۱۲۰

نشریه تخصصی امنیت سایبری مرکز آپا دانشگاه کردستان
شماره دوم/ مردادماه ۱۳۹۷

در این شماره می‌خوانید

- بررسی تخصصی باج‌افزارها و سیر تکاملی آن‌ها
- بررسی تخصصی امنیت در اینترنت اشیاء
- بررسی و تحلیل تهدیدات DDOS برای فراهم‌کنندگان سرویس در سال ۲۰۱۷
- بررسی تخصصی پروتکل SSL و تفاوت‌های گواهی‌نامه‌های آن
- معرفی ابزار Metasploit
- بررسی تخصصی بدافزار Emotet و روند تکثیر آن
- توصیه‌های امنیتی در شبکه‌های اجتماعی
- مهندسی اجتماعی چیست؟

درباره

مرکز آپا دانشگاه کردستان

آپا مخفف عبارت آگاهی‌رسانی، پشتیبانی و امداد رخدادهای رایانه‌ای است و معادل بومی اصطلاح CERT می‌باشد. مرکز آپا دانشگاه کردستان، در راستای انجام فعالیت‌های خود در زمینه آگاهی و اطلاع رسانی، با بکارگیری نیروهای متخصص و پتانسیل‌های پژوهشی در استان کردستان اقدام به انتشار نشریه ای الکترونیکی در حوزه امنیت فضای سایبری نموده است.

مخاطبان اصلی نشریه کارشناسان و متخصصان فناوری اطلاعات و شبکه، دانشجویان و علاقمندان فضای سایبری است. مطالب این نشریه عموماً محورهای زیر را شامل می شود:

- اطلاع رسانی رخدادهای اخیر فضای سایبری
- آگاهی‌رسانی نسبت به آخرین تهدیدات و آسیب‌پذیری ابزارهای فضای مجازی
- آموزش‌های عمومی در جهت ارتقاء دانش عمومی امنیت

شایان ذکر است، ویرا، اسم نشریه، واژه‌ای در زبان کردی به معنی صاحب‌فکر و هوشمند است.

سردبیر: هادی گلباغی
ویراستار : تیم فنی مرکز آپا دانشگاه کردستان
طراحی و صفحه‌آرایی: آریان اسماعیل زاده
نویسندگان :فرشته کیاست / محمد حبیبی/ هادی گلباغی/ اسرین عبدالهی
نویسنده مهمان: آرام یوسفی

تلفن مرکز :۰۸۷۳۳۶۶۲۹۳۲
نشاني مجله:کردستان- بلوار پاسداران-دانشگاه کردستان-مرکز آپا
نشاني وبسایت: www.cert.uok.ac.ir
ایمیل : apa@uok.ac.ir

راهنمایی:

- در فهرست مطالب می‌توانید با کلیک روی هریک از بخش‌ها، به صفحه مورد نظر منتقل شوید.
- در هر یک از صفحات با کلیک کردن روی مثلث زرد به فهرست مطالب باز می‌گردید.
- با کلیک روی QRکد ها می‌توانید مستقیما به لینک ها منتقل شوید.

فهرست

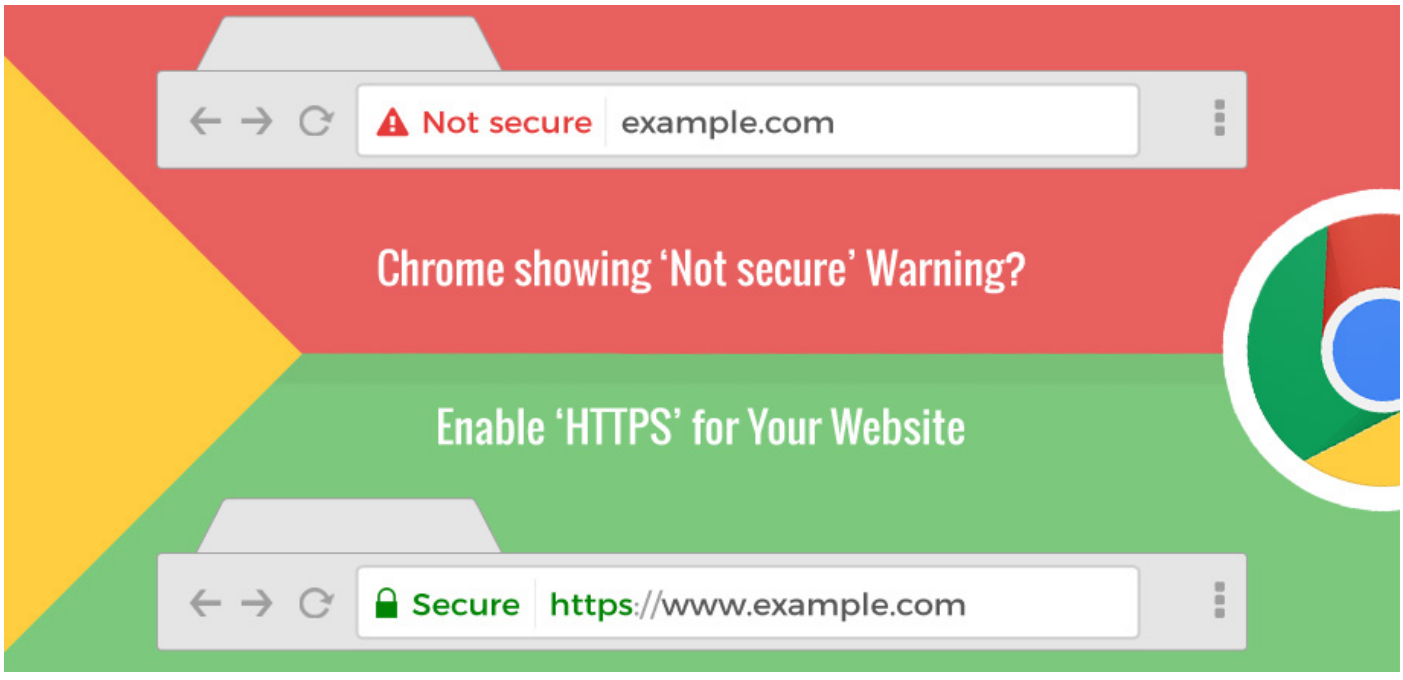
مطالب

تازه‌ها |

سرتیتر خبرهای مهم ماه گذشته

- آسیب‌پذیری‌های چندگانه درPHP و اجازه اجرای کد دلخواه
- رمزگشایی فایل‌های رمز شده توسط باج‌افزار LockCrypt
- آلودگی تعداد زیادی از روترهای میکروتیک در کشور
- آسیب‌پذیری‌های چندگانه در سیستم‌عامل Juniper Junos می‌تواند موجب حمله منع سرویس شود
- آسیب پذیری جدید و خطرناک بر روی Oracle WebLogic
- هشدار مرکز ماهر در خصوص سوء استفاده از آسیب‌پذیری ADB (پورت ۵۵۵۵) در سطح شبکه کشور
- اخاذی ۶ میلیون دلاری باج افزار SamSam از زمان انتشار تاکنون
- ایران در میان ۲۰ کشور اول دنیا در نشت اطلاعات، به دلیل بی‌توجهی سازمان‌های دولتی به سیستم‌های DLP
- خطر حمله سایبری شبکه گسترده‌ای از حمل‌ونقل دریایی را تهدید می‌کند

Chrome برچسب سایت‌های از نوع http را به عنوان "not secure"(نا امن) درنظر می‌گیرد



این خبری بد برای بسیاری از وب سایت‌هایی است که هنوز اتصالات رمزگذاری شده را پشتیبانی نمی‌کنند.

گوگل نسخه ۶۸ مرورگر Chrome خود را به نمایش گذاشته است که برچسب سایت‌های از نوع http را به عنوان "not secure" در نظر می‌گیرد.

این نسخه آخر در مرورگر کروم ویندوز، مک و لینوکس یک نشانگر "not secure" را به سمت چپ نوار آدرس برای هر وب سایتی که از اتصال HTTP رمزگذاری نشده بین سرور سایت و رایانه کاربر استفاده می‌کند قرار می‌دهد.

Emily Schechter مدیر امنیت بخش Chrome شرکت گوگل اعلام کرد:

این امر باعث می‌شود که بدانید اطلاعات شخصیتان هنگامی که وبگردی می‌کنید یا حساب بانکی خود را چک کنید امن است یا نه.

این حرکت که در ماه فوریه هم در مورد آن اطلاع داده بودیم، بخشی از فشار طولانی مدت گوگل برای از بین بردن اتصالات بدون رمزگذاری است که موجب می‌شود، صاحب وب‌سایت مجبور شود، وب‌سایتش را به HTTPS، که نسخه محافظت شده HTTP است تبدیل کند.

HTTPS یا Hypertext Transfer Protocol secure ، ترافیک وب را رمزگذاری می‌کند، بنابراین اطمینان حاصل می‌شود که داده‌های ارسال شده در هنگام انتقال از دسترس مهاجمان خارج و غیر قابل رصد است. در طرفی دیگر، حضور این پروتکل به تنهایی به این معنی نیست که سایت می‌تواند ۱۰۰٪ مورد اعتماد باشد، زیرا حتی یک سایت HTTPS هم می‌تواند مخرب باشد.

Schechter پیشرفتی باور نکردنی را در اتخاذ HTTPS طی دو سال گذشته ذکر کرده است، یعنی از زمان اعلام گوگل که سایت‌های بدون رمزگذاری HTTPS در نهایت به عنوان "not secure" برچسب‌گذاری می‌شوند. ۸۳ مورد از ۱۰۰ سایت برتر در وب به طور پیش فرض از HTTPS استفاده کرده‌اند.

بدیهی است، هنوز هم بسیاری از سایت‌های محبوب هنوز سایت خود را به HTTPS تبدیل نکرده‌اند. سرویس‌دهنده امنیت فضای ابری شرکت cloudflare گفت که در ماه گذشته حدود ۵۴۰،۰۰۰ وب‌سایت از نزدیک به ۱ میلیون وب‌سایت برتر در سراسر جهان کاربران را به HTTPS هدایت نمی کنند.

HTTPS های بیشتری در راه است

کار گوگل تنها با تغییرات در نحوه برخورد امنیتی با صفحات HTTP و HTTPS تمام نمی‌شود و در نسخه ۶۹ گوگل کروم در ماه سپتامبر، نشانگر "secure" را برای صفحات HTTPS خواهد گذاشت.

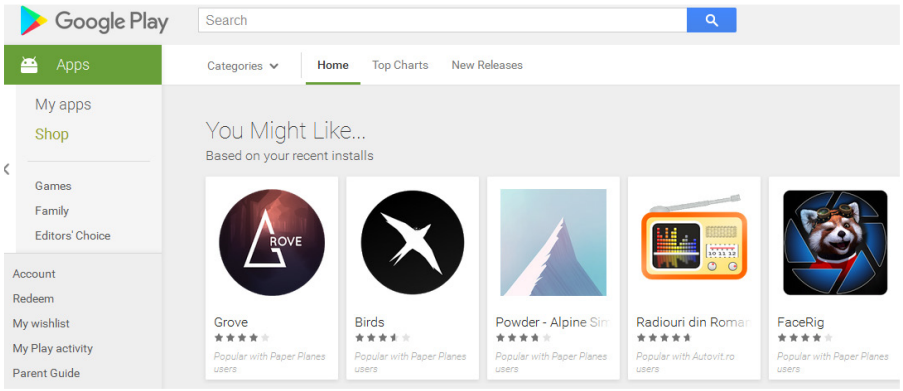
گوگل در ماه می اعلام کرد:

کاربران باید انتظار داشته باشند که وب به طور پیش فرض امن باشد و هنگام بروز یک مشکل هشدار داده شود،و از آنجایی که به زودی تمام صفحات HTTP به عنوان "not secure" برچسب زده می‌شود، پس صفحات HTTPS بدون برچسب و به صورت پیش‌فرض ایمن در نظر گرفته می‌شوند. سپس در نسخه ۶۹ گوگل کروم هر بار که یک کاربر وارد یک صفحه HTTP شود، یک نشانگر "not secure" به رنگ قرمز نشان داده می‌شود.

منبع:

بازگشت به فهرست مطالب

Droppers راهی مخفی برای ورود به Play Store و مقابله با آن توسط Play Protect



در سال‌های گذشته، بدافزار نویسان اندروید به طور فزاینده‌ای روی فریب دادن و دور زدن اسکن‌های امنیتی گوگل و مخفیانه وارد کردن نرم‌افزارهای مخرب به Play Store آن تاکید کرده‌اند.

این فریب به نوعی مشابه تکنیک بدافزارهای مبتنی بر دسکتاپ است،که در طول سال گذشته نیز در بازار اندروید متداول شده بود.

این تکنیک شامل استفاده از Dropper ها می‌شود که این اصطلاح یک فرآیند آلوده‌سازی دومرحله‌ای یا چندمرحله‌ای است که در مرحله اول نرم افزار مخرب اغلب یک تهدید ساده و با قابلیت‌های محدود هستند و نقش اصلی آن این است که به منظور دریافت تهدیدات قوی‌تر، راهی را از طریق دستگاه برای دریافت بدافزارهای دیگر پیدا کند.

Dropper ها در زمینه‌ی موبایل و تلفن‌های هوشمند بسیار موثر و خطرناک می‌باشند

در محیطهای دسکتاپ Dropper ها خیلی کارآمد نیستند، زیرا استفاده گسترده از آنتی‌ویروس‌ها،آنها و همچنین بارگذاری‌های مرحله دومشان را تشخیص می‌دهد ولی در زمینه‌ی موبایل بسیار موثر هستند و این به دلیل آن است که اکثر تلفن‌های همراه از آنتی‌ویروس استفاده نمی‌کنند و هیچ شناساگر تهدیدی روی دستگاه برای تشخیص بارگذاری‌های مرحله دوم آن وجود ندارد.

این بدان معنی است که تنها اقدامات امنیتی که در تلفن‌ها قرار دارند، اسکن‌های امنیتی است که Google قبل از تأیید هر برنامه‌ای که در Play Store قرار دارد، انجام می‌دهد.

نویسندگان بدافزار در سال‌های گذشته متوجه شده‌اند که گوگل کار بسیار سخت و زمانبری را در برداشتن Dropper های پنهان در برنامه‌های قانونی دارد . همچنین، بیشتر عملیات‌های مخرب از طریق این حقه که از تقسیم کد به دو قسمت Dropper و نرم‌افزار مخرب واقعی است، صورت گرفته‌است.

دلیل آن این است که Dropper نیاز به تعداد کمتری از مجوزها دارد و رفتار محدودی را از خود نشان می‌دهد که می‌تواند دیرتر به عنوان نرم افزار مخرب طبقه‌بندی شود. علاوه بر این، اضافه کردن تایمر که اجرای هر کد مخرب را چند ساعت به تاخیر می‌اندازد کمک می‌کند تا بدافزار در اسکن گوگل شناسایی نشود.

این ترفندهای ساده، تکه‌های کوچکی از کد مخرب را در داخل Play Store در همه نوع برنامه‌ها، از دسته‌های مختلف پنهان می‌کند. هنگامی که کاربران برنامه‌ها را اجرا می‌کنند، در اکثر موارد تبلیغاتی آن برنامه اجرا می‌شود، کد مخرب اجرا می‌شود. همچنین Dropper ها درخواست مجوزهای مختلف می‌کنند و اگر این مجوزها تایید شود، می‌توانند بدافزارهایی قوی‌تر را بارگیری کنند.

Dropper بیشترین پشتیبانی را از تروجان‌های بانکداری تلفن همراه می‌کند

این ترفند عمدتا توسط نویسندگان بدافزار نسخه‌های LokiBot، Exobot و Mobile BankBot منتشر شده است اما در عین حال توسط بسیاری دیگر از نویسندگان بدافزار نیز به تصویب رسیده است.

محققان امنیتی از ThreatFabric در مورد افزایش استفاده، محبوبیت و کارایی برنامه‌های دارای Dropper در Play Store در ماه مه ۲۰۱۷، اوت ۲۰۱۷، سپتامبر ۲۰۱۷، نوامبر ۲۰۱۷ و ژانویه ۲۰۱۸، از حملات با ابزارهای تروجان اندروید مانندBankBot، Red Alert (Anubis I)، BankBot (Anubis II)، LokiBot ۲٫۱ / ۲٫۰ و Exobot خبر داده‌اند.

در این ماه، این تکنیک باری دیگر در یک گزارش IBM X-Force مورد بررسی قرار گرفت که مربوط به بررسی توزیع بدافزار Anubis II بود که Anubis II یکی از جدیدترین نسخه های BankBot می‌باشد.

تیم IBM گفت: این کمپین حداقل ۱۰ برنامه دانلودگر را به عنوان برنامه‌های مخرب لیست کرده است که همه آن‌ها تروجان‌های بانکداری تلفن همراه را بر روی دستگاه‌های مبتنی بر اندروید اجرا می‌کنند و اگرچه تعداد دانلودگرها ممکن است نسبتا کم به نظر برسد ولی هر یک از این برنامه‌ها می‌توانند بیش از ۱۰۰۰ نمونه از سرورهای C&C مخرب را اجرا کنند.

DaaS - دانلود کننده به عنوان یک سرویس

این روند اخیر استفاده از بدافزارهای مشابه از نوع Dropper (که همچنین به عنوان بدافزارهای دانلودگر شناخته می‌شوند) کارشناسان IBM را به این باور رسانده که برخی از باندهای سایبری در حال حاضر عملیات «دانلود کننده به عنوان یک سرویس» (DaaS) را اجرا می‌کنند که در آن فضای نصب برنامه‌های Dropper خود را همزمان به گروه‌های دیگر اجاره می‌دهند.

این امر توضیح می‌دهد که چرا اکثر Dropper ها یکسان هستند و بارگذاری‌های مختلف و گسترده‌ای را به صورت جمعی از بدافزارها توزیع می‌کنند.

به گفته گیتان ون دیمن، محقق امنیتی ThreatFabric که تئوری IBM را درباره سرویس DaaS برای اپراتورهای مخرب اندروید تایید کرد :

« در اکوسیستم بدافزاری بانکداری اندروید ، برای مهاجمان امری معمول است که Dropper را از مهاجمان دیگر خریداری کنند

و Dropper ها محبوب‌تر شده‌اند چون اجازه می‌دهند تا توزیع گسترده‌تری از نرم‌افزارهای مخرب و بدافزارها از منابع قابل اعتمادی مثل Play Store انجام گیرد و در نتیجه تعداد بیشتری از قربانیان را به دست می‌آورد و نتیجه آن یک مدل کسب و کار جدید است که در آن برنامه‌های مخرب و نصب و راه‌اندازی آن‌ها در Play Store به هکرها و مهاجمان فروخته می‌شود.

بدافزارهای موبایلی ، از بازار بدافزارهای مبتنی بر دسکتاپ تقلید می کنند

در نهایت این امر تعجب آور نیست، چون این دقیقا همان چیزی است که در بازار بدافزارهای دسکتاپ اتفاق می‌افتد زیرا اجرای عملیات Dropper برای گروه‌های مخرب ، کسب و کار مالی قابل ملاحظه‌تری نسبت به اجرای تروجان‌های بانکی واقعی دارد.

به عنوان مثال، این هفته سیمانتک یک گزارش منتشر کرد که نشان می‌دهد چگونه تروجان بانکی کمیاب و بسیار خطرناک Emotet به عنوان یک Dropper استفاده می‌شود که در حال حاضر فضای دانلود اجاره می‌دهد و تروجان های بانکی را با تروجان‌هایی که قبلا با آن‌ها کار کرده است توزیع می‌کند. در همین شماره مجله این بدافزار به صورت تخصصی بررسی شده است.

اقدامات متقابل گوگل در مقابل Dropper ها

محبوبیت رو به رشد برنامه‌های خرابکار اندروید مثل Dropper یکی از دلایلی است که گوگل سرویس Play Protect را راه اندازی کرده است که یک ویژگی امنیتی ساخته شده در برنامه Play Store است که به طور مداوم برنامه‌های محلی نصب شده را که در طول روند تایید اعتبار اولیه آن‌ها را بررسی نکرده است، به امید پیدا کردن رفتار و تغییرات مخرب اسکن می‌کند.

اما ون دیمن معتقد است گوگل در حال حاضر در معرض خطر است زیرا مهاجمان انرژی زیادی را برای غیرقابل تشخیص بودن بدافزارها صرف می‌کنند پس تشخیص برنامه‌های شامل Dropper هم به طبع کار خیلی سختی است.

به عنوان مثال، کد مخرب برخی از برنامه‌های Dropper تنها زمانی فعال می‌شوند که یک فرمان از سرور C&C دریافت می‌کنند به این معنی که بدون تاخیر خاص یا اقدامات خاص، رفتار برنامه به نظر خوش‌بینانه است.

در بعضی موارد، بدافزارهای بانکی مخرب تنها بر اساس یک تاخیر خاص یا زمانی که برنامه به شدت در دستگاه استفاده می‌شود فعال می‌شوند، به عنوان مثال یک بازی.

چنین تکنیک‌هایی به اندازه کافی ساده هستند، اما شناسایی و تشخیص Dropper در محیطهای تست خودکار خیلی دشوار است. گوگل برای شبیه‌سازی استفاده مداوم برنامه‌ها در مقیاس بزرگ به بررسی‌های مجدد میلیون‌ها برنامه که در Play Store آپلود شده‌اند، نیاز دارد.

اما ون دیمن اشاره می کند گوگل در هنگام انجام اسکن‌هایش می‌تواند شاخص‌های اضافی فعالیت‌های مخرب را هم بررسی کند و شگفت آور این است که اطلاعات دقیق و فنی در مورد بسیاری از Dropper ها به صورت عمومی در دسترس هستند و می‌تواند به گوگل اجازه دهد تا این برنامه‌ها را با راحتی تشخیص دهد.

برای مثال، کمپین Exobot همچنان از همان کد Dropper استفاده می‌کند که اولین بار از آن استفاده شده است، پس این اطلاعات هم باید توسط اسکنر داخلی گوگل و یا Google Play Protect مورد استفاده قرار گیرد. با توجه به مشکلاتی که در زمینه Dropper ها برای گوگل پیش آمده است نیاز است که برخی از آگاهی رسانی ها بر روی این موضوع مهم مطرح شود.

منبع:

باگی در بلوتوث که می‌تواند دستگاه‌ها را در معرض حمله مهاجمان قرار دهد

محققان در برخی از پیاده‌سازی‌های بلوتوث به مشکلی پی برده‌اند که می‌تواند به یک مهاجم، اجازه ردیابی و جاسوسی اطلاعات رد و بدل شده میان دو دستگاه آسیب‌پذیر را بدهد.

این باگ رمزنگاری که به عنوان CVE- ۵۳۸۳-۲۰۱۸ شناخته می‌شود، دو ویژگی مهم بلوتوث را تحت‌تاثیر قرار می‌دهد:

۱- Secure Simple Pairing

۲- اتصالات LE(Low Energy) ایمن با نام تجاری Smart Bluetooth

گروه ویژه بلوتوث (SIG) که بدنه حاکم در ورای استانداردهای بلوتوث می‌باشد، در این باره عنوان کرده است: برخی از پیاده‌سازی‌های بلوتوث یا درایورهای نرم افزاری سیستم عامل، در تایید اعتبار رمزنگاری عمومی در جفت‌سازی وایرلس (بی سیم) دستگاه‌ها، شکست خورده‌اند.

جهت حصول اطمینان در این باره، نه تنها چنین بررسی لازم نیست، بلکه تنها مشخصات بلوتوث کفایت می‌کند. یا همانگونه که SIG اعلام کرده است: به‌روزرسانی مشخصات بلوتوث به این معنا که باید تمام پارامترهای رمزنگاری عمومی در اتصالات بلوتوث تایید اعتبار شوند.

مرکز هماهنگی‌های CERT ایالات متحده (CERT/CC) جزئیات بیشتری را درمورد این آسیب‌پذیری منتشر کرده و گفته است: مکانیزم جفت‌سازی بلوتوث، بر «منحنی بیضوی تبادل کلید دیفی-هلمن» یا (ECDH) استوار می‌باشد. جفت کلیدهای ECDH شامل یک کلید خصوصی و یک کلید عمومی است. کلیدهای عمومی برای ایجاد یک کلید جفت‌سازی به اشتراک گذاشته شده، تبادل می شوند. این دستگاه‌ها همچنین باید با پارامترهای منحنی بیضی شکلی که مورد استفاده قرار می‌گیرد، موافقت کنند.

به گفته CERT/CC، در برخی از پیاده‌سازی‌های بلوتوث، پارامترهای منحنی بیضوی، توسط الگوریتم‌های رمزنگاری، معتبر شناخته نمی‌شوند. ممکن است از این طریق به یک مهاجم از راه دور در محدوده وایرلس (بی‌سیم) اجازه داده شود که یک کلید عمومی نامعتبر را تزریق کند. چنین مهاجمی می‌تواند بصورت منفعل، تمام پیام‌های دستگاه را ردیابی و رمزگشایی کند و یا پیام‌هایی با محتوای مخرب را جعل و تزریق نماید.

اما هنوز همه چیز از دست نرفته است!

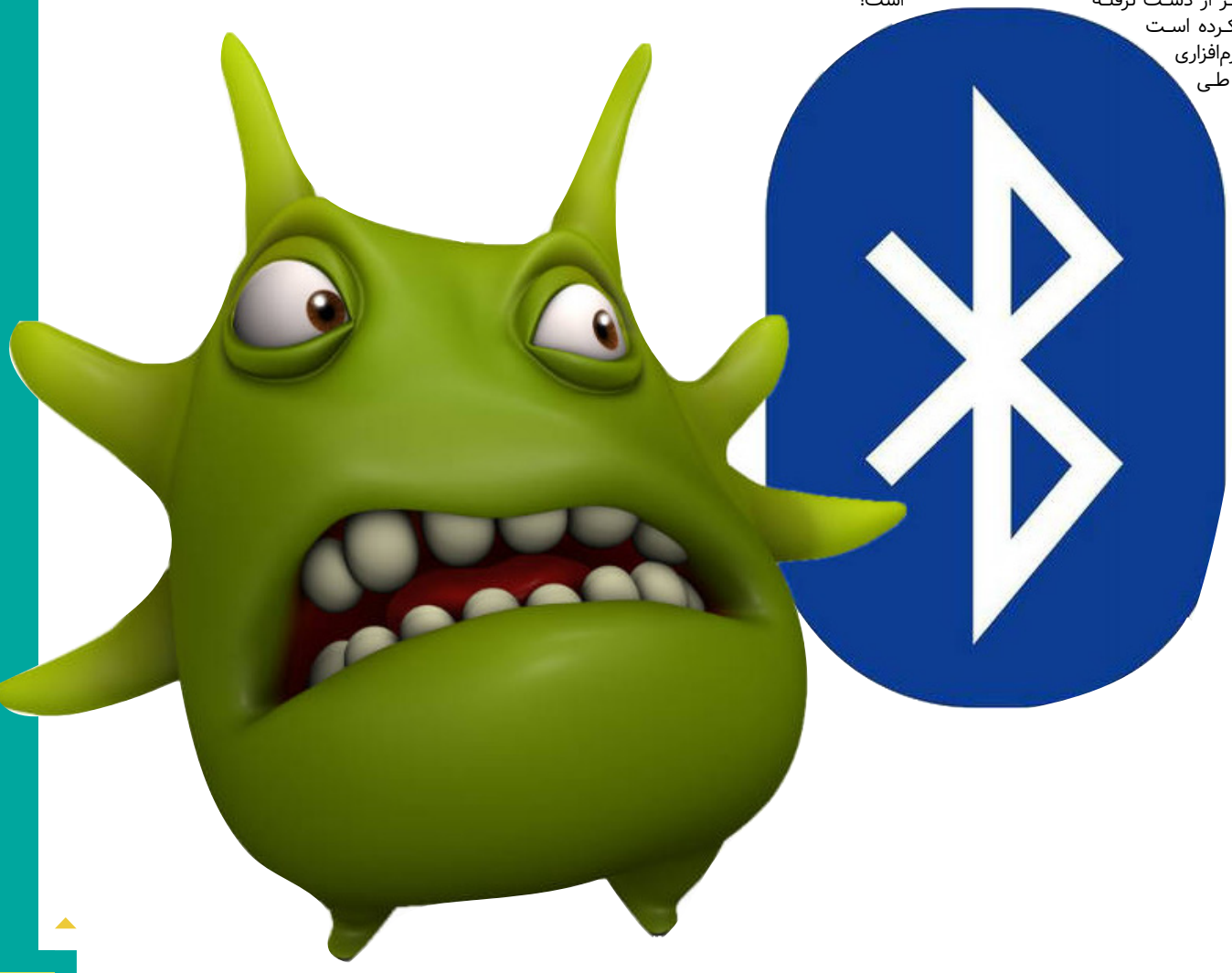
CERT/CC عنوان کرده است که به‌روزرسانی‌های نرم‌افزاری و سخت‌افزاری در طی هفته‌های آینده، منتشر خواهد شد. بنابراین به کاربران توصیه می‌شود که برای به‌روزرسانی‌های لازم به فروشندگان دستگاه مراجعه فرمایند.

Apple، Broadcom و Intel همگی این نقص بلوتوثی را تایید کرده و دو مورد نخست یعنی Apple و Broadcom قبلا به‌روزرسانی‌های خود را منتشر نموده‌اند. CERT/CC عنوان کرده است که: چیپ‌ست‌های Qualcomm نیز تحت تاثیر این باگ بلوتوثی قرار گرفته‌اند. درحالیکه آسیب‌پذیری اندروید، گوگل و لینوکس در برابر این مشکل، هنوز نامشخص است.

به گفته SIG ، از این نقص بلوتوثی، گزارشی مبنی بر سو استفاده ارائه نشده است. اما در هر صورت در چنین حمله‌ای لازم است که مهاجم، خود را در محدوده بلوتوث فعال شده هر دو دستگاه مورد هدفی قرار دهد که از طریق فرآیند جفت‌سازی به یکدیگر متصل شده‌اند. علاوه بر این، برای موفقیت آمیز بودن این حمله، لازم است که هر دو دستگاه آسیب پذیر باشند.

مسلما ساده‌ترین راه مقابله با این حمله این است که، هر زمان از بلوتوث خود استفاده نمی‌کنید، آن را خاموش نمایید.

