بسمه تعالی

بررسی باج‌افزار

بررسی باج‌افزار Goldeneye/Petya

فهرست مطالب

۱ مقدمه

طبق آخرین اخبار، یک باج‌افزار جدید به نام Goldeneye/Petya در حال گسترش است. نحوه گسترش این باج‌افزار و نیز عملکرد آن بسیار مشابه به باج‌افزار WannaCry می‌باشد. در حال حاضر این باج‌افزار شرکت‌های کامپیوتری، کمپانی‌های تولیدکننده برق و نیز بسیاری از بانک‌ها را در کشورهای روسیه، اوکراین، اسپانیا، فرانسه، انگلیس، و هند، آلوده کرده است. این باج‌افزار نیز همانند WannaCry، توسط آسیب‌پذیری SMB سیستم‌عامل ویندوز، گسترش پیدا می‌کند.

۲ شرح

باج‌افزار Petya همانند یکی از فایل‌های dll ویندوز در سیستم قربانی قرار می‌گیرد که ظاهراً توسط یک برنامه دیگر اجرا و راه‌اندازی می‌شود. یک‌بار که این فایل اجرا شود تقریباً کار تمام است و تنظیمات سیستم قربانی را طوری تغییر می‌دهد که طبق برنامه‌ریزی خاصی سیستم دوباره راه‌اندازی شود. همین‌که سیستم قربانی دوباره راه‌اندازی شود، اطلاعات آن رمزنگاری‌شده و یک پیغام با محتوای اخاذی ظاهر خواهد شد.

باج‌افزار Petya تفاوت‌هایی با دیگر باج‌افزارها دارد. مهم‌ترین و خطرناک‌ترین این تفاوت‌ها آن است که این باج‌افزار فایل‌های روی یک سیستم را به‌صورت جداگانه آلوده نمی‌کند، بلکه کامپیوتر قربانی را راه‌اندازی مجدد کرده و سپس MFT[۱] مربوط به دیسک سخت قربانی را رمزگذاری می‌کند. این رمزگذاری باعث می‌شود MBR[۲] بی‌استفاده و ناکارآمد شود و درنتیجه دسترسی به‌تمامی اطلاعات مربوط به فایل‌ها (نام، حجم و آدرس) را محدود می‌نماید. باج‌افزار Petya در واقع کد خود را به‌جای MBR جایگزین می‌کند که در نهایت موجب می‌شود هنگام روشن شدن سیستم کاربر با چنین پیامی مواجه شود:

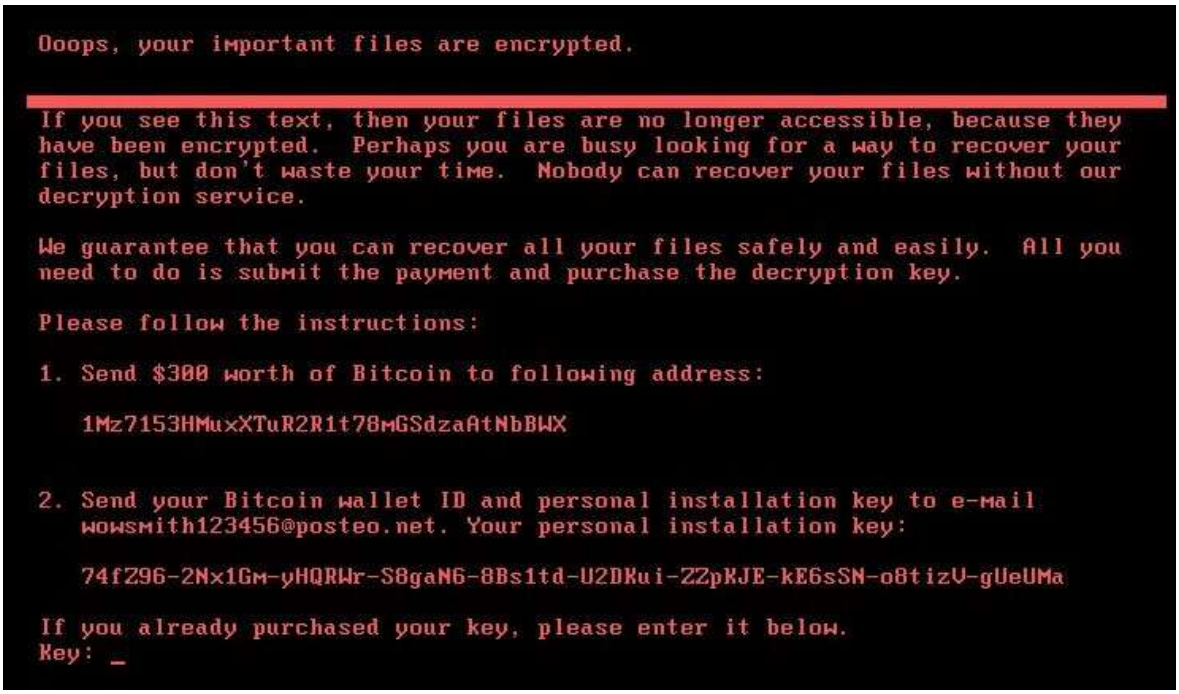
"If you see this text, then your files are no longer accessible, because they are encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service."

