بسمه‌تعالی

هشدار فوری مرکز ماهر در خصوص رواج احتمالی بدافزار VPNFilter در فضای مجازی کشور

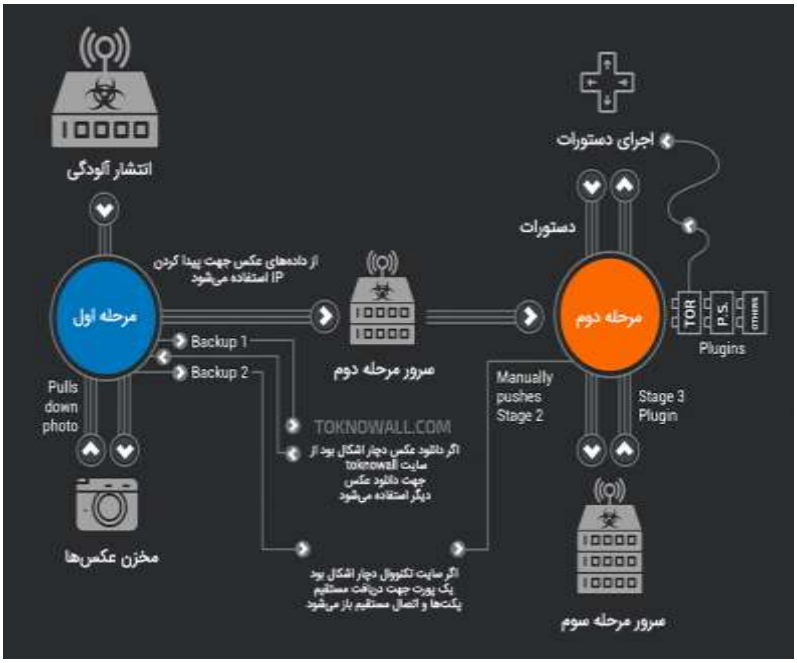
خبرهای دریافتی و رصد و پایش انجام گرفته، خبر از انتشار احتمالی بدافزار VPNFilter در ساعات و روزهای آینده در کشور می‌دهد. گزارش‌های موجود حاکی از آن است که این بدافزار تاکنون بیش از ۵۰۰ هزار قربانی در جهان داشته‌است و این عدد نیز افزایش خواهد داشت. لازم به ذکر است که قربانیان این بدافزار به یک نقطه جغرافیایی خاص تعلق ندارند و این بدافزار در تمامی مناطق فعال می‌باشد.

تجهیزات و دستگاه‌های برندهای مختلف شامل Linksys، Mikrotik، NETGEAR و TP-Link و همچنین تجهیزات ذخیره‌سازی QNAP در صورت عدم بروز رسانی مستعد آلوده شدن به این بدافزار هستند. با توجه به استفاده‌ی بالای برندهای فوق در کشور، هشدار حاضر ارائه دهندگان سرویسها، مدیران شبکه‌ها و کاربران را مخاطب قرار می دهد که نسبت به جلوگیری از آلودگی و ایمن‌سازی، اقدامات لازم را که در ادامه به آنها اشاره شده‌است در دستور کار قراردهند. لازم به ذکر است نوع دستگاه‌های آلوده به این بدافزار بیشتر از نوع دستگاه‌های غیر Backbone هستند و قربانیان اصلی این بدافزار، کاربران و شرکت‌های ISP کوچک و متوسط می‌باشند. در این گزارش شرح مختصری از شیوه عمل این بدافزار و روش‌های مقابله با آن ارایه خواهد شد.

تشریح بدافزار:

VPNFilterیک بدافزار چند مرحله است که توانایی جمع‌آوری داده از دستگاه قربانی و انجام حملات مخرب را دارد. در مرحله اول، این بدافزار یک مکان دائمی برای ذخیره کدهای مخرب به دست می‌آورد. بر خلاف بسیاری از بدافزارها روی دستگاه‌های IOT که با راه‌اندازی مجدد دستگاه از بین می‌روند، این بدافزار با راه‌اندازی مجدد از میان نخواهد رفت! هدف مرحله اول، ایجاد یک بستر جهت اجرای مرحله دوم بدافزار است. در مرحله اول، دستورات مختلفی (و در برخی اوقات تکراری) جهت استفاده در مرحله دوم به سیستم عامل دستگاه قربانی اضافه می‌شود. در این مرحله آدرس IP دستگاه جهت استفاده

در مرحله دوم و شیوه تعامل با دستگاه قربانی در اختیار قرار می‌گیرد. شکل زیر نمایی از چرخه حیات و ارتباطات بدافزار را نشان می دهد.



