جمهوری اسلامی ایران
ریاست جمهوری
مرکز مدیریت راهبردی افتا

راهنمای شناسایی و پاکسازی بدافزار منتسب به گروه APT-27

دی ماه ۱۳۹۸

فهرست مطالب

مقدمه

گروه هکری APT 27 که به نام های دیگری همچون TG-3390، Emissary Panda، BRONZE UNION، Iron Tiger و LuckyMouse نیز شناخته می شوند، چندین سال است که در مناطق مختلف از جمله خاورمیانه فعال است. این گروه در حملات انجام شده در طی مدت زمان فعالیت‌شان از تکنیک‌ها و ابزارهای متنوعی استفاده‌کرده‌اند و با وجود شباهت کلی حملات در مناطق جغرافیایی مختلف، در جزییات تفاوت‌هایی وجود دارد.

در این راستا مرکز مدیریت راهبردی افتا با همکاری شرکت بیت‌بان اقدام به تولید دو ابزار در جهت شناسایی شواهد نفوذ/آلودگی و همچنین پاکسازی سامانه‌ها از آلودگی مربوطه نموده است. نسخه اول این ابزار بر اساس رفتار دیده شده در اکثر سامانه‌های مورد نفوذ قرار گرفته شده توسط گروه APT 27 ایجاد گردیده است و در صورت نیاز بروزرسانی خواهد شد.

به جهت انتقال و اشتراک دانش میان کارشناسان این حوزه، کد منبع[1] هر دو ابزار در کنار فایل‌های اجرایی منتشر شده است. خواهشمند است که ابتدا ابزار آشکارساز (تحت عنوان "AFTA-APT27-Detector.exe") را اجرا نمایید و در صورت وجود نشانه‌های نفوذ، قبل از اجرای ابزار پاک ساز (تحت عنوان "AFTA-APT27-Removal.exe")، سریعا مراتب را به صورت شبانه‌روزی به مرکز مدیریت راهبردی افتا منعکس نمایید. همچنین پیشنهادات در جهت بهبود عملکرد ابزار را به پست الکترونیک مرکز افتا ارسال نمایید:

- **تلفن: ۰۲۱۴۳۴۳۹۹۹۹**
- **پست الکترونیک: info@afta.gov.ir**

لازم به ذکر است از آنجایی که هر دو ابزار منتشر شده، اجرایی و فاقد امضا هستند و جدیدا تولید شده‌اند، ممکن است که بعضا توسط آنتی‌ویروس‌ها به عنوان فایل مشکوک تلقی شوند. این تشخیص در نسخه‌های مختلف هر آنتی‌ویروس نیز ممکن است متفاوت باشد. به عنوان مثال آنتی ویروس Symantec ممکن است این ابزار را به عنوان ws.reputation بشناسد[2] که با مراجعه به وبسایت این آنتی ویروس میتوان مشاهده کرد که اینگونه فایل‌ها به دلیل امتیاز شهرت[3] پایین، مشکوک در نظر گرفته شده‌اند. این امتیاز توسط Symantec و براساس معیارهایی همچون میزان شیوع و استفاده ابزار در بین کاربران کل دنیا و وجود امضای دیجیتال تعیین می‌شود. بنابراین بدیهی است که ابزار منتشر شده توسط مرکز افتا امتیاز بالایی نداشته باشد و آنتی ویروس مانع از اجرای آن شود.

در این مستند نحوه کارکرد هردو ابزار و اطلاعات مورد نیاز برای گزارش حادثه به مرکز افتا معرفی شده اند.

[1] Source Code

[2] https://www.symantec.com/security-center/writeup/2010-051308-1854-99

[3] Reputation score

نحوه کارکرد آشکارساز

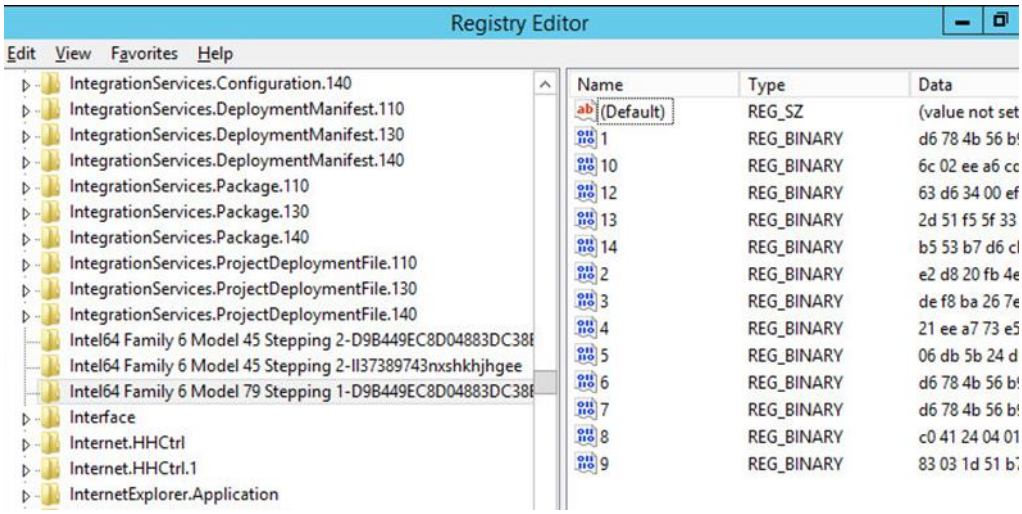
درحال حاضر برای یافتن نشانه‌های نفوذ گروه APT 27 از سه روش استفاده شده است. البته نشانه‌های دیگری نیز وجود دارد که نیاز به بررسی بیشتری داشته و در نسخه‌های بعدی بروزرسانی خواهد شد.

۱-۱ کلید رجیستری حاوی تنظیمات بدافزار

بدافزار تنظیمات خود را در کلیدهایی که با فرمت خاصی تولید می‌شوند ذخیره می‌کند. به عنوان مثال در یکی از نمونه‌های شایع، بدافزار اقدام به خواندن شناسه پردازنده در مسیر رجیستری زیر کرده و با توجه به مقدار Identifier اقدام به ساختن کلیدی در مسیر HKEY_CLASSES_ROOT می‌کند.

HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0

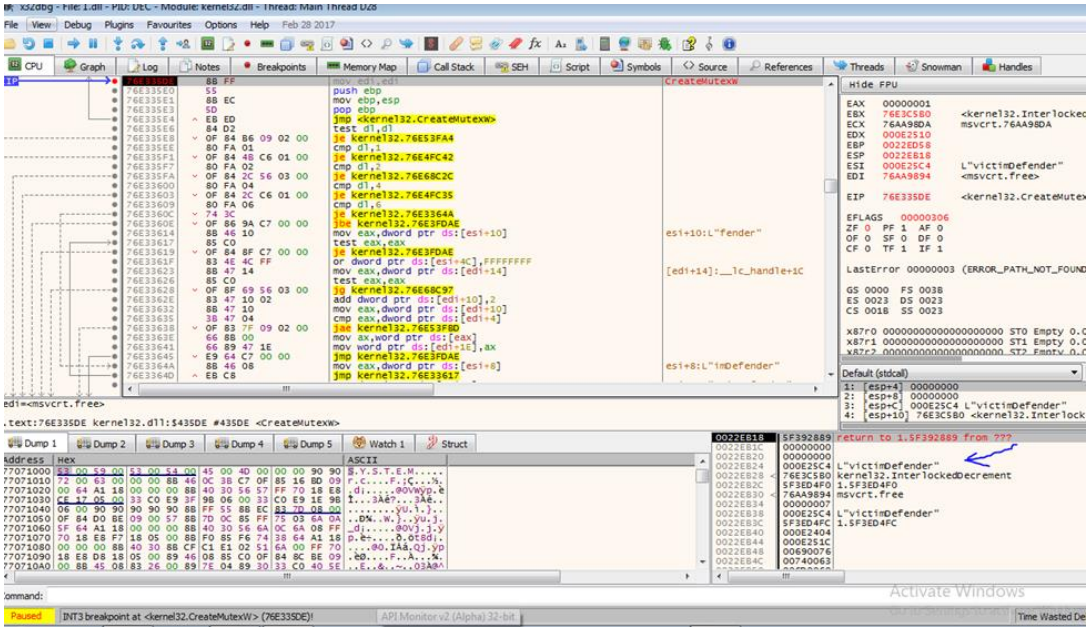
مقادیر این کلیدها با الگوریتم DES رمز شده‌اند که با رمزگشایی آنها مشخص شد که بدافزار اطلاعاتی همچون آدرس C&C و مسیر فایل‌های مخرب خود را در آنها ذخیره کرده است.



