آنچه باید در مورد باج‌افزار WannaCry بدانیم

(آشنایی با باج‌افزار WannaCty و اقدامات لازم برای پیشگیری از آلودگیِ سیستم‌ها)

اردیبهشت ۱۳۹۶

فهرست مطالب

مقدمه

در روزهای اخیر باج‌افزاری تحت عنوان WannaCry با قابلیت خودـ انتشاری در شبکه کشورها شیوع یافته است. براساس رصدهای انجام شده توسط مرکز ماهر، این بدافزار در سطح شبکه کشور ما نیز مشاهده شده است. تا این لحظه بیش از ۲۰۰ قربانی این باج‌افزار در کشور شناسایی شده و اقداماتی جهت رفع آلودگی و پاک‌سازی آن‌ها از سوی گروه‌های امداد و نجات مرکز ماهر (مراکز آپا) مستقر در استان‌های کشور در دست انجام است. گفتنی است بیشتر این آلودگی‌ها در حوزه سیستم‌های پزشکی و سلامت بوده است.

این حمله را می‌توان بزرگترین حمله‌ی باج‌افزاری نامید که تاکنون مشاهده شده است. این باج‌افزار به نام‌های مختلفی همچون WannaCry، Wana Decrypt0r، WannaCryptor و WCRY شناخته می‌شود. عملکرد باج‌افزارها به این شکل است که بر روی سیستم قربانی، فایل‌ها را رمزنگاری می‌کند و برای رمزگشایی و برگرداندن آن‌ها، از قربانی باج درخواست می‌کند. عملکرد باج‌افزار WannaCry نیز دقیقاً به همین شکل است.

باج‌افزار مذکور برای توزیع از یک ابزار اکسپلویت (بهره‌برداری) متعلق به آژانس امنیت ملی آمریکا به نام EternalBlue استفاده می‌کند که مدتی پیش توسط گروه نفوذ shadow brokers منتشر شد. این گروه نفوذ، ابزارها و بهره‌برداری‌های آژانس امنیت ملی آمریکا را به سرقت برده و در ادامه آن‌ها را منتشر کرد.

این اکسپلویت از یک آسیب‌پذیری در سرویس SMB سیستم‌های عامل ویندوز با شناسه MS17-010 استفاده می‌کند. در حال حاضر این آسیب‌پذیری توسط مایکروسافت وصله شده است اما کامپیوترهایی که به‌روزرسانی مربوطه را دریافت ننموده‌اند نسبت به این حمله و آلودگی به این باج‌افزار آسیب‌پذیر هستند. تصویر زیر پیامی است که باج‌افزار به قربانی نمایش می‌دهد. پیام باج‌افزار به زبان‌های مختلف قابل مشاهده است.

شکل ۱ پیامی که باج‌افزار WannaCry به قربانی نمایش می‌دهد

این باج‌افزار با استفاده از شبکه‌ی گمنامی TOR و استفاده از حساب‌های بیت‌کوین هویت خود را مخفی نموده است. حساب‌های بیت‌کوین متعلق به این باج‌افزار از ساعات ابتدایی آلودگی، پول زیادی به عنوان باج دریافت نموده‌اند. تابحال بیش از ۲۸ پرداخت گزارش شده است. یعنی تنها در ساعات اولیه، عوامل این باج‌افزار بیش از

۹۰۰۰ دلار باج به جیب زده‌اند. نحوه تاثیرگذاری این باج‌افزار هنوز به صورت دقیق مشخص نشده اما موردی که مشخص است، استفاده از ایمیل‌های فیشینگ و لینک‌های آلوده در سایت‌های غیر معتبر برای پخش باج‌افزار است.

این باج‌افزار فایل‌هایی با پسوند زیر را رمزنگاری کرده و هدف قرار می‌دهد:

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

باتوجه به فعالیت این باج‌افزار در کشور ما، لازم است جهت پیشگیری از آلودگی به آن، مدیران شبکه نسبت به به‌رورزرسانی سیستم‌های عامل ویندوز، تهیه کپی پشتیبان از اطلاعات مهم خود، به‌روزرسانی آنتی‌ویروس‌ها و اطلاع‌رسانی به کاربران جهت عدم اجرای فایل‌های پیوست در ایمیل‌های ناشناس در اسرع وقت اقدام کنند.

