شماره پنجم – نیمه اول دی ۱۳۹۶

خبرنامه "آپا" دانشگاه محقق اردبیلی

در این شماره می‌خوانیم:

- ✓ ده آسیب پذیری کاربران در حوزه امنیت مجازی
- ✓ مشاهده و تشخیص روزانه ۳۶۰ هزار نمونه بدافزار جدید در سال ۲۰۱۷
- ✓ شیوع باج‌افزار جدید با نام Satan's Doom
- ✓ افشای RootsWeb حاوی اطلاعات ۳۰۰هزار کاربر
- ✓ آسیب‌پذیری با درجه بحرانی در محصولات VMware
- ✓ هدف قرار دادن سرورهای پایگاه‌داده برای استخراج پول دیجیتالی
- ✓ اعداد و ارقام باج‌افزارها در سال ۲۰۱۷ [اینفوگرافی]
- ✓ برجسته‌ترین نفوذهای سال ۲۰۱۷
- ✓ کشف درپشتی در افزونه Captcha وردپرس
- ✓ بهره‌برداری بات‌نت Satori از آسیب‌پذیری روز صفر مسیریاب‌های Zombify شرکت Huawei
- ✓ شیوه‌های رایج استفاده شده توسط بدافزار
- ✓ آشنایی با واژگان حوزه امنیت

045 31505718
cert@uma.ac.ir
اردبیل - خیابان دانشگاه - دانشگاه محقق اردبیلی

ده آسیب پذیری کاربران در حوزه امنیت مجازی

ایمن سازی فضای مجازی هرگز به اندازه زمان فعلی، مهم و دشوار نبوده است. برای بسیاری از مدیران فناوری اطلاعات، تشخیص اینکه تامین امنیت را از کجا شروع کنند، یک چالش بزرگ است. گام اول تامین امنیت، تنظیم برنامه امنیت فضای مجازی می‌باشد. این برنامه باید به صورت منظم و دوره‌ای حداقل سالی یکبار بررسی شود. در ادامه ده آسیب‌پذیری کاربران در حوزه امنیت فضای مجازی ذکر می‌شود که باید در برنامه سالیانه بررسی شود.

عدم وجود یا ناقص بودن برنامه امنیتی: ضروری است تا سازمان یک برنامه مصوب و رسمی داشته باشد که وظایف افراد مشخص و هر فردی مسئول پاسخ‌گویی به کار از قبل تعیین شده باشد. عدم وجود یک برنامه مصوب برای برقراری امنیت فضای مجازی یک مشکل مهم بوده و نتیجه آن آسیب‌پذیری سیستم در برابر تهدیدات می‌باشد. اگر سازمان شما یک برنامه امنیتی مصوب دارد، باید آن را هرساله بازبینی و بروزرسانی کنید و مطمئن شوید که سازمان با برنامه همراستا می‌باشد. فراموش نکنیم در امنیت فضای مجازی هر شخص مسئول است.

عدم انجام ارزیابی آسیب‌پذیری: انجام ارزیابی امنیت موجب شناسایی درزهای موجود در سیاست‌های امنیتی، روال‌های پاسخ‌گویی به رخدادها و مکانیزم‌های ایمن سازی (مانند دیوار آتش) می‌شود. این ارزیابی امنیتی، امکان بهره‌برداری از آسیب‌پذیری‌های امنیتی را کاهش می‌دهد.

عدم ارزیابی ضعف‌ها و درزهای سیستم با توجه به نیازهای قانونی: در واقع این آسیب‌پذیری‌ها به ایرادات موجود در موارد حقوقی مرتبط است که از ضعف فنی و مدیریتی خصوصا در سرویس‌های مالی، سیستم‌های درمانی و بخش‌هایی که باید حریم خصوصی کاربران تامین گردد، سرچشمه می‌گیرد.

عدم وصله کردن منظم: عدم آگاهی سریع از آسیب‌پذیری‌های شناخته شده، تبعات فراوانی دارد. وجود یک سند که تمام الزامات وصله کردن در آن بیان شده باشد و اعمال به موقع وصله آسیب‌پذیری‌های شناخته شده، موجب جلوگیری از سوءاستفاده نفوذگران خواهد شد.

عدم وجود برنامه برای تهدیدات داخلی: در بسیاری از موارد افشای اطلاعات توسط کارمندان و یا مشتریان مورد اعتماد انجام می‌شود. عدم وجود برنامه‌ای جهت ارزیابی تهدیدات داخلی، آسیب‌پذیری به این نوع از تهدیدات افزایش می‌دهد.

عدم ارتباط با جامعه مجازی: آیا از شکسته شدن معروف‌ترین پروتکل رمزنگاری wifi باخبر هستید؟ آیا می‌دانید موسسه ملی استانداردها و تکنولوژی (NIST) راهنمایی‌های جدیدی برای مدیریت پسورد ارائه داده است؟ این موارد چشم‌اندازی از تغییرات مداوم امنیت فضای مجازی می‌باشد. شما باید با جامعه امنیت فضای مجازی، از جمله مشاوران امنیتی در ارتباط باشید تا در حوزه امنیت آموزش دیده و از بهترین شیوه‌ها و تکنولوژی‌های ایمن‌سازی بهره‌مند شوید.

فقدان مدیریت دقیق تنظیمات: سازمان‌ها جهت جلوگیری از آسیب‌پذیری سیستم در برابر تهدیدات، قبل از هر تغییر در پیاده‌سازی یا هر انتشار آنلاین سامانه، باید تنظیمات مهم امنیتی سیستم ارتباطی و سخت افزارهای مرتبط را بررسی کنند. در حال حاضر استفاده از تنظیمات پیش‌فرض مانند پسورد پیش‌فرض خطری است که امنیت بسیاری از سیستم‌ها را تهدید می‌کند و سازمان‌ها باید این تنظیمات را بازبینی کنند.

عدم مدیریت دقیق دسترسی راه دور: اگر پرسنل شما اجازه دسترسی از راه دور داشته باشند، ممکن است از این طریق مورد حمله قرار بگیرید. تامین امنیت سرویس‌های دسترسی از راه دور، نیازمند استفاده از نیروی متخصص و مکانیزم‌های کنترلی مانند نظارت بر دسترسی‌های راه دور می‌باشد.

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir

عدم توجه به داده‌های فضای مجازی: هر حوزه صنعتی دارای داده‌های مخصوص به خود می‌باشد. در صورت عدم توجه به این داده‌ها، نمی‌توانید تصمیم‌های آگاهانه در مورد تجزیه و تحلیل آسیب‌پذیری‌های موجود در سامانه‌های صنعت خود بگیرید.

عدم وجود برنامه‌ای برای پاسخ به حوادث: در هر سطحی از امنیت، باز هم باید برای احتمال وجود یک حادثه یا خرابی داده آماده باشید. عدم وجود برنامه مدون، جامع و تست‌شده برای پاسخ‌گویی به حوادث، شما را در برابر حملات آسیب‌پذیر می‌کند.

باید توجه داشت که این یک لیست کامل نبوده و ممکن است لیست شما متفاوت باشد. امید است که این توصیه-ها شما را به تفکر درمورد حفاظت از فضای مجازی خود وادارد.

منبع خبر: natlawreview مترجم: مهندس سمیرا سیفی

مشاهده و تشخیص ۳۶۰ هزار نمونه بدافزار جدید در هر روز از سال ۲۰۱۷

در سال ۲۰۱۷ هر روز بطور متوسط حداقل ۳۶۰ هزار فایل خطرناک شناسایی شده که نسبت به سال گذشته رشد ۱۱,۵ درصدی داشته است.

