ویژه نامه امنیتی

مرکز تخصصی آپا دانشگاه بیرجند

باج افزار

RANSOMWARE

2018

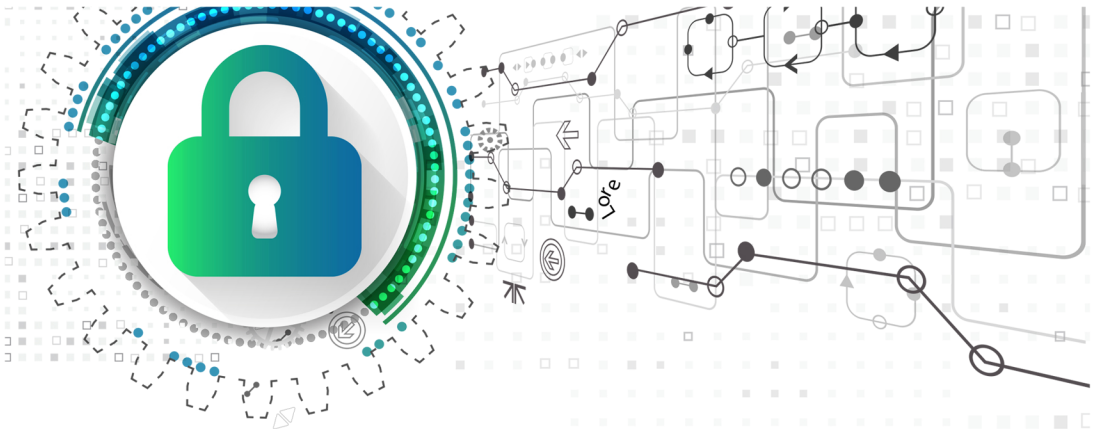
مروری بر تهدیدات باج‌افزارها

مقدمه

امروزه یکی از تهدیدات سایبری اصلی و از پرهزینه‌ترین تهدیداتی که متوجه سازمان‌ها می‌باشد باج‌افزار است. تهدید حملات باج‌افزاری هدفمندی که آسیب‌رسانی به شبکه سازمان و آلوده کردن کامپیوترهای متعدد را در بر می‌گیرند، همچنان ادامه دارد. گرچه حمله هدفمند نسبت به ارسال انبوه ایمیل‌های مخرب شیوع کمتری دارد، اما خسارت ناشی از حمله هدفمند به مراتب سنگین‌تر است.

خانواده‌های باج‌افزار رمزنگار نوین از رمزنگاری قدرتمندی استفاده می‌کنند که هر فایل رمزنگاری شده‌ای را از دسترس خارج می‌کند؛ مگر اینکه یک کلید رمزگشایی تهیه شود. این کار، هر سازمانی را که از داده‌های خود پشتیبان‌گیری نکرده باشد مجبور به انتخابی ناخوشایند بین از دست دادن داده‌های مهم یا باج دادن به مجرمان سایبری می‌کند و تضمینی هم وجود ندارد که مهاجمان سر قول خود بمانند و کلید رمزگشایی را فراهم کنند.

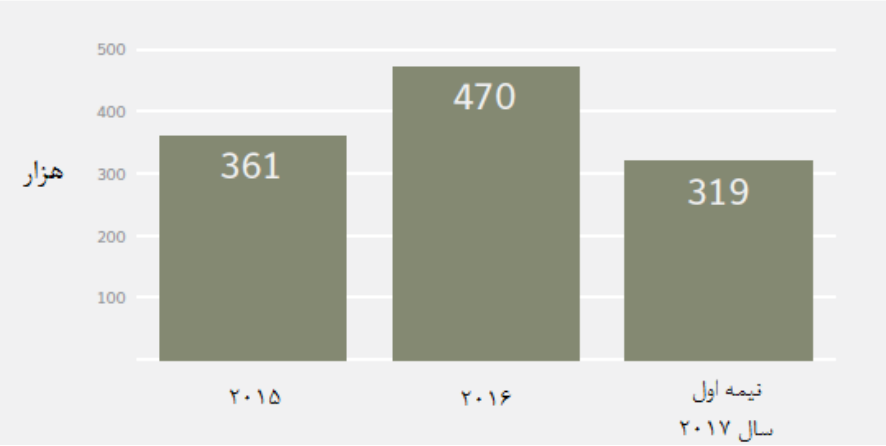
مجموع باج‌های تقاضا شده از کسب‌وکارها در حملاتی که ده‌ها یا حتی صدها کامپیوتر را آلوده می‌سازند، می‌تواند بسیار هنگفت باشد؛ اما تقاضای باج تنها منشاء احتمالی ضرر و زیان نیست. شمار زیادی از مؤسسات تجاری، تأثیرگذاری باج‌افزار بر کسب‌وکارشان را اعلام نموده‌اند و شرکت‌های متعددی نیز گفته‌اند که حملات باج‌افزاری تأثیر قابل توجهی بر درآمدشان داشته است. حمله باج‌افزاری می‌تواند موجب وقفه قابل توجهی شود که نتیجه آن از دست دادن بهره‌وری، عدم توانایی برای عمل به وظایف در موعدهای مقرر و هزینه‌های پاکسازی است که می‌تواند منجر به زیان‌های مالی، اخلال در کار و تخریب وجهه و اعتبار شوند.



نرخ آلودگی‌های باج‌افزاری

بعد از افزایش ۳۶ درصدی نرخ آلودگی‌های باج‌افزاری بین سال‌های ۲۰۱۵ و ۲۰۱۶، آلودگی‌هایی که توسط شرکت نرم‌افزاری symantec شناسایی شدند در حال افزایش بودند. در سال ۲۰۱۶ مجموعاً از ۴۷۰۰۰۰ آلودگی جلوگیری به عمل آمد؛ اما symantec در شش ماهه نخست سال ۲۰۱۷ از بیش از ۳۱۹۰۰۰ آلودگی باج‌افزاری پیشگیری نمود. اگر این نرخ آلودگی در تمام طول سال ادامه می‌یافت، نرخ سال ۲۰۱۷ نسبت به ۲۰۱۶ افزایشی چشمگیر به حساب می‌آمد.

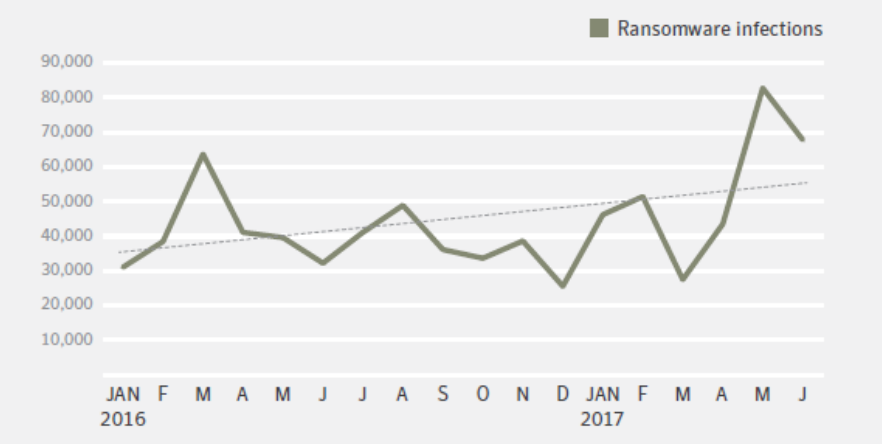
شایان ذکر است که نمودارهای ارائه شده شناسایی حملات، معرف بخش کوچکی از مجموع باج‌افزارهای متوقف شده توسط symantec است که اکثر این حملات در مراحل ابتدایی‌تر در فرایند آلودگی متوقف شده‌اند. به‌عنوان مثال، سیستم پیش‌گیری از نفوذ (IPS)[1] شرکت symantec تقریباً تمام حملات WannaCry را در مراحل اولیه متوقف کرد و از رسیدن باج‌افزار به کامپیوتر جلوگیری نمود.