نحوه‌ی عملکرد باج‌افزار

این باج‌افزار پس از نصب بر روی سیستم قربانی، شامل دو مولفه اصلی است: مولفه‌ی اول تلاش می‌کند تا آسیب‌پذیری سرویس SMB را بر روی دیگر کامپیوترهای شبکه کشف کند. به همین دلیل گفته می‌شود این باج‌افزار در زمان توزیع، عملکردی مانند کرم دارد. مولفه‌ی دوم همان باج‌افزار WannaCrypt است که از آسیب‌پذیری SMB EternalBlue بهره‌برداری می‌کند.

این بدافزار تلاش می‌کند تا به آدرس

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

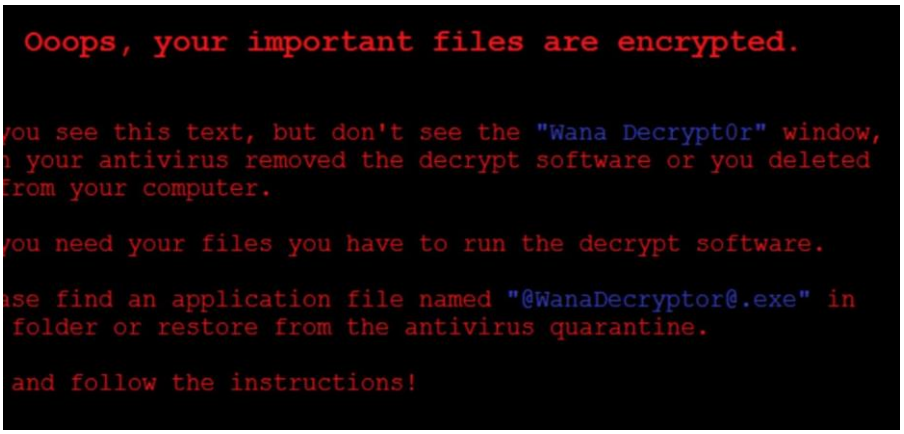
متصل شود. در صورتی که اتصال برقرار شد، باج‌افزار هیچ عملیات دیگری انجام نمی‌دهد و متوقف می‌شود. در صورتی که اتصال برقرار نشد، شروع به اجرای باج‌افزار و ایجاد يك سرویس در سیستم مي‌کند. لذا مسدود نمودن آدرس مذکور توسط فایروال، باعث رمزنگاری فایل‌های رایانه قربانی خواهد شد.

سرویس ایجادشده توسط این باج‌افزار mssecsvc 2.0 نام دارد. این سرویس وظیفه دارد بر روی شبکه‌ای که مستقر شده، بر روی دیگر سیستم‌های شبکه نیز به دنبال آسیب‌پذیری SMB بگردد. با اجرای برنامه‌ی باج‌افزار، کلیدهای زیر در رجیستری ایجاد می‌شود:

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

همچنین عکس پس‌زمینه ویندوز را نیز با دستکاری کلید رجیستری زیر تغییر می‌دهد:

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



شکل2 پس‌زمینه پس از آلوده شدن به باج‌افزار WannaCry

نشانه‌های آلودگی سیستم به باج‌افزار

۱. وجود فایل‌های با مقادیر درهم‌سازی (هش) SHA-1 زیر:

- 51e4307093f8ca8854359c0ac882ddca427a813c
- e889544aff85ffaf8b0d0da705105dee7c97fe26

۲. ایجاد فایل‌های 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 ترافیك نامتعارف SMB از سیستم

اقدامات پیشگیرانه

در این قسمت راه‌حل‌هایی که ارائه داده‌ایم به دو روش عمده تقسیم می‌شود. در راه‌حل اول ضروری است تا سیستم عامل‌های ویندوز را به‌روزرسانی کنید تا آسیب‌پذیری با شناسه‌ی MS17-010 وصله شود. در راه‌حل دیگر توصیه می‌کنیم سرویس SMB را بر روی سیستم‌عامل‌های خود غیرفعال کنید. روش‌های غیرفعال کردن این سرویس بر روی سیستم عامل‌های مختلف را در ادامه توضیح داده‌ایم.