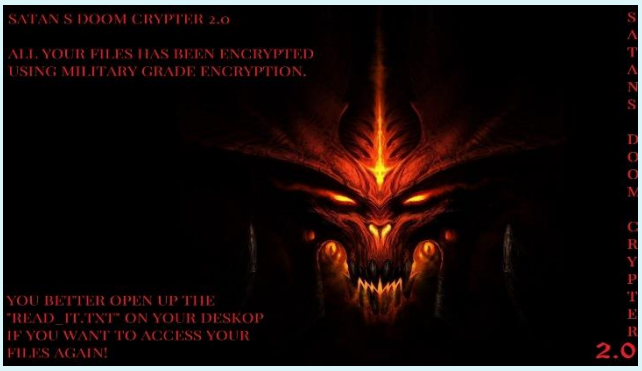
بر اساس گزارش آزمایشگاه شرکت کسپرسکی در سال ۲۰۱۷، ۷۸ درصد از این فایل‌های مخرب جدید (که در آزمایشگاه این شرکت تشخیص و بررسی شده‌اند) در گروه بدافزار قرار می‌گیرند. ویروس‌ها نیز ۱۴ درصد از این فایل‌ها را به خود اختصاص داده‌اند و فایل‌های باقی مانده (یعنی ۸ درصد) نرم‌افزارهای تبلیغاتی بوده‌اند. بر اساس یافته‌های کسپرسکی تأثیرات رشد این فایل‌ها بطور گسترده قابل مشاهده است. این یافته‌ها نشان می‌دهد که ۲۹,۴ درصد از کامپیوترهای کاربران حداقل یک بار در سال، تجربه حملات بدافزارهای آنلاین را داشته‌اند و ۲۲ درصد از کامپیوترهای کاربران تحت حمله برنامه‌های تبلیغاتی قرار گرفته‌اند. از جمله نکات قابل توجهی که در این گزارش آمده است، می‌توان به این مورد اشاره کرد که فعالیت ویروس‌ها در ۵ تا ۷ سال گذشته با توجه به پیچیدگی توسعه و بهره‌وری کم آن‌ها به طور چشم‌گیری کاهش یافته‌است. با این حال، تعداد کمی از آن‌ها همچنان توسعه داده می‌شوند و ۱۴ درصد از آمار تشکیل یافته را به خود اختصاص داده است.

افزایش چمشگیر حملات باج‌افزاری در طول چندین سال گذشته بدلیل وجود یک اکوسیستم جنایی در حال رشد، پشت این نوع از تهدیدات می‌باشد. براساس اظهارات محققان شرکت کسپرسکی، بازیگران این اکوسیستم هر روز صدها نمونه جدید از بدافزارها را تولید می‌کنند. گذشته از آن، در سال ۲۰۱۷ شاهد Crypto-Minerها، گونه‌ای از بدافزارها که مجرمان اینترنتی به تازگی شروع به استفاده از آن‌ها کرده‌اند، بوده‌ایم. با این حال، افزایش میزان کشف این بدافزارها می‌تواند باعث بهتر شدن تکنولوژی تشخیص شده و به شناسایی و به دام انداختن بدافزارهای بیشتر کمک بسزایی کند. تعداد بدافزارهای جدید برای اولین بار در سال ۲۰۱۱ محاسبه گردید که تعداد کل آن‌ها برابر با ۷۰ هزار بود. از آن زمان تاکنون، این رقم پنج برابر شده است. همچنین، پس از یک کاهش جزئی در سال ۲۰۱۵، تعداد فایل‌های مخربی که روزانه شناسایی می‌شوند برای بار دوم در حال افزایش است. Vyacheslav Zakorzhevsky مدیر تیم ضدبدافزار در شرکت کسپرسکی بیان کرد که: "در سال ۲۰۱۵، ما شاهد افت قابل ملاحظه‌ای در تشخیص‌های روزانه بوده-ایم. تصور ما در آن زمان این بود که تولید بدافزارهای جدید برای مجرمان اهمیت کمتری پیدا کرده است و ممکن است توجه خود را به استفاده مجدد از بدافزارهای قدیمی تغییر داده باشند. در طول دو سال گذشته، تعداد بدافزارهای جدیدی که کشف کرده‌ایم در حال افزایش بوده که نشان دهنده این است که علاقه به تولید بدافزارهای جدید دوباره احیا شده است."

منبع :info-security مترجم: مهندس ابوالفضل علیقلی وند

شیوع باج‌افزار جدید با نام Satan's Doom

Satan's Doom یک بدافزار از نوع رمزگذار فایل می‌باشد که تا امروز تعداد زیادی از آنتی‌ویروس‌ها قادر به شناسایی آن شده‌اند. در چند روز اخیر، هدف اصلی این باج‌افزار، کاربران ویندوزی بوده است. فشار حمله این باج‌افزار روزبه‌روز رو به افزایش است و این مسئله، مشکل نسبتا بزرگی برای سازمان‌ها به وجود آورده است. این باج‌افزار مانند بقیه باج‌افزارها دسترسی به فایل‌های سیستم را غیرفعال و به آن‌ها پسوند locked. اضافه کرده و از کاربران با نشان دادن پیامی، برای بازگرداندن فایل-های رمزشده درخواست پرداخت مبلغی به عنوان باج می‌کند. این باج‌افزار بگونه‌ای طراحی شده است که می-تواند بصورت مخفیانه سیستم را قفل کرده و تقریبا تمامی داده‌های مهم را رمزگذاری کند.



باج‌افزار Satan's Doom عمدتا برای ترساندن کاربر استفاده می‌شود و روشی برای دریافت پول از کاربر قربانی شده می‌باشد. مکانیزم پیاده‌سازی این باج‌افزار به گونه‌ای است که بعد از بازگردانی فایل‌های رمز شده با استفاده از کلید ارائه شده توسط مهاجمان، همچنان دسترسی به سیستم توسط مهاجمان امکان‌پذیر بوده و قادر به رمزگذاری مجدد فایل‌ها می‌باشند.

از جمله روش‌های نفوذ این باج‌افزار در سیستم‌های کامپیوتری، می‌توان به موارد زیر اشاره کرد:

۱- انتقال از طریق برنامه‌های رایگان، نرم‌افزارهای جاسوسی، دستگاه‌های آلوده شده مانند فلش، منابع اشتراک فایل، هکرهای تورنت و بسیاری روش‌های دیگر.