شکل ۱- آلودگی‌های باج‌افزاری به تفکیک سال

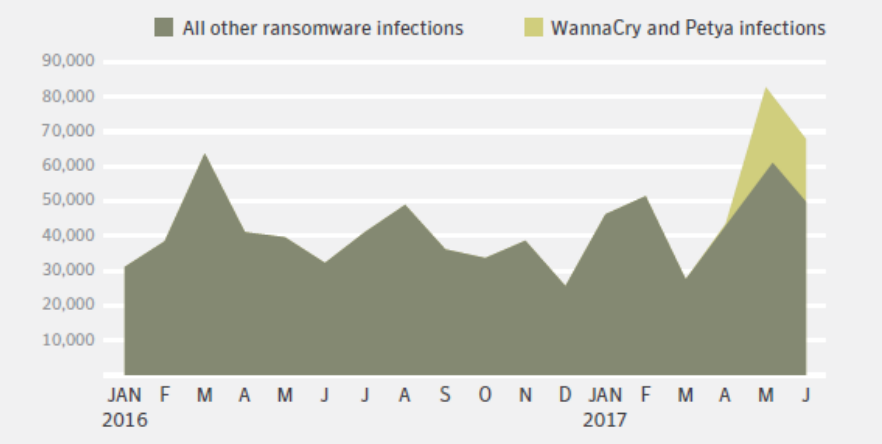
در نرخ آلودگی به تفکیک ماه بین ژانویه ۲۰۱۶ و ژوئن ۲۰۱۷ روندی صعودی همراه با افزایشی قابل توجه در تعداد آلودگی‌های رخ داده در ماه‌های می و ژوئن ۲۰۱۷ مشاهده می‌شود.

[1] Intrustion Prevention System



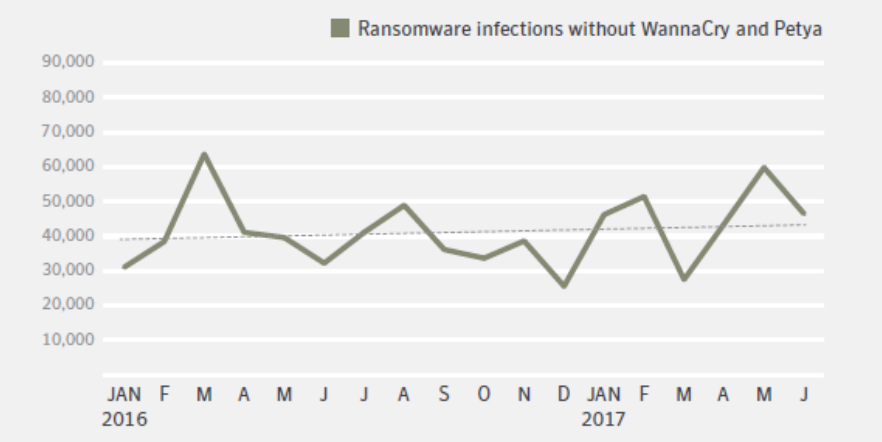
شکل ۲- آلودگی‌های باج‌افزاری به تفکیک ماه

این نوسان آلودگی‌ها تا حد زیادی ناشی از شیوع WannaCry و Petya بود که باعث ۲۸ درصد از آلودگی‌های ماه می و ۲۱ درصد از آلودگی‌های ماه ژوئن بودند.



شکل ۳- تأثیر شیوع WannaCry و Petya بر نرخ آلودگی ماهانه

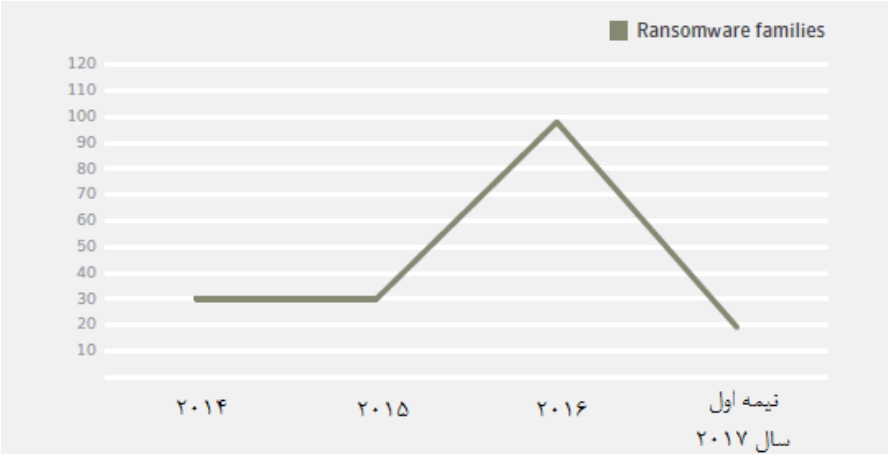
اگر تعداد آلودگی‌های WannaCry و Petya از نمودارهای ماهانه برداشته شود، نرخ آلودگی باز هم از ژانویه ۲۰۱۶ تا ژوئن ۲۰۱۷ روند افزایشی هرچند با شیبی بسیار ملایم‌تر خواهد داشت.



شکل ۴- تعداد آلودگی‌های باج‌افزاری به صورت ماهانه بدون WannaCry و Petya

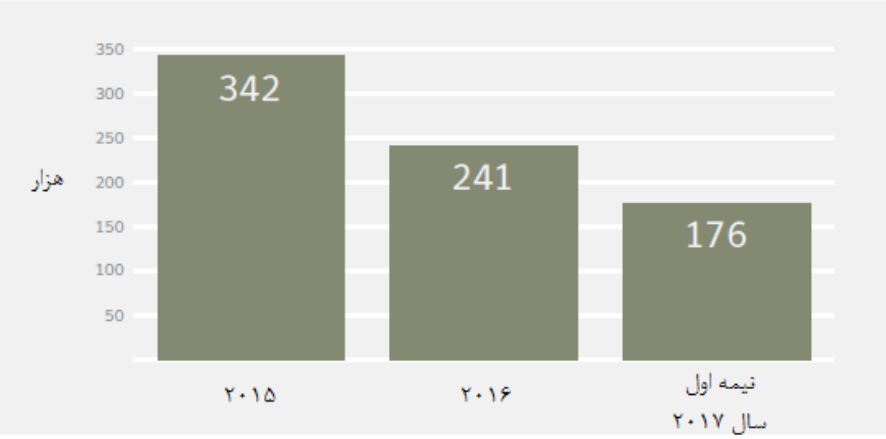
خانواده‌های باج‌افزار

بعد از افزایشی چشمگیر در سال ۲۰۱۶ یعنی هنگامی که تعداد خانواده‌های جدید باج‌افزار به بیش از سه برابر رسید، تعداد خانواده‌های جدید در شش ماهه نخست سال ۲۰۱۷ به ۱۶ عدد کاهش یافت.



