امنیت فناوری اطلاعات

ویـژه‌نـامـه نـوروز ۱۳۹۸

شبکه گستر

امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

در سال‌های اخیر، صنعت فناوری اطلاعات ایران به پیشرفت‌های قابل‌توجهی دست یافته است. توسعه دولت الکترونیک و گسترش سرویس‌های موسوم به بانکداری الکترونیکی، ظهور برنامک‌های خدمات‌دهی در حوزه‌های مختلف و استقبال کاربران ایرانی از این خدمات در سال ۹۷ به اوج خود رسید. با وجود مزایای بی‌شمار بهره‌گیری از صنعت پاک فناوری اطلاعات، این واقعیت را باید پذیرفت که الکترونیکی شدن امور عملا به‌معنای ورود اطلاعات شخصی و کاری هر چه بیشتر به شبکه‌ها و پایگاه‌های داده کامپیوتری است. موضوعی که بی‌تردید مورد توجه خاص هکرهایی که در پی اطلاعات شهروندان ایرانی هستند قرار خواهد گرفت. بدیهی است که در صورت عدم حفاظت صحیح و رعایت نکردن اصول امنیتی، خسارات چه بسا جبران‌ناپذیری متوجه میلیون‌ها شهروند ایرانی شده و حتی موجب بروز بحران‌هایی حیاتی در زیرساخت‌های حساس کشور خواهد شد. در آستانه سال نو، شرکت مهندسی شبکه گستر در این ویژه‌نامه، ضمن مرور رویدادها و تجارب کسب شده در گذشته و با نگاهی به بدافزارها و تهدیدات سایبری در سال ۹۷، دورنمایی از مهمترین موضوعات و چالش‌های حوزه امنیت فناوری اطلاعات در سال ۹۸ را ترسیم کرده است. شرکت مهندسی شبکه گستر، ارائه‌دهنده محصولات و خدمات در زمینه امنیت شبکه از زمان تأسیس در سال ۱۳۷۰، همواره به امر آگاه‌سازی در زمینه امنیت فناوری اطلاعات به عنوان یکی از اصلی‌ترین راهکارهای مقابله با تهدیدات سایبری توجه خاص داشته است. امید است مطالب این ویژه‌نامه که حاصل تحقیق و پژوهش کارشناسان این شرکت است راهنمایی برای ارتقای دانش کاربران این حوزه باشد.

پیش‌بینی‌ها

به‌طور خلاصه انتظار می‌رود که موارد زیر اصلی‌ترین موضوعات سال ۹۸ در دنیای امنیت فناوری اطلاعات باشند:

- حذف هکرهای خرده‌پا و تشکیل گروه‌های نفوذگری حرفه‌ای‌تر
- هدفمندتر شدن حملات
- هرزنامه‌ها؛ همچنان اصلی‌ترین روش آلوده‌سازی و رخنه به سازمان‌ها
- RDP؛ درگاه مورد علاقه مهاجمان
- حملات فیشینگ بیشتر و حرفه‌ای‌تر
- گسترش تهدیدات موبایلی
- تلگرام؛ جولانگاهی برای ویروس‌نویسان و هکرها
- اطلاعات کاربران ایرانی بر روی سرویس‌های آنلاین از اهداف هکرها
- ادامه روند روبه‌رشد بدافزارهای استخراج ارز رمز
- بهره‌جویی سریع‌تر از آسیب‌پذیری‌های امنیتی
- استفاده هر چه بیشتر از تکنیک‌های موسوم به گریز
- ادامه بهره‌جویی از تجهیزات موسوم به اینترنت اشیا

در ادامه این بخش، به تفصیل به هر یک از این موارد پرداخته شده است.

حذف هکرهای خرده‌پا
و افزایش گروه‌های نفوذگری حرفه‌ای‌تر

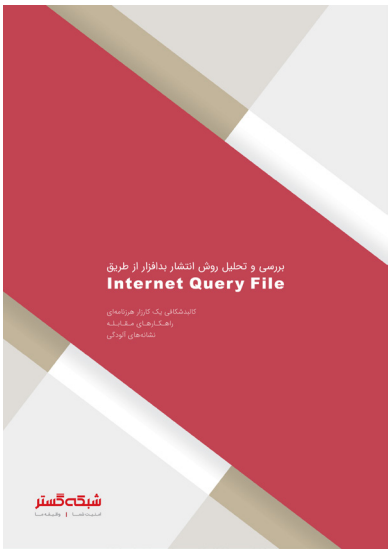
شرکت‌های امنیتی به‌طور مستمر در حال بهبود محصولات خود و خلق فناوری‌های جدید برای مقابله با بدافزارها و حملات سایبری هستند. ضمن اینکه آگاهی عمومی در خصوص این تهدیدات در مقایسه با سال‌های قبل، اگر چه نه به اندازه کافی که حداقل تا حدودی افزایش یافته است. عواملی که سبب گردیده که بدافزارهای با کدنویسی ضعیف و حملات سایبری ساده، کمتر به مرحله بهره‌برداری برای گردانندگانشان برسند. از سویی دیگر در سال ۹۷ شراکت میان برخی از گروه‌های نفوذگری و نویسندگان بدافزار بیش از هر زمان دیگر جلب توجه می‌کرد؛ شاخص‌ترین نمونه آن، باج‌افزار (Ransomware) مخرب GandCrab است. منافع مالی حاصل از انتشار GandCrab سبب ملحق شدن شرکای جدید به جمع گردانندگان این باج‌افزار گردیده است. در نسخه ٤، GandCrab مجهز به بسته بهره‌جوی (Exploit Kit) جدید Fallout شد. موفقیت‌های ناشی از آن موجب گردید تا بکارگیری این بسته بهره‌جو در نسخه ۵ نیز ادامه پیدا کند. به‌نحوی که نویسندگان GandCrab به‌طور عمومی از صاحبان Fallout قدردانی کردند. در نسخه ۵ شراکتی دیگر، این بار با یک سرویس رمزگذار با عنوان NTCrypt برقرار گردید. این سرویس کدهای بدافزار را مبهم‌سازی (Obfuscation) کرده و در عمل امکان فرار از سد محصولات امنیتی ضدبدافزار را برای کد مخرب فراهم می‌کند. مشارکت مذکور از طریق مناقصه‌ای که در روزهای ابتدایی مهر ماه در یک تالار گفتگوی اینترنتی توسط نویسندگان GandCrab برگزار شد حاصل گردید. در پنجم مهر ماه، NTCrypt خود را برنده این مناقصه اعلام کرد. برای یک کسب‌وکار تبهکاری سایبری نظیر GandCrab این گونه اتحادها روشی مؤثر برای از پا انداختن راهکارهای امنیتی است. در عمل بکارگیری چنین رویکردی ضمن ترکیب چندین ابزار مخرب و در نتیجه کارآمدتر شدن بدافزار، ریسک افشای کدها و فاش شدن هویت واقعی گردانندگان را نیز که در بسیاری مواقع به دلیل دخیل شدن تأمین‌کنندگان ناآشنا و نامطمئن صورت می‌پذیرد کاهش می‌دهد. از نگاه امنیتی، موفقیت استراتژی‌های گردانندگان GandCrab موضوعی نگران‌کننده است. استراتژی‌هایی که با شراکت‌های هر چه بیشتر و تجهیز به ابزارهای تهاجمی مخرب و کارآمدتر، توان چنین بدافزارهایی را افزایش داده و از سویی خود به الگویی برای سایر تبهکاران تبدیل شده است. پیش‌بینی می‌شود که در سال آینده ویروس‌نویسان و هکرهای کم‌تجربه و با تخصص ناکافی عملا به حاشیه رانده شده و شاهد اتحاد بیشتر میان نفوذگران نخبه و مخرب‌تر شدن محصولات آنها باشیم. نفوذگرانی که دیگر نه همچون قبل از تکنیک‌های ساده که از روش‌های پیچیده برای دور زدن و عبور از سد محصولات امنیتی مجهز به قابلیت‌های هوش مصنوعی و یادگیری ماشین بهره خواهند گرفت. انتظار می‌رود که هکرهای با دانش و توانایی کمتر به‌عنوان مصرف‌کننده به بازارهایی همچون "بدافزار به‌عنوان سرویس" (Rasnomware-as-a-Service - به اختصار RaaS) روی بیاورند. ضمن اینکه تعداد بیشتری از بدافزارهای مخرب و صاحب‌نام در قالب چنین سرویس‌هایی در اختیار سایرین قرار خواهند گرفت. بکارگیری محصولات امنیتی قدرتمند امنیت نقاط پایانی از جمله محصولات مبتنی بر رویکردهای Endpoint Detection and Response – به اختصار EDR – و Endpoint Protection Platform – به اختصار EPP – از مؤثرترین راهکارها در مقابله با نسل جدید تهدیدات پیشرفته است.

هدفمندتر شدن حملات

SamSam نمونه‌ای از موفق‌ترین تهدیدات سایبری چند سال اخیر است. در جریان انتشار این باج‌افزار، شرکت‌ها و سازمان‌های با درآمد بالا یا خدمات حساس مورد هدف قرار می‌گرفتند که حاصل آن برای مهاجمان کسب سودی سرشار با دردسرهایی به مراتب کمتر بوده است. بجای اخاذی ارز رمز (Cryptocurrency)، با ارزش چندصد دلار از هزاران نفر، در حملات SamSam هزاران دلار تنها از چند قربانی پردرآمد طلب می‌شد. قربانیانی که سرورهای هر کدام از آنها حاوی داده‌ها و سرویس‌هایی با ارزش میلیون‌ها دلار است و وقفه‌ای کوچک در خدمات‌رسانی آنها خساراتی بسیار بیشتر از مبلغ اخاذی شده را متوجه کسب‌وکار آنها خواهد کرد. GandCrab، مثالی است که گردانندگان آن در برخی حملات، روش انتشار SamSam را الگو قرار داده‌اند. بسته به نوع قربانی در برخی نمونه‌ها از آلودگی به GandCrab مبلغ باج ۷۰۰ هزار دلار گزارش شده است! انتظار می‌رود که در سال آینده شاهد اجرای حملات کاملا هدفمند و سازمان‌یافته بیشتری از سوی نویسندگان بدافزار باشیم.

