جمهوری اسلامی ایران

ریاست جمهوری

مرکز مدیریت راهبردی افتا

بررسی گروه هکری APT-27

بهمن ماه 1398

فهرست مطالب

معرفی گروه APT-27

گروه‌های هکری وابسته به دولت‌ها موضوع جدیدی تلقی نمی‌شوند. در سال‌های اخیر شاهد حمله‌های زیادی به زیرساخت‌های سازمان‌های حساس در کشورهای مختلف از جمله کشور ایران، توسط گروه‌های مختلف بوده‌ایم. برخی از این حملات هدفمند[1] و سازمان‌یافته و برخی دیگر عمومی و صرفا جهت توسعه بستر بدافزاری می‌باشند. به زبان ساده حملات هدفمند به زیرساخت‌های حیاتی یک کشور اعم از بسترهای دولت الکترونیک از اهداف حملات APT یا Advanced Persistent Threat شمرده می‌شوند. اما باید توجه داشته هر حمله‌ی بدافزاری را نمی‌توان یک APT دانست. APTها از لحاظ ساختار دارای اجرایی پیچیده و در چندین لایه اتفاق می‌افتند و در بیشتر موارد با مدارکی که به دست می‌آید می‌توان حمایت یک دولت، کشور و یا یک گروه خاص را از حملاتAPT مشاهده کرد. APTها برخلاف دیگر حملات سایبری تا حد امکان از رصد کارشناسان امنیتی دور می‌مانند زیرا در بیشتر موارد بعد از اینکه به اهداف از قبل تعیین شده خود می‌رسند، به سکوت طولانی فرو می‌روند و از چشم کارشناسان به دور می‌مانند. در واقع این حملات چند مرحله‌ای بوده و پس از نفوذ اولیه، مرحله گسترش، نصب، گرفتن دسترسی، ارتباط با مرکز فرماندهی[2] و در نهایت اجرای هدف مخرب را در یک زمان‌بندی عموما طولانی اجرا می‌کنند. در برخی موارد کشف APT ها بعد از چند سال از حمله اصلی صورت می‌گیرد؛ زمانی که مرحله مخرب حمله برای دستیابی به هدف اولیه اجرا شده و اطلاعات حساسی به دست گروه‌ها یا کشورهای طراح APT رسیده است.

حملات APT نیاز به زمان، نیروی فنی و در بعضی موارد هزینه‌های مالی بالا دارند، بعد از حملات Stuxnet و Flame، Duqu شرکت‌های امنیتی شروع به بررسی حملات APT کرده و آن‌ها را از لحاظ فنی و کشوری که به نظر می‌رسد از آن حمایت میکند (که البته چندان قابل استناد نیست) با شماره‌گذاری از یکدیگر جدا ساخته‌اند. چند نمونه ازAPT هایی که در سالهای اخیر کشف شده‌اند عبارتند از APT1 چین، APT3 چین، APT12 چین، APT28 روسیه، APT29 روسیه، APT32 ویتنام،APT33 ایران، APT37 کره شمالی و ... .

گروه هکری APT 27 که به نام‌های دیگری همچون TG-3390، Emissary Panda، BRONZE UNION، Iron Tiger و LuckyMouse نیز شناخته می‌شوند، 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 استفاده کرده‌اند و با وجود شباهت کلی حملات در مناطق جغرافیایی مختلف، در جزییات تفاوت‌هایی وجود دارد. در ادامه ابزار و آسیب‌پذیری‌هایی که عموما توسط این گروه استفاده می‌شود، آورده شده است.

ابزار:

- PlugX: یک تروجان با دسترسی از راه دور
- HttpBrowser: یک درپشتی
- ChinaChopper: یک webshell برای اجرای دستور در سیستم قربانی
- Hunter: ابزار تحت وب اسکن آسیب‌پذیری
- OwaAuth: یک webshell برای سرقت اطلاعات احرازهویت
- ASPXTool: نسخه ویرایش شده از ابزار ASPXSpy

[1] Targeted
[2] Command & Control

- nbtscan و netview
- یک نسخه ویرایش شده از mimikatz
- استفاده از تکنیک سرقت DLL یا DLL Hijacking
- HyperBro: یک تروجان با دسترسی از راه دور
- Rcmd: ابزار اجرای دستور در سیستم قربانی
- Wrapikatz: ابزاری برای دور زدن شناسایی mimikatz توسط ابزارهای امنیتی
- Netview و Kekeo که ابزارهای در دسترس عموم هستند

آسیب‌پذیری:

- CVE-2011-3544: آسیب‌پذیری در Java Runtime Environment
- CVE-2010-0738: آسیب‌پذیری در JBoss
- CVE-2017-11882: آسیب‌پذیری در آفیس
- CVE-2019-0604: آسیب‌پذیری اجرای کد از راه دور در Microsoft SharePoint
- CVE-2017-0144: آسیب‌پذیری اجرای کد در Windows SMB
- CVE-2014-6324: آسیب‌پذیری در پروتکل Kerberos

بدافزار بعد از سوء استفاده از آسیب‌پذیری موجود در سازمان هدف (همچون آپلود وب‌شل بر روی IIS)، وارد شبکه شده و اقدام به آپلود فایل‌های دیگری بر روی سرور سازمان می‌کند. این فایل‌ها اقداماتی از جمله پویش شبکه برای پیدا کردن آسیب‌پذیری، گرفتن لیست نام کاربری و رمز عبور کاربران شبکه و آلوده کردن سیستم‌های دیگر در شبکه انجام می‌دهند. این بدافزار در تمامی سیستم‌های آلوده شده شامل پوشه‌ای با 3 فایل است. فایل اول فایل اجرایی سالمی است که دارای آسیب‌پذیری DLL Side Loading می‌باشد. فایل دوم DLL بدافزاری است که به علت آسیب‌پذیری ذکر شده در نرم‌افزار اجرا شده و اقدام به رمزگشایی فایل سوم می‌نماید. این فایل یک بار اقدام به پچ کردن فایل اول و رمزگشایی بخش‌های از خود در چندین مرحله می‌نماید، تا به این ترتیب تحلیل آن پیچیده و دشوار گردد. فایل سوم فایل رمز شده‌ای است که بعد از اجرا شدن DLL دوم توسط نرم‌افزار، رمزگشایی شده و در یک پردازش جدید با نام svchost اجرا می‌شود (به این تکنیک RunPE گفته می‌شود).
بدافزار بعد از گرفتن دسترسی اولیه اقدام به نصب سرویس بر روی سیستم هدف کرده است. این سرویس به محض ورود کاربر به سامانه اجرا شده و اقدام به اجرای بدافزار از طریق فایل سالم می‌نماید. این بدافزار بعد از آلوده کردن سیستم‌های داخلی اقدام به پاکسازی فایل‌های خود کرده و اثری از خود باقی نمی‌گذارد.

نشانه‌های خاص APT-27

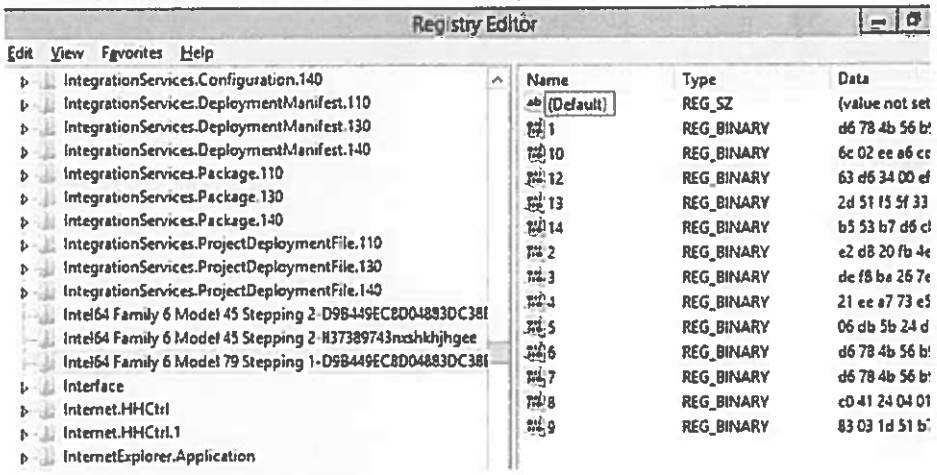
درحال حاضر برای یافتن نشانه‌های نفوذ گروه APT 27 از پنج روش استفاده می‌شود. البته نشانه‌های دیگری نیز وجود دارد که نیاز به بررسی بیشتری دارد.

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. در شکل 2 نمونه‌ای از کلید رجیستری یکی از سامانه‌های آلوده نشان داده شده است.