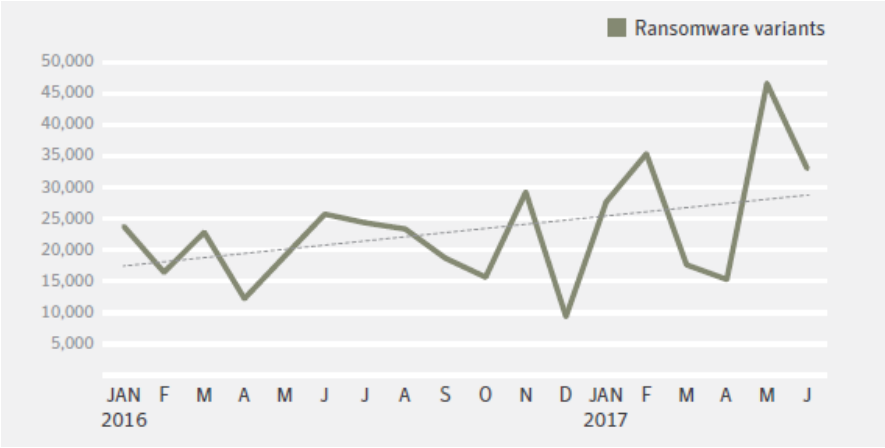
شکل ۵- خانواده‌های جدید باج‌افزار به تفکیک سال

تعداد گونه‌های باج‌افزار (به عبارت دیگر، انواع متفاوتی از خانواده‌های باج‌افزار که برای اولین بار مشاهده شدند) پس از اینکه بین سال‌های ۲۰۱۵ تا ۲۰۱۶ کاهش یافت، بار دیگر رو به فزونی نهاد. symantec در مقایسه با ۲۴۱۰۰۰ گونه باج‌افزاری جدید در کل سال ۲۰۱۶، ۱۷۶۰۰۰ گونه باج‌افزاری جدید را نیز در شش ماهه نخست سال ۲۰۱۷ به ثبت رساند.



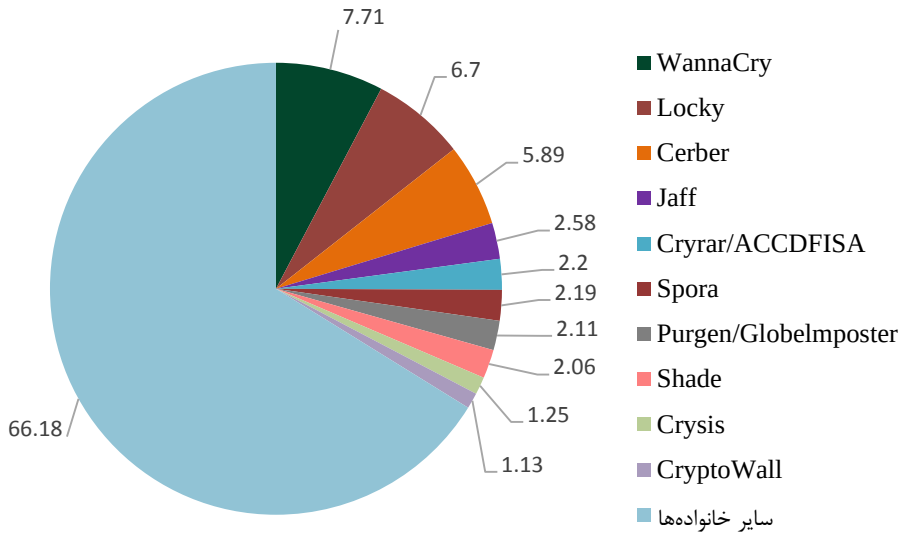
شکل ۶- گونه‌های جدید باج‌افزار به تفکیک سال

تعداد گونه‌های جدید باج‌افزار، سال به سال روند صعودی پیدا کرده و به‌خصوص در ماه‌های می و ژوئن یعنی همان ماه‌هایی که WannaCry و Petya شیوع پیدا کردند، افزایش چشمگیری داشته است.



شکل ۷- گونه‌های جدید باج‌افزار به تفکیک ماه

۱۰ مورد از شایع‌ترین خانواده‌های رمزنگارها



شکل ۹- ۱۰ مورد از شایع‌ترین خانواده‌های رمزنگارها در سال ۲۰۱۷

باج‌افزار WannaCry صدها هزار کامپیوتر را در سراسر جهان تحت تأثیر خود قرار داده است؛ بنابراین جای تعجب نیست که این خانواده، شایع‌ترین باج‌افزار رمزنگار در سال ۲۰۱۷ باشد.

انتشار کلیدهای اصلی برای چندین خانواده باج‌افزاری

در سه ماهه دوم سال ۲۰۱۷ چندین گروه از مجرمانِ پشت پرده باج‌افزارهای رمزنگار مختلف، به فعالیت خود خاتمه دادند و کلیدهای رمز موردنیاز برای رمزگشایی فایل‌های قربانیان را منتشر نمودند.

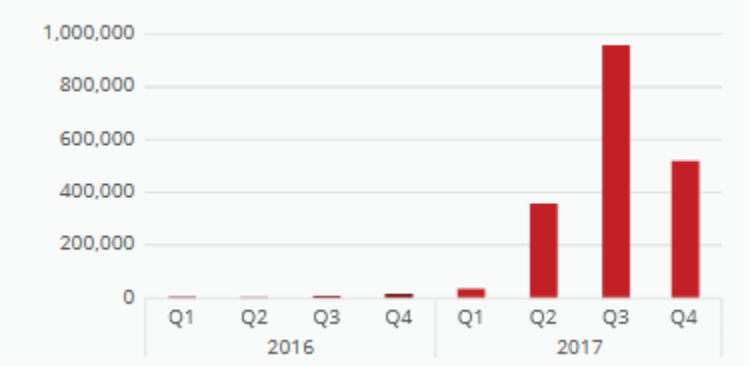
در زیر، لیست خانواده‌هایی از باج‌افزارها که در سه ماهه دوم سال ۲۰۱۷ کلیدهایشان عمومی شدند قرار گرفته است:

Crysis (Trojan-Ransom.Win32.Crusis)
AES-NI (Trojan-Ransom.Win32.AecHu)
xdata (Trojan-Ransom.Win32.AecHu)
Petya/Mischa/GoldenEye (Trojan-Ransom.Win32.Petr)

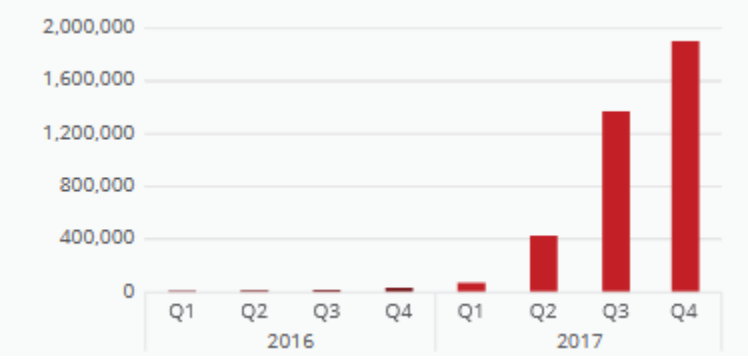
کلید اصلی Petya/Mischa/GoldenEye در مدت کوتاهی پس از شیوع باج‌افزار ExPetr منتشر شد که امکان دارد این تلاش‌ها توسط نویسندگان اصلی Petya برای نشان دادن اینکه آن‌ها از افراد پشت پرده ExPetr نیستند، صورت گرفته باشد.

حملات باج‌افزاری به دستگاه‌های موبایل

بر اساس گزارش McAfee، تعداد خانواده‌های جدید باج‌افزار موبایل کاهش یافته‌اند، اما افزایش تعداد آلودگی‌ها همچنان ادامه یافته است. در صحت این بخش از گزارش McAfee تردید وجود دارد؛ چون گزارش مشابه دیگری از ESET اعلام کرده است که تعداد حملات باج‌افزاری موبایل در سال ۲۰۱۷ کاهش یافته - است.