منبع:



XSS-Filter نرم افزار Microsoft Edge ممکن است از دسترس خارج شده باشد

به گفته Gareth Heyes، محقق شرکت امنیت اینترنتی PortSwigger، این ویژگی امنیتی مرورگر Microsoft Edge متوقف شده است. ویژگی امنیتی مورد نظر « XSS-Filter» نامیده می‌شود و مکانیزمی امنیتی توسعه‌یافته توسط شرکت مایکروسافت است که می‌تواند از حملات به سایت از نوع (XSS) در داخل مرورگرها جلوگیری کند.

مایکروسافت XSS-Filter را در سال ۲۰۰۸ برای اولین بار روی اینترنت اکسپلورر ۸ طراحی و راه اندازی کرد، و بعداً این ویژگی به نسخه Edge گسترش داده شد و همچنین با سایر مرورگرها مانند Google Chrome و Safari هم تطبیق داده شد.

هنگامی که مرورگر یک صفحه را بارگذاری می‌کند ابتدا هدر آن را شناسایی کرده و حفاظت‌های امنیتی XSS Filter را بر اساس مقدار آن هدر اجرا می‌کند که می‌تواند یکی از سه مقدار زیر باشد.

• هنگامی که مرورگر یک header به صورت
`«X-XSS-Protection: 0»`
می‌بیند، XSS-Filter را غیرفعال می‌کند.
• هنگامی که مرورگر یک header به صورت
`«X-XSS-Protection: 1»`
می‌بیند، آن صفحه را از کدهایی که الگوهای آن مخصوص حملات XSS هستند، پاکسازی می‌کند.
• هنگامی که مرورگر یک header به صورت
`«X-XSS-Protection: %1 mode = block»`
می‌بیند، در صورت تشخیص الگوهای خاصی از حملات XSS، نمایش هرگونه محتوا در صفحه را بلوکه می‌کند.

در سه سال گذشته، از زمانی که نسخه Edge منتشر شده است ، این نسخه مقدار دوم را به عنوان تنظیم پیش‌فرض مورد استفاده قرار داده است، به این معنا که Edge سعی خواهد کرد که کد هر صفحه‌ای را که بارگذاری می‌شود از الگوهای خاص حملات XSS پاکسازی کند، صرف نظر از اینکه آیا header دارای پیکربندی حفاظت X-XSS است یا نه.

XSS-Filter در نسخه‌های قبلی Edge به صورت پیش‌فرض خاموش نیست

اما این هفته Gareth Heyes کشف کرد که Edge تنظیمات XSS-Filter را آنگونه که قبلا اجرا می‌کرد اجرا نمی‌کند.

Heyes گفت: XSS-Filter باید به صورت پیش‌فرض روشن باشد اما اکنون به طور پیش فرض خاموش است و حتی اگر سعی کنیم آن را با
`«X-XSS-Protection: 1»`
روشن کنیم باز هم خاموش می‌ماند.

دلیل اینکه چرا فیلترXSS به صورت پیشفرض برای همه سایت‌ها خاموش است نامعلوم است، چرا که هیچ اطلاعیه رسمی از مایکروسافت یا تیم Edge منتشر نشده است و به نظر نمی‌رسد که بازنگری در این بخش از مایکروسافت درحال اجرا باشد. به نظر می‌رسد یک نقص یا اشکال باشد زیرا این ویژگی در مرورگر اینترنتی دیگر مایکروسافت یعنی اینترنت اکسپلورر کار می‌کند و به صورت پیش فرض روشن است و اگر مایکروسافت می‌خواست این ویژگی را حذف کند، این کار را در هر دو مرورگر خود انجام می‌داد.

علاوه بر این، XSS-Filter همچنان در Edge می‌تواند فعال شود اما فقط هنگامی که وب سایت‌ها به طور خاص از تنظیم سوم خود استفاده می‌کنند که بیشتر مدیران سایت‌ها از استفاده از آن جلوگیری می‌کنند زیرا بلوک Edge از نمایش همه سایت‌ها با هم طور کامل جلوگیری می‌کند.

Heyes افزود: تنها راهی که در واقع می‌توان آن را فعال کرد زمانی است که هدر
`«X-XSS-Protection: %1 mode = block»`
فعال باشد.

راهی برای حذف XSS-Filter

محققان PortSwigger یک مورد را طراحی کرده‌اند که حذف XSS-Filter نیز ممکن است یک ایده خوب باشد و به همین دلیل است که بسیاری از محققان امنیتی در مورد آن شکایتی ندارند.

• اولاً بسیاری از محققان این ویژگی را کنار گذاشته‌اند و یا از آن در مقابل حملات دیگر به زیرلایه browser استفاده می‌کنند.
• دوماً مرورگر Mozilla هرگز از این ویژگی پشتیبانی نمی‌کند و هرگز از این قابلیت برای تبدیل شدن به یک مکانیسم anti-XSS cross-browser-supported پشتیبانی نکرده است.
• سوماً با توجه به پورتال MDN که سایت اسناد رسمی ویژگی‌های وب است، ویژگی XSS-Filter دیگر به اندازه قبل اهمیت ندارد. هنگامی‌که سایت‌ها یک سیاست امنیتی قوی را اجرا می‌کنند که قابلیت استفاده از inline JavaScript ('unsafe-inline')را غیرفعال می‌کند، در مرورگرهای مدرن این محافظت‌ها غیرممکن است. در حالی که این XSS-Filter هنوز هم می‌تواند حمایت‌هایی را برای کاربران مرورگرهای قدیمی‌تر که هنوز از CSP پشتیبانی نمی‌کنند، فراهم کند.
• چهارماً این ویژگی اغلب توسط مدیران وب سایت اشتباه گرفته شده و بد پیکربندی می‌شود ، از این رو به ندرت پتانسیل کامل آن مورد استفاده قرار می‌گیرد.

بنابراین، حتی اگر این یک اشکال باشد یا اینکه مایکروسافت آن‌را با هدفی غیرفعال کرده باشد، به نظر می‌رسد که این ویژگی طرفداران آنچنان زیادی ندارد که دوباره راه اندازی شود.

منبع:

سایت‌های بزرگ هنوز هم تا حد زیادی در مورد اینکه کاربران به دنبال انتخاب رمز عبور امن‌تر باشند، سهل انگاری می‌کنند

در این زمینه یک مطالعه از دانشگاه پلیموث مورد بررسی قرار گرفت که آیا محبوب‌ترین وب سایت‌های به زبان انگلیسی به کاربران کمک می‌کنند تا امنیت خود را تقویت کنند و آن‌ها را در ایجاد رمز عبورهای امن‌تر در هنگام ثبت‌نام یا فرآیندهای تغییر رمز عبور راهنمایی می‌کنند یا خیر.

این بررسی نشان می‌دهد برخی از بزرگترین نام‌های اینترنتی به طور عمده کاربران را در انتخاب امن‌تر رمز عبور زمانی که آن را ایجاد یا تغییر می‌دهند،سهل انگاری و کم کاری می‌کنند.

استیون فارل، استاد امنیت اطلاعات در دانشگاه بریتانیایی، اخیرا در بدست آوردن شیوه‌های رمز عبور گوگل، فیس بوک، ویکی پدیا، ردیت، یاهو، آمازون، توییتر، اینستاگرام، مایکروسافت لایو و نت فلیکس مطالعاتی انجام داده است.

نتایج خلاصه شده در یک مقاله به نام "ارزیابی شیوه های رمز عبور وب سایت بیش از یک دهه پیشرفت؟ Assessing website password practices – over) (a decade of progress" جمع آوری شده است.

به طور خلاصه، برخی از بزرگترین سرویس‌های آنلاین در جهان هنوز اجازه می‌دهند مردم از واژه "password" استفاده کنند، در حالی که سرویس‌های دیگری هم وجود دارند که امکان انتخاب رمزهای عبور تک کاراکتری و کلمات اساسی از جمله نام خانوادگی فرد و یا تکرار شماره شناسایی کاربر را فراهم می‌کنند.

با وجود پیشرفت‌های جزئی در برخی از حساب‌ها شکل ۱ در طول سال‌ها عمدتا بدون تغییر ثابت مانده است. این به رغم افزایش تهدیدات سایبری و نقض حریم خصوصی ، همراه با این واقعیت است که شمار زیادی از افراد با استفاده از کلمه عبور نامناسب ، یکی از رایج‌ترین اشتباهات امنیتی را به وجود می‌آورند.

تعدادی از سایت‌های بسیار محبوب به زبان انگلیسی که به کاربران اجازه می‌دهند از واژه "password" به عنوان رمز عبور خود استفاده کنند. در نتیجه میزان گذرواژه‌های امن در طی این سال‌ها کاهش یافته است. همچنین تعداد خدمات مربوط به احراز هویت دو فاکتوره که موجب محافظت از حساب افراد می‌گردد در بین سال‌های ۲۰۱۱ تا ۲۰۱۸ افزایش بیشتری داشته است.

از ده سرویس آنلاین تحت بررسی گوگل ، مایکروسافت و یاهو بهترین کمک به کاربران را در طراحی یک رمزعبور قوی را ارائه کردند.

آمازون در ارائه سرویس‌های امنیتی رمز عبور بدترین بوده و در حال حاضر و همچنین چهار سال پیش، به همراه ردیت و ویکی پدیا به عنوان بدترین اجرا کنندگان امنیت کلمه عبور انتخاب شده‌اند.

در حال حاضر، با وجود عدم راهنمایی کامل برخی از بزرگترین وب سایت‌ها توضیحاتی در مورد چگونگی اجتناب از خطرات کلمه عبور، استفاده مجدد از آن‌ها و در واقع چگونه از لو رفتن رمز عبور خود جلوگیری کرده و در انتخاب یک گذرواژه مناسب اطمینان حاصل کنیم، داده شده است. همچنین در شماره نخست از مجله ویرا نیز مقاله‌ای در خصوص انتخاب رمز عبور صحیح توضیحاتی را ارائه کرده است.

منبع:

Site	Restrictions enforced at sign-up						Other Support		
	Enforces min length (+max if stated)	Prevents surname	Prevents user ID	Prevents 'password'	Enforces composition	Prevents dictionary words	Password meter	Extra protection	Prevents reuse
Amazon	6	✘	✘	✘	✘	✘	✘	✓	✘
Facebook	6	✓	–	✓	✘	✓	✘	✓	✘
Google	8	✓	✓	✓	✓	✓	✘	✓	✓
Instagram	6	✘	✓	✓	✘	~	✘	✓	✓
Microsoft Live	8	–	✓	✓	✓	~	✘	✓	✓
Netflix	4–60	–	✘	✘	✘	✘	✘	✘	✓
Reddit	6	–	✘	✘	✘	✘	✓	✓	✘
Twitter	6	✘	✘	✓	✘	~	✘	✓	✘
Wikipedia	✘	✘	✓	✓	✘	~	✘	✘	✘
Yahoo!	7	✓	✓	✓	✘	✓	✘	✓	✓

شکل ۱. اجرای محدودیت‌های رمز عبور و در دسترس بودن پشتیبانی اضافی
(منبع: ارزیابی شیوه‌های رمز عبور وب سایت - بیش از یک دهه پیشرفت. نوشته شده توسط TechCrunch)

| مقاله‌های آموزشی

بررسی تخصصی امنیت در اینترنت اشیاء

■ اسرین عبدالهی

مقدمه

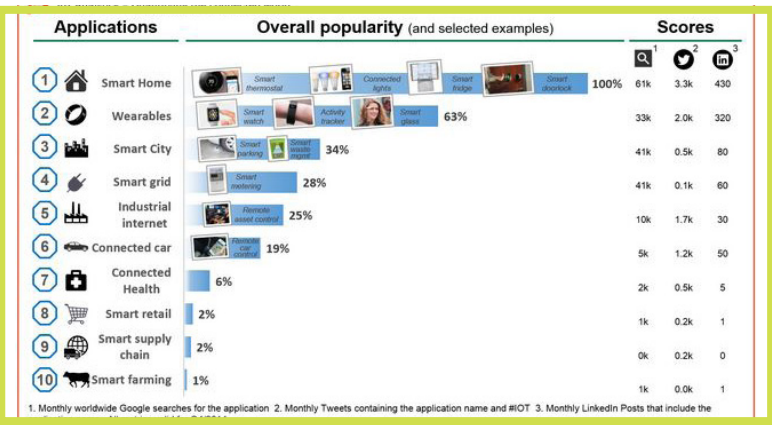
اینترنت اشیاء (IoT) یکی از جدیدترین بحث های روز دنیا در زمینه فناوری اطلاعات و ارتباطات است به گونه‌ای که تاکنون تلاش های زیادی برای پیاده سازی و سازگاری آن با اینترنت سنتی صورت گرفته است. هدف این تکنولوژی هویت بخشیدن به دستگاه های وصل شده به اینترنت و کاهش نقش انسان در مدیریت و کنترل این دستگاه ها می‌باشد.

تاکنون تعاریف زیادی برای اینترنت اشیاء ارائه شده است. McKinsey، اینترنت اشیاء را مجموعه ای از سنسورها و محرک های جاسازی‌شده در اشیاء فیزیکی تعریف کرده است که از طریق شبکه های سیمی و بیسیم به اینترنت متصل می شوند. اما اصطلاح اینترنت اشیاء برای اولین بار در سال ۱۹۹۹ توسط کوین اشتون مطرح شد. این اشیاء تنها به کامپیوترها و موبایل ها محدود نیستند، بلکه هر شی اطراف ما را شامل می شود که در بخش‌های مختلف زندگی چون کسب و کار، سلامت و غیره جهت جمع آوری اطلاعات تعبیه شده است. اینترنت اشیاء به طور چشمگیری بخش های وسیعی از زندگی ما را فرا گرفته است و کاربرد های مختلفی چون خانه های هوشمند، شهرهای هوشمند، حوزه سلامت و غیره را برای آن می‌توان نام برد. در شکل ۱ نمونه‌هایی از اینترنت اشیا نشان داده شده‌اند. در همین راستا IoT Analytics، کاربردهای مختلف اینترنت اشیاء را با توجه به میزان سرچ گوگل، بررسی ها و نوشته های افراد مختلف در سایت های معتبری چون توییتر و LinkedIn به‌صورت شکل ۲ رتبه‌بندی کرده است.

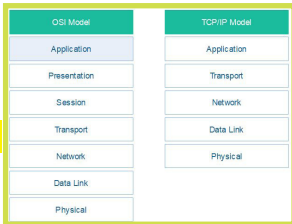
ساختار اینترنت اشیاء با توجه به مدل TCP/IP، از لایه‌های فیزیکی، لینک، شبکه، انتقال و برنامه کاربردی تشکیل شده است. هر لایه خصوصیات خاص خود را دارد به عنوان مثال لایه فیزیکی که در پایین-ترین سطح قرار دارد، اطلاعات را به صورت لحظه‌ای جمع‌آوری و پردازش می‌کند و آن ها را به لایه لینک، جهت ارسال به لایه های بالاتر می سپارد. لایه بعدی لایه شبکه است که وظیفه فراهم کردن امکانات شبکه‌ای مورد نیاز برای IoT را دارد. این لایه باید بتواند حجم بالای داده‌های اینترنت اشیا را که توسط حسگرهای بی-سیم و دستگاه‌های هوشمند تولید می‌شوند را پشتیبانی کند. در شکل ۳ مقایسه لایههای بین مدل OSI با مدل TCP/IP نشان داده شده است.

بسیاری از دستگاه های IoT بسیار کوچک و ارزان هستند که می‌توان آن ها را در هر کجا که ممکن است مورد استفاده قرار داد و منجر به یک مجموعه کامل از برنامه های کاربردی انقلابی، در استفاده از فن‌آوری ICT در زمینه های مختلف زندگی می‌شود. با این وجود، ارتباطات شبکه‌های IoT، خطرناک است زیرا سیستم ها مورد تهاجم حملات مخرب میشوند. به عنوان مثال می توان حملات DoS را نام برد که مانع ارتباط دستگاه های IoT با ایستگاه های پایه می شود. بنابراین، مسائل امنیتی باید برای مهندسی و استقرار شبکه های IoT مورد توجه قرار گیرد.

شکل ۱: نمونه‌هایی از اینترنت اشیاء در اطراف ما



شکل ۲ : مقایسه میزان استفاده مردم از کاربردهای اینترنت اشیاء



شکل۳ : مقایسه لایه های بین مدل OSI با مدل TCP/IP

در ادامه ضمن برشمردن چالش های امنیتي در شبکه IoT و انواع حملات رایج در این شبکه، به روش های پیشنهادی برای امنیت اینترنت اشیاء نیز پرداخته مي شود.

چالش های IoT

اینترنت اشیاء در هنگام پیاده سازی مکانیسم های امنیتی، با توجه به خصوصیات و ویژگی های منحصر به فردی که دارد با چالش‌ها و مشکلات زیر روبه رو می شود:

* تکنولوژی های چندگانه: اینترنت اشیاء ترکیبی از فن آوری های متعددی چون شناسایی فرکانس رادیویی(RFID)، شبکه های حسگر بی سیم، محاسبات ابری و مجازی سازی است. هر یک از این فن آوری ها آسیب پذیری های خاص خود را دارند، مشکل اینترنت اشیاء این است که باید زنجیره‌ای از تمام این تکنولوژی ها را ایمن نگه دارد.

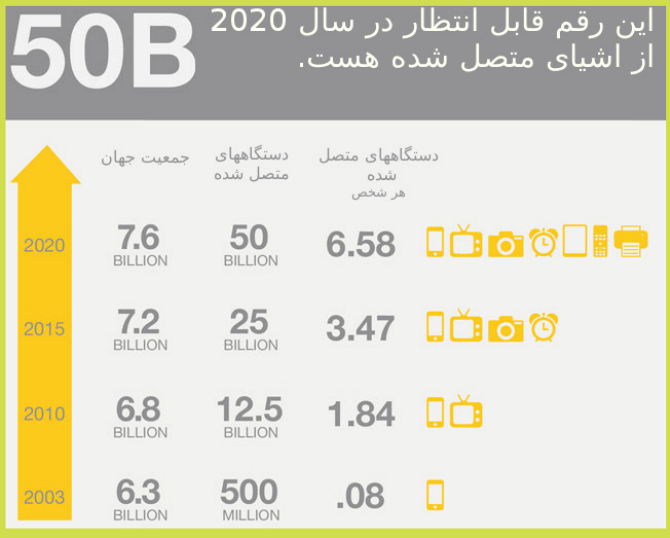
• کاربردهای چندگانه: همانطور که اشاره شد، اینترنت اشیاء کاربرد های متعددی از جمله سلامت، خانه‌های هوشمند، صنعت و غیره را دارد. مشکلی که در این‌جا وجود دارد این است که امنیت هر بخش از بخش های دیگر کاملاً مجزا بوده و مکانیزم های خاص خودش را می طلبد.

• مقیاس‌پذیری: طبق گفته سیسکو، تعداد دستگاه های متصل‌شده به اینترنت تا سال ۲۰۲۰ را نزدیک به ۵۰ میلیارد دستگاه تخمین زده است. این تعداد زیاد دستگاه متصل‌شده به اینترنت باعث می‌شود مقیاس پذیری مسئله مهمی در ایجاد مسائل امنیتی باشد، چرا که کارکرد و اعمال امنیت با اضافه‌شدن حجم وسیعی از این دستگاه ها که حاصل از افزایش درخواست های افراد و سازمان ها است، پیچیده تر شود. در شکل ۴ این موارد با جزئیات نشان داده شده است.

• داده‌های حجیم: با افزایش تعداد دستگاه های IoT، جریان های عظیمی از اطلاعات در طول زمان تولید می شوند که این امر باعث می شود مکانیزم های کارآمد و موثرتری برای امنیت این حجم بزرگ داده های تولید شده، ایجاد شود.

• دسترسی: فراهم ساختن دسترسی به سرویس ها و دستگاه ها در هر مکان و هر زمان برای مشتری‌ها به طور مداوم برای مدت زمان مطلوب یکی از چالش های IoT محسوب می شود چرا که با خاموش شدن و یا از دسترس خارج شدن دستگاه ها به هر دلیلی، عملکرد امنیتی سیستم ها مختل می شود. پس یکی از ملزومات امنیت IoT، در دسترس بودن همیشگی این شبکه ها است.

• محدودیت منابع: به دلیل وجود محدودیت منابع در اکثر دستگاه های IoT مانند CPU، توان مصرفی، پردازش، حافظه و غیره امکان پیاده‌سازی الگوریتم های قوی



شکل۴ : تعداد دستگاه‌های متصل‌شده به اینترنت در سال‌های مختلف و مشاهده روند رو به رشد آن

رمزنگاری به دلیل بالا بودن بار محاسباتی و همچنین استفاده از پروتکل های موجود در اینترنت سنتی وجود ندارد. از این رو باید از پروتکل های سبک تر که توان مصرفی کمتری نیاز دارند، برای هر لایه استفاده شود. در کنار مشکلات اشاره شده، با وجود این چالش احتمال وقوع حملات DoS نیز بیشتر می شود و مهاجم به راحتی می تواند منابع محدود این دستگاه ها را مصرف کرده و باعث اختلال در سرویس شود. با توجه به این موارد، طرح های امنیتی مطرح‌شده در اینترنت اشیا باید در کنار دارا بودن حداکثر عملکرد امنیتی، دارای حداقل منابع مصرفی باشد.

• مکان های دور از دسترس: برخی از دستگاه های IoT با توجه به کاربردی که خواهند داشت ممکن است در مکان های دور از دسترس یا مکان هایی که دسترسی به آن ها دشوار باشند نصب شوند. به همین دلیل به روز رسانی، تعمیر و نگهداری دستگاه هایی که به‌صورت روزمره در حال فعالیت هستند بسیار مهم است چرا که با این روش تا حدودی می‌توان از دسترسی و کنترل شبکه توسط مهاجمان جلوگیری کرد.

• تحرک: انتظار می رود تعدادی از دستگاه های IoT بر حسب وظیفه ای که دارند متحرک باشند و مرتباً تغییر مکان دهند، که یکی دیگر از چالش های امنیتی را ایجاد می کند.

حملات رایج در IoT

با توجه به چالش های اشاره شده در معماری شبکه های بي سیم از قبیل کانال های مخابراتي ناامن و غیرقابل اطمینان، شبکه های IoT در مقابل نفوذ و حملات امنیتي آسیب پذیر هستند. بنابراین با توجه به تهدیدات موجود در این شبکه ها سطح گوناگوني از حملات وجود دارد که این حملات را مي‌توان بر اساس لایه هایي که در آن‌ها قرار دارند و یا بر اساس الگو حملات تقسیم بندی کرد.

گروهی از حملات تحت عنوان حملات سایبری شناخته می شوند. حملات سایبری به دسته حملاتی گفته می شود که هکرها با استفاده از آن، در تلاش برای آسیب رساندن یا نابود کردن یک شبکه کامپیوتری یا سیستم هستند. تعدادی از این حملات شامل:

• **بات نت:** در میان انواع متعددی از نرم افزارهای مخرب، بات نت ها از گسترده ترین و جدی ترین تهدیدات امنیتی محسوب می‌شوند که امروزه به طور معمول برای ایجاد حملات سایبری استفاده می-شوند. بات‌نت‌ها شامل مجموعه دستگاه های مختلف متصل به یکدیگر مانند کامپیوترها، موبایل‌ها، تبلت ها و دستگاه های هوشمند است که دو ویژگی اصلی مشترک یعنی قابل اتصال بودن به اینترنت و قابلیت انتقال اطلاعات به صورت خودکار از طریق شبکه را دارا هستند و هدف آن ها ارسال هزاران درخواست به یک هدف به منظور سقوط شبکه یا سرور مورد نظر است. از بات نت ها برای مقاصد خرابکارانه ای چون حملات زیر استفاده می شوند:

- DDoS
- Spamming
- Sniffing Traffic
- Key logging
- Spreading new malware
- Mass identify theft

• **مفهوم MITM:** مرد میانی به گونه ای از حملات گفته می شود که مهاجم یا هکر به دنبال نفوذ و قطع ارتباط بین دو سیستم جداگانه است. این حمله می تواند خطرناک باشد؛ زیرا مهاجم می تواند به طور مخفیانه پیام های بین دو طرف را متوقف کند، تغییر دهد و آن‌ها را انتقال دهد، در حالی که دو طرف ارتباط از وجود شخص سوم بی‌خبر هستند.

• **اطلاعات و سرقت هویت:** استراتژی اصلی سرقت هویت، جمع آوری اطلاعات جهت دسترسی به اطلاعات شخصی و مهم افراد است که تاکنون انواع نفوذ های چشمگیر و مهمی با همین استراتژی صورت گرفته است. پس نگهداری دستگاه های متصل به اینترنت (مانند تلفن همراه، iPad، Kindle، smartwatch و غیره) از الزامات امنیتی جهت جلوگیری از این حملات به‌شمار می رود.

• **مهندسی اجتماعی:** مهندسی اجتماعی به دسته ای از حملات گفته می شود که اقدام به سوءاستفاده و فریب افراد به منظور دست یابی به اطلاعات محرمانه صورت می گیرد و نوع اطلاعاتی که مجرمان در جستجوی آن هستند می تواند با توجه به افراد هدف مورد نظر متفاوت باشند. به طور معمول، هک‌های مهندسی اجتماعی در قالب ایمیل های فیشینگ انجام می شود که به دنبال آن هستند که قربانی اطلاعات خود را افشاکرده یا به محض وارد کردن اطلاعات بانکی در سایت‌های خرید که باید امن باشند به اطلاعات مهم و شخصی قربانی دسترسی پیدا می کنند.

• **DoS:** حملات DoS یا منع سرویس به حملاتی اشاره دارد که هدف آن ها از کار انداختن سرور یا شبکه است. دلایل زیادی برای عدم دسترسی وجود دارد اما معمولاً به زیرساخت‌هایی اشاره می کند که نمی توانند به دلیل اضافه بار و زیاد بودن درخواست های ارسالی پاسخگو باشند. DDoS یک حمله منع سرویس توزیع شده است که در آن تعداد زیادی از سیستم های مخرب به یک هدف مشخص به صورت همزمان درخواست سرویس دهی دارند. این حملات اغلب از طریق دستگاه های برنامه ریزی شده چون بات نت انجام می شود.

رایج ترین تقسیم بندی حملات، تقسیم بندی براساس پشته پروتکل یا قرارگیری در لایه های IoT است که در جدول ۱ نشان داده شده‌اند.

گروهی دیگر از محققان حملات موجود در IoT را برحسب نوع حمله به چهار دسته مجزای زیر تقسیم‌بندی کردند:

۱) حملات فیزیکی: به دسته حملاتی گفته می شود که بر اجزای سخت‌افزاری سیستم IoT متمرکز شده و نیازمند آن است که به صورت فیزیکی نزدیک یا درون سیستم IoT باشد. به علاوه، حملاتی که به طول عمر یا قابلیت سخت‌افزار آسیب می‌رسانند نیز در این دسته گنجانده شده‌اند.

۲) حملات شبکه: این حملات در شبکه سیستم IoT متمرکز شده و مهاجم لزوماً برای حمله نیاز به نزدیک شدن به شبکه را ندارد.

۳) حملات نرم افزار: حملات نرم‌افزاری منبع اصلی آسیب‌پذیری های امنیتی در هر سیستم کامپیوتری هستند که از برنامه هایی چون تروجان، کرم ها، ویروس ها، نرم افزارهای جاسوسی و اسکریپت های مخرب بهره می گیرند و می توانند اطلاعات را سرقت یا دستکاری کنند و یا حتی به دستگاه‌های IoT آسیب برسانند.

۴) حملات رمزنگاری: این حملات صرفاً بر پایه شکستن طرح رمزنگاری در سیستم IoT استوار است و در مجموع، حملات مرتبط با هر بخش در جدول ۲ خلاصه می‌شود.

امنیت IoT

سیستم IoT امن شده، سیستمی است که در آن اطلاعات مبادله شده توسط شخص ثالث قابل تغییر نباشد (Integrity). این اطلاعات فقط برای افراد مشخص شده در دو طرف ارتباط قابل فهم باشد (confidentiality). مطمئن باشید که نهادهای درگیر

ارتباط خودشان باشند و شخص دیگری آن را جعل نکرده باشد (Authentication) و سیستم قطع نشده باشد، چرا که ممکن است توسط حملات DoS سیستم از کار افتاده باشد (Availability) و نهادهای دارای مجوز فقط اجازه انجام عملیات را داشته باشند (Authorization) و به منظور جلوگیری از حملات Reply attack، تازه و جدید بودن اطلاعات بررسی شود(Freshness).

طبق نتایج جمع‌آوری شده در نظرسنجی الکترونیکی در رابطه با اینترنت اشیاء در نوامبر و سپتامبر ۲۰۱۳ توسط SANS، موارد زیر حاصل شد:

• در رابطه با نظر افراد در مورد اینترنت اشیاء و امنیت آن، نزدیک به نیمی از پاسخ‌ها حاکی آن است که IoT تقریباً همان سطح موارد امنیتی را دارد که تکنولوژی‌های قبلی داشته‌اند. نتایج سایر پاسخ‌ها را در شکل ۵ می‌توان مشاهده کرد.

• بزرگترین تهدید با اکتساب درصد ۳۱ برای اینترنت اشیاء را مربوط به مدیریت پچ دانستند که به دلیل دشوار بودن در پچ کردن آن‌ها، این اشیاء به‌صورت آسیب‌پذیر رها می‌شوند. بیشترین تهدیدات دیگر به ترتیب مربوط به بدافزارها، حملات DoS، خرابکاری و تخریب اشیاء متصل شده و تنها ۱۰ درصد از بزرگترین خطاها مربوط به خطای کاربر است و موارد دیگر به صورت دقیق‌تر در شکل ۶ نشان داده شده‌اند.

• هنگامی که در مورد چگونگی استفاده از کنترل‌های امنیتی سوال شد، چهار دسته برتر مشاهده می‌شوند که شامل احراز هویت ، نظارت بر سیستم، رمزنگاری ارتباطات و ارزیابی امنیتی و تست اشیاء جدید قبل از تولید است.

امنیت لایه های IoT

با توجه به محدودیت ها و چالش های اینترنت اشیاء (محدودیت حافظه، باتری و غیره)، امکان پیاده‌سازی مکانیسم های امنیتی موجود در اینترنت از قبیل استفاده از رمزنگاری های پیشرفته ای چون RSA و همچنین استفاده از همان پروتکل های امنیتی اینترنت سنتی، امکان پذیر نیست. به همین دلیل اولین قدم برای رسیدن به امنیت ارتباطات IoT، امن کردن لایه های پنج گانه با استفاده از پروتکل های سبک و سازگار با IoT است.