شناسایی قربانیان:

بر اساس بررسی‌های انجام شده توسط آزمایشگاه‌ها و محققان امنیتی، قربانیان این بدافزار به یک نقطه جغرافیایی خاص تعلق ندارند و این بدافزار در تمامی مناطق فعال بوده است. دستگاه‌های قربانیان پس از آلودگی شروع به پویش بر روی درگاه‌های2000 ,80 ,23 و 8080 پروتکل TCP می‌کنند و از این طریق قابل شناسایی است (دستگاه‌هایی که مداوم این ۴ پورت را پایش می‌کنند مشکوک به آلودگی هستند).

مقابله با آلودگی:

به خاطر ماهیت دستگاه‌های آلوده شده و هم به سبب نوع آلودگی چندمرحله‌ای که امکان پاک کردن آن را دشوار می‌کند، مقابله با آلودگی مقداری برای کاربران معمولی دشوار می‌باشد، مشکل از آنجا آغاز می‌شود که بیشتر این دستگاه‌ها بدون هیچ دیواره‌ی آتش یا ابزار امنیتی به اینترنت متصل هستند. دستگاه‌های آلوده شده دارای قابلیت‌های ضدبدافزار داخلی نیز نیستند.

بر همین اساس باید به دنبال روشی جهت جلوگیری از انتشار این آلودگی بود. گروه پژوهشی Talos حدود ۱۰۰ امضاء سیستم تشخیص نفوذ اسنورت را به صورت عمومی منتشر کرده است که می‌تواند جهت جلوگیری از انتشار این آلودگی به دستگاه‌های شناخته‌شده مورد استفاده قرار گیرد.

پیشنهادات:

- در صورت آلودگی، بازگردانی تنظیمات به حالت پیش‌فرض کارخانه منجر به حذف کدهای غیرمقیم می‌شود.
- میان‌افزار و لیست تجهیزاتی که در ادامه گزارش قید شده‌اند حتما به‌روز رسانی شوند.
- شرکت‌های ارائه دهنده‌ی سرویس های اینترنتی نیز با رصد و پایش ترافیک عبوری، از وجود آلودگی مشتریان خود آگاه و اقدامات بیان شده را اطلاع رسانی نمایند.
- مسدود سازی ارتباطات با دامنه ها و آدرس های آپی که در تحلیل های امینتی و گزارشات به آنها اشاره شده است.(رجوع به انتهای گزارش حاضر)
- با توجه به مقیم بودن مرحله ۱ بدافزار و احتمال انجام اعمال خرابکارانه مانند پاک کردن میان افزار، عدم اقدام به موقع و سهل‌انگاری در این زمینه ممکن است باعث عدم پایداری شبکه قربانی شود.

جمع‌بندی:

VPNFilterیک بدافزار بسیار خطرناک و دارای قدرت زیاد در به‌کارگیری منابع قربانی است که به شدت در حال رشد است. این بدافزار ساختاری پیمانه‌ای دارد که به آن امکان افزودن قابلیت‌های جدید و سوء استفاده از ابزارهای کاربران را فراهم می‌کند. با توجه به استفاده بسیار زیاد از دستگاه‌هایی مورد حمله و دستگاه‌های IOT عدم توجه به این تهدید ممکن است منجر به اختلال فلج کننده در بخش‌هایی از سرویس‌ها و خدمات گردد. در بدترین حالت این بدافزار قادر به از کار

انداختن دستگاه‌های متصل به اینترنت کشور و هزینه بسیار زیاد جهت تجهیز مجدد این دستگاه‌ها شود. توجه به این نکته مهم است که این بدافزار به راحتی قابل پاک کردن از دستگاه‌های آلوده نمی‌باشد.

دامنه‌های مرتبط به مخزن عکس

- photobucket.com/user/nikkireed11/library
- photobucket.com/user/kmila302/library
- photobucket.com/user/lisabraun87/library
- photobucket.com/user/eva_green1/library
- photobucket.com/user/monicabelci4/library
- photobucket.com/user/katyperry45/library
- photobucket.com/user/saragray1/library
- photobucket.com/user/millerfred/library
- photobucket.com/user/jeniferaniston1/library
- photobucket.com/user/amandaseyfried1/library
- photobucket.com/user/suwe8/library
- photobucket.com/user/bob7301/library
- toknowall.com

آدرسهای IPها:

- 91.121.109.209
- 217.12.202.40
- 94.242.222.68
- 82.118.242.124
- 46.151.209.33
- 217.79.179.14
- 91.214.203.144
- 95.211.198.231
- 195.154.180.60
- 5.149.250.54
- 91.200.13.76
- 94.185.80.82
- 62.210.180.229

جهت بررسی و کسب اطلاعات جزیی و بیشتر به پیوند زیر مراجعه شود:

مرجع:

https://blog.talosintelligence.com/2018/05/VPNFilter.html