مهاجمین، فراهم می‌شود. همچنین مهاجمین می‌توانند حملات منع سرویس روی پایگاه داده اجرا کنند و آن را از دسترس خارج نمایند. همچنین ممکن است از پایگاه داده به عنوان طعمه‌ای برای انجام حمله DDoS روی سیستم‌های دیگر در هر جای دنیا استفاده شود که باعث افزایش سطح تهدید به سیستم قربانی خواهد شد.



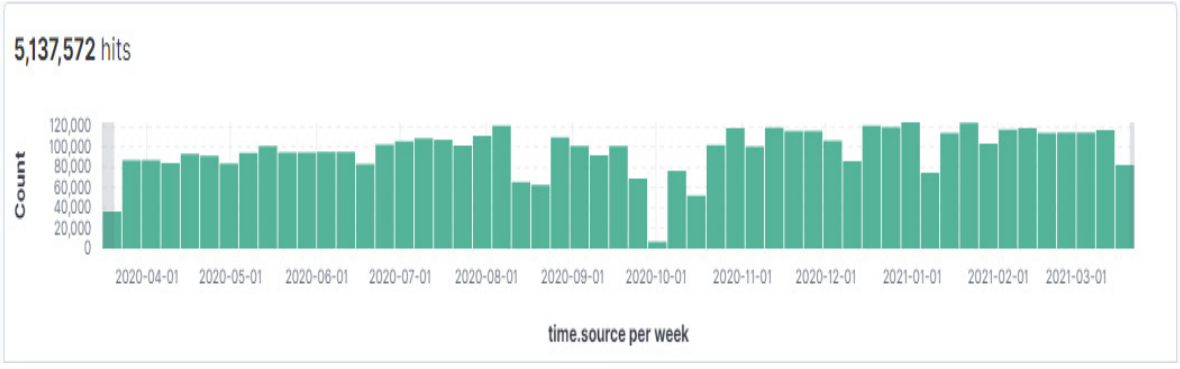
نمودار ۴-۱ پایگاه داده‌های قابل دسترس

دستگاه‌های دارای RDP متصل به اینترنت

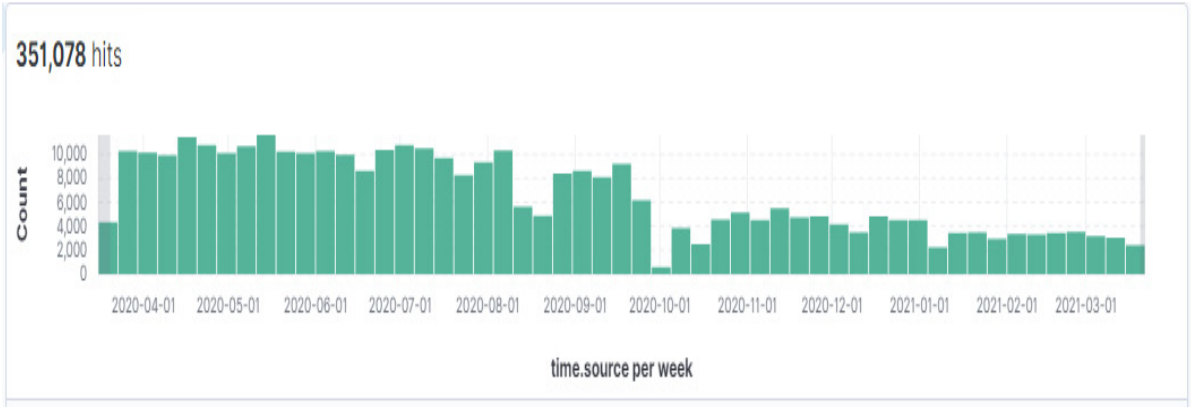
یکی از وقایع پس از شیوع کرونا، دورکاری کارمندان و کار در منزل از راه دور بوده است. عنصر کلیدی این دورکاری، استفاده از پروتکل RDP یا پروتکل دسکتاپ از راه دور است. این پروتکل برای کاربران امکان اتصال به سیستم‌هایشان در محل کار از راه دور را فراهم می‌کند. برای برقراری ارتباط با سیستم موجود در محل کار کارمند می‌بایست سیستم خود را برخط نگه دارد. به این ترتیب مهاجمین بسیاری جذب این پروتکل می‌شوند. آمارها حاکی از این است که در ۷۰-۸۰ درصد نفوذهای شبکه، سیستم‌های RDP متصل به اینترنت نقطه شروع حمله بوده‌اند. به عنوان نمونه طبق گزارش‌های دریافتی در سال اخیر، بسیاری از باج‌افزارها از طریق RDPهای در معرض اینترنت، خود را به سیستم قربانیان رسانده‌اند. مهاجمین برای شروع از حمله ساده حدس رمز عبور کاربر یا بروت‌فرس استفاده می‌کنند که این امر لزوم اهمیت بیش از پیش انتخاب رمز عبور پیچیده را برای RDP نشان می‌دهد. مهاجمین رمز عبورهای فروانی را آزمایش می‌کنند و در صورت رسیدن به رمز عبور صحیح، می‌توانند با موفقیت به سیستم شما دستیابی پیدا کرده و فعالیت‌های دلخواه خود را در سیستم انجام دهند.

زنگ خطر! به خاطر بسپارید هرگز از رمز عبورهایی مشابه با ۱۲۳۴۵۶ و موارد دیگری که توسط بسیاری از افراد استفاده می‌شوند و به راحتی قابل حدس زدن هستند استفاده نکنید.

بر اساس آمارهای ارائه شده توسط سامانه ملی مقابله با بات و آسیب‌پذیری، در سال گذشته در حدود ۵ میلیون دستگاه در کشور در حال استفاده از RDP و متصل به اینترنت بوده‌اند.



از این تعداد، ۳۵۱،۵۲۴ سیستم یعنی حدود ۷درصد سیستم‌ها دارای نسخه RDP نسبت به BlueKeep آسیب‌پذیر هستند.



برای مراقبت از سیستم‌های دارای RDP خود، رعایت موارد زیر توصیه می‌شود:

- استفاده از رمز عبورهای قوی
- استفاده از پورت‌های غیراستاندارد
- به روز رسانی و وصله کردن RDPهای آسیب‌پذیر
- در تنظیمات RDP ویندوز، Network Level Access را فعال کنید.
- سیستم‌های RDP خود را به طور مستقیم به اینترنت متصل نکنید و آنها را پشت دیوار آتش قرار بدهید.

حملات بروت‌فورس

در این حملات مورد توجه‌ترین پورت‌ها عبارتند از ۲۳، ۲۲ و ۷۵۴۷ که به ترتیب برای پروتکل‌های تلنت، SSH و CWMP هستند. مهاجمین به حمله به SSH علاقه فراوانی دارند به دلیل این که دسترسی شل را برای آن‌ها فراهم می‌کند.

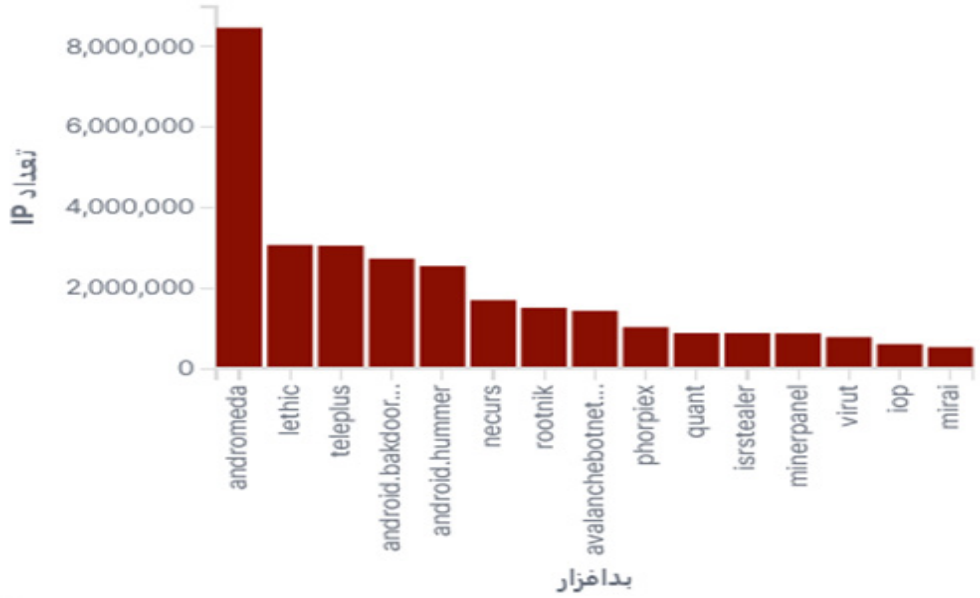
برای جلوگیری از خطر این حمله توصیه می‌شود که

- از رمز عبورهای قوی برای این سرویس‌ها استفاده کنید و رمز عبورهای خود را به صورت دوره‌ای تغییر دهید.

- با توجه به این که حملات خودکار روی SSH از پورت پیش فرض ۲۲ استفاده می‌کنند، سعی کنید از پورتی متفاوت برای این پروتکل استفاده نمایید. به طور کلی پورت‌های پیش فرض مورد استفاده پروتکل‌ها استفاده نکنید.

وضعیت آلودگی به بدافزار

گزارش‌های ارائه‌شده توسط سامانه ملی مقابله با آسیب‌پذیری‌های شبکه و بات نشان می‌دهد که بدافزار اندرومدا (Andromeda) که با نام‌های Gamarue و Wauchos نیز شناخته شده است در صدر آلودگی‌های سال ۹۹ قرار داشته است. بدافزار اندورمدا بات‌نتی است که برای توزیع بدافزارهای دیگر، سرقت اطلاعات و انجام فعالیت‌هایی مانند دزدی کلیک استفاده می‌شود. این بات‌نت برای اولین بار در سال ۲۰۱۱ ظاهر شد اما تاکنون در حال رشد و ادامه فعالیت خود است، به طوری که در حال حاضر



این بات‌نت، بیش‌ترین نرخ آلودگی در ایران را دارد. در سطح بین المللی برای مقابله با این بدافزار اقداماتی انجام شده و سرورهای فرماندهی و کنترل آن تحت کنترل محققین است. برای رفع آلودگی به این بدافزار به نظر می‌رسد اسکن و پاکسازی سیستم آلوده‌شده با آنتی ویروس به‌روز موثر باشد.

طبق گزارش‌های سامانه ملی مقابله با آسیب‌پذیری‌ها در کشور، دو بدافزار اندرویدی تله‌پلاس (teleplus) و پرایزمس (prizmes) نیز در صدر بدافزارهای اندرویدی سال ۹۹ بوده‌اند. تله‌پلاس از جمله اپلیکیشن‌هایی است که پس از فیلتر شدن تلگرام، به عنوان نسخه‌ای غیر رسمی از تلگرام در میان مردم رواج پیدا کرده است. کم نیستند از این دست برنامه‌های اندرویدی که در آشفتگی بازار پیام‌رسان‌ها از فیلتر شدن تلگرام برای رسیدن به مقاصد خود استفاده می کنند .

پزایزمس نیز یک تروجان اندرویدی است که در برخی از گوشی‌های ارزان قیمت چینی به صورت از پیش نصب شده قرارگرفته و در زنجیره تأمین، دستگاه پیش از رسیدن به دست مشتری آلوده به این بدافزار شده است. این بدافزار قابلیت دانلود، نصب و حذف برنامه، اجرای فرمان‌های شِل و بارگذاری یک URL در مرورگر را دارند که بسیار خطرناک هستند. اگرچه هم اکنون دامنه‌های کنترل و فرماندهی این بدافزارها تحت کنترل محققین است و خطر چندانی ندارند اما به طور کلی توصیه می‌شود پیش از واردات تلفن‌های هوشمند از ایمنی برنامه‌های نصب شده روی آنها اطمینان حاصل شود.