IEEE ۸۰۲٫۱۵٫۴ پروتکل امنیتی سبک معرفی شده به جای IEEE ۸۰۲٫۱۱، برای لایه فیزیکی IoT و مناسب برای محیط های ارتباطی بی سیم کم انرژی مانند شبکه های حسگر بی سیم و IoT بوده که توانایی ارسال بسته ها در ۱۶ کانال ۲/۴ گیگاهرتزی با حداقل احتمال خطا را داراست. جهت امنیت لایه لینک، لایه دوم IoT، از پروتکل IEEE ۸۰۲٫۱۵٫۴ MAC استفاده می شود که رمزنگاری اطلاعات و یکپارچگی را فراهم می کند. پروتکل رایج معرفی شده برای لایه شبکه ۶LowPAN است که همان پروتکل IPv۶ بوده که برای شبکه های موجود در محیط های با توان پایین طراحی شده است و در کنار این پروتکل، یک پروتکل مسیریاب نیز در لایه شبکه وجود دارد که از الگوریتم RPL پیروی می کند که حملات مسیریابی مانند سینکهول را شناسایی می‌کند. TLS پروتکل نام آشنای لایه ترانسپورت است که برای رسیدن به امنیت(End-to-End (E2E، به وجود پروتکل‌های TLS یا SSL نیاز است اما با توجه به چالش های IoT به دلیل داشتن دست‌دهی دوطرفه قابل استفاده نیستند. در همین راستا جهت کاهش بار محاسباتی و سازگار بودن با شبکه‌های ۶LowPAN از UDP که ورژن سبک تری از TCP است استفاده‌کردند که بعداً DTLS نامیده شد. مورد دیگر، استفاده از پروتکل لایه اپلیکیشن یعنی CoAP است. در واقع از DTLS نیز می‌توان به عنوان استانداردی برای امن کردن

جدول ۱: تقسیم بندی حملات بر اساس لایه های IoT

Physical Layer	Data link Layer	Network Layer	Transport Layer	Application Layer
Jamming	Exhaustive channel access	Interruption, Interception and Replay attacks	Flooding attack	Reprogram attack
Tampering	Collison	Modification and Fabrication Modification attack	Desynchronization attack	Overwhelm attack
	Interrogation attack	Sinkhole attack		
		Selective forwarding attack		
		Sybil Attack		
		Hello flood attack		
		Wormhole attack		

جدول ۲: تقسیم بندی حملات بر اساس نوع حمله

Encryption Attacks	Saftware Attacks	Network Attacks	Physical Attacks
Side Channel	Virus and Worm	Traffic Analysis	Node Tampering
		RFID Spoofing	RF Interference
Ciphertext only Attack	Spyware and Adware	RFID cloning	Malicious Node Injection
		Man In The Middle	
Known Plaintext Attack	Trojan Horse	RFID Unauthorised Access	Node jamming
Chosen Plaintext Attack	Maliciouse scripts	Routing Information	Physical Damage
Man In The Middle	Denial of Service	Sybil	Sleep Deprivation Attack
		Denial of Service	Social Engineering
		Sinkhole	Malicious Code Injection on the Node

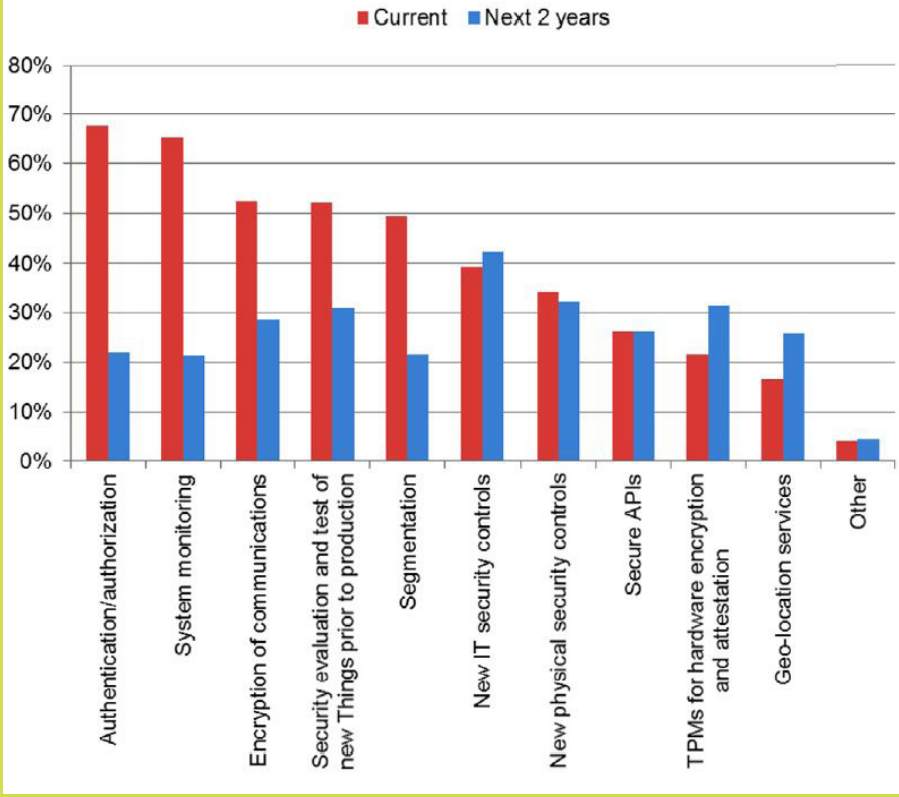
CoAP استفاده‌کرد. در شکل ۷ مقایسه‌ای بین پروتکل های پشته IoT و Web انجام گرفته است.

سیستم های تشخیص نفوذ

با وجود امنکردن تک تک لایه‌هایIoT ، با استفاده از پروتکل های معرفی شده، ممکن است تعدادی از حملات توسط این روش قابل مقابله نباشند به همین دلیل اقدام به پیاده سازی سیستم های تشخیص نفوذ در کنار این پروتکل ها شد. سیستم‌های تشخیص نفوذ (IDS) به ابزار یا مکانیسمهایی گفته می شود که حملات وارده بر یک سیستم یا یک شبکه را به وسیله آنالیزکردن رفتار دستگاه ها یا سنسورها تشخیص می‌دهند. این آنالیزکردن در قالب تشخیص بر اساس امضا، تشخیص بر اساس آنومالی و هیبرید صورت می‌گیرد.

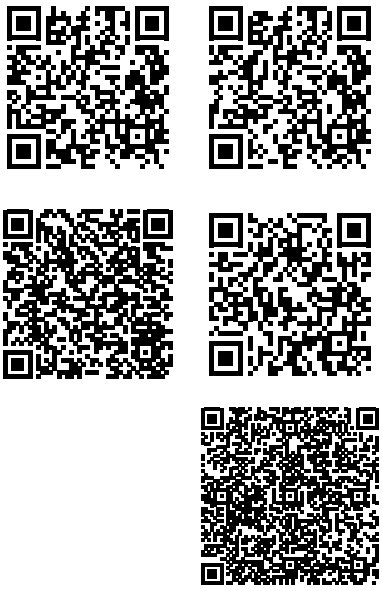
تاکنون IDS های مختلف با روش ها و ویژگی های گوناگونی پیشنهاد شده اند از جمله SVELTE را می‌توان نام برد که از RPL به عنوان پروتکل مسیریابی جهت تشخیص حملات سینکهول استفاده می کند و همچنین InDReS که با شمارش تعداد بسته های از دست رفته و مشاهده چگونگی کنترل بسته ها در شبکه، گره های مخرب را تشخیص می دهد.

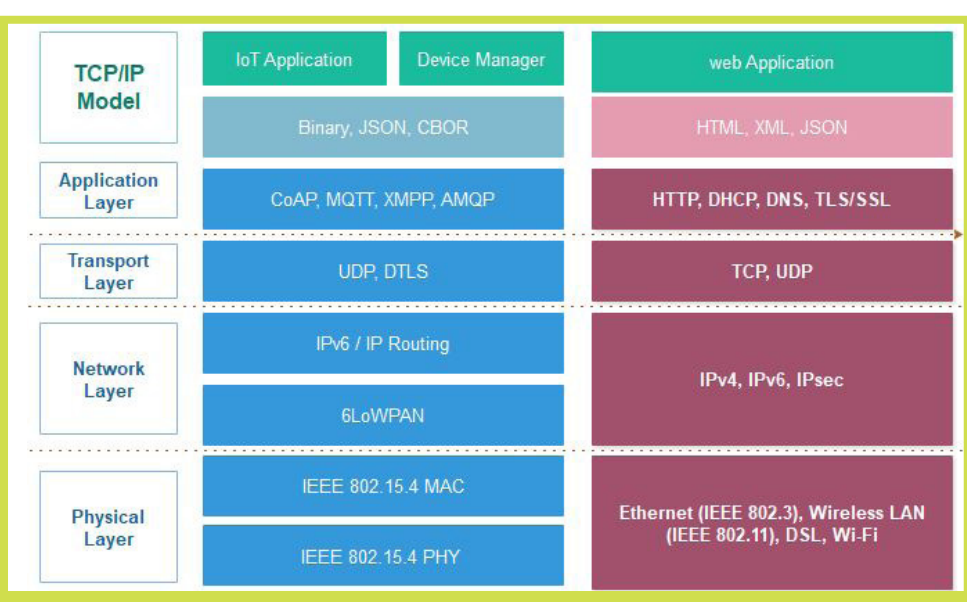
شکل ۵: مقایسه نظر افراد در مورد امنیت اینترنت اشیاء



شکل ۶: درصد استفاده پاسخ‌دهندگان به استفاده از هر روش امنیتی، و مقایسه روش های کنترل امنیتی

منابع:





شکل ۷: مقایسه بین پروتکل های پشته IoT و Web

بررسی تخصصی پروتکل SSL و تفاوت‌های گواهی‌نامه‌های آن

■ اسرین عبدالهی- هادی گلباغی

مقدمه

به همان اندازه که تعداد برنامه‌های مبتنی بر پایگاه داده در بازار سیستم‌ها درحال افزایش است، امنیت اطلاعات ذخیره شده نیز افزایش می‌یابد. پایگاه داده‌هایی چون SQL Server، Oracle و Access برای ایجاد سیستم‌های هوشمندتر و پیچیده‌تر مورد استفاده قرار می‌گیرند. همان‌طور که سیستم‌ها به سرعت درحال توسعه هستند، کاربران مخرب و غیرمجاز نیز راه‌هایی جهت دسترسی و نفوذ به این سیستم‌ها و دسترسی به اطلاعات حساس مورد نظر خود پیدا می‌کنند، چرا که سیستم‌های تازه توسعه‌یافته در مقایسه با سیستم‌های قبلی پیچیده‌تر شده و حاوی اطلاعات بسیار حساس هستند و این در حالی است که با سیستم‌های دیگر نیز در ارتباط هستند. پس برای امنیت این اطلاعات، نیازمند ارتباطات و اتصالات امن و مطمئن هستیم.

برقراری یک ارتباط محافظت نشده بسیار آسان است اما برای ایجاد امنیت، نیازمند ارتباط رمزگذاری شده و استفاده از پروتکل‌های رمزنگاری چون SSL و یا TLS هستیم، با این وجود پیاده‌سازی و پیکربندی صحیح آن‌ها کار آسانی نیست. با به‌کارگیری روش‌های امنیتی می‌توان تا حد زیادی امنیت ارتباطات را تامین کرد. برای بررسی این موارد پاسخگویی به سوالات زیر ضروری به نظر می‌رسد.

SSL و TLS چیست؟ آیا برای ایجاد امنیت نیازمند دریافت گواهی تصدیق و دانستن تفاوت بین SSL و TLS هستیم؟ هر کدام از گواهی‌های تصدیق دیجیتال جهت ایجاد امنیت استفاده می‌شوند اما این گواهی‌ها به چه صورت استفاده می‌شوند و چه تفاوت‌هایی دارند؟

در ادامه توضیحاتی را در این خصوص ارائه می‌دهیم تا سوالاتی را که در این حوزه مطرح می‌شوند را پاسخ دهیم. برای شروع نگاهی به HTTP و HTTPS که در بخش آدرس مرورگر نشان داده شده‌اند خواهیم داشت.

۱- HTTP و HTTPS برای انتقال اطلاعات

زمانی‌که یک بازدیدکننده اطلاعاتی را در یک وب‌سایت خوانده یا کلیک می‌کند، اطلاعات در بین سرور که میزبان سایت است و سیستم شخص رد و بدل می‌شوند. این فرآیند توسط یک پروتکل انتقال داده به نام HTTP (Hypertext Transfer Protocol)صورت گرفته و مدیریت می‌شود.

پروتکل HTTP یک افزونه به نام HTTPS (Hypertext Transfer Protocol Secure) دارد. این نسخه امن، انتقال اطلاعات مابین کاربر و سرور را به صورت رمزگذاری شده انجام می‌دهد به این معنی که اطلاعات مبادله شده بین سرور و کاربر فقط برای خود آن‌ها در دسترس خواهد بود و نه شخص سوم. داده‌های ارسال شده از سوی کاربر به سمت سرور با استفاده از پروتکل رمزنگاری، رمزگذاری می‌شوند. اولین پروتکل استفاده شده برای این هدف SSL (Secure Sockets Layer) است. چندین نسخه از پروتکل SSL موجود است که همه آن‌ها در برخی مواقع دارای مشکلات امنیتی هستند. امروزه نسخه اصلاح‌شده آن با نام تجاری(TLS(Transport Layer Security شناخته می‌شود که مورد استفاده است. با این حال نسخه اولیه این پروتکل SSL است و هنوز هم نسخه جدید از این پروتکل با نام قدیمی آن یعنی SSL خوانده می‌شود.

برای استفاده از رمزگذاری، یک سایت باید دارای گواهی تصدیق باشد که یک امضای دیجیتال نامیده می‌شود که شامل تایید مکانیزم رمزگذاری قابل اعتماد و مطابق با پروتکل بوده است. علاوه بر اینکه یک حرف S در HTTPS اضافه شده است که نشانگر یک قفل سبز کوچک (یا محافظ در برخی مرورگرها) با کلمه Secure یا نام شرکت در نوار آدرس مرورگر نشان داده شده است که در شکل بالا نیز این مورد نشان داده شده است. به هر صورت در بالای پنجره مرورگر می‌توان نشانی را از استفاده از آن پیدا کرد که از HTTPS بهره می‌برند و اخیراً رویه به این منوال شده است که نشانگری به نام Not Secure نیز برای عدم استفاده از این پروتکل در مرورگرها به صورت پیش‌فرض تعبیه شده است.

۲- پروتکل SSL

SSL به عنوان یک پروتکل امن انتخاب شده برای بخش بزرگی از جامعه اینترنت است و به عنوان یک مکانیسم، جهت ایجاد یک حریم خصوصی و قابل اطمینان بین دو اپلیکیشن ارتباطی معرفی شده است. اپلیکیشن‌های زیادی وجود دارند که با استفاده از پروتکل SSL می‌توانند هرگونه اطلاعات بر روی TCP را به صورت امن منتقل کنند. استفاده از HTTP یا HTTPS امن از اپلیکیشن‌های نام آشنا از SSL در تجارت الکترونیک است. این پروتکل هر سه ضلع مثلث امنیتی، یعنی حریم خصوصی (با استفاده از ارتباط رمزنگاری‌شده)، احراز هویت (شناسایی کاربر مقابل با استفاده از گواهی‌ها) و قابلیت اطمینان بودن (نگهداری قابل اعتماد یک ارتباط امن از طریق بررسی یکپارچگی پیام) را فراهم می‌کند.

امروزه نیاز به ارسال اطلاعات حساس چون اطلاعات کارت بانکی به یک سرویس‌دهنده وب فروشگاه‌های آنلاین در حال افزایش است به همین دلیل برای امن کردن چنین ارتباطی نیاز به استفاده از پروتکل SSL است. پروتکل SSL در بسیاری از مرورگرهای وب یکپارچه شده است و این مرورگرها به طور معمول برای دسترسی به اپلیکیشن‌های وب استفاده می‌شوند. برای اعمال SSL از جانب مشتری هیچ‌گونه پیکربندی‌ای لازم نیست و باید از جانب سرور پیکربندی انجام شود.

SSL چگونه کار می‌کند

پروتکل SSL با استفاده از چهار مکانیزم تمام ارتباطات بین مشتری و سرور را در قالب ارتباط امن کپسول شده ارائه می‌دهد که در ادامه توضیح داده خواهند شد.

- لایه record

این لایه پیام‌های پروتکل، ChangeCipherSpec، Alert، Handshake و Application را قالب‌بندی می‌کند. در

این قالب‌بندی برای هر پیام یک هدر و یک Hash فراهم می‌کند. این هدر ۵ بایتی است که ۱ بایت آن مربوط به تعریف پروتکل، دو بایت مربوط به نسخه پروتکل و ۲ بایت دیگر طول آن را تشکیل می‌دهد. باید توجه داشت که طول پیام‌هایی که هدر را دنبال می‌کنند نباید بیشتر از ۱۶/۳۸۴ بایت باشند.

• پروتکل ChangeCipherSpec

این لایه از یک پیام تشکیل شده که شروع ارتباطات امن بین سرویس گیرنده و سرور را نشان می دهد. با وجود آنکه پروتکل ChangeCipherSpec از فرمت لایه Record استفاده می‌کند، اما پیام واقعی ChangeCipherSpec، فقط یک بایت طول دارد و تغییر در پروتکل‌های ارتباطی را با داشتن مقدار "۱" نشان می‌دهد.

• پروتکل Alert

این پروتکل وظیفه ارسال خطاها، مشکلات یا اخطارها را بین دو طرف بر عهده دارد. این لایه از دو فیلد Severity Level و نوع Alert تشکیل شده است. Severity level مقادیر "۱" و "۲" را ارسال می‌کند که مقدار "۱" نشان دهنده پیام هشدار است و به دو طرف ارتباط توصیه می‌کند که ارتباط خود را قطع کرده و مجدداً با استفاده از یک Handshake یک ارتباط جدید برقرار کنند. مقدار "۲" یک پیام هشدار وخیم است و نیازمند قطع ارتباط سریع توسط دو طرف ارتباط است. اما نوع Alert نشان‌دهنده خطا خاصی است که منجر به ارسال پیام خطا توسط آن بخش می‌شود. این فیلد از یک بایت تشکیل شده است و می‌تواند انواع مختلفی از اخطار (شکست Handshake، نبود گواهی‌نامه، RecordMac ناصحیح و غیره) را نشان دهد.

• پروتکل Handshake

لازم است قبل از ارسال پیام‌ها بین مشتری و سرور، جهت امن‌کردن ارتباطات یک دست‌دهی SSL صورت گیرد که در شکل ۲ نیز روال آن نشان داده شده است. این روش به‌صورت زیر است:

Client Hello

مشتری از یک وب سرویس درخواست برقراری ارتباط امن را دارد، به همین دلیل پیامی حاوی نسخه SSL استفاده شده، CipherSuites پشتیبانی شده و روش‌های فشرده‌سازی استفاده شده توسط مشتری را به سرور ارسال می‌کند. سایر اطلاعات موجود در این پیام شامل یک عدد تصادفی ۳۲ بایتی است که به مشتری در ایجاد ارتباطات رمزنگاری شده کمک می‌کند. در این قسمت بخش SessionID خالی می‌ماند.

ServerHello

در این پیام، سرور انتخابش را با توجه به پیام ClientHello انجام می‌دهد. سرور در پاسخ، همانند مشتری پنج فیلد را به مشتری ارسال می‌کند اما این بار فیلد SessionID را پر می‌کند. سرور با توجه درخواست ClientHello تصمیم می‌گیرد که چه رمزنگاری، چه روش فشرده‌سازی و CipherSuite را استفاده کند. در این بخش برچسب زمان و تاریخ جایگزین فیلد عدد تصادفی شده تا از مقادیر تصادفی تکراری اجتناب شود. سایر بایت‌های باقی مانده باید توسط مولد امن عدد تصادفی به صورت رمزنگاری ایجاد شوند.

تبادل ServerKey

اکنون سرور برای ارسال اطلاعات تصمیم می‌گیرد که اطلاعات چگونه رمزگذاری شوند. پس سرور گواهی دیجیتالی خود را به همراه کلید عمومی خود به مشتری می‌فرستد. گواهی دیجیتال در واقع به مشتری اطمینان می‌دهد که طرف ارتباط واقعاً خود سرور مورد نظر است.

ServerHelloDone

هنگامی که سرور پیام ServerKeyExchange را تکمیل کند، مشتری یک پیام ServerHelloDone را نیز دریافت می‌کند که نوعی تایید برای پیام فرستاده شده از جانب مشتری و دریافت و تکمیل آن پیام توسط سرور است.

ClientKeyExchange

در این بخش مشتری با بررسی گواهی دریافتی از سرور و اطمینان از اینکه طرف ارتباط سرور است، اطلاعات مربوط به کلیدی که سرور و مشتری می‌خواهند برای رمزنگاری اطلاعات از آن به طور مشترک استفاده کنند را با کلید عمومی سرور رمزنگاری کرده و برای سرور ارسال می‌کند. همان‌طور که مشاهده می‌کنیم SSL از کلیدهای عمومی و خصوصی مشتری استفاده نمی‌کند، با این روش احتمال حمله مرد میانی تا حد زیادی کاهش پیدا می‌کند چرا که مرد میانی کلید خصوصی سرور را جهت مشاهده کلید مشترک استفاده شده ندارد.

ChangeCipherSpec

از دو بخش سرور و مشتری تشکیل شده است و نشان می‌دهد که مشتری و سرور برای برقراری ارتباط امن آماده هستند.

۳- پروتکل TLS

پروتکل لایه ترانسپورت یا همان TLS در ژانویه سال ۱۹۹۹ به عنوان استانداردی برای ایجاد ارتباطات محافظت شده، ایجاد شد. این پروتکل به اپلیکیشن‌های سرور یا مشتری اجازه می‌دهد که در مسیری با یکدیگر ارتباط برقرار کنند که در مقابل حملات شنود و جعل پیام، ایمن باشد. اهداف این پروتکل امنیتی شامل رمزنگاری، توسعه‌پذیری و کارایی نسبی است که این اهداف از طریق پیاده‌سازی پروتکل TLS در دو مرحله زیر صورت می‌گیرد:

• پروتکل TLS Record

این پروتکل برای ایجاد یک ارتباط قابل‌اطمینان و محافظت شده بین سرور و مشتری توافق می‌کند. هرچند که می‌توان از این پروتکل در حالت بدون رمزنگاری استفاده کرد، اما برای اطمینان از یک ارتباط محافظت شده از رمزنگاری متقارن و توابع هش تولید شده به‌وسیله کد احراز هویت پیام استفاده می‌شود.

• پروتکل TLS Handshake

مشابه Handshake اشاره شده در بخش SSL است. که با وجود این پروتکل می‌توان یک ارتباط امن را بین سرور و مشتری ایجاد کرد. این پروتکل به طرفین ارتباط اجازه می‌دهد که با یک زبان مشابه صحبت کنند به عبارت دیگر آن‌ها در مورد الگوریتم رمزنگاری مورد استفاده و کلیدهای رمزنگاری توافق می‌کنند و پشته پروتکل TLS در شکل ۳ نشان داده شده است.

۴- تفاوت اصلی TLS با SSL

تفاوت‌های متعددی بین SSL و TLS وجود دارند که می‌توان آن‌ها را در هفت تفاوت اصلی به صورت زیر خلاصه کرد:

• نسخه پروتکل در پیام

نسخه مورد استفاده برای SSL مقدار ۳/۰ وبرای TLS عدد ۱/۰ است که از جهات مختلفی این دو نسخه یکی بوده، به عبارت دیگر TLS ۱٫۰ کامل کننده SSL ۳٫۰ است.

• نوع پیام پروتکل هشدار

انواع پیام‌های هشدار برای پروتکل TLS مجاز است اما در SSL گزینه "NoCertificate" از لیست SSL حذف شده است. پس چنین فرض می‌شود که اگر هیچ گواهی برای کاربر وجود نداشته باشد آنگاه نیازی به ارسال پیام جداگانه نیست.

• احراز هویت پیام

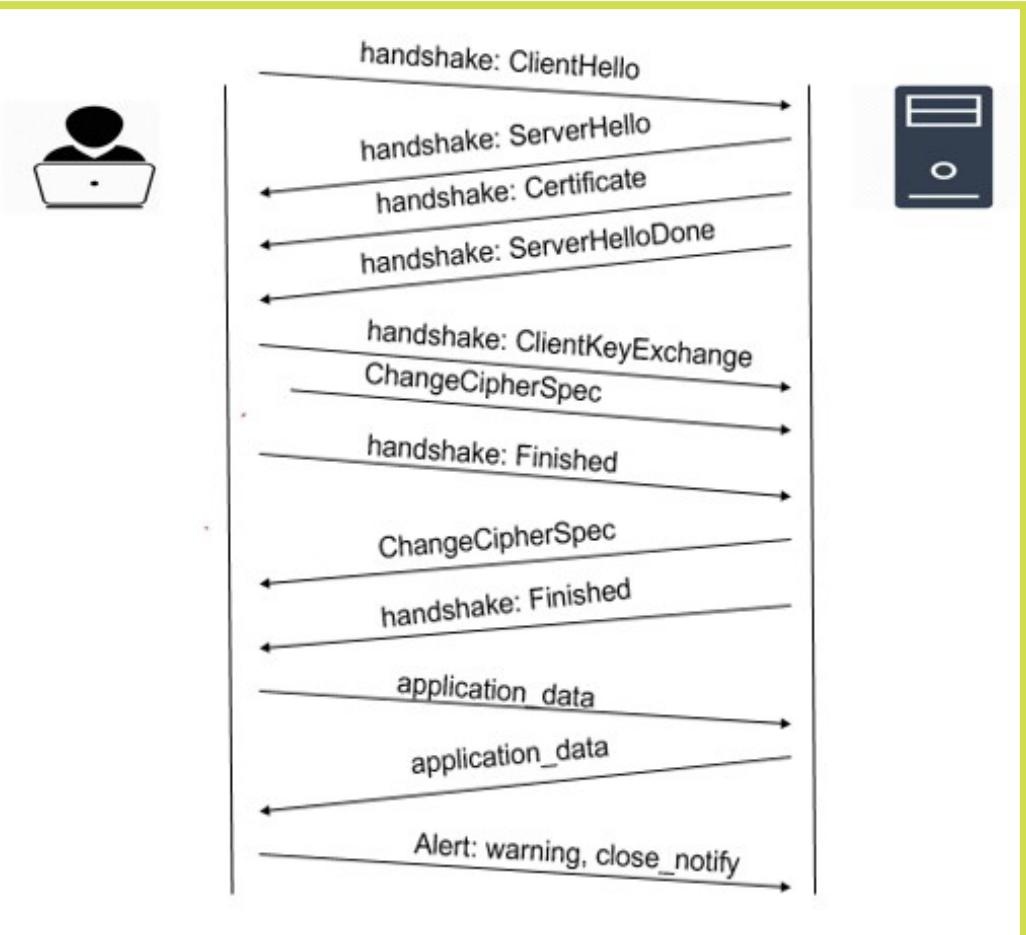
TLS از یک MAC استاندارد شده (H-MAC) استفاده می‌کند. مزیت این کار این است که برخلاف SSL که فقط با MD۵ یا SHA های معرفی شده عمل می‌کند، TLS با هرگونه تابع هش دیگری کار می‌کند.

• تایید گواهی‌نامه

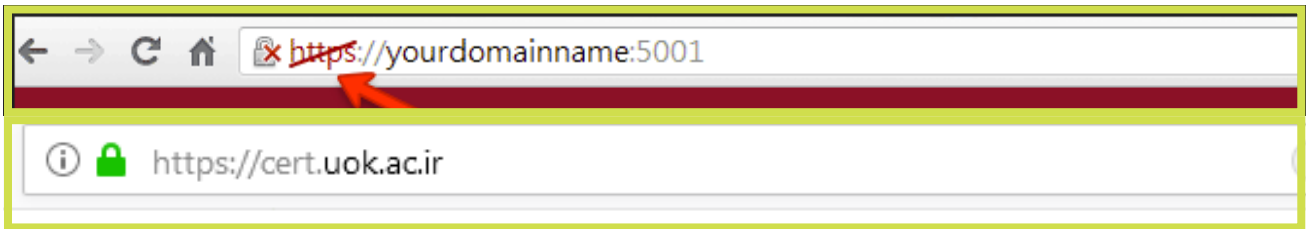
در SSL تایید گواهی کار آسانی نیست. با این حال، از پیش در TLS، اطلاعات تایید شده به صورت کامل در طول رد و بدل پیام‌های Handshake ارسال می‌شوند.

• تولید موارد کلیدی

TLS از استاندارد H-MAC و خروجی تابع شبه تصادفی (PRF) برای تولید موارد کلیدی استفاده



شکل ۲: Handshake واقعی به کار برده شده در SSL



شکل ۴: تفاوت بین یک سایت امن با سایت ناامن در انتقال اطلاعات

می‌کند. این در حالی است که SSL از خروجی RSA، Deffine-Hellman یا Fortezza/DMS استفاده می‌کند.

• Finished

در TLS برای ایجاد پیام Finished از خروجی PRF الگوریتم H-MAC همراه با master secret به صورت "Client finished" یا "server finished" استفاده می‌کند اما در SSL، به همان شیوه ad-hoc که مواد کلید تولید شده‌اند، ایجاد می‌شود.

• Cipher Suiteهای پایه

همانطور که قبلا اشاره شد، SSL به صورت خاص از Deffine-Hellman ، RSA و Fortezza/DMS استفاده می‌کند اما TLS استفاده از Fortezza/DMS را متوقف کرده است.

۵- چگونه یک سایت گواهی SSL دریافت می‌کند

دو راه برای دریافت این گواهی وجود دارد. یک وب مستر می‌تواند گواهی صادر کرده و امضا کند و کلیدهای رمزنگاری ایجاد کند. چنین گواهی‌هایی را گواهی self-signed گویند. هنگام دسترسی به یک سایت، کاربر هشدار گواهی نامعلوم را دریافت می‌کند. در چنین سایت‌هایی پنجره مرورگر یا یک قفل که خطی روی آن کشیده شده، یک سپر قرمز، کلمه Not Secure، حروف HTTPS قرمز رنگ به جای رنگ سبز و یا حروف HTTPS که در بخش آدرس مرورگر خط قرمزی بر روی حروف کشیده شده است، را نشان می‌دهد که توسط مرورگرهای مختلف و نسخه‌های متفاوت مرورگرها این نشانه‌ها متفاوت خواهد بود و در شکل ۴ این مورد نشان داده شده است.