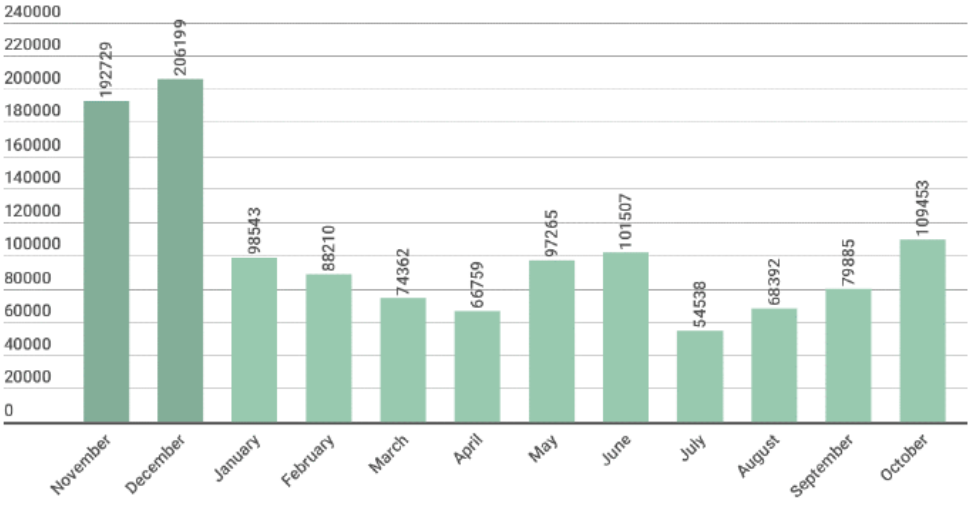
شکل ۱۲- بدافزارهای جدید قفل‌کننده صفحه‌نمایش اندروید



شکل ۱۳- مجموع بدافزارهای قفل‌کننده صفحه‌نمایش اندروید

تعداد کاربران مورد حمله توسط رمزنگارها

۹۳۹,۷۲۲ کاربر مختلف از شبکه امنیتی کسپرسکی[۲] در سال ۲۰۱۷ توسط رمزنگارها مورد حمله قرار گرفتند که بیش از ۲۴۰ هزار نفر از آن‌ها کاربران شرکت‌ها بودند.



شکل ۱۴- تعداد کاربران مورد حمله توسط باج‌افزار رمزنگار از نوامبر ۲۰۱۶ تا اکتبر ۲۰۱۷

تعداد واقعی حملات باج‌افزاری بالاتر از این است. این آمار فقط نتایج تشخیص‌های مبتنی بر امضاء و هیوریستیک را نشان می‌دهد، در حالیکه محصولات آزمایشگاه کسپرسکی، نمونه بدافزارهای جدید و ناشناخته مانند تروجان‌های رمزنگار را بر اساس مدل‌های تشخیص مبتنی بر رفتار شناسایی می‌کنند.

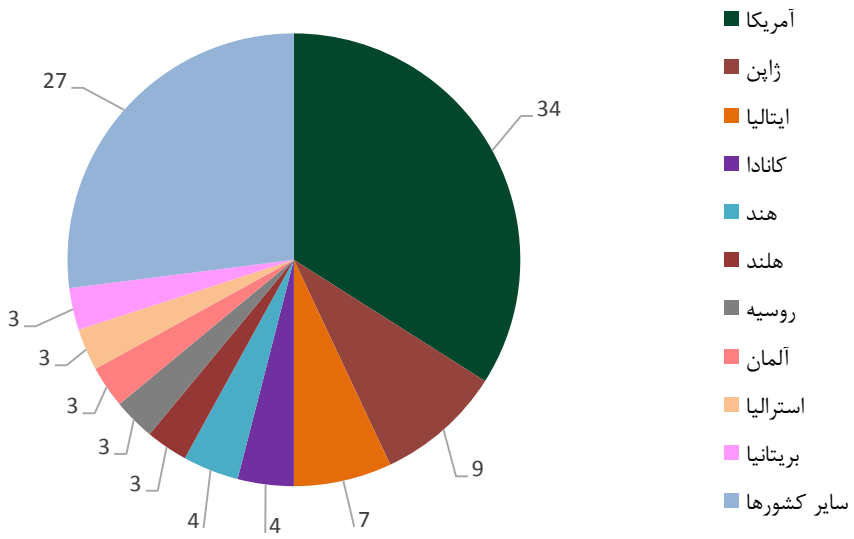
جغرافیای حملات

آمریکا طی شش ماهه نخست سال ۲۰۱۷ با سهم ۲۹ درصدی‌اش از تمام آلودگی‌ها، رتبه اول را در آلودگی‌های باج‌افزاری دارد. در این برهه زمانی، ژاپن (۹ درصد)، ایتالیا (۸ درصد)، هند (۴ درصد) و آلمان (۴ درصد) نیز به شدت تحت تأثیر حملات باج‌افزاری قرار گرفتند. لیست ده کشور نخست با هلند (۳ درصد)، بریتانیا (۳ درصد)، استرالیا (۳ درصد)، روسیه (۳ درصد) و کانادا (۳ درصد) تکمیل می‌شود.

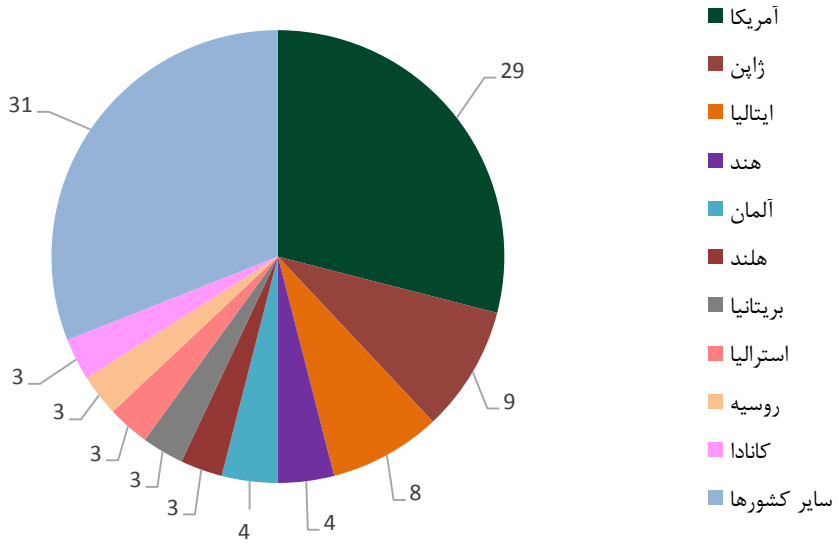
لیست ۱۰ کشور با بیشترین تأثیرپذیری از باج‌افزار در نیمه اول سال ۲۰۱۷ با لیست سال ۲۰۱۶ یکسان است. تنها تفاوت عمده در این است که سهم آمریکا از آلودگی‌های باج‌افزاری از ۳۴ درصد در سال ۲۰۱۶ به

[2] Kaspersky Security Network

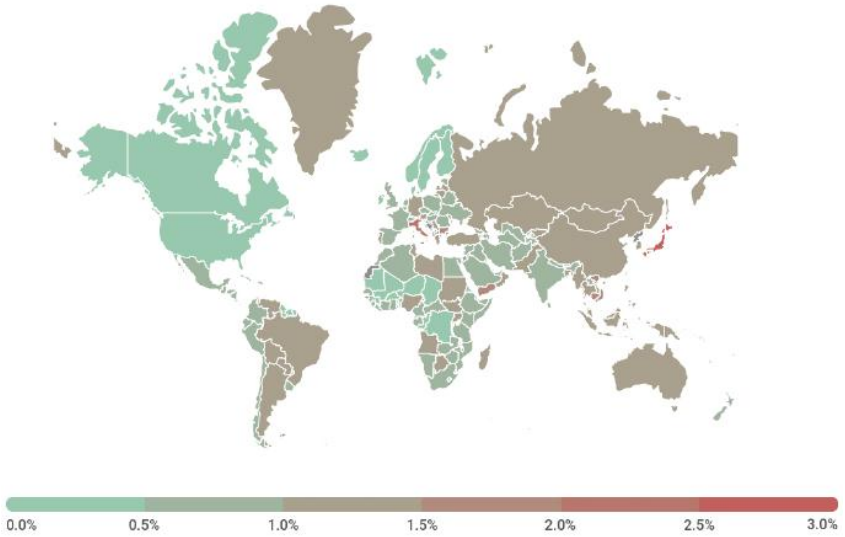
۲۹ درصد در نیمه اول سال ۲۰۱۷ کاهش یافت. به جز این کاهش، هیچ تغییر عمده دیگری رخ نداد و سهم هیچ منطقه دیگری بیش از یک درصد جابجا نشد.