هرزنامه‌ها، همچنان اصلی‌ترین روش آلوده‌سازی و رخنه به سازمان‌ها

مدتهاست که ایمیل‌های ناخواسته اما فریبنده که به هرزنامه (Spam) معروف هستند به یکی از اصلی‌ترین درگاه‌های آلوده‌سازی سیستم‌ها تبدیل شده‌اند. در سالی که گذشت افزایش استفاده مهاجمان از فایل‌های غیرمتداول در کارزارهای هرزنامه‌ای بیش از قبل به چشم می‌خورد. هدف از بکارگیری این فایل‌ها، عبور از سد سیستم‌های حفاظتی ایمیلی است که وظیفه آنها پویش فایل‌های پیوست پراستفاده‌ای همچون فایل‌های فشرده‌شده، اسکریپت‌ها و مواردی از این دست است. برای مثال، در سال ۹۷ هرزنامه‌هایی با پیوست فایل IQY شناسایی شد که اجرای آنها منجر به آلوده‌سازی دستگاه می‌شد. فایلی حاوی متن ساده و در ظاهر فاقد هر گونه عملکرد مخرب. نقش این فایل دریافت یک اسکریپت مخرب PowerShell بر روی دستگاه قربانی بود.



در اتاق خبر
شبکه گستر بخوانید...

از دیگر پسوندهای در ظاهر بی‌خطر اما با توانایی بالقوه اجرای کد مخرب می‌توان به موارد زیر اشاره کرد:

- فایل‌های مرتبط با نرم‌افزار Office نظیر DOC و PPT – در این فایل‌ها از بخش VBA – Visual Basic for Applications – که به مـاکـرو معروف است سوءاستفاده می‌شود. به این نوع فایل‌ها، ماکروی مخرب اطلاق می‌شود.
- HTA – فایل‌های HTA، قابلیت اجرا شدن بر روی مرورگر – فارغ از محدودیت‌های امنیتی لحاظ شده در آن مرورگر – را دارا هستند.
- JS – این فایل‌ها، حاوی کدهای JavaScript هستند.
- VBS – این نوع فایل‌ها، حاوی کدهای VB Script هستند.
- JSE – این فایل‌ها که می‌توانند حاوی اسکریپت باشند برای محافظت کدگذاری شده‌اند.
- WSF – فایل‌های متنی حاوی کدهای XML هستند. این نوع فایل‌ها با هر دو زبان اسکریپت‌نویسی JavaScript و VBScript سـازگار بوده و برنامه‌نویس حتی می‌تواند از هر دوی این زبان‌ها در یک فایل WSF استفاده کند.
- CHM – این فایل‌ها می‌توانند حاوی کدهای HTML و زبان‌های اسکریپت‌نویسی باشند.
- LNK – فایل‌های LNK میانبری برای اجرای یک برنامه یا فایل هستند. برخی نویسندگان باج‌افزار از این نوع فایل برای اجرای کد مخرب باج‌افزار از طریق پروسه‌های مجازی نظیر Windows PowerShell استفاده می‌کنند.

توضیح اینکه در اکثر نمونه‌ها فایل‌های مذکور به‌صورت فشرده شده به هرزنامه پیوست می‌شوند.

پیش‌بینی می‌شود در سال آتی پیوست کردن فایل‌های با پسوندهای غیرمتداول به هرزنامه‌ها رواج بیشتری در میان گردانندگان آنها داشته باشد. همچنین از نکات قابل توجه در خصوص کلاهبرداری‌های (Scam) جدید مبتنی بر هرزنامه، بهره‌گیری هر چه بیشتر و حرفه‌ای‌تر گردانندگان آنها از روش‌های مهندسی اجتماعی است. به‌عنوان مثال، در سالی که گذشت، یک هکر با ارسال ایمیل به برخی کاربران این طور وانمود می‌کرد که با تزریق اسکریپت به سایتی غیراخلاقی موفق به فعال کردن دوربین دستگاه کاربر و تصویربرداری از او در زمان مراجعه به آن سایت شده است. در ایمیل، کاربر تهدید می‌شد که در صورت عدم پرداخت مبلغ باج با ارز رمز بیت‌کوین، به ارزش ۹۶۹ دلار، فیلم‌های ضبط شده از او به کاربرانی که فهرست آنها بر روی دستگاه قربانی ذخیره شده ارسال خواهد شد. اگر چه این ایمیل صرفا یک کلاهبرداری اینترنتی بود و جنبه واقعیت نداشت اما نکته خاص در مورد آن اشاره به رمز عبوری بود که متعلق به کاربر در سایت مورد نظر مهاجم است. به‌نظر می‌رسد که مهاجم رمزهای عبور را از اطلاعات نشت شده در جریان حملات پیشین نفوذگران دیگر استخراج کرده باشد. بدیهی است که چنین تکنیک‌های مهندسی اجتماعی، شانس موفقیت مهاجمان را در فریب کاربر و قابل باور کردن متن درون ایمیل به‌شدت افزایش می‌دهد. در کنار استفاده از ضدویروس قدرتمند و به‌روز و محصولات پیشرفته ضدهرزنامه، آگاهی‌رسانی به کاربران به‌منظور پرهیز از اجرای پیوست و عدم کلیک کردن بر روی لینک‌های درون ایمیل‌های ناشناس و مشکوک نقشی اساسی در ایمن‌سازی سازمان از گزند این تهدیدات دارد.

RDP؛ درگاه مورد علاقه مهاجمان

پودمان RDP یا Remote Desktop Protocol قابلیتی در سیستم عامل Windows است که امکان اتصال از راه دور کاربران تعیین شده را به دستگاه فراهم می‌کند. علاوه بر مدیران شبکه که از این پودمان برای اتصال به سرورها و ایستگاه‌های کاری سازمان استفاده می‌کنند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره استفاده می‌شود. تبهکاران از ابزارهایی همچون Shodan برای شناسایی سرورهای با درگاه RDP باز بر روی اینترنت استفاده کرده و در ادامه با بکارگیری ابزارهایی نظیر NLBrute اقدام به اجرای حملات موسوم به Brute Force می‌کنند. هدف از اجرای حملات Brute Force رخنه به دستگاه از طریق پودمانی خاص – در اینجا RDP – با بکارگیری ترکیبی از نام‌های کاربری و رمزهای عبور رایج است. بنابراین در صورتی که دسترسی به پودمان RDP از طریق کاربری با رمز عبور ساده و غیرپیچیده باز شده باشد مهاجمان نیز به‌راحتی امکان اتصال به دستگاه را خواهند داشت. در صورت فراهم شدن اتصال، مهاجمان نرم‌افزاری را بر روی سرور اجرا کرده و از آن برای دست‌درازی به تنظیمات و سرویس‌های نرم‌افزارهای ضدبدافزار، پشتیبان‌گیری و پایگاه داده نصب شده بر روی آن استفاده می‌کنند. در ادامه نیز فایل مخرب باج‌افزار را دریافت کرده و بر روی سرور به اجرا در می‌آورند.

جدول زیر فهرستی از چند باج‌افزار مخرب و پرانتشار در سال ۹۷ را نمایش می‌دهد. همانطور که پیداست بهره‌جویی از پودمان RDP برای آلوده‌سازی دستگاه‌ها در میان همه آنها مشترک است.

	BitPaymer	SamSam	Ryuk	Dharma	GandCrab
نوع	هدفمند	هدفمند	هدفمند	هدفمند	باج‌افزار به‌عنوان سرویس
انتشار	RDP	RDP	RDP	RDP	RDP / ایمیل / بهره‌جو
میانگین مبلغ باج	۵۰،۰۰۰ تا ۱،۰۰۰،۰۰۰ دلار	۴۰،۰۰۰ دلار	۱۰۰،۰۰۰ دلار	۵،۰۰۰ دلار	متغیر
فراوانی حمله	چند بار در هفته	حداقل یکبار در هر روز	چند بار در هفته	چند بار در هر روز	متغیر
سیستم‌های مورد هدف	کلیه سرورها	تمامی سرورها و نقاط پایانی	کلیه سرورها	سرورهای با عملکرد حیاتی و حساس	همه
مناطق مورد نظر مهاجمان	تمامی کشورها	تمامی کشورها با تمرکز بر روی آمریکا	تمامی کشورها	تمامی کشورها	تمامی کشورها
امکان رمزگشایی بدون نیاز به پرداخت باج	خیر	خیر	خیر	خیر	برخی نسخه‌ها
روش پرداخت	بیت‌کوین از طریق ایمیل و در برخی نمونه‌ها از طریق سایتی در وب تاریک	بیت‌کوین از طریق سایتی در وب تاریک	بیت‌کوین از طریق ایمیل	بیت‌کوین از طریق ایمیل	بیت‌کوین از طریق سایتی در وب تاریک
ملاحظات	صرف زمان برای اطمینان از حذف شدن نسخه‌های پشتیبان قبل از اجرای حمله	سابقه حمله هدفمند به مراکز درمانی	صرف زمان برای اطمینان از حذف شدن نسخه‌های پشتیبان و غیرفعال‌سازی ضدویروس پیش از اجرای حمله	تلاش برای غیرفعال کردن دستی ضدویروس قبل از اجرای فایل مخرب باج‌افزار	به روزرسانی‌ها مستمر و دخیل کردن تبهکاران مختلف

در اکثر مواقع این سرورها هستند که پودمان RDP آنها در بستر اینترنت قابل دسترس است. سرورها بنا به ماهیت و عملکردشان عمدتا حاوی اطلاعاتی بسیار حساس، با ارزش‌های مالی و معنوی بالا هستند. به همین خاطر در صورت موفقیت در آلوده‌سازی و رخنه به آنها منافع قابل توجهی متوجه مهاجمان خواهد شد. در سالی که گذشت، مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در چندین اطلاعیه نسبت به حمله باجگیران سایبری به سرورهای ایرانی از طریق پودمان RDP هشدار داد. لازم به ذکر است که علیرغم اجرای گسترده حملات مبتنی بر RDP در اسفند ماه سال ۱۳۹۷، موردی از آلودگی توسط مشترکین شبکه گستر به این شرکت گزارش نشد؛ موضوعی که می‌تواند بیانگر آگاهی مشتریان و اثربخش بودن اقدامات امنیتی صورت پذیرفته توسط آنها باشد.