راه‌حل بهتر برای دریافت گواهی خرید یک گواهی امضا شده توسط Certificate Authority(CA) معتبر است. CA ها اسناد مسئول سایت و حق مالکیت دامنه را بررسی می‌کنند سپس صدور یک گواهی، مشخص کننده یک شرکت مشروع ثبت شده در یک منطقه خاص است.

میزان خوش‌نامی و اعتبار CA ها تعیین کننده این است که چه میزان توسعه‌دهندگان مرورگرها به آن اعتماد دارند و سایت‌های دارای گواهی‌نامه خود را چگونه نمایش می‌دهند. قیمت گواهی بستگی به نوع و مدت اعتبار و همچنین میزان اعتبار CA نیز دارد.

انواع گواهی SSL

گواهی‌های امضا شده توسط CA ها در انواع مختلفی وجود دارند که میزان اعتبار، مدت، چگونگی دریافت و قیمت می‌تواند این انواع را از هم جدا کند. همان‌طور که گفته شد گواهی‌نامه SSL دارای انواع مختلفی است، که هر نوع آن تامین کننده نیاز خاصی می‌باشد و از اعتبار و قیمت متفاوتی برخوردار است و علاوه بر تامین امنیت می تواند اعتبار یک سازمان را نمایش دهد. به منظور انتخاب بهترین نوع گواهی‌نامه SSL و صرف مناسب‌ترین هزینه به منظور برآورده نمودن نیاز و کارایی مطلوب، لازم است ابتدا تعریفی از آن‌ها داشته باشیم. البته در بین مواردی که در ادامه توضیح خواهیم داد گواهی‌های Self-signed SSL را توضیح نمی‌دهیم به این دلیل که اعتبار خاصی ندارند.

گواهی‌نامه اعتبارسنجی دامنه

این نوع از گواهی‌نامه SSL که آنرا Domain Validation DV نیز می‌نامند مرجع صادرکننده گواهینامه بر اساس نام دامنه اعتبارسنجی را انجام می‌دهد و به بررسی صحت یا اعتبار سازمان یا صاحب دامنه نمی‌پردازد. به طور مثال از اطلاعات به دست آمده از WHOIS اغلب استفاده می‌کنند. همچنین مدت زمانی که برای دریافت گواهی لازم است بسیار کوتاه می‌باشد به این دلیل‌که صادرکنندگان به صورت آنلاین و در لحظه این گواهی را صادر می‌کنند. این گواهی بیشتر برای صاحبان وب‌سایت و اشخاص عادی یا به اصطلاح شخص حقیقی مناسب است که هدف از تهیه گواهی SSL برای آن‌ها صرفاً تغییر HTTP به HTTPS می‌باشد. از نکات مثبت این گواهی می‌توان به سرعت صدور و قیمت کمتر و از نکات منفی آن به اعتبار و امنیت کمتر اشاره کرد. چون‌که در این گواهی هیچ نامی از صاحب گواهی SSL یا سازمان مربوطه در بخش اصلاعات گواهی‌نامه در مرورگر به بازدید کننده نمایش داده نمی‌شود نمی‌توان آن را معتبر دانست.

گواهی‌نامه اعتبار سنجی سازمانی

این نوع گواهینامه SSL که آنرا با نامOV(Organization Validation)نیز می‌شناسند برای تایید اعتبار یک سازمان و یا شرکت استفاده شده و سطح اعتبار آن بسیار بالاتر از گواهینامه SSL DV است و کاربرانی که به سایت این سازمان یا شرکت مراجعه می‌کنند در بخش اطلاعات مربوط به گواهی‌نامه جزئیاتی را در مورد آن‌ها دارند و با اطمینان بیشتری فعالیت‌های خود را انجام می‌دهند. صدور این نوع گواهی‌نامه نیازمند تایید کامل هویت درخواست کننده است و باید از سازمان‌ها و شرکت‌های رسمی باشند. شرکت‌ها، سازمان‌های دولتی، بانک‌ها، وزارتخانه‌ها و به طور کل اشخاص حقوقی از متقاضیان این نوع گواهینامه SSL هستند. درخواست‌کننده باید مدارک کامل ثبتی و قانونی و هویتی شرکت، سازمان و نهاد مربوطه را به همراه فرم‌های درخواست و معرفی یک شخص مسئول همراه مدارک در مرحله اول به صورت اینترنتی ارسال نموده و پس از قبول درخواست از سمت صادر کننده، نسخه ترجمه شده تمام مدارک مهر شده را از طریق پست بین‌المللی مانند DHL به صادرکننده ارسال نماید. در صورت تهیه و فعال نمودن این نوع از گواهی‌نامه، اطلاعات تایید شده هویت آن سازمان در بخش جزئیات گواهینامه SSL نشان داده می‌شود که خاص آن سازمان، شرکت و یا نهاد می‌باشد.

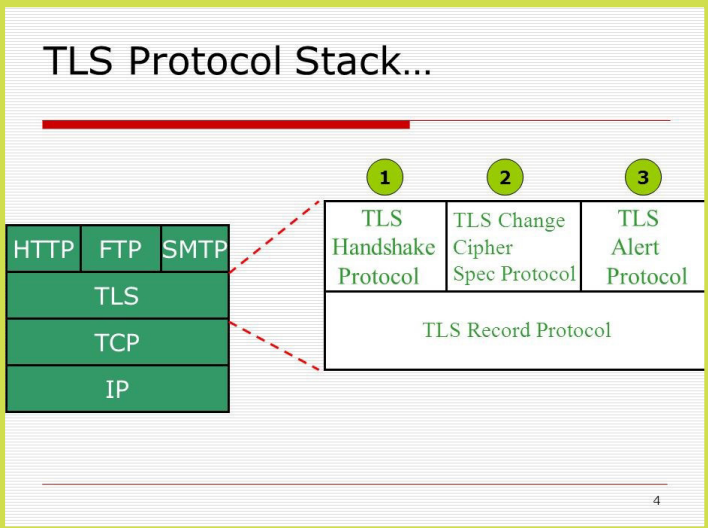
گواهی‌نامه اعتبارسنجی گسترش یافته

مشخصه اصلی این گواهی‌نامه که Extended(EV Validation) نیز نام دار نشان سبز رنگ قفل در مرورگر است و برای صدور آن روندی که در گواهی‌نامه OV طی شد نیز در این گواهی باید طی شود اما روند بررسی‌ها و ارزیابی برای این گواهی بسیار دقیق‌تر و با حساسیت بالاتری خواهد بود به همین دلیل از اعتبار و ارزش بالاتری برخوردار است و معمولاً سازمان‌های بزرگ در دنیا از جمله شرکت‌هایی مثل گوگل از این نوع گواهی‌نامه استفاده می‌کنند. مدارک مورد نیاز برای سفارش این نوع از گواهی‌نامه SSL همانند گواهی‌نامه OV می‌باشد با این تفاوت که احراز هویت سازمان و یا شرکت دقیق‌تر بوده و مدارک بیشتری و با دقت بالاتری مورد رسیدگی قرار می‌گیرد، به علاوه هزینه آن بالاتر است برای اعتبارسنجی کلیه اطلاعات از جمله شماره تلفن‌ها و اطلاعات وب بررسی می‌شود. در جدول ۱ مقایسه‌ای در مورد گواهی‌نامه‌ها انجام شده است که ملاحظه آن می‌تواند مفید باشد.

مشکلات گواهی‌نامه‌ها

یک سیاست‌گذاری بسیار مهم و اصول کلیدی برای توسعه‌دهندگان مرورگرهایی مانند گوگل کروم و فایرفاکس موزیلا امنیت آنلاین و محافظت از داده‌های کاربران است. به عنوان مثال در فصل پاییز سال ۲۰۱۷ گوگل اعلام کرد که صفحاتی که از HTTP استفاده می‌کنند را نا امن یا با عبارت "Not Secure" نشان می‌دهد و در قدم‌های بعد اساساً مانع دسترسی کاربران به چنین صفحاتی می‌شود. این حرکت گوگل به صورت موثری سایت‌هایی که HTTP بودند را مجبور به خرید گواهی معتبر کرده است. بر این اساس تقاضا برای خدمات CA ها افزایش یافته است و این افزایش تقاضا باعث می‌شود به موجب تعجیل در چک کردن اسناد، تاثیر منفی بر کنترل کیفیت داشته باشد.

نتیجه این امر آن است که امروزه گواهی‌های قابل اعتماد و معتبر به وب‌سایت‌هایی که کاملاً غیر قابل اعتماد هستند صادر شود. یک مطالعه گوگل نشان می‌دهد که یکی از بزرگترین و معتبرترین CA ها بیش از ۳۰ هزار گواهی‌نامه را بدون انجام اقدامات قانونی صادر کرده است. پیامدهای ناشی از این مطالعات در قبال این CA به این صورت بود که گوگل اعلام کرده است که تا عدم اصلاح کامل سیستم تائید و معرفی استانداردهای جدید، تایید اعتبار گواهی‌نامه‌های آن‌ها را متوقف خواهد ساخت. موزیلا نیز قصد دارد سخت‌گیری بیشتری را در خصوص اعتبار گواهی‌نامه‌ها انجام دهد. با وجود این موارد هنوز هم نمی‌توان به طور کامل مطمئن شد که یک گواهی‌نامه و صاحب آن دارای اطمینان هستند. حتی در



شکل۳. پشته پروتکل TLS

مورد گواهی‌های EV که به صورتی تمامی الزامات امنیتی را در مورد آن رعایت می‌کنند نیز نشان سبز رنگ قفل هم به طور کامل قابل اعتماد نخواهد بود.

متاسفانه اخیراً وضعیت گواهی‌نامه‌های EV نیز نا امیدکننده بوده است. یک جاعل (Phisher) به عنوان مثال یک شرکت را تحت نام مشابه یک شرکت شناخته شده ثبت کند و یک گواهی EV برای این سایت به دست آورد. نام شرکت چون مشابه یک شرکت معتبر بوده و دارای قفل سبز رنگ معتبر است می‌تواند برای عملیات فیشینگ مورد استفاده قرار گیرد و بسیاری از کاربران نیز متوجه این نام مشابه نخواهند شد. بنابراین کاربران هنگام استفاده از صفحات وب کاملاً مراقب این موضوع بوده و آدرس را به صورت دقیق چک کنند.

۶- توصیه‌ها

توصیه‌های زیر در این زمینه می‌تواند راه‌گشا باشد.

• همیشه در ورود اطلاعات در حساب کاربری، رمزهای عبور، اعتبارنامه‌های بانکی و یا هر اطلاعات شخصی دقت کنید و اطمینان حاصل شود که آدرس و نام دامنه کاملاً صحیح باشد. معمولاً سایت‌های جعلی بسیار مشابه سایت‌های اصلی هستند و قبل از کلیک کردن بر روی لینکی حتماً اطمینان حاصل شود که لینک قابل اعتماد است یا خیر.

• همیشه در مورد خدماتی که یک سایت ارائه می‌دهد و در واقع مواردی که شما نیاز دارید تا در سایت ثبت‌نام کنید، هوشیار باشید.

• اطمینان حاصل کنید که سیستم مورد استفاده شما به خوبی توسط یک سامانه امنیتی مورد محافظت است.

منابع:

جدول ۱. مقایسه بین گواهی‌نامه‌های SSL

	Domain Validation (EV) SSL	Organization Validation (OV) SSL	Extended Validation (DV) SSL
Proves domain ownership	■	■	■
Validates organization		■	■
Shows business is legitimate			■
Boosts Google ® ranking	■	■	■
Strongest SHA-2048 & 2-bit encryption	■	■	■
Padlock in address bar	■	■	■
Green address bar			■
Protects 1 website	■	■	■
Protects multiple websites (Multi-domain SAN SSL)	■	■	■
Protects all subdomains (Wildcard SSL)	■	■	
Security trust seal	■	■	■

دفتر تقلب

ساختار کلی

{نوع اسکن} [گزینه ها] {هدف} Nmap

تعیین هدف

192.168.1.1	ای پی ورژن چهار
AABB:CCDD::FF%eth0	ای پی ورژن شش
www.target.tgt	نام هاست
255-255.0-192.168.0	محدوده ای پی
16/192.168.0.0	بلاک CIDR
-iL <نام فایل>	خواندن لیست هدف‌ها از یک فایل

مشخص کردن پورت هدف

-F	اسکن صد پورت محبوب
-p <port1>-<port2>	اسکن یک محدوده از پورت‌ها
-p <port1>,<port2>,...	اسکن لیستی از پورت‌ها
-p U:53,U:110,T445-20	اسکن پورت‌های TCPوUDP
--top-ports <n>	اسکن n پورت محبوب
-p-	اسکن تمامی پورت‌های موجود
-p-0	اسکن تمامی پورت‌ها از آخر به اول

انواع اسکن

-sn	فقط درخواست Prob ارسال میکند.(میتواند فعال بودن هاست ها را تشخیص دهد، پورت اسکن نمی‌کند.)
-sS	اسکن SYN
-sT	اسکن TCP Connect
-sU	اسکن UDP Scan
-sV	اسکن ورژن (به عنوان مثال ورژن سرویس موجود بر پورت‌های متفاوت را تشخیص می‌دهد.)
-o	این اسکن سیستم عامل هدف را تشخیص میدهد
-scanflags	یک درخواست tcp سفارشی برای هدف ارسال میکند.(به عنوان مثال ACKPSH یا RSTSYN و ...)

موتور اسکریپتی

-sC	استفاده از اسکریپت پیشفرض
--script <نام اسکریپت>	استفاده از یک اسکریپت مشخص
--script-args= <Name=Value>	اسکن لیستی از پورت‌ها
--script-updatedb	به روز رسانی اسکریپت‌ها

زمانبندی برای اسکن

-T0	بسیار کند،برای عبور از IDS استفاده می‌شود.
-T1	کند ولی سریعتر از T۰. برای عبور از IDS استفاده می‌شود.
-T2	ده مرتبه کند تر از اسکن معمولی برای کاهش پهنای باند استفاده شده کاربرد دارد.
-T3	حالت پیشفرض. یک مدل داینامیک زمانبدی است که بر اساس پاسخ گویی هدف عمل می‌کند.
-T4	اسکن سریع ممکن است با درخواست های زیادی که برای هدف میفرستد آن را مختل کند.
-T5	نسبت به T۴سریع تر است و علاوه بر احتمال ایجاد اختلال در هدف ممکن است در اسکن پورت‌هایی را از دست بدهد.

گزینه‌های کاوش

-Pn	درخواست probe ارسال نمی‌شود، با فرض اینکه تمامی هاست‌ها فعال هستند.
-PB	درخواست prob پیشفرض ارسال میشود.(TCP ۸۰ و ۴۴۵ و ICMP)
-PS <ports>	چک می‌کند که آیا هاست مورد نظر فعال است با چک کردن لیست پورت‌های TCP که به آن داده‌ایم.
-PE	از درخواست ICMP Echo استفاده می‌کند.
-PP	از درخواست ICMP Timestamp استفاده می‌کند.
-PM	از درخواست ICMP Netmask استفاده می‌کند.

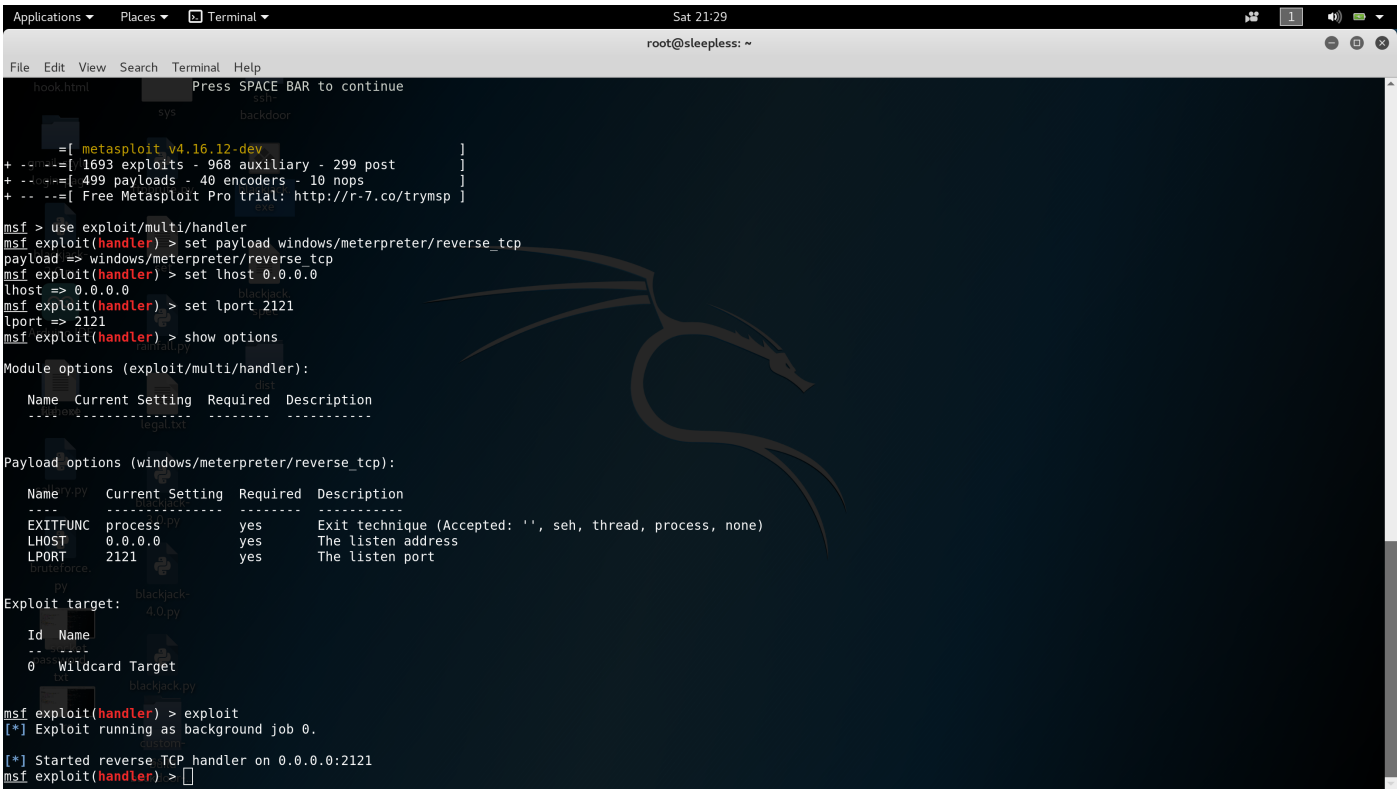
فرمت‌های خروجی

-oN	خروجی استاندارد Nmap
-oG	خروجی با قابلیت Grep شدن
-oX	خروجی به صورت XML
-oA <basename>	خروجی به هر سه فرمت ذکر شده (nmap,gnmap,xml) در فایل‌های جداگانه با نام تعیین شده

| معرفی ابزار، مقاله، کتاب

معرفی ابزار

متا اسپلویت



متا اسپلویت فریمورکی سورس باز است که به صورت اختصاصی برای متخصصان تست نفوذ، هکرها، محققین امنیتی و دیگر فعالان موجود در زمینه امنیت شبکه نوشته شده است. شما با استفاده از این فریمورک می‌توانید آسیب‌پذیریهای موجود در سیستم‌ها، شبکه‌ها و نرم‌افزارهای گوناگون را بکار گرفته و به این سیستم‌ها نفوذ کنید. این اپلیکیشن به صورت پیش‌فرض دارای اکسپلویت‌های بسیاری می‌باشد ولی علاوه بر آن شما می‌توانید خودتان اکسپلویت دلخواه خود را ایجاد کنید و به آن اضافه کنید.

متا اسپلویت دارای ۳ نسخه زیر است که استفاده از هر نسخه بستگی به نیاز شما و سطح کاری که میخواهید انجام بدهید بستگی دارد:

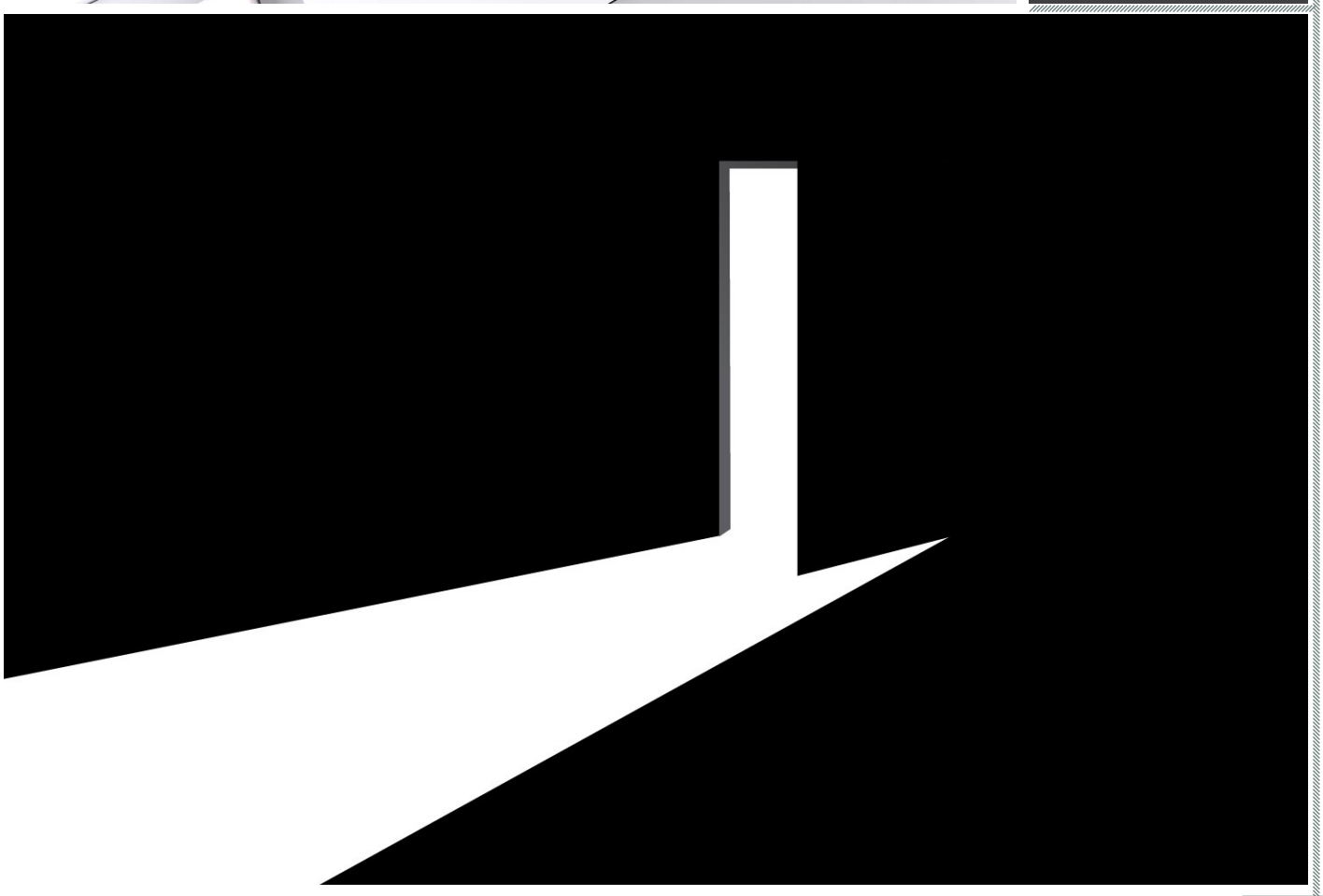
- Metasploit Pro
- Metasploit Community
- Metasploit Framework

متخصصان امنیتی، متخصصان تست نفوذ، مدیران شبکه، برنامه نویسان و همه اشخاصی که در زمینه امنیت فعالیت می‌کنند نیاز دارند تا مهارت کار با ابزار متا اسپلویت را کسب کنند. متخصصان امنیتی و متخصصان تست نفوذ در فازهای جمع آوری اطلاعات، کشف و اسکن آسیب‌پذیری، بکارگیری، اکسپلویت، نفوذ و حمله به سیستم‌ها و حملات پس از بکارگیری این ابزار می‌توانند به آسانی یک تست نفوذ را پیاده‌سازی کرده و هدف خود را عملی کنند. قابل ذکر است که ابزار متا اسپلویت یکی از کلیدی‌ترین ابزارهای تست نفوذ می‌باشد.

نسخه‌های رایگان متا اسپلویت را می توانید در kali و pentesterbox مشاهده نمایید.

معرفی مقاله

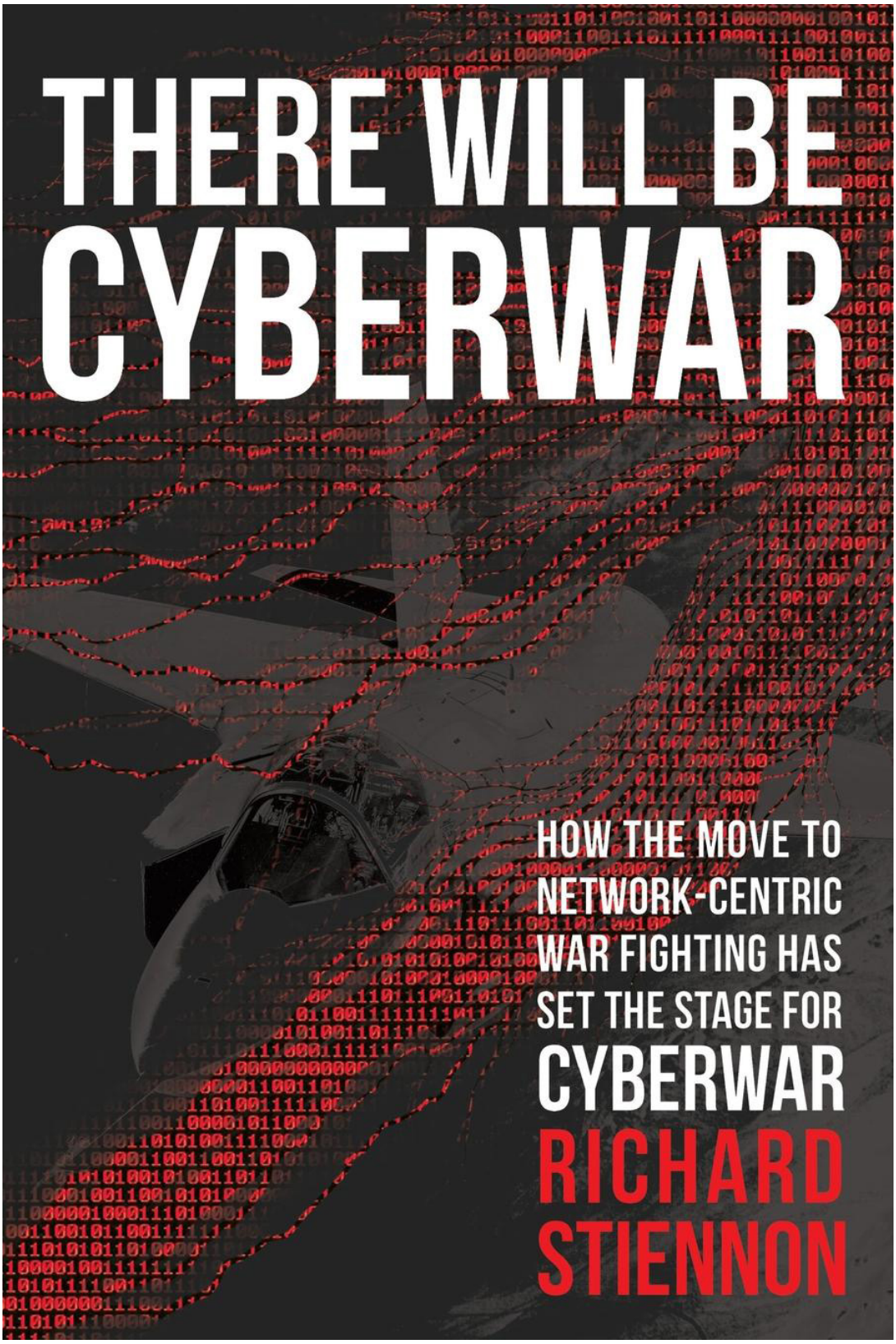
مقدمه‌ای بر نحوه ایجاد درب پشتی به صورت دستی



در علوم امنیت، درب پشتی به نوعی از بدافزار گفته می‌شود که بتوان از آن بدون اجازه به قسمت‌های مشخصی از یک رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد. درهای پشتی ممکن است از قبل در سیستم‌عامل وجود داشته باشند یا اینکه فرد نفوذگر با فریب کاربر، او را نسبت به نصب درب پشتی ترغیب کند (حملات مهندسی اجتماعی و ...). معمولا درب‌های پشتی با هدف دسترسی دوباره به سیستم‌عامل یا سامانه‌ای خاص ایجاد می‌شود تا مهاجم بتواند بعد از نفوذ به آن سامانه روشی را برای خود جهت نفوذ دوباره ایجاد کند تا مجبور به انجام تمام مراحل قبل‌تر از آن که بعضا بسیار زمان‌بر است، نباشد. این مقاله به بررسی نحوه ایجاد یک درب پشتی می‌پردازد که شما با داشتن دانش در این مورد می‌توانید درک بهتری از آنالیز و تحلیل سیستم‌ها داشته باشید.

نویسنده:abatchy۱۷(نام کاربری نویسنده در سایتexploit-db.com)

لینک دانلود:



معرفی کتاب

جنگ سایبری در راه است

اگر علاقه‌مند به مطالعه خلاصه‌ای از جنگ‌های سایبری که علیه دولت‌ها، ارتش و مراکز نظامی، زیرساخت‌های حساس و کسب‌وکارها در بیست سال گذشته رخ داده است هستید این کتاب را مطالعه کنید. هم‌چنین در این کتاب می‌توانید مثال‌های کوچکی را ببینید که برای جلوگیری از هر یک از این عملیات سایبری نیاز بوده است. این کتاب برخلاف کتاب‌هایی که با محوریت بدافزار استاکس‌نت با نگاه ویژه به سامانه‌های کنترل صنعتی نوشته شده‌اند، محوریت خود را بررسی انواع حملات سایبری با اهداف متفاوت قرار داده است. اگرچه این کتاب اطلاعات زیادی در مورد آینده جنگ سایبری نمی‌دهد اما بررسی جنگ‌های سایبری گذشته ممکن است روند این جنگ‌ها را نشان دهد. حتی این کتاب در مورد این مسئله بحث می‌کند که در دنیای امروز سامانه‌های ارتباطی و اغلب اجزایی که برای جنگ فیزیکی نیاز است، از راه شبکه به یکدیگر متصل شده‌اند و بیش‌تر به نرم‌افزارهای آسیب‌پذیر وابسته هستند که احتمال حملات سایبری را افزایش می‌دهد. نویسنده این کتاب Richard Stiennon است، وی پس از تعریف جنگ سایبری و بیان این مسئله که با احتمال زیادی جنگ سایبری از مدت‌ها پیش آغاز شده و در زمان مناسب اثرات آن مشخص می‌شود، در مورد سلاح‌های سایبری به کار رفته در هر حمله سایبری اطلاعاتی را ارائه می‌دهد.

