وزارة الاتصالات والتقانة

الهيئة الوطنية لخدمات الشبكة

مركز أمن المعلومات

دراسة بحثية عن البرنامج الخبيث

The VPNFilter Malware

إعداد

ماجد اسماعيل

رئيس دائرة الدراسات والأبحاث

حزيران-2018

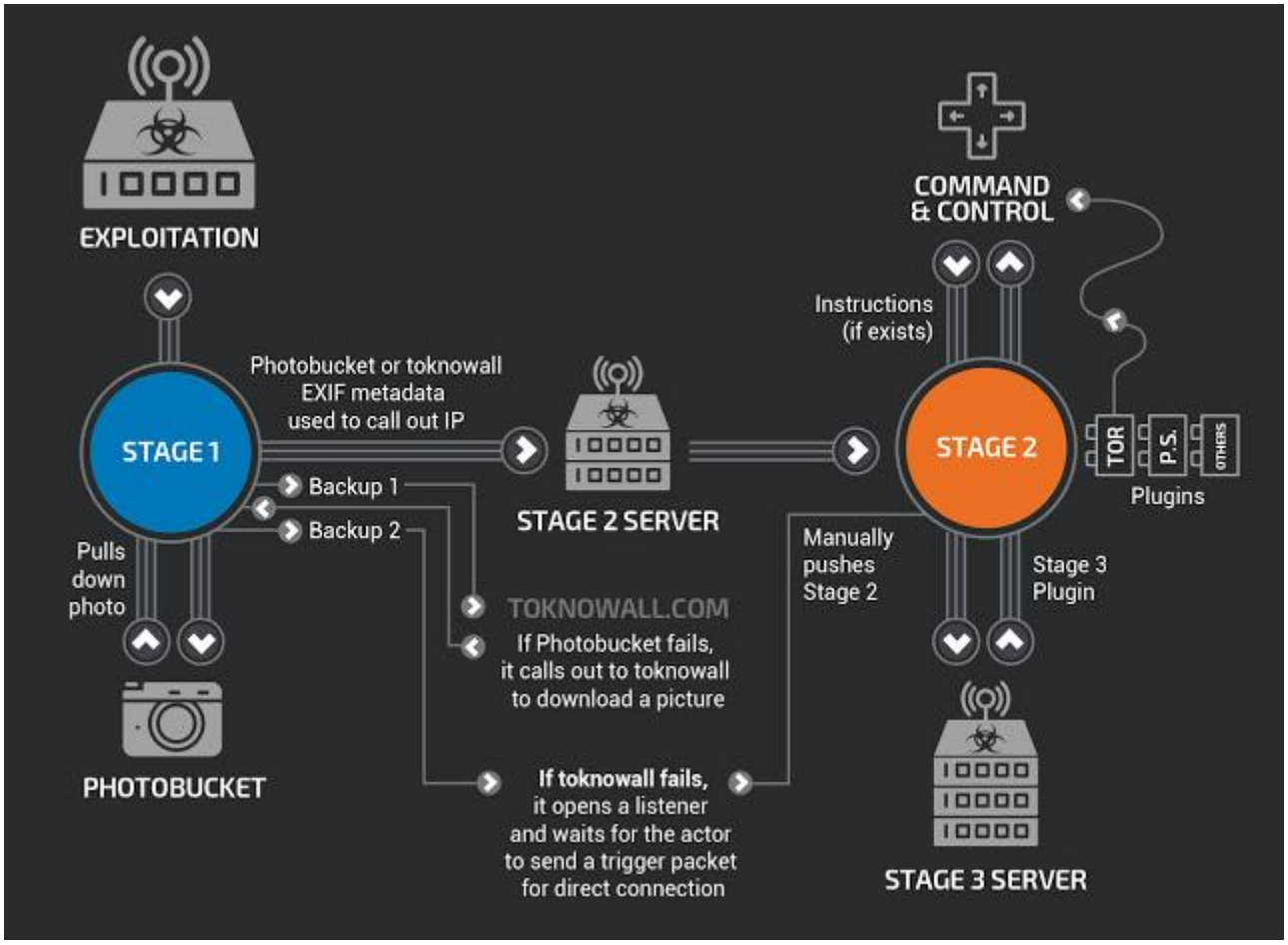
The VPNFilter Malware

منذ عدة أشهر بدأت الدراسات والأبحاث المتعلقة بالبرنامج الخبيث The VPNFilter Malware حيث خلصت نتائج هذه الدراسات إلى أن عدد الأجهزة المصابة التي تم إحصاؤها حتى أيار 2018 حوالي 500000 جهازاً على الأقل وهي موزعة على 54 بلداً وعلى الأنواع التالية: Linksys, MikroTik, Netgear, TP-Link, ASUS, D-Link, Huawei, Ubiquiti, UPVEL, ZTE، تعتبر هذه الأجهزة من فئة الشبكات المنزلية وفئة شبكات الأعمال المكتبية الصغيرة أو ما يطلق عليه اصطلاحاً SOHO: Small Office/ Home Office، بالإضافة إلى وحدات التخزين NAS المنتجة من قبل شركة QNAP، إن المهمة الرئيسية لهذا البرنامج هي الحصول على بيانات الدخول المختلفة الخاصة بالمستخدمين ومراقبة بروتوكولات Modbus SCADA بالإضافة إلى تخريب الجهاز المضيف وقطع الاتصال الشبكي عن الأجهزة المتصلة بالشبكة المصابة. يُعتقد بأن الأجهزة التي تمت إصابتها لم تكن تحوي أنظمة منع التطفل Intrusion Prevention System IPSs أو حتى نظام حماية Host Based كتطبيقات مكافحة البرمجيات الخبيثة Antimalware ، بالإضافة إلى أن هذه الأجهزة تميزت بأنها تعمل بأنظمة تشغيل قديمة نسبياً تحوي العديد من الثغرات المعروفة وكيفية استغلالها أو أنه يتم الدخول إليها ببيانات دخول افتراضية Default Credentials، على الأرجح أن بداية عمليات اطلاق البرنامج VPNFilter كانت في العام 2016.

معلومات تقنية Technical Details

يعتبر البرنامج الخبيث VPNFilter أحد أنوع البرمجيات الخبيثة متعددة المراحل Multi Stage لجهة عمليات التنصيب والتشغيل، بالإضافة إلى كونه برنامجاً خبيثاً يتمتع بقدرات وإمكانات متعددة Versatile Capabilities حيث تم تصميمه وتطويره لإنجاز العديد من المهام التي تتعلق بالتجسس وجمع المعلومات والقيام بالعديد من الهجمات السيبرانية المختلفة والتي قد تكون شديدة التأثير. تتميز المرحلة الأولى بضمان تمكين واستمرار عمل البرنامج أثناء عملية إعادة إقلاع الجهاز الهدف، وبالطبع التحضير للمرحلة الثانية التي تعتمد بشكل رئيسي على تقانات متقدمة للقيادة والتحكم Command and Control C2 من أجل إجراء عمليات البحث الضرورية لاكتشاف العنوان الرقمي IP المناسب للمرحلة الثانية، الغاية هنا هي المرونة في التأقلم والتكيف الفوري مع أي