۲- انتقال از طریق فایل آلوده پیوست‌شده به ایمیل‌ها

طراحان این باج‌افزار روش‌های انتقال و آلوده‌سازی سیستم را بصورت مداوم تغییر می‌دهند اما این باج‌افزار عمدتا از طریق اینترنت توزیع می‌گردد. بنابراین به‌شدت توصیه می‌گردد که هنگام کار در اینترنت محتاط بوده و از دانلود فایل‌های ناشناس خودداری کنید. فایل‌هایی که این باج افزار بر روی آن‌ها کار کرده و عمل رمزگذاری را روی آن‌ها اعمال می‌کند شامل موارد زیر می‌باشد:

txt – jar – exe – dat – contact – setting – doc – docx – xls – xldx – ppt – pptx – odt – jpg – png – csv – py – sql – mdb – sln – php – asp – aspx – html – htm – xml – psd – pdf – dll – c – cs – mp3 – mp4 – f4d – dwg – cpp – zip – rar – mov – rtf – bmp – mkv – avi – apk – lnk – iso - 7zip – ace – arj – bz2 – cab – gzip – lzn – tar – uue – xz – z – 001 – mpeg – mpg – core – crproj – pdb – ico – pas – db – torrent – asf – waw – docm – wmv – wav – ac3 – raw – cms – js

منابع: nowremovevirus ، removemalwarevirus

تحلیل‌گر و مترجم: مهندس ابوالفضل علیقلی وند

افشای فایلی حاوی اطلاعات ۳۰۰هزار کاربر

سرور RootsWeb، از سال ۲۰۰۰ میزبان سایت Ansectory می‌باشد. این سرور فایلی حاوی ایمیل، اطلاعات ورود و کلمه عبور ۳۰۰،۰۰۰ کاربر را در یک پست انتشار داد و خوانندگان این پست پس از مشاهده لیست، تیم امنیتی Ancestry را از افشای این اطلاعات باخبر کردند. برخی از اطلاعات این فایل متعلق به افرادی است که دیگر سرویسی دریافت نمی‌کنند اما اطلاعات ۵۵۰۰ کاربر فعال که از سرویس‌های رایگان و پولی دو سایت RootsWeb.com و Ancestry.com استفاده می‌کنند، نیز افشا شده است.

Ancestry به همه کاربرانی که اطلاعات آن‌ها افشا شده، اطلاع داده است که برای جلوگیری از قفل شدن حساب خود باید پسورد جدید ثبت کنند. همچنین RootsWeb.com برای مدتی به جهت بهبود زیرساخت امنیتی آفلاین می‌باشد.

منبع خبر:darkreadin مترجم: مهندس سمیرا سیفی

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir

آسیب‌پذیری با درجه اهمیت بحرانی در محصولات VMware

پژوهشگران امنیت، چند آسیب‌پذیری با درجه اهمیت بحرانی در محصولات مربوط به VMware یافته‌اند که این آسیب‌پذیری‌ها امکان اجرای دستورات از راه دور را برای نفوذگران فراهم می‌کنند. برخی از تحلیل‌هایی که بر روی این آسیب‌پذیری‌ها صورت گرفته است، نشان‌دهنده سوءاستفاده از اجرای Virtual Network Computing در محصولات VMware است. VNC یک سیستم اشتراک‌گذاری دسکتاپی گرافیکی است که از پروتکل RBF برای کنترل از راه دور کامپیوتر دیگر استفاده می‌کند. آسیب‌پذیری‌ها به شرح زیر است:

شناسه CVE-2017-4941 و CVE-2017-4933: این دو آسیب‌پذیری توانست به یک نشست VNC احراز هویت شده، اجازه دهد تا از طریق یک مجموعه خاص از بسته‌های VNC به ترتیب سرریز پشته و سرزیر heap ایجاد کند. بهره‌برداری موفق از این آسیب‌پذیری‌ها موجب اجرای کد از راه دور در ماشین مجازی از طریق یک نشست VNC احزار هویت شده می‌شود. شایان ذکر است، به منظور بهره‌برداری موفق از این آسیب‌پذیری‌ها در نرم افزار VMware ESXi باید VNC به صورت دستی در فایل تنظیمات vmx. ماشین مجازی فعال شده باشد و ترافیک VNC از طریق فایروال داخلی ساخته شود.

شناسه CVE-2017-4940: این آسیب‌پذیری ممکن است امکان ذخیره XSS را فراهم کند. مهاجم می‌تواند این آسیب‌پذیری را با تزریق کد JavaScript مورد سوء-استفاده قرار دهد و زمانی که سایر کاربران به Host Client دسترسی پیدا می‌کنند، آن کد اجرا گردد.

لازم به ذکر است آسیب‌پذیری‌های فوق در نسخه‌های ESXi550-201709101-SG, ESXi550-201709102-SG, ESXi600-201711101-SG, ESXi600-201711103-SG, ESXi650-201710401-BG, ESXi650-201712103-SG Workstation 12.5.8, Fusion 8.5.9 رفع شده است.

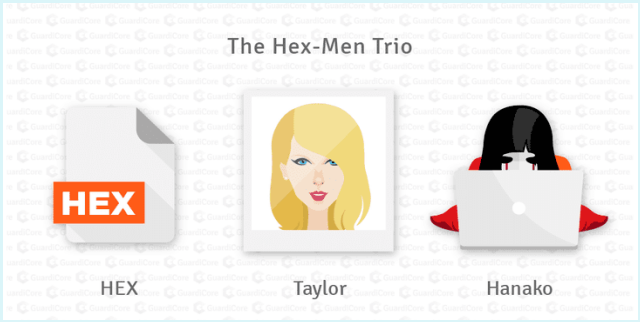
منبع خبر: securitytracker. جمع‌آوری: مهندس معصومه خیری

نرم‌افزار	نسخه آسیب‌پذیر	شناسه آسیب‌پذیری
VMware EXSi	نسخه 6.0 قبل از ESXi600-201711101-SG	CVE-2017-4941
	نسخه 5.5 قبل از ESXi550-201709101-SG	CVE-2017-4941
	نسخه 6.5 قبل از ESXi650-201710401-BG	CVE-2017-4933
	نسخه 6.0 قبل از ESXi650-201712103-SG نسخه 5.5 قبل از ESXi600-201711103-SG نسخه 5.5 قبل از ESXi550-201709102-SG	CVE-2017-4940
VMware WorkStation	نسخه‌های قبل از 12.5.8	CVE-2017-4941 CVE-2017-4933
VMware Fusion	نسخه‌های قبل از 8.5.9	CVE-2017-4933 CVE-2017-4941

هدف قرار دادن سرورهای پایگاه‌داده برای استخراج پول دیجیتالی

محققان امنیتی چندین حمله را که توسط یک گروه چینی صورت گرفته، شناسایی کرده‌اند. این گروه سرورهای پایگاه‌داده را برای استخراج پول دیجیتالی، دزدیدن اطلاعات حساس و ساخت بات‌نت برای انجام حملات DDOS مورد حمله قرار می‌دهند.

محققان شرکت امنیتی GuardiCore Labs هزاران حمله را که در ماه‌های اخیر اتفاق افتاده است، مورد بررسی قرار داده و حداقل سه نوع حمله به نام‌های HEX، Hanako و Taylor را شناسایی کردند. این حملات سرورهای MSSQL و MySQL را در سیستم‌عامل‌های ویندوز و لینوکس مورد هدف قرار می‌دهند.



اهداف این سه حمله متفاوت می‌باشد:

- حمله Hex تروجان‌هایی با قابلیت دسترسی از راه دور (RATs) و استخراج کننده پول دیجیتالی را بر روی دستگاه‌های مورد حمله نصب می‌کند
- حمله Taylor یک درپشتی و Keylogger نصب می‌کند
- حمله Hanako از دستگاه‌های آلوده به منظور ساخت بات‌نت برای حملات DDoS استفاده می‌کند

تاکنون، هر ماه محققان صدها حمله Hex و Hanako و ده‌ها هزار حمله Taylor را ثبت کرده و پی برده‌اند که بیشتر سیستم‌های آسیب‌دیده در چین و بعضی از آن‌ها در تایلند، ایالات‌متحده و ژاپن قرار دارند.