"اگر در حال خواندن این متن هستید، فایل‌های شما رمزگذاری شده و دیگر قابل‌دسترس نیستند. احتمالاً شما در حال حاضر به دنبال راهی هستید که فایل‌های خود را بازیابی نمایید، اما وقت خود را تلف نکنید. هیچ‌کس بدون سرویس‌های رمزگشایی ما قادر به بازگرداندن فایل‌های شما نیست."

[۱] Master File Table

[۲] Master Boot Record

شکل ۱ تصویری از سیستم آلوده را نشان می‌دهد.



شکل ۱: سیستم آلوده

با توجه به اسکرین‌شات‌های تهیه شده از دستگاه‌های آلوده، این باج‌افزار از شما درخواست مبلغی برابر 300 دلار برحسب BitCoin می‌کند. پس از اجراشدن باج‌افزار، سیستم قربانی هیچ‌گونه کارایی ندارد و درواقع بین سیستم قربانی و افراد حمله‌کننده یا هر شخصی دیگری هیچ راه ارتباطی وجود نخواهد داشت.

۱-۲ پسوندهای مورد حمله

پسوندهایی که باج‌افزار Petya پس از آلوده کردن رایانه شروع به رمزنگاری آن‌ها می‌کند در شکل ۲ نشان داده شده است. فهرست این پسوندها در ادامه آمده است.

3ds, 7z, accdb, ai,asp, aspx, avhd, back, bak, c, cfg, conf, cpp, cs, ctl, dbf, disk, djvu, doc, docx, dwg, eml, fdb, gz,h, hdd, kdbx, mail, mdb, msg, nrg, ora, ost, ova, ovf, pdf, php, pmf, ppt, pptx, pst, pvi, py, pyc, rar, rtf, sln, sql, tar, vbox, vbs, vcb, vdi, vfd, vmc, vmdk, vmsd, vmx, vsdx, vsv, work, xls, xlsx, xvd, zip.

شکل ۲: پسوندهایی که باج‌افزار پس از آلوده کردن رایانه شروع به رمزنگاری آن‌ها می‌کند

دستورات اجرا شده پس از آلوده‌سازی رایانه:

PSEXEC: %PROGRAMDATA%\dllhost.dat is dropped and is legit PSEXEC bin
Remote WMI, “process call create \"C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\perfc.dat\\\" #1”
Log clean, «wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:»
Creates a scheduled task that reboots 1 hour after infection. If task removed before the hour, does not reschedule and can buy time

۳ آسیب‌ها

همان‌طور که گفته شد این باج‌افزار تاکنون رایانه‌های بسیاری را در کشورهای مختلف آلوده کرده است. این باج‌افزار کمپانی بزرگ نفتی روسی به نام Rosneft و نیز کمپانی‌های تولیدکننده برق اوکراینی به نام‌های Kyivenergo و Ukrenergo را آلوده کرده است. تعدادی از بانک‌ها مانند NBU (National Bank of Ukraine) و Oschadbank نیز آلودگی دستگاه‌های خود را توسط باج‌افزار Petya اعلام کرده‌اند. همچنین کمپانی بین‌المللی Maersk آلودگی دستگاه‌های خود توسط باج‌افزار Petya را در صفحه Twitter خود اعلام کرده است. علاوه بر این، این باج‌افزار تعدادی از شاخه‌های کمپانی استخراج معدن Evraz را آلوده کرده است. در این میان بزرگ‌ترین آسیب توسط اوکراین گزارش‌شده است. هم‌اکنون دستگاه‌های متروی محلی و همچنین فرودگاه Kiev’s Boryspil اوکراین توسط این باج‌افزار آسیب‌دیده‌اند. سه اپراتور ارتباطی اوکراین شامل Kyivstar،LifeCell و Uktelecom نیز در حملات اخیر دچار آسیب شده‌اند.

تاکنون ۳۲ قربانی که توسط باج‌افزار Petya آسیب دیده و فایل‌هایشان رمزگذاری شده است، برای رمزگشایی فایل‌های خود، به آدرس بیت کوین 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX پرداخت انجام داده‌اند، که مبلغی معادل ۸,۱۵۰ دلار می‌باشد.

۴ پیش‌گیری

۴–۱ به‌روزرسانی

در حال حاضر تنها راه پیش‌گیری از آلودگی دستگاه‌ها به این باج‌افزار، این است که تمامی دستگاه‌های روی شبکه خود را با توجه به MS17-010 و CVE-2017-0199 به‌روزرسانی نمایند. همان‌طور که گفته شد، این باج‌افزار توسط آسیب‌پذیری پروتکل SMBv1 در حال گسترش است، و این پروتکل در سیستم‌عامل‌های زیر همچنان فعال است:

- Windows XP (all services pack) (x86) (x64)
- Windows Server 2003 SP0 (x86)
- Windows Server 2003 SP1/SP2 (x86)
- Windows Server 2003 (x64)
- Windows Vista (x86)
- Windows Vista (x64)
- Windows Server 2008 (x86
- Windows Server 2008 R2 (x86) (x64)
- Windows 7 (all services pack) (x86) (x64)

همچنین به‌موازات به‌روزرسانی دستگاه‌های خود، پیشنهاد می‌شود که استفاده از SMBv1 را در شبکه محلی خود ممنوع کنید. به جهت اطمینان می‌توانید جریان ترافیک روی شبکه خود را بررسی کنید. معمولاً پروتکل SMB از پورت TCP 445 استفاده می‌کند و بنابراین تشخیص آن کار سختی نیست. طبیعتاً اگر درخواست‌هایی با این پورت روی شبکه موجود باشد، باید فوراً مورد بررسی قرار گیرد. به منظور به‌روزرسانی دستی این آسیب‌پذیری می‌توان از جدول زیر کمک گرفت.

Product	Latest security update rollup (install this if you don't know what to install)	Standalone update
Windows 10 / Server 2016 v1703	You're already safe, but you might as well update to be safe	N/A
Windows 10 / Server 2016 v1607	KB4022715 (OS Build 14393.1358)	N/A
Windows 10 / Server 2016 v1511	KB4022714	N/A

Windows 10 / Server 2016 Initial Release	KB4022727	N/A
Windows 8.1 / Server 2012 R2	KB4022717	KB4012213
Windows 8 / Server 2012 [3]	N/A	KB4012598
Windows 7 / Server 2008 R2	KB4022722	KB4012212
Windows Vista / Server 2008	N/A	KB4012598
Windows XP / Server 2003 [3]	N/A	KB4012598

اطلاعاتی غیر رسمی از کارشناسان امنیتی اوکراینی وجود دارد که نشان می‌دهد آسیب‌پذیری CVE-2017-0199 توسط این باج‌افزار مورد استفاده قرار می‌گیرد. از این رو پیشنهاد می‌شود که نرم‌افزار Microsoft Office جهت جلوگیری از آلوده شدن به این باج‌افزار به‌روزرسانی گردد. به منظور به‌روزرسانی دستی نرم‌افزار Microsoft Office می‌توان از جدول زیر کمک گرفت.