تغيير غير متوقع في بنية القيادة والتحكم C2. بالنسبة للمرحلة الثانية فهي تبدأ بالعمل بعد الإقلاع مباشرة وهي تتميز بالعديد من القدرات كجمع المعلومات عن الملفات، تنفيذ تعليمات معينة وإدارة الجهاز المضيف، تحوي بعض الإصدارات بالإضافة إلى ما سبق إمكانية التعديل على رماز نظام تشغيل الجهاز المضيف وفرض إعادة إقلاع قسرية مع الحرص على جعل الجهاز غير صالحاً للاستخدام. المرحلة الثالثة هي عبارة عن وحدات متعددة تعمل معاً ضمن إطار عمل موحد كإضافات Plugins لصالح المرحلة الثانية، هذه الإضافات تقوم بتزويد المرحلة الثانية بعدد من الوظائف والمهام الإضافية، تحوي المرحلة الثالثة وحدتين أساسيتين الوحدة الأولى مسؤولة عن التجسس وجمع البيانات ضمن الدفق الشبكي الذي يمر عبر الجهاز المصاب وبشكل خاص البيانات التي تحوي معلومات دخول المستخدمين المختلفة بالإضافة إلى مراقبة برتوكولات Modbus SCADA، الوحدة الثانية هي وحدة اتصالات مهمتها تأمين اتصال موثوق للمرحلة الثانية عبر شبكة Tor.



الاستغلال Exploitation

لم تعرف حتى الآن الآلية الحقيقية لعمليات الاستغلال التي يستخدمها البرنامج الخبيث للنفاذ إلى موارد أنظمة تشغيل الأجهزة المستهدفة ولكن الدراسات المختلفة أكدت أن الأجهزة التي تمت إصابتها كانت تحوي ثغرات مشهورة ومعروفة التفاصيل وطرق الاستغلال، بمعنى آخر أن برنامج VPNFilter لا يحتاج بالضرورة إلى تقنية استغلال اليوم الأول Zero-Day Exploitation، أو أن الدخول لهذه الأجهزة Login قد يتم بواسطة بيانات الدخول الافتراضية Default Credentials أو بكلمات مرور ضعيفة...

المرحلة الأولى (Persistent Loader) Stage1

تستهدف المرحلة الأولى من البرنامج VPNFilter الأجهزة التي تحوي أنظمة التشغيل Firmware المبنية على أساس كل من Busybox و Linux والمصممة للعمل ضمن بيئة متعددة المعالجات Several CPU Architectures، تتمتع هذه المرحلة بإمكانية الوصول إلى الذاكرة غير القابلة للتطاير NVRAM حيث يمكنها الكتابة ضمن هذه الذواكر وتعديل العديد من القيم، ومن ثم تقوم المرحلة الأولى بإضافة نفسها إلى نظام جدولة المهام الدورية Crontab في أنظمة Linux كي تضمن ميزة استمرارية العمل حتى أثناء وبعيد إقلاع الجهاز.

تمت دراسة وتحليل عينات وأمثلة عن هذه المرحلة تعمل ضمن معالجات MIPS و x86 وتبين أن قنوات الاتصال التي يقوم البرنامج بعمليات التحميل عبرها هي قنوات عبر شبكة Tor أو قنوات مشفرة بالبروتوكول SSL، حيث إن بعض الرمازات التي يتم تحميلها تكون بصيغة مشفرة ويتم فك تشفيرها لاحقاً أثناء عمليات التنفيذ Runtime، بالنسبة لمنهجية التشفير المستخدمة فهي أقرب ما تكون -احتمالاً- للمنهجية RC4 ولكن بأسلوب مغاير لأسلوب المنهجية التقليدي بالإضافة إلى ضبط بعض المؤشرات التي تشير لاستخدام مطوري البرنامج المنهجية S-boxes.

بعد عمليات الإقلاع الأساسية يقوم البرنامج بالبدء بعمليات تحميل صفحات من روابط URLs معينة يشير بعضها للمجال Photobucket.com وهو موقع لمشاركة ملفات صور Images، حيث يقوم البرنامج بتحميل الصورة الأولى ومن ثم استخراج العنوان الرقمي IP Address الخاص بمخدم التحميل من ست قيم صحيحة من قيمتي الطول والعرض لـ GPS تكون ضمن معلومات الملف وهو بالصيغة EXIF. في حال فشل البرنامج بتحميل الصورة المطلوبة واستخراج العنوان الرقمي للمخدم من الموقع Photobucket.com يلجأ البرنامج إلى الموقع البديل toknowall[.]com لتنفيذ العمليات السابقة وفي حال فشل هذه الخطوة فلدى البرنامج إجراء احتياطي وهو فتح متنصت Listener والذي بدوره يقوم بالخطوات التالية:

1. تحديد العنوان الرقمي الحقيقي الحالي Public IP بواسطة المجال api.ipify[.]org.
2. تفحص الرزم الشبكية TCP/IPv4 بواسطة سلسلة من إشارات SYN flag
3. مقارنة العنوان الرقمي الهدف Destination IP بالقيمة الناتجة من الخطوة 1، ويقوم البرنامج بتجاوز هذه الخطوة في حال فشل الخطوة 1
4. التأكد من أن حجم الرزمة الشبكية 8Bytes فما فوق.
5. فحص البيانات الموجودة في الرزمة والبحث عن كل من \x0c\x15\x22\x2b
6. البايتات الأربعة التي تلي مباشرة تلك الأربعة –من الخطوة 5– هي التي تمثل العنوان الرقمي المطلوب حيث يتم تفسيرها مثلاً \x01\x02\x03\x04 تمثل العنوان 1.2.3[.]4
7. طلب العنوان الرقمي الجديد وتحديده للمرحلة 2.
8. التأكد من أن المرحلة الثانية تعادل على الأقل 1,001 Bytes

المرحلة الثانية (Non-Persistent) Stage2

يبدأ البرنامج المرحلة الثانية بإنشاء كل من المجلدات التالية:

- مجلد الوحدات Modules Folder في المسار /var/run/vpnfilterm
- مجلد العمل Working Directory في المسار /var/run/vpnfilterw

ثم يدخل البرنامج في حلقة عمل يقوم أولاً بالاتصال بمخدم C2 Server وثانياً تنفيذ التعليمات التي تم جلبها من المخدم، أسماء هذه التعليمات مشفرة بنفس الأسلوب المخصص للمنهجية RC4 المشار إليه في المرحلة 1.

المهام المنجزة من قبل إصدارات البرنامج العاملة على المعالجات x86:

1. تعديل الـ 5000 Bytes الأولى من الملف /dev/mtdblock0 وكتابة أصفار فوق القيم الأصلية ثم إعادة إقلاع الجهاز.
2. exec: تنفيذ رمازات shell commands
3. tor: ضبط إشارة إعداد شبكة tor للقيمة 0 او 1
4. copy: نسخ ملف معين من العميل (الجهاز المضيف) إلى المخدم C2
5. seturl: ضبط الرابط للوحة الإعداد الحالية.
6. proxy: ضبط عنوان المخدم الوكيل الحالي.