مهاجمان از حملات Brute Force برای دسترسی غیرمجاز به سرورهای پایگاه‌داده هدف استفاده کرده و به منظور دسترسی مداوم به پایگاه‌داده و جلوگیری از ثبت شدن اقداماتشان در لاگ‌ها یک سری دستورات SQL از پیش تعریف‌شده‌ای را اجرا می‌کنند. مهاجمان به منظور دسترسی مداوم به پایگاه‌داده قربانی، در هر سه نوع حمله (Hex، Hanako و Taylor) نام کاربری مخفی در پایگاه‌داده ایجاد کرده و پورت Remote Desktop را باز می‌کنند. این کارها کمک می‌کنند تا مهاجمان بتوانند از راه دور مرحله بعدی حمله خود را به انجام برسانند. این مرحله شامل دانلود و نصب یک استخراج کننده‌ی پول دیجیتالی، تروجانی با قابلیت دسترسی از راه دور یا یک بات‌نت برای حملات DDoS می‌باشد. درنهایت، مهاجمان برای مخفی کردن ردپای خود، هرگونه رجیستری ویندوز، فایل و فولدر ورودی غیرضروری را با استفاده از فایل‌های اجرایی batch و اسکریپت‌های ویژوال‌بیسیک حذف می‌کنند.

اگر نام‌های کاربری زیر در پایگاه‌داده یا سیستم شما موجود است باید سیستم خود را جهت تشخیص این که آیا توسط این گروه هکری چینی مورد حمله قرار گرفته-اید یا خیر، بررسی کنید:

- hanako
- kisadminnew1
- 401hk$
- Guest
- Huazhongdiguo110

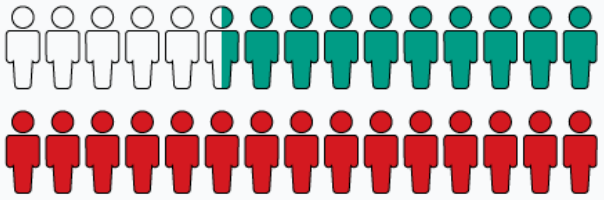
محققان توصیه می‌کنند که برای جلوگیری از به خطر افتادن سیستم‌هایتان، نه تنها از رمز عبور قوی برای پایگاه‌داده خود استفاده کنید بلکه همیشه راهنماهای سخت‌افزاری پایگاه‌داده‌ها (که توسط تیم توسعه‌دهندگان MySQL و مایکروسافت ارائه شده‌اند) را دنبال کنید. همچنین سیستم‌هایی که به پایگاه‌داده متصل هستند را کنترل کرده و این فهرست را به حداقل برسانید و هر تلاش اتصال از یک IP یا دامنه‌ای که به این لیست تعلق ندارد را مسدود کنید.

منبع خبر: thehackernews مترجم: مهندس سحر علیزاده

اعداد و ارقام باج افزارها در سال ۲۰۱۷

در حدود ۹۵۰,۰۰۰

نفر از کاربران محصولات شرکت کسپرسکی در سال ۲۰۱۷ مورد حمله قرار گرفته اند، در حالی که این عدد در سال ۲۰۱۶ برابر ۱,۵ میلیون کاربر بود.



نصف شدن

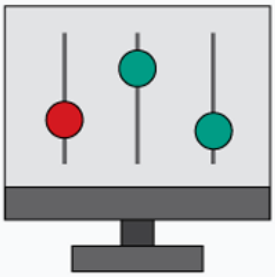
تعداد خانواده های باج افزاری جدید:

کاهش پیدا کردن تعداد خانواده ها از ۶۲ مورد در سال ۲۰۱۶ به ۳۸ مورد در سال ۲۰۱۷

دو برابر شدن

تقریبی تعداد تغییرات باج افزارها

به بیش از ۹۶,۰۰۰ در سال ۲۰۱۷
۵۴,۰۰۰ مورد در سال ۲۰۱۶



از قربانیان مورد حمله قرار گرفته توسط باج افزارها

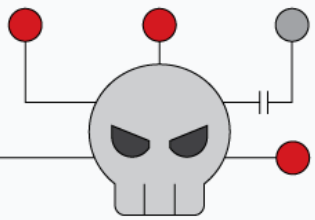
کاربران بخش تجاری و سازمانی

۶۵% بخش‌های تجاری موردحمله در سال ۲۰۱۷ با

از دست رفتن دسترسی

به قسمت قابل توجهی از داده خود مواجه شدند

سه شیوع باج افزاری بزرگ سال



WANNACRY در ۱۲ ماه May،
EXPETR در ۲۷ ماه June، و
BADRABBIT در اواخر ماه October

WANNACRY به تنهایی ۷۰۰,۰۰۰ قربانی داشته است

یک نفر از هر ۶ نفری که **باج را پرداخت کرده‌اند**

هیچ وقت

داده خود را بازیابی نکردند

برجسته‌ترین نفوذهای سال ۲۰۱۷

با توجه به پایان رسیدن سال ۲۰۱۷ میلادی سعی کردیم چند مورد از مطرح‌ترین نفوذها و اتفاقات این سال را برای شما معرفی کنیم.

بدافزارهای Crashoverride و Triton: تحلیل‌گران در سال‌های قبل درمورد افزایش تعداد نفوذ به زیرساخت‌ها هشدارهای لازم را داده بودند. با توجه به اینکه برای سالیان متمادی ویروس Stuxnet تنها بدافزار شناخته شده برای تجهیزات صنعتی بود (برای اولین بار در سال ۲۰۱۰ کشف گردید)، این احتمال روزبه‌روز قوت می‌گرفت تا اینکه در سال ۲۰۱۷ تحقیقات گروه‌های مختلف امنیتی دو نوع سلاح دیجیتالی جدید را آشکار کرد. متخصصان شرکت‌های امنیتی ESET و Dragos علت خاموشی‌های پایتخت اوکراین(شهر کیف) در اواخر سال ۲۰۱۶ را بدافزاری با نام Industroyer یا Crashoverride اعلام نمودند. ابزاری که می‌تواند خود را براساس زیرساخت‌های موجود انطباق داده و باعث بروز مشکلات جدی گردد. امکان استفاده و دسترسی مجدد و همچنین مورد حمله قرار دادن چندین هدف در یک زمان نیز از دیگر ویژگی‌های این بدافزار جدید می‌باشد.

از سوی دیگر متخصصان امنیتی FireEye نیز بدافزار دیگری تحت عنوان Triton یا Trisis کشف کرده‌اند که منطقه خاورمیانه را موردهدف قرارداده است. این بدافزار که هنوز مشخص نیست برای زیرساخت‌های کدام کشور توسعه داده شده است، در تجهیزات شرکت Schneider Electric که اغلب در صنایع گاز و نفت و در برخی موارد در صنایع هسته‌ای مورد استفاده قرار می‌گیرند، دیده شده است.

شرکت Equifax: نشت اطلاعاتی بیش از ۱۴۵ میلیون نفر شامل تاریخ تولد، نشانی محل زندگی، شماره کارت-های بانکی مواردی بود که در این نفوذ به بیرون درز پیدا کرد. به دلیل حساسیت اطلاعات لو رفته ، این ماجرا یکی از بزرگترین نشت‌های اطلاعاتی تاریخ بوده است.

Yahoo: این شرکت در ماه سپتامبر سال ۲۰۱۶ اعلام کرد که ۵۰۰ میلیون از حساب‌های کاربری این شرکت در سال ۲۰۱۴ مورد سرقت اطلاعات قرار گرفته است. سپس در ماه دسامبر سال ۲۰۱۶ نیز اعلام کرد که یک میلیارد از حساب‌های کاربری در سال ۲۰۱۶(ماه آگوست) تحت تاثیر نفوذی دیگر قرار گرفته‌اند. جالب‌تر اینکه یاهو بعدا در ماه اکتبر ۲۰۱۷ اعلام کرد اطلاعات تمامی حساب‌های کاربری موجود (در آن زمان ۳ میلیارد) به سرقت رفته است.