Product	Update
Office 2007	KB3141529
Office 2010	KB2141538
Office 2013	KB3178710
Office 2016	KB3178703

۲-۴ کلید مرگ[۳]

درون این باج‌افزار یک کلید مرگ قرار دارد که توانایی متوقف کردن باج‌افزار را دارد، اما متأسفانه این کلید محلی[۴] است و برای فعال‌سازی آن نیاز به دسترسی به رایانه موردحمله می‌باشد. این مسأله باعث بی‌ارزش شدن این کلید می‌شود، زیرا در صورت دسترسی به رایانه آسیب‌پذیر توانایی رفع مشکل امنیتی وجود دارد. از این رو ایجاد کلید مرگ امری غیرضروری به نظر می‌رسد. برای ایجاد کلید مرگ باید فایلی با نام perfc.dat را در پوشه C:\Windows\ ایجاد کرد (محتوای فایل اهمیتی ندارد و می‌تواند حتی فایلی بدون محتوا باشد).

[۳] Kill switch

[۴] Local

۵ بازگردانی فایل‌ها

متأسفانه تاکنون راهکاری برای بازگردانی فایل‌های رمزشده کشف نشده است، اما با توجه به این‌که این باج‌افزار فایل‌ها را در زمان بارگذاری مجدد سیستم‌عامل شروع به رمزنگاری می‌کند، درصورت عدم راه‌اندازی مجدد سیستم‌عامل پس از آلوده شدن، با قرار دادن دیسک لایو می‌توان به فایل‌ها دسترسی داشت. همچنین درصورتی که سیستم‌عامل پس از آلوده شدن مجدداً راه‌اندازی شد، اگر قبل از به اتمام رسیدن رمزنگاری رایانه خاموش شود، احتمالاً امکان بازگردانی فایل‌های باقیمانده با استفاده از دیسک لایو وجود داشته باشد.
نکته: این باج‌افزار درصورت آلوده کردن رایانه در زمان بارگذاری مجدد، رایانه را مجبور به توقف ۳۰ الی ۴۰ دقیقه‌ای با استفاده از تابع sleep می‌کند که این امر می‌تواند نشان‌دهنده‌ی آلوده شدن رایانه‌ی کاربر باشد.

۶ نتیجه‌گیری

برخلاف توصیه‌های انجام‌شده در راستای باج‌افزار WannaCry در ماه مِه سال ۲۰۱۷ میلادی (کمتر از ۲ ماه پیش)، بازهم بسیاری از دستگاه‌هایی که از ویندوز استفاده می‌کردند این آسیب‌پذیری را جدی نگرفته و برای رفع آن اقدامی نکرده‌اند. این باج‌افزار از معدود باج‌افزارهایی است که علاوه بر کارایی مخرب خود بر روی سیستم قربانی، برای توسعه و تکثیر از بستر اینترنت و شبکه استفاده می‌کند، و بنابراین همانند کرم‌های بسیار خطرآفرین شده است و در نهایت باید یادآور شویم که از پرداخت پول به این باج‌افزار خودداری کنید. با پرداخت پول نمی‌توانید فایل‌های خود را برگردانید. افرادی که این حمله را سازمان‌دهی می‌کنند از طریق یک ایمیل از شما درخواست پول می‌کنند که هم‌اکنون (۲۷ ژوئیه۲۰۱۷ میلادی) شرکت آلمانی ارائه‌دهنده‌ی سرویس Posteo، این ایمیل را به دلیل جرائم اینترنتی مسدود کرده است. این ایمیل در سیستم قربانی جهت ارسال پول درخواستی و همچنین دریافت کلید بازگردانی فایل‌ها استفاده می‌شد که هم‌اکنون مسدود می‌باشد.