7. port: ضبط المنفذ الحالي للمخدم الوكيل.
8. delay: ضبط زمن التأخير لحلقة التنفيذ الرئيسية.
9. reboot: إعادة إقلاع الجهاز في حال كانت قيمة زمن العمل Up Time أكثر من 256 ثانية، وكان اسم بناء النسخة الحالية Build Name موجودة ضمن متغير Parameter معين.
10. download: تحميل عنوان URL لملف، هذه الخطوة قد تكون لجميع الأجهزة أو لنسخ محددة باسم البناء Build Name

المهام التالية تقوم بها إصدارات البرنامج العاملة على المعالجات MIPS إضافة لما سبق:

- stop: إيقاف عمل البرنامج الخبيث.
- relay: هي تعليمة delay مكتوبةً بشكل خاطئ.

أثناء عملية تنصيب وحدة Tor تقوم المرحلة 2 باستخدام عنوان رقمي واحد أو أكثر One or more IPs مخزنة ضمن إعدادات المرحلة كعناوين لمقابس مخدمات وكيلة SOCKS5 Proxies لشبكة Tor وتحاول الاتصال بلوحة تحكم Control panel موجودة ضمن الاعدادات أيضاً، وكما في المرحلة الأولى الاتصال بين البرنامج الخبيث والمخدمات الوكيلة يتم عبر البروتوكول SSL، بعد الانتهاء من تنصيب وحدة Tor يقوم البرنامج بعدها بالاتصال بأحد مجالات onion. عن طريق المخدم الوكيل المحلي SOCKS5 والذي ستقوم وحدة Tor بتزويد البرنامج به، هذا الاتصال سيتم عن طريق البروتوكول HTTP، وبنتيجة مراقبة بيانات الاتصال تبين ما يلي:

أمثلة عن الطلبات الموجهة من البرنامج إلى المخدم:

```
{
"uq":"px(01:02:03:04:05:06)",
"pv":"pPRXi686QNAPX86",
"ad":"10.0.0.1",
"bv":"0.11.1a/0.3.9qa",
"nn":"YnVpbGRyb290",
"tn":"",
"on":"1"
}
```

uq: رقم معرف للجهاز المصاب وهو عادة العنوان الفيزيائي MAC Address

pv: منصة عمل نظام التشغيل التي يعمل ضمنها البرنامج .

ad: العنوان الرقمي الحقيقي Public IP Address للجهاز.

bv: أرقام إصدارات:

Version of Stage1 Loader 0.3.9qa, Version of Stage2 Binary 0.11.1a

nn: اسم العقدة Node Name

tn: إشارة The Tor flag

on: إشارة The Onion flag

يقوم البرنامج بترميز الطلبات بواسطة JSON Object بالطريقة Base64 وإرسالها إلى المسار /bin32/update.php بواسطة المنهجية HTTP POST بالمتغير "me"، ويتم ذلك بواسطة وكيل مستخدم:

User Agent (Mozilla/6.1 (compatible; MSIE 9.0; Windows NT 5.3; Trident/5.0))

وهو وكيل مستخدم غير قياسي حيث إن النسخة "Windows NT 5.3" غير موجودة أصلاً.

يقوم المخدم لاحقاً بالإجابة على طلبات البرنامج الخبيث كما يلي:

```
{
"tr":3060,
"pxs":["217.12.202.40","94.242.222.68","91.121.109.209"],
"tor":"tor 1",
"mds":[]
}
```

Tr: ضبط التأخير الزمني للحلقة الرئيسية.

pxs: قائمة بلوحات التحكم التي سيتم الاتصال بها وهي عناوين المخدمات C2

tor: اسم نسخة وحدة The Tor Module

mds: قائمة بالوحدات التي سيتم جلبها Modules to Fetch حيث إن كل قيمة ستكون بالتنسيق:

"<command_id> <module_id> <module_name> <module_args (base64-encoded)>"

سيقوم البرنامج بتحميل الوحدة من المسار /bin32/update.php بواسطة اسناد المتغير me في نموذج POST لاسم الوحدة Module Name مثال: tor_i686 لوحدة Tor Module، ويتم تنفيذ ذلك لكل دورة Iteration. ورود قائمة فارغة Blank List هنا سيعني ذلك إلغاء كافة التعليمات الموجودة من خلال إلغاء تفعيل هذه التعليمات وإيقاف عمل الإجراءات المتعلقة بها Kill Running Processes.

المرحلة الثالثة (Non-Persistent) Stage3

تتألف المرحلة الثالثة بشكل رئيسي من وحدتين أساسيتين كإضافات Plugin Modules، الوحدة الأولى عبارة عن وحدة تجسس على الرزم الشبكية Packet Sniffer ووحدة الاتصالات Communication Plugin والتي تؤمن اتصال البرنامج الخبيث بشبكة Tor، ولكن تبين من خلال الاختبارات العملية وجود عدد من الوحدات المضافة الأخرى منها وحدة التجسس Packet Sniffer خاصة بمعالجات MIPS في المرحلة الثانية حيث تقوم هذه الوحدة باعتراض Intercepts الدفق الشبكي والبحث ضمن الرزم الشبكية عن البيانات المتعلقة بأي عمليات مصادقة عبر الويب HTTP Basic Authentications، بالإضافة إلى أنها تقوم بتعقب Track الرزم الشبكية للبروتوكول Modbus TCP/IP، يتم أرشفة كل المهام السابقة ضمن ملف سجل Log File ويتم حفظه في مجلد عمل المرحلة الثانية /var/run/vpnfilterw/، مما يمنح مشغلي البرنامج الخبيث القدرة على دراسة والتقاط وتعقب Understand, Capture, Trackالدفق الشبكي الذي يمر عبر الجهاز المصاب.

إن وحدة Tor Plugin Module تعمل بشكل جزئي ضمن المرحلة الثانية Stage2، ولكنها عملياً تحوي رمازاً تنفيذياً منفصلاً Tor Executable والذي يتم تحميله إلى المسار /var/run/tor/ ويتم إطلاق عمله بواسطة إجراء Process منفصل تماماً عن المرحلة الثانية، يشبه هذا الملف التنفيذي إلى حد بعيد العميل Tor Client الذي يعمل ضمن الجهاز حيث إنه يقوم بإنشاء ملف إعدادات Configuration File في المسار /var/run/torrc/ وملف عمل Working Directory في المسار /var/run/tord/.

الوحدة Ssler Module:

مهمة هذه الوحدة هي حقن رمازات خبيثة كرمازات JavaScript ضمن الدفق الشبكي Web Traffic الذي يمر عبر الجهاز المصاب في المنفذ 80، ويتم ذلك بتقنية المهاجم في الوسط Man-in-The-Middle، تم تأكيد وجود عدد من المتغيرات Parameters التي تقوم بضبط وتنظيم عمليات الحقن هذه وفق التالي:

dst: يستخدم من قبل Iptables Rules لتحديد العنوان الهدف IP أو مجال CIDR لتطبيق القاعدة Rule عليه

src:يستخدم من قبل Iptables Rules لتحديد العنوان المصدر IP أو مجال CIDR لتطبيق القاعدة Rule عليه

dump: إن المجال Domain الذي يوجد ضمن هذا المتغير سيتم توثيق ترويسات HTTP Headers العائدة له ضمن الملف reps_*.bin

site: سيتم تحديد صفحات ويب المجال الوارد هنا كهدف لحقن رمازات JavaScript Injection

hook: يتضمن عنوان URL ملف JavaScript لعملية الحقن.