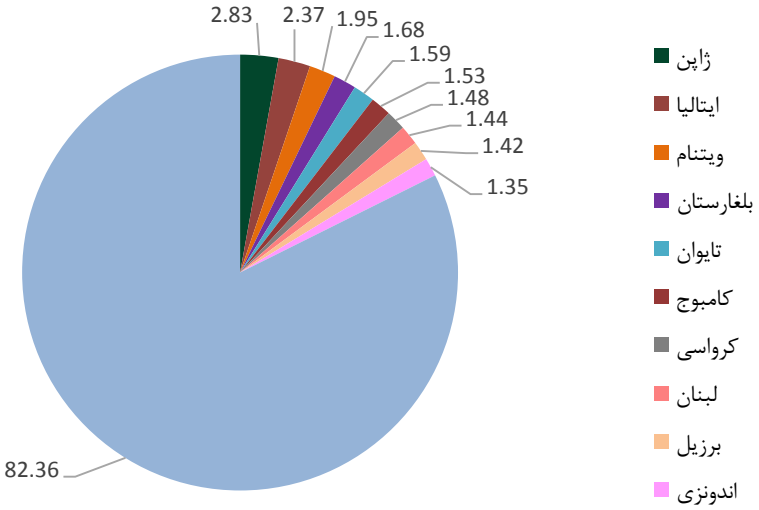
شکل ۱۵- کشف و شناسایی باج‌افزارها به تفکیک منطقه در سال ۲۰۱۶



شکل ۱۶- کشف و شناسایی باج‌افزارها به تفکیک منطقه در نیمه اول سال ۲۰۱۷



شکل ۱۷- جغرافیای حملات باج‌افزار رمزنگار در سال ۲۰۱۷ (بر حسب درصد کاربران کسپرسکی مورد حمله)



شکل ۱۸- درصد کاربران کسپرسکی مورد حمله توسط رمزنگارها در ۱۰ کشور نخست لیست در سال ۲۰۱۷
(نادیده گرفتن کشورهایی که تعداد کاربران محصولات کسپرسکی در آن‌ها نسبتاً کم است (کمتر از ۵۰۰۰۰ نفر))

آمار کلی باج‌افزار در سال ۲۰۱۷

- در سال ۲۰۱۷ حدود ۹۵۰۰۰۰ کاربر محصولات کسپرسکی مورد حمله باج‌افزارها قرار گرفتند که این تعداد در سال ۲۰۱۶ حدود ۱/۵ میلیون نفر بود. این نتایج، هر دو نوع رمزنگار و downloader را در بر می‌گیرد؛ اما اگر فقط آمارِ مربوط به رمزنگارها در نظر گرفته شود، اطلاعات مربوط به این حمله در سال ۲۰۱۷ مشابه سال ۲۰۱۶ خواهد بود.
- با وجود WannaCry، ExPetr و BadRabbit تعداد حملاتی که شرکت‌ها را مورد هدف قرار دادند با کمی افزایش از ۲۲/۶ درصد در سال ۲۰۱۶ به ۲۶/۲ درصد در سال ۲۰۱۷ رسید. در سال ۲۰۱۷، بیش از ۴ درصد افراد از طریق پروتکل SMB[3] ویندوز مورد حمله قرار گرفته بودند.
- پیش‌بینی می‌شود که باج‌افزار تا پایان سال ۲۰۱۹ در هر ۱۴ ثانیه یک کسب‌وکار را مورد حمله قرار دهد، در حالیکه این رقم در سال ۲۰۱۷ هر ۴۰ ثانیه یک بار بوده است.
- طبق گزارش سالانه امنیت سایبری cisco، پیش‌بینی شده که نرخ سالانه باج‌افزار در سال ۲۰۱۷ تا ۳۵۰ درصد رشد کرده باشد.
- بین سه ماهه دوم سال ۲۰۱۶ تا سه ماهه دوم سال ۲۰۱۷ مجموع باج پرداختی توسط شرکت‌های با اندازه کوچک و متوسط ۳۰۱ میلیون دلار بوده است.

طبق آمار سالانه امنیت فناوری اطلاعات آزمایشگاه کسپرسکی:

- ۶۵ درصد از کسب‌وکارهایی که در سال ۲۰۱۷ توسط باج‌افزارها مورد حمله قرار گرفتند، اعلام کردند که دسترسی به حجم عظیم یا حتی تمام داده‌های خود را از دست داده‌اند و همچنین ۲۹ درصد از کسب‌وکارها با اینکه قادر به رمزگشایی داده‌های خود بودند؛ اما میزان قابل توجهی از فایل-های خود را برای همیشه از دست دادند. این ارقام تا حدود زیادی با سال ۲۰۱۶ مطابقت دارد.
- ۳۴ درصد از کاربرانی که در سال ۲۰۱۷ مورد حمله باج‌افزارها قرار گرفتند حداقل یک هفته طول کشید تا مجدداً به داده‌های خود دسترسی کامل داشته باشند، در حالیکه این رقم در سال ۲۰۱۶ تنها ۲۹ درصد بود.

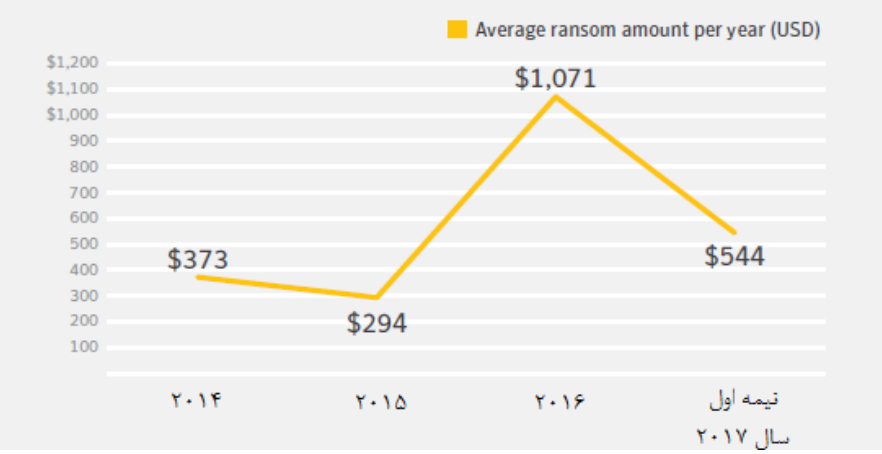
[3] Server Message Block

- ۳۶ درصد از افراد در سال ۲۰۱۷ باج تقاضا شده را پرداخت کردند؛ اما ۱۷ درصد از این افراد هرگز نتوانستند داده‌های خود را بازگردانند. در سال ۲۰۱۶، ۳۲ درصد افراد باج را پرداخت نمودند و داده-های ۱۹ درصد از این افراد برگشت داده نشد.

تثبیت تقاضای باج

میانگین تقاضای باج خانواده‌های جدید باج‌افزار در طول سال ۲۰۱۶ به شدت افزایش یافت و از ۲۹۴ دلار به بیش از سه برابر یعنی ۱۰۷۱ دلار رسید. احتمالاً مهاجمان با این باور که می‌توانند از قربانیان بالقوه مقادیر بسیار بیشتری به دست آورند برانگیخته شدند و در سال ۲۰۱۶ نرخ باج را تا بیشترین بازده ممکن بالا بردند. میانگین تقاضای باج از آن هنگام به بعد کاهش یافت و در شش ماهه نخست سال ۲۰۱۷ این میانگین از خانواده‌های جدید باج‌افزار ۵۴۴ دلار بود. اگرچه این مقدار نسبت به سال ۲۰۱۶ بسیار پایین‌تر است؛ اما هنوز ۸۵ درصد از سال ۲۰۱۵ بیشتر است و شاید مهاجمان بعد از مدتی آزمون و خطا، در حال تثبیت باج حول تقاضای ۵۰۰ دلاری هستند و آن را نقطه‌ای بهینه و مطلوب می‌دانند.

ممکن است تقاضای باج به مقدار ۵۰۰ دلار حتی برای یک شرکت کوچک نیز مبلغ زیادی به نظر نرسد؛ اما سازمان‌ها باید به یاد داشته باشند که میانگین تقاضا مربوط به یک آلودگی واحد است. مجموع باج‌های تقاضا شده در حملاتی که ده‌ها یا حتی صدها کامپیوتر را آلوده می‌کنند، بسیار بالاتر خواهد بود.



شکل ۱۹- میانگین مقدار باج به تفکیک سال

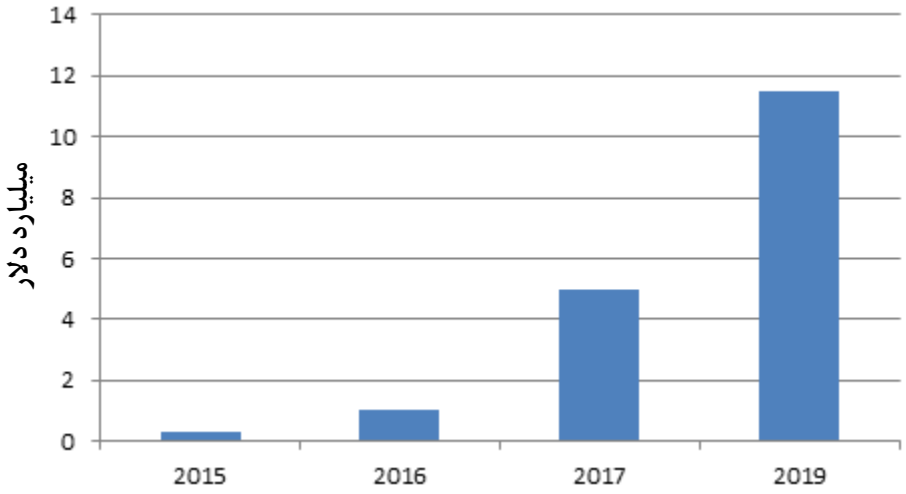
چه تعداد از افراد باج می‌دهند؟

طبق پژوهش انجام شده توسط Norton، ۳۴ درصد از قربانیان، باج خواسته شده را پرداخت می‌کنند. این نسبت در آمریکا به ۶۴ درصد می‌رسد که تا حدودی نشان می‌دهد چرا این کشور به شدت هدف حمله قرار می‌گیرد.

احتمالاً تمایل به پرداخت باج، عاملی برای افزایش و ادامه فعالیت باج‌افزارها است. در حال حاضر، عملیات پرداخت باج آسان‌تر نیز شده است. مهاجمان اغلب برای تشویق قربانیان به پرداخت باج، آن‌ها را در روند پرداخت مبلغ یاری می‌کنند و دسترسی گسترده به خدمات پرداخت، استفاده از بیت‌کوین را بیش از پیش آسان نموده است، به‌خصوص اکنون که بیت‌کوین مانند گذشته ناشناخته نیست.

میزان خسارات باج‌افزارها

شرکت Cybersecurity Ventures پیش‌بینی کرده است که میزان خسارات باج‌افزار در سال ۲۰۱۷ به ۵ میلیارد دلار رسیده باشد و این رقم تا سال ۲۰۱۹ به ۱۱/۵ میلیارد دلار افزایش پیدا کند. میزان این خسارت در سال ۲۰۱۵ تنها ۳۲۵ میلیون دلار بود. این آمار بدین معنا است که در دو سال افزایش ۱۵ برابری رخ داده است و انتظار می‌رود که میزان خسارات باج‌افزار بیشتر شود. پس از افزایش حملات، Cybersecurity Ventures پیش‌بینی کرده بود که میزان خسارات باج‌افزار و هزینه‌های مرتبط با آن در سال ۲۰۱۶ به ۱ میلیارد دلار رسیده است.



شکل ۲۰- میزان خسارات باج‌افزارها

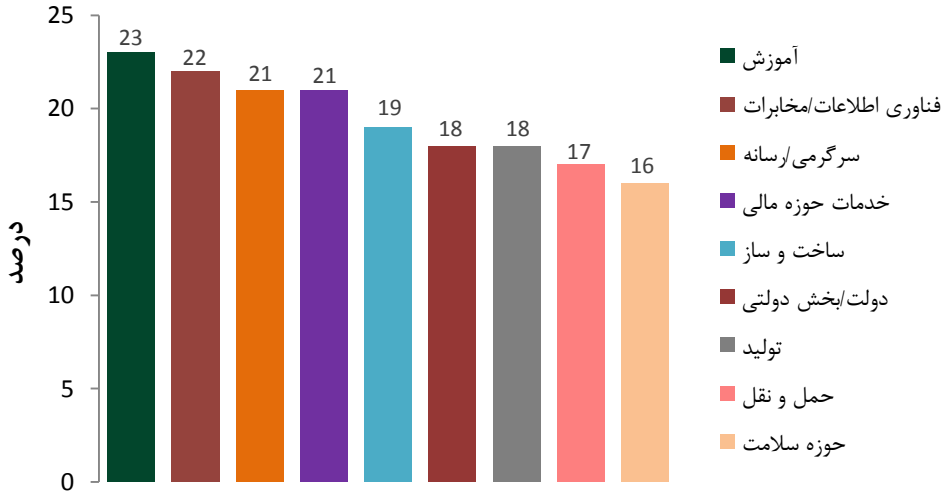
شرکت Cybersecurity Ventures پیش‌بینی می‌کند که حملات باج‌افزاری به سازمان‌های حوزه سلامت تا سال ۲۰۲۰ تا چهار برابر افزایش یابد. بیمارستان‌ها هدف اول مجرمان سایبری هستند و بالاخص در برابر باج‌افزارها آسیب‌پذیرتر هستند.

بر اساس گزارش Cybersecurity Ventures پیش‌بینی می‌شود که هزینه‌های جهانی در ارتباط با آگاهی امنیتی به کارکنان تا سال ۲۰۲۷ به ۱۰ میلیارد دلار برسد. اگر سازمان‌های جهانی، آموزش کارکنان خود را برای آگاهی امنیتی در نظر بگیرند، میزان خسارات حملات باج‌افزاری ممکن است کاهش پیدا کند.