شکل ۱ کلید رجیستری حاوی تنظیمات بدافزار

۱-۲ Mutex منحصربه فرد بدافزار

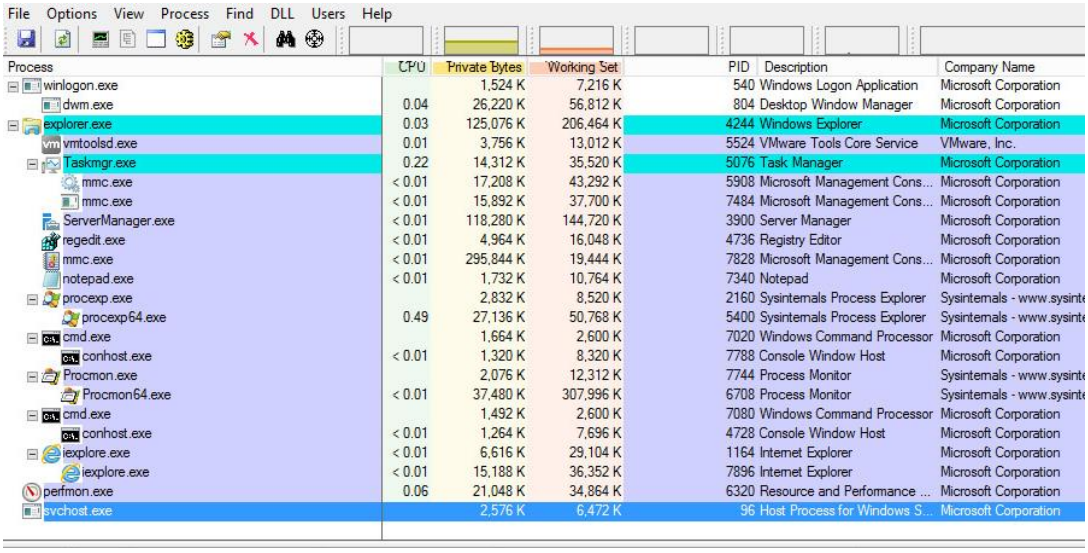
بدافزار برای جلوگیری از اجرای مجدد خود از یک mutex که با فرمت خاصی ایجاد می‌شود، استفاده می‌کند. به عنوان مثال در یکی از نمونه‌ها، بدافزار اقدام به دریافت نام کاربری کرده و سپس عبارت "Defender" را به آن اضافه می‌کند.



شکل ۲ Mutex مورد استفاده توسط بدافزار

۳-۱ پردازه و سرویس مشکوک

بدافزار برای عملیات خود نیاز به اجرای سرویس و همچنین پردازه[۴] دارد. یکی از مواردی که در سامانه‌های آلوده دیده شد، وجود یک پردازه‌ی svchost است که والد آن services نیست. در واقع والد این پردازه یک برنامه سالم و دارای امضای معتبر است که توسط یک سرویس اجرا شده و بعد از اجرای پردازه از بین می‌رود و در نتیجه این پردازه والدی ندارد.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
winlogon.exe		1,524 K	7,216 K	540	Windows Logon Application	Microsoft Corporation
dwm.exe	0.04	26,220 K	56,812 K	804	Desktop Window Manager	Microsoft Corporation
explorer.exe	0.03	125,076 K	206,464 K	4244	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.01	3,756 K	13,012 K	5524	VMware Tools Core Service	VMware, Inc.
Taskmgr.exe	0.22	14,312 K	35,520 K	5076	Task Manager	Microsoft Corporation
mmc.exe	< 0.01	17,208 K	43,292 K	5908	Microsoft Management Cons...	Microsoft Corporation
mmc.exe	< 0.01	15,892 K	37,700 K	7484	Microsoft Management Cons...	Microsoft Corporation
ServerManager.exe	< 0.01	118,280 K	144,720 K	3900	Server Manager	Microsoft Corporation
regedit.exe	< 0.01	4,964 K	16,048 K	4736	Registry Editor	Microsoft Corporation
mmc.exe	< 0.01	295,844 K	19,444 K	7828	Microsoft Management Cons...	Microsoft Corporation
notepad.exe	< 0.01	1,732 K	10,764 K	7340	Notepad	Microsoft Corporation
procexp.exe		2,832 K	8,520 K	2160	Sysinternals Process Explorer	Sysinternals - www.sysinte
procexp64.exe	0.49	27,136 K	50,768 K	5400	Sysinternals Process Explorer	Sysinternals - www.sysinte
cmd.exe		1,664 K	2,600 K	7020	Windows Command Processor	Microsoft Corporation
conhost.exe	< 0.01	1,320 K	8,320 K	7788	Console Window Host	Microsoft Corporation
Procmon.exe		2,076 K	12,312 K	7744	Process Monitor	Sysinternals - www.sysinte
Procmon64.exe	< 0.01	37,480 K	307,996 K	6708	Process Monitor	Sysinternals - www.sysinte
cmd.exe		1,492 K	2,600 K	7080	Windows Command Processor	Microsoft Corporation
conhost.exe	< 0.01	1,264 K	7,696 K	4728	Console Window Host	Microsoft Corporation
iexplore.exe	< 0.01	6,616 K	29,104 K	1164	Internet Explorer	Microsoft Corporation
iexplore.exe	< 0.01	15,188 K	36,352 K	7896	Internet Explorer	Microsoft Corporation
perfmon.exe	0.06	21,048 K	34,864 K	6320	Resource and Performance ...	Microsoft Corporation
svchost.exe		2,576 K	6,472 K	96	Host Process for Windows S...	Microsoft Corporation