نام بات	تعداد
andromeda	8,455,533
lethic	3,005,431
teleplus	3,004,194
android.bakdoor-prizmes	2,684,591

جدول ۴-۳- آسیب‌پذیری ۵۲۴ سیستم دارای نسخه RDP نسبت به BlueKeep در ایران ۱۳۹۹

۲.۴ رمزارزها و تهدیدات امنیتی سایبری آن‌ها

افزایش کاربران ایرانی بیتکوین و سایر رمزارزها

در نیمه اول سال ۹۹ قیمت جهانی بیتکوین به طور ملایم از ۶۰۰۰ دلار تا ۱۱۰۰۰ دلار افزایش داشت اما در ایران با وجود افزایش نرخ دلار، قیمت بیتکوین از تقریباً ۹۵ میلیون تومان به تقریباً

۳۶۰ میلیون تومان در اواسط سال رسید که رشد به شدت چشم‌گیری برای دارندگان ایرانی بیتکوین به حساب می‌آمد. اما این تنها نیمه اول سال بود. نیمه دوم سال ۹۹، روزهای عجیبی در تاریخ بیتکوین رقم زد. قیمت جهانی آن هر روز رشد چشم‌گیری داشت تا این که اواخر آذرماه با گذشت از ۱۹,۸۳۴ دلار، رکورد قبلی قیمت خود را شکست و وارد کانال ۲۰ هزار دلار شد. آخرین رکورد قیمت بیتکوین ۱۹,۷۸۳ دلار بود که دقیقاً سه سال پیش از این تاریخ، یعنی در ۲۷ام آذرماه ۹۶ به ثبت رسیده بود. در نیمه دوم سال ۹۹، بیتکوین و البته به تبع آن، بسیاری از رمزارزهای دیگر روزبه‌روز رکورد جدیدی در قیمت خود به ثبت می‌رساندند. نمودار بیتکوین که کانال‌های قیمت دلاری خود را یکی از پس دیگری طی کرده بود در پایان سال ۹۹، همچنان شیب مثبتی داشت اما سال ۱۴۰۰ روی دیگری به بازار رمزارزها نشان داد. بیتکوین در اواخر فروردین‌ماه امسال، آخرین رکورد خود (تا زمان نوشتن این گزارش) یعنی رقمی نزدیک به ۶۳ هزار دلار (معادل تقریباً ۱ میلیارد و ۴۶۰ میلیون تومان) را ثبت کرد. پس از آن، گویی حباب بازار رمزارزها ترکید و قیمت دلاری بیتکوین که همچون فواره‌ای به اوج خود رسیده بود، سقوط خود را آغاز کرد. شیب شدیداً منفی نمودار بیتکوین، قیمت آن را در این روزها به ۳۳,۵۵۷ دلار رسانده است.

این افزایش شدید قیمت سبب شد تا روزبه روز مردم بیشتری چه در کشور ما و چه در سراسر جهان به سرمایه‌گذاری از طریق رمزارزها فکر کنند. به ویژه این که در سال ۹۹، شیب صعودی بازار بورس ایران، بیشتر اقشار جامعه را به سرمایه‌گذاران بورسی تازه‌کار اما پرامید تبدیل کرده بود. روزهای پر رونق بازار بورس، آمادگی ذهنی‌ای در کشور ما برای سرمایه‌گذاری در بازارهای مالی به وجود آورده بود که در کنار کاهش سقوط ارزش ریال، استقبال گسترده‌ای از رمزارزها در میان ایرانیان را رقم زد به طوری که در اوایل سال ۱۴۰۰ ارزش معاملات رمزارزها در ایران حدوداً ۱۰ هزار میلیارد تومان تخمین زده می‌شد. بسیاری از هم‌وطنان ما بدون کمترین اطلاعاتی از سازوکار رمزارزها و توجه به این نکته که بازار رمزارزها از جمله پرریسک‌ترین و غیرقابل‌پیش‌بینی‌ترین بازارهای مالی است به سرمایه‌گذاری دارایی خود در این بازارها پرداختند که همچون هر سرمایه‌گذاری بدون دانش و آگاهی، زیان‌ها و تهدیدهای فراوانی را برای آن‌ها به همراه داشت.

پروژه‌های کلاهبردارانه و مشکوک حوزه رمزارزها

سرمایه‌گذاری در رمزارزها، پروژه‌ها و صرافی‌های مشکوک و نامعتبر یکی از بزرگترین آفات این بازار بوده و هست. یکی از مشکوک‌ترین رمزارزهایی که توانسته بود به واسطه موسس ایرانی خود تبلیغات بسیاری در کشور بکند، توکن بریج اوراکل (BRG) است که مبتنی بر زنجیره بلوکی ترون (TRON) است. این توکن به عنوان اولین فناوری اوراکل عمومی بر روی شبکه ترون، هدف خود را کاهش هزینه‌ها برای کاربران عادی در در پرداخت‌های بریج اوراکل معرفی کرد. برخی از کارشناسان این پروژه جنجالی را کلاه‌برداری از نوع پانزی می‌دانستند. با این وجود، قیمت این رمزارز از اواسط آذرماه روند صعودی خود را آغاز کرد و در ششم اسفندماه به اوج خود یعنی ۰,۴۳ دلار رسید. پس از آن این رمزارز با وجود

قرار گرفتن در فهرست صرافی‌های مختلف در روند نزولی قیمت قرار گرفت.
۲۷ام اردیبهشت‌ماه سال جاری، خبر دستگیری سینا استوی، موسس این رمزارز تیر خلاصی بر آن بود. قیمت بریج اوراکل سقوط کرد و تاکنون ۹۹ درصد کاهش داشته است. سینا استوی، علاوه بر تأسیس توکن بریج اوراکل، مدیرعامل صرافی کریپتولند است. این صرافی از اولین پلتفرم‌های معاملات و خرید و فروش‌های رمزارزی است که خدمات معاملاتی بیش از ۳۰۰ رمز ارز را پشتیبانی می‌کرد و توانسته بود تندیس بهترین سایت کسب‌وکار سال ۹۹ در جشنواره وب و موبایل و تندیس مردمی بهترین شرکت‌ها و مؤسسه‌های خصوصی سیزدهمین جشنواره وب و موبایل را دریافت کند. سینا استوی همچنین نخستین توییت منتشرشده در توییتر را به مبلغ ۲.۵ میلیون دلار خریداری کرده بود.

با دستگیری سینا استوی، مرکز بررسی جرایم سازمان‌یافته سایبری، بیانیه‌ای در خصوص غیرمعتبربودن رمزارز بریج اوراکل منتشر کرد. نداشتن پشتوانه، تبلیغات شعاری، تمرکز عمده سرمایه در چند کیف پول، ایجاد نوسان جهت تخلیه سرمایه مردم، موج‌سازی‌های جعلی و غیرواقعی و همچنین قیمت‌سازی جعلی و .... تنها بخشی از شاخصه‌های کلاهبردارانه پروژه BRG طبق این بیانیه است. آقابابا‌گل، وکیل دادگستری و پژوهشگر حوزه زنجیره بلوکی، این پرونده را یکی از پیچیده‌ترین موارد به ویژه در استرداد دارایی مال‌باختگان می‌داند. چراکه از طرفی دارندگان این توکن همچنان مالک توکن خود (ولو با ارزش سقوط‌کرده) محسوب می‌شوند و این که برای آن‌ها خسارتی تعریف شود یا خیر، مورد ابهام است. از طرفی باید مشخص شود این توکن چه میزان سرمایه کلان جذب کرده است و اکنون چه میزان از این دارایی در اختیار سینا استوی است. خروجی دارایی از کشور، مبادله شدن با سایر رمزارزها و از بین رفتن دارایی به طرق مختلف، همگی از احتمالاتی هستند که ردگیری دارایی ازدست‌رفته سهام‌گذاران بریج اوراکل را سخت‌تر می‌کند.

در پی بازداشت استوی، وب‌سایت کریپتولند به حالت تعلیق درآمده و امکان واریز و برداشت پول برای کاربران وجود ندارد. این در حالی است که به دلیل نرخ پایین کارمزد، این صرافی تعداد بسیار زیادی کاربر داشت که اکنون نگران سرمایه مسدودشده خود هستند و تاکنون چندین بار در ورودی دادسرای ویژه رسیدگی به جرائم اقتصادی تجمع کرده‌اند. البته معاون اجتماعی پلیس فتا با تاکید براینکه دارایی مردم حفظ خواهد شده است از کاربران کریپتولند خواسته به سایت گرداب مراجعه کرده و اطلاعات خود، میزان دارایی و سرمایه‌ای را که وارد این مجموعه کرده‌اند به انضمام مدارک و مستندات وارد کنند تا شکایت آنها مورد بررسی قرار گیرد. اما همچنان زمان مشخصی برای بازگشت پول اعلام نشده است.

انجمن بلاکچین ایران با هدف روشن کردن چراغ قرمز و ایجاد حساسیت نسبت به پروژه‌های مشکوک در حوزه رمزارزها،اخیراً اقدام به تهیه فهرستی از رمزارزهای تحت ظن کلاهبرداری کرده است. در این فهرست نام صرافی‌های تبدیل آنلاین، آریانا، ای‌آی‌تریدز (AiTrades)، سینکروبیت (SynchroBit)، پرشیااکسچنج (Persia exchange)،کوین‌بیت‌اکسچنج (Coinobit Exchange)و ... آورده شده است. از

علاقه‌منـــدان حـــوزه رمزارزهـــا دعـــوت می‌شـــود کـــه بـــه مراجعـــه بـــه وب‌ســـایت آگاهـــی خـــود را در زمینـــه پروژه‌هـــای مشـــکوک ایـــن حـــوزه افزایـــش دهنـــد.
«متاســـفانه نبـــود قوانیـــن درســـت و دقیـــق در حـــوزه رمزارزهـــا آمـــار جرائـــم در ایـــن حـــوزه را نیـــز افزایـــش داده اســـت.» ســـرهنگ رامیـــن پاشـــایی، معـــاون اجتماعـــی پلیـــس فتـــا ناجـــا، در گفت‌وگـــو بـــا ایســـنا تاکیـــد کـــرده اســـت کـــه «بـــرای خریـــد و فـــروش رمزارزهـــا تاکنـــون هیـــچ صرافـــی مجـــازی در کشـــور وجـــود نـــدارد و تنهـــا برخـــی مجـــوز محـــدود دریافـــت کرده‌انـــد کـــه بـــر اســـاس ایـــن مجـــوز می‌تواننـــد رمـــزارز را فقـــط بـــرای مبـــادلات تجـــاری در اختیـــار کســـب‌وکارهای محـــدودی قـــرار دهنـــد.» ایـــن در حالـــی اســـت کـــه بســـیاری از ایـــن صرافی‌هـــا بـــه درگاه‌هـــای رســـمی بانـــک مرکـــزی متصـــل هســـتند کـــه همیـــن امـــر ســـبب ایجـــاد ابهـــام در قانونـــی بـــودن یـــا نبـــودن خریـــدو فـــروش رمزارزهـــا بـــرای علاقه‌منـــدان ایـــن حـــوزه شـــده اســـت. از طرفـــی، در ســـال اخیـــر شـــاهد پلتفرم‌هـــای تبـــادل رمـــزارز جعلـــی بوده‌ایـــم کـــه بـــا درگاه‌هـــای پرداخـــت جعلـــی، اقـــدام بـــه فیشـــینگ می‌کردنـــد.
ازدســـت‌رفته ســـهام‌گذاران بریـــج اوراکل را ســـخت‌تر می‌کنـــد.
در پـــی بازداشـــت اســـتوی، وب‌ســـایت کریپتولنـــد به حالـــت تعلیـــق درآمـــده و امکان واریـــز و برداشـــت پـــول بـــرای کاربـــران وجـــود نـــدارد. ایـــن در حالـــی اســـت کـــه بـــه دلیـــل نـــرخ پاییـــن کارمـــزد، ایـــن صرافـــی تعـــداد بســـیار زیـــادی کاربـــر داشـــت کـــه اکنـــون نگـــران ســـرمایه مسدودشـــده خـــود هســـتند و تاکنـــون چندیـــن بـــار در ورودی دادســـرای ویـــژه رســـیدگی بـــه جرائـــم اقتصـــادی تجمـــع کرده‌انـــد. البتـــه معـــاون اجتماعـــی پلیـــس فتـــا بـــا تاکیـــد براینکـــه دارایـــی مـــردم حفـــظ خواهـــد شـــده اســـت از کاربـــران کریپتولنـــد خواســـته بـــه ســـایت گـــرداب مراجعـــه کـــرده و اطلاعـــات خـــود، میـــزان دارایـــی و ســـرمایه‌ای را کـــه وارد ایـــن مجموعـــه کرده‌انـــد بـــه انضمـــام مـــدارک و مســـتندات وارد کننـــد تـــا شـــکایت آنهـــا مـــورد بررســـی قـــرار گیـــرد. امـــا همچنـــان زمـــان مشـــخصی بـــرای بازگشـــت پـــول اعـــلام نشـــده اســـت.
انجمـــن بلاکچیـــن ایـــران بـــا هـــدف روشـــن کـــردن چـــراغ قرمـــز و ایجـــاد حساســـیت نســـبت بـــه پروژه‌هـــای مشـــکوک در حـــوزه رمزارزها،اخیـــراً اقـــدام بـــه تهیـــه فهرســـتی از رمزارزهـــای تحـــت ظـــن کلاهبـــرداری کـــرده اســـت. در ایـــن فهرســـت نـــام صرافی‌هـــای تبدیـــل آنلایـــن، آریانـــا، اِی‌آی‌تریـــدز (AiTrades)، ســـینکروبیت (SynchroBit)، پرشیااکســـچنج (Persia exchange)،کوین‌بیت‌اکســـچنج (Coinobit Exchange)و ... آورده شـــده اســـت. از علاقه‌منـــدان حـــوزه رمزارزهـــا دعـــوت می‌شـــود کـــه بـــه مراجعـــه بـــه وب‌ســـایت آگاهـــی خـــود را در زمینـــه پروژه‌هـــای مشـــکوک ایـــن حـــوزه افزایـــش دهنـــد.
«متاســـفانه نبـــود قوانیـــن درســـت و دقیـــق در حـــوزه رمزارزهـــا آمـــار جرائـــم در ایـــن حـــوزه را نیـــز افزایـــش داده اســـت.» ســـرهنگ رامیـــن پاشـــایی، معـــاون اجتماعـــی پلیـــس فتـــا ناجـــا، در گفت‌وگـــو بـــا ایســـنا تاکیـــد کـــرده اســـت کـــه «بـــرای خریـــد و فـــروش رمزارزهـــا تاکنـــون هیـــچ صرافـــی مجـــازی در کشـــور وجـــود نـــدارد و تنهـــا برخـــی مجـــوز محـــدود دریافـــت کرده‌انـــد کـــه بـــر اســـاس ایـــن مجـــوز می‌تواننـــد رمـــزارز را فقـــط بـــرای مبـــادلات تجـــاری در اختیـــار کســـب‌وکارهای محـــدودی قـــرار دهنـــد.» ایـــن در حالـــی اســـت کـــه بســـیاری از ایـــن صرافی‌هـــا بـــه درگاه‌هـــای رســـمی بانـــک مرکـــزی متصـــل هســـتند کـــه همیـــن امـــر ســـبب ایجـــاد ابهـــام در قانونـــی بـــودن یـــا نبـــودن خریـــدو فـــروش رمزارزهـــا بـــرای علاقه‌منـــدان ایـــن حـــوزه