مسدودسازی دسترسی به سرویس SMB بدون توقف سرویس: همچنین ضروری است اشاره کنیم که در یک راه‌حل جایگزین، اگر از فایروال استفاده می‌کنید، پیشنهاد می‌کنیم پورت‌هایی را که سرویس SMB از آن‌ها استفاده می‌کند، بر روی فایروال مسدود کنید. پورت‌های مورد استفاده توسط سرویس SMB ویندوز، پورت‌های ۴۴۵ و ۱۳۹ هستند.

۱. نصب وصله برای آسیب‌پذیری MS17-010

آسیب‌پذیری MS17-010 در پیاده‌سازی سرویس SMB (پروتکل اشتراک گذاری فایل) در همه نسخه‌های ویندوز وجود دارد. برای مقابله با این آسیب‌پذیری و جلوگیری از سوءاستفاده از آن لازم است آخرین به‌روزرسانی‌های سیستم عامل ویندوز اعمال گردد. برای این منظور با استفاده از ابزار به‌روزرسانی ویندوز (windows update)، آخرین به‌روزرسانی‌های سیستم عامل را دریافت کرده و نصب کنید.

در خصوص سیستم‌های عامل ویندوز xp و ۲۰۰۳ که مدتی است مورد پشتیبانی شرکت مایکروسافت قرار ندارند، خوشبختانه با توجه به اهمیت موضوع، شرکت مایکروسافت وصله‌های اختصاصی خود را در لینک زیر در دسترس قرار داده است:

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

۲. غیرفعال‌سازی سرویس SMB در سیستم عامل‌های ویندوز

چنانچه به دلیلی امکان به‌روزرسانی سیستم عامل یا نصب وصله مربوطه وجود نداشته باشد، لازم است دسترسی به سرویس SMB مسدود گردد. برای این منظور می‌توان با توجه به نسخه سیستم عامل نسبت به حذف و توقف سرویس و یا مسدودسازی پورت‌های آن اقدام نمود. توجه داشته باشید برای اینکه تنظیمات بالا اعمال شود، باید کامپیوتر خود را ریستارت کنید.

غیر فعال‌سازی سرویس SMB در ویندوز ۷، ویستا و ویندوز سرورهای ۲۰۰۸ و ۲۰۰۸ R2 با استفاده از محیط powershell:

- برای غیرفعال کردن SMBV1 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 0 -Force
```

- برای غیرفعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -
Type DWORD -Value 0 -Force
```

- برای فعال کردن SMBV1 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -
Type DWORD -Value 1 -Force
```

- برای فعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB2 -
Type DWORD -Value 1 -Force
```

غیرفعالسازی سرویس SMB در ویندوز ۸ و ویندوز سرور ۲۰۱۲ به بعد با استفاده از محیط powershell:

- برای مشاهده وضعیت پروتکل سرور SMB:

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
```

- برای غیرفعال کردن SMBV1 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- برای غیرفعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- برای فعال کردن SMBV1 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

- برای فعال کردن SMBV2 و SMBV3 روی سرور SMB:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

روش‌های حذف آلودگی به باج‌افزار WannaCry از سیستم

۱. سیستم را در حالت Safe Mode راه‌اندازی (بوت) نمایید.
۲. کلیه فایل‌ها را از حالت مخفی خارج کنید.
۳. در msconfig در قسمت startup برنامه‌های ناشناخته را از حالت شروعِ خودکار خارج کنید.
۴. فایل‌های آلوده را پاک کنید.
۵. فایل‌های داخل پوشه‌ی %tmp% را حذف کنید.
۶. فایل‌های آلوده با نام Wanna و پوشه‌ی tor را از پوشه‌ی %appdata% حذف کنید.
۷. فایل‌های hosts را بررسی نموده و در صورت مشاهده‌ی لینک‌های مشکوک آن‌ها را حذف کنید.
۸. سیستم را با یک آنتی‌ـویروس به‌روز اسکن نمایید.
۹. سیستم را در حالت Normal بوت (راه‌اندازی) نمایید.

تذکر: فایل‌ها رمزنگاری‌شده در صورت عدم تهیه نسخه پشتیبان، تا به امروز قابل بازیابی نیستند. بهتر است ویندوز آلوده را حذف و مجدداً نصب کنید و بلافاصله توسط یک آنتی‌ـویروس به‌روز کل فایل‌های دیسک را اسکن نمایید.