شکل ۳ وجود پردازه svchost مشکوک

[۴] Process

لازم به ذکر است در سامانه‌های قربانی عموما سه فایل وجود دارد که مورد استفاده‌ی بدافزار است. اسامی این فایل‌ها در سامانه‌های مختلف، متفاوت بوده ولی بطور کلی دارای ویژگی‌های زیر هستند:

- یک فایل اجرایی EXE که مربوط به یک نرم‌افزار قانونی و دارای امضای معتبر است. این فایل دارای یک مشکل امنیتی است که با استفاده از آن می‌توان یک فایل مخرب را درون برنامه بارگیری کرد (DLL Side Loading).
- یک فایل مخرب DLL که اقدام به رمزگشایی برخی از کدهای خودش و سپس تغییر کدهای فایل EXE اصلی در Entry Point نموده و Entry Point خودش را دوباره اجرا می‌کند. در ادامه این DLL اقدام به کدگشایی فایل سوم می‌نماید.
- یک فایل مخرب فشرده و رمزشده که در واقع Payload اصلی است.

۴-۱ ارسال شواهد به مرکز مدیریت راهبردی افتا

پس از اجرای برنامه آشکارساز، خروجی متناسب در پنجره برنامه و در قسمت ‘‘وضعیت سیستم’’نشان داده خواهد شد. در صورتی که سیستم آلوده نباشد، در قسمت وضعیت سیستم پیغام "نشانه ای از آلودگی یافت نشد" نشان داده خواهد شد. در این حالت خروجی هر چهار متغیر سمت چپ پنجره برنامه برابر "false" می باشد و نیاز به اقدام دیگری نخواهد بود. اما اگر وضعیت سیستم، آلودگی را نشان داد، لازم است که به کمک گزینه "ذخیره داده‌ها و ارسال به مرکز افتا" شواهد را ذخیره کرده و از طریق راه‌های ارتباطی ذکر شده، مراتب را سریعا به مرکز افتا منعکس نمایید.

شکل ۴ ابزار آشکارساز

نحوه کارکرد پاک‌ساز

بر اساس شواهد بدست آمده از نفوذ مهاجمین، در این ابزار سعی می‌گردد تنظیمات بدافزار و همچنین فایل‌های آلوده مورد استفاده مهاجمین از سامانه پاک شود. لازم به تذکر مجدد است که قبل از اجرای این ابزار شواهد بدست آمده توسط ابزار "آشکارساز" به مرکز افتا گزارش شود و در صورت تایید این مرکز، ابزار پاک‌ساز اجرا شود. پس از اجرای موفقیت آمیز برنامه پاک‌ساز، پیغام متناسب به پاک‌شدن آلودگی نمایش داده خواهد شد. جهت اطمینان از پاکسازی آلودگی، می‌توان برنامه آشکارساز را مجددا اجرا کرد تا وجود شواهد آلودگی بررسی شود.

۱. حذف کلید رجیستری مربوطه
۲. حذف سرویس مربوطه برای جلوگیری از اجرای مجدد آن
۳. حذف پردازه svchost مربوطه
۴. حذف فایل‌های آلوده‌ی مورد استفاده‌ی بدافزار

مشخصات فایل‌های پیوست

در پیوست این مستند دو فایل اجرایی قرار داده شده است که مشخصات آن‌ها در جدول زیر آمده است.

نام فایل	MD5	حجم فایل
AFTA-APT27-Detector.exe	77df3fb2382ae5f77c69cd199560725b	435 KB
AFTA-APT27-Removal.exe	28f9ef5798ea561936fae36ffa680753	380 KB