بدايةً ستقوم الوحدة Ssler بإعداد تقنية Iptables من أجل إعادة توجيه Redirect الدفق الشبكي الوارد للمنفذ 80 إلى الخدمة المحلية العائدة لها والتي تقوم بالتنصت على المنفذ 8888، حيث تقوم بواسطة التعليمة insmod بإضافة ثلاث وحدات Iptables ضمن نواة نظام التشغيل Kernel وهي:

ip_tables.ko, iptable_filter.ko, iptable_nat.ko

ثم تقوم الوحدة Ssler بتنفيذ الرمازات التالية لإضافة قواعد Rules:

- iptables -I INPUT -p tcp --dport 8888 -j ACCEPT
- iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8888
- Example: ./ssler logs src:192.168.201.0/24 dst:10.0.0.0/16 -A PREROUTING -s 192.168.201.0/24 -d 10.0.0.0/16 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8888

وللتأكيد على بقاء هذه القواعد موجودة بشكل دائم وتحسباً لإزالتها ربما من قبل أي مستخدم تقوم الوحدة Ssler بعملية حذف لهذه القواعد ثم إضافتها مجدداً وتتم هذه العملية بشكل دوري كل أربع دقائق تقريباً.

أصبحت الآن كل طلبات البروتوكول HTTP عبر المنفذ 80 يتم اعتراضها وتدقيقها وتعديلها قبل ذهابها إلى وجهتها الحقيقية، تقوم الوحدة Ssler بعمل التعديلات التالية على طلبات HTTP قبل إرسالها لوجهتها:

- تبديل البادئة HTTPS:// للبروتوكول الآمن بـ HTTP://، كي يتمكن البرنامج الخبيث لاحقاً من كشف البيانات التي يتم تبادلها وخاصة بيانات الدخول.
- في حال وجود الترويسة Connection: keep-alive، يتم استبدالها بـ Connection: close، والغاية هي فرض تأسيس اتصال TCP جديد لكل طلب بين المخدم والعميل.
- في حال وجود ترويسة Accept-Encoding: gzip، يتم استبدالها بـ Accept-Encoding: plaintext/none وعليه لن يتم تهيئة وضغط الاستجابة لهذه الطلبات بتقنية gzip

تعتمد الوحدة على عدد من المتغيرات Parameters لضبط عمليات التجسس والحقن، من هذه المتغيرات dump حيث إن وجود اسم مضيف Host ما ضمن هذا المتغير هذا يعني أن كافة تفاصيل الطلب بما فيها الترويسات والقيم المسندة إليها سيتم حفظها، وفي حال لم يكن اسم المضيف Host موجوداً ضمن dump سيتم حفظ الطلبات التي تحوي ترويسة Authorization أو تحوي بيانات مصادقة، تعتمد الوحدة Ssler على البحث والتقصي ضمن الطلبات على عدد من السلاسل المحرفية لتحديد ما إذا كانت هذه الطلبات تحوي بيانات مصادقة أم لا وهي:

assword=

ass=

sername=

ser=

ame=

ogin=

ail=

hone=

session%5Busername

session%5Bpassword

session[password

accounts.google.com with string signin

بعد إجراء هذه التعديلات على طلبات HTTP تقوم الوحدة Ssler بتمرير الطلبات المعدّلة إلى وجهتها الحقيقية عبر المنفذ 80، ثم تبدأ الوحدة Ssler باستقبال الإجابات الواردة على هذه الطلبات وتقوم بإجراء التعديلات التالية عليها قبل تمريرها إلى وجهتها عبر الجهاز المصاب:

- تبديل البادئة //:HTTPS للبروتوكول الآمن بـ //:HTTP.
- في حال وجود أي من الترويسات التالية سيتم تجاهلها وإلغاؤها من بيانات الإجابة:
  - Alt-Scv
  - Vary
  - Content-MD5
  - content-security-policy
  - X-FB-Debug
  - public-key-pins-report-only
  - Access-Control-Allow-Origin
- تحويل الطلبات المشفرة إلى طلبات مجردة من أي تشفير Sslstripped واستخدام تقانات خداع خاصة.
- في حال وجود مجال ما ضمن المتغير site سيتم حقن رمازات JavaScript خبيثة ضمن كل الاستجابات التي تحوي الترويسة:

Content-Type: text/html or Content-Type: text/javascript، ويتم استبدال الوسم < meta name= … > بالوسوم <"script type="text/javascript" src="[hook value]> حيث hook هو المتغير Parameter الذي يحوي رابط ملف الحقن، بعدها سيتم دمج اسم الموقع مع العنوان الرقمي للجهاز الضحية وإضافة الناتج إلى قائمة داخلية Internal Whitelist في الوحدة Ssler حيث لن يتم استهدافه مرة أخرى بعمليات الحقن حتى يتم تفريغ هذه القائمة Clear List كل أربعة أيام.

أخيراً جميع المجالات التي يتم تجريد عملية الاستجابة منها من التشفير Sslstripped يتم إضافتها إلى قائمة Stripped Domains، إن المواقع التي تم توثيقها في هذه القائمة والتي سيتم اعتراض الطلبات الموجهة إليها من قبل الوحدة Ssler وسيتم تحويلها إلى HTTPS عبر المنفذ 443 بدل HTTP عبر المنفذ 80، المواقع

الأربعة التالية موجودة وبشكل افتراضي في قائمة Stripped Domaines وهي: www.google.com, twitter.com, www.facebook.com, or www.youtube.com. معنى هذا أن الوحدة Ssler ستتصل بهذه المواقع دائماً بالبروتوكول HTTPS وعبر المنفذ 443.

الوحدة Dstr Module :

تأخذ هذه الوحدة على عاتقها تنفيذ العمليات الخاصة بتنظيف أي وجود للبرنامج الخبيث VPNFilter وأي ملفات تابعة له ومحاولة إخفاء أي وجود له تحسباً لعمليات التدقيق والتحليل الجنائي Forensic Analysis، بالإضافة إلى تنفيذ عمليات حذف الملفات الضرورية لعمل الجهاز المصاب وبالتالي إخراجه من الخدمة بالطبع. الإصدارات الخاصة بمعالجات x86 تقوم أولاً بحذف نفسها من القرص ثم إيقاف تنفيذ الإجراء الأساسي للمرحلة Parent Stage2 Process ثم تقوم بالبحث عن كل الإجراءات العاملة والتي تحوي ضمن اسمها vpnfilter, security, tor وإيقاف Kill هذه الإجراءات وبعدها يأتي دور نظام التشغيل حيث ستقوم هذه الوحدة بحذف كل من المجلدات والملفات التالية:

/var/tmp/client_ca.crt
/var/tmp/client.key
/var/tmp/client.crt
/var/run/vpnfilterm/htpx
/var/run/vpnfilter
/var/run/vpn.tmp
/var/run/vpn.pid
/var/run/torrc
/var/run/tord/hidden_ssh/private_key
/var/run/tord/hidden_ssh/hostname
/var/run/tor
/var/run/msvf.pid
/var/run/client_ca.crt
/var/run/client.key
/var/run/client.crt
/var/pckg/mikrotik.o
/var/pckg/.mikrotik.
/var/msvf.pid

/var/client_ca.crt

/var/client.key

/var/client.crt

/tmp/client_ca.crt

/tmp/client.key

/tmp/client.crt

/flash/nova/etc/loader/init.x3

/flash/nova/etc/init/security

/flash/nova/etc/devel-login

/flash/mikrotik.o

/flash/.mikrotik.