شکل 2: کلید رجیستری حاوی تنظیمات بدافزار

Mutex منحصربه فرد بدافزار

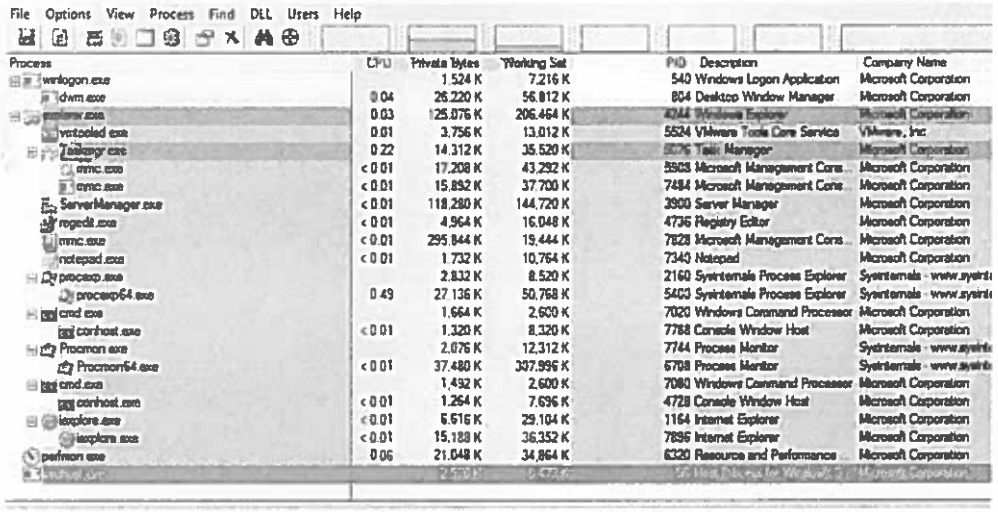
بدافزار برای جلوگیری از اجرای مجدد خود از یک mutex که با فرمت خاصی ایجاد می‌شود، استفاده می‌کند:

- فرمت نوع اول: شناسه بدافزار + نام کاربری + عبارت "Defender"
- فرمت نوع دوم: نام کاربری + عبارت "Defender"

شکل 3: Mutex مورد استفاده توسط بدافزار

پردازه و سرویس مشکوک

بدافزار برای عملیات خود نیاز به اجرای سرویس و همچنین پردازه[3] 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.



شکل 4: وجود پردازه svchost مشکوک

فایل‌های مورد نیاز برای اجرای بدافزار

در سامانه‌ی قربانیان 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:

[3] Process

- 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.
- یک فایل مخرب DLL که اقدام به رمزگشایی برخی از کدهای خودش کرده و در ادامه فایل سوم را کدگشایی می‌نماید.
- یک فایل مخرب فشرده و رمزشده که در واقع Payload اصلی بدافزار است.

جدول 1: مجموعه فایل‌های در نمونه‌های آلوده بررسی شده

نام مجموعه/ نام فایل‌ها		مقدار hash
مجموعه فایل یک	plugin_host.exe PYTHON33.dll PYTHON33.hlp	F0B05F101DA059A6666AD579A035D7B6 5F01FC0668E2337BD614E4B246818709 8F83C9FC5F89A0601B30837C1C7F7B69
مجموعه فایل دو	AppPatch.exe GameuxInstallHelper.dll url.sys.bin	13435101240F78367123EF01A938C560 CDCD0EA8838301A2152E9617D56ECFDC D77EAA0C63090364EA8DCF1E38AF0E97
مجموعه فایل سه	gdf.exe GameuxInstallHelper.dll sys.bin	13435101240F78367123EF01A938C560 9EA44B384E8E34C2AFE893FFBE22731E 1DBC50E35FF93122EC322305C58F6641
مجموعه فایل چهار	gdf.exe GameuxInstallHelper.dll sys.bin	13435101240F78367123EF01A938C560 CDCD0EA8838301A2152E9617D56ECFDC 8544BF7CD507502538F7F26CB5943126
مجموعه فایل پنج	ThunderBrowser.exe libcef.dll 123xxx	7E5F7AC1B7526725ACE35C7680052F17 340688CF02CB91CABAE9316C76C9F7D9 D56F6FE82DE58DF5B455ECD3B3F8ECF7

سرویس نصب شده توسط بدافزار

بدافزار بعد از گرفتن دسترسی اولیه، غالبا اقدام به نصب یک سرویس برای اجرای خودکار خود بر روی سیستم هدف کرده است.

مشخصات C&Cهای APT-27

پس از بررسی سیستم‌های مورد نفوذ قرار گرفته شده، لیستی از C&Cهایی که در APT27 مورد استفاده قرار میگرفتند، جمع آوری گردید.

مالک	آدرس IP
کشور هلند شرکت Linode[4]	178.79.143.78
کشور استرالیا شرکت Linode	172.105.179.74
کشور هند شرکت Linode	172.105.40.94
کشور کانادا شرکت Rogers Communications[5]	173.239.165.198
کشور آلمان شرکت Digitalocean[6]	178.128.198.154
کشور کانادا شرکت Novus Entertainment[7]	216.19.191.20
کشور آلمان شرکت Digitalocean	46.101.255.16
کشور لیتوانی شرکت FastServ[8]	85.204.74.143
کشور بلغارستان شرکت FastServ	89.45.67.194
کشور بریتانیا شرکت Digitalocean	138.68.154.133

این آدرس‌های IP پس از بررسی کلیدهای رجیستری حاوی تنظیمات بدافزار و پس از دیکد کردن آنها بدست آمده است. در ادامه نمونه کلیدهای رجیستری دیکد شده نشان داده شده است.

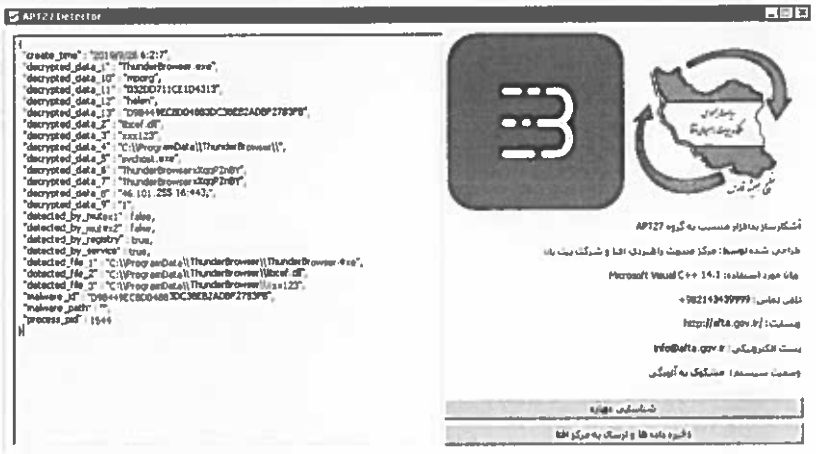
[4] فراهم کننده خدمات ابری

[5] ارائه دهنده خدمات اینترنتی، تلفن و ...

[6] ارائه دهنده خدمات زیرساخت ابری به کمک دیتاسنترهایی در نقاط مختلف دنیا

[7] ارائه دهنده خدمات تلکام

[8] ارائه دهنده خدمات هاستینگ



```
"decrypted_data_1" : "ThunderBrowser.exe",
"decrypted_data_10" : "mporg",
"decrypted_data_11" : "032DD711CE1D4313",
"decrypted_data_12" : "helen",
"decrypted_data_13" : "D9B449EC8D04883DC38EB2ADBF2783FB",
"decrypted_data_2" : "libcef.dll",
"decrypted_data_3" : "xxx123",
"decrypted_data_4" : "C:\\ProgramData\\ThunderBrowser\\",
"decrypted_data_5" : "svchost.exe",
"decrypted_data_6" : "ThunderBrowserxXqqPZnBY",
"decrypted_data_7" : "ThunderBrowserxXqqPZnBY",
"decrypted_data_8" : "46.101.255.16:443;",
"decrypted_data_9" : "1",
```

```
"decrypted_data_1" : "ThunderBrowser.exe",
"decrypted_data_10" : "mporg",
"decrypted_data_11" : "FED37B0F499B4383",
"decrypted_data_12" : "helen",
"decrypted_data_13" : "D9B449EC8D04883DC38EB2ADBF2783FB",
"decrypted_data_2" : "libcef.dll",
"decrypted_data_3" : "xxx123",
"decrypted_data_4" : "C:\\ProgramData\\ThunderBrowser\\",
"decrypted_data_5" : "svchost.exe",
"decrypted_data_6" : "ThunderBrowsersL5PQNJvO",
"decrypted_data_7" : "ThunderBrowsersL5PQNJvO",
"decrypted_data_8" : "178.79.143.78:443;",
"decrypted_data_9" : "1",
```

```
"decrypted_data_1" : "plugin_host.exe",
"decrypted_data_10" : "Default",
"decrypted_data_11" : "FE6133FC85E5435e",
"decrypted_data_12" : "idapro",
"decrypted_data_13" : "1137389743nxshkhjhgee",
"decrypted_data_2" : "PYTHON33.dll",
"decrypted_data_3" : "PYTHON33.hlp",
"decrypted_data_4" : "C:\\ProgramData\\plugin_host\\",
"decrypted_data_5" : "svchost.exe",
"decrypted_data_6" : "plugin_host377jcEmUc",
"decrypted_data_7" : "plugin_host377jcEmUc",
"decrypted_data_8" : "138.68.154.133:443;",
"decrypted_data_9" : "1:1",
```