گروه Shadow Brokers: گروه هکری که در ماه آگوست سال ۲۰۱۶ با ارائه یک نمونه ابزار از مجموعه ابزاری که از آژانس ملی امنیت آمریکا (NSA) به سرقت برده بود، خود را به جهانیان معرفی کرد. این گروه با انتشار بعضی از نکات، آسیب‌پذیری‌ها و ابزارهای امنیتی در طول سال ۲۰۱۶ برای خود نامی دست‌وپا کرد تا اینکه در ماه آوریل ۲۰۱۷ با ارائه اکسپلویت EternalBlue باعث به وجود آمدن بدافزارهای خطرناکی مانند WannaCry گردید. این گروه با راه‌اندازی یک حراجی قصد فروش ابزارهای سرقت شده با قیمت پایه یک میلیون دلار را نیز داشت که از نتیجه این حراجی اطلاعاتی دردست نیست.

باج‌افزار WannaCry: در دوازدهم ماه می ۲۰۱۷، نوعی باج‌افزار در سرتاسر جهان ظهور پیدا کرد که با نام WannaCry شناخته شد. این باج‌افزار با استفاده از آسیب‌پذیری موجود در سرویس SMB سیستم‌عامل‌های ویندوز با نام EternalBlue به شیوع خود پرداخت. میزان شیوع و گستردگی این باج‌افزار به حدی بود که از شرکت‌های بزرگ تا مراکز خدمات عمومی مانند بیمارستان‌ها تحت تاثیر قرار گرفتند. خوشبختانه با توجه به رفتار و مکانیزم این بدافزار متخصصان امنیتی توانستند این باج‌افزار را کنترل کنند.

باج‌افزاهای NotPetya و BadRabbit: در اواخر ماه ژوئن ۲۰۱۷ بود که موج جدیدی از باج‌افزارها کشورهای مختلف رو تحت تاثیر خود قرار داد. باج‌افزار NotPetya

کشورهای اکراین و روسیه را برای آغاز حمله خود انتخاب نمود. در کشور اوکراین بخش‌های مختلف از جمله بانک مرکزی اوکراین و سیستم حمل‌ونقل عمومی قربانی این باج‌افزار بودند. در ماه اکتبر نیز باج‌افزار BadRabbit موج جدید دیگری را عمدتا در کشورهای آلمان، ترکیه، بلغارستان و چند کشور دیگر اروپای شرقی شکل داد. برای اطلاعات بیشتر و مشاهده بررسی باج‌افزار BadRabbit می‌توانید به خبرنامه نیمه دوم آبان مراجعه فرمائید.

افشاگری سایت ویکی‌لیکس درمورد سازمان سیا:

در هفتم ماه مارس ۲۰۱۷ وبسایت معروف افشاگری، ویکی لیکس، مجموعه اسنادی منتسب به سازمان سیا را منتشر کرد. اسناد منتشر شده شامل ابزار هک و عملیات جاسوسی، اشکالات سیستم‌عامل ویندوز و آسیب‌پذیری‌های سیستم‌عامل Android و IOS می‌باشد. ویکی‌لیکس این افشا را در بخش‌های کوچک از یک مجموعه به نام Vault 7 منتشر کرد. این اسناد همچنین توضیحاتی را درباره استفاده از سیگنال Wifi برای ردیابی افراد دارا بود. بر طبق گفته ویکی‌لیکس Vault 7 زرادخانه سازمان سیا در زمینه هک بوده که برای بدافزارها، ویروس‌ها، تروجان‌ها، حملات روز صفر، بدافزارهای کنترل کننده سیستم از راه دور و اسناد مرتبط با آن‌ها بوده است.

همچنین در اوایل ماه نوامبر ویکی‌لیکس دست به افشاگری دیگری نیز زد که بر اساس آن کد منبع ابزارها و روش‌های معرفی شده در مجموعه Vault 7 برای عموم منتشر و این مجموعه را Vault 8 نامید. ویکی‌لیکس در یک پست، کد منبعی تحت عنوان Hive معرفی نمود که ابزار هکی برای ساخت گواهی‌نامه‌های تقلبی برای ارتباط با بدافزارهای موجود در دستگاه‌های آلوده می‌باشد. با اینکه برای ارزیابی میزان تهدید و خسارات احتمالی ناشی از Vault 8 بسیار زود می‌باشد، سازمان‌ها و شرکت‌های مختلف باید میزان مراقبت خود را افزایش دهند تا به بحران امنیتی مشابه با عواقب ابزارهای سرقت شده توسط گروه Shadow Brokers از NSA مانند Wannacry دچار نشوند.

منبع خبر:wired مترجم: مهندس وحید فتحی

کشف درپشتی در افزونه Captcha وردپرس

خرید افزونه‌های پرطرفدار و استفاده از آن‌ها برای اهداف مخرب تبدیل به یک گرایش عمومی در بین نفوذگران شده است. اخیرا شرکت BestWebSoft یکی از افزونه‌های Captcha سیستم مدیریت محتوا وردپرس را به یک خریدار ناشناس فروخت. این خریدار افزونه را به نوعی تغییر داد تا بتواند یک درپشتی (backdoor) را روی سرور استفاده کننده از آن، دانلود و نصب کند.

شرکت WordFence با بررسی کدهای این Captcha دلیل آسیب‌پذیری آن را در وبلاگ خود بیان کرده و با دلایل حذف این افزونه از وبسایت رسمی فروش افزونه‌های وردپرس را شرح داد. با این وجود در حال حاضر بیش از ۳۰۰،۰۰۰ وبسایت از این افزونه استفاده می‌کنند.

افزونه Captcha پس از نصب از پایگاه رسمی وردپرس، به صورت خودکار و بدون اجازه کاربر مدیر، نسخه حاوی درپشتی را از یک آدرس ثانویه بارگزاری می‌کند.

این درپشتی یک Session ورود با دسترسی سطح مدیر برای نفوذگر ایجاد می‌کند و به مهاجم امکان دسترسی به سایتی که از این Captcha استفاده می‌کند را می‌دهد. متاسفانه با فعال کردن فرآیند بروزرسانی خودکار، آثار فایل‌های درپشتی حذف می‌شود و به نظر می‌رسد که اصلا از قبل وجود نداشته است. به عبارتی بروزرسانی به شناسایی نشدن مهاجم کمک می‌کند.

دلیل اضافه کردن درپشتی تا این لحظه مشخص نیست، اما پرداخت هزینه قابل توجه برای یک افزونه پرطرفدار حتما با انگیزه مهمی انجام شده است. در موارد مشابه دیده شده است که باندهای تبهکار سازماندهی شده فضای مجازی، افزونه‌ها و برنامه‌های کاربردی محبوب را با اهداف جاسوسی و تبلیغاتی خریداری می‌کنند. بررسی هویت اصلی خریدار افزونه Captcha نشان می‌دهد که

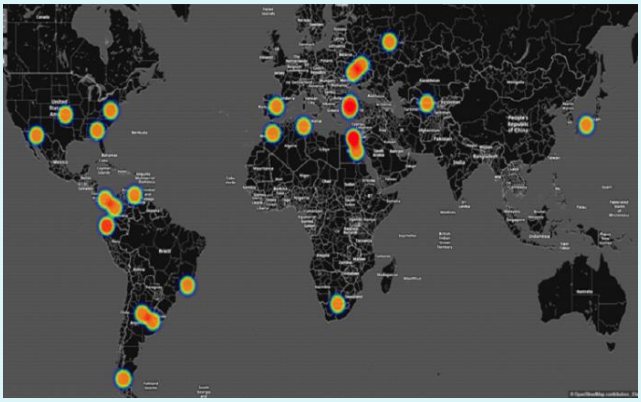
تعداد زیادی وبسایت به نام این فرد در پایگاه‌داده‌های Whois ثبت شده است. نکته جالب این است که تمام این وبسایت‌ها از همین Captcha استفاده می‌کنند.