شده است. از طرفی، در سال اخیر شاهد پلتفرم‌های تبادل رمزارز جعلی بوده‌ایم که با درگاه‌های پرداخت جعلی، اقدام به فیشینگ می‌کردند.

۳.۴ حملات سایبری به سازمان‌ها و شرکت‌های ایرانی

حمله سایبری وسیع به سازمان بنادر

در روز ۲۲ام مهرماه سال ۹۹ در فضای مجازی، زمزمه‌هایی در مورد حمله سایبری به چند سازمان دولتی منتشر شد. در این روز، کارشناسان فناوری اطلاعات سازمان‌های دولتی، هشدارها و توصیه‌های امنیتی مبنی بر متوقف کردن سریع فرآیندهای به‌روزرسانی سیستمی، آنتی‌ویروس‌ها و فایروال‌ها دریافت کردند. فردای آن روز نیز مرکز ماهر در اطلاعیه‌ای از حمله مهم سایبری به دو سازمان دولتی خبر داد و اعلام کرد این حملات در حال پیگیری و رفع هستند. در همان روز ابوالقاسم صادقی، معاون امنیت فضای تولید و تبادل اطلاعات سازمان فناوری اطلاعات ایران در باره این حمله اشاره کرد که رخدادی مبتنی بر یک آسیب‌پذیری مهم و حیاتی از مراجع بین‌المللی بوده است و در وب‌سایت مرکز ماهر در رابطه با آن هشدارهایی داده شده بوده است. منظور آقای صادقی، آسیب‌پذیری مهم معروف به زیرولوگان با شناسه CVE-2020-1472 است که دو ماه پیش از تاریخ حمله، یعنی در ۲۱ مردادماه سال ۹۹ توسط مایکروسافت اطلاع‌رسانی عمومی شده بود. این آسیب‌پذیری با بالاترین سطح خطر (۱۰ از ۱۰) مربوط به فرآیند ویندوزی سروری Netlogon است که وب‌سایت مرکز تخصصی آپا دانشگاه صنعتی اصفهان نیز در همان هفته انتشار عمومی این آسیب‌پذیری در مورد آن هشدار داده بود. وب‌سایت مرکز ماهر نیز هشدارهایی در مورد این آسیب‌پذیری در تاریخ‌های ۲۶ شهریورماه و سوم مهرماه منتشر کرد. بنابراین با وجود اطلاع‌رسانی‌های عمومی چه در خارج و چه در داخل کشور و آن هم از طریق مراجع رسمی، متاسفانه این آسیب‌پذیری در سازمان‌های دولتی مهمی همچون سازمان بنادر وصله نشده بود.

پس از وقوع این حمله مرکز ماهر بیانیه‌ای صادر کرد و در آن توضیح داد که اگرچه هشدارهای پیشگیرانه برای مسئولین و کارشناسان دولتی در سطح ملی صادر شده است اما حمله صرفاً مربوط به دو سازمان دولتی بوده است. همچنین برخی دستگاه‌های دولتی بر اساس برداشت یا تحلیل خود پس از دریافت هشدارها اقدام به قطع موقت برخی خدمات و انجام تستهای فنی کردند که به دلیل احتیاط صورت گرفته است. اگرچه از نظر مرکز ماهر این اقدام ضرورتی نداشته است.

این حمله به گفته ابوالقاسم صادقی در ساعات اولیه تشخیص و متوقف می‌شود.

ایشان در مورد تشخیص این حمله توضیح داد که: «هماهنگی و انسجام بین دستگاه مربوطه مانند مرکز ماهر و افتای ریاست جمهوری و پلیس فتا همیشه در جریان است که در چنین مواقعی این هماهنگی و انسجام بیشتر هم می‌شود. رصد این حملات توسط این سه نهاد انجام شد و به صورت موازی از این رخداد باخبر شدیم.» وی همچنین در مورد خسارت این حملات عنوان کرد که خسارتی به مراکز وارد نشده است، البته وقتی حمله‌ای رخ می‌دهد نمی‌توان گفت اتفاقی نیفتاده است، اما مسئله مهم این است که زمان بروز چنین اتفاقاتی به سرعت عکس‌العمل نشان دهیم و سعی کنیم آسیب‌ها را به حداقل برسانیم که همین اتفاق نیز رخ داده است.

در ۲۴ مهرماه، سازمان بنادر و دریانوردی درخصوص حمله سایبری به این سازمان در بیانیه‌ای اعلام کرد که کلیه ماموریت‌های این سازمان در بنادر بدون وقفه در جریان است. همچنین در این اطلاعیه ذکر شده است که اقدامات فنی خوبی توسط کادر مجرب فناوری اطلاعات این سازمان برای تقویت پایداری خدمات برخط در حال انجام است تا روند تخلیه و بارگیری و ورود و خروج کالا از کشور؛ حتی لحظه ای دچار خلل نشود.

قابل ذکر است که آسیب‌پذیری زیرولوگان بازتاب جهانی بسیاری نیز داشته است که در بخش رخدادهای خارجی این گزارش نیز به آن‌ها پرداخته شده است.

چنین مواقعی این هماهنگی و انسجام بیشتر هم می‌شود. رصد این حملات

توسط این سه نهاد انجام شد و به صورت موازی از این رخداد باخبر شدیم.» وی همچنین در مورد خسارت این حملات عنوان کرد که خسارتی به مراکز وارد نشده است، البته وقتی حمله‌ای رخ می‌دهد نمی‌توان گفت اتفاقی نیفتاده است، اما مسئله مهم این است که زمان بروز چنین اتفاقاتی به سرعت عکس‌العمل نشان دهیم و سعی کنیم آسیب‌ها را به حداقل برسانیم که همین اتفاق نیز رخ داده است.

در ۲۴ مهرماه، سازمان بنادر و دریانوردی درخصوص حمله سایبری به این سازمان در بیانیه‌ای اعلام کرد که کلیه ماموریت‌های این سازمان در بنادر بدون وقفه در جریان است. همچنین در این اطلاعیه ذکر شده است که اقدامات فنی خوبی توسط کادر مجرب فناوری اطلاعات این سازمان برای تقویت پایداری خدمات برخط در حال انجام است تا روند تخلیه و بارگیری و ورود و خروج کالا از کشور؛ حتی لحظه ای دچار خلل نشود.

قابل ذکر است که آسیب‌پذیری زیرولوگان بازتاب جهانی بسیاری نیز داشته است که در بخش رخدادهای خارجی این گزارش نیز به آن‌ها پرداخته شده است.

حمله سایبری ناموفق به بندر شهید رجایی

روز دوشنبه ۲۹ اردیبهشت‌ماه سال ۹۹، روزنامه واشنگتن پست در گزارشی به نقل از یک مقام دولت آمریکا و مقامات رسمی «یک دولت خارجی» مدعی شد که رژیم صهیونیستی علیه تأسیسات بندر شهید رجایی ایران حمله سایبری داشته است. در این خبر نوشته شده

است که سیستم‌های کامپیوتری که جریان شناورها، کامیون‌ها و کالاها را تنظیم می‌کنند همه یک باره از کار افتاده‌اند و فرآیند پشتیبان‌گیری گسترده‌ای را در آبراه‌ها و جاده‌های منتهی به تأسیسات منجر شده‌اند. این روزنامه همچنین ادعا کرد بود که این حمله در واکنش به عملیات سایبری‌ای رخ داد است که به «تاسیسات آبی روستایی اسرائیل» انجام شده است. در پنج و ششم اردیبهشت‌ماه، زیرساختهای شبکه اسکادای شرکت‌های تصفیه فاضلاب در اسرائیل مورد حملات سایبری قرار گرفتند. یک ماه پس از این حمله، ادعایی فاکس‌نیوزی مطرح شد که این حمله را به هکرهای ایران مرتبط می‌دانست. ادعایی که از جانب مقامات کشور ما تکذیب شده است. در پی این ادعا، اسرائیل یک «نشست فوق محرمانه» برگزار کرد تا در مورد نحوه انتقام از حمله منتسب به ایران، تصمیم‌گیری شود. از این رو روزنامه واشنگتن پست، اختلال ایجاد شده در بندر شهید رجایی ایران را حمله رژیم صهیونیستی و برای انتقام می‌دانست. این روزنامه همچنین تلاش کرده است تا در متن گزارش خود ابعاد این اختلال را وسیع جلوه دهد.

اما به نظر می‌رسد برخلاف ادعاهای انجام شده مبنی بر گستردگی اختلال در بندر شهید رجایی، این حمله سایبری چندان موفق نبوده است. مسئولان ذیربط در بندر شهید رجایی تاکید کرده‌اند که با توجه به آمادگی کامل واحدهای پدافند غیرعامل در تأسیسات بندر شهید رجایی و مقابله به موقع و مؤثر با اشکالات به وجود آمده، این حمله نتوانسته هیچ‌گونه اخلالی در روند فعالیت‌های جاری ایجاد کند و موجب توقف هیچ یک از عملیات پهلوگیری، تخلیه و بارگیری کشتی‌ها نشده است. مدیرکل بنادر و دریانوردی هرمزگان در این رابطه اعلام کرد که این اختلال از روز گذشته آغاز شده بود و علت آن در دو سِرور شرکت‌های سینا و بتا در بندر شهید رجایی بررسی شده است. طبق گفته ایشان طبق، کمتر از یک روز با تلاش کارشناسان فنی این اختلال برطرف می‌شود. قابل ذکر است که بندر شهید رجایی دروازه طلایی اقتصاد ایران نامیده می‌شود که سهم ۵۰ درصدی از تجارت ایران را به خود اختصاص داده است.

حمله سایبری گسترده به زیرساخت‌های ابر آروان

اواخر اسفندماه ۹۹، زیرساخت رایانش ابری آروان در دیتاسنتر IR-THR-AT1 تحت حملات سایبری قرار گرفت که هدف از آن‌ها تخریب و حذف اطلاعات مشتریان گزارش شد. به گزارش وب‌سایت رسمی این شرکت، این حمله در حدود ۱۶درصد از مشتریان غیررایگان ابر آروان را متاثر کرد. در این حمله، آن گروهی از مشتریان دچار مشکل اساسی شدند که از داده‌های خود نسخه پشتیبان نداشتند، یا معماری آن‌ها به شکل ابرزی (Cloud Native) نبود و به شکل Multi Availability Zone طراحی نشده بودند.

