دانشگاه شیراز

آزمایشگاه و مرکز تخصصی آپا

باج افزار WannaCry

مرکز تخصصی آپا دانشگاه شیراز

اردیبهشت ۱۳۹۶

۱- مقدمه

در ۱۲ می ۲۰۱۷ یک باج افزار جدید به نام WannaCry یا WannaCrypt با استفاده از یک حفره امنیتی در سرویس SMB ویندوز به رایانه های سراسر دنیا حمله نمود. یکی از تفاوت های عمده این باج افزار با باج افزارهای دیگر در روش انتشار و نفوذ آن به سیستم قربانی است. بر خلاف دیگر باج افزارها که معمولا از طریق ایمیل منتشر می شوند و روند انتشار کندی خواهند داشت، این باج افزار با استفاده از حفره امنیتی SMB EternalBlue (که به نام MS17-010 شناخته می شود) در سیستم عامل ویندوز بوسیله ارسال بسته های دستکاری شده به سرور SMBv1 مقصد، به سیستم قربانی نفوذ و شروع به رمزنگاری فایل های قربانی می‌کند.

مایکروسافت در ماه مارس این حفره امنیتی کشف شده را برای ویندوزهای پشتیبانی شده حال حاضر وصله نمود و از طریق به روزرسانی منتشر کرد. لذا کاربرانی که از سیستم عامل هایی با قابلیت دریافت به روزرسانی استفاده می کنند و سیستم عامل خود را از قبل به روزرسانی نموده اند از این خطر در امان خواهند بود. البته ویندوز ۱۰ از این حمله در امان بوده است.

ویندوزهایی که در ماه مارس وصله شدند، Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows 10, Windows Server 2012 R2, Windows Server 2016 بودند.

در روزهای گذشته پس از انتشار این باج افزار، با توجه به حجم گسترده حملات، مایکروسافت یک وصله امنیتی برای ویندوز هایی که هم اکنون پشتیبانی رسمی نمی شوند منتشر کرد. این ویندوز ها شامل Windows XP, Windows 8, and Windows Server 2003 هستند. برای دریافت آخرین نسخه این وصله ها به لینک http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598 مراجعه شود.

[Web: apa.shirazu.ac.ir] | [Email: cert@shirazu.ac.ir] | [Tel/Fax: +98 71 36474280]

۲- نحوه عملکرد باج افزار

این بدافزار پس از جایگیری بر روی سیستم قربانی شامل دو مولفه اصلی است: مولفه اول تلاش می کند تا حفره امنیتی SMB EternalBlue را بر روی دیگر کامپیوترهای شبکه کشف کند. مولفه دوم همان باج افزار WannaCrypt است.

این بدافزار تلاش می کند تا به آدرس

hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

متصل شود. در صورتی که اتصال برقرار شد، باج افزار هیچ عملیات دیگری انجام نمی دهد و متوقف می شود. در صورتی که اتصال برقرار نشد، شروع به اجرای باج افزار و ایجاد یک سرویس در سیستم می کند. لذا بلاک نمودن آدرس مذکور توسط فایروال باعث رمزنگاری فایل های رایانه قربانی خواهد شد.

سرویس ایجاد شده توسط این باج افزار mssecsvc2.0 نام دارد که وظیفه بررسی آسیب پذیری SMB بر روی دیگر کامپیوترهای قابل دسترسی را دارد.

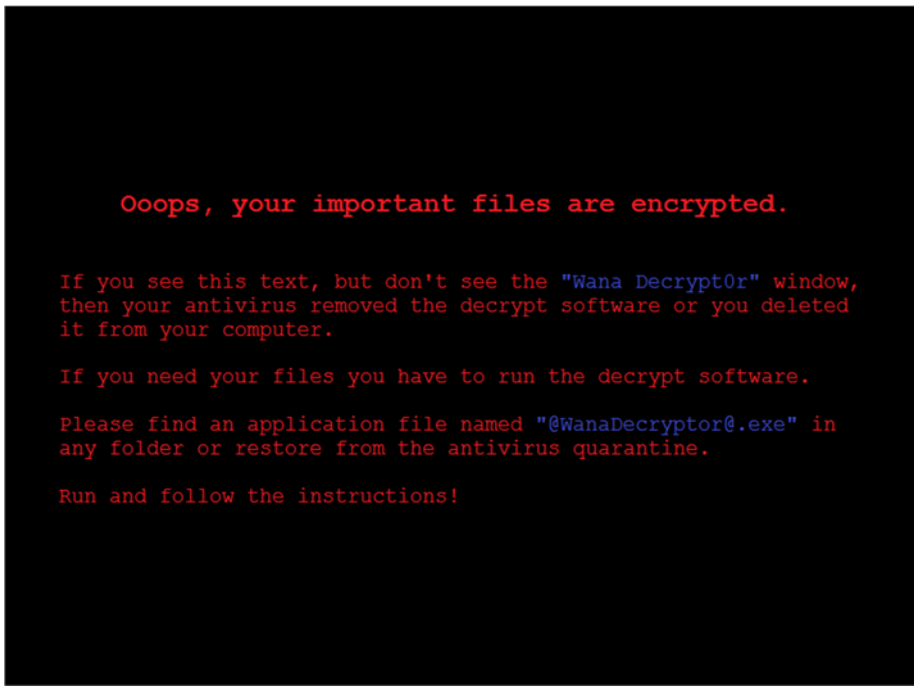
با اجرای برنامه باج افزار، کلید های زیر در رجیستری ایجاد می شود:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\\<random string> = “<malware working directory>\tasksche.exe”
- HKLM\SOFTWARE\WanaCrypt0r\\wd = “<malware working directory<

همچنین عکس پس زمینه ویندوز را نیز با دستکاری کلید رجیستری زیر تغییر می دهد:

HKCU\Control Panel\Desktop\Wallpaper: “<malware working directory>\@WanaDecryptor@.bmp”

[Web: apa.shirazu.ac.ir] | [Email: cert@shirazu.ac.ir] | [Tel/Fax: +98 71 36474280]



عکس پس زمینه ویندوز پس از آلودگی

فایل های زیر نیز در مسیر دایرکتوری کاری بدافزار ایجاد می شود:

- 00000000.eky
- 00000000.pky
- 00000000.res
- 274901494632976.bat
- @Please_Read_Me@.txt
- @WanaDecryptor@.bmp
- @WanaDecryptor@.exe
- b.wnry
- c.wnry
- f.wnry
- m.vbs
- msg\m_bulgarian.wnry
- msg\m_chinese (simplified).wnry

- msg\m_chinese (traditional).wnry
- msg\m_croatian.wnry
- msg\m_czech.wnry
- msg\m_danish.wnry
- msg\m_dutch.wnry
- msg\m_english.wnry
- msg\m_filipino.wnry
- msg\m_finnish.wnry
- msg\m_french.wnry
- msg\m_german.wnry
- msg\m_greek.wnry
- msg\m_indonesian.wnry
- msg\m_italian.wnry
- msg\m_japanese.wnry
- msg\m_korean.wnry
- msg\m_latvian.wnry
- msg\m_norwegian.wnry
- msg\m_polish.wnry
- msg\m_portuguese.wnry
- msg\m_romanian.wnry
- msg\m_russian.wnry
- msg\m_slovak.wnry
- msg\m_spanish.wnry
- msg\m_swedish.wnry
- msg\m_turkish.wnry
- msg\m_vietnamese.wnry
- r.wnry
- s.wnry
- t.wnry
- TaskData\Tor\libeay32.dll
- TaskData\Tor\libevent-2-0-5.dll
- TaskData\Tor\libevent_core-2-0-5.dll
- TaskData\Tor\libevent_extra-2-0-5.dll
- TaskData\Tor\libgcc_s_sjlj-1.dll
- TaskData\Tor\libssp-0.dll

- TaskData\Tor\ssleay32.dll
- TaskData\Tor\taskhsvc.exe
- TaskData\Tor\tor.exe
- TaskData\Tor\zlib1.dll
- taskdl.exe
- taskse.exe
- u.wnry

علاوه بر اینها، باج افزار فایل های زیر را نیز ایجاد می نماید:

- %SystemRoot%\tasksche.exe
- %SystemDrive%\intel\<random directory name>\tasksche.exe
- %ProgramData%\<random directory name>\tasksche.exe

این باج افزار یک سرویس با نام تصادفی با مسیر اجرایی " cmd.exe /c "<malware working directory>\tasksche.exe" در سیستم ایجاد می کند.

فایل هایی با پسوند های زیر مورد رمزنگاری این باج افزار قرار خواهند گرفت:

.123, .jpeg , .rb , .602 , .jpg , .rtf , .doc , .js , .sch , .3dm , .jsp , .sh , .3ds , .key , .sldm , .3g2 , .lay , .sldm , .3gp , .lay6 , .sldx , .7z , .ldf , .slk , .accdb , .m3u , .sln , .aes , .m4u , .snt , .ai , .max , .sql , .ARC , .mdb , .sqlite3 , .asc , .mdf , .sqlitedb , .asf , .mid , .stc , .asm , .mkv , .std , .asp , .mml , .sti , .avi , .mov , .stw , .backup , .mp3 , .suo , .bak , .mp4 , .svg , .bat , .mpeg , .swf , .bmp , .mpg , .sxc , .brd , .msg , .sxd , .bz2 , .myd , .sxi , .c , .myi , .sxm , .cgm , .nef , .sxw , .class , .odb , .tar , .cmd , .odg , .tbk , .cpp , .odp , .tgz , .crt , .ods , .tif , .cs , .odt , .tiff , .csr , .onetoc2 , .txt , .csv , .ost , .uop , .db , .otg , .uot , .dbf , .otp , .vb , .dch , .ots , .vbs , .der" , .ott , .vcd , .dif , .p12 , .vdi , .dip , .PAQ , .vmdk , .djvu , .pas , .vmx , .docb , .pdf , .vob , .docm , .pem , .vsd , .docx , .pfx , .vsdx , .dot , .php , .wav , .dotm , .pl , .wb2 , .dotx , .png , .wk1 , .dwg , .pot , .wks , .edb , .potm , .wma , .eml , .potx , .wmv , .fla , .ppam , .xlc , .flv , .pps , .xlm , .frm , .ppsm , .xls , .gif , .ppsx , .xlsb , .gpg , .ppt , .xlsm , .gz , .pptm , .xlsx , .h , .pptx , .xlt , .hwp , .ps1 , .xltm , .ibd , .psd , .xltx , .iso , .pst , .xlw , .jar , .rar , .zip , .java , .raw

پسوند فایل های رمز شده، WNCRY. خواهد بود، که البته پسوند فایل اصلی را نیز قبل از این پسوند همچنان به عنوان قسمتی از نام فایل، نگهداری می کند. نام فایل بدون تغییر باقی می ماند.

این باج افزار در دایرکتوری های رمز شده، فایل "Please_Read_Me@.txt@" را نیز می سازد.

پس از عملیات رمز نگاری، این باج افزار Shadow Copy ها را نیز با دستورات زیر حذف می کند:

cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet

همچنین پیامی را به کاربر نمایش می دهد که در ازای پرداخت ۳۰۰ دلار، فایل های قربانی بازگردانی می شود. این پیام به زبان های Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, and Vietnamese موجود است.

پیام نمایش داده شده به کاربر

همچنین برای اطمینان خاطر قربانی از امکان بازگردانی فایل، ابزار decryptor باج افزار به صورت رایگان تعدادی از فایل ها را بازگردانی می کند.

ابزار decryptor همراه با باج افزار

پس از جایگیری این باج افزار بر روی سیستم قربانی، این بدافزار سعی در آلوده سازی دیگر رایانه های شبکه محلی می کند. علاوه بر آن یک جستجوی سنگین بر روی آدرس های IP اینترنتی نیز انجام می دهد (این آدرس ها به صورت تصادفی در محدوده آدرس های عمومی اینترنت انجام می گیرد) تا رایانه های آلوده را شناسایی کند. از این رو حجم ترافیک SMB شدیدی از رایانه های قربانی منتشر خواهد شد که نشانگر وجود آلودگی روی سیستم است.

برخی از حملات مشاهده شده از روش های مرسوم فیشینگ مانند attachment های آلوده به فایل هایی نظیر مستندات word استفاده می کنند.

۳-نشانه های آلودگی

۱. وجود فایل هایی با هش SHA1 زیر:

- 51e4307093f8ca8854359c0ac882ddca427a813c
- e889544aff85ffaf8b0d0da705105dee7c97fe26

۲. ایجاد فایل های زیر در سیستم:

- %SystemRoot%\mssecsvc.exe
- %SystemRoot%\tasksche.exe
- %SystemRoot%\qeriuwjhrf
- b.wnry
- c.wnry
- f.wnry
- r.wnry
- s.wnry
- t.wnry
- u.wnry
- taskdl.exe
- taskse.exe
- 00000000.eky
- 00000000.res
- 00000000.pky
- @WanaDecryptor@.exe
- @Please_Read_Me@.txt
- m.vbs
- @WanaDecryptor@.exe.lnk
- @WanaDecryptor@.bmp
- 274901494632976.bat
- taskdl.exe
- Taskse.exe
- Files with ".wnry" extension
- Files with ".WNCRY" extension

۳. ایجاد کلید رجیستری زیر در سیستم:

HKLM\SOFTWARE\WanaCrypt0r\wd

۴. مشاهده حجم ترافیک نامتعارف SMB از سیستم.

۴-روش های مقابله

۱. آپدیت نمودن ویندوز های پشتیبانی شده توسط مایکروسافت
۲. نصب وصله رسمی از سوی مایکروسافت برای ویندوز هایی که توسط به روزرسانی دریافت نمی کنند.
۳. استفاده از ویندوز نسخه ۱۰
۴. استفاده از قابلیت DeviceGuard برای محیط های سازمانی
۵. حذف سرویس mssecsvc2.0
۶. بستن پورت های غیر ضروری سیستم
۷. استفاده از آنتی ویروس های به روزرسانی شده
۸. حذف فایل ها و کلیدهای رجیستری ذکر شده

۵-روش های پاک سازی

۱. سیستم را در حالت Safe mode بوت نمایید.
۲. کلیه فایل ها را از حالت مخفی خارج نمایید.
۳. در msconfig در قسمت startup برنامه های ناشناخته را از حالت شروع خودکار در آورید.
۴. فایل های آلوده را پاک کنید.
۵. فایل های درون فولدر %tmp% را حذف نمایید.
۶. فایل های آلوده به نام wanna و فولدر tor را از فولدر %appdata% حذف نمایید.
۷. فایل hosts را بررسی نموده و در صورت مشاهده لینک مشکوک آن را حذف نمایید.
۸. سیستم را با یک آنتی ویروس به روز اسکن نمایید.
۹. سیستم را به حالت Normal بوت نمایید.

[Web: apa.shirazu.ac.ir] | [Email: cert@shirazu.ac.ir] | [Tel/Fax: +98 71 36474280]

- تذکر: فایل های رمز شده در صورت عدم تهیه نسخه پشتیبان تا به امروز قابل بازگردانی نیستند.
- تذکر: بهتر است ویندوز آلوده شده مجددا پاک و نصب شود و بلافاصله توسط یک آنتی ویروس به روز کل فایل های دیسک اسکن شود.

[Web: apa.shirazu.ac.ir] | [Email: cert@shirazu.ac.ir] | [Tel/Fax: +98 71 36474280]