تیم توسعه‌دهندگان وردپرس با همکاری WordFence این آسیب‌پذیری را وصله کرده است. بنابراین به مدیران وب‌سایت‌هایی که از این افزونه استفاده می‌کنند، توصیه می‌شود که افزونه خود را به آخرین نسخه رسمی Captcha (نسخه ۴,۴,۵) بروزرسانی کنند.

منبع خبر:thehackernew مترجم: مهندس سمیرا سیفی

بهره‌برداری بات‌نت Satori از آسیب‌پذیری روز صفر مسیریاب‌های Zombify شرکت Huawei

با وجود این‌که سازندگان بدافزار اینترنت اشیا Mirai دستگیر شده و به زندان فرستاده شده‌اند اما به دلیل وجود کد منبع آن در اینترنت، هنوز هم انواع مختلفی از این بات‌نت در حال گسترش می‌باشد.



بات‌نت Satori نسخه جدیدی از بات‌نت مشهور Mirai است که هکرها آن را به منظور استفاده از تعداد زیادی از دستگاه‌های اینترنت اشیا مانند مسیریاب‌های خانگی، برای راه‌اندازی مجموعه وسیعی از بات‌ها جهت آغاز حملات DDoS، به کار می‌برند. بات‌نت Satori با استفاده از آسیب‌پذیری روز صفر موجود در مسیریاب‌های Huawei مدل HG532، در حال گسترش می‌باشد.

طبق گزارش ۵ دسامبر سال ۲۰۱۷ شرکت امنیتی چینی Netlab 360، این بات‌نت که در اواخر ماه نوامبر شناسایی شد، توانسته است تنها در مدت ۱۲ ساعت بیش از ۲۰۰ هزار دستگاه را آلوده کند.

طبق گزارش جدید منتشر شده توسط Check Point در روز پنج‌شنبه ۲۱ دسامبر سال جاری، محققان به یک هکر غیر حرفه‌ای به نام "Nexus Zeta" مظنون هستند که با بهره‌برداری از آسیب‌پذیری روز صفر اجرای کد از راه دور (CVE-2017-17215) به این مدل از مسیریاب‌های Huawei دسترسی پیدا کرده است.

این آسیب‌پذیری به دلیل این‌که پیاده‌سازی TR-064 دستگاه‌های Huawei (که یک پروتکل لایه کاربردی برای مدیریت از راه دور است) از طریق پروتکل UPnP(Universal Plug and Play) و پورت ۳۷۲۱۵ در سطح اینترنت افشا شد، رخ داده است.

این آسیب‌پذیری به مهاجمان اجازه داد تا بتوانند از راه دور دستورات خود را اجرا کرده و از این نقص برای دانلود و اجرای کد مخرب بر روی مسیریاب‌های Huawei و آپلود بات‌نت Satori استفاده کنند.

در حمله Satori، هر بات‌نت به گونه‌ای برنامه‌ریزی‌شده است که بتواند سیل عظیمی از بسته‌های TCP و UDP ساخته‌شده را به سمت قربانیان خود ارسال کند.

محققان در سراسر جهان بر روی دستگاه‌های Huawei مدل HG532 حملات مختلفی را مشاهده کرده‌اند، اما کشورهای مورد هدف بیشتر ایالات‌متحده، ایتالیا، آلمان و مصر می‌باشند.

محققان Check Point این آسیب‌پذیری را به شرکت Huawei گزارش داده‌اند و این شرکت آسیب‌پذیری را تأیید کرده و یک بروزرسانی را در جمعه ۲۲ دسامبر ۲۰۱۷ منتشر کرده و به مشتریان خود پیشنهاد داده است که از Huawei NGFW و یا فایروال‌های دیتاسنتر استفاده کنند. همچنین پایگاه‌داده امضا IPS خود را به آخرین نسخه یعنی IPS_H20011000_2017120100 که در تاریخ ۱ دسامبر ۲۰۱۷ منتشر شده است، ارتقا دهند تا بتوانند در برابر این آسیب‌پذیری از خود محافظت کنند.

منبع خبر: thehackernews مترجم: مهندس سحر علیزاده

شیوه‌های رایج شیوع بدافزارها

زندگی در دوران دیجیتال مدرن کامپیوترها می‌تواند بسیاری از خطرات را برای شما و کامپیوتر شما به همراه داشته باشد. کامپیوترها بسیار آسیب‌پذیر هستند و اگر شخصی در سوی دیگر شبکه، بداند که چگونه می‌تواند رخنه‌ای را در سیستم شما پیدا کند ممکن است باعث از بین رفتن اطلاعات و آسیب دائمی به کامپیوتر شما گردد.روش‌های مختلفی توسط بدافزارها جهت آلوده کردن سیستم شما مورد استفاده قرار می‌گیرد. در ادامه رایج‌ترین شیوه‌هایی که مهاجمان برای گسترش بدافزارها استفاده می‌کنند، شرح می‌دهیم.

۱- توزیع از طریق دانلود شدن

بدیهی است هر کسی می‌تواند هر چیزی را در یک فایل قرار دهد و نام دلخواهی برای آن برگزیند و شما زمانی از اطلاعات داخل آن باخبر می‌شوید که آن را دانلود کرده و باز کنید. اکثر بدافزارها با شیوه Drive-by Download (اجرا بعد از دانلود شدن) به سیستم نفوذ می‌کنند. بهترین راه برای مقابله با این نوع تهدیدات این است که ابتدا سیستم و فایل را اسکن نموده و سپس باز کنید. برای این کار می‌توانید از ارائه‌دهنده‌های سرویس‌های اسکن آنلاین (مانند virus total) استفاده کنید.

۲- توزیع از طریق ایمیل

آمارگسترش بدافزارها توسط ایمیل‌ها شگفت انگیر است. ارسال ۱۲ میلیون ایمیل آلوده به باج‌افزار در هر ۶ ساعت، نشان می‌دهد که امروزه اکثر ایمیل‌های ارسال شده شامل نوعی بدافزار هستند. خوشبختانه سرویس‌های ایمیل که ما استفاده می‌کنیم مانند Gmail، Yahoo و Outlook دارای مکانیزم امنیتی مانند فیلتر Spamها هستند. همچنین این سرویس‌ها در برخی موارد اجازه باز کردن فایل خاصی را نمی‌دهند.

۳- درایوهای USB

همه دستگاه‌های USB یک فایل به نام Autorun دارند که به محض این که شما USB را به سیستم متصل می‌کنید Autorun اجرا می‌گردد. مشکل از زمانی شروع می‌شود که متوجه شوید این فایل Autorun را می‌توان تغییر داد. در گذشته حملات USB بسیار محبوب بودند و از آن برای جاسوسی از افراد، تماشای صفحه نمایش و کارهای در حال انجام قربانی استفاده می‌شد. برای مقابله با این نوع تهدیدات سعی کنید که USBها را از افرادی که اعتماد دارید دریافت کنید و اطمینان حاصل نمایید که آنتی‌ویروس شما همیشه فعال است.

۴- شبکی داخلی (LAN)

امروزه اسکریپت‌های مختلف بدافزار نوشته می‌شوند و آنچه که واقعا ترسناک است این است که هنگامی که یک کامپیوتر آلوده شود، تمام کامپیوترهای دیگر در همان شبکه محلی نیز در خطر آلوده شدن قرار می‌گیرند. بنابراین جهت کاهش شیوع این نوع تهدیدات، از شبکه داخلی خود مراقبت کنید.

۵- نرم‌افزارهای بروزرسانی‌نشده

به دلیل عدم بروزرسانی نرم‌افزارها، سیستم شما ممکن است با انواع تهدیدات مختلف روبرو گردد. بروزرسانی نرم‌افزارها به این دلیل انجام می‌شود که برنامه‌نویسانی که آن‌ها را تولید می‌کنند، اشکالاتی در آن پیدا می‌کنند که نیازمند تصحیح می‌باشد. اگر هکرها قبل از توسعه‌دهندگان اصلی، این اشکالات را پیدا کنند، می‌توانند از آن سوءاستفاده کنند، که به آن سوءاستفاده روز صفر نیز گفته می‌شود. همچنین تا زمانی که بروزرسانی‌های برطرف کننده این آسیب‌پذیری‌ها ارائه نشود،شما و هر شخص دیگر که از آن محصول استفاده می‌کنید، آسیب‌پذیر خواهید بود

منبع خبر: hackread جمع‌آوری: مهندس معصومه خیری

آشنایی با واژگان حوزه امنیت

در این بخش با چندین واژه حوزه امنیت آشنا می‌شویم. ادامه این توضیحات در شماره‌های بعدی خبرنامه منتشر خواهد شد.

- **بدافزار (Malware)**

Malware یک کلمه ترکیبی است که از دو کلمه Malicious به معنای مخرب و Software به معنای نرم-افزار گرفته شده است. اگرچه غالبا کلمه Virus به جای آن مورد استفاده قرار می‌گیرد. این کلمه گسترهٔ وسیعی از تهدیدات از جمله ویروس‌ها، تروجان‌ها، کرم‌ها (Worm)، جاسوس‌افزارها (Spyware)، آگهی‌افزارها (Adware)، Keyloggerها و Rootkitها را شامل می-شود.

- **ویروس (Virus)**

ویروس‌های کامپیوتری نرم‌افزارهای مخربی هستند که می‌توانند خود را باز تولید کنند. آن‌ها دستگاه‌ها را آلوده کرده و از فایلی به فایل دیگر و از دستگاهی به دستگاه دیگر گسترش می‌یابند و معمولا از طریق ایمیل، دانلود از منابع نامعتبر و درگاه USB وارد سیستم می‌شوند.

اهداف: بیشتر ویروس‌ها خود را به یک فایل اجرایی می-چسبانند و در موارد خاص روی ماکروهای مجموعه برنامه آفیس، اسکریپت‌هایی که به‌صورت خودکار اجرا می‌شوند و MBR (اولین سکتور از دیسک که اطلاعات پارتیشن‌ها روی آن قرار دارند و فرآیند راه‌اندازی رایانه از روی آن آغاز می‌شود) تاثیر می‌گذارند. ویروس‌ها به طور طبیعی بسیار مخرب هستند و باعث ایجاد مشکلاتی از قبیل نمایش پیام‌های آزاردهنده، ایجاد اختلال در کار سیستم و تخریب یا حذف فایل‌ها می‌شوند. همچنین در موارد خاص اطلاعات سیستم آلوده شده را سرقت می‌کنند.

ویروس‌های شناخته‌شده: ویروس Concept که به طور تصادفی در سال ۱۹۹۵ روی CD-ROMهای ساخته‌شده توسط شرکت مایکروسافت عرضه شد. ویروس Melissa که از طریق ایمیل انتشار یافت و طبق گزارش‌ها ۸۰ میلیون دلار خسارت به همراه داشته است.

- **باج‌افزار (Ransomware)**

دو نوع باج‌افزار وجود دارد: Crypto-Ransomware که فایل‌ها را رمزگذاری می‌کند (فایل‌ها را غیرقابل خواندن می‌کند) و Screen-lock Ransomware که صفحه نمایش را قفل می‌کند. در هر دو مورد توسعه‌دهندگان این باج‌افزارها از قربانی‌های خود درخواست باج می‌کنند تا به آن‌ها اجازه دسترسی به فایل و سیستم را بدهند.

شیوه گسترش: باج‌افزارها عموما از طریق ایمیل گسترش می‌یابند. مهاجم به قربانی یک ایمیل به همراه یک فایل ضمیمه شده ارسال می‌کند و کاربر فایل مخرب ضمیمه شده را که بی‌خطر به نظر می‌آید ناآگاهانه باز می‌کند، این فایل مخرب توصیه می‌کند که ماکرو را در صورتی که کدگذاری متن اشتباه باشد فعال کنید (این توصیه در ساختار برنامه تعبیه گردیده است و فایل مخرب به گونه‌ای طراحی شده که این توصیه به قربانی توسط برنامه داده شود). فعال کردن ماکرو به باج‌افزار اجازه می‌دهد تا به صورت پنهانی دانلود شود.

اهداف: باج‌افزارهای رمزگذار تمام فایل‌ها از قبیل عکس، ویدئو، فایل متنی و ... را که به آن‌ها دسترسی داشته باشد، رمزگذاری می‌کنند. این باج‌افزار حتی فایل‌های موجود در حافظه‌های خارجی را نیز هنگام اتصال به سیستم قربانی رمزگذاری می‌کند. وقتی که تمامی فایل-ها رمزگذاری شد، این باج‌افزار در قبال رمزگشایی فایل‌ها درخواست باج می‌کند. در صورتی که نوع باج درخواست شده پول باشد، معمولا بصورت بیتکوین می‌باشد که می-

تواند ارزش آن تا چند صد هزار دلار نیز افزایش یابد. باج‌افزار Screen-lock صفحه اول را قفل می‌کند و از دسترسی قربانی به سیستم جلوگیری کرده و در مقابل دسترسی دوباره به سیستم از قربانی تقاضای باج می‌کند.

باج‌افزارهای مشهور: CryptoLocker، Locky و FBI Ransomware سه باج افزار شناخته شده‌ای هستند که به میلیون‌ها قربانی ضرر رسانده‌اند.

محافظت در برابر باج‌افزار: توصیه می‌شود که به صورت منظم از داده‌های خود نسخه پشتیبان تهیه نمایید. در این صورت اگر داده‌های شما رمزگذاری شد، همچنان به آن‌ها دسترسی خواهید داشت.

برای شناسایی و جلوگیری از آلوده شدن به باج‌افزارها می‌توانید از نرم‌افزارهای امنیتی قدرتمند استفاده کنید.

- **بات‌نت (Botnet)**

بات‌نت یک شبکه کامپیوتری متصل به هم می‌باشد، که معمولا توسط سرور مرکزی مهاجم کنترل می‌شود و با یکدیگر برای رسیدن به هدف خاص در ارتباطاند . گرچه بات‌نت‌ها همیشه مخرب نیستند ولی غالبا برای انجام فعالیت‌های غیرقانونی مورد استفاده قرار می‌گیرند.

موارد استفاده از بات‌نت‌ها: از آنجاییکه بات‌ها برای جستجوی غیرقانونی مورد استفاده قرار می‌گیرند (در اینجا بات یک نوع بدافزار است که بر روی یک میزبان آسیب‌پذیر نصب می‌شود)، بات‌نت‌ها معمولا توسط هکرها ایجاد شده و کنترل دیگر سیستم‌های متصل به شبکه را بدست می‌گیرند. به این سیستم‌ها بعد از آلوده شدن زامبی نیز می‌گویند.

سیستم‌هایی که بخشی از بات‌نت هستند برای ارسال اسپم، حملات DOS و انتقال منابع مالی برای فعالیت-های مجرمانه استفاده می‌شوند. هکر همچنین می‌تواند خدمات بات‌نت را برای ارسال اسپم به فروش برساند، این امر از لحاظ قابل شناسایی نبودن و کاهش هزینه برای اسپمرها مناسب بوده و همچنین صاحب سیستم آلوده، پول اینترنت مورد نیاز برای ارسال اسپم را پرداخت می-کند.

بات‌نت‌های شناخته شده: از بات‌نت‌های مشهوری که غیرفعال شده‌اند می‌توان به Grum (مسئول ۲۶ ٪ از ایمیل‌های اسپم بین سال‌های ۲۰۱۲ – ۲۰۰۸)، GameoverZeus، ZeroAccess و Kraken اشاره کرد.

- **تروجان (Trojan)**

تروجان یک برنامه مخرب می‌باشد که در ظاهر خود را برنامه‌ای معمولی و مفید جلوه می‌دهد ولی در واقع رفتارهای مخرب در داخل آن تعبیه شده‌اند.

شیوه گسترش: تروجان‌ها عموما از طریق ایمیل، برنامه‌های جاسوسی، برنامه‌های فعالساز (مانند فعالساز فتوشاپ)، دانلود از منابع نامعتبر و حملات فیشینگ گسترش می‌یابند. یکی از خطرناک‌ترین تروجان‌ها Zeus نام داشت که تروجان بانکی بوده و اطلاعات محرمانه بانکی را به سرقت می‌برد. Zeus بر روی کامپیوتر و دستگاه‌های تلفن همراه گسترش یافت و بر اساس گزارش‌ها میلیون‌ها کاربر را آلوده کرده و اطلاعات میلیون‌ها نفر را از حساب‌های بانکی خصوصی و شرکتی آنها به سرقت برده است. همچنین تروجان‌ها اغلب به صورت مخفیانه دستگاه آلوده را از راه دور، مستقیم و یا بخشی از بات‌نت کنترل می‌کنند.

تروجان‌های شناخته شده: Zeus با سرقت تقریبا ۴۷ میلیون دلار یکی از موفق‌ترین تروجان‌های ساخته‌شده است. از دیگر تروجان‌هایی که می‌توان به آن‌ها اشاره کرد، Shedun می‌باشد که در دوران اوج خود روزانه تقریبا ۲۰۰۰ کاربر را آلوده می‌کرد. همچنین تروجان بانکی BankerTiny، که از روی اسم آن می‌توان فهمید، یکی از کوچک‌ترین تروجانی‌هایی است که ساخته‌شده و شناسایی آن بسیار سخت بوده است.

منبع :avira

مترجم: هادی برزگر

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

با توجه به افزایش تعداد حوادث امنیتی رایانه‌ای و لزوم وجود مراکز تخصصی دانشگاهی برای پشتیبانی و رفع نیازهای پژوهشی جامعه در این حوزه، و با انگیزه ارتقای دانش و توان مهندسی در حوزه امنیت سیستم‌های کامپیوتری و پردازش اطلاعات و انتقال نتایج به جامعه، آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی، از اواخر سال ۱۳۹۴ فعالیت خود را آغاز نمود و از زمان آغاز فعالیت، اقدامات زیر صورت گرفته است:

۱. ارزیابی امنیتی و انجام آزمون نفوذپذیری سامانه‌ها و شبکه‌های رایانه‌ای

تست نفوذ یا ارزیابی امنیتی روشی است که توسط آن قادر می‌توان آسیب‌پذیری‌های موجود در نرم‌افزارها، شبکه، وب‌سایت و بانک‌های اطلاعاتی خود را شناسایی کرده و پیش از آنکه نفوذگران واقعی به سیستم وارد شوند، امنیت سیستم خود را افزایش داد. این روش با استفاده از ارزیابی جنبه‌های مختلف امنیتی کمک می‌کند تا با کاهش دادن ریسک‌های امنیتی موجود، احتمال نفوذ غیرمجاز به شبکه کاهش یابد.

۲. مشاوره در زمینه امن‌سازی سامانه‌ها و شبکه رایانه‌ای

با توجه فعالیت‌های مختلفی که آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی در زمینه زیرساخت‌های امنیتی مانند پیاده‌سازی سیستم مدیریت امنیت اطلاعات، پیاده‌سازی انواع ابزارهای امنیتی، تدوین الگوهای امنیتی داشته است، کارشناسان این مرکز دارای دیدی جامع نسبت به مسایل امنیتی با توجه به اهداف استراتژیک و راهبردی و با توجه به موجودیت‌های هر سازمان دارند و آماده ارائه راهکار امنیت اطلاعات و شبکه در تمامی سازمان‌ها با ویژگی‌ها و موجودیت‌های مختلف می‌باشند. خدمات و راهکارهای امنیت اطلاعات و سیستم‌های کامپیوتری این مرکز، با بررسی وضعیت فعلی

سیستم‌های موجود در سازمان آغاز می‌شود و با بهره‌گیری از تکنولوژی و تخصص روز، با معماری و اجرای راه حل‌های جامع ایمن سازی سیستم های کامپیوتری ، کامل می گردد.

۳. برگزاری دوره‌های آموزشی در زمنیه دانش امنیتی برای سازمان‌ها و نهادهای زیربط

امنیت فضای سایبری فرآیندی است و باید آن را گام به گام و به روز جلو برد بنابراین آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقائ دانش امنیت اطلاعات متولیان فاوای سازمان‌ها و نیز به منظور تربیت نیروهای متخصص چندین دوره کارگاه‌های آموزشی برگزار نموده است.

۴. تولید نرم‌افزارهای امنیتی

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی با هدف ارتقا سطح امنیت فضای سایبری به تولید نرم افزارهای امنیتی اقدام نموده است که عبارت است از: سامانه تحلیل‌گر فایل‌های اجرائی (ستفا)، دیده‌بان، رادار

۵. پاسخگویی به حملات

آزمایشگاه و مرکز تخصصی آپای دانشگاه محقق اردبیلی به محض دریافت درخواستی مبنی بر وقوع حملاتی تحت وب، زیرساخت‌های شبکه، سامانه‌های اداری و حملات بدافزاری در اسرع وقت با سازمان مورد حمله ارتباط برقرار می‌کند و با شناسایی نوع و فرایند حمله، مولفه‌های مربوط به آسیب‌پذیری سیستم، راهکارهای مناسب برای جلوگیری از حمله مجدد و بهره‌برداری از ضعف سیستم را ارائه می‌دهد همچنین با شناسایی نقاط ضعف سیستم و ارائه مشاوره برای رفع این نقاط آسیب‌پذیر سیستم را در مقابل حملات جدید مقاوم می سازد.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیل www.cert.uma.ac.ir

آدرس: دانشگاه محقق اردبیلی، دانشکده فنی و مهندسی، مرکز آپا دانشگاه محقق اردبیلی ۳۱۵۰۵۷۱۸(۴۵)
cert.uma.ac.ir | cert@uma.ac.ir