در گزارش این حمله آمده که پس از تشخیص حمله، ابر آروان تمام دسترسی‌ها به این دیتاسنتر را قطع می‌کند تا از توسعه‌ی آسیب‌رسانی جلوگیری شود. سپس اینترنت و شبکه‌ی مدیریتی، هر دو به‌شکل کامل قطع و کارشناسان به محل دیتاسنتر اعزام می‌شوند تا بدون نیاز به دسترسی از

راه دور -که ریسک گسترش یا تکرار حمله را افزایش می‌داد- به بررسی و حل موضوع بپردازند.

با فیکس‌کردن و یکپارچه‌سازی داده در سطح کلاستر، ابر آروان می‌تواند امکان دسترسی به اطلاعات را در صبح ۲۷ام فراهم کند. با تداوم کار تیم‌های فنی صبح روز پنج‌شنبه ۲۸ اسفند مشکلات ریکاوری برطرف و دسترسی مشتریان به این دیتاسنتر باز شد. اما فردای آن روز، ابرآروان برای پایدارسازی کلاستر ذخیره‌سازی، دوباره مجبور به قطع دسترسی مشتریان خود می‌شود. درنهایت از روز ۱۷ام فروردین ۱۴۰۰ با پایدارسازی زیرساخت و امکان دسترسی به ابرک‌ها، روند بازگردانی سرورهای ابری مشتریان از سر گرفته می‌شود. ابرآروان برای جبران خسارت مشتریان خود پس از راه‌اندازی مجدد سرورهای ابری‌اش، تا پایان بهار ۱۴۰۰، محصول فضای ذخیره‌سازی ابری خود را تا سقف ۱۰ ترابایت برای هر مشتری در این دیتاسنتر و بدون محدودیت ترافیک، رایگان کرد تا روند پشتیبان‌گیری از اطلاعات برای مشتریان تسهیل شود. هم‌چنین حساب کاربری تمام مشتریان این دیتاسنتر برای محصول رایانش ابری که در این حمله آسیب دیده بود، سه‌برابر مصرف اسفند ۹۹ آنان، شارژ شد تا به این شکل تا پایان بهار ۱۴۰۰ بتوانند به رایگان از زیرساخت رایانش ابری آروان استفاده کنند.

درنتیجه این حمله و با وجود کوشش این شرکت، امکان بازیابی ۶.۴ درصد از ابرک‌ها وجود نداشت که تلاش شد داده‌های این ابرک‌ها به ابرک جدید منتقل شود. ابر آروان مدعی است که در این حمله، مهاجمین هیچ‌گونه دسترسی به داده‌های مشتریان پیدا نکرده‌اند و تنها موفق به آسیب زدن به اطلاعات و پاک کردن بخشی از آن شدند.

۴.۴ پروژه عظیم شبکه ملی اطلاعات

شبکه‌ای ملی اطلاعات پروژه‌ای است که ایده آن در سال ۱۳۸۴ در کشور مطرح شد و مهمترین دلیل پیاده‌سازی این شبکه درآن سال کاهش وابستگی به شبکه جهانی اینترنت اعلام شد. این پروژه که با نام‌های دیگری مانند اینترنت ملی، اینترانت ملی ایران و شبکه ملی اینترنت نیز شناخته می‌شود، در طی این سال‌ها روندی کند و فرسایشی داشته است اما به نظر می‌رسد اقدامات انجام شده در سال ۹۹، به تحقق آن سرعت بخشیده است. در شهریور ماه سال ۹۹، شورای عالی فضای مجازی، مصوبه‌ای با موضوع «طرح کلان و معماری شبکه ملی اطلاعات» را به تصویب رساند. در مقدمه این مصوبه در باب اهمیت این پروژه نوشته است که:

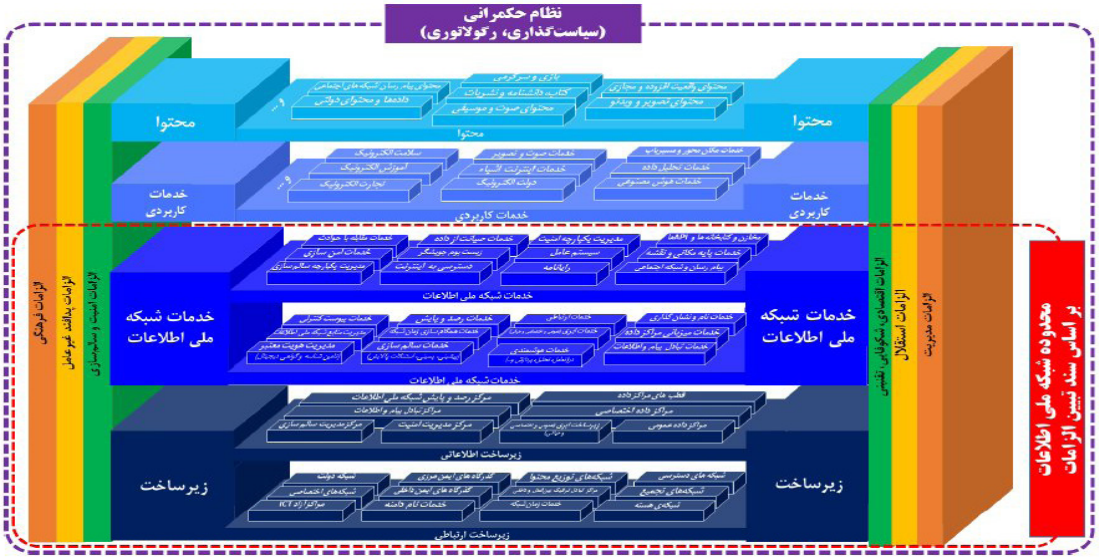
«تحقق استقلال کشور، کاهش وابستگی و جلوگیری از دست‌اندازی بیگانگان در فضای مجازی، تأمین نیازهای عمومی مردم و ایجاد زیست بوم متناسب با فرهنگ اسلامی ـ ایرانی، منوط به تحقق شبکه ملی اطلاعات و مستلزم فعالیت نظام مند و فراگیر در تقویت، ساماندهی و توسعه محتوا و خدمات کاربردی فضای مجازی است.»

تعدد نام‌ها و مصوبات متعددی که درباره این شبکه وجود دارد، نشان می‌دهد تاکنون این پروژه چندین بار مورد بازبینی قرار گرفته است. تا پیش از انتشار این مصوبه در برداشت از شبکه ملی اطلاعات ابهامات زیادی وجود داشت و حتی بین مسئولان در مجموعه‌های مختلف متولی راه‌اندازی و نظارت بر این شبکه، درباره تعریف و وظایف آن اتفاق‌نظر وجود نداشت. یکی از موضوعات مهم مورد سوال و ابهام هم زیرساخت شبکه ملی اطلاعات و تفاوت آن با توسعه زیرساخت های فعلی خارج از شبکه ملی است.

یکی از ابهامات مهم در تعداد لایه‌هایی بوده است که این پروژه در بر می‌گیرد. در ابتدا شورای عالی فضای مجازی در اولین مصوبه جلسه پانزدهم خود، فضای مجازی را با یک مدل چند لایه‌ای مطابق شکل ۴-۴ تعریف کرد. در آن زمان، پروژه شبکه ملی اطلاعات قرار بود به عنوان زیرساخت ارتباطی فضای مجازی کشور، تنها لایه زیرین این ساختار را در برگیرد. شبکه ملی اطلاعات در آن زمان محدود به شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده بود؛ به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری شود، به هیچ وجه از طریق خارج کشور مسیریابی نشود تا امکان ایجاد شبکه‌های اینترانت، خصوصی و امن داخلی در آن فراهم شود.

شکل ۴-۴ شبکه ملی اطلاعات به عنوان تنها یک زیرساخت فضای مجازی براساس اولین مصوبه جلسه پانزدهم شورای عالی فضای مجازی

همانطـــور کـــه ذکـــر شـــده در طـــی ایـــن سـال‌ها، شـــورای عالـــی فضـــای مجـــازی چنـد مصوبـه در مـورد شـبکه ملـی اطلاعـات ظـرف سـال‌های گذشـته داشـته اسـت. آنچـه کـه در ایـن مصوبه‌هـا مشـخص نبـود ایـن اسـت کـه آیـا شـبکه ملـی اطلاعـات در مصوبه‌هـا جدیـد، عـلاوه بـر زیرسـاخت، بخـش محتـوا و خدمـات را نیـز در بـر می‌گیـرد یـا خیـر. مصوبـه اخیـر توانسـت پـروژه شـبکه ابنترنـت ملـی، همچـون بسـیاری از پروژه‌هـای کلان کشـوری موافقیـن و مخالفیـن خـود را دارد. از مـوارد بسـیاری مهمـی کـه موافقیـن ایـن طـرح بـر آن تاکیـد می‌کننـد، موضـوع امنیـت اطلاعـات کاربـران اسـت. معـاون راهبـری فنـی مرکـز ملـی فضـای مجـازی در ایـن رابطـه بـه خبرگـذاری ایرنـا تصریـح کـرده



شکل ۴-۵ مدل مفهومی از فضای مجازی کشور براساس مصوبه شصت و ششم شورای عالی فضای مجازی

مشـخص کنـد کـه دقیقـاً معمـاری شـبکه ملـی اطلاعـات چیسـت و تمایـز بیـن شـبکه ملـی اطلاعـات و فضـای مجـازی در حـال حاضـر چگونـه تعریـف می‌شـود. در ایـن مصوبـه، مـدل مفهومـی کامل‌تـری از فضـای مجـازی کشـور ترسـیم شـده اسـت (شـکل ۴-۵) کـه نشـان می‌دهـد کـه لایه‌هـای محتـوا و خدمـات کاربـردی خـارج از قلمـرو شـبکه ملـی اطلاعـات براسـاس سـند تبییـن الزامـات ایـن شـبکه اسـت. البتـه در ایـن سـند ذکـر شـده اسـت کـه تأمیـن نیازهـای ملـی فضـای مجـازی، تحقـق اسـتقلال و کاهـش وابسـتگی و مداخلـه بیگانـگان در فضـای مجـازی کشـور، مسـتلزم شـکل گیـری و پیشـرفت تمامـی لایه‌هـا، بـه صـورت همگـن و هماهنـگ اسـت.

اسـت کـه: «اکنـون تمامـی خدمـات فضـای مجـازی توجـه ویـژه بـه تأمیـن امنیـت خـود دارنـد، بـا ایـن حـال همچنـان حمـلات متعـدد داخلـی و خارجی، خسـارات زیـادی را متوجـه کسـب و کارهـای آنلایـن می‌کنـد. مـا معتقدیـم رکـن اصلـی برقـراری امنیـت فضـای مجـازی توسـط شـبکه ملـی اطلاعـات تأمیـن می‌شـود و تـا آن نقطـه مسـیر طولانـی در پیـش داریـم...آن انتظـاری کـه شـورای عالـی فضـای مجـازی از شـبکه ملـی اطلاعـات ایـن اسـت کـه شـبکه ملـی اطلاعـات بایـد به‌عنـوان سـپر محافظتـی محتـوا و خدمـات فضـای مجـازی کشـور عمـل کنـد و فرقـی هـم نمی‌کنـد کـه تهدیـدات و حمـلات از مبـدأ خارجـی باشـد یـا داخلـی.»

۵.۴ تنظیم قرارداد برای پروژه ملی ابر ایران

در اواسط دی‌ماه سال ۹۹، سازمان فناوری اطلاعات، پروژه ملی «ابر ایران» را با همکاری بخش خصوصی رونمایی کرد. این پروژه در حقیقت قراردادی است که به‌منظور توسعه، تجهیز و راه‌اندازی سرویس ابری روی ۱۰ دیتاسنتر موجود در کشور منعقد شد. در این پروژه ۲۴۰۰ میلیاردی، آورده دولت ۵۰۰ میلیارد تومان و مابقی توسط مجموعه‌های خصوصی همچون «آسیاتک»، «ابر آروان»، «فناپ»، «امید ژرف نگر» و «ابر زس» تأمین شده است. امیر ناظمی، رییس سازمان فناوری اطلاعات ایران، این طرح را موجب تمرکززدایی از حیطه خدمات و توزیع ترافیک داده معرفی کرد. اتفاقی که از نظر وی هم منافع اقتصادی دارد و هم به منافع امنیتی کمک می‌کند. اما در میان اهداف کلانی که ناظمی برای این پروژه ذکر کرد، مورد «کاهش وابستگی به اینترنت بین‌الملل» نگرانی بسیاری از کاربران در فضای مجازی را برانگیخت. به گزارش زومیت، باتوجه‌به قطعی اینترنت در آبان ۱۳۹۸، حال کاربران از این موضوع می‌ترسند که توسعه‌ی شبکه ملی اطلاعات و زیرساخت‌های مدنظر آن، به قطع دسترسی به اینترنت بین‌الملل منجر شود. از این رو نگرانی‌هایی بابت «ملی‌شدن» اینترنت و دریافت رانت از شرکت‌های خصوصی در همکاری با حاکمیت مطرح می‌کردند. انگشت اتهام بیش از همه به‌سمت شرکت ابر آروان بود که پیش‌ازاین هم اعلام کرده قطع دسترسی مردم ایران به اینترنت بین‌الملل خط‌قرمزش است. ابرآروان این گونه واکنش نشان داد که: «پروژه‌ی ابر ایران هیچ ارتباطی با ایجاد پدیده ناموزون و نامیمون اینترنت ملی ندارد. تمام اینترنت ایران به‌شکل انحصاری به‌وسیله‌ی شرکت ارتباطات زیرساخت و در لایه‌ی بعدی اپراتورهای موبایل و FCP تهیه می‌شود و هیچ یک از زیرساخت‌های ابری ایران، مسیری برای دسترسی به اینترنت، خارج از این محدوده ندارند.» این شرکت ادعا می‌کند که پروژه ابر ایران برای وی هیچ چیز، جز اضافه شدن ۵ دیتاسنتر در شهرهای تبریز، کرج، شیراز، اصفهان و اهواز به این ابر یکپارچه نیست. ابرآروان در رابطه با «کاهش وابستگی به اینترنت بین‌الملل» توضیح می‌دهد که این جمله به افزایش نسبت ترافیک داخل ایران به ترافیکی که از کشورهای همسایه ترانزیت می‌شود، اشاره دارد. در این رابطه، حامد سعیدی یکی از فعالان مجازی در حوزه فناوری اطلاعات در توییتر از امیر ناظمی خواست تا در مورد پروژه ابر ایران شفافیت‌سازی بیشتری کند. در پاسخ، برخی اسناد پروژه ابر ایران منتشر شد. در این اسناد، طبق ماده چهارم با عنوان دفاع ملی و امنیت عمومی، شرکت ابرآروان در قرارداد ابر ایران به سازمان فناوری اطلاعات متعهد است که امکان شنود قانونی (LI) کلیه تجهیزات و سرویس‌ها را در صورت نیاز فراهم آورد. همچنین مدیریت قطع یا وصل و یا ایجاد محدودیت و اعمال

سیاست‌های کوتاه مدت و بلند مدت از تعهدات دیگر ابر آروان در پروژه ابر ایران است که حساسیت‌زا بودند.

ابر آروان در رابطه با شنود اطلاعات کاربران، ضمن اشاره به این که شنود قانونی (LI) به‌معنای وجود ابزار شنود نیست، توضیح می‌دهد که «ابر آروان در هیچ زمانی ترافیک مشتریان و کاربرانش را به‌شکل غیرقانونی و غیرمجاز شنود نخواهد کرد و هیچ نرم‌افزار یا تجهیزاتی وابسته به مراجع امنیتی یا قضایی با هدف ذخیره‌سازی یا شنود اطلاعات به‌شکل کلی یا جزیی در هیچ نقطه از شبکه ابرآروان وجود نداشته و ندارد. این شرکت کلید رمزنگاری و تایید هویت خود یا مشتریان خود را به‌شکل غیرقانونی در اختیار هیچ شخص یا نهادی نمی‌گذارد». البته ابر آروان در توضیح خود اشاره نکرده است که منظور از شنود قانونی و مجاز طبق قوانین کشور ما چیست.

ابر آروان همچنین در رابطه با دستور قطع یا محدودیت در ارایه خدمات دیتاسنترها این گونه پاسخ می دهد که: «مطابق با قرارداد ابر ایران و با توجه به این‌که این دیتاسنترها در مالکیت سازمان فناوری اطلاعات ایران قرار دارد، طرف اول قرارداد می‌تواند ابر آروان و سایر شرکت‌های برنده در مزایده را ملزم به قطع یا محدودیت در سرویس‌دهی کند. این موضوع ارتباطی با قطع اینترنت نخواهد داشت و تنها دسترسی مشتریان به خدمات ابری در دیتاسنترهای مذکور را محدود خواهد کرد.»

با وجود توضیحات این شرکت، همچنان انتقادات و حساسیت‌های زیادی متوجه پروژه ابر ایران و شرکت‌های خصوصی درگیر در آن است. در پی این اعتراضات در اردیبهشت‌ماه سال جاری، برخی کاربران معترض در اقدامی غیراخلاقی به انتشار تصاویر کارکنان ابر آروان به همراه پیام‌های تهدیدآمیز در شبکه‌های اجتماعی پرداختند. این شرکت با محکوم کردن این اقدام، یادآوری کرد که خود این شرکت سامانه‌ای با نام رادار را برای عموم مردم راه‌اندازی کرده است تا بتوانند درلحظه، اختلالات اینترنت در ایران را رصد کنند.

۶.۴ پدیده شوم سایت‌های شرط‌بندی

سایت‌های شرط‌بندی، پدیده‌ای شومی که چند سالی است بسیاری از هم‌وطنان ما را درگیر کرده است. برای جلوگیری از تداوم این پدیده، رئیس پلیس فتا تهران در مرداد ۹۹ اعلام کرد که یکی از مهم‌ترین اولویت‌های پلیس فتا در سال ۹۹ برخورد با سایت‌های شرط بندی بوده است. به گفته ایشان، اکثر کسانی که مورد طعمه سایت‌های شرط‌بندی و قمار قرار می‌گیرند بین ۲۰ تا ۲۵ سال سن دارند و بیشتر جوانانی هستند که سودای یک‌شبه پولدار شدن را در سر می‌پرورانند.

به گزارش راه پرداخت، وب‌سایت‌هایی شرط‌بندی که از درگاه‌های پرداخت اینترنتی استفاده می‌کنند، دارای چندین درگاه پرداخت هستند. زمانی که نهاد ناظر یکی از درگاه‌های این سایت‌ها را شناسایی می‌کند، به‌سرعت آن را قطع

خواهد کرد. از این رو این سایت‌ها تلاش می‌کنند در فاصله بین زمان شناسایی و مسدود شدن، بلافاصله درگاه بعدی را جایگزین کنند. گردش مالی این سایت‌های قمار و شرط‌بندی به‌شدت بالا است و این را می‌توان از تبلیغات زیادی که در شبکه‌های مجازی انجام می‌دهند، متوجه شد. در دی‌ماه سال ۹۹، بنابر اعلام مهران محرمیان، معاون فناوری‌های نوین بانک مرکزی ایران، اطلاعات ۷۰ هزار کاربر فعال ایرانی در سایتهای شرط‌بندی به قوه قضائیه ارسال شده است که این افراد توسط «سامانه هوشمند کشف جرایم مالی شبکه پرداخت» شناسایی شده‌اند.

در ابتدای سال ۱۴۰۰ نیز به گفته عبدالناصر همتی، رئیس پیشین بانک مرکزی از هموطنان درگیر در شبکه قمار و شرط‌بندی، ۶۰۰ هزار نفر توسط بانک مرکزی شناسایی شده‌اند که با ارسال پیامک به آن‌ها، در حدود ۹۲ درصد از آن‌ها فعالیت خود در این شبکه فاسد و غیرقانونی را متوقف کرده‌اند.

با وجود این تلاش‌های مثبت در سال اخیر همچنان لازم است اقدامات گسترده‌تر و جدی‌تری برای از بین بردن این پدیده شوم در کشور و به ویژه توسط بانک مرکزی و وزارت ارتباطات اتخاذ شود. در این مورد کارشناسان امنیت سایبری پیشنهاد می‌کنند که پس از شناسایی این وب‌سایت‌ها بلافاصله و بدون هیچ تعللی، درگاه خرید وب‌سایت مسدود شود تا فرصت کافی برای جایگزینی درگاه جدید وجود نداشته باشد. همچنین با مدیران بانک‌ها و درگاه‌های پرداخت واسط و غیرواسط متخلف برخورد جدی‌تری شود.

۷.۴ زنجیره پی‌درپی نشت‌های اطلاعاتی

نشت اطلاعات ۴۲ میلیون کاربر ایرانی تلگرام از عجیب‌ترین و قابل‌تأمل‌ترین اخبار سال ۹۹ است که در نخستین روزهای فروردین ۹۹ رخ داد. این اطلاعات روی سامانه‌ای به نام «سامانه شکار» قرار داشته که پایگاه داده الاستیک سرچ آن بدون کلمه عبور یا مکانیزم احزار هویت رها شده بوده است. به نظر می‌رسد اطلاعات این سرور در ۲۵ اسفندماه سال ۹۸ روی موتور جستجوی BinaryEdge ایندکس شده بود. باب دیاچنکو، کارشناس امنیت سایبری، این سروز را در ۲ فروردین‌ماه کشف می‌کند و مورد تحلیل قرار می‌دهد. سپس در پنجم فروردین‌ماه به صاحبان این پایگاه داده، مشکل را گزارش داده و اطلاعات در ششم فروردین از این پایگاه داده حذف شده‌اند. اما متاسفانه حذف اطلاعات در آن زمان نتوانست جلوی انتشار عمومی داده‌ها را بگیرد و اطلاعات در فروم‌های هکری با قیمت ۵۰۰ دلار به فروش رفت. در رابطه با منشا نشت این اطلاعات ابهاماتی وجود دارد.

برخی معتقد بودند که این اطلاعات از طریق پوسته‌های غیررسمی تلگرام افشا شده است اما یاشار شاهین‌زاده، یکی از کارشناسان امنیت سایبری فرضیه دیگری را مطرح کرد. وی در وب‌سایت خود این گونه توضیح می‌دهد که « قوی‌ترین فرضیه در مورد چگونگی جمع‌آوری این داده‌ها، ساخت مخاطب (contact) ساختگی با نام مستعار و کلیه شماره تلفن‌های موبایل و تعامل با API های تلگرام است. هدف جمع‌آوری این داده‌ها نگاشت شناسه تلگرام به شماره تلفن و نگاشت نام کاربری به شماره تلفن بوده است».

حتی اگر فرضیه دوم صحیح باشد یادآوری این نکته بسیار مهم است که تعداد نصب پوسته‌های غیررسمی تلگرام در میان کاربران ایرانی به عدد ۲۰ میلیون نزدیک است! پوسته‌هایی که گوگل‌پلی آنها را به‌دلیل مشکلات امنیتی حذف کرده است و حتی مدیر تلگرام هم آن‌ها را ناامن تلقی می‌کند ولی به علت فیلتر شدن تلگرام در ایران، محبوبیت و شهرت چندانی پیدا کردند. میلاد نوری، یکی از کارشناسان امنیتی در گفتگو با ایسنا از تشبیه جالبی در مورد پوسته‌های غیررسمی تلگرام استفاده می‌کند. وی می‌گوید: «خطر استفاده از تلگرام‌های غیررسمی هم مانند ویروس کرونا است. اگر خود شما رعایت کنید اما دیگران رعایت نکنند، شما همچنان در خطرید. اگر ۱۰۰ مخاطب داشته باشید که ۱۰ نفر آنها از تلگرام ناامن استفاده می‌کنند، چت‌های شما با ۱۰ نفر دراختیار پوسته‌های تلگرام است و زمانی که یک نفر از دو طرفی که با هم گفت‌وگو می‌کنند، به این پوسته‌ها دسترسی بدهد، اطلاعات دو نفر در معرض خطر است.»

قابل ذکر است که با وجود افشای

اطلاعات، اکنون برای جبران این خسارت کار خاصی نمی‌توان کرد. با این حال برخی پیشنهاد می‌کنند که تنها راهکار موجود پاک کردن اکانت و داده‌های موجود در آن و ساخت اکانت جدید با نام کاربری جدید است. هرچند این کار به قیمت از دست رفتن اطلاعات بر ابر تلگرام است. این نکته را نیز مدنظر قرار دهید که هرگز از پوسته‌های غیررسمی تلگرام استفاده نکنید.

زنجیره بعدی، نشت اطلاعات ۵ میلیون از کاربران فروشگاه اپلیکیشن سیب‌اپ بود. این اطلاعات که شامل نام، شماره تلفن و آدرس ایمیل برخی از مشتری‌ها می‌شد نیز بلافاصله پس از به حراج گذاشتن اطلاعات تلگرام و توسط همان گروه هکری به حراج گذاشته شد. در همین راستا این اپاستور ایرانی دو بیانیه منتشر کرد و ضمن تأیید این قضیه و عذرخواهی از مشتریانش، اشاره کرد که این نشت اطلاعات در اثر پیکربندی اشتباه فایروال یکی از ابزارهای مورداستفاده اتفاق افتاده است.
پس از آن، اطلاعات سازمان ثبت احوال بود که از طریق یک بات تلگرامی منتشر می‌شد. اطلاعات منتشرشده شامل نام و نام خانوادگی، کدملی و شماره تماس برخی از هم‌وطنانمان بود. با توجه به سخنان آقای ابوترابی، سخنگوی سازمان ثبت احوال، این اطلاعات برای تکمیل پرونده سلامت الکترونیک به وزارت بهداشت داده شده بود که متاسفانه وزارت بهداشت این اطلاعات را به اشتباه در سامانه غربالگری ویروس کرونا بارگزاری می‌کند که منجر به این نشت اطلاعات می‌شود. هکرها با توجه به اطلاعات افشاشده، بات تلگرامی توسعه می‌دهند که ادعا می‌کرد اطلاعات ۸۰ میلیون ایرانی را در اختیار دارد. البته در حال حاضر این بات غیرفعال شده است.

در اواسط خردادماه، اطلاعات ۵.۵ میلیون مشترک رایتل به قیمت ۱۰۰۰ دلار به فروش گذاشته شد. معاون وزیر ارتباطات و فناوری اطلاعات این خبر را تایید و اظهار کرد رایتل مسئول حفاظت از داده مشترکین است و باید برخورد مسئولانه‌ای از خود نشان دهد. رایتل نیز با صدور بیانیه‌ای درباره موضوع انتشار اطلاعات پنج و نیم میلیون مشترک این اپراتور رایتل اعلام کرد اخبار منتشره درخصوص درخواست فرد باجگیر از رایتل کذب محض است و حدس اصلی رایتل در خصوص نشر اطلاعات، توسط منشاء انسانی مربوط به سال ۹۴ و پیش از آن است.

در بهمن ماه نیز افشای اطلاعات برخی کاربران «پونیشا» توسط خود این استارتاپ تأیید شد. پونیشا در بیانیه‌ای نشت اطلاعات کاربرانش را تایید و اعلام کرده این داده‌ها مربوط به بخشی از پروفایل می‌شوند که اطلاعاتی از جمله نام، نام‌خانوادگی، شماره موبایل و موارد مرتبط با اطلاعات عمومی پروفایل کاربران است. البته پونیشا تاکیده کرده است که خوشبختانه دسترسی مستقیم به بانک اطلاعاتی و ذخیره اطلاعات کاربران رخ نداده است.»

در جریان این رخدادها، فرصت مناسبی برای مجرمین سایبری ایجاد شد که داده‌های ساختگی‌ای را تحت عنوان داده‌های مراکز مختلف به فروش برسانند. از جمله می‌توان به داده‌های جعلی اشاره کرد که تحت عنوان اطلاعات ۶۳ میلیون کاربر بانک صادرات در یکی

از بازارهای سیاه به فروش گذاشته شده بود یا اخبار کذبی که در رابطه با افشای اطلاعات قوه قضاییه، افشای اطلاعات محرمانه سایت آی‌نماد، انتشار حجم انبوهی از اطلاعات محرمانه وزات علوم، افشای اطلاعات کاربران پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک) و ... در فضای به گوش می‌رسید و همگی از طرف مراجع رسمی و برخی با ارائه دلایل مستدل فنی تکذیب شده‌اند.
مرکز ماهر در اقدامی برای جلوگیری از این نشت‌های اطلاعاتی در ۱۵ فروردین‌ماه سال ۹۹ اطلاعیه‌ای را منتشر کرد که در پی آن به ۳۶ پایگاه داده الاستیک سرچ فاقد احراز هویت اخطار داده می‌شد. این پایگاه‌داده‌ها می‌بایست در اسرع وقت از دسترس خارج و در غیر این صورت توسط مرکز ماهر به مراجع قضایی معرفی می‌شدند.
دو روز بعد مرکز ماهر اعلام کرد که تعداد پایگاه داده‌های الاستیک سرچ فاقد احراز هویت از ۳۶ مورد به ۳۰ مورد رسیده و در صورتی که مابقی همچنان فاقد احراز هویت باقی بمانند، به مراکز قضایی معرفی خواهند شد.

قابل ذکر است که بنا به تخمین‌های شرکت امنیتی سیمنتک، نشت اطلاعات در سازمان‌ها بطور متوسط ۲۰۵ روز پس از وقوع، کشف می‌شود. بیشترین آنها ۲۹۸۲ روز طول می‌کشد و البته برخی از نشت‌ها هرگز کشف نمی‌شوند. یکی از اقداماتی که می‌تواند خطر نشت اطلاعات سازمان‌ها را کاهش دهد، به کارگیری فرآیند DLP یا جلوگیری از فقدان داده است. جلوگیری از نشت اطلاعات در حین جابجایی، تشخیص ریسک‌های مربوط به خسارت اطلاعات و ایجاد یک استراتژی مناسب برای جلوگیری از هر

گونه نشت غیر مجاز به بیرون سازمان از جمله اقدامات DLP می‌تواند باشد.

همچنین علی کیایی‌فر، مدیر توسعه محصول شرکت مدبران در گفتگو با افتانا، برای کاهش نشت‌های اطلاعاتی به GDPR اشاره می‌کند که راهکار اتحادیه اروپا برای دفاع از حریم خصوصی شهروندان است. طبق قانون GDPR اگر یک شرکت در حراست از حریم خصوصی شهروندان سهل‌انگاری کرده و امنیت شهروندان را به خطر بیندازد باید ۴ درصد از سود سالیانه خود و یا ۲۰ میلیون یورو (هرکدام که بیشتر باشد) به عنوان جریمه پرداخت کند. این جریمه آن‌قدر سنگین و بازدارنده است که کسب‌وکارهای استارتاپی را وادار می‌کند که حفاظت از اطلاعات شهروندان را واقعا جدی بگیرند. زیرا می‌دانند سهل‌انگاری در این حوزه به معنای نابودی آنهاست. وی همچنین توضیح می‌دهد می‌توان با بومی‌سازی این قانون ریل‌های قانونی و ضوابط اجرایی آن را شفاف‌تر کرد.

این بخش را با پیامی از مرکز ماهر به پایان می‌رسانیم که در باب اهمیت اطلاع رسانی نشت اطلاعات به سازمان‌ها و دستگاه‌های مختلف یادآور می‌شود که «سکوت، پاسخ‌گویی مناسب نیست؛ بلکه تنها سرمایه اجتماعی را کاهش می‌دهد».

۵

رخدادهای مهم امنیتی جهان در سال ۱۳۹۹

سال ۱۳۹۹ به‌دلیل شیوع کرونا بی‌شک سالی فراموش‌نشدنی در حوزه فناوری اطلاعات است. مجرمان سایبری با استفاده از موضوعات مرتبط با کرونا و با استفاده از روش‌های مهندسی اجتماعی، کاربران بسیاری را هدف حملات خود قرار داده‌اند.

۵ رخدادهای مهم امنیتی جهان در سال ۹۹

۱.۵ مقدمه

سال ۱۳۹۹ به‌دلیل شیوع کرونا بی‌شک سالی فراموش‌نشدنی در حوزه فناوری اطلاعات است. مجرمان سایبری با استفاده از موضوعات مرتبط با کرونا و با استفاده از روش‌های مهندسی اجتماعی، کاربران بسیاری را هدف حملات خود قرار داده‌اند. حملات سایبری به مجموعه‌های بهداشتی/درمانی افزایش دوبرابری داشته است. شیوع کرونا، اهمیت امنیت زیرساخت‌های سایبری دردنیا را نشان داد؛ بسیاری از کسب‌وکارها دچار تعطیلی شده و به دنبال آن دورکاری کارمندان و استفاده گسترده از فضای سایبری را تجربه کردند. این امر موجب استفاده هر چه بیشتر از پروتکل‌هایی همچون دسکتاپ از راه دور (RDP) و شبکه‌های خصوصی VPN سازمان‌ها و ادارات شد که هدف حملات سایبری بسیاری واقع شدند. همچنین سال ۱۳۹۹ شاهد نشت اطلاعات حساس شرکت‌های مهم بودیم. به‌علاوه چندین آسیب‌پذیری بحرانی در محصولات مهم و پرکاربرد شناسایی و به‌طور گسترده در حملات سایبری مورد سوءاستفاده واقع شدند؛ از جمله آسیب‌پذیری‌های Solarwinds که پیش‌تر گفته شد و آسیب‌پذیری‌های مهم محصولات مایکروسافت که در این بخش به آن‌ها پرداخته می‌شود. در پایان این بخش نگاهی اجمالی به مهم‌ترین بدافزارهای سال برای بسترهای مختلف شده است.

۲.۵ اثرات سوء کرونا بر امنیت سایبری

در سال یکه‌تازی کووید-۱۹، مجرمان سایبری با استفاده از موضوعات مرتبط با کرونا همچون راه‌های درمانی کرونا، راه‌های تشخیصی، تعداد مبتلایان، اخبار مربوط به کشف واکسن و... و با استفاده از انواع روش‌های مهندسی اجتماعی، درصدد فریب کاربران بوده‌اند. کاربران با فرض این که چنین پیام‌هایی از سوی سازمان‌های بهداشت و درمان ارسال شده است؛ بر لینک‌های آلوده پیام‌ها کلیک کرده و/یا ایمیل‌های آلوده را می‌گشایند. بدین ترتیب عمدتاً سیستم‌های آنها به انواع بدافزارها از جمله باج‌افزارها، ویروس‌های خطرناک و... آلوده می‌شود. دورکاری و تعطیلی بسیاری از مدارس و دانشگاه‌های جهان نیز مزید بر علت شده است چراکه تعداد بیشتری می‌توانند هدف حملات سایبری قرار بگیرند.

علاوه بر این، حملات سایبری به سازمان/شرکت‌های مرتبط با بهداشت و درمان افزایش چشمگیری داشته است. به نقل از پژوهشگران، حملات سایبری با هدف قرار دادن سازمان/شرکت‌های مرتبط با بهداشت و درمان کرونا در سال ۱۳۹۹ دو برابر میزان معمول این حملات در سال ۱۳۹۸ بوده است. سازمان/شرکت‌های هدف عبارتند از: بیمارستان‌ها، تولیدکنندگان دارو، شرکت‌های درمانی و شرکت‌های فعال در حوزه انرژی که در زنجیره پیشگیری و درمان کرونا نقش دارند. عدم وجود اختلال در سیستم‌های این مجموعه‌ها، از اهمیت بسزایی برخوردار است. از این رو این مجموعه‌ها در صورت وقوع حمله، با انجام خواسته مجرمین سایبری، تلاش می‌کنند تا اختلالات سیستم‌های خود را رفع کنند.

شیوع کرونا، اهمیت زیرساخت‌های سایبری دردنیای امروز را نشان داد و میدان مبارزه با مجرمین سایبری را به حوزه بهداشت و درمان تغییر داد. مجموعه‌هایی که در گذشته کم‌تر مورد توجه بودند؛ با شیوع کرونا به صدر مهم‌ترین اهداف مهاجمین و گروه‌های تهدید رسیدند. از سوی دیگر در سال ۱۳۹۹ شاهد تلاش گروه‌های تهدید وابسته به دولت‌ها برای ایجاد اختلال در روند ساخت واکسن‌های کووید- ۱۹ و/یا سرقت اطلاعات مرتبط بودیم. برای مثال مایکروسافت در ماه نوامبر خبر از فعالیت گسترده مهاجمین منتسب به کره شمالی و روسیه داد و مدعی شد که بسیاری از آن‌ها، شرکت‌های دارویی و سازمان‌های پژوهشی را هدف قرار داده‌اند.

در یک مثال تازه‌تر، مهاجمین در جریان یک حمله سایبری علیه آژانس دارویی اروپا، به مستندات مربوط به واکسن دو شرکت فایزر و BioNTech دسترسی یافتند. این ماجرا تنها چند روز بعد از آن اتفاق افتاد که IBM هشدار داد که یک کمپین فیشینگ جهانی علیه سازمان‌هایی آغاز شده است که در حوزه نگه‌داری واکسن کووید-۱۹ در دمای مطلوب و حمل و نقل آن فعالیت دارند.

۳.۵ دورکاری و پیامدها امنیتی مرتبط با آن

یکی از بزرگ‌ترین تغییراتی که بسیاری از کسب‌وکارها در سال ۱۳۹۹ تجربه کرده‌اند؛ تعطیلی ادارات و به دنبال آن دورکاری کارمندان و استفاده گسترده از فضای سایبری بوده است. پژوهش‌ها نشان می‌دهد حدود ۹۱ درصد از شرکت‌ها و کسب و کارها در نقاط مختلف جهان شاهد افزایش حملات سایبری بوده‌اند و این مشکل به خصوص برای کارکنان دورکار آنها رخ داده است. از این رو امنیت سایبری اکنون از هر زمان دیگر اهمیت بیشتری دارد و در عین حال، هنگام پشتیبانی از کارمندان دورکار، دسترسی امن به سیستم‌های آن‌ها بزرگ‌ترین چالش پیش روی کارشناسان امنیت اطلاعات بوده است.

تفاوت قابل‌توجهی وجود دارد میان زیرساختی که کارکنان با استفاده از سیستم‌های خانگی برای دسترسی به برنامه‌های کاربردی به‌کار می‌برند و معماری شبکه‌های ارتباطی سازمان‌ها برای دسترسی کارکنان به تمام اطلاعات و خدماتی که به‌منظور ایفای نقش‌ها و وظایف روزمره از آن بهره می‌برند. زیرساخت‌هایی که به‌منظور انجام امور اداری از راه دور طراحی شده‌اند؛ پذیرای استفاده در مقیاس بزرگ و انتقال فوری نیروی کار به دورکاری نبودند. معمولاً معماری‌های VPN که برای گسترش شبکه‌های سازمانی/شرکتی استفاده می‌شوند قادر به کنترل باری که تمامی کاربران متصل به شبکه‌ها و دستگاه‌های غیرقابل‌اعتماد بر روی زیرساخت قرار می‌دهند، نیستند. این اتفاق منجر به عملکرد ضعیف و مسائل

دیگری می‌شود. مهاجمان با علم به این موضوع، کمپین های نقض سرویس توزیع‌شده یا DDoS را با موفقیت علیه زیرساخت‌های دسترسی از راه دور راه‌اندازی کردند.

آن دسته از سازمان‌هایی که فاقد هر گونه قابلیت دورکاری بوده‌اند؛ به سرعت با فراهم کردن دسترسی مستقیم RDP (پروتکل دسترسی از راه دور به دسکتاپ) به سیستم‌ها، به کاربران قابلیت اتصال از راه دور دادند. مهاجمان همچنین از این افزایش استفاده از RDP خارجی برای به خطر انداختن سیستم‌ها استفاده کردند. بدین‌ترتیب پروتکل RDP، از محبوب‌ترین مسیرهای نفوذ به سیستم قربانیان و عامل اصلی بیشتر حملات باج افزاری در سال ۱۳۹۹ بوده است. چندین شرکت امنیت سایبری با انتشار گزارش‌هایی بر این موضوع صحه گذاشته‌اند. برای مثال به نقل از یکی از این شرکت‌ها، بیش از هفتاد درصد حملات باج افزاری سال گذشته از حملات جستجوی فراگیر RDP نشأت گرفته است.

همزمان با افزایش دورکاری کارمندان ادارات و استفاده آنها از VPN برای دسترسی به شبکه‌های خصوصی شغلی، فعالیت مهاجمین برای نفوذ به VPNها نیز افزایش یافته است و سوءاستفاده از VPN یکی از رویکردهای مهاجمین برای انجام حملات باج‌افزاری در سال ۱۳۹۹ بوده است. بدین ترتیب با سوءاستفاده از آسیب پذیری VPN، مهاجمین به شبکه هدف نفوذ کرده و بسته به تخصص و توانمندی، به سرقت مایملک مادی و معنوی(اطلاعات) سازمان/شرکت‌ها پرداخته‌اند.

۴.۵ نشت اطلاعات کاربران و شرکت‌ها

سال ۱۳۹۹، اطلاعات بسیاری از کاربران برنامه‌های پرکاربرد نشت پیدا کرد. شهریورماه، پایگاه داده‌ای شامل اطلاعات استخراج‌شده از پروفایل نزدیک به ۲۳۵ میلیون کاربر TikTok، Instagram و YouTube یافت شد. همچنین اطلاعات مخاطبین میلیون‌ها کاربر تلگرام در دارک‌نت منتشر شد که ۷۰٪ این اطلاعات مربوط به کاربران ایرانی و ۳۰٪ مربوط به کاربران روسی بود. همچنین با نشت اطلاعات هفت نرم‌افزار ارائه‌دهنده VPN (لیست زیر)، ۱٫۲ ترابایت اطلاعات کاربرانشان در معرض دید عموم قرار گرفت. جالب آن که این نرم‌افزارها پیش‌تر مدعی بودند اطلاعات کاربران خود را ذخیره نمی کنند.

- Secure VPN
- SUPER VPN
- FAST VPN
- FREE VPN
- Rabbit VPN
- UFO VPN
- Flash VPN

علاوه بر کاربران، اطلاعات شرکت‌های بسیاری نیز سال ۱۳۹۹ نشت یافت؛ از جمله اطلاعات حساس سرورهای VPN شرکت Pulse Secure که متعلق به بیش از ۹۰۰ شرکت بود؛ افشا و در بازار سیاه خرید و فروش شد. نکته حائز اهمیت آن است که این اطلاعات زمینه را برای نفوذ مهاجمین به شبکه داخلی این شرکت‌ها فراهم کرد.

۵.۵ آسیب‌پذیری بحرانی Zerologon

آسیب‌پذیری Zerologon با شناسه آسیب‌پذیری CVE-2020-1472 یکی از خطرناک‌ترین آسیب‌پذیری‌های سال ۱۳۹۹، یک آسیب پذیری بحرانی در ویندوز سرور است که سطح خطر آن طبق استانداردCVSS ، ۱۰ از ۱۰ برآورد شده است. علت نامگذاری Zerologon آن است که مهاجم برای سوءاستفاده از آن نیازی به سرقت یا استفاده از کلمات عبور به‌منظور دسترسی به کنترل‌کننده‌های دامنه ندارد. در صورت موفقیت، مهاجم قادر است تا هر سیستم کامپیوتری در شبکه هدف از جمله سرور کنترل‌کننده دامنه که اکتیو دایرکتوری را اجرا می‌کند، جعل کند.

هنگام ورود کاربر به یک سرور ویندوزی عضو دامنه، از پروتکل از راه دور Netlogon برای برقراری ارتباط با کنترل کننده دامنه و تأیید اعتبار استفاده می‌شود. چنانچه رمز عبور صحیح باشد؛ کنترل کننده دامنه مکانیزم احراز اصالت را انجام داده و مجوز ورود صادر می‌شود. ویندوز سرور برای احراز اصالت از اتصال RPC رمزنگاری‌شده استفاده می‌کند. در صورت سوءاستفاده مهاجم می‌تواند با تغییر رمز عبور کنترل‌کننده دامنه، سطح دسترسی خود را به مدیر دامنه ارتقاء دهد و آن را در اختیار بگیرد. مهاجم با داشتن امتیاز مدیر دامنه به طور کامل به سرور کنترل کننده دامنه دسترسی پیدا خواهد کرد و قادر است هر دستوری را اجرا کند. در ادامه با دسترسی کامل به شبکه، مهاجم می‌تواند بدافزار دلخواه خود را در سرور مستقر سازد و یا اطلاعات حساس شبکه را برباید. به نقل از شرکت امنیتی «Secura» که این آسیب‌پذیری را شناسایی و گزارش کرده است؛ نفوذ به شبکه با سوءاستفاده از این آسیب‌پذیری تنها به ۳ ثانیه زمان نیاز دارد.

آژانس امنیت سایبری و زیرساخت ایالات متحده آمریکا- CISA بلافاصله هشدار دستوری به تمامی ادارات و آژانس‌های فدرال در خصوص رفع آسیب‌پذیری Zerologon صادرکرد تا به‌موجب آن شبکه‌های دولتی در معرض خطرات غیرقابل‌جبران قرار نگیرند. اگرچه دستور صادرشده CISA تنها ادارات و آژانس‌های فدرال را شامل می‌شود؛ این آژانس به تمام شرکت‌ها، سازمان‌ها، بخش خصوصی و بخش دولتی هشدار داد که در اسرع وقت به‌روزرسانی مایکروسافت را نصب کنند.

تا کنون گروه‌های تهدید بسیاری، از این آسیب پذیری سوءاستفاده کرده‌اند که از جمله آن‌ها می‌توان به حملات گسترده به سیستم‌های ایالتی و فدرال و همچنین سیستم‌های دولت‌های محلی و قبیله‌ای ایالات متحده اشاره کرد. به نقل از FBI و CISA، مهاجمین با سوءاستفاده از دو آسیب‌پذیری CVE-2018-13379 (که سال میلادی گذشته شناسایی شد) و آسیب‌پذیری Zerologon به سرورهای Fortinet نفوذ کرده و سپس از طریق Zerologon کنترل شبکه‌های داخلی را در دست می‌گیرند. سپس با استفاده از ابزارهای دسترسی از راه دور معتبر مثل

VPN و پروتکل دسترسی از راه دور RDP با نام کاربری و رمزعبور سرقت شده به سیستم‌های هدف دسترسی پیدا می کنند .

برای رفع این آسیب‌پذیری بایستی وصله‌های امنیتی مایکروسافت که آگوست ۲۰۲۰ منتشر شده است؛ بر تمام کنترل‌کننده‌های دامنه در اکتیودایرکتوری ها نصب شود. وصله‌ای که آسیب‌پذیری Zerologon را رفع نموده، مکانیزم‌های دفاعی بیشتری را نیز ارائه داده است که ماشین‌هایی که به دامنه ملحق می شوند را مجبور به استفاده از ویژگی‌های امنیتی می‌سازد که پیش‌تر اختیاری بودند.

۶.۵ آسیب‌پذیری‌های Microsoft Exchange

آخرین ماه سال ۱۳۹۹ چندین آسیب‌پذیری در محصولات مهم مایکروسافت منتشر شد که برای مدتی سرتیتر اخبار امنیت نرم‌افزار بود. مایکروسافت به‌روزرسانی‌های امنیتی مهمی را برای سرورهای Exchange منتشر کرد تا بدین‌وسیله آسیب‌پذیری‌های این محصولات از جمله چهار آسیب‌پذیری روز صفر آن‌ها را وصله کند. شناسه آسیب‌پذیری‌های یادشده عبارتند از: CVE-2021-26858، CVE-2021-26857، CVE-2021-26855 و CVE-2021-27065 که بر Exchange Server ۲۰۱۳ و Exchange Server ۲۰۱۶ و Exchange Server ۲۰۱۹ اثر می‌گذارند.

مهم‌ترین این آسیب‌پذیری‌ها CVE-2021-26855 را ProxyLogon می‌نامند. این آسیب‌پذیری به مهاجم اجازه می‌دهد تا مکانیزم احراز اصالت داخلی با قابلیت دریافت اتصالات غیرقابل‌اعتماد از یک منبع خارجی روی پورت ۴۴۳ را دور بزند. به دنبال آن سوءاستفاده از CVE-2021-26858، CVE-2021-26857 و CVE-2021-27065 پس از دور زدن احراز اصالت صورت می‌پذیرد که برای مهاجم دسترسی از راه دور را فراهم می‌سازد. برای رفع این آسیب‌پذیری‌ها شرکت مایکروسافت به‌روزرسانی‌های امنیتی را خارج از موعد همیشگی در دسترس مشتریان خود قرار داد تا آسیب‌پذیری‌های امنیتی فوق‌الذکر را که امکان تسخیر سرور را برای مهاجم ایجاد می‌کند، برطرف سازد.

از ابتدا هشدارهای شرکت مایکروسافت معطوف به گروه‌های تهدید چینی بود؛ ولیکن هشدارها از مانایی این حملات نکاسته و به موجب چهار آسیب‌پذیری روز صفر مذکور، سرویس ارائه‌دهنده خدمات تجاری ایمیل تحت حملات گروه‌های تهدید است. به نقل از منابع خبری حداقل ۳۰،۰۰۰ سازمان/شرکت که عمدتاً مرتبط با مشاغل کوچک در شهرها و دولت‌های محلی در سراسر ایالات متحده آمریکا هستند توسط گروه تهدیدی موسوم به «هافنیوم» با سوءاستفاده از آسیب‌پذیری‌های منتشرشده در Exchange Server به خطر افتادند. مایکروسافت مدعی است هافنیوم از چهار آسیب‌پذیری جدید برای نفوذ به سرورهای سرویس ایمیلی Exchange استفاده کرده تا بتواند اطلاعات حساس را از سازمان/شرکت‌های هدف به دست آورد و حتی در سرورها بدافزار کار بگذارد.

اطلاعات مدنظر مهاجمین شامل حساب ایمیل و دفاتر آدرس‌های افراد بوده است. در مجموع برآورد شمار قربانیان جهانی حمله به خدمات Exchange تقریبا به چند صد هزار می‌رسد و طبق تحلیل‌های آماری، تلاش برای سوءاستفاده از این آسیب‌پذیری‌ها و حمله به Microsoft Exchange Server با وجود انتشار وصله‌های امنیتی، همچنان در حال افزایش است.

۷.۵ مهم‌ترین بدافزارهای سال ۹۹

تعجب‌آور نیست که در سال ۱۳۹۹ مشابه سال‌های پیشین، حملات فیشینگ و نفوذ از طریق پروتکل دسکتاپ از راه دور یا به‌اختصار RDP همچنان مهم‌ترین رویکردهای پیاده‌سازی حملات سایبری بودند. اگر چه سال گذشته، سال بروز و ظهور انواع رویکردهای خلاقانه در حملات بود (مانند بدافزارهای مرتبط با داستان Solarwinds)؛ ولیکن بازیکنان قدیمی این عرصه، همچون باج‌افزارها همچنان بر صحنه مسلطند.

حملات باج‌افزاری با ۲۳ درصد، محبوب‌ترین رویکرد حملات سایبری در نیمه‌ی اول سال ۱۳۹۹ بوده‌اند. خانواده باج‌افزاری Sodinokibi نیز پرثمرترین باج‌افزار این نیمه از سال شناخته شد؛ به گونه‌ای که دو سوم حملات پیاده‌شده از طریق این باج‌افزار با موفقیت همراه بوده‌اند. همچنین خانواده بدافزارهای مبتنی بر لینوکس نیز ۴۰ درصد رشد داشته‌اند و توسعه بدافزار به زبان Go programming نیز رشد ۵۰۰ درصدی را تجربه کرده است. علت آن است که مهاجمین از بدافزارهایی که توانایی اجرای بهتری بر روی سیستم‌های مختلف شامل فضای ابری را دارند، استفاده می‌کنند. اما رویکرد رایج سال ۱۳۹۹ در مورد باج‌افزارها آن است که مهاجمین وب‌سایت نشست داده یا حراج داده را به زنجیره حملات خود افزوده‌اند و در صورتی که قربانی از پرداخت باج، خودداری کند؛ اطلاعات وی را فاش می‌کنند یا به حراج می‌گذارند. چنین رویکردی، قربانیان را بیشتر برای پرداخت باج تهییج می‌کند؛ چرا که نگران اعتبار خود در میان مشتریان و ... هستند. رویکرد مهم دیگر این سال، ماژولار بودن بدافزارهاست. مهاجمین از متدولوژی مؤلفه‌ای در بدافزارها استفاده و انواع تاکتیک‌های حمله را به‌صورت ترکیبی استفاده کردند و با این رویکرد احتمال پیاده‌سازی و بقای بدافزار را افزایش داده‌اند. چرایی این مهم از آن جهت است که اولاً مؤلفه راه‌انداز به طریقی (مثلاً از طریق مهندسی اجتماعی) به سیستم هدف نفوذ کرده و جای‌گذاری می‌شود. پس از آن این مولفه، رأساً سایر مولفه‌ها را در سیستم نصب، رمزگشایی و اجرا می‌کند. همچنین از آنجا که مولفه‌ها مجزا از یکدیگرند؛ در صورت شناسایی یک مؤلفه، هنوز سایر مؤلفه‌ها در سیستم هدف باقی مانده‌اند و گاهی برای جانشینی مؤلفه از دست‌رفته، به سرور فرمان و کنترل اطلاع‌رسانی و از آن کسب تکلیف می‌کنند.

در ادامه مهم‌ترین بدافزارهای سال ۱۳۹۹ برای بسترهای متفاوت معرفی می‌شوند:

۵-۶-۱- بدافزارهای ویندوز

Emotet: برای چندمین بار، Emotet سرلیست مهم‌ترین بدافزارها است. از سال ۲۰۱۴ میلادی این تروجان به انواع روش‌ها قربانی گرفته است. از جمله آن که به‌عنوان مکانیزم راه‌اندازی سایر بدافزارها به‌ویژه باج‌افزارها عمل می‌کند. اگرچه پیلود این بدافزار باج‌افزاری نیست؛ از آن برای آلوده‌سازی سیستم‌ها به انواع باج‌افزارها استفاده می‌شود. این بدافزار، مکرراً با TrickBot، BitPaymer، Conti/Ryuk، QakBot، Dridex و REvil دیده شده است.

Kovter: بدافزار بدون‌فایلی که رجیستری کامپیوتر را هدف قرار می‌دهد و شناسایی آن بسیار پیچیده است. حیات این بدافزار با پنهان شدن پشت هشدارهای جعلی برای دانلودهای غیرقانونی و اشتراک فایل، آغاز می‌شود. سپس به اعمال خرابکارانه درقالب تبلیغ‌افزار یا تولید کلیک‌های جعلی می‌پردازد.

Prometei: بات‌نت جدید Prometei از نوع رباینده رمزارزها از بهار سال گذشته در حال انتشار در اینترنت است. بات‌نت رباینده رمزارزها یا Cryptojacking گروهی از بدافزارهایی است که از منابع سیستم قربانی برای استخراج رمزارز استفاده می‌کنند. در این نوع حملات قربانی بدون آن که حتّی فعالیتی در حوزه استخراج رمزارز داشته باشد با آلوده شدن به این بدافزار، رمزارز استخراج می‌کند اما نه برای خود بلکه برای فرد مهاجم. هدف این بات‌نت استخراج رمزارزهای Monero(XMR) بوده و بدین منظور چندین روش از جمله سوءاستفاده از آسیب‌پذیری پروتکل ارتباطی SMB ویندوز را به کار بسته است. متأسفانه با وجود شناسایی بدافزار Prometei و سرورهای C&C آن، این بات‌نت هنوز متوقّف نشده و فعّال است.

Poison Ivy: تولکیت دسترسی از راه دوری است که تنظیمات کلاینت-سروری برای دسترسی مهاجمین به سیستم هدف فراهم می‌کند و در بسیاری از کمپین‌هایی که گروه‌های تهدید راه‌اندازی می‌کنند؛ به‌منظور جاسوسی و سرقت اطلاعات و اعتبارنامه‌ها استفاده می‌شود. برای توزیع بدافزار عمدتاً از الصاق‌های ایمیل که فایل‌های آفیس مایکروسافت را شامل می‌شوند، استفاده می‌شود.

Qakbot: بدافزار دیگری با یک دهه سابقه که به‌مرور زمان پیشرفت کرده و خطرناک‌تر شده است. پیشرفت این بدافزار در جهت دور زدن مکانیزم‌های شناسایی و تسریع آلوده‌سازی و توزیع در شبکه بوده است. این بدافزار قادر است حساب کاربر یا مدیر را قفل کند و بدین‌ترتیب حذف آن سخت‌تر می‌شود.

Ramnit: یک ویروس پارازیتیک با قابلیت‌های کرم که می‌تواند خود را تکثیر کند و مانایی آن در سیستم هدف بالاست. این بدافزار قادر است فایل‌های HTML را آلوده سازد و اعتبارنامه‌ها را برباید.

Ursnif: این تروجان که با نام‌های Gozi و Dreambot نیز شناخته می‌شود؛ تروجان بانکی است که پس از چند سال غیبت، سال ۱۳۹۹ مجدد ظاهر شد. این تروجان عمدتاً با TrickBot و تروجان IcedID دیده شده است.

۵-۶-۲- بدافزارهای مک

CallMe: این بدافزار از مهم‌ترین بدافزارهای دنیای مک است؛ یک درپشتی از سیستم آلوده به سرور فرمان‌وکنترل. این بدافزار، عمدتاً از طریق الصاق فایل‌های مایکروسافت به سیستم راه می‌یابد.

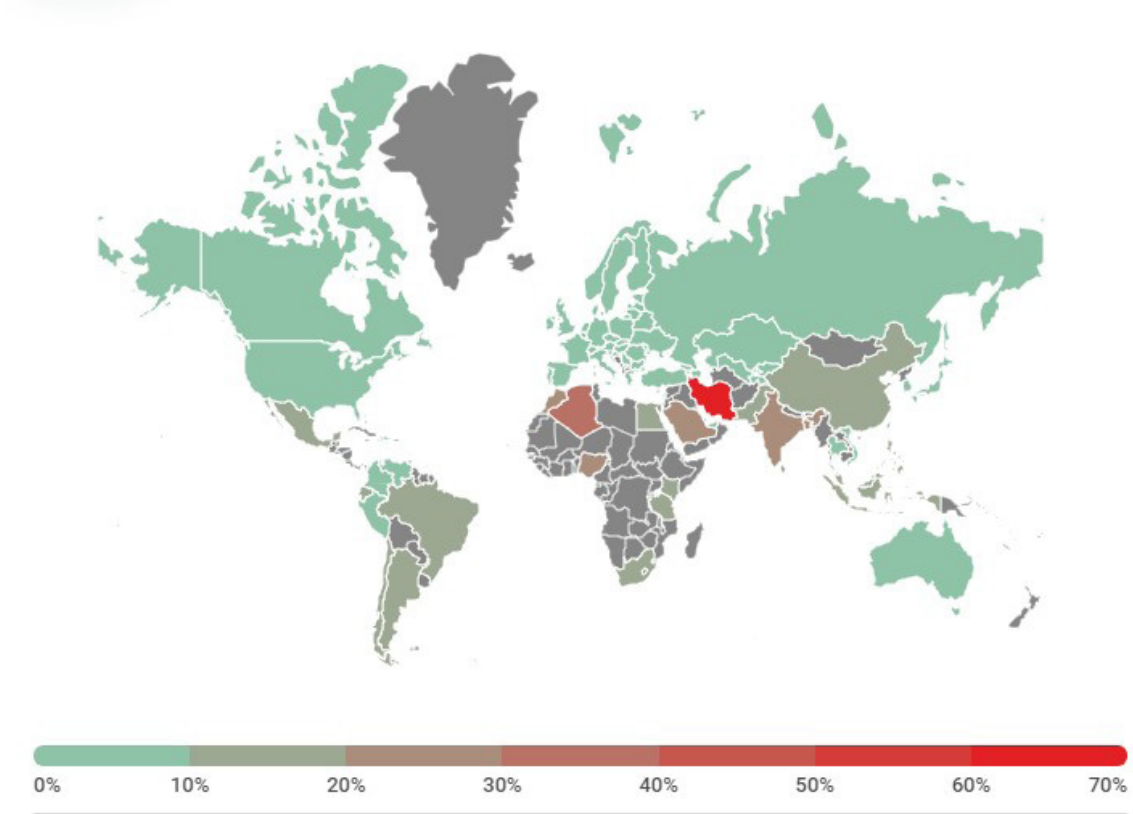
KeRanger: یکی از اولین باج‌افزارهای مک که انواع فایل‌ها را رمز و از قربانی باج‌خواهی می‌کند.

LaoShu: تروجان دسترسی از راه دور یا RAT که از طریق فایل‌های PDF آلوده توزیع می‌شود. بدافزار انواع خاصی از فایل‌ها را جستجو می‌کند و به‌صورت فشرده‌شده برای مهاجمین ارسال می کند .

NetWiredRC: بدافزار محبوب گروه تهدید ایرانی APT۳۳، یک RAT که بر بسترهای ویندوز و مک عمل می‌کند. تمرکز بدافزار بیشتر بر جاسوسی و سرقت اطلاعات حساس است.

۵-۶-۳- بدافزارهای موبایل

به نقل از کسپراسکی، سهم کاربران ایرانی آلوده به بدافزارهای موبایل، ۶۷,۷۸ درصد است. به‌عبارت دیگر بیش از دوسوم کاربران ایرانی آلوده به بدافزار هستند. با ۵۷,۲۶ درصد بیشترین بدافزارهای موبایل تبلیغ‌افزارها هستند. پس از آن انواع تروجان‌ها، بارگذارها و راه‌اندازهای تروجان بیشترین سهم را در میان بدافزارهای موبایل دارند.



شکل ۵-۱- کاربران ایرانی بیشترین آلودگی به بدافزارهای موبایل را دارند

مرکز تخصصی آپا
دانشگاه صنعتی اصفهان

تابستان ۱۴۰۰