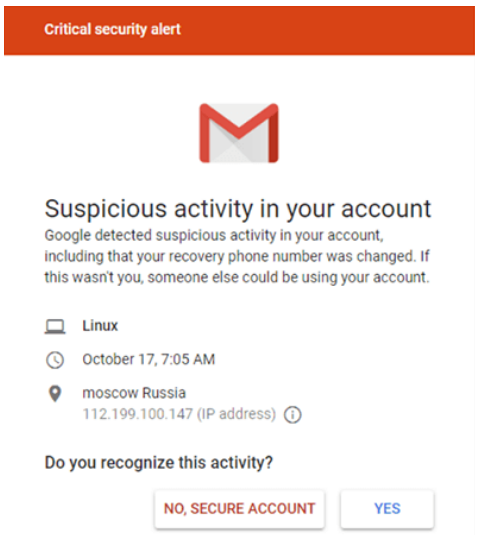
در اتاق خبر
شبکه گستر بخوانید...

حملات فیشینگ بیشتر و حرفه‌ای‌تر

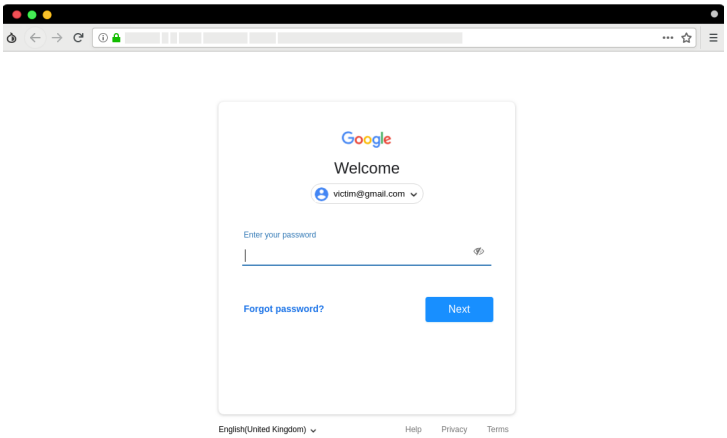
اگر چه در سال ۹۷ برای مدتی تعداد نشانی‌های جدید فیشینگ روندی نزولی داشت اما خیلی زود سیری صعودی به خود گرفت. در این سال نمونه‌های متعددی از حملات فیشینگ را شاهد بودیم. از جمله می‌توان به گروه معروف به Charming Kitten اشاره کرد که سیاستمداران و افراد دخیل در تحریم‌های اقتصادی و نظامی بر ضد ایران را هدف حملات فیشینگ خود قرار دادند. آن چه که حملات Charming Kitten را برجسته می‌کند تکنیک‌هایی است که این گروه برای هک کردن سرویس‌های حفاظت‌شده توسط مکانیزم‌های موسوم به احراز هویت دوعاملی (Two-factor Authentication - به اختصار 2FA) مورد استفاده قرار دادند. در جریان این حملات مهاجمان اقدام به ارسال ایمیل‌هایی فریبنده از نشانی‌های در ظاهر معتبر نظیر موارد زیر می‌کردند:

- notifications.mailservices@gmail[.]com
- noreply.customermails@gmail[.]com
- customer]email-delivery[.]info

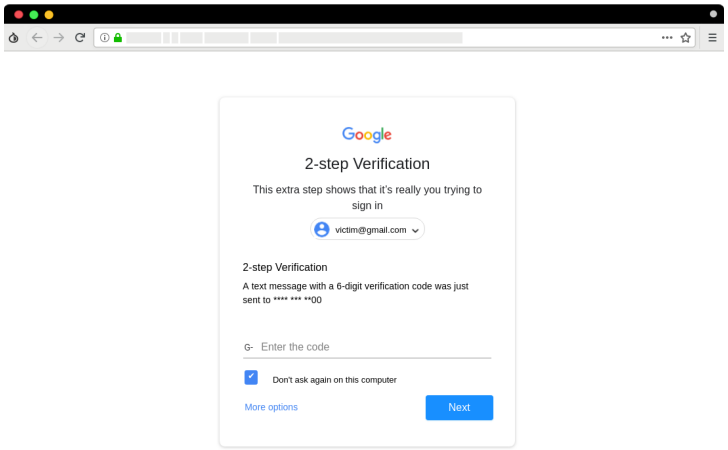
در این ایمیل‌ها این‌طور تظاهر می‌شد که افرادی تلاش داشته‌اند تا به‌صورت غیرمجاز به حساب ایمیل دسترسی پیدا کنند و کاربر می‌بایست در اسرع وقت با ورود به حساب ایمیل خود دسترسی‌های مشکوک را مسدود کند.



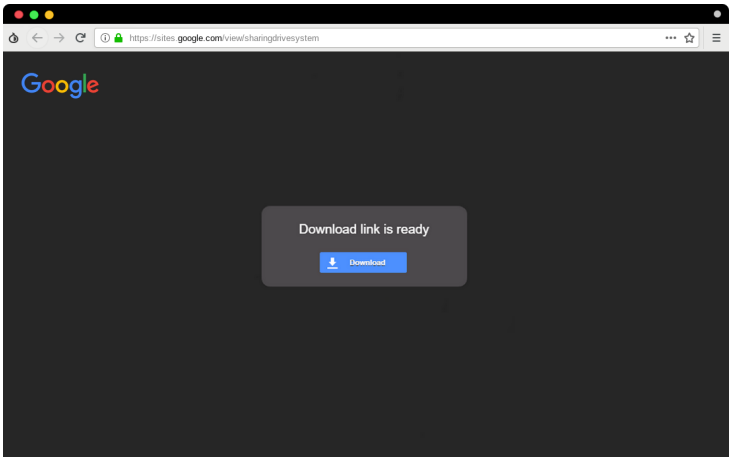
محتوای این ایمیل‌ها نه به‌صورت متن که کاملا در قالب تصویری ارسال می‌شد. هدف از این اقدام فرار از سد ابزارهای ضدهرزنامه‌ای بود که نسبت به کلمات خاص و مشکوک در ایمیل‌ها واکنش نشان می‌دهند. در صورت ورود کاربر به صفحه مذکور، همان‌طور که در تصویر زیر نمایش داده شده است در صفحه‌ای کاملا مشابه با سایت اصلی از کاربر خواسته می‌شد تا اطلاعات اصالت‌سنجی خود را وارد کند. لازم به ذکر است که در ایمیل‌های ارسالی، تصویری مخفی جاسازی شده بود که با فراخوانی شدن آن – در نتیجه باز شدن ایمیل توسط کاربر – موضوع به مهاجمان اطلاع‌رسانی می‌شد تا از این طریق بلافاصله فعالیت‌های کاربر در صفحه اینترنتی فیشینگ مورد رصد آنها قرار بگیرد.



در صورت ورود اطلاعات اصالت‌سنجی توسط کاربر در صفحه فیشینگ، مهاجمان نیز به‌طور همزمان رونوشتی از آن اطلاعات را در سایت واقعی وارد می‌کردند. چنانچه حساب توسط سیستم احراز هویت دوعاملی حفاظت شده باشد در نتیجه این اقدام مهاجمان، کاربر پیامکی حاوی کد عامل دوم را دریافت می‌کرد. برای دستیابی به این کد، مهاجمان نیز کاربر را به صفحه فیشینگ دیگری هدایت می‌کردند که در آن خواسته می‌شد تا کد پیامک‌شده وارد شود. با این تکنیک عملا مهاجمان قادر بودند تا دسترسی کامل به حساب کاربر را در اختیار بگیرند.



همچنین مهاجمان Charming Kitten با ایجاد صفحات جعلی در ظاهری مشابه با صفحه به‌اشتراک‌گذاری فایل در سرویس Google Drive، وانمود می‌کردند که فایلی را با قربانی به اشتراک گذشته‌اند. اما در حقیقت در صورت کلیک بر روی دگمه Download کاربر به صفحه فیشینگ ورود به حساب کاربری Gmail که در بالا به آن اشاره شد هدایت می‌شد.



هکرهای Charming Kitten برای هدایت اهداف خود به این صفحات جعلی، از حساب‌های کاربری هک‌شده در توییتر، فیس‌بوک و تلگرام بهره گرفته بودند. مهاجمان از سرویس GoogleSites برای ساخت صفحات مذکور استفاده کرده بودند. این سرویس شرکت گوگل امکان ساخت صفحات اینترنتی و به‌اشتراک‌گذاری آنها را فراهم می‌کند. نشانی صفحات ایجادشده می‌تواند مسیری از sites.google.com باشد. برای مثال، hxxps://sites.google[.]com/view/sharingdrivesystem یکی از نشانی‌های به‌کار گرفته شده توسط این مهاجمان بود. بدیهی است که اشاره به دامنه google.com، معتبر بودن صفحه را برای قربانیان این حملات فیشینگ باورپذیرتر می‌کرده است. قطعا مهاجمان پیش از اجرای حملات فیشینگ، اطلاعات کاملی را درباره اهداف خود گردآوری کرده بودند. به‌نحوی که با در نظر گرفتن سطح دانش سایبری، دامنه ارتباطات، فعالیت‌ها و ساعات کاری بر اساس موقعیت جغرافیایی کاربر مورد نظر، سناریوی خاصی را برای هر هدف پیاده‌سازی می‌کردند. بسیاری از منابع، Charming Kitten را گروهی متشکل از نفوذگران ایرانی می‌دانند. این گروه که با نام‌های زیر نیز شناخته می‌شود جاسوسی از سازمان‌های مالی، هوافضا، زیرساخت، دولتی و تحقیقاتی آمریکا را در کارنامه خود دارد.