/var/run/vpnfilterw/

/var/run/vpnfilterm/

/var/run/tord/hidden_ssh/

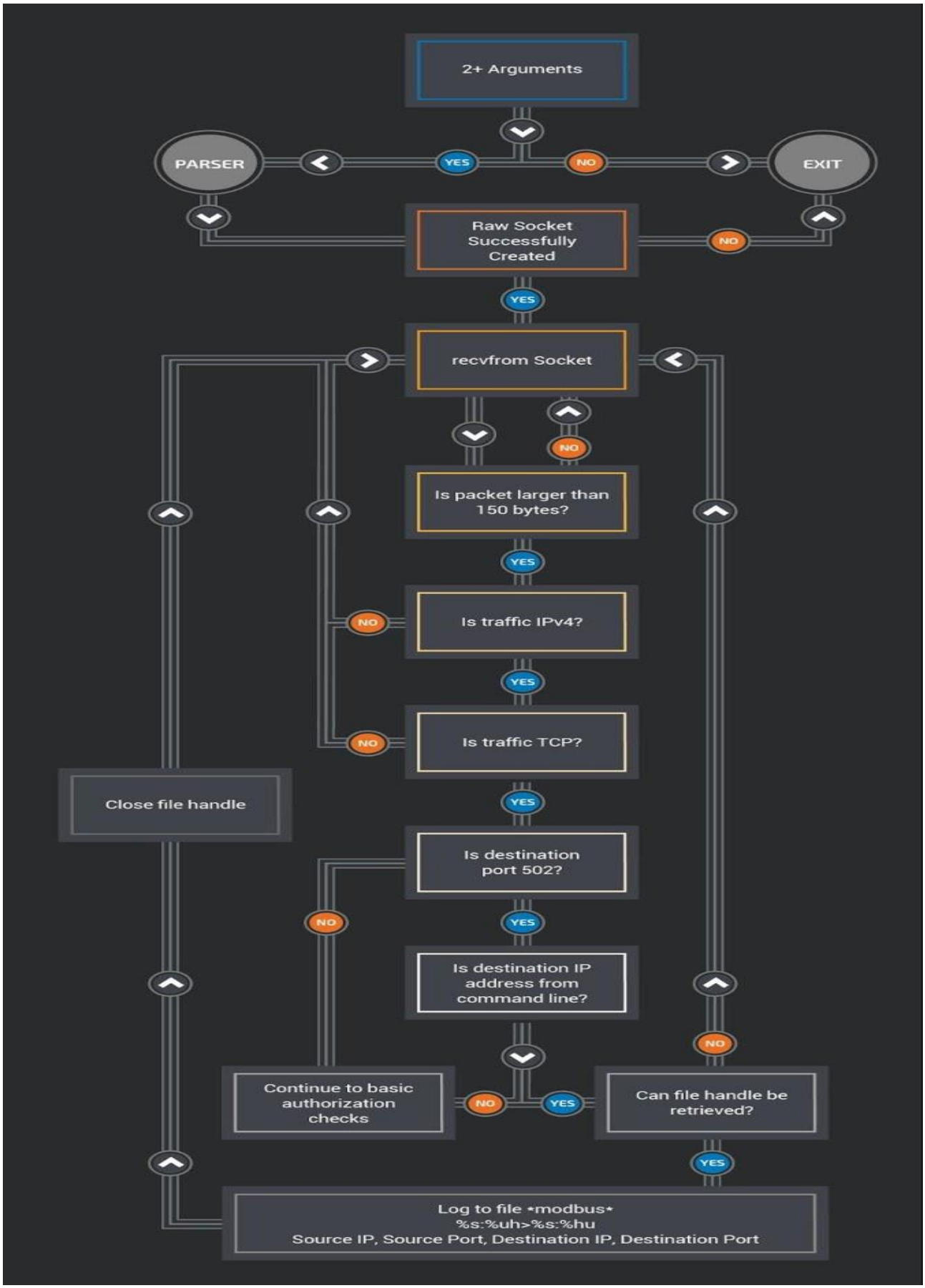
/var/run/tord/

/flash/nova/etc/loader/

/flash/nova/etc/init/

تعمل الوحدة dstr على حذف موجودات ذاكرة الجهاز Flash Memory بواسطة إعادة الكتابة فوق الإدخالات المتوفرة في الدليل /dev/mtdX/ حيث سيتم استبدال جميع Bytes المتوفرة بالـ 0xFF Byte، وأخيراً تقوم الوحدة بتنفيذ التعليمة */ rf- rm لحذف بقية ملفات نظام التشغيل وإعادة إقلاع الجهاز وعندها بالطبع لن يتمكن الجهاز من الإقلاع بسبب عدم وجود ملفات نظام التشغيل الضرورية لذلك.

الوحدة Ps Packet Sniffer:



وهي وحدة التجسس على الدفق الشبكي وخاصة الرزم الشبكية المتعلقة ببيانات المصادقة، تستخدم الوحدة مقابس خاصة Raw Sockets للبحث عن اتصالات لعناوين رقمية معرفة بشكل مسبق حيث تقوم بالبحث ضمن هذه الاتصالات عن رزم TCP Packets تتميز بأحجام 150 Bytes وما فوق، تمتلك الوحدة Ps Packet Sniffer الإمكانيات اللازمة للاطلاع View على محتويات الرزم الشبكية وليس لتعديل محتوياتها.
حيث إن الرزم التي ليست على المنفذ 502 سيتم البحث فيها عن BasicAuth ويتم أرشفة هذه البيانات.
بالنسبة للدفق الشبكي non-Modbus، سيتم التجسس عليها وأرشفة بيانات الدخول HTTP basic auth وذلك بحسب الشروط التالية:

- Destination IP Address == command line argument IP address
- Source port > 1024
- Source port != 8080
- Source port != 8088
- Packet Data length > 20 bytes
- Packet does not contain:
    - </ and >
    - <?xml
    - Basic Og==
    - /tmUnblock.cgi
    - Password Required
    - <div
    - <form
    - <input
    - this. and .get
    - {
    - }
    - 200 OK
    - <span
    - <SPAN
    - <DIV
- Packet contains 'Authorization: Basic' OR one user/pass combination
    - User

        - User=
        - user=
        - Name=
        - name=
        - Usr=
        - usr=
        - Login=
        - login=
    - Pass
        - Pass=
        - pass=
        - Password=
        - password=
        - Passwd=
        - passwd=

أخيراً الرزم الشبكية التي تحوي بيانات دخول ولكنها لا تحوي المنفذ 502 فإنه لن يتم تطبيق معايير الدفق الشبكي للبروتوكول Modbus:

- بالنسبة لـ Modbus يتم أرشفة كل من:

SourceIP, SourcePort, DestinationIP, DestinationPort ويتم وسمها بالعلامة *modbus*

- بالنسبة للرزم الأخرى يتم أرشفة كامل الرزمة فقط في حال توافقها مع شروط وجود بيانات الدخول.