نویسنده : Richard Stiennon

لینک کتاب:

گزارش تحلیلی و آسیب پذیری

باج افزار چیست؟

■ هادی گلباغی

باج افزارها (Ransomware) نوعی بدافزار هستند که در سال‌های اخیر یک تهدید امنیتی جدی به شمار می‌آیند. باج‌افزارها دسترسی به فایل‌ها و سیستم را محدود می‌کنند و حتی ممکن است دسترسی به کل سیستم‌عامل قطع شود و قربانی را به پرداخت باج به مهاجم مجبور کنند تا دسترسی به فایل‌ها و سیستم دوباره برقرار شود. اولین نسخه باج افزارها در اواخر دهه ۱۹۸۰ میلادی توسعه یافت و تا سال‌ها این نوع بدافزار مورد استفاده نبود.

با توجه به رشد قابل توجه حملات باج‌افزارها، بسیار مهم است تا روش‌های پیش‌گیرانه و محافظتی در مقابل این نوع بدافزار مدنظر قرار گیرد. باج‌افزار یک تهدید در حال رشد است که فایل‌های کاربر را رمزنگاری کرده و کلید رمزگشایی را تا پرداخت باج که معمولاً به‌صورت ارزهای مجازی است توسط قربانی نگه می‌دارد. این نوع بدافزار سالانه، مسئول ده‌ها میلیون دلار اخاذی است. نرخ گسترش باج‌افزار در سال‌های اخیر روندی بسیار شدیدی را داشته است به شکلی که از ۴ میلیون نمونه آلودگی در سال ۲۰۱۵ به ۶۳۸ میلیون مورد آلودگی در سال ۲۰۱۶ رسیده‌اند. همچنین در طول سال ۲۰۱۶ در حدود ۴۸ درصد شرکت‌های تجاری به صورت میانگین یک حمله باج‌افزار را تجربه کرده‌اند که می‌توان گفت در هر ۴۰ ثانیه یک حمله انجام گرفته است. این آمارآلودگی به باج‌افزار برای حوزه آموزشی ۲۳ درصد، حوزه فناوری اطلاعات ۲۲ و حوزه رسانه ۲۱ درصد بوده است. همچنین در کمپانی بالای هزار نفر کارمند ۲۵ درصد و در کمپانی‌های کوچک ۲۰ درصد از آن‌ها حداقل یک حمله باج‌افزار را تجربه کرده‌اند و ۷۱ درصد از کمپانی‌هایی که مورد حمله باج‌افزارها قرار گرفته‌اند سیستم‌هایشان آلوده شده است. در دو سال گذشته ۶۰ درصد از کل حملات بدافزارها مربوط به حملات باج‌افزارها بوده است.

در شکل ۱ رشد این باج‌افزارها در سال ۲۰۱۷ و در شکل ۲ و ۳ تعداد باج‌افزارهای جدید و مجموع باج‌افزارها در سه ماهه اول سال ۲۰۱۸ نشان داده شده‌اند.

روند تکاملی باج‌افزارها از ابتدا تا کنون به صورت جدول ۱ (صفحه ۲۶) است که در سالیان اخیر نمونه‌های بیشتری از باج‌افزارها معرفی شده‌اند و توجه به نمونه‌هایی بوده است که دارای بیشترین تخریب و تکثیر بوده‌اند.

باج‌افزارها در حالت کلی به دو دسته تقسیم می‌شوند که در ادامه هر کدام بررسی خواهند شد.

• قفل‌کننده‌های سیستم و صفحات (Screen Lockers)

این نوع از باج‌افزارها از ابتدا مورد استفاده قرار گرفتند که با نام Winlocker نیز شناخته می‌شوند. وقتی سیستم به این نوع باج افزار آلوده شود با پیامی روی صفحه نمایش مواجه خواهد شد به این معنی که تمام فعالیت‌های کامپیوتر شما قفل یا منجمد و یا Freeze شده است. پس از راه اندازی مجدد سیستم، پنجره‌ای با اندازه کامل ظاهر می شود که اغلب همراه با نماد FBI و وزارت دادگستری آمریکا است و نشان می‌دهد که فعالیت غیر قانونی بر روی کامپیوتر شما شناسایی شده است و شما باید بابت فعالیت‌های غیر قانونی مانند جرایم سایبری و ... هزینه ای پرداخت کنید.

• باج‌افزارهای رمزگذار (Encryption Ransomware)

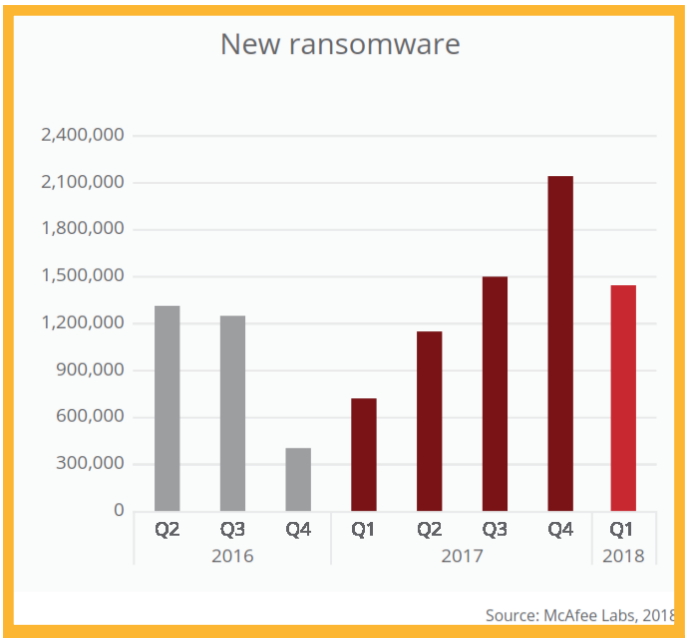
بعد از مدت زمانی باج‌افزارها علاوه بر قفل کردن صفحه کلیه اطلاعات سیستم کاربر را نیز رمزنگاری و غیرقابل دسترس کردند. این نوع بدترین نوع باج افزارها هستند و پس از رمزگذاری فایل‌ها خواستار پرداخت هزینه برای رمزگشایی و بارگذاری مجدد فایل‌ها هستند. دلیل اینکه این نوع باج افزار بسیار خطرناک هستند این است که بعد از اینکه مجرمان سایبری فایل های شما را رمزگذاری کردند، هیچ نرم افزار امنیتی قادر به بازیابی و بازگردانی فایل های شما نخواهد بود بجز اینکه هزینه را پرداخت کنید و حتی در صورت پرداخت هزینه نیز تضمینی برای بازگردانی فایل ها نخواهد بود.

نکته‌ای که بسیار با اهمیت به نظر می‌رسد شاید این باشد که باج‌افزارها از چه منابعی ممکن است منتشر شوند. منابعی که باعث انتشار و تکثیر باج‌افزارها می‌شوند به صورت زیر هستند:

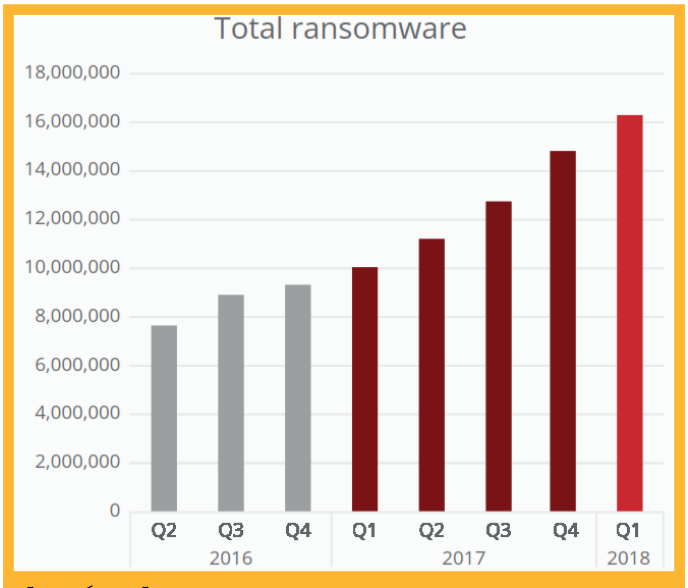
- وب‌سایت‌های آلوده
- هرزنامه‌ها و ایمیل‌های فیشینگ
- نرم‌افزارهای مخرب
- سو استفاده از آسیب‌پذیری‌ها
- شبکه داخلی

در توضیح موارد بالا می‌توان گفت که تکثیر باج‌افزارها بیشتر از طریق هرزنامه‌ها و ایمیل‌های فیشینگ صورت می‌گیرد. در آماری ۶۴ درصد از تکثیر باج‌افزارها مربوط به تکثیر از طریق هرزنامه‌ها و ۱۶ درصد از طریق وب‌سایت‌ها و وب‌اپلیکیشن‌های آلوده صورت گرفته است. تکثیر از طریق هرزنامه‌ها به این شکل است که ایمیلی‌هایی به صورت انبوه به کاربران ارسال می‌گردد که این ایمیل‌ها ممکن است شامل پیوست‌های مخرب مانند فایل‌های PDF یا اسناد Word باشد یا ممکن است حاوی پیوندهایی به وب سایت های مخرب باشد. هرزنامه‌ها با استفاده از روش‌های مهندسی اجتماعی به منظور فریب مردم برای باز کردن پیوست‌ها و یا کلیک روی لینک‌ها، در قالب فرآیندی مطمئن به دنبال اهداف خرابکارانه خود هستند. مجرمان سایبری و نویسندگان باج افزارها، به منظور ترساندن کاربران و ترغیب آن‌ها، از نمادهایی مانند FBI استفاده می‌کنند تا کاربران را مجاب به باز کردن فایل‌های پیوست و در نهایت آلوده کردن آنها

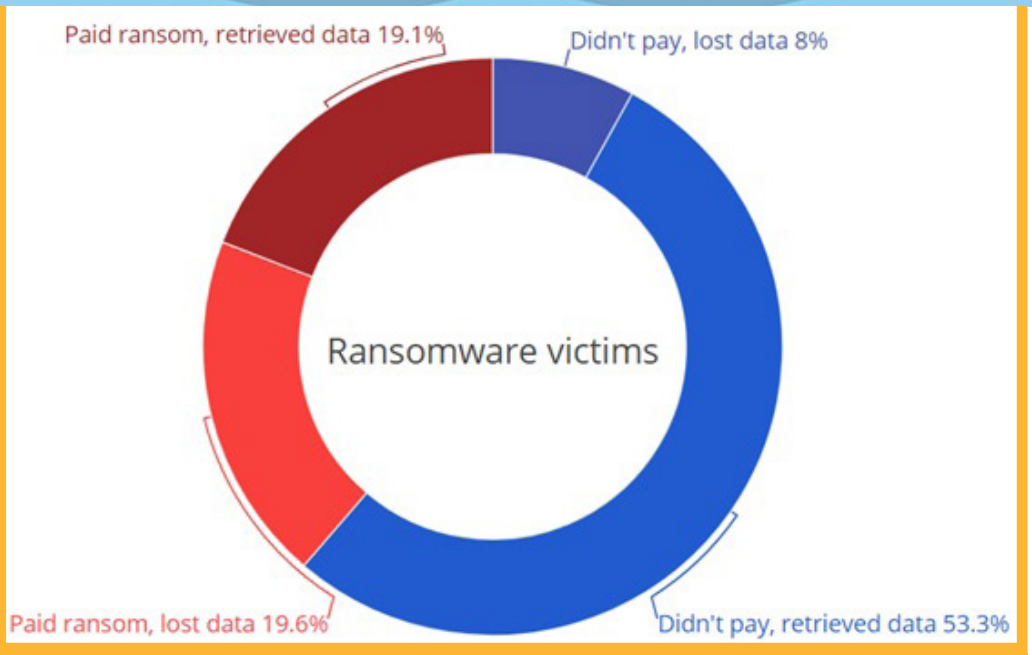
شکل ۱. رشد باج‌افزارهای جدید در سه ماهه چهارم سال ۲۰۱۷



شکل ۲. نمودار باج‌افزارهای جدید تا سه ماه نخست سال ۲۰۱۸ از آزمایشگاه مک‌آفی



شکل ۳. نمودار تعداد کل باج‌افزارها تا سه ماه نخست سال ۲۰۱۸ از آزمایشگاه مک‌آفی



شکل ۴. آماری از برگشت داده ها و پرداخت باج در باج افزارها

کنند.

یکی دیگر از روش های آلوده‌سازی رایج که در اواسط سال ۲۰۱۶ به اوج خود رسید، استفاده از تبلیغات است یعنی به این شکل که با استفاده از تبلیغات آنلاین مخرب نرم افزارها یا باج‌افزارهای مخرب را توزیع و تکثیر کرد.

همچنین باج‌افزارها در چه پلتفرم‌های مختلفی وجود دارند که می‌توان به موارد زیر اشاره کرد:

- ویندوز
- مک
- لینوکس
- دستگاه‌های IOT
- اندروید
- IOS

با آلودگی به وسیله باج‌افزار داده‌ها چگونه از دست می‌روند؟

باج افزار وارد سیستم قربانی می‌شود. در این بخش دو حالت وجود دارد:

۱. صفحه نمایش را قفل می‌کند.

۲. تمامی فایل‌ها در سیستم رمزگذاری می‌شوند.

در هر دو حالت پیغامی برای باج‌خواهی منتشر می‌شود که مهلت و نحوه پرداخت را اعلام کرده است و معمولاً این باج به صورت پرداخت از طریق ارسال کد ارزهای مجازی است.

سوالی که مطرح می‌شود به این صورت است که در مقابل باج‌افزار چگونه از خود محافظت کنیم؟ در زیر به مواردی که می‌تواند در این حوزه مفید باشند اشاره شده است:

- هرگز ضمیمه ایمیل‌های مشکوک و فایل‌های دانلود شده مشکوک را باز نکنید.
- سیستم‌عامل و نرم‌افزارهایتان را به روز رسانی کنید.
- به طور منظم از داده‌هایتان فایل پشتیبان تهیه کرده و در مکان‌های مختلفی قرار دهید.
- یک برنامه ضد بدافزار مطمئن و یا ضد باج‌افزار نصب کرده و به طور مداوم به روزرسانی کنید.

در صورت آلودگی به باج‌افزار چه کاری می‌توان کرد؟

- روی هیچ فایلی کلیک نکنید و به حساب‌های کاربری و ایمیل خود وارد نشوید.
- به هیچ‌وجه پرداخت باج توصیه نمی‌شود چون که هیچ تضمینی نیست که حتی پس از پرداخت باج اطلاعات برگردانده شوند. در شکل ۴ آماری در این خصوص نشان داده شده است.
- دسترسی شبکه سیستم را فوراً قطع کنید.
- در صورت عدم تسلط کافی سیستم را به نزدیک‌ترین مرکز آپا یا شرکت امنیتی انتقال دهید تا مشکل را حل کنند.
- در صورت تسلط با نصب ویندوز و فرمت ویندوز آلوده قبلی و بازیابی سیستم با استفاده از نسخه‌های پشتیبان مشکل حل خواهد شد.

درخصوص کاربرانی که سیستم‌هایشان با باج‌افزار آلوده می‌شود آزمایشگاه امنیتی کسپرسکی تحقیقاتی را انجام داده است که نتایج آن در ادامه بررسی خواهند شد. طبق تحقیقات کسپرسکی۵۳ درصد از کاربران با وجود اینکه می‌دانند ممکن است فایل‌های دیجیتال شامل عکس‌ها و ویدئوهای خود را از دست بدهند حاضر به پرداخت باج نیستند. همچنین به طور میانگین کاربرانی که حاضر به پرداخت باج در ازای برگرداندن فایل‌های دیجیتال‌شان می‌شوند، فقط حاضر به پرداخت مبلغ کمی هستند. ۷۲ درصد از سیستم‌های آلوده مربوط به شرکت‌های تجاری دسترسی به داده‌هایشان دو روز یا بیشتر از دو روز را از دست داده‌اند. از ۲۶ درصد از آمریکایی‌ها و ۲۴ درصد از کانادایی‌ها اعلام کردند که حاضر هستند به طور دائم شبکه‌های اجتماعی را کنار بگذارند به شرطی که در آینده از فایل‌های دیجیتالی و شخصی‌شان محافظت شود. سه مورد از اطلاعات مهمی که نگرانی از دست دادن آن وجود دارد شامل اطلاعات حساب بانکی، شماره تامین اجتماعی و اطلاعات کارت اعتباری هستند. برای افرادی که بیشترین ارتباطات را در فضای سایبری دارند ۴۲ درصد اعلام کردند که نمی‌دانند باج‌افزار چیست و تنها ۱۳ درصد نسبت به باج‌افزار نگران بوده‌اند.

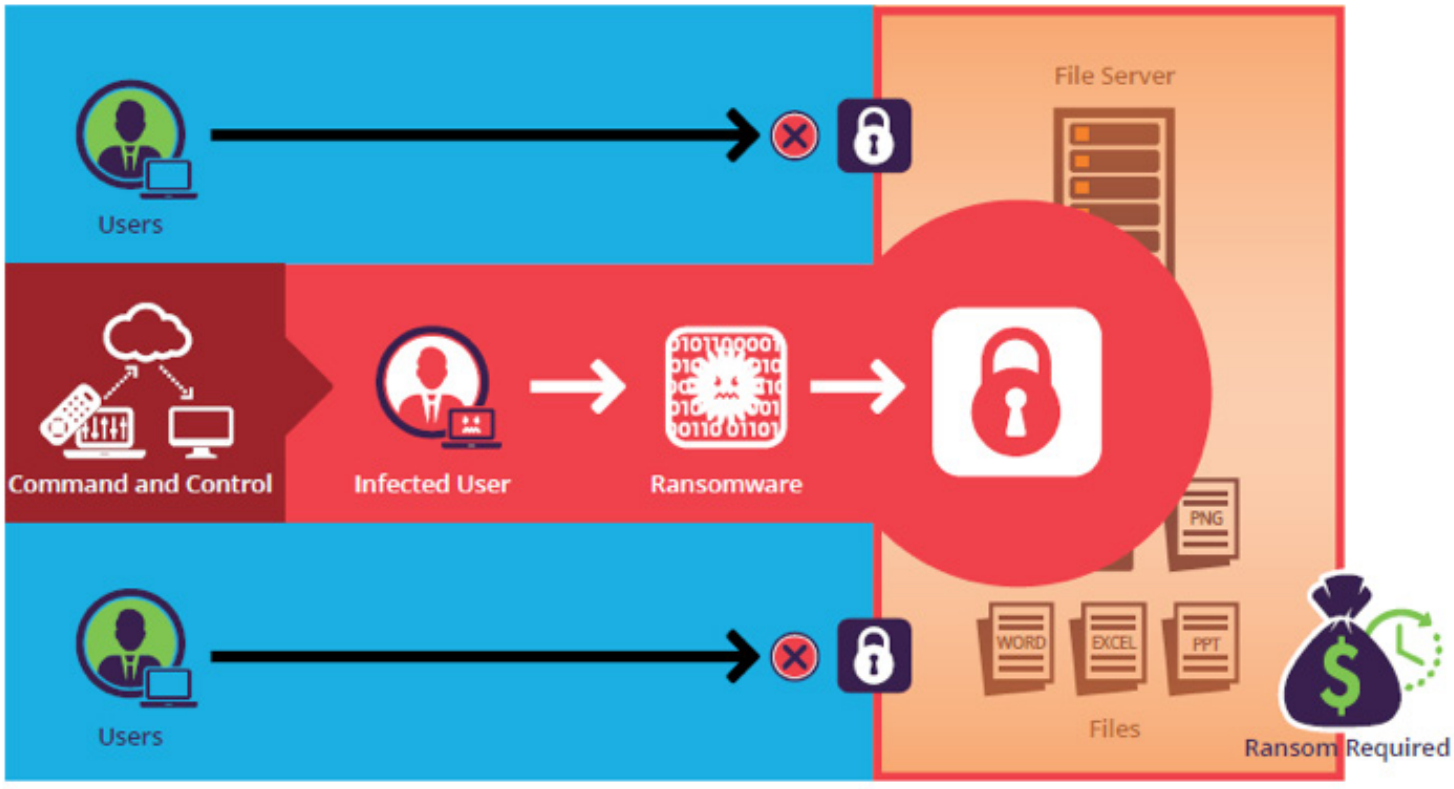
با وجود تمام موارد گفته شده اما هنوز هم باج‌افزارها بزرگ‌ترین نگرانی در سال ۲۰۱۸ در حوزه تهدیدات سایبری هستند که این مورد شان می‌دهد که راه‌حل‌های پیش‌گیرانه از طرف کاربران باید با جدیت پیگیری شود و تهدید باج‌افزارها را باید بسیار جدی گرفت.

منابع:

جدول ۱. سیر تکاملی باج‌افزارها از ابتدا تا کنون

نام باج‌افزار	تاریخ تکثیر اولیه	توضیحات
AIDS Trozen (PC cyborg)	۱۹۸۹	توزیع‌شده در کنفرانس بین‌المللی WHO AIDS به وسیله فلاپی درایو
Trozen.Gpcoder	۲۰۰۵	تکثیر به وسیله هرزنامه‌ها و ایمیل‌های فیشینگ برای افراد جوینده کار
Trojan.Cryzip	۲۰۰۶	حذف فایل‌ها و ایجاد یک رمز عبور محافظت شده
Trojan.archiveus	۲۰۰۶	باج‌افزاری مانند Trojan.cryzip
GPcode.AK	۲۰۰۸	رمزنگاری bit RSA-۱۰۲۴ و پرداختی بین ۱۰۰ تا ۲۰۰ دلار
Citadel	۲۰۱۲	انتشار برای هزینه ۳ هزار دلاری به منظور آماده‌سازی و توزیع باج افزار
Lyposit	۲۰۱۲	به عنوان یک Pop-up در قالب فعالیت قانونی اجرا شده و نمایش صفحه قفل شدن توسط FBI
Trojan.Randso.C	۲۰۱۲	نمایش خودش به عنوان مرکز پاسخگویی امنیتی ویندوز
CryptoLocker	۲۰۱۳	رمزنگاری حدوداً ۶۷ نوع فایل مانند فایل‌های مجموعه آفیس و مهلت سه روزه برای پرداخت باج
CryptoLocker 2.0	۲۰۱۳	نوشته شده با زبانی متفاوت با نسخه اول و حدوداً ۶ برابر تکثیر بیشتر از ژانویه تا دسامبر ۲۰۱۳
CryptoDefense	۲۰۱۳	نسخه دیگری از باج‌افزار CryptoLocker که با الگوریتم رمزنگاری ۲۰۴۸ بیتی RSA رمز می‌کند و تا زمان پرداخت پول، پرونده‌های رمزشده باقی می‌مانند.
Nemucod	۲۰۱۵	در اصل Nemucod یک تروجان است که فایل‌های مخرب را به داخل یک سیستم آلوده دانلود می‌کند و دانلودهای آن شامل باج‌افزار Teslacrypt نیز می‌باشد.
CryptoWall	۲۰۱۵	در نسخه CryptoDefense توسعه‌دهندگان فراموش کرده بودند کلید رمزگشایی را از محتویات پرونده‌های باج‌افزار حذف کنند و این باعث شکست این نوع شد. برای غلبه بر چنین شکستی توسعه‌دهندگان باج‌افزار Cryptowall را ایجاد کرده‌اند که این‌بار بدون کلید رمزگشایی پرونده‌ها منتشر می‌شود و امکان بازپس‌گیری پرونده‌ها وجود نخواهد داشت.
LockerPin	۲۰۱۵	آلوده سازی سیستم‌های اندرویدی و تغییر PIN
Linus.Encoder.1	۲۰۱۵	کشف شده توسط Dr.Web
New CryptoWall	۲۰۱۵	شامل پروتکل‌های متفاوت برای فرار از شناسایی شدن و سخت شدن شناسایی فایل‌های سالم از رمزنگاری شده
CTB Locker	۲۰۱۶	این باج افزار ویژگی‌های نمونه‌های قبلی از جمله CryptoLocker و CryptoWall را دارد. همچنین مبلغ اخاذی حدود ۷۵۰ دلار و مهلت پرداخت باج ۹۶ ساعت می باشد. این گونه بصورت پیوست ایمیل، در قالب یک فایل ZIP منتشر می‌گردد.
JavaScript-only	۲۰۱۶	یک باج‌افزار مبتنی بر سرویس Ransomware as a Service است. از سال ۲۰۱۵ باج‌افزارها بیشتر برای فروش سورس کد آن‌ها و استفاده کردن باج‌افزار و سفارشی سازی توسط خریداران مورد استفاده بوده است که این دسته به صورت مخفف RaaS خوانده می‌شوند.
Petya	۲۰۱۶	با نام GoldenEye نیز شناخته می شود و همانند WannaCry بوده و از آسیب پذیری پروتکل SMB سیستم عامل ویندوز برای نفوذ استفاده می کند.
KeRanger	۲۰۱۶	اولین باج‌افزار که هدف آن حمله به سیستم‌های اپل بوده و برای رمزنگاری بیش از ۳۰۰ نوع فایل طراحی شده است.
Xbot	۲۰۱۶	سعی در سرقت اطلاعات بانکی داشته و برای دستگاه‌های اندرویدی در روسیه و استرالیا بوده است.
Jigsaw	۲۰۱۶	تعبیه شده در یکی از مجموعه فیلم‌های اره در قالب هرزنامه‌ها و ایمیل‌های فیشینگ و هزینه پرداختی در حدود ۱۵۰ دلار بوده است.
Locky	۲۰۱۶	پیاده‌سازی و رمزنگاری پیچیده و استفاده از مکانیزم قفل اطلاعات مدرن
Cerber	۲۰۱۶	این باج‌افزار از روش های پیشرفته ضدتحلیل و فرار از سد نرم افزارها و تجهیزات امنیتی بهره می‌برد و همانند بسیاری از باج‌افزارها از ماکروهای تزریق شده در فایل های Word یا Excel استفاده کرده و از طریق هرزنامه‌ها و ایمیل‌های فیشینگ منتشر می شود.
Spora	۲۰۱۶	در این باج‌افزار پس از پرداخت باج فقط پرونده‌های رمزنگاری شده برگردانده نمی‌شود بلکه می‌توان از حملات بعدی باج افزار نیز مصون ماند. Spora بسیار حرفه‌ای طراحی شده است چرا که از الگوریتم قوی برای رمزنگاری پرونده‌ها استفاده کرده و وب‌گاه پرداخت مناسبی دارد. همچنین این باج‌افزار بسته‌هایی را ارائه می‌دهد که قربانیان با پرداخت وجه مورد نظر می‌توانند این بسته‌ها را بخرند. در این باج‌افزار گزینه‌هایی برای انتخاب وجود دارد. قربانی می‌تواند تنها با پرداخت باج، پرونده‌های خود را بازیابی کند یا اینکه با پرداخت‌های دیگری، بدافزار را به کلی از سامانه‌ی خود حذف کرده و از حملات آتی بدافزار مصون بماند.
Notpetya	۲۰۱۷	همراه با یک به‌روزرسانی نرم‌افزار جعلی نفوذ انجام می‌گیرد و در بیش از ۱۰۰ کشور آلوده سازی انجام شد.
WannaCry	۲۰۱۷	سازنده WannaCry از اکسپلویت شناخته شده ویندوزEternalBlue استفاده کرد و با استفاده از این آسیب پذیری باج افزار WannaCry قادر بود تا به کامپیوترهای آلوده از راه دور دسترسی یافته و رمزنگار خودش را بر روی آن نصب نماید و بعد از آلوده کردن یک سیستم در یک شبکه با یک رفتار کرم گونه خود را در شبکه منتشر می‌کند.
Jaff	۲۰۱۷	در می ۲۰۱۷ به وسیله هرزنامه‌ها منتشر شد و شبیه به باج‌افزار Locky می‌باشد.
Crysis	۲۰۱۷	تمامی فایل ها را به فرمت .arena در هنگام رمزنگاری داده‌ها تغییر می دهد و پس از اتمام فرآیند رمزنگاری، دستورالعملی برای کاربر نمایش می‌دهند که او چگونه قادر است اطلاعات خود را رمزگشایی کند. در دستورالعمل به نمایش گذاشته شده از کاربر خواسته می‌شود که در ازای بازگردانی فایل‌های خود، مبلغی مشخص را از طریق بیت‌کوین پرداخت کند.

New Samsam	۲۰۱۸	Samsam یک باج افزار همیشگی نیست که اقدام به آلوده سازی همگانی کند بلکه یک باج افزار سفارشی می‌باشد که مختص حملات هدف دار است و فایل های سیستم آلوده را قفل کرده و پیامی مبنی بر "متاسفم (Sorry)" نشان می‌دهد و درآمدی در حدود ۳۰۰ هزار دلار تاکنون داشته است.
PSCrypt	۲۰۱۸	این باج‌افزار ابتدا در سال ۲۰۱۷ کشف شد و اغلب کاربران خانگی و سازمان‌های اوکراین را مورد هدف قرار داده بود. به نظر می رسد این باج‌افزار از خانواده باج افزارهای‌GI ("GlobeImposter") باشد. مشاهدات حاکی از آن است که باج افزار پس از نفوذ به سیستم قربانی و اتمام فرایند رمزگذاری فایل‌ها، به انتهای آن‌ها پسوند .docs را اضافه می‌کند و پیغام باج‌خواهی را به صورت یک فایل با نام document.html.docs در هر مکانی که رمزگذاری انجام شده و همچنین بر روی دسکتاپ قربانی قرار می‌دهد.
CyberSCCP	۲۰۱۸	شیوع آن بیشتر در خاورمیانه و به‌خصوص در میان جامعه ایرانیان است و کاربران شبکه‌های اجتماعی هدف اصلی این باج‌افزار می باشند. این باج‌افزار از خانواده باج‌افزار متن باز HiddenTear می‌باشد که تحت عنوان Cyber.exe با حجم ۱.۴۲ مگابایت و در پوشش اپلیکیشنی برای جعل مدارک هویتی از جمله کارت ملی و شناسنامه در حال گسترش در بین کاربران تلگرام فارسی زبان است



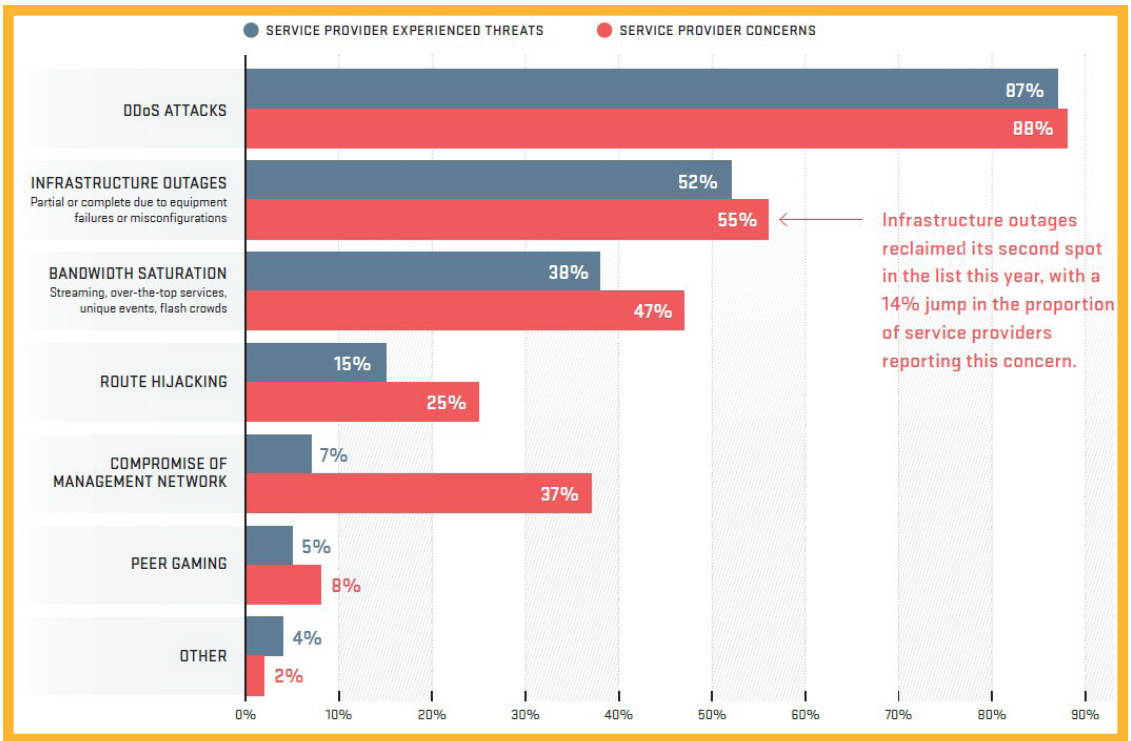
بررسی و تحلیل تهدیدات DDOS برای فراهم‌کنندگان سرویس در سال ۲۰۱۷

■ فرشته کیاست

حمله DDoS مخفف distributed denial of) service) به معنی سرازیر کردن تقاضاهای زیاد به یک سرور و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) به طوری که سرویس‌دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود. در این نوع حمله‌ها در یک لحظه یا در طی یک زمان به صورت مداوم از طریق کامپیوترهای مختلف که ممکن است خواسته یا حتی ناخواسته مورد استفاده قرار گرفته باشند، به یک سرور (با آی پی مشخص) درخواست دریافت اطلاعات ارسال می‌شود و موجب از دسترس خارج شدن سرور می‌شود.

حملات DDoS در رأس تهدیدات فراهم‌کنندگان سرویس در سال ۲۰۱۷ با سهم ۸۷ درصد از کل تهدیدات قرار دارد(شکل ۱)خرابی‌های زیرساخت (Infrastructure outages) نیز به عنوان یک تهدید ۵۲ درصد عامل‌های تهدیدات فراهم‌کنندگان سرویس را شامل می‌شود که نسبت به سال ۲۰۱۶ شش درصد افزایش یافته است. درصد اشباع پهنای باند (bandwidth saturation) نیز نسبت به سال ۲۰۱۶ ثابت مانده است. به طور مکرر نگرانی اصلی ۸۸ درصد فراهم‌کنندگان سرویس در سال ۲۰۱۸ حملات DDoS است. با توجه به نگرانی‌های مربوط به بات‌نت‌های IOT و آسان‌تر شدن کار مهاجمان برای دستیابی به حملات پیشرفته این مسئله تعجب‌آور نخواهد بود.

همانطور که در سال‌های گذشته ابزارهای مختلفی برای تشخیص تهدیدات علیه شبکه‌های کامپیوتری استفاده می‌شد، این بررسی نشان می‌دهد که ابزارهای تحلیلی NetFlow-base گزینه انتخابی فراهم‌کنندگان سرویس در این سال‌ها باقی مانده است و تنها در سال ۲۰۱۸ استفاده از آن از ۸۶ درصد به ۸۱ درصد کاهش یافته است (شکل ۲)همچنین استفاده از ابزارهای SNMP-based به ۶۴ درصد افزایش یافته است که در سال ۲۰۱۶ این درصد ۵۳ بود. استفاده از لاگ‌های فایروال نیز همراه با IDS/IPS در رتبه چهارم قرار دارند.

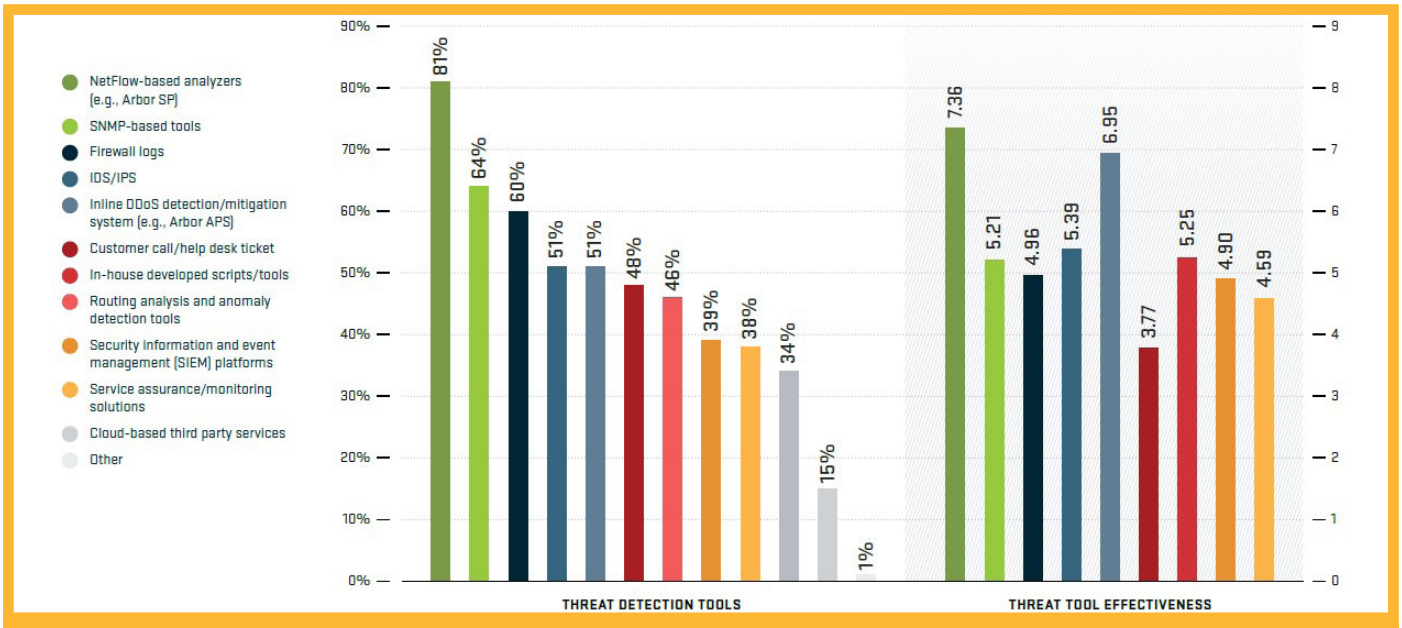


شکل ۱. تهدیدات و نگرانی‌های فراهم‌کنندگان سرویس

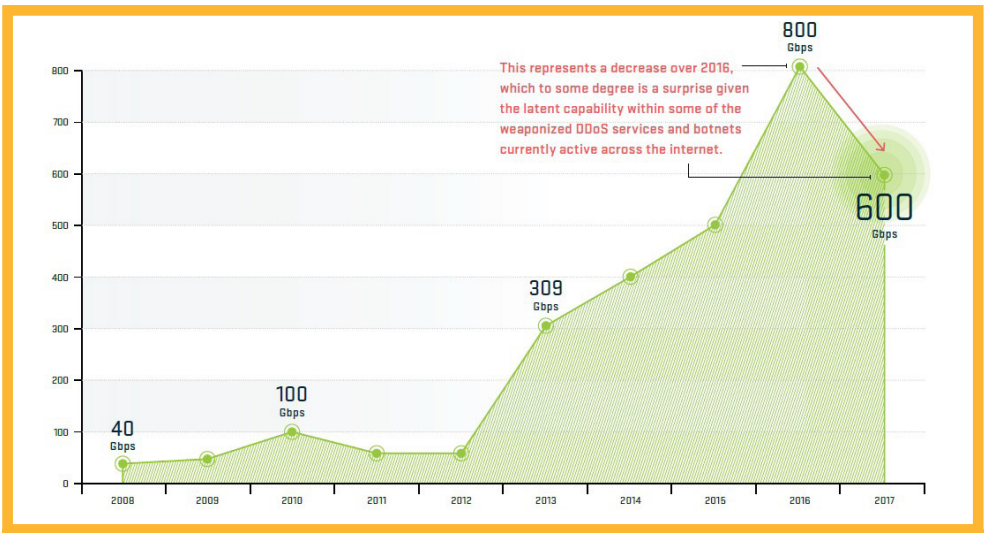
استفاده از سیستم تشخیص یا کاهش DDoS درونی (Inline DDoS detection/ mitigation system) از ۴۲ درصد به ۵۱ درصد افزایش داشته است. استفاده از راه‌حل‌های دفاع DDoS ترکیبی یک روند در حال پیشرفت است.

به طور کلی، نتایج اثربخشی ابزارهای تشخیص تهدید مشابه با سال ۲۰۱۶ بوده است. نتایج بررسی‌ها نشان می‌دهند که ابزارهای تحلیلی NetFlow-based و inline DDoS detection/mitigation بهترین و موثرترین راه‌حل‌های مقابله با تهدیدات DDoS بوده‌اند.

در سال ۲۰۱۷، مهاجمان با استفاده از تکنیک‌های بازتاب/تقویت (reflection/ amplification techniques) از آسیب‌پذیری‌های موجود در DNS، NTP، SSDP، CLDAP، Chargen و پروتکل‌های دیگر برای به حداکثر رساندن مقیاس حملات خود استفاده کردند. علاوه براین افزایش قابل ملاحظه‌ای در بهره‌برداری از دستگاه‌های IOT برای تولید سیلی از بسته‌های بزرگ و حملات لایه کاربردی به وجود آمده است. بزرگترین حمله گزارش شده توسط یک فراهم کننده سرویس ۶۰۰ گیگابایت در ثانیه بوده است و حملات دیگری نیز مانند ۵۸۸، ۳۳۸ و ۳۱۶ گیگابایت در ثانیه گزارش شده‌اند (شکل ۳).



شکل ۲. اثربخشی و میزان استفاده ابزارهای تشخیص تهدید



شکل ۳. اندازه حملات

شکل ۴. اهداف حملات

در شکل ۴ شایع‌ترین اهداف این حملات نشان داده شده است که از این بین کاربران نهایی با ۷۰ درصد در رأس اهداف حملات قرار دارند. خدمات مالی در بالاتر از خدمات ابری و هاستیگ و حکومت جزو اهداف اصلی حملات هستند.

انواع رایج حملات DDoS

مهاجمان سایبری به صورت مداوم در حال توسعه روش‌های استفاده از بردارهای حمله متفاوت برای فرار از دفاع و تشخیص هستند. به طور کلی بردارهای حمله به سه گروه تقسیم می‌شوند.

۱-حملات حجمی (Volumetric Attacks)

این حملات تلاش می‌کنند تا پهنای باند را در داخل شبکه یا سرویس هدف، یا بین شبکه هدف یا سرویس و اینترنت مصرف کنند. این حملات به سادگی باعث ایجاد ازدحام می‌شوند.

۲-حملات TCP State-Exhaustion

این حملات سعی در مصرف جداول حالت اتصال را دارند که در بسیاری از اجزای زیرساخت مانند load balancers، firewall، IPS و سرورهای اپلیکیشنی استفاده می‌شوند. آن‌ها همچنین می‌توانند دستگاه‌های با ظرفیت بالا را که قادر به نگهداری میلیون‌ها اتصال هستند از دسترس خارج کنند.

۳-حملات لایه کاربرد (Application-Layer Attacks)

این حملات مربوط به سرویس‌ها و قابلیت‌های لایه ۷ شبکه هستند. این نوع حملات پیچیده‌تر بوده زیرا آن‌ها می‌توانند با تولید یک ترافیک با نرخ کم بسیار موثر باشند.

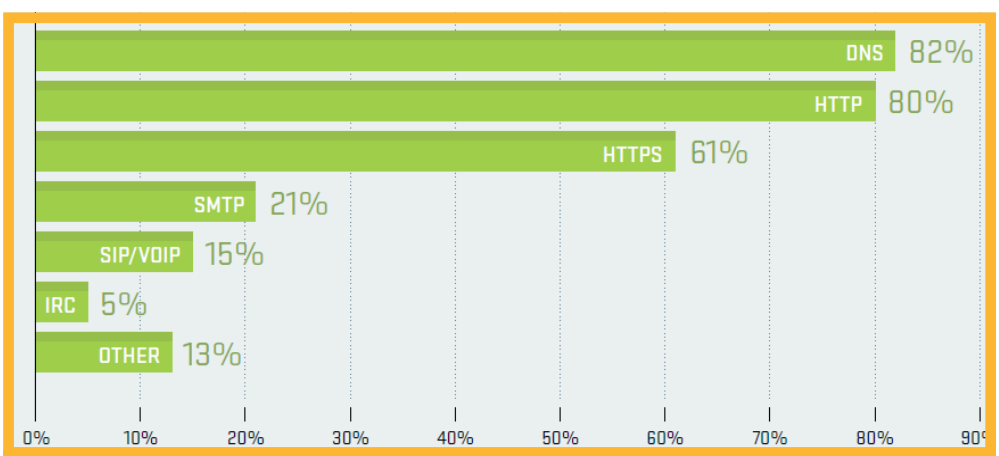
با نگاهی به ترکیب انواع حملات بر فراهم‌کنندگان سرویس، حملات حجمی رایج‌ترین نوع حمله گزارش شده است. همچنین این نوع حمله در سال ۲۰۱۷ افزایش قابل ملاحظه‌ای داشته است (شکل ۵).

نکته قابل توجه این است که حملات لایه شبکه همچنان به استفاده از سرویس‌های آسیب‌پذیر ادامه می‌دهند. سرویس DNS در سال گذشته بیشترین هدف حملات لایه شبکه بوده است. طبق گزارش‌های بدست آمده ۸۲ درصد فراهم‌کنندگان سرویس از این طریق آسیب‌پذیر بوده‌اند (شکل ۶). پروتکل HTTP با ۸۰ درصد در جایگاه بعدی قرار دارد. میزان سوءاستفاده از پروتکل HTTPS نسبت به سال گذشته از ۵۲ درصد به ۶۱ درصد افزایش داشته است که به

شکل ۵. انواع حملات DDoS

این معنی است که همیشه رمزنگاری تنها راه‌حل موفقی برای مقابله با حملات DDoS نیست و راه‌حل های مقیاس پذیر موردنیاز است.

منبع:



شکل ۶. سرویس‌های هدف حملات لایه کاربرد

گزارش آسیب‌پذیری

۱ آسیب‌پذیری رمز عبور پیش‌فرض در پایگاه داده Policy Suite Cluster Manager محصولات سیسکو

■ فرشته کیاست

یک آسیب پذیری در مدیریت خوشه (cluster Manager) رابط Policy Builder سیسکو به یک مهاجم از راه دور اجازه می‌دهد با استفاده از حساب root که دارای اعتبار کاربری پیش‌فرض است به سیستم آسیب‌پذیر لاگین کند.
این آسیب‌پذیری ناشی از اعتبار پیش‌فرض در حساب root است. یک مهاجم می‌تواند با استفاده از این حساب به سیستم آسیب‌پذیر لاگین نموده و دستورات دلخواه را در سطح کاربر ریشه اجرا کند.
سیسکو به‌روزرسانی‌های نرم‌افزاری را که مربوط به این آسیب‌پذیری است، منتشر کرده است.

محصولات آسیب‌پذیر

نرم‌افزار Cisco Policy Suite نسخه ۱۸،۲،۰ و نسخه‌های پیش از آن تحت تاثیر این آسیب‌پذیری قرار دارند. مدیران شبکه می‌توانند با استفاده از دستور about.sh در CLI دستگاه نسخه فعلی Cisco Policy Suite اجرا شده بر روی آن را بیابند. در مثال زیر نسخه ۱۸،۰،۰ اجرا می‌شود.

```
[root@installer ~]# about.sh
Cisco Policy Suite - Copyright (c) 2015. All
rights reserved.
CPS Multi-Node Environment
CPS Installer Version - 18.0.0
CPS Core Versions
----------------------------
CPS Patch History
----------------------------
No patches have been applied
```

بحرانی (Critical)	Cisco Policy Suite Cluster Manager Default Password Vulnerability
عنوان	آسیب‌پذیری رمز عبور پیش‌فرض در پایگاه داده Policy Suite Cluster Manager
شناسه آسیب‌پذیری	CVE0375-2018-
CVSS Score	Base - 9.8
نسخه	1.0
شناسه باگ‌های سیسکو	CSCvh02680
تاثیر	آسیب‌پذیری رمز عبور پیش‌فرض (Default Password)
تاریخ انتشار	2018 July 16:00 18 GMT

راه حل

سیسکو ابتدا این آسیب‌پذیری را در نسخه ۱۸،۲،۰ نرم‌افزار Cisco Policy Suite رفع کرده است. این نرم‌افزار را می‌توانید در بخش Software Center سایت cisco.com دانلود نمایید.
۱. بر روی Browse all کلیک کنید.
۲. مسیر Wireless > Mobile Internet > Policy Suite for Service Providers > Policy Suite for Mobile را دنبال کنید.
۳. با استفاده از پنل سمت چپ صفحه Policy Suite for Mobile نسخه به‌روزشده را دانلود کنید.

گزارش آسیب‌پذیری

۲ آسیب‌پذیری دسترسی نامعتبر به اینترفیس Cisco Policy Suite OSGi

یک آسیب‌پذیری در اینترفیس (Open Systems Gateway initiative (OSGi به یک مهاجم از راه دور اجازه می‌دهد بدون نیاز به تایید اعتبار به این اینترفیس دسترسی داشته باشد.
این آسیب‌پذیری ناشی از فقدان احراز هویت یا تایید اعتبار در این اینترفیس است. یک مهاجم می‌تواند با دسترسی مستقیم به اینترفیس OSGi امکان دسترسی یا تغییر هر فایلی که توسط فرایند OSGi قابل دستیابی است را فراهم می‌کند.
سیسکو به‌روزرسانی‌های نرم‌افزاری را که مربوط به این آسیب‌پذیری است، منتشر کرده است.

محصولات آسیب‌پذیر

نرم‌افزار Cisco Policy Suite نسخه ۱۸،۱،۰ و نسخه‌های پیش از آن تحت تاثیر این آسیب‌پذیری قرار دارند. مدیران شبکه می‌توانند با استفاده از دستور about.sh در CLI دستگاه نسخه فعلی Cisco Policy Suite اجرا شده بر روی آن را بیابند. در مثال زیر نسخه ۱۸،۰،۰ اجرا می‌شود.

```
[root@installer ~]# about.sh
Cisco Policy Suite - Copyright (c) 2015. All
rights reserved.
CPS Multi-Node Environment
CPS Installer Version - 18.0.0
CPS Core Versions
----------------------------
CPS Patch History
----------------------------
No patches have been applied
```

بحرانی (Critical)	Cisco Policy Suite OSGi Interface Unauthenticated Access Vulnerability
عنوان	آسیب‌پذیری دسترسی نامعتبر به اینترفیس Cisco Policy Suite OSGi
شناسه آسیب‌پذیری	CVE0377-2018-
CVSS Score	Base - 9.8
نسخه	1.0
شناسه باگ‌های سیسکو	CSCvh18017
تاثیر	آسیب‌پذیری دسترسی نامعتبر (Unauthenticated Access)
تاریخ انتشار	2018 July 16:00 18 GMT

راه‌حل

سیسکو ابتدا این آسیب‌پذیری را در نسخه ۱۸،۲،۰ نرم‌افزار Cisco Policy Suite رفع کرده است. این نرم‌افزار را می‌توانید در بخش Software Center سایت cisco.com دانلود نمایید.
۱. بر روی Browse all کلیک کنید.
۲. مسیر Wireless > Mobile Internet > Policy Suite for Service Providers > Policy Suite for Mobile را دنبال کنید.
۳. با استفاده از پنل سمت چپ صفحه Policy Suite for Mobile نسخه به‌روزشده را دانلود کنید.

منبع:

جدیدترین بدافزارها

۱۰ بدافزار مخرب در ماه ژوئن ۲۰۱۸

■ هادی گلباغی

آمار مربوط به رشد بدافزارها در ماه ژوئن سال ۲۰۱۸ بر خلاف ماه آوریل دارای روند صعودی بوده است. در بین ۱۰ بدافزار با رشد بالا رشد قابل توجهی در فعالیت‌های WannaCry و Emotet وجود داشته است که در حدود ۹۵ درصد افزایش فعالیت ۱۰ بدافزار با رشد بالا به دلیل رشد این دو خانواده بوده است. همچنین این رشد قابل توجه باعث افزایش ۶۰ درصدی آمار کل بدافزارها نیز شده است. در ماه ژوئن ۲۰۱۸ ، نمودار مربوط به Malspam دارای روند صعودی شدیدی در فعالیت‌ها نسبت به سه ماه گذشته بوده است. از ماه می تا ژوئن Malspam رشد ۱۴۷ درصدی در فعالیت‌ها را داشته است که بیشتر به دلیل رشد قابل توجه WannaCry و Emotet بوده است.

نمودار فعالیت‌ها در این ماه بیشتر نشانگر فعالیت‌های غالب Malspam است. در بین ۱۰ بدافزار با رشد بالا هیچ موردی از Malvertising وجود نداشته است. فعالیت‌های Zeus در ماه ژوئن کاهش داشته است که منجر به روند نزولی در چندین بردار شده است. سطح فعالیت‌ها در نمودار Dropped پایین بوده است و مانند سه ماه گذشته در این ماه نیز کاهش فعالیت را تجربه کرده است.

خانواده‌های مخربی که در این ماه بسیار مطرح بوده‌اند به صورت زیر است :

Dropped : این بدافزارها از بدافزارهای موجود بر روی سیستم و یا از کیت‌های بهره‌برداری، استفاده می‌کنند.

Malvertising : بدافزارهایی که برای تبلیغات مخرب استفاده می‌شوند.

Multiple : بدافزارهایی که در حال حاضر دارای حداقل دو بردار خواهند بود.

Malspam : ایمیل‌های ناخواسته که کاربر را ترغیب به دانلود بدافزار از سایت‌های مخرب یا باز کردن پیوست‌های مخرب ایمیل‌ها می‌کند.

۱۰ بدافزاری که بیشترین تخریب را در ماه ژوئن سال ۲۰۱۸ داشته‌اند :

۱. WannaCry : یک نوع باج‌افزار است که به صورت کرم‌گونه با استفاده از آسیب‌پذیری EternalBlue تکثیر شده و سیستم‌ها را آلوده می‌کند و نسخه‌های مختلفی از آن از سال ۲۰۱۷ منتشر شده است.

۲. Emotet : یک تروجان ماژولار است که بیشتر برای دانلود بدافزارهای بانکی مورد استفاده است و آلوده‌سازی اولیه آن در اغلب موارد با استفاده از هرزنامه‌های تبلیغاتی و ایمیل‌های فیشینگ است.

۳. Kovter : یک تروجان است که بیشتر از طریق پیوست‌های هرزنامه‌های تبلیغاتی که حاوی ماکروهای مخرب هستند منتشر می‌شوند.

۴. Zeus : یک تروجان بانکی ماژولار است که از سال ۲۰۱۱ که نسخه اولیه آن منتشر شده بسیاری از بدافزارهای دیگر بر مبنای آن نوشته شده‌اند.

۵. Mirai : یک نوع بدافزار بات نت شناخته شده است که به صورت خاص برای دستگاه‌های IOT به منظور حملات منع سرویس توزیع شده به صورت گسترده تکثیر شده است.

۶. NanoCore : یک نوع تروجان دسترسی از راه دور یا RAT است که از طریق هرزنامه‌های تبلیغاتی در قالب فایل اکسل منتشر شده است.

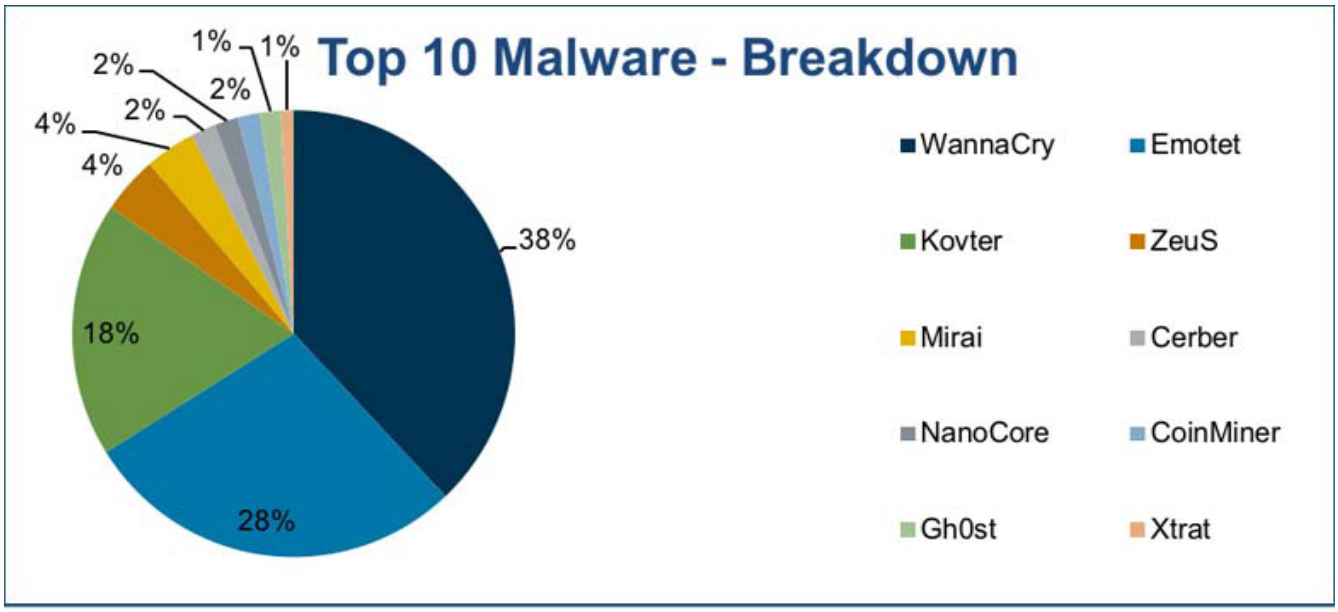
۷. Cerber : یک باج‌افزار است که قادر به رمزنگاری فایل‌ها در حالت آفلاین بوده و خود را از طریق افزونه‌هایی در سیستم به روز کرده و ماندگار می‌کند.

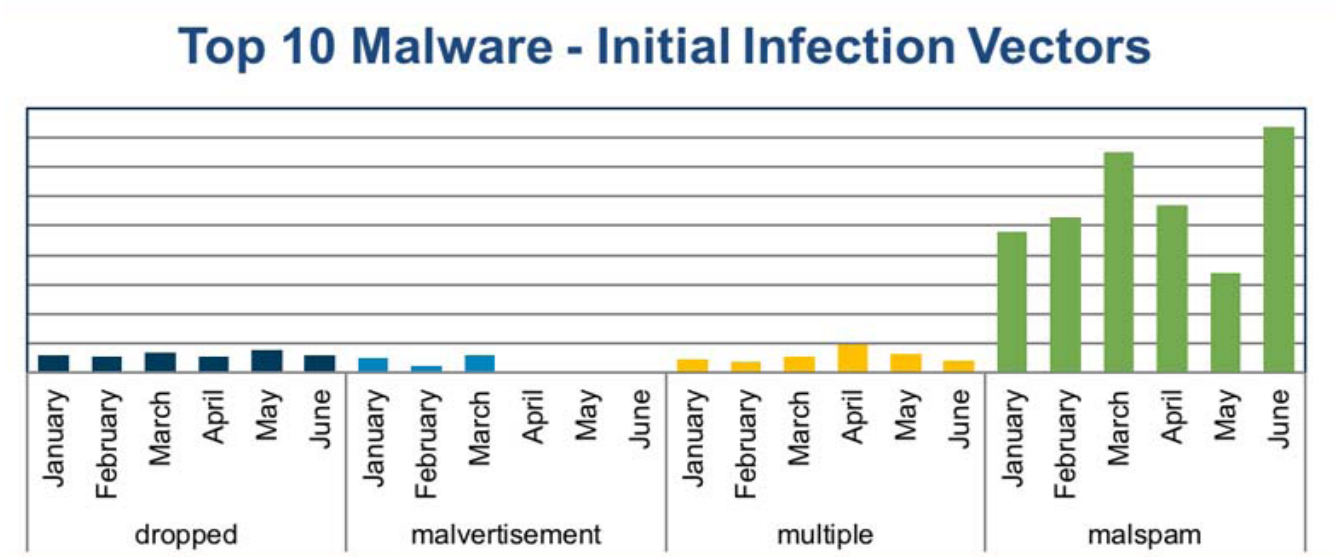
۸. Ch•st : یک تروجان دسترسی از راه دور یا RAT است که برای کنترل سیستم‌های آلوده استفاده می‌شود.

۹. CoinMiner : برای استخراج ارز مجازی که معمولاً بیت کوین است مورد استفاده می‌باشد و اخیراً تکثیر آن با رشد بالایی همراه بوده است.

۱۰. Xtrat : یک RAT است که از طریق هرزنامه‌های تبلیغاتی تکثیر شده و قابلیت دریافت دستوراتی برای مدیریت فایل مانند دانلود، آپلود و اجرای فایل‌ها و مدیریت ریجستری را دارد.

منبع :





بررسی تخصصی بدافزار Emotet و روند تکثیر آن

■ هادی گلباغی

تاکنون در سال ۲۰۱۸ تعداد زیادی از اسپم‌های مخرب (malspam) از بدافزار Emotet استفاده کرده‌اند و همواره در آمارها بالاترین نرخ شیوع را در سال ۲۰۱۸ داشته‌اند. در سال ۲۰۱۸ شرکت‌ها و مراکز امنیتی گزارش‌های متعددی را در ارتباط با بدافزار Emotet منتشر کرده‌اند که می‌توان به گزارش Symantec در ۱۸ جولای، US-CERT در ۲۰ جولای، Palo Alto Networks در ۱۸ جولای و MalFind در ۲۳ جولای اشاره کرد. همچنین می‌توان هشتگ‌های # Emotet را در شبکه‌های اجتماعی به وفور دید. در شکل ۱ دو نمونه از وقایع منجر به آلودگی توسط Emotet نشان داده شده است.

بدافزار Emotet یک تروجان پیشرفته ماژولار بانکی است که در اکثر موارد به عنوان یک دانلود کننده برای تروجان‌های بانکی دیگر مورد استفاده است. این بدافزار یکی از پر هزینه‌ترین و مخرب‌ترین بدافزارها برای سازمان‌های دولتی و شرکت‌های خصوصی با هر اندازه بزرگی است. ویژگی‌های کرم‌گونه این بدافزار باعث شده که به سرعت در سطح شبکه آلودگی ایجاد کند که مبارزه با آن را بسیار دشوار کرده است. با بررسی‌هایی که انجام شده هزینه‌های ناشی از آلودگی سازمان‌های بزرگ دولتی توسط Emotet بالغ بر یک میلیون دلار بوده است.

با تحلیلی اولیه در ارتباط با بررسی ترافیک Emotet مواردی قابل تامل مشاهده می‌شود. در ادامه توضیحاتی را در مورد تحلیل اولیه خواهیم دید. شکل ۲ این موضوع را نشان می‌دهد و در جدول ۱ توضیح فایل‌های بدازفار Emotet و Hash SHA۲۵۶ مربوط به هر کدام نشان داده شده است.

در ادامه Domain ها، IP آدرس‌ها و URLهایی که در ترافیک آلوده وجود دارند نشان داده خواهند شد.

ترافیک آلوده اولیه :

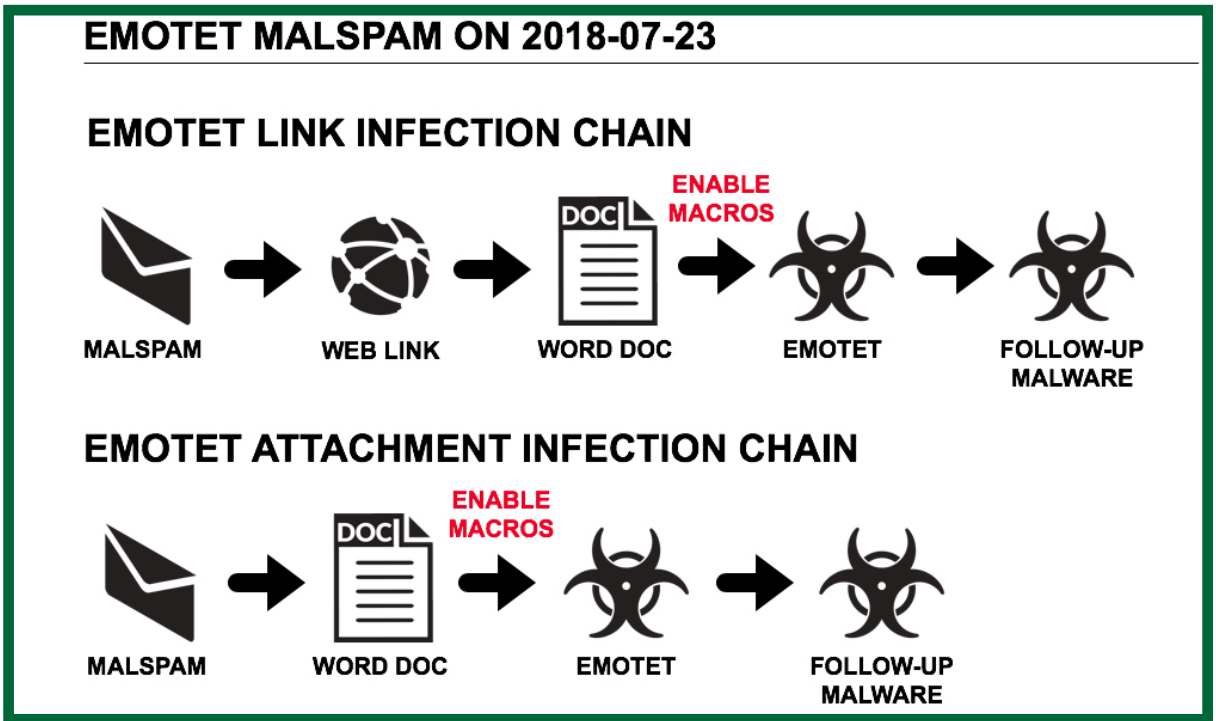
```
64.71.36.11 port 80 - misico.com - GET /sites/US/Client/Invoice2018-23-07-0361376097-/
198.71.233.87 port 80 - www.ocyoungactors.com - GET /NzGucd/
```

ترافیک Emotet پس ازآلوده شدن:

```
 24.40.239.62 port 24.40.239.62 - 80 - GET /whoami.php
 24.40.239.62 port 24.40.239.62 - 80 - POST /
 46.105.131.69 port 46.105.131.69:8080 - 8080 - GET /
 47.201.208.154 port 47.201.208.154:443 - 443 - GET /
 70.183.113.54 port 70.183.113.54:8443 - 8443 - GET /
 71.8.1.188 port 71.8.1.188 - 80 - GET /
 71.71.3.84 port 71.71.3.84 - 80 - GET /
 71.165.252.144 port 71.165.252.144:990 - 990 - GET /
 71.177.184.128 port 71.177.184.128:990 - 990 - GET /
 71.244.60.231 port 71.244.60.231:4143 - 4143 - GET /
 73.27.38.128 port 73.27.38.128 - 80 - GET /
 73.178.169.180 port 73.178.169.180 - 80 - GET /
 79.78.160.225 port 79.78.160.225 - 80 - GET /
 96.95.159.237 port 96.95.159.237 - 80 - GET /
 96.95.159.237 port 96.95.159.237:8080 - 8080 - GET /
 108.170.54.171 port 108.170.54.171:8080 - 8080 - GET /
 118.244.214.210 port 118.244.214.210:443 - 443 - GET /
 129.89.95.110 port 129.89.95.110 - 80 - GET /
 129.89.95.241 port 129.89.95.241 - 80 - GET /
 149.62.173.247 port 149.62.173.247:8080 - 8080 - GET /
 186.85.246.153 port 186.85.246.153:8080 - 8080 - GET /
 190.147.41.94 port 190.147.41.94:443 - 443 - GET /
 199.120.92.245 port 199.120.92.245 - 80 - GET /
 216.21.168.27 port 216.21.168.27:443 - 443 - GET /
```

تلاش‌ها برای برقراری ارتباط TCP از طریق Emotet که پاسخی از سرور دریافت نشد:

```
 12.238.114.130 port 80
 27.50.89.209 port 8080
 46.105.131.87 port 80
 47.150.11.161 port 7080
 50.92.101.60 port 465
 71.214.17.130 port 443
 73.183.145.218 port 8443
 78.47.182.42 port 8080
 80.11.163.139 port 8080
```



شکل ۱. دو نمونه از وقایع منجر به آلودگی توسط Emotet

```
108.246.196.73 port 80
118.190.60.27 port 20
146.185.170.222 port 8080
157.7.164.23 port 8080
192.42.116.41 port 443
194.88.246.242 port 443
194.150.118.8 port 443
199.119.78.9 port 443
199.119.78.38 port 443
222.214.218.192 port 4143
```

ترافیک Zeus Panda Banker :

```
185.216.35.22 port 443 - thevisitorsfilm.top - SSL/TLS traffic
```

بررسی تخصصی این بدافزار نشان می‌دهد که Emotet یک تروجان بانکی چندریختی است که قادر است از شناسایی شدن توسط روش‌های مبتنی بر امضا فرار کند. این بدافزار با استفاده از تکنیک‌های متعدد برای حفظ و پایداری خود تلاش می‌کند که شامل ایجاد کلیدهایی در ریجستری و سرویس‌ها برای شروع خودکار هم می‌شود. این بدافزار با استفاده از DLL هایی به طور مداوم تکامل پیده کرده و به‌روزرسانی در آن انجام می‌شود. به علاوه این‌که به دلیل طراحی پیشرفته آن، اگر در محیطهای مجازی برای شناسایی اجرا گردد قادر است در این نوع محیطها فعالیت‌های مخرب خود را انجام ندهد تا شناسایی نگردد و معمولاً روش‌های تحلیل پویا در مقابل آن شکست خواهند خورد.

تروجان Emotet از طریق Malspam (ایمیل‌هایی حاوی پیوست‌ها و یا لینک‌های آلوده) تکثیر شده که برای افراد این ایمیل‌ها آشنا هستند. آلودگی‌های اولیه به این بدافزار زمانی اتفاق افتاد که کاربر یک لینک، فایل PDF و یا فایل Word که دارای ماکرو مخرب است را باز کرده که شامل Malspam بوده است. پس از دانلود شدن، سعی اولیه این بدافزار در ماندگاری در سیستم و سپس انتشار گسترده در سطح شبکه محلی با استفاده از ماژول‌هایی که در آن طراحی شده است، خواهد بود. در شکل ۳ ایمیل مخرب شامل Emotet نشان داده شده است. همچنین فرآیند آلوده شدن توسط بدافزار Emotet در شکل ۴ نشان داده شده است.

در حال حاضر با بررسی انجام گرفته این بدافزار شامل پنج ماژول پخش‌کننده شناخته‌شده به نام‌های NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper و یک credential enumerator است.

NetPass.exe یک ابزار شناخته‌شده توسعه داده شده توسط Nirsoft است که برای بازیابی تمامی رمزهای عبور شبکه ذخیره شده بر روی سیستم کاربر است. این ابزار همچنین قادر است که رمزهای عبور ذخیره شده در فایل اعتباری را بر روی یک حافظه جانبی بازیابی کند.

جدول ۱. توضیح‌فایل‌های Emotet و Hash SHA۲۵۶ مربوط به هر کدام

توضیح فایل	فایل Word doc دانلود شده همراه با ماکرو مخرب که Emotet را نصب می‌کند.
SHA256 Hash	9914881d35a7fa7ce6f9ec06d4e5c19f 12c6916a57fcc4facbb28f144e921283
توضیح فایل	فایل دودویی بدافزار Emotet بازیابی شده توسط ماکرو word
SHA256 Hash	83d54beb3fdecfc7bcb0eb048aa4634a5 e4208dc0a3067a35d2cfb4598cb99b2
توضیح فایل	Zeus Panda Banker
SHA256 Hash	b1ebf3d44d496ee574831266474b10b55 c06e30aea56d41ac8830ba2b28f7a0f

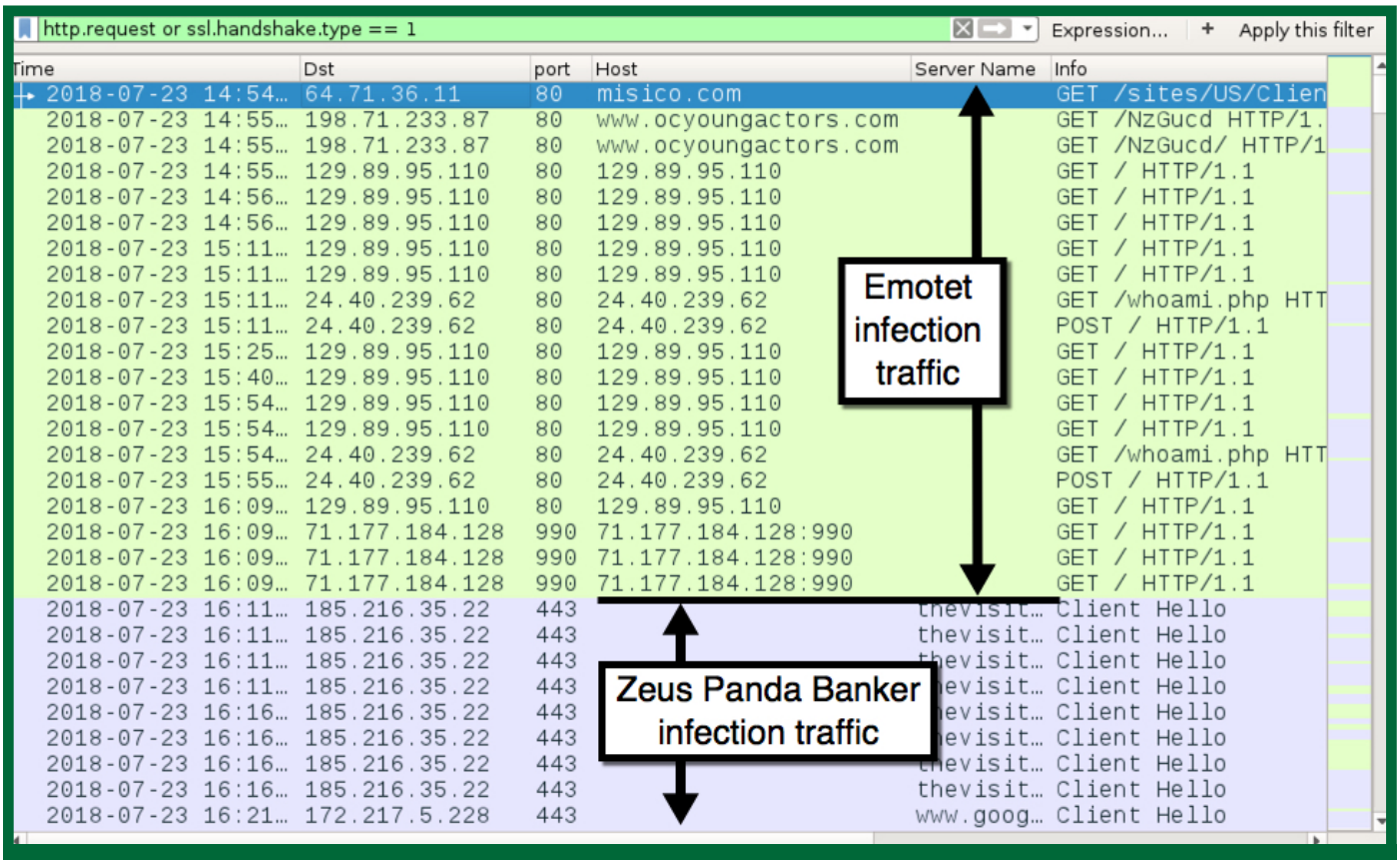
Outlook scraper یک ابزار است که نام‌ها و آدرس‌های ایمیل را از حساب‌کاربری Outlook قربانی استخراج کرده و از این اطلاعات برای ارسال ایمیل‌های فیشینگ برای حساب‌های دیگران استفاده می‌کند.

WebBrowserPassView یک ابزار بازیابی رمز عبور است که رمزهای عبور ذخیره شده در Internet Explorer, Mozilla Firefox, Google Chrome, Safari و Opera را استخراج کرده و آن را برای ماژول credential enumerator ارسال می‌کند.

Mail PassView ابزاری برای بازیابی رمز عبور است که رمز عبور و اطلاعات حساب کاربری ایمیل‌های مختلف کاربر مانند Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail و Gmail را دریافت کرده و آن را برای ماژول credential enumerator ارسال می‌کند.

Credential enumerator یک ابزار خودکار استخراج فایل‌های RAR است که شامل دو کامپوننت bypass component و service component می‌باشد. کامپوننت bypass component برای شمارش (enumeration) منابع شبکه و پیدا کردن درایوهای اشتراک‌گذاری قابل نوشتن که از (SMB (Server Message Block استفاده می‌کنند و یا سعی در brute force اکانت‌های کاربران که شامل اکانت ادمین نیز هست می‌شود. هنگامی‌که یک سیستم پیدا شد، بدافزار Emotet سرویس کامپوننت را بر روی سیستم اجرا کرده که Emotet را درون دیسک می‌نویسد. دسترسی emotet به SMB می‌تواند منجر به آلودگی کل دامنه شود.

برای حفظ و ماندگاری در سیستم، Emotet کدی را در Explorer.exe و پروسس‌های در حال اجرای دیگر تزریق می‌کند. همچنین می‌تواند داده‌هایی را ارسال کند که شامل اطلاعات حساس، نام سیستم، موقعیت مکانی و نسخه سیستم‌عامل و ارتباط از راه دور با سرور C&C برقرار گردد که معمولاً یک دامنه ۱۶ حرفی است که با .eu ختم می‌شود. هنگامی‌که Emotet یک ارتباط با C&C برقرار می‌کند گزارش‌هایی از آلودگی جدید،



شکل ۲. ترافیک فیلتر شده ویندوز آلوده شده توسط Emotet با ابزار Wireshark

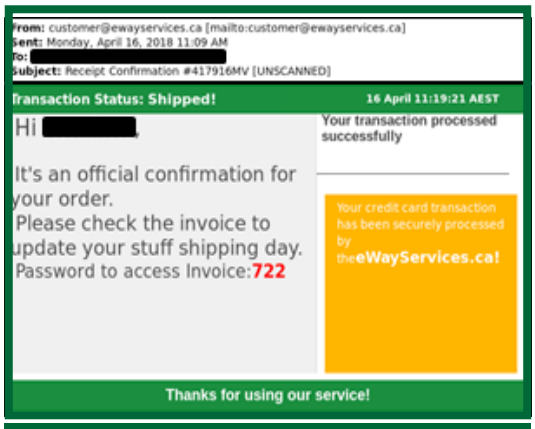
منابع:

داده‌های پیکربندی دریافتی، دانلودها و فایل‌های اجرایی، دستورات دریافتی و داده‌های آپلودی برای سرور C&C ارسال می‌شود.

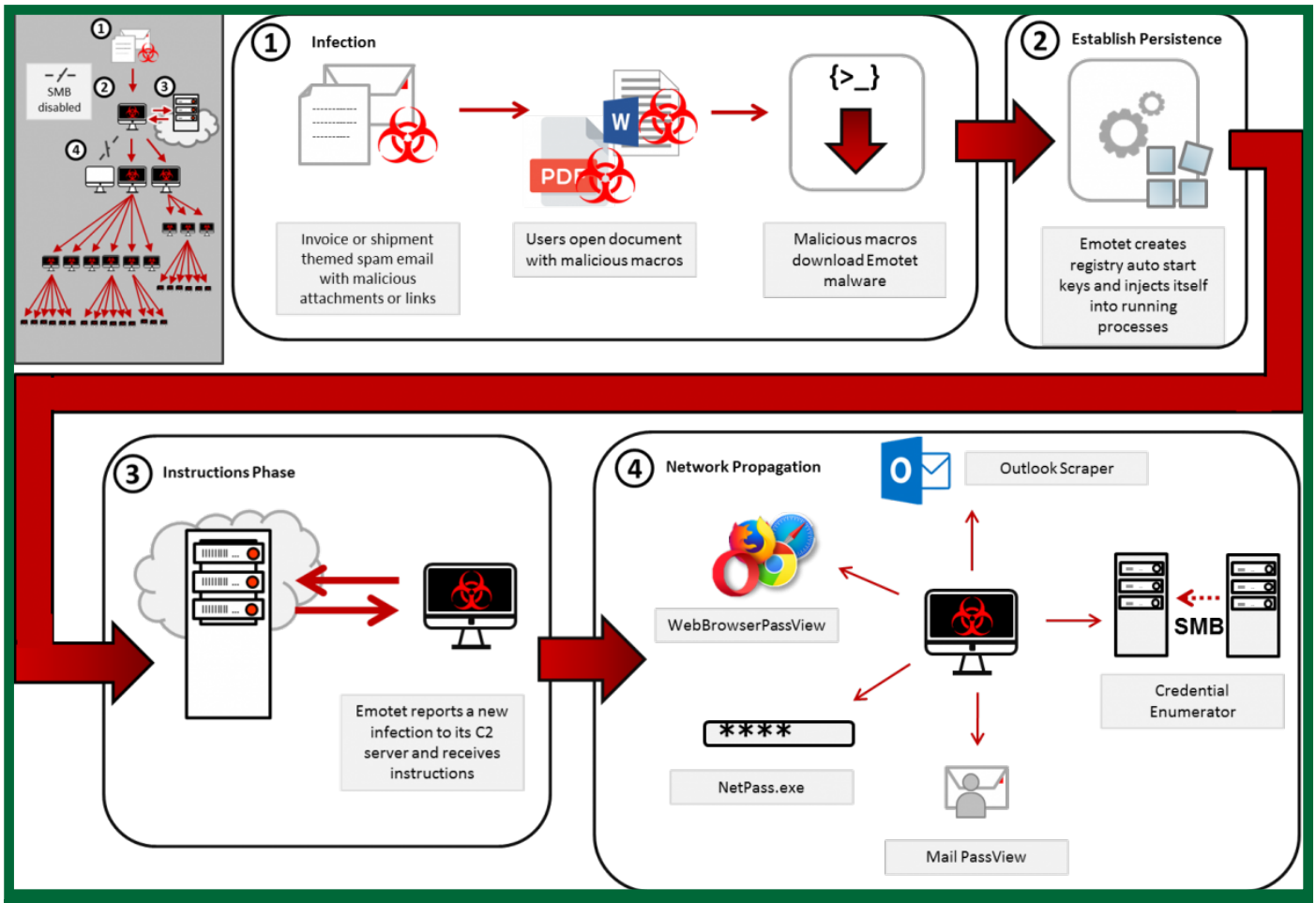
مستندات emotet معمولاً در مسیرهای دلخواه مانند AppData\Local و AppData\Roaming مستقر شده است. این مستنداتِ معمولاً به نام فایل‌های قابل اجرای شناخته شده هستند. ماندگاری آن معمولاً به وسیله زمانبندی وظایف و یا کلیدهای ریجستری انجام می‌شود. به علاوه اینکه Emotet به صورت راندوم نام فایل‌ها را در دایرکتوری ریشه سیستم عوض کرده که به صورت سرویس ویندوز اجرا شوند. وقتی که این بدافزار اجرا می‌شود این سرویس‌ها سعی در انتشار آن به وسیله قابلیت اشتراک‌گذاری دارند. در شکل ۵ نمونه نام فایل‌ها، مسیرها، کلیدهای ریجستری و ریشه دایرکتوری‌های سیستم نشان داده شده‌اند.

در نهایت بررسی‌های انجام گرفته بر روی بدافزار Emotet نشان می‌دهد که تاثیرات این تروجان بسیار منفی و مضر بوده است و شامل موارد زیر می‌شود:

* از دست دادن موقتی و یا دائمی اطلاعات حساس
* اختلال در روند فعالیت‌های روتین
*زیان‌های مالی برای بازگرداندن سیستم‌ها و فایل‌ها
* آسیب‌های احتمالی به شهرت برند و سازمان



شکل ۳.ایمیل مخرب شامل Emotet



شکل ۴.فرآیند آلوده شدن توسط Emotet

Example filenames and paths:

C:\Users\<username>\AppData \Local\Microsoft\Windows\shedaudio.exe
C:\Users\<username>\AppData\Roaming\Macromedia\Flash Player\macromedia\bin\flashplayer.exe

Typical Registry Keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

System Root directories:

C:\Windows\11987416.exe
C:\Windows\System32\46615275.exe
C:\Windows\System32\shedaudio.exe
C:\Windows\SysWOW64\f9jwqSbS.exe

شکل ۵. نمونه نام فایل‌ها، مسیرها، کلیدهای ریجستری و ریشه دایرکتوری‌های سیستم

پنج بدافزار شایع در ماه گذشته

■ هادی گلباغی

۱

نام بدافزار شناسایی شده :
PUA.Win.Adware.Mywebsearch::1201

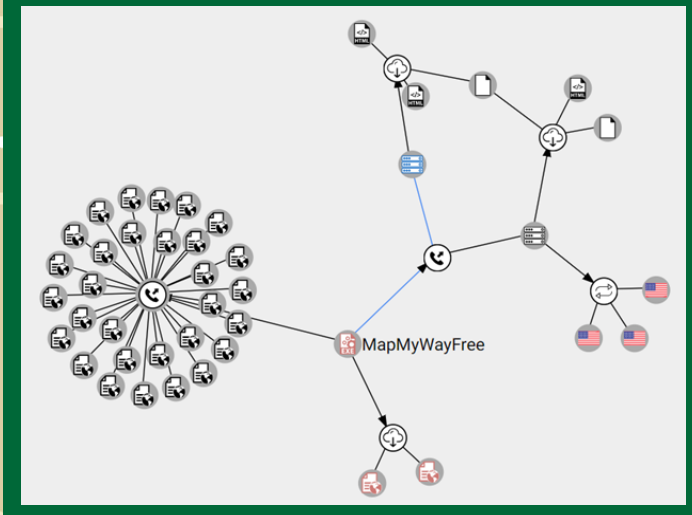
اطلاعاتی مختصر از بدافزار:

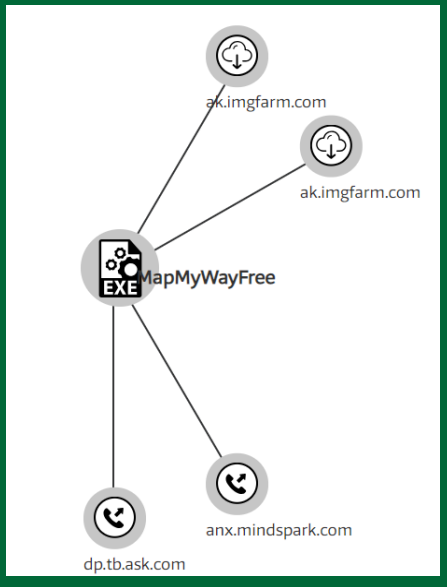
نام فایل	mapmywayfree.7bbf20dc02d24710bb860586aabc073e.exe
نوع بدافزار	Trojan
SHA 256	3b6668948967c873a19ec7e1bc1e700652edf33f8d8cd53f87832797af99f99c
MD5	3c9f59ab554831d75044daa402703af83c9
نوع فایل	Win32 EXE
حق نشر	MapMyWay Free
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win32 Executable MS Visual C++ (generic) (%41) Win64 Executable (generic) (%36.3) Win32 Dynamic Link Library (generic) (%8.6) Win32 Executable (generic) (%5.9) OS/2 Executable (generic) (2.6%)
حجم فایل	369.45 KB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Avast	Win32:UnwantedSig [PUP]
AVG	Win32:UnwantedSig [PUP]
Avira	PUA/MyWebSearch.Gen
Comodo	CloudScanner.Trojan.Gen
Drweb	Adware.MyWebSearch.120
ESET-NOD32	Win32/Toolbar.MyWebSearch.BA potentially unwanted
GData	Win32.Adware.Mindspark.E
Kaspersky	not-a-virus:HEUR:AdWare.Win32.Agent.gen
Microsoft	PUA:Win32/MyWebSearch
Sophos AV	Generic PUA LN (PUA)
TrendMicro	TROJ_GEN.R002H0CGM18
ZoneAlarm	not-a-virus:HEUR:AdWare.Win32.Agent.gen

گراف ارتباطات مربوط به بدافزار:





۲

نام بدافزار شناسایی شده :

W32.Generic:Gen.21gl.1201

اطلاعاتی مختصر از بدافزار:

نام فایل	mf2016341595.exe
نوع بدافزار	Trojan
SHA 256	15716598f456637a3be3d6c5ac91266142266a9910f6f3f85cfd193ec1d6ed8b
MD5	799b30f47060ca05d80ece53866e01cc
نوع فایل	Win32 EXE
حق نشر	نامشخص
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win64 Executable (generic) (%61.7) Win32 Dynamic Link Library (generic) (%14.7) Win32 Executable (generic) (%10) OS/2 Executable (generic) (%4.5) Generic Win/DOS Executable (%4.4)
حجم فایل	939 KB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
AegisLab	Ml.Attribute.Gen!c
ClamAV	Win.Trojan.Agent0-6583322-
CrowdStrike Falcon	malicious_confidence_%100 (W)
McAfee	BehavesLike.Win32. Downloader.dh
Rising	Trojan.Win32.Ransom.dz (CLASSIC)
Sophos AV	heuristic
TrendMicro	Suspicious_GEN.F47V0723

نام بدافزار شناسایی شده :
PUA.Osx.Trojan.Mackeeper::1201

اطلاعاتی مختصر از بدافزار:

نام فایل	bfa9b296d648a5eac19e0d6bb23139e9104cfd55ee8a02cd1aa9d768ef398747~.x86
نوع بدافزار	Trojan
SHA 256	4bd61a7f2b1287e2c94973062b91ad075ce73637441982f426d269c527069015
MD5	5e414220b8e34fcfb2c315e772527a255e4
نوع فایل	Mach-O
حق نشر	MacKeeper Helper
Magic	Mach-O executable i386
TRiD	Mac OS X Mach-O 32bit Intel executable (%100)
حجم فایل	151.3 KB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Ad-Aware	Gen:Variant.Application.MAC.PazaCA.1
BitDefender	Gen:Variant.Application.MAC.PazaCA.1
ClamAV	Osx.Malware.Agent0-6456392-
DrWeb	Program.Mac.Unwanted.MacKeeper.315
eScan	Gen:Variant.Application.MAC.PazaCA.1
ESET-NOD32	a variant of OSX/Mackeeper.AR potentially unwanted
GData	Gen:Variant.Application.MAC.PazaCA.1
Sophos AV	Generic PUA PM (PUA)
Symantec	OSX.MacKeeper
TrendMicro	Suspicious_GEN.F47V0224

گراف ارتباطات مربوط به بدافزار:

۴

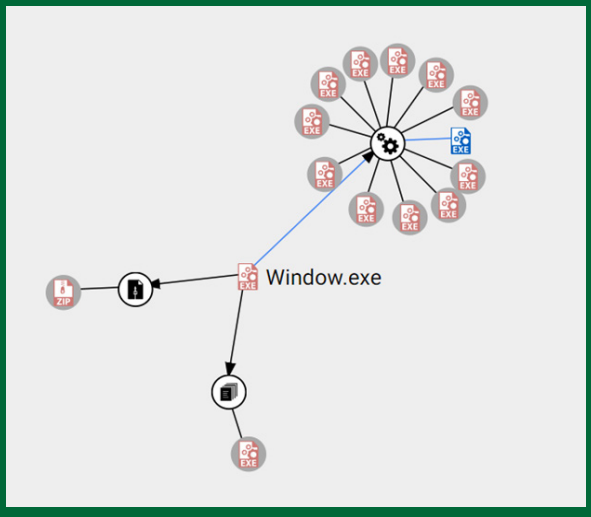
نام بدافزار شناسایی شده :
W32.GenericKD:Malwaregen.21il.1201
اطلاعاتی مختصر از بدافزار:

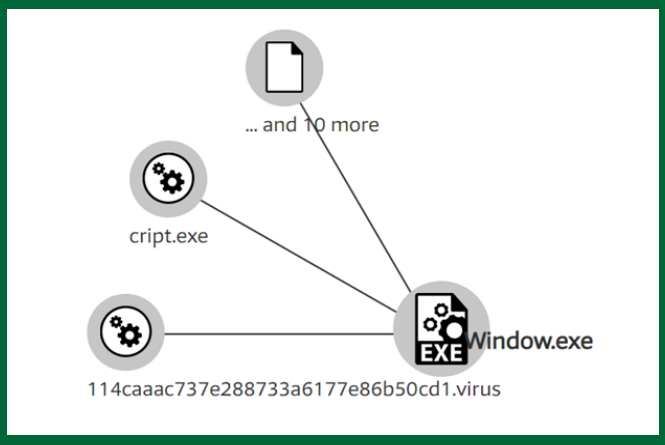
نام فایل	svchost (1).exe
نوع بدافزار	Trojan
SHA 256	d7d80bf3f32c20298cad1d59ca8cb4508bad43a9be5e027579d7fc77a8e47be0
MD5	d8461f2978de84045e7ad6bea7a60418
نوع فایل	Win32 EXE
حق نشر	نامشخص
Magic	PE+32 executable for MS Windows (console) Mono/.Net assembly
TRiD	Win64 Executable (generic) (%82) OS/2 Executable (generic) (%6) Generic Win/DOS Executable (%5.9) DOS Executable Generic (%5.9)
حجم فایل	4.63 MB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Ad-Aware	Application.CoinMiner.CE
BitDefender	Application.CoinMiner.CE
DrWeb	Trojan.Crossrider1.22656
eScan	Application.CoinMiner.CE
ESET-NOD32	a variant of Win64/CoinMiner. ER potentially unwanted
F-Secure	Application.CoinMiner.CE
Fortinet	Riskware/Generic
GData	Application.CoinMiner.CE
Kaspersky	not-a-virus:RiskTool.Win64. BitCoinMiner.irmr
McAfee	W64/CoinMiner
Microsoft	PUA:Win64/CoinMiner
Panda	Trj/CI.A
Sophos AV	Claymore's Cryptonote CPU Miner (PUA)
Symantec	Miner.Bitcoinminer
TrendMicro	Coinminer_MALREP.THDAAAH

گراف ارتباطات مربوط به بدافزار:





نام بدافزار شناسایی شده :

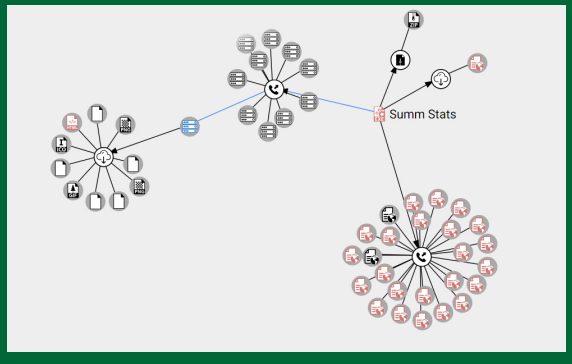
W32.GenericKD:Gen.21ij.1201

اطلاعاتی مختصر از بدافزار:

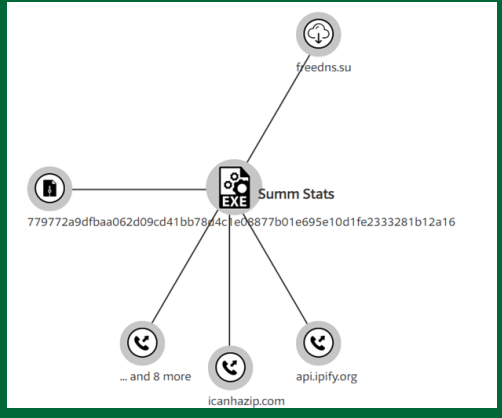
نام فایل	Summ Stats.exe
نوع بدافزار	Trojan
SHA 256	7a5495a7ac93598e62353e1f69f017ceeb66de2858737617f551161fc8aba542
MD5	f8605587f467ed5bc3d532088c170823f86
نوع فایل	Win32 EXE
حق نشر	KERT Srl
Magic	PE32 executable for MS Windows (GUI) Intel -32 80386bit
TRiD	Win32 Executable Microsoft Visual Basic %82.7) 6) Win32 Dynamic Link Library (generic) (%6.6) Win32 Executable (generic) (%4.5) OS/2 Executable (generic) (%2) Generic Win/DOS Executable (%2)
حجم فایل	320 KB

آنتی ویروس شناسایی کننده و نام بدافزار در این آنتی ویروس به صورت جدول زیر است.

نام آنتی ویروس	نام بدافزار
Ad-Aware	Trojan.GenericKD.40306076
Avast	Win32:Malware-gen
AVG	Win32:Malware-gen
Avira	TR/Kryptik.odanp
BitDefender	Trojan.GenericKD.40306076
eScan	Trojan.GenericKD.40306076
ESET-NOD32	a variant of Win32/Injector.DZJX
F-Secure	Trojan.GenericKD.40306076
GData	Trojan.GenericKD.40306076
Kaspersky	Trojan.Win32.Mansabo.bhq
McAfee	Artemis!F8605587F467
Microsoft	Trojan:Win32/Totbrick.H
Panda	Trj/RnkBend.A
Sophos AV	Mal/Generic-S
Symantec	Trojan.Gen.2
TrendMicro	TROJ_GEN.R004C0DG718
ZoneAlarm	Trojan.Win32.Mansabo.bhq



گراف ارتباطات مربوط به بدافزار:



منابع:

امنیت عمومی

امنیت در شبکه‌های اجتماعی

■ هادی گلباغی

فضای مجازی و شبکه‌های اجتماعی در سال‌های اخیر با سرعت بسیار بالایی در حال گسترش هستند و تاثیرات زیادی را در زندگی روزمره انسان‌ها گذاشته‌اند و بسیار از مردم، شخصیت‌ها و کسب و کارها هرکدام به نوعی با این شبکه‌ها در ارتباط هستند. ضریب نفوذ آن‌ها را می‌توان از جنبه‌های مختلفی بررسی کرد که چه ابعاد مثبت و منفی مختلفی داشته‌اند و این تاثیرات هر روز در ابعاد فرهنگی، اجتماعی، اقتصادی، سیاسی، امنیتی و دفاعی در عرصه ملی و بین‌المللی نمود بیشتری پیدا می‌کند. طبق بررسی‌هایی که انجام گرفته نزدیک به ۹۰ درصد از جمعیت کاربران آنلاین از شبکه‌های اجتماعی استفاده می‌کنند و آمارها نشان می‌دهد که دسترسی‌ها از دستگاه‌های مختلفی به اکانتی در شبکه اجتماعی انجام می‌گیرد و ۶۸ درصد کاربران در استفاده از شبکه‌های اجتماعی احساس ناامنی می‌کنند و طی گزارش‌هایی از نشت اطلاعات از شبکه‌های اجتماعی، ۱۴ درصد دستیابی غیر مجاز به اکانت‌ها گزارش شده است.

فضای مجازی ویژگی‌های مختلفی دارد که می‌توان به دسترسی جهانی و فرامرزی بودن، دستیابی آسان به آخرین اطلاعات، جذابیت و تنوع در عرضه، آزادی اطلاعات و ارتباطات، تعاملی بودن و ارتباط دو طرفه اشاره کرد. این فضا با تمام نکات مثبت اما نکاتی منفی نیز دارد که می‌توان قرار گرفتن در معرض اطلاعات نامناسب بر اساس سن، صفحات قمار و شرطبندی، تشویق به استفاده از سیگار و مشروبات الکلی و مواد مخدر، صفحات با موضوعات سو استفاده جنسی، ایجاد مشکلات مالی و قانونی و تجاوز به حریم خصوصی افراد اشاره کرد. نکته حائز اهمیت در خصوص فضای مجازی فرهنگ‌سازی صحیح و توجه به نکات امنیتی در شبکه‌های اجتماعی است که از جهات مختلفی می‌توان به آن نگاه کرد. در این مطلب توصیه‌هایی در ارتباط با حفظ امنیت در فضای مجازی و شبکه‌های اجتماعی به صورت عمومی بیان خواهند شد. بدیهی است که با رعایت این نکات تا حد زیادی کاربران در این فضا مصون خواهند ماند. در ادامه توصیه‌ها و نکاتی توضیح داده می‌شوند.

• تنظیمات امنیت و حریم خصوصی دستگاه‌ها را به طور مرتب بررسی کنید.

• تنظیمات حریم خصوصی حساب‌های کاربری را به صورت مداوم بررسی کنید.

• تمامی شبکه‌های اجتماعی تنظیماتی را برای حفظ حریم خصوصی و امنیت کاربران فراهم ساخته‌اند لذا بهتر است قبل از استفاده و قرار دادن اطلاعات شخصی در یك شبکه اجتماعی تنظیمات حفظ حریم خصوصی آن را بررسی کنید.

• از رمز عبور مناسب برای اکانت‌ها در شبکه‌های اجتماعی استفاده کنید. (برای اطلاعات بیشتر به شماره نخست مجله ویرا مراجعه کنید)

• رمزهای عبور اکانت‌های شبکه اجتماعی را با هیچ شخصی به اشتراک نگذارید.

• از سرویس‌های ایمیل امن و مطمئن برای ثبت نام در شبکه‌های اجتماعی بهره ببرید. همچنین به ایمیل‌هایی که از طریق یک شبکه اجتماعی خاص برای شما ارسال می‌شود دقت کنید.

• برای ایجاد حساب‌های کاربری در شبکه‌های اجتماعی از یک آدرس ایمیل و برای امور شخصی از آدرس ایمیل دیگری استفاده کنید.

• به اطلاعاتی که در شبکه‌های اجتماعی به اشتراک می‌گذارید دقت کنید. از به اشتراک گذاری اطلاعات مهم و حساس اکیداً خودداری فرمایید.

• دستگاه‌هایی که از حساب‌کاربری شبکه اجتماعی یا پیام رسان شما استفاده می‌کنند را مرتباً چک کنید. این کار با بررسی لیست نشست‌های فعال (Active Session list) و حذف نشست‌های ناشناس انجام شود.

• در شبکه‌های اجتماعی مواظب مهندسی اجتماعی باشید. در ادامه همین شماره در خصوص مهندسی اجتماعی توضیحاتی ارائه شده است.

• برای دسترسی به حساب کاربری شبکه‌های اجتماعی خود از کامپیوترهای عمومی و یا ارتباطات WIFI نا امن استفاده نکنید.

• اطلاعات بانکی، شماره‌های کارت‌های اعتباری و اطلاعات خصوصی خود را در پیام رسان‌ها و شبکه‌اجتماعی ذخیره یا انتقال ندهید.

• در کلیک بر روی لینک‌های مشکوک و مخرب در شبکه‌های اجتماعی دقت کنید.

• حدالامکان از چت با اشخاص ناشناس خودداری کنید و در صورت چت از ارسال هرگونه اطلاعات شخصی خودداری کنید.

• حدالامکان تنظیم موقعیت مکانی را غیر فعال کنید.

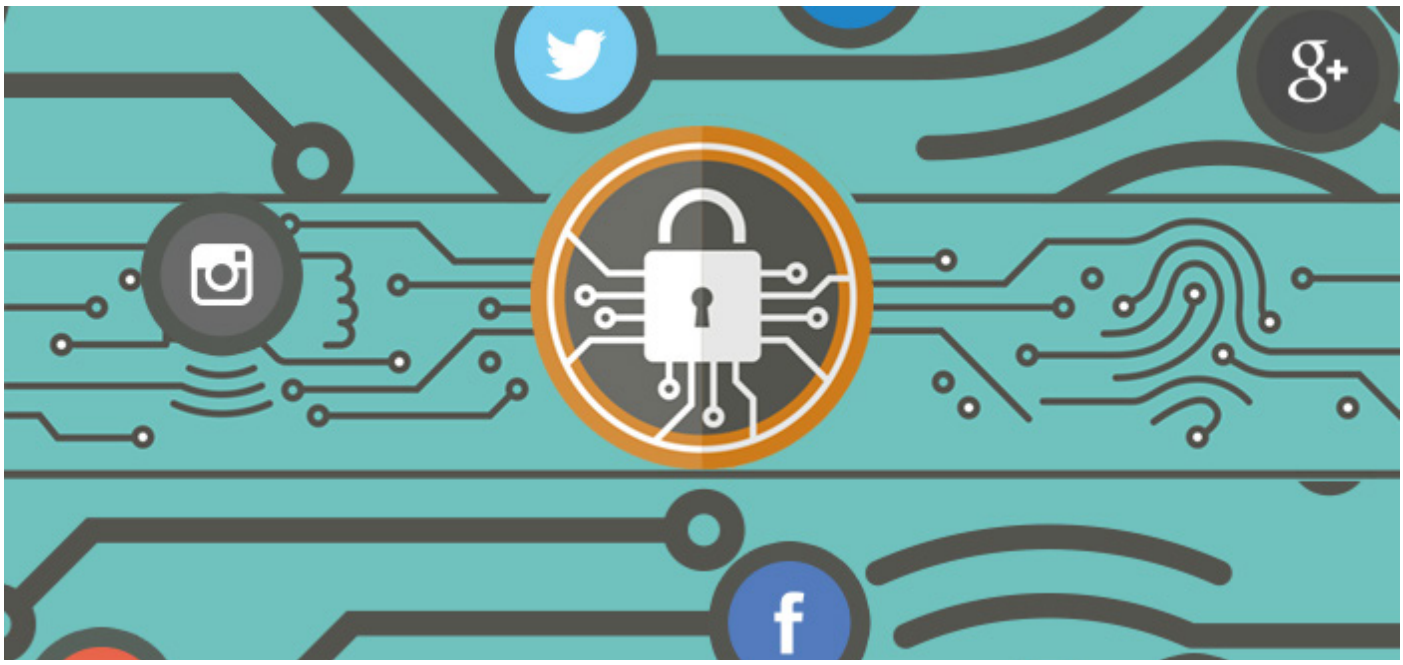
• بررسی کنید که چه اپلیکیشن هایی بر روی تلفن همراه‌تان به حساب‌های کاربری‌تان دسترسی دارند و آن را مدیریت کنید.

• افرادی با نیت سو همواره شبکه‌های اجتماعی را زیر نظر دارند تا ببینند چه زمانی چه کسانی به مسافرت می‌روند. از پست کردن عکس یا ویدیو همراه با موقعیت زمانی و مکانی جداً خودداری کنید.

• بهتر است از گذاشتن عکس‌هایی با محتوای نامناسب در پروفایل خود خودداری کنید. همچنین در بخش بیوگرافی نیز اطلاعاتی شخصی و خصوصی را قرار ندهید.

• عضو شدن در گروه‌ها، پیج‌ها و کانال‌ها لازم است با دقت بیشتری انجام گیرد.

• توصیه می‌شود رمز عبور یا احراز هویت دو مرحله‌ای (Two Step Verification) فعال شود.



مهندسی اجتماعی

■ هادی گلباغی

مهندسی اجتماعی یا Social Engineering چیست؟

در مهندسی اجتماعی فعالیتی انجام گرفته تا بستری فراهم گردد که با بهره‌برداری از روان‌شناسی انسانی بدون نفوذ یا استفاده از تکنیک‌های هک فنی برای دسترسی به سازمان‌ها، سیستم‌ها یا داده‌ها که بسیار نیز مورد استفاده است. این فعالیت‌ها هم بسیار پیچیده و هم بی‌نهایت ساده است. مهندسي اجتماعي در واقع به معناي كار روي يك شخص، با هدف ترغيب وي به انجام كارهايي براي حصول فرد ترغيب‌كننده به اهداف مدنظر براي انجام كاري خاص تعريف مي‌شود. نفوذ به افراد بسيار آسان‌تر از نفوذ به سازمان‌ها و سيستم‌ها است و مهندسي اجتماعي از ضعيف‌ترين اتصال در خطوط دفاعي امنيت اطلاعات هر سازمان، يعني نيروي انساني بهره‌گيري مي‌نمايد. ساده‌ترين مثالی که در این مورد می‌توان گفت این است که یک مهندس اجتماعی به جای تلاش برای یافتن یک آسیب‌پذیری نرم افزاری، با تظاهر به اینکه یک شخص پشتیبان IT است، تلاش می‌کند تا یک یا چند کارمند را به منظور افشای رمز عبور خودشان فریب دهد. طبق آمار ۲۹ درصد از نفوذها توسط تاکتیک‌های مهندسی اجتماعی انجام می‌شود. باید توجه داشت که مهندسی اجتماعی لزوماً فنی نیست و لازم نیست تا یک فرد متخصص یا هکر به شما حمله کند پس باید به محیط اطراف آگاه بود چرا که هر یک از افراد جامعه می‌تواند نقش یک مهاجم را ایفا کند. همچنین باید توجه داشت که در مهندسی اجتماعی مهاجم شما را در حالت‌های خاص روانی قرار می‌دهد یعنی در حالت‌هایی مانند اضطراب، هیجان، ترس و به صورت کلی در حالات خاص روانی قرار می‌دهد تا تمرکز و توان تصمیم‌گیری شما را کاهش دهد. همچنین این حملات به صورت فریبنده انجام می‌گیرند و در اکثر موارد پیشنهاداتی بسیار پر سود و جذاب ارائه می‌کنند.

استفاده از روش‌های مختلف مهندسی اجتماعی بسیار شایع است و در ادامه روش‌های مختلف آن بررسی شده و توصیه‌هایی برای مقابله با آن‌ها بیان می‌شود.

انواع حملات مهندسی اجتماعی به صورت زیر خواهد بود:

• فیشینگ (Phishing): طبق بررسی‌های انجام گرفته فیشینگ رایج‌ترین نوع مهندسی اجتماعی است. در این نوع حمله مهاجم وب‌سایت یا پورتال پشتیبانی یک ارگان دولتی، بانکی،شرکت، سازمان مشهور را از نظر رابط کاربری یا UI بازسازی می‌کند و لینک آن را از طریق روش‌های مختلفی از قبیل ایمیل، تبلیغات و یا شبکه‌های اجتماعی به صورت گسترده ارسال می‌کند. افراد با مراجعه به این وب‌سایت و مشاهده ظاهر شبیه‌سازی شده آن از واقعیت ماجرا اطلاعی ندارند و به منظور خرید یا هر فعالیت دیگری اطلاعات شخصی و حتی اطلاعات کارت اعتباری و بانکی خود را به خطر می اندازند. همچنین در ایمیل‌های فیشینگ مهاجم تظاهر می‌کند که ایمیل‌ها از طرف دوست، همکار، موسسه و ... ارسال شده‌اند اما هدف آن‌ها به دست آوردن اطلاعات کاربر است و از شما می‌خواهد یا به ایمیل پاسخ دهید و یا بر روی لینکی کلیک کرده و یا پیوست ایمیل را باز کنید. بررسی‌ها نشان می‌دهد که حساب‌هایی که هدف این حمله هستند شامل سرویس‌های مالی ۳۷ درصد، پورتال‌های جهانی اینترنت ۲۶ درصد، وب‌سایت‌های شبکه‌های اجتماعی ۱۷ درصد و ۲۰ درصد به سایر بسترها اختصاص دارد. باید توجه داشت که ۹۱ درصد حمله‌های پیشرفته با یک ایمیل هدف‌دار شروع می‌شوند و ایمیل‌های فیشینگ هدف‌دار را مدنظر قرار داد.

•ویشینگ یا Voice Phishing: فیشینگ صوتی به معنی فریب دادن کاربر از طریق تماس تلفنی و گرفتن اطلاعات مهم و حیاتی از قربانی است. مهندسین اجتماعی می‌توانند بر هر بستری انجام گیرد اما بسیاری راه قدیمی را ترجیح می‌دهند و از تلفن استفاده می کنند. بانک‌های بریتانیا در سال ۲۰۱۴ در حملات ویشینگ ۲۱ میلیون دلار را از دست داده‌اند.

• فیشینگ از طریق پیام کوتاه یا SMS Phishing : این روش نیز سال‌هاست مورد استفاده است و طبق برآوردها روزانه ۲۰۰ میلیون پیام کوتاه فیشینگ در سراسر جهان فرستاده می‌شود.

• استخراج اطلاعات از طریق شبکه‌های اجتماعی: یکی از روش‌های مهندسی اجتماعی است که در سال‌های اخیر نیز گسترش یافته است و مهاجم سعی دارد از طریق جمع‌آوری اطلاعات کاربر هدف در شبکه‌های اجتماعی، حمله به یک کاربر را سفارشی کند. طبق بررسی‌ها بین ۵۲ تا ۹۷ میلیون حساب کاربری جعلی در شبکه اجتماعی فیسبوک وجود دارد.

• روش‌های دیگر: در مهندسی اجتماعی روش‌های مختلفی وجود دارد که تا به اینجا چند مورد بررسی شدند و روش‌های دیگری نیز مانند زباله‌گردی سازمان‌ها و شرکت‌ها، استفاده از موتورهای جستجو، اعتمادسازی حضوری در محل شرکت، بهره‌برداری از روابط و فریب از طریق جملات و رفتارها را نام برد که هر کدام دارای روش‌های مختلفی هستند.

در ادامه توصیه‌هایی برای مقابله و جلوگیری از مهندسی اجتماعی بیان خواهند شد:

• ساده‌ترین و کارآمدترین راه‌کار برای مقابله با مهندسی اجتماعی، آموزش افراد و آگاهی آن‌ها است تا در لحظات حساس به درستی تصمیم‌گیری کنند و فریب وسوسه‌های مهاجمین را نخورند.

• در انتشار اطلاعات در شبکه‌های اجتماعی و فضای سایبری دقت کنید که مهمترین منبع مهندسی اجتماعی همین اطلاعاتی است که خودتان به صورت عمومی منتشر کرده‌اید.

• برای شرکت‌ها و سازمان‌هایتان سیاست‌های امنیتی مشخصی برای نشر اطلاعات تعیین کرده و افراد را ملزم به پیروی از این سیاست‌ها کنید.

• با وجود اینکه نشان قفل سبز رنگ در مرورگر (HTTPS) نماد امن بودن وب‌سایت است اما گاهاً مهاجمین اقدام به خریداری گواهی‌نامه SSL کرده و برای صفحات جعلی(فیشینگ) خود از HTTPS نیز بهره می‌برند. در نتیجه پس از ورود به یک وب‌سایت توجه اصلی به آدرس وب‌سایت یکی دیگر از اقدامات در تشخیص صفحات فیشینگ است به عنوان مثال .Shaparak ir دارای صفحات جعلی متعددی مانند Shapark.org و یا Shaparak.in است که باید دقت بیشتری در این وب‌سایت‌ها داشت.

• هیچگاه بر روی لینک‌ها یا پیوست‌هایی که در ایمیل یا شبکه‌های اجتماعی یا پیام‌رسان‌ها برایتان به صورت ناشناس ارسال می‌گردد کلیک نکنید و به این ایمیل‌ها نیز پاسخ ندهید.

• در شرکت‌ها و سازمان‌هایی که دارای اطلاعات حساس هستند حتما از سیستم‌هاي كاغذ خردكن Cross-Shredding استفاده كنيد.

• در شركت يا سازمان‌ها هيچ‌گاه به يك غريبه اجازه ندهيد كه به يكي از پورت‌هاي شبكه يا شبكه بي‌سيم شما متصل شود. يك مهاجم مي‌تواند در مدت زمانِ بسيار كوتاهي يك تحليل‌گر شبكه و يا بدافزار را مستقيماً بر روي سيستم و شبكه شما قرار دهد.

• در صورت دریافت ایمیل، پیام و یا تماس افراد برای دریافت اطلاعات، به هر شخص به اندازه‌ای که لازم است اطلاعات بدهید و نه بیشتر. بهتر است در این زمینه از سیاست‌های تدوین شده سازمان یا شرکت خود پیروی کنید.

• نسبت به پیام‌هایی شامل اغواگری که هدف آن فریب افراد است دقت داشته باشید. این پیام‌ها از قبیل "جایزه‌ای برنده شده‌اید" یا "برنده قرعه‌کشی این دوره ما" و یا "ازدواج دو بازیگر مشهور" و یا نمونه‌های اینچنینی را در این قالب در نظر داشته باشید.

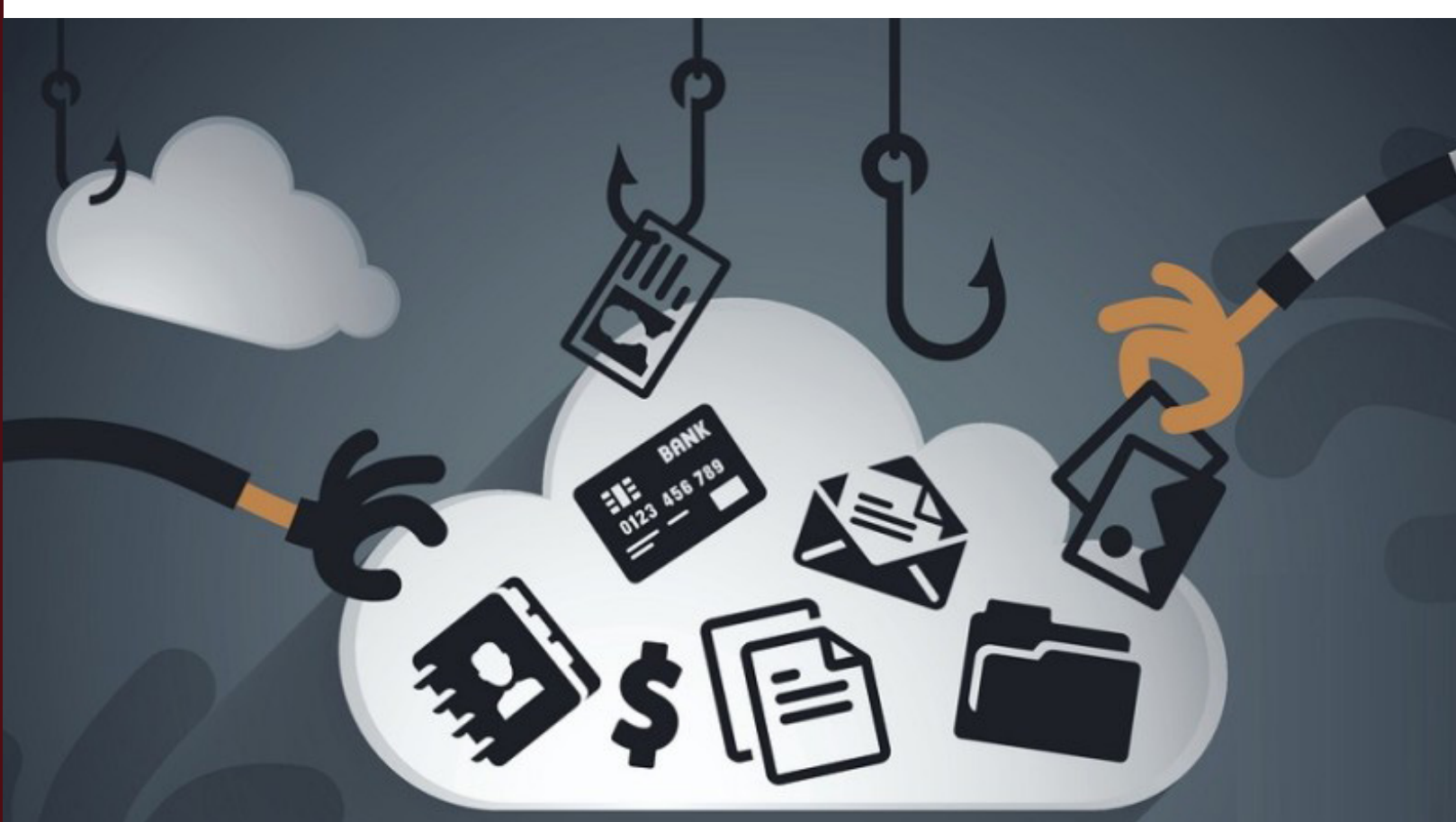
• دسته دیگری از پیام‌ها شامل پیغام‌هایی جعلی در خصوص حساب‌های کاربری شما است به عنوان مثال "لطفا حساب کاربری خود را تایید کنید" یا "حساب کاربری شما بسته شده است" و یا "کد رمز ارسالی را به این شماره ارسال کنید". در صورت دریافت این نوع پیام‌ها هیچ اقدامی را انجام ندهید.

• مرورگرها و سرویس‌های ایمیل در تلاش هستند تا شما را از حملات فیشینگ در امان نگه دارند؛ با این حال آنچنان که باید در این امر موفق نبوده‌اند. بهترین راه‌کار دقت خود کاربر است.

• پیش از ارسال و یا تکمیل فرم‌ها، اطمینان حاصل کنید که اطلاعات شخصی خود را در اختیار افراد و یا وب‌سایت‌های مشروع و مطمئن قرار می‌دهید.

• برای دسترسی به وب‌سایت بانک ها، آدرس آن‌ها را به صورت مستقیم در مرورگر خود وارد کنید و از کلیک بر روی لینک‌های پرداخت موجود در ایمیل‌ها که قرار است شما را به صفحه بانک منتقل کنند ولی ممکن است در عمل شما را به صفحه‌ای مشابه و جعلی هدایت می‌کنند، جدا پرهیز کنید.

منابع:



مرکز آپا دانشگاه کردستان

www.cert.uok.ac.ir