- OilRig
- Helix Kitten
- Newscaster
- Newsbeef

همچنین در سالی که گذشت نمونه‌های متعددی از اجرای حملات فیشینگ با هدف سرقت اطلاعات بانکی کاربران ایرانی گزارش شد. برای نمونه می‌توان به باج‌افزار ایرانی PooleZoor اشاره کرد که در اطلاعیه باج‌گیری آن کاربر تشویق به ورود به سایتی که تصویری از آن در ادامه نمایش داده شده است هدایت می‌شد. نشانی استفاده شده در سایت مذکور، سایتی فیشینگ است که هدف آن کلاهبرداری و سرقت اطلاعات بانکی کاربر است. بنابراین در صورت مراجعه قربانی به سایت مذکور و وارد کردن اطلاعات کارت بانکی در آن نه فقط ابزار رمزگشایی در اختیار او قرار نمی‌گیرد که تمام اطلاعات بانکی وارد شده نیز در خدمت نویسنده یا نویسندگان PooleZoor قرار خواهد گرفت.

اوایل سال ۱۳۹۷ نیز مرکز ماهر در اطلاعیه‌ای نسبت به افزایش حملات فیشینگ بانکی هشدار داد.

گسترش تهدیدات موبایلی

چندین سال است که دستگاه‌های همراه شامل گوشی‌های هوشمند، تبلت‌ها و به‌طور کلی دستگاه‌های مبتنی بر هر یک از سیستم‌های عامل Android و iOS به‌شدت مورد توجه هکرها و نویسندگان بدافزار قرار گرفته‌اند. بسیاری از این دستگاه‌ها عملا گنجینه‌ای از اطلاعات باارزش شخصی و کاری هستند که دسترسی به آنها امکان انواع سوءاستفاده‌ها را برای مهاجمان فراهم می‌کند. عمده حوزه فعالیت بدافزارهای مخرب، جاسوسی و سرقت اطلاعات شخصی، تجاری و بانکی، استخراج ارز رمز و نمایش تبلیغات ناخواسته است. در دی ماه ۹۷، مرکز ماهر در سه گزارش به بررسی بیش از ۲۰۰ برنامک ایرانی تحت اندروید که خدمات مرتبط با اینستاگرام را ارائه می‌دهند پرداخت. نتایج تحقیقات این مرکز نشان می‌دهد که بخش زیادی از برنامک‌های مذکور، پس از نصب اقدام به اجرای امور مخربی همچون سرقت اطلاعات کاربر می‌کنند. ماهر تخمین می‌زند که اطلاعات بیش از یک میلیون کاربر اینستاگرام در ایران در اختیار تولیدکنندگان این برنامک‌ها قرار گرفته است. این مرکز در گزارشی دیگر ضمن بررسی یکی از قدیمی‌ترین و پرانتشارترین بدافزارهای ایرانی با نام پوشفا تخمین زد که چندین میلیون از دستگاه‌های تحت سیستم عامل Android کاربران ایرانی به نمونه‌ای از این بدافزار آلوده شده است. در مواردی متعدد نیز نفوذگران ایرانی از طریق سایت‌ها و پیام‌رسان‌ها از جمله تلگرام اقدام به انتشار بدافزارهای تحت Android کردند. برای مثال در آذر ماه و در پی آغاز ثبت‌نام کارت سوخت بانکی در سامانه خدمات دولت همراه و انتشار برنامک مربوطه، نسخه‌های جعلی متعددی از یک برنامک مخرب با تبلیغات گسترده در کانال‌های تلگرامی و سایر شبکه‌های اجتماعی توسط سودجویان منتشر شد. در آن زمان ماهر اعلام کرد از امکان آلوده‌سازی تلفن همراه کاربر و انواع سوءاستفاده از اطلاعات وی توسط این برنامک خبر داد.

بررسی‌های انجام شده توسط برخی از شرکت‌های امنیتی نیز از پیشرفت هکرهای ایرانی در حوزه توسعه بدافزارهای سیستم عامل Android حکایت دارد. در این خصوص می‌توان به حمله گروه "باغ وحش" در سال گذشته اشاره کرد. "باغ وحش" – یا ZooPark به زبان روسی – عنوان گروه نفوذگری، احتمالا ایرانی است که از ژوئن سال ۲۰۱۵ میلادی، با بکارگیری بدافزارهای تحت سیستم عامل اندروید کاربران را در منطقه خاورمیانه هدف قرار می‌داده است. در سال گذشته این مهاجمان از طریق سایت‌های هک شده توسط این گروه کاربر را به سایتی دیگر هدایت کرده و در آن مراجعه‌کننده تشویق به دریافت برنامک‌های مخرب اندرویدی می‌شد. در صورت آلوده شدن دستگاه قربانی به هر یک از این برنامک‌ها، کد مخرب تزریق شده در برنامک، اطلاعات شخصی و حساس را از روی دستگاه سرقت می‌کرد. بدافزارهای مورد استفاده این گروه را می‌توان به چهار نسخه تقسیم‌بندی کرد. در حالی که نسخه نخست این بدافزارها تنها قادر به استخراج فهرست شماره افراد و اطلاعات حساب کاربری بوده، نسخه چهارم به‌عنوان جدیدترین نسخه، قادر به انجام فرامین پیشرفته متعدد از جمله تصویربرداری، ضبط صدا و ویدئو و حتی برقراری تماس بدون اطلاع کاربر است. کشورهای ایران، مراکش، مصر، لبنان و اردن از جمله اهداف گروه سایبری "باغ وحش" اعلام شدند. علاوه بر هک سایت‌ها، کانال‌های تلگرام و تبلیغ دریافت برنامک‌هایی نظیر رأی‌گیری در این کانال‌ها که نمونه‌ای از آن در تصویر زیر نمایش داده شده است، دیگر روش این گروه برای آلوده‌سازی دستگاه‌ها گزارش شده بود.

انتخاب دهم

38 members

نظر سنجی در خصوص کاندیداهای استان کردستان به همراه
نرم افزار موبایلی رای گیری
ارتباط با ادمین: @Entekhab_10_Admin

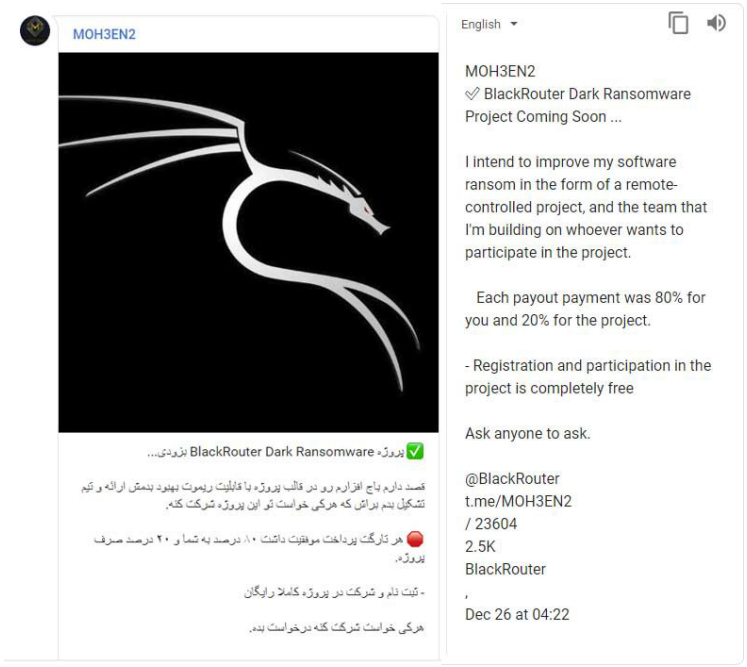
VIEW CHANNEL

باید توجه داشت که در اکثر مواقع این بازارهای غیررسمی هستند که میزبان برنامک‌های مخربند. بر اساس گزارشی که شرکت گوگل آن را منتشر کرده دستگاه‌های تحت سیستم عامل Android که برنامک‌های آنها تنها از Play Store – انباره رسمی به‌اشتراک‌گذاری برنامک گوگل – دریافت می‌شود نه برابر امن‌تر از دستگاه‌های با برنامک دریافت شده از حداقل یک بازار ثالث هستند. البته این به‌معنای صددرصد ایمن بودن برنامک‌های میزبانی شده بر روی این بازار نبوده و در مواقعی برنامک‌های مخربی نیز بوده‌اند که نویسندگانشان موفق به اشتراک‌گذاری آنها در Play Store شده‌اند. از جمله این برنامک‌های مخرب، یک جاسوس‌افزار با نام MobSTSPY است که در قالب برنامک‌های به ظاهر معتبر اقدام به سرقت اطلاعات کاربر می‌کرده است. برنامک‌های مذکور حداقل برای مدتی در Play Store قابل دسترس بوده‌اند. موضوعی که اهمیت نصب محصولات ضدویروس بر روی این دستگاه‌ها را پررنگ‌تر می‌کند. انتظار می‌رود که در سال آتی حوزه برنامک‌های مخرب بیش از قبل مورد توجه مهاجمان ایرانی و آن دسته از هکرهایی که در پی اطلاعات شهروندان ایرانی هستند قرار بگیرد. با رعایت موارد زیر می‌توان تا حد زیادی در برابر بدافزارهای تحت سیستم عامل Android در امان ماند:

- سیستم عامل و برنامک‌های نصب شده بر روی دستگاه همراه خود را همیشه به آخرین نسخه ارتقا دهید.
- برنامک‌ها را فقط از بازار توزیع دیجیتال Play Store یا حداقل بازارهای مورد اعتماد معروف دریافت کنید. همچنین از غیرفعال بودن گزینه Unknown sources در بخش Settings و از فعال بودن گزینه Scan device for security threats در قسمت Google Settings دستگاه اطمینان داشته باشید. با غیرفعال بودن گزینه نخست، از اجرا شدن فایل‌های APK میزبانی شده در بازارهای ناشناخته بر روی دستگاه جلوگیری می‌شود. وظیفه گزینه دوم نیز پایش دوره‌ای دستگاه است.
- پیش از نصب هر برنامک امتیاز و توضیحات کاربران آن را مرور کرده و به نکات منفی توضیحات کاربران بیشتر توجه کنید.
- به سطوح دسترسی درخواستی برنامک در زمان نصب توجه کنید. اگر فهرست آن بطور غیرعادی طولانی بود از نصب آن اجتناب کنید.
- از راهکارهای امنیتی قدرتمند برای حفاظت از دستگاه‌های همراه خود یا سازمانتان استفاده کنید.

تلگرام؛
جولانگاهی برای ویروس‌نویسان و هکرها

در سالی که گذشت برخی فروشندگان نیز با خروج از شبکه ناشناس TOR به عرضه محصولات و خدمات غیرقانونی خود در بستر تلگرام روی آوردند. همچنین این پیام‌رسان به یکی از بسترهای مورد علاقه ویروس‌نویسان و هکرها از جمله مهاجمان ایرانی برای ارتباطات و معاملات زیرزمینی آنها تبدیل شده است. یکی از این نمونه‌ها نسخه جدیدی از باج‌افزار BlackRouter – که با نام Blackheart نیز شناخته می‌شود – است که در قالب خدمات موسوم به "باج‌افزار به‌عنوان سرویس" توسط هکری ایرانی در تلگرام به مهاجمان دیگر عرضه می‌شود. در این خدمات، صاحب باج‌افزار، فایل مخرب را به‌عنوان یک خدمت به متقاضی اجاره می‌دهد. متقاضی که ممکن است در برنامه‌نویسی تخصصی نداشته باشد تنها وظیفه انتشار باج‌افزار را بر عهده دارد. در نهایت بخشی از مبلغ اخاذی شده از قربانی به متقاضی و بخشی دیگر به نویسنده می‌رسد. بر طبق توضیحات فارسی درج شده در کانال تلگرام هکر مذکور، این سهم در باج‌افزار BlackRouter، ۸۰ و ۲۰ درصد است. بدین‌نحو که ۸۰ درصد از مبلغ باج به فرد یا گروهی که کار انتشار BlackRouter را برعهده داشته‌اند می‌رسد و ۲۰ درصد باقیمانده به هکر گرداننده کانال تعلق می‌گیرد.



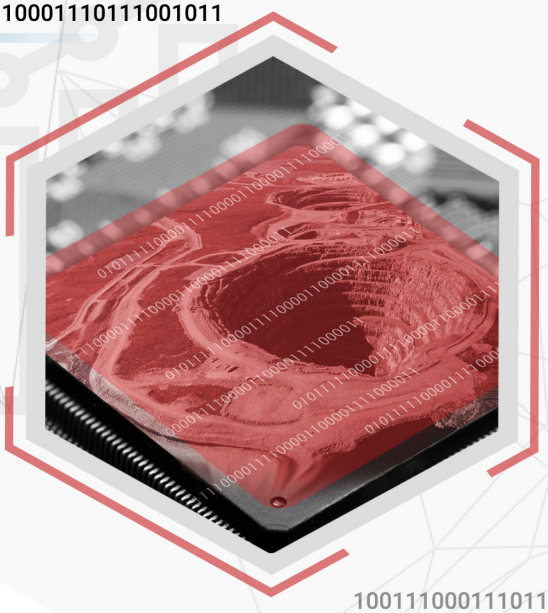
یا در پستی دیگر در تلگرام این هکر آن‌طور که خود ادعا می‌کند در حال توسعه یک اسب تروای دسترسی از راه دور (Remote Access Trojan) با نام BlackRAT با قابلیت‌های متعدد است که به گفته او به‌زودی آماده استفاده خواهد شد.

انتظار می‌رود که استقبال نفوذگران از پیام‌رسان تلگرام در سال آینده همچنان ماندگار باقی بماند.

اطلاعات کاربران ایرانی بر روی سرویس‌های آنلاین؛ هدف هکرها

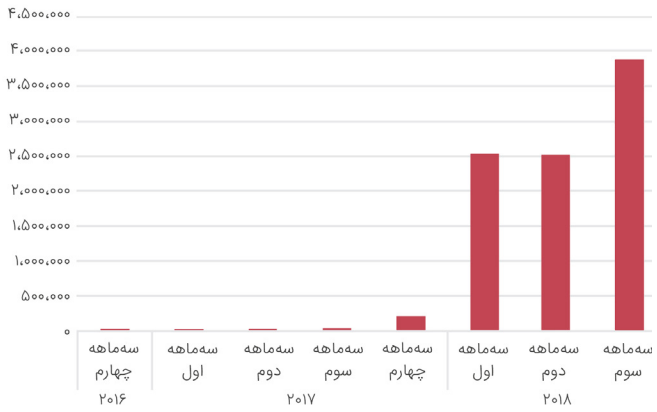
در سال‌های اخیر، تعداد قابل‌توجهی از سازمان‌ها اقدام به ارائه خدمات خود در قالب دولت الکترونیک کرده‌اند. ضمن اینکه گسترش روزافزون سرویس‌های موسوم به بانکداری الکترونیکی، ظهور برنامک‌های خدمات‌دهی در حوزه‌های مختلف و استقبال هر چه بیشتر کاربران از آنها را شاهد هستیم. تنها یکی از این برنامک‌ها دارای بیش از ۳۰ میلیون کاربر فعال در سطح کشور است.

ارائه خدمات منسجم‌تر، مناسب‌تر و سریع‌تر، کاهش روال‌های دست‌وپاگیر اداری، بهبود بهره‌وری، شفافیت امور و اثرات مثبت زیست‌محیطی تنها بخشی از مزایای دولت الکترونیک و بهره‌گیری از فناوری اطلاعات در امور مختلف خدمات‌رسانی است. اما از سویی دیگر، الکترونیکی شدن امور به‌معنای ورود اطلاعات شخصی و کاری هر چه بیشتر به شبکه‌ها و پایگاه‌های داده کامپیوتری است. موضوعی که بی‌تردید مورد توجه هکرهایی که در پی اطلاعات شهروندان ایرانی هستند قرار خواهد گرفت. بدیهی است که در صورت عدم حفاظت صحیح و رعایت نکردن اصول امنیتی، خسارات چه بسا جبران‌ناپذیری متوجه میلیون‌ها شهروند ایرانی شده و حتی موجب بروز بحران‌هایی حیاتی در زیرساخت‌های حساس کشور شود. باید توجه داشت علیرغم اینکه در سال‌های اخیر مؤسسات مالی در بسیاری از کشورها تلاش فراوانی برای حفاظت هر چه بیشتر از حساب‌های آنلاین کاربران خود – نظیر بکارگیری مکانیزم تصدیق هویت دو عاملی در زمان ورود آنلاین به حساب بانکی و در حین اجرای اموری نظیر انتقال وجه به حساب - به‌عمل آورده‌اند مهاجمان در بدافزارهای معروفی همچون Zeus Panda و با استفاده از روش‌هایی همچون "تزریق وبی" موفق به دور زدن این مکانیزم‌ها شده‌اند. ایمن‌سازی زیرساخت سرویس‌دهنده، کدنویسی امن، رعایت اصول امنیتی در فرایند توسعه نرم‌افزار و توزیع آن و مقاوم‌سازی محصول / سرویس اگر چه ضروری اما قطعا ناکافی است و نیاز است که افزایش دانش کاربران و آگاهی‌رسانی به آنها مورد توجه جدی نهادهای مربوطه قرار گیرد.



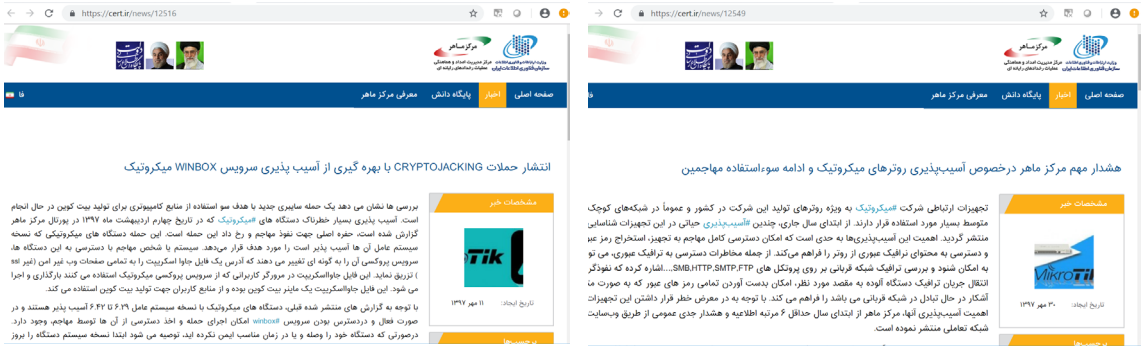
ادامه روند روبه‌رشد بدافزارهای استخراج ارز رمز

در یک سال اخیر استخراج ارز رمز از طریق بدافزار یکی از مباحث اصلی در حوزه امنیت فناوری اطلاعات بوده است. بر اساس آخرین گزارش فصلی شرکت مک‌آفی، تعداد این نوع بدافزارها در پایان سه‌ماهه سوم ۲۰۱۸ در مقایسه با یک سال قبل از آن ٤،۰۰۰ درصد افزایش داشته است (نمودار زیر).



در ارز رمزها، فرایندی با عنوان استخراج (Mining) وجود دارد که یکی از اصلی‌ترین وظایف آن تایید اطلاعات تبادل شده در شبکه این واحدهای پولی است. فرایند استخراج مستلزم فراهم بودن توان پردازشی بسیار بالاست. در نتیجه شبکه ارز رمز نیز در قبال تلاشی که برای این پردازش‌ها انجام می‌شود به استخراج‌کنندگان پاداشی اختصاص می‌دهد. از همین رو، برخی افراد نیز با بکارگیری برنامه‌های Cryptocurrency Miner تلاش می‌کنند تا در ازای استخراج ارز دیجیتال، مشمول پاداش شبکه واحد دیجیتال شوند. اما با توجه به نیاز به توان پردازش بالا، انجام استخراج می‌تواند یک سرمایه‌گذاری هزینه‌بر برای استخراج‌کننده باشد. به همین خاطر در حملات موسوم به رمز ربایی (Cryptojacking)، استخراج‌کننده بدخواه با آلوده نمودن دستگاه دیگران به بدافزارهای ویژه استخراج، از توان پردازشی آنها به نفع خود بهره‌گیری می‌کند. در حقیقت در رمز ربایی، این مهاجمان هستند که همه منافع حاصل از استخراج را بدون هر گونه سرمایه‌گذاری کسب می‌کنند؛ در حالی که دستگاه قربانی انجام دهنده امور اصلی بوده است. اهمیت ایمن و مقاوم ساختن تجهیزات موسوم به اینترنت اشیا بیش از هر زمانی دیگر پررنگ شده است. اگر چه در نگاه اول این تجهیزات فاقد منابع قدرتمند برای اموری همچون استخراج ارز رمز هستند اما در مقیاس بالا و با توجه به پیکربندی امنیتی ناصحیح بسیاری از آنها عملا با لشکری از دستگاه‌های آسیب‌پذیر مواجه هستیم که می‌توانند در مجموع عملکردی بالاتر و مناسب‌تر در مقایسه با حتی سرورهای قدرتمند برای مهاجمان فراهم کنند.

برای مثال ماه‌هاست مهاجمان با رخنه به روترهای میکروتیک، اسکریپت‌های استخراج‌کننده ارز رمز را بر روی دستگاه‌های متصل به این روترها به اجرا در می‌آورند. این حملات که به‌نظر می‌رسد در ابتدا محدود به کشور برزیل بوده به سرعت دامنه آنها به کشورهای مختلف جهان از جمله ایران گسترش پیدا کرده است. نفوذگران با آلوده نمودن دستگاه میکروتیک سبب می‌گردند تا در صفحات فراخوانی شده در مرورگر کاربرانی که در سطح شبکه از طریق این تجهیزات به اینترنت متصل می‌شوند اسکریپت‌های Coinhive که وظیفه آنها استخراج ارز رمز با استفاده از منابع سخت‌افزاری دستگاه کاربر است تزریق شود. جالب اینکه به‌منظور کاهش حساسیت و شک کاربران به افزایش پردازش‌های صورت گرفته بر روی دستگاه – در نتیجه اسکریپت‌های اجرا شده -، عملیات تزریق صرفا محدود به صفحات حاوی پیام‌های خطا – از هر نوع – شده است. با این حال با در نظر گرفتن تعداد حداقل ده‌ها هزار روتر آلوده و با فرض اینکه هر یک از آنها ده‌ها و شاید صدها کامپیوتر را به اینترنت متصل می‌کنند می‌توان نتیجه‌گیری کرد که حتی با این روش محدودسازی، همچنان سود سرشاری نصیب گردانندگان این حملات می‌شود. در حملات مذکور از یک آسیب‌پذیری حیاتی در بخش Winbox روترهای ساخت میکروتیک بهره‌جویی می‌شود. شرکت میکروتیک اصلاحیه این آسیب‌پذیری را در ماه آوریل سال میلادی گذشته عرضه کرد. اما تعداد بسیار بالای روترهای آلوده بیانگر عدم نصب اصلاحیه توسط بسیاری از راهبران تجهیزات میکروتیک است. لازم به ذکر است، مرکز ماهر در چندین نوبت نسبت به اجرای حملات گسترده بر ضد روترهای میکروتیک در سطح کشور هشدار داده است.

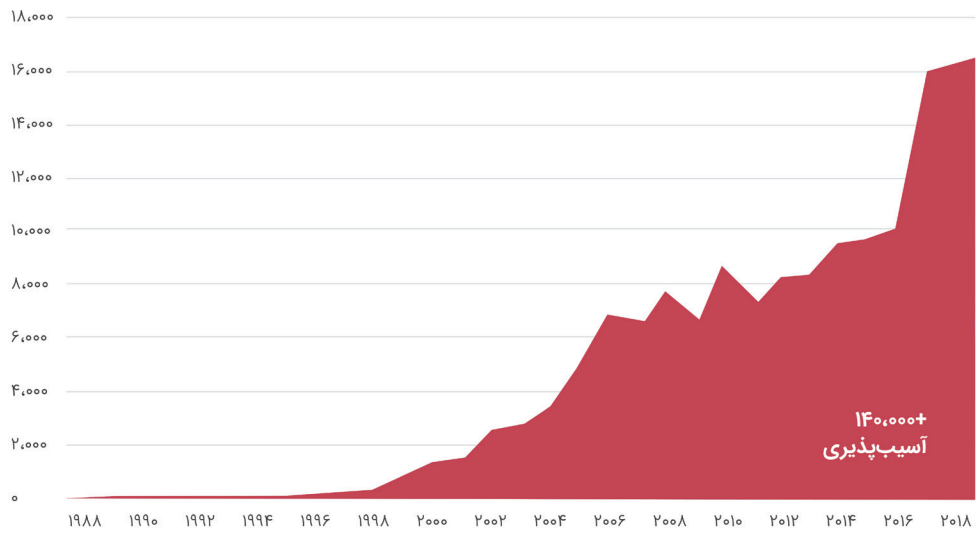


ایران نیز از جمله اهداف مهاجمان در حملات رمز ربایی بوده است. بر طبق گزارشی که شرکت افسکیور آن را منتشر کرده است از اواسط ماه نوامبر سال ۲۰۱۸ کشورهای مختلف از جمله ایران هدف آخرین نسخه از بدافزار NRSMiner قرار گرفته‌اند. NRSMiner بدافزاری است که از طریق ابزار XMRig اقدام به استخراج ارز رمز مونرو با استفاده از منابع دستگاه آلوده‌شده می‌کند. به‌منظور انتشار در سطح اینترنت و شبکه سازمان، نویسندگان NRSMiner نسخه جدید آن را مجهز به بهره‌جوی EternalBlue کرده‌اند. ماجرای بهره‌جوی EternalBlue به دو سال قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به سازمان امنیت ملی آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، ابزارهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر (Zero-day) در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور – با شناسه CVE-2017-0144 – نموده بود. باج‌افزار WannaCry نخستین بدافزاری بود که با بکارگیری بهره‌جوی EternalBlue توانست در کمتر از ۲۴ ساعت صدها هزار کامپیوتر آسیب‌پذیر را در کشورهای مختلف به خود آلوده کند. نکته قابل توجه اینکه علیرغم گذشت نزدیک به دو سال از عرضه اصلاحیه MS17-010 و اطلاع‌رسانی‌های گسترده در خصوص لزوم نصب آن همچنان بسیاری از سیستم‌ها فاقد اصلاحیه مذکور هستند. در گزارش افسکیور، ایران پس از ویتنام، بیشترین سهم از آلودگی‌ها به این بدافزار را به خود اختصاص داده که آن را می‌توان نشانه‌ای از تعداد بالای سیستم‌های آسیب‌پذیر فاقد اصلاحیه MS17-010 در سطح کشور دانست. گفته می‌شود که گردانندگان حملات موسوم به رمز ربایی در سال ۲۰۱۸ میلادی در مجموع ۱۷ میلیارد دلار درآمد به جیب زده‌اند. انتظار می‌رود که بدافزارهای مرتبط با استخراج ارز رمز با بهره‌گیری از هوش مصنوعی بر اساس توان سخت‌افزار پردازشگر دستگاه آلوده شده و ارزش آنی ارز رمزها اقدام به استخراج یک نوع ارز رمز با بالاترین کارایی کنند. علاوه بر استفاده از ضدویروس قدرتمند و به‌روز، بهره‌گیری از ابزارهایی همچون McAfee WebAdvisor و نصب به‌موقع اصلاحیه‌های امنیتی، حساسیت نسبت به نشانه‌های رمزربایی از جمله کندی شبکه، فعالیت غیرعادی پردازشگر و افزایش هزینه‌های برق اهمیت بسزایی دارد.

10011100011110111001011

بهره‌جویی بیشتر و سریع‌تر از آسیب‌پذیری‌های امنیتی

بر اساس آمار منتشر شده از سوی شرکت آی‌بی‌ام، در فاصله بین سال‌های ۱۹۸۸ تا ۲۰۱۸ میلادی، در روندی به شدت صعودی، بیش از ۱۴۰،۰۰۰ آسیب‌پذیری و ضعف امنیتی منحصربه‌فرد در محصولات مختلف فناوری اطلاعات، به‌صورت عمومی گزارش شده است. همانطور که در نمودار زیر نمایش داده شده است حدود یک‌سوم (۳۰ درصد) آسیب‌پذیری‌های ثبت شده در سه دهه اخیر، متعلق به سه سال گذشته بوده است.



نکته قابل توجه، تمرکز هر چه بیشتر تبهکاران سایبری بر روی ضعف‌های امنیتی جدید است. بخصوص آنکه در سالی که گذشت مهاجمان در بدافزارها و حملات سایبری متعددی از آسیب‌پذیری‌های روز صفر و ضعف‌های امنیتی به‌تازگی ترمیم شده بهره‌جویی کردند. برای مثال در بهمن ماه، تنها چند روز پس از عرضه اصلاحیه برای ترمیم دو آسیب‌پذیری در دو مدل از رهیاب‌های سیسکو افشای نمونه کدی از نحوه بهره‌جویی از آن آسیب‌پذیری‌ها، موجب سوءاستفاده مهاجمان از نمونه بهره‌جو و هک شدن برخی از این تجهیزات گردید.

یا در نمونه‌ای دیگر ۲۸ آذر ماه، شرکت مایکروسافت خارج از برنامه زمانبندی معمول خود (سه‌شنبه دوم هر ماه میلادی) اصلاحیه‌ای حیاتی را برای Internet Explorer منتشر کرد. اصلاحیه مذکور، ضعفی را در این مرورگر ترمیم می‌کند که سوءاستفاده از آن مهاجم را قادر به اجرای کد مورد نظر خود به‌صورت از راه دور با سطح دسترسی کاربر وارد شده به سیستم (Logged in User) می‌سازد. لازم به ذکر است که گروه Threat Analysis شرکت گوگل که وجود ضعف مذکور را به مایکروسافت گزارش کرده از مورد بهره‌جویی قرار گرفتن این آسیب‌پذیری به شناسه CVE-2018-8653 در حملات هدفمند خبر داده بود. انتشار جزییات این آسیب‌پذیری پس از عرضه اصلاحیه موجب استفاده برخی گروه‌های نفوذگری دیگر از آن شد. Satan دیگر نمونه‌ای است که مهاجمان این باج‌افزار با سوءاستفاده از حداقل ده ضعف امنیتی، دستگاه‌های با هر یک از سیستم‌های عامل Windows و Linux را هدف قرار می‌دادند. اگر چه از زمان عرضه اصلاحیه برخی از آسیب‌پذیری‌های مورد استفاده این باج‌افزار سال‌ها می‌گذرد اما چندین آسیب‌پذیری آن نیز کاملا جدید و به‌تازگی ترمیم شده بودند. از سویی دیگر مشاهدات میدانی از شبکه‌های ایرانی و گزارش‌های منتشر شده توسط نهادهای نظارتی حاکی از آن است که متأسفانه نصب به‌موقع به‌روزرسانی‌های امنیتی مورد توجه کافی مدیران و راهبران شبکه قرار نمی‌گیرد. برای سال آینده، انتظار می‌رود فاصله میان کشف آسیب‌پذیری و مورد بهره‌جویی قرار گرفتن آن کاهش قابل‌توجهی یابد. تبهکاران سایبری نیز در فرایند توسعه بهره‌جوها چابک‌تر از قبل عمل خواهند کرد. به‌نحوی که شرکت امنیتی مک‌آفی پیش‌بینی کرده که در آینده‌ای نزدیک تبهکاران سایبری گاهی تنها با صرف یک روز یا حتی چند ساعت حملاتی را بر ضد آخرین آسیب‌پذیری‌های کشف شده در نرم‌افزارها و سخت‌افزارها به اجرا در آورند. ضمن اینکه هکرها و ویروس‌نویسان بیشتری به سمت ابزارهای مخرب موسوم به بسته‌های بهره‌جو برای رخنه به اهداف خود و آلوده‌سازی سیستم‌ها روی خواهند آورد. نصب به‌موقع اصلاحیه‌های امنیتی از جمله به‌روزرسانی‌های با درجه اهمیت "حیاتی" از جمله مواردی است که می‌بایست همواره مدنظر مدیران شبکه و کاربران قرار گیرد. همچنین باید توجه داشت که در برخی موارد علیرغم انتشار جزییات آسیب‌پذیری، شرکت سازنده عرضه اصلاحیه را به زمانی بعد موکول می‌کند. در این‌گونه مواقع شرکت سازنده یا کارشناسان امنیتی اقدام به انتشار توصیه‌نامه‌ای به‌منظور پوشش موقت آسیب‌پذیری می‌کنند. بنابراین اکتفای صرف به قابلیت به‌روزرسانی خودکار نمی‌تواند تضمین کننده ایمن ماندن از گزند تهدیدات مبتنی بر بهره‌جو باشد و راهبران باید همواره مطالعه اخبار را در دستور کارهای خود قرار دهند.

استفاده هر چه بیشتر از تکنیک‌های موسوم به گریز

10011100011110111001011

در ۲۰ خرداد ۱۳۹٤ شرکت ضدویروس کسپرسکی اعلام کرد که شبکه سازمانی این شرکت برای ماه‌ها مورد نفوذ گونه جدیدی از بدافزار Duqu موسوم به Duqu 2.0 قرار گرفته بوده. پس از اضافه شدن فرمول شناسایی این گونه جدید به محصولات ضدویروس کسپرسکی، بر اساس گزارش‌های جمع‌آوری شده از سیستم‌های مشتریان این شرکت، ۱۰۰ مورد آلودگی به Duqu 2.0 در کشورهای غربی، آسیایی، خاورمیانه و روسیه شناسایی می‌شود؛ از جمله محل‌های ملاقات ایران با گروه مذاکره کننده ۵+۱ در کشورهای اتریش و سوئیس. شرکت امنیتی سیمانتک نیز بر اساس تحقیقات خود بر روی بدافزار Duqu 2.0، نمونه‌هایی از آن را در یکی از شرکت‌های مخابراتی اروپا و یک شرکت مخابراتی در آفریقای شمالی و همچنین یک تولیدکننده محصولات الکترونیکی در جنوب آسیا، کشف و شناسایی می‌کند. کارشناسان سیمانتک اعلام می‌کنند هدف از نفوذ و آلوده ساختن شرکت‌های مخابراتی و تولیدکننده تجهیزات الکترونیکی، شنود مکالمات تلفن همراه قربانیان Duqu بوده. گونه جدید Duqu بسیار پیچیده‌تر از گونه قبلی این بدافزار بود که در اواسط سال ۱۳۹۰ کشف و شناسایی شد. در آن زمان، با توجه به تعداد محدود آلودگی‌های گزارش شده همه شرکت‌های امنیتی اتفاق نظر داشتند که انتشار Duqu در ارتباط با یک حمله کاملا هدفمند بوده است. در آمار ارائه شده درباره کشورهای هدف، بین شرکت‌های ضدویروس اختلاف نظر وجود داشت اما نام ایران در میان همه این آمارها به چشم می‌خورد. روش‌های مورد استفاده در این گونه جدید بسیار فراتر از فناوری‌های مورد استفاده در تهدیدات پیشرفته و مستمر بود. Duqu 2.0 نمونه‌ای موفق از یک بدافزار Fileless بود. بدان معنا که برخلاف بدافزارهای دیگر، به‌نحوی طراحی شده بود که کد مخرب آن تنها بر روی حافظه اجرا شده و با هر بار راه‌اندازی سیستم از بین برود. گرچه هر دو شرکت کسپرسکی و سیمانتک از اشاره مستقیم به حامی و پشتیبان بدافزار Duqu 2.0 خودداری کردند ولی در مصاحبه‌ها و مطالب منتشر شده بر روی سایت این دو شرکت، دخالت یک یا چند دولت در این ماجرا مطرح شده بود. اما روزنامه Wall Street Journal به نقل از یکی از مقامات سابق آمریکا که نخواست نامش فاش شود این حملات را به اسرائیل نسبت داد. بدیهی است که شناسایی و کشف بدافزارهای از نوع Fileless بسیار دشوارتر از گونه‌های معمول بدافزارها می‌باشد. از آن زمان تا کنون نمونه‌های متعددی از بدافزارهای Fileless پیشرفته گزارش شده است. اگر تا چند سال قبل ساخت چنین بدافزارهایی تنها در انحصار چند گروه نفوذگری بود در سالی که گذشت هزاران نمونه از این نوع بدافزارها شناسایی شد. سیستم عامل پرطرفدار Windows 10 مجهز به ابزارهایی همچون PowerShell، WMI و Windows Scripting Host است که توانایی‌های پرشماری را برای اجرا کننده فراهم می‌سازند. در حالی که استفاده از این ابزارها در جریان حمله در یکی دو سال اخیر محدود به گروه‌های نفوذگر حرفه‌ای بوده اما انتظار می‌رود که سال آینده گروه‌های بیشتری از تکنیک‌های موسوم به "بدون فایل" استقبال کنند. همچنین استفاده از روش‌های دیگر گریز به روالی عادی و متداول در میان بدافزارها تبدیل شده است. خلاقیت و نوآوری نیز در خلق این تکنیک‌ها به‌طور مستمر ادامه دارد. برای مثال، در سال ۹۷ شاهد بودیم که استخراج کننده WaterMiner بسادگی در زمان باز شدن Task Manager یا پویش دستگاه توسط ضدویروس، پروسه استخراج‌کننده را متوقف می‌کرد. باید توجه داشت که استفاده از تکنیک‌های گریز توسط تبهکاران به یکی از الزامات عبور از سد محصولات امنیتی پیشرفته تبدیل شده و بنابراین تداوم بهره‌گیری و تکامل آن تنها راه برای باقی ماندن در صحنه جرایم سایبری است. پیش‌بینی می‌شود که در آینده‌ای نزدیک، هکرهای حرفه‌ای بدافزارهای خود را مجهز به فناوری‌های موسوم به هوش مصنوعی برای خودکارسازی اموری همچون انتخاب هدف، بررسی بستر و تصمیم‌گیری در خصوص نحوه اجرا بر روی دستگاه قربانی کنند. در سال‌های اخیر برخی شرکت‌های به‌نام امنیتی قابلیتی را به محصولات ضدویروس خود افزوده‌اند که از طریق آن بطور پیوسته عملکرد پروسه‌های سیستم مورد رصد قرار گرفته و با تحلیل رفتار، در صورت تشخیص مخرب بودن هر یک، اقدام به متوقف نمودن آن پروسه می‌شود.

ادامه بهره‌جویی از تجهیزات موسوم به اینترنت اشیا

چندین سال است که کارشناسان در خصوص امنیت ضعیف وسایل و تجهیزات متصل به اینترنت، موسوم به اینترنت اشیا (Internet of Things - به اختصار IoT) هشدار داده‌اند. بر اساس آماری که شرکت آی‌بی‌ام آن را منتشر کرده است تعداد کل آسیب‌پذیری‌های گزارش شده در حوزه محصولات اینترنت اشیا در سال ۲۰۱۸ میلادی در مقایسه با پنج سال قبل از آن ۵،۴۰۰ درصد افزایش داشته است. امنیت ضعیف و پیکربندی آسیب‌پذیر این تجهیزات از یک سو و اتصال آنها به شبکه اینترنت از سویی دیگر، این تجهیزات را به هدفی بسیار مناسب و در عین حال آسان برای مهاجمان تبدیل کرده است. یکی از اصلی‌ترین بهره‌جویی‌های تبهکاران سایبری از این وسایل و تجهیزات، تسخیر نمودن آنها برای اجرای حملات توزیع‌شده برای از کاراندازی سرویس (Distributed Denial of Service - به اختصار DDoS) است. در جریان این حملات، لشکری از این تجهیزات هک شده با ارسال درخواست‌های همزمان به سرور قربانی آن را بمباران می‌کنند. دریافت همزمان درخواست، از هزاران و در برخی مواقع ده‌ها هزار دستگاه با نشانی‌های IP مختلف، در نهایت، منجر به کندی و یا حتی توقف خدمات‌دهی سرور به کاربران می‌شود. واقعیت آن است که دستگاه‌های متصل به اینترنت، صرفا دستگاه‌هایی با منابع محدود نیستند. بلکه کامپیوترهایی هستند که اگر به‌طور صحیح پیکربندی و ایمن‌سازی نشوند، می‌توانند به ابزاری مخرب در دست نفوذگران تبدیل شوند. علاوه بر بهره‌جویی از این محصولات برای اجرای استخراج ارز رمز در سال گذشته می توان به بدافزار VPNFilter اشاره کرد. دوم خرداد، شرکت سیسکو در گزارشی از شناسایی شبکه مخرب (Botnet) عظیمی، متشکل از روترها و تجهیزات ذخیره‌ساز متصل به شبکه (Network-attached Storage - به اختصار NAS) هک شده‌ای خبر داد که به باور برخی محققان هدف از تشکیل آن اجرای حمله سایبری گسترده‌ای بر ضد اوکراین بوده است. این روترها و تجهیزات ذخیره‌ساز متصل به شبکه به بدافزاری با نام VPNFilter آلوده شده‌اند. در مقایسه با سایر بدافزارهای ویژه دستگاه‌های موسوم به اینترنت اشیا، VPNFilter، بدافزاری بسیار پیچیده محسوب می‌شود که قابلیت‌های خاص و پیشرفته‌ای نظیر پویش ارتباطات برای یافتن دستگاه‌های کنترل صنعتی SCADA را در سطح شبکه داراست. انتظار می‌رود که در سال ۹۸ نیز اینترنت اشیا از موضوعات مورد علاقه برخی گروه‌های نفوذگری باشد. رعایت موارد زیر آسان‌ترین راه برای حفاظت از دستگاه‌های موسوم به اینترنت اشیا است:

- رمزهای عبور پیش‌فرض دستگاه به رمزهای عبور پیچیده تغییر داده شده‌اند. نام‌های کاربری و رمزهای عبور پیش‌فرض براحتی دستگاه را به تسخیر شبکه‌های مخرب در می‌آورند.
- دستگاه‌های اینترنت اشیاء به آخرین نسخه به‌روز شوند.
- پودمان‌های Telnet و SSH و همچنین پودمان‌های مرتبط با UPnP بر روی این دستگاه‌ها غیرفعال شود؛ مگر آنکه واقعاً به آن نیاز باشد.
- از دستگاه‌های متصل به اینترنت توسط دیواره‌های آتش کارآمد حفاظت شود.
- دستگاه‌های متصل به اینترنت حتی الامکان از شرکت‌های خوشنام خریداری شود.

جمع‌بندی

تا چند سال قبل، اکثر فایل‌های مخرب به‌راحتی در گروهی از بدافزارها (ویروس، باج‌افزار، بهره‌جو، درب‌پشتی، اسب‌تروا، کرم و ...) دسته‌بندی می‌شدند. اما این روزها کمتر فایل مخربی را می‌توان یافت که عملکرد آن تنها محدود به یک نوع از بدافزارها باشد. موضوعی که در بسیاری مواقع شناسایی هدف اصلی مهاجمان را به چالش تبدیل می‌کند. حمله‌ای را تصور کنید که با ارسال یک هرزنامه آغاز می‌شود. در متن هرزنامه به لینکی اشاره شده که با بهره گیری از مهندسی اجتماعی کاربر ناآگاه متقاعد به کلیک بر روی آن می شود. لینک مذکور کاربر را به سایتی اینترنتی هدایت می‌کند که در آن - در ظاهر - ویدئویی درج شده است. ویدئویی جعلی که این طور تظاهر می‌شود که برای مشاهده آن می‌بایست با کلیک بر روی لینکی در صفحه یک افزونه بر روی دستگاه نصب شود. در صورت انجام آن اسکریپت مخربی بر روی دستگاه دریافت می‌شود که از طریق یکی از پروسه‌های معتبر سیستم عامل اقدام به ساخت یک فرمان زمانبندی‌شده بر روی دستگاه قربانی می‌کند. این اسکریپت پس از اجرا در حافظه، مشخصات سخت‌افزاری سیستم را مورد ارزیابی قرار داده و بر اساس یافته‌ها تصمیم می گیرد که دستگاه را آلوده به باج‌افزار کند و یا یک استخراج‌کننده ارز رمز را بر روی آن به اجرا در آورد. با چنین تصویری سئوالات زیادی در ذهن یک تحلیلگر تداعی می‌شود. با چه چیز طرف هستیم؟ حمله‌ای هرزنامه‌ای، فیشینگ، بدون فایل، باج‌افزاری یا رمزربایی؟ مشخص است که تمرکز بر روی یکی از این موارد ما را از سایر اهداف مهاجم غافل ساخته و عملا در مقابله مؤثر با حملات آتی آن عاجز. حتی اگر موفق به متوقف کردن تهدید در میانه زنجیره حمله شوید کشف گام‌های اولیه و نهایی نمی‌بایست نادیده گرفته شود. کنجکاوی و خلاقیت لازمه ردیابی حملات پیشرفته امروزی و پی بردن به اهداف اصلی مهاجمان است؛ آیا ممکن است این حمله باج‌افزاری در ارتباط با موضوعی بااهمیت‌تر باشد؟ چه می‌شود اگر ایمیل ارسالی مبتنی بر ترفندی باشد که کاربران برای مقابله با آن آموزش ندیده باشند؟ و ده‌ها سئوال دیگر از این دست. با این سئوالات نه تنها تصویری واقعی از حمله شکل می‌گیرد که بهبود راهکارهای مقابله و پیشگیری نیز فراهم می‌شود. پس کنجکاو، خلاق و آگاه به استقبال سال ۱۳۹۸ برویم. شرکت مهندسی شبکه گستر سال امنی را برای صنعت فناوری اطلاعات ایران آرزومند است.

فهرست منابع

- https://businessinsights.bitdefender.com/bitdefender-top-10-cybersecurity-predictions-for-2019
- https://learn.bromium.com/social-platforms-2019-web-of-profit.html
- https://newsroom.ibm.com/2019-02-26-IBM-X-Force-Report-Ransomware-Doesnt-Pay-in-2018-as-Cybercriminals-Turn-to-Crypto-jacking-for-Profit
- https://newsroom.shabakeh.net/16261/cyberwarfare-duqu.html
- https://newsroom.shabakeh.net/18219/crypto-ransomware.html
- https://newsroom.shabakeh.net/18625/wannacry-analysis.html
- https://newsroom.shabakeh.net/19298/zeus-panda-analysis.html
- https://newsroom.shabakeh.net/19647/maher-and-recent-phishing-attacks.html
- https://newsroom.shabakeh.net/19684/zoopark-targets-android-users-in-the-middle-east.html
- https://newsroom.shabakeh.net/19749/hardening-rdp.html
- https://newsroom.shabakeh.net/19771/vpnfilter-what-you-need-to-know.html
- https://newsroom.shabakeh.net/19932/mikrotik-coinhive.html
- https://newsroom.shabakeh.net/19957/poolezoor.html
- https://newsroom.shabakeh.net/20126/cryptojacking-using-mikrotik-routers.html
- https://newsroom.shabakeh.net/20200/phishing-report-q3-2018.html
- https://newsroom.shabakeh.net/20374/the-latest-charming-kitten-campaign.html
- https://newsroom.shabakeh.net/20383/maher-report-regarding-instagram-related-apps.html
- https://newsroom.shabakeh.net/20413/mobstspy.html
- https://newsroom.shabakeh.net/20421/gandcrab-analysis.html
- https://newsroom.shabakeh.net/20429/nrsminer-targeting-iranian-users.html
- https://newsroom.shabakeh.net/20438/maher-report-regarding-android-game-apps.html
- https://newsroom.shabakeh.net/20497/blackrouter-promoted-as-raas-by-an-iranian-hacker.html
- https://newsroom.shabakeh.net/20507/roguerobin-using-google-drive-as-a-c2.html
- https://newsroom.shabakeh.net/20515/mcafee-threat-report-2018q3.html
- https://newsroom.shabakeh.net/20535/hackers-targeting-cisco-rv320-rv325-routers.html
- https://newsroom.shabakeh.net/20545/maher-report-regarding-pushfa-malware.html
- https://newsroom.shabakeh.net/20554/new-scam-stating-user-webcam-was-hacked.html
- https://newsroom.shabakeh.net/20625/cr1ptt0r.html
- https://newsroom.shabakeh.net/20644/ibm-says-most-hackers-use-powershell.html
- https://newsroom.shabakeh.net/20649/cybercrime-economy-in-social-media-platforms.html
- https://newsroom.shabakeh.net/20653/maher-cve-2019-3924.html
- https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/
- https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-threats-report-highlights-cryptojacking-block-chain-mobile-security-issues/
- https://securingtomorrow.mcafee.com/consumer/family-safety/cryptojacking-up-4000-how-you-can-block-the-bad-guys/
- https://www.fireeye.com/blog/executive-perspective/2018/11/facing-forward-cyber-security-in-2019-and-beyond.html
- https://www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf
- https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf
- https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-2019-threat-report.pdf

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شبکه گستر
شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳
تلفن / دورنگار ۴۲۰۵۲-۰۲۱
info@shabakeh.net
www.shabakeh.net