همچنین این شرکت پیش‌بینی کرده که هزینه سالانه جرایم سایبری در جهان از بیش از ۳ تریلیون دلار در سال ۲۰۱۵ به بیش از ۶ تریلیون دلار در سال ۲۰۲۱ برسد. انتظار می‌رود که وضعیت حملات باج‌افزاری در سال‌های آتی بدتر شود و تا سال ۲۰۲۱ نسبتاً سهم بیشتری از کل جرایم سایبری را به خود اختصاص دهد.

حوزه‌های مورد هدف توسط باج‌افزار

هیچ حوزه‌ای از حملات باج‌افزار در امان نیست. حوزه آموزش با سهم ۲۳ درصدی‌اش، رتبه اول را به خود اختصاص داده است. همچنین فناوری اطلاعات/مخابرات (۲۲ درصد)، سرگرمی/رسانه (۲۱ درصد)، خدمات حوزه مالی (۲۱ درصد)، ساخت و ساز (۱۹ درصد)، دولت/بخش دولتی (۱۸ درصد)، تولید (۱۸ درصد)، حمل و نقل (۱۷ درصد) و حوزه سلامت (۱۶ درصد) از دیگر حوزه‌هایی هستند که تحت تأثیر باج‌افزارها قرار گرفته‌اند.



شکل ۲۱- حوزه‌های مورد هدف توسط باج‌افزار

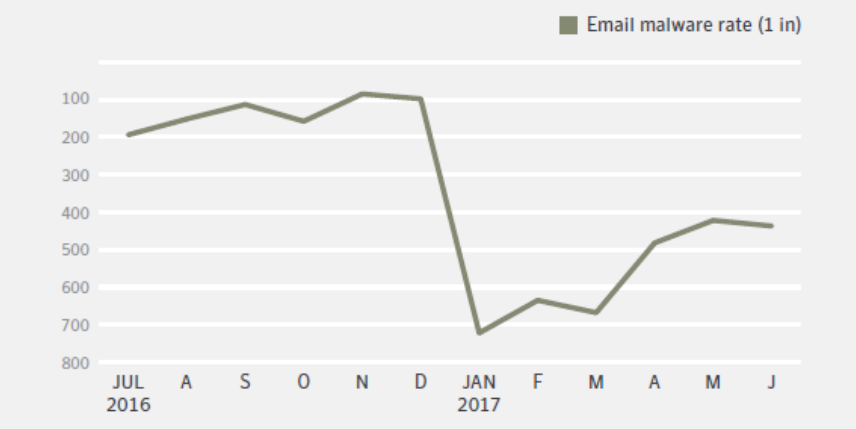
مسیرهای آلودگی باج‌افزار

باج‌افزار به چند روش مختلف یا همان مسیرهای آلودگی منتشر می‌شود. با وجود وقفه‌هایی در کار خدمات توزیع مخرب، هنوز هم ایمیل کانال اصلی توزیع باج‌افزار محسوب می‌شود. اکسپلویت‌کیت‌ها و اخیراً خودتکثیری در قالب باج‌افزارهای کرمی نیز در کنار تعدادی از مسیرهای آلودگی مناسب‌تر مورد استفاده قرار می‌گیرند. پی بردن به منشاء باج‌افزارها، گامی مهم در ایجاد روش‌های دفاعی علیه آن در یک سازمان است. یکی از مؤثرترین روش‌های حفاظت این است که تهدیدات قبل از فرصت یافتن برای دانلود شدن در کامپیوترهای داخل یک شبکه، در منشاء خود متوقف شوند.

ایمیل: منبع اصلی تهدید

کمپین‌های ارسال انبوه هرزنامه‌های مخرب، یکی از کانال‌های اصلی توزیع باج‌افزار هستند. این هرزنامه‌ها با استفاده از بات‌نت‌ها توزیع می‌شوند. بسیاری از این بات‌نت‌ها قادر به ارسال هرزنامه به تعداد زیاد و به‌صورت روزانه می‌باشند و اکثر آن‌ها به منظور فریفتن دریافت‌کنندگان برای آلوده کردن کامپیوترشان، از روش‌های ساده مهندسی اجتماعی استفاده می‌کنند. اگر کاربر هر کدام از اعمالی را که در ذیل می‌آیند انجام دهد، ممکن است آلودگی رخ دهد:

- باز کردن یک فایل پیوست مخرب که مستقیماً باج‌افزار را نصب می‌کند.
- کلیک روی لینکی که دانلود و نصب باج‌افزار را آغاز می‌کند. معمولاً برای فریفتن کاربر و وادار کردن او به کلیک روی چنین لینکی، از مهندسی اجتماعی استفاده می‌شود.
- کلیک روی لینکی که به یک اکسپلویت‌کیت می‌رسد و این کیت در نهایت باعث نصب بدافزار روی کامپیوتر می‌شود.



شکل ۲۲- نرخ ایمیل آلوده به بدافزار ثبت شده توسط symantec (یک در هر ایمیل)

سایر مسیرهای آلودگی

با اینکه ایمیل و اکسپلویت‌کیت‌ها دو روش غالب برای توزیع باج‌افزار هستند، تکنیک‌هایی که در ذیل می‌آیند نیز برای این منظور به کار گرفته می‌شوند:

- **خودتکثیری**

گونه‌های جدید WannaCry و Petya از خودتکثیری استفاده کرده‌اند و اثر چشمگیری از خود به جا گذاشته‌اند. آن‌ها نخستین خانواده‌های باج‌افزاری نبودند که از این تکنیک استفاده می‌کردند. این تکنیک قبلاً هم توسط ZCryptor به کار رفته بود که قبل از آغاز رمزنگاری فایل‌ها، تمام درایوهای قابل حمل را با یک کپی از خود آلوده می‌کرد. علاوه بر این، تعدادی از خانواده‌های باج‌افزار اندرویدی با انتشار به تمام مخاطبان موجود در لیست مخاطبان دستگاه از طریق پیام کوتاه، رفتاری کرم‌مانند از خود نشان می‌دهند.

- **تبلیغات مخرب**

تبلیغات مخرب در شبکه‌هایی تبلیغاتی که پیام‌های تبلیغاتی‌شان از طریق وب‌سایت‌های معتبر با حجم بازدید بالا منتشر می‌گردد، قرار داده می‌شوند. در برخی موارد حتی لازم نیست که بازدیدکننده روی لینک کلیک کند؛ به طوریکه بارگذاری صفحه وب حاوی تبلیغات مخرب به سادگی منجر به آلودگی خواهد شد و این کار اغلب از طریق هدایت به سمت یک اکسپلویت‌کیت صورت می‌گیرد.

- **جستجوی فراگیر[4] گذرواژه‌ها**

یک روش جدید برای انتشار باج‌افزار، جستجوی فراگیر اطلاعات موردنیاز برای ورود کاربر در نرم‌افزارهایی است که بر روی سرور مورد استفاده قرار می‌گیرند. مهاجمانی که باج‌افزار Bucbi را به کار می‌برند، از این روش برای به دست آوردن دسترسی ثابت به سرورهای دارای پروتکل RDP[5] استفاده می‌کنند. سپس Bucbi فایل‌های موجود در کامپیوترها و سایر سرورهایی که از طریق RDP به آن‌ها دسترسی دارد را رمزنگاری می‌کند.

- **بهره‌برداری از آسیب‌پذیری‌های سرور**

همچنین دیده شده است که مهاجمان برای دسترسی به شبکه یک سازمان، نرم‌افزارهای آسیب‌پذیری را که روی سرور اجرا شده‌اند هدف قرار می‌دهند. باندی که در پشت پرده باج‌افزار SamSam قرار دارد، برای یافتن و بهره‌برداری از آسیب‌پذیری‌ها از ابزارهایی که به طور آزاد در دسترس عموم هستند استفاده می‌کنند و از این طریق بدافزار خود را در سرتاسر شبکه منتشر می‌کنند.

علاوه بر این، خانواده باج‌افزار Linux.Encoder وب‌سرورهای لینوکس را هدف قرار می‌دهد. مهاجمان به منظور آلوده کردن قربانیان از آسیب‌پذیری‌های موجود در افزونه‌های سایت یا نرم‌افزارهای شخص ثالث بهره می‌برند و سپس Linux.Encoder پوشه‌های مرتبط با فایل‌های وب‌سایت را رمزنگاری می‌کند.

- **پیام کوتاه و اپ‌استورهای شخص ثالث**

تهدیدات باج‌افزاری اندرویدی از طریق پیام کوتاه منتشر می‌شوند؛ ضمن اینکه این تهدیدات می‌توانند از راه اپ‌استورهای نامعتبر شخص ثالث نیز به درون دستگاه نفوذ کنند.

[4] Brute-forcing
[5] Remote Desktop Protocol

تداوم مقابله با باج‌افزار

- **مقابله از طریق همکاری**

در ۲۵ ژوئیه سال ۲۰۱۶، کسپرسکی با همکاری پلیس ملی هلند، یوروپل (پلیس اروپا) و McAfee پروژه‌ای تحت عنوان No More Ransom را آغاز کردند که یک نمونه منحصر به فرد از توانایی همکاری مشترک دولتی و خصوصی برای مبارزه با مجرمان سایبری و کمک به قربانیان با استفاده از تخصص، راهنمایی و ابزار رمزگشایی است. در حال حاضر این پروژه ۱۲۵ مشارکت‌کننده دارد و به ۳۲ زبان مختلف در دسترس قرار گرفته است. همچنین در پورتال آنلاین آن ابزارهای رمزگشایی فراهم شده که تعدادی از خانواده باج‌افزارها را پوشش می‌دهد. تا اواخر سال ۲۰۱۷، بیش از ۲۸۰۰۰ دستگاه رمزگشایی شده است و آن‌طور که برآورد شده است مجرمان سایبری از دریافت ۹/۵ میلیون دلار باج بی‌نصیب مانده‌اند.

- **مقابله از طریق اطلاع‌رسانی**

آزمایشگاه‌های امنیتی معتبر از ابتدا تهدیدات باج‌افزار را کنترل کرده‌اند و به طور منظم اخبار مربوط به تهدیدات بدافزارهای باج‌گیر را به‌روزرسانی می‌کنند تا آگاهی راجع به این موضوع را افزایش دهند.

- **مقابله از طریق فناوری**

کسپرسکی روش حفاظت چند لایه از جمله ابزار رایگان آنتی‌باج‌افزار را برای مقابله با این تهدید توسعه و ارائه می‌دهد که هر کسی می‌تواند آن را بدون نیاز به نصب آنتی‌ویروس کسپرسکی دانلود و استفاده کند. همچنین محصولات کسپرسکی شامل یک فناوری جدید با نام "مراقب سیستم"[6] است که می‌تواند تغییرات مخرب ایجاد شده بر روی یک دستگاه مانند رمزنگاری فایل‌ها یا دسترسی مسدود شده به مانیتور را مسدود و به حالت اول برگرداند.

[6] System Watcher

راهکارهای پیشنهادی

- بدون شک همیشه پیش‌گیری از آلودگی بهترین نتیجه را می‌دهد. ایمیل و اکسپلویت‌کیت‌ها متداول‌ترین مسیرهای آلودگی برای باج‌افزار هستند؛ اما سازمان‌ها باید از نسل جدید باج‌افزار خودتکثیر که با استفاده از اطلاعات کاربری مسروقه و بهره‌برداری از آسیب‌پذیری‌ها در سرتاسر شبکه منتشر می‌شوند نیز آگاه باشند. اتخاذ یک شیوه دفاعی قدرتمند در مقابل تمام این مسیرهای آلودگی، به کاهش ریسک آلودگی کمک خواهد کرد.
- توصیه می‌شود که کاربران نهایی، هر ایمیل مشکوکی که دریافت می‌کنند (به‌خصوص آن‌هایی که حاوی لینک و یا پیوست هستند) را بلافاصله حذف کنند.
- در مورد اسناد پیوست شده microsoft office که کاربران را وادار به فعال‌سازی ماکروها می‌کنند احتیاط ویژه به خرج دهید. با اینکه می‌توان از ماکروها استفاده‌های قانونی نظیر خودکارسازی وظایف را انجام داد؛ اما مهاجمان اغلب برای انتقال بدافزار از طریق اسناد office از ماکروهای مخرب استفاده می‌کنند. microsoft به منظور کاهش خطر این مسیر آلودگی، بارگذاری ماکروها را در اسناد office خود از حالت پیش‌فرض خارج کرده است. ممکن است مهاجمان به منظور قانع کردن کاربران برای فعال‌سازی اجرای ماکروها، از روش‌های مهندسی اجتماعی استفاده کنند؛ در نتیجه توصیه می‌شود که کاربران از فعال‌سازی ماکروها در microsoft office اجتناب کنند.
- شبکه را برای شناسایی تمام کامپیوترهای آلوده به طور کامل اسکن کنید. کامپیوترهای آلوده باید تا وقتی که به طور کامل پاکسازی و ترمیم نشده‌اند، از شبکه جدا بمانند.
- پشتیبان‌گیری از داده‌های مهم، یکی از ارکان اساسی مبارزه با آلودگی‌های باج‌افزاری است؛ اما با توجه به اینکه در مواردی از حملات باج‌افزار، فایل‌های پشتیبان نیز رمزنگاری شده‌اند، روش پشتیبان‌گیری نباید جایگزین یک راهبرد امنیتی قوی شود.
- قربانیان باید آگاه باشند که پرداخت مبلغ باج همیشه جواب نمی‌دهد. ممکن است مهاجمان کلید رمزگشایی را نفرستند، فرایند رمزگشایی را با بی‌دقتی انجام دهند و به فایل‌ها آسیب بزنند و یا اینکه بعد از دریافت مبلغ اولیه، درخواست بیشتری را مطرح نمایند.

در پایان ممکن است این سوال پیش بیاید که آیا جایگزین سودآورتری برای مجرمان سایبری با انگیزه سود مالی وجود دارد؟ همان‌طور که گزارش کسپرسکی با عنوان "پیش‌بینی تهدیدات سایبری برای پول‌های رمزنگاری شده در سال ۲۰۱۸" حاکی از افزایش حملات هدفمند به منظور نصب استخراج‌کنندگان است، احتمال جایگزینی حملات باج‌افزاری با استخراج پول رمزنگاری شده وجود دارد. در حالیکه باج‌افزار درآمدزایی زیاد اما فقط برای یک بار را دارد، استخراج‌کنندگان می‌توانند کسب درآمد پایین‌تر اما درازمدتی را داشته باشند و همین مسئله می‌تواند در وضعیت آشفته فعلی باج‌افزار برای بسیاری از مهاجمان وسوسه-انگیز باشد؛ اما مطمئناً حملات باج‌افزاری در حال حاضر متوقف نخواهند شد.

منابع:

[1] Kaspersky Lab, "*Overall Statistics for 2017*", Kaspersky Security Bulletin, 14 December 2017.
[2] Kaspersky Lab, "*Story of the Year 2017*", Kaspersky Security Bulletin, 28 November 2017.
[3] Symantec, "*Ransomware 2017",* An ISTR Special report, July 2017, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf
[4] https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html
[5] https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
[6] https://www.bleepingcomputer.com/news/security/necurs-and-gamut-botnets-account-for-97-percent-of-the-internets-spam-emails/