نطاقات وعناوين المخدمات Known C2 Domains and IPs

النطاقات المرتبطة بالمرحلة الأولى Stage1:

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

النطاقات والعناوين المرتبطة بالمرحلة الثانية Stage2:

91.121.109209[.]
217.12.20240[.]
94.242.22268[.]
82.118.242124[.]
46.151.20933[.]
217.79.17914[.]
91.214.203144[.]
95.211.198231[.]
195.154.18060[.]
5.149.25054[.]
94.185.8082[.]
62.210.180229[.]
91.200.1376[.]
23.111.177114[.]

6b57dcnonk2edf5a[.]onion/bin32/update.php
tljmmy4vmkqbdof4[.]onion/bin32/update.php
zuh3vcyskd4gipkm[.]onion/bin32/update.php
4seiwn2ur4f65zo4.onion/bin256/update.php
zm3lznxn27wtzkwa.onion/bin16/update.php

قيم تجزئة ملفات البرنامج Known File Hashes

ملفات المرحلة الأولى Stage1 Malware

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec

0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92

b9770ec366271dacdae8f5088218f65a6c0dd82553dd93f41ede586353986124

51e92ba8dac0f93fc755cb98979d066234260eafc7654088c5be320f431a34fa

6a76e3e98775b1d86b037b5ee291ccfcffb5a98f66319175f4b54b6c36d2f2bf

313d29f490619e796057d50ba8f1d4b0b73d4d4c6391cf35baaaace71ea9ac37

ملفات المرحلة الثانية Stage2 Malware

9683b04123d7e9fe4c8c26c69b09c2233f7e1440f828837422ce330040782d17

d6097e942dd0fdc1fb28ec1814780e6ecc169ec6d24f9954e71954eedbc4c70e

4b03288e9e44d214426a02327223b5e516b1ea29ce72fa25a2fcef9aa65c4b0b

9eb6c779dbad1b717caa462d8e040852759436ed79cc2172692339bc62432387

37e29b0ea7a9b97597385a12f525e13c3a7d02ba4161a6946f2a7d978cc045b4

776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d

8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1

0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b

2ffbe27983bc5c6178b2d447d8121cefaa5ffa87fe7b9e4f68272ce54787492f

1e741ec9452aab85a2f7d8682ef4e553cd74892e629012d903b521b21e3a15bf

90efcaeac13ef87620bcaaf2260a12895675c74d0820000b3cd152057125d802

eaf879370387a99e6339377a6149e289655236acc8de88324462dcd0f22383ff

081e72d96b750a38ef45e74d0176beb982905af4df6b8654ea81768be2f84497

24b3931e7d0f65f60bbb49e639b2a4c77de83648ff08e097ff0fa6a53f5c7102

4497af1407d33faa7b41de0c4d0741df439d2e44df1437d8e583737a07ec04a1

579b2e6290c1f7340795e42d57ba300f96aef035886e80f80cd5d0bb4626b5fc

eeb3981771e448b7b9536ba5d7cd70330402328a884443a899696a661e4e64e5

952f46c5618bf53305d22e0eae4be1be79329a78ad7ec34232f2708209b2517c

e70a8e8b0cd3c59cca8a886caa8b60efb652058f50cc9ff73a90bc55c0dc0866

5be57b589e5601683218bb89787463ca47ce3b283d8751820d30eee5e231678c

fe46a19803108381d2e8b5653cc5dce1581a234f91c555bbfff63b289b81a3dc

ae1353e8efe25b277f52decfab2d656541ffdf7fd10466d3a734658f1bc1187a

2ef0e5c66f6d46ddef62015ea786b2e2f5a96d94ab9350dd1073d746b6922859
181408e6ce1a215577c1daa195e0e7dea1fe9b785f9908b4d8e923a2a831fce8
2aa7bc9961b0478c552daa91976227cfa60c3d4bd8f051e3ca7415ceaeb604ca
375ededc5c20af22bdc381115d6a8ce2f80db88a5a92ebaa43c723a3d27fb0d6
0424167da27214cf2be0b04c8855b4cdb969f67998c6b8e719dd45b377e70353
7e5dca90985a9fac8f115eaacd8e198d1b06367e929597a3decd452aaa99864b
8de0f244d507b25370394ba158bd4c03a7f24c6627e42d9418fb992a06eb29d8
7ee215469a7886486a62fea8fa62d3907f59cf9bf5486a5fe3a0da96dabea3f9
ff70462cb3fc6ddd061fbd775bbc824569f1c09425877174d43f08be360b2b58
f5d06c52fe4ddca0ebc35fddbbc1f3a406bdaa5527ca831153b74f51c9f9d1b0
bc51836048158373e2b2f3cdb98dc3028290e8180a4e460129fef0d96133ea2e
d9a60a47e142ddd61f6c3324f302b35feeca684a71c09657ddb4901a715bd4c5
95840bd9a508ce6889d29b61084ec00649c9a19d44a29aedc86e2c34f30c8baf
3bbdf7019ed35412ce4b10b7621faf42acf604f91e5ee8a903eb58bde15688ff
9b455619b4cbfeb6496c1246ba9ce0e4ffa6736fd536a0f99686c7e185eb2e22
bfd028f78b546eda12c0d5d13f70ab27dff32b04df3291fd46814f486ba13693
a15b871fcb31c032b0e0661a2d3dd39664fa2d7982ff0dbc0796f3e9893aed9a
d1bc07b962ccc6e3596aa238bb7eda13003ea3ca95be27e8244e485165642548
eec5cd045f26a7b5d158e8289838b82e4af7cf4fc4b9048eaf185b5186f760db
29ae3431908c99b0fff70300127f1db635af119ee55cd8854f6d3270b2e3032e
ca0bb6a819506801fa4805d07ee2ebaa5c29e6f5973148fe25ed6d75089c06a7
6d8877b17795bb0c69352da59ce8a6bfd7257da30bd0370eed8428fad54f3128
5cf43c433fa1e253e937224254a63dc7e5ad6c4b3ab7a66ec9db76a268b4deeb
a6e3831b07ab88f45df9ffac0c34c4452c76541c2acd215de8d0109a32968ace
f4f0117d2784a3b8dfef4b5cb7f2583dd4100c32f9ee020f16402508e073f0a1
7093cc81f32c8ce5e138a4af08de6515380f4f23ed470b89e6613bee361159e1
350eaa2310e81220c409f95e6e1e53beadec3cffa3f119f60d0daace35d95437
776cb9a7a9f5afbaffdd4dbd052c6420030b2c7c3058c1455e0a79df0e6f7a1d
d2de662480783072b82dd4d52ab6c57911a1e84806c229f614b26306d5981d98
c8a82876beed822226192ea3fe01e3bd1bb0838ab13b24c3a6926bce6d84411b
f30a0fe494a871bd7d117d41025e8d2e17cd545131e6f27d59b5e65e7ab50d92
8a20dc9538d639623878a3d3d18d88da8b635ea52e5e2d0c2cce4a8c5a703db1

0649fda8888d701eb2f91e6e0a05a2e2be714f564497c44a3813082ef8ff250b
2c2412e43f3fd24d766832f0944368d4632c6aa9f5a9610ab39d23e79756e240
218233cc5ef659df4f5fdabe028ab43bc66451b49a6bfa85a5ed436cfb8dbc32
cccbf9bff47b3fd391274d322076847a3254c95f95266ef06a3ca8be75549a4b
ab789a5a10b4c4cd7a0eb92bbfcf2cc50cb53066838a02cfb56a76417de379c5
4896f0e4bc104f49901c07bc84791c04ad1003d5d265ab7d99fd5f40ec0b327f
5e715754e9da9ed972050513b4566fb922cd87958ecf472d1d14cd76923ae59a
797e31c6c34448fbecda10385e9ccfa7239bb823ac8e33a4a7fd1671a89fe0f6
48bfcbc3162a0b00412cba5eff6c0376e1ae4cfbd6e35c9ea92d2ab961c90342
7a66d65fa69b857beeeaaef67ec835900eee09a350b6f51f51c83919c9223793
b0edf66d4f07e5f58b082f5b8479d48fbab3dbe70eba0d7e8254c8d3a5e852ef
840ba484395e15782f436a7b2e1eec2d4bf5847dfd5d4787ae64f3a5f668ed4f
80c20db74c54554d9936a627939c3c7ea44316e7670e2f7f5231c0db23bc2114
5dabbce674b797aaa42052b501fb42b20be74d9ffcb0995d933fbf786c438178
055bbe33c12a5cdaf50c089a29eaecba2ccf312dfe5e96183b810eb6b95d6c5a
c084c20c94dbbffed76d911629796744eff9f96d24529b0af1e78cda54cdbf02
5f6ee521311e166243d3e65d0253d12d1506750c80cd21f6a195be519b5d697f
fcb6ff6a679ca17d9b36a543b08c42c6d06014d11002c09ba7c38b405b50debe
a168d561665221f992f51829e0b282eeb213b8aca3a9735dbbaecc4d699f66b9
98112bd4710e6ffe389a2beb13ff1162017f62a1255c492f29238626e99509f3
afacb38ea3a3cafe0f8dbd26dee7de3d0b24cdecae280a9b884fbad5ed195de7
b431aebc2783e72be84af351e9536e8110000c53ebb5db25e89021dc1a83625e
2b39634dce9e7bb36e338764ef56fd37be6cd0faa07ee3673c6e842115e3ceb1
11533eedc1143a33c1deae105e1b2b2f295c8445e1879567115adebfdda569e2
36e3d47f33269bef3e6dd4d497e93ece85de77258768e2fa611137fa0de9a043
e6c5437e8a23d50d44ee47ad6e7ce67081e7926a034d2ac4c848f98102ddb2f8
1cb3b3e652275656b3ae824da5fb330cccd8b27892fb29adc96e5f6132b98517
ec88fe46732d9aa6ba53eed99e4d116b7444afd2a52db988ea82f883f6d30268
99944ad90c7b35fb6721e2e249b76b3e8412e7f35f6f95d7fd3a5969eaa99f3d
8505ece4360faf3f454e5b47239f28c48d61c719b521e4e728bc12d951ecf315
dd88273437031498b485c380968f282d09c9bd2373ef569952bc7496ebadadde
6e7bbf25ea4e83229f6fa6b2fa0f880dde1594a7bec2aac02ff7d2d19945d036

f989df3aeede247a29a1f85fc478155b9613d4a416428188eda1a21bd481713a
4af2f66d7704de6ff017253825801c95f76c28f51f49ee70746896df307cbc29
ba9fee47dcc7bad8a7473405aabf587e5c8d396d5dd5f6f8f90f0ff48cc6a9ce
5d94d2b5f856e5a1fc3a3315d3cd03940384103481584b80e9d95e29431f5f7a
33d6414dcf91b9a665d38faf4ae1f63b7aa4589fe04bdd75999a5e429a53364a
14984efdd5343c4d51df7c79fd6a2dfd791aa611a751cc5039eb95ba65a18a54
879be2fa5a50b7239b398d1809e2758c727e584784ba456d8b113fc98b6315a2
c0cfb87a8faed76a41f39a4b0a35ac6847ffc6ae2235af998ee1b575e055fac2
fc9594611445de4a0ba30daf60a7e4dec442b2e5d25685e92a875aca2c0112c9
81cbe57cd80b752386ee707b86f075ad9ab4b3a97f951d118835f0f96b3ae79d
4e022e4e4ee28ae475921c49763ee620b53bf11c2ad5fffe018ad09c3cb078cc
a3cf96b65f624c755b46a68e8f50532571cee74b3c6f7e34eecb514a1eb400cf
ff471a98342bafbab0d341e0db0b3b9569f806d0988a5de0d8560b6729875b3e
638957e2def5a8fda7e3efefff286e1a81280d520d5f8f23e037c5d74c62553c
4ffe074ad2365dfb13c1c9ce14a5e635b19acb34a636bae16faf9449fb4a0687
4c596877fa7bb7ca49fb78036b85f92b581d8f41c5bc1fa38476da9647987416
49a0e5951dbb1685aaa1a6d2acf362cbf735a786334ca131f6f78a4e4c018ed9
0dc1e3f36dc4835db978a3175a462aa96de30df3e5031c5d0d8308cdd60cbede
e74ae353b68a1d0f64b9c8306b2db46dfc760c1d91bfdf05483042d422bff572
00c9bbc56388e3fffc6e53ef846ad269e7e31d631fe6068ff4dc6c09fb40c48b
c2bcde93227eb1c150e555e4590156fe59929d3b8534a0e2c5f3b21ede02afa0
70c271f37dc8c3af22fdcad96d326fe3c71b911a82da31a992c05da1042ac06d
ffb0e244e0dabbaabf7fedd878923b9b30b487b3e60f4a2cf7c0d7509b6963ba
dbede977518143bcee6044ed86b8178c6fc9d454fa346c089523eedee637f3be
4d6cbde39a81f2c62d112118945b5eeb1d73479386c962ed3b03d775e0dccfa0
fa229cd78c343a7811cf8314febbc355bb9baab05b270e58a3e5d47b68a7fc7d
4beba775f0e0b757ff32ee86782bf42e997b11b90d5a30e5d65b45662363ece2
a41da0945ca5b5f56d5a868d64763b3a085b7017e3568e6d49834f11952cb927
f3d0759dfab3fbf8b6511a4d8b5fc087273a63cbb96517f0583c2cce3ff788b8
fa4b286eeaf7d74fe8f3fb36d80746e18d2a7f4c034ae6c3fa4c917646a9e147
be3ddd71a54ec947ba873e3e10f140f807e1ae362fd087d402eff67f6f955467
6449aaf6a8153a9ccbcef2e2738f1e81c0d06227f5cf4823a6d113568f305d2a

39dc1aded01daaf01890db56880f665d6cafab3dea0ac523a48aa6d6e6346fff
01d51b011937433568db646a5fa66e1d25f1321f444319a9fba78fd5efd49445
099a0b821f77cb4a6e6d4a641ed52ee8fea659ee23b657e6dae75bb8ca3418c3
4cbf9ecb6ca4f2efed86ba6ebf49436c65afe7ae523ec9dae58e432a9d9a89d0
66a98ad0256681313053c46375cb5c144c81bf4b206aaa57332eb5f1f7176b8c
97d00fc2bc5f5c9a56b498cf83b7a801e2c11c056772c5308ee7adea50556309
9e854d40f22675a0f1534f7c31626fd3b67d5799f8eea4bd2e2d4be187d9e1c7
a125b3e627ecd04d0dd8295e12405f2590144337481eb21086c4afb337c5b3f2
a7d154eaee39ff856792d86720a8d193da3d73bfe4ac8364da030d80539e9ac2
b2dd77af9dd9e8d7d4ebc778f00ff01c53b860a04c4e0b497f2ae74bb8a280c0

الوحدات المضافة في المرحلة الثالثة Stage3 Plugins

f8286e29faa67ec765ae0244862f6b7914fcdde10423f96595cb84ad5cc6b344
afd281639e26a717aead65b1886f98d6d6c258736016023b4e59de30b7348719
acf32f21ec3955d6116973b3f1a85f19f237880a80cdf584e29f08bd12666999
47f521bd6be19f823bfd3a72d851d6f3440a6c4cc3d940190bdc9b6dd53a83d6
d09f88baf33b901cc8a054d86879b81a81c19be45f8e05484376c213f0eedda2
2af043730b632d237964dd6abd24a7f6db9dc83aab583532a1238b4d4188396b
4bfc43761e2ddb65fedab520c6a17cc47c0a06eda33d11664f892fcf08995875
cd8cf5e6a40c4e87f6ee40b9732b661a228d87d468a458f6de231dd5e8de3429
bad8a5269e38a2335be0a03857e65ff91620a4d1e5211205d2503ef70017b69c
ff118edb9312c85b0b7ff4af1fc48eb1d8c7c8da3c0e1205c398d2fe4a795f4b
6807497869d9b4101c335b1688782ab545b0f4526c1e7dd5782c9deb52ee3df4
3df17f01c4850b96b00e90c880fdfabbd11c64a8707d24488485dd12fae8ec85
1367060db50187eca00ad1eb0f4656d3734d1ccea5d2d62f31f21d4f895e0a69
94eefb8cf1388e431de95cab6402caa788846b523d493cf8c3a1aa025d6b4809
78fee8982625d125f17cf802d9b597605d02e5ea431e903f7537964883cf5714
3bd34426641b149c40263e94dca5610a9ecfcbce69bfdd145dff1b5008402314

قائمة الأجهزة المستهدَفة

ASUS DEVICES:
RT-AC66U
RT-N10
RT-N10E
RT-N10U
RT-N56U
RT-N66U

D-LINK DEVICES:
DES-1210-08P
DIR-300
DIR-300A
DSR-250N
DSR-500N
DSR-1000
DSR-1000N

HUAWEI DEVICES:
HG8245

LINKSYS DEVICES:
E1200
E2500
E3000
E3200
E4200
RV082
WRVS4400N

MIKROTIK DEVICES:
CCR1009
CCR1016
CCR1036
CCR1072
CRS109
CRS112
CRS125
RB411
RB450
RB750
RB911

RB921
RB941
RB951
RB952
RB960
RB962
RB1100
RB1200
RB2011
RB3011
RB Groove
RB Omnitik
STX5

NETGEAR DEVICES:
DG834
DGN1000
DGN2200
DGN3500
FVS318N
MBRN3000
R6400
R7000
R8000
WNR1000
WNR2000
WNR2200
WNR4000
WNDR3700
WNDR4000
WNDR4300
WNDR4300-TN
UTM50

QNAP DEVICES:
TS251
TS439 Pro
Other QNAP NAS devices running QTS software

TP-LINK DEVICES:
R600VPN
TL-WR741ND
TL-WR841N

UBIQUITI DEVICES:
NSM2
PBE M5

UPVEL DEVICES:
Unknown Models

ZTE DEVICES:
ZXHN H108N

الحماية Defending Against This Threat

تعتبر الحماية ضد البرنامج الخبيث VPNFilter صعبة نسبياً ومعقدة إلى حد ما، ويعود ذلك إلى طبيعة الأجهزة المستهدَفة، حيث إن المهمة الرئيسية لهذه الأجهزة هي الاتصال المباشر مع شبكة الانترنت ويتم ذلك عادةً بدون تجهيزات أو برمجيات حماية Security Devices, Services أي أن هذه الأجهزة موجودة وجهاً لوجه مع مطوري ومشغلي البرنامج VPNFilter، بالإضافة إلى وجود العديد من الثغرات في معظم هذه الأجهزة إن كان لجهة أنظمة التشغيل OS Vulnerabilities أو لجهة الإعدادات Misconfigurations والتي أي هذه الثغرات يتطلب إغلاقها إجراءات وعمليات ترقيع معينة وخبرة ومعرفة قد لا تتوفر لدى عامة مستخدمي هذه الأجهزة، علماً بأن معظم هذه الأجهزة لا تمتلك إمكانيات مدمجة للحماية والتعامل مع البرمجيات الخبيثة.

الأسباب الثلاثة السابقة مجتمعةً تجعل من الصعب كما ذكرنا بدايةً الدفاع ضد والتعامل مع هذا البرنامج الخبيث. وكخطوة تهدف لحماية الأجهزة بشكل استباقي قامت العديد من الشركات بتطوير عدد من القواعد الخاصة بنظام كشف التطفل الشهير Snort IDS Rules، حيث تحوي هذه القواعد معرفات رقمية خاصة Signatures وذلك من أجل الثغرات المعروفة والأكثر انتشاراً المرتبطة بالبرنامج VPNFilter، يمكن لأي مستخدم تحميل هذه القواعد مع المعرفات الرقمية من مصادر تحميل وتحديث Snort، بالإضافة إلى إعداد قائمة Blacklist تحوي أسماء المجالات Domains والعناوين الرقمية IP Addresses الخاصة بأنظمة القيادة والتحكم Command and Control ومخدمات التحميل Download Servers العائدة للبرنامج، بالإضافة إلى نشر العديد من التنبيهات والتحذيرات ونشرها في أشهر المواقع التي تعمل في مجال أمن المعلومات.

بعض التوصيات العامة:

- على مستخدمي الأجهزة المستهدفة من قبل برنامج VPNFilter إعادة ضبط أجهزتهم وإعادة تشغيلها بطريقة Factory Default Reset Reboot وذلك للتأكد من إزالة البرنامج الخبيث مع كافة مكوناته في حال وجوده.
- على مزودي خدمات الانترنت الحرص على إجراء المرحلة السابقة على جميع أنواع الأجهزة المستهدفة، وذلك قبل تسويقها وتركيبها لدى مشتركيهم.

- يجب تحديث أنظمة التشغيل لآخر الإصدارات والتحديثات المتوفرة بالإضافة إلى تطبيق الترقيات الأمنية المتوفرة، مع الحرص على أن يتم ذلك من مصادر وروابط الشركات المطورة لهذه الأجهزة حصراً.
- يجب على مزودي خدمة الانترنت إن أمكن مراقبة تجهيزات مشتركيهم والتأكد من خلوها من البرنامج.
- يستطيع أي مستخدم اجراء عملية اختبار لأي جهاز من الأجهزة المستهدفة بواسطة أدوات مجانية خاصة تقوم بعمليات المسح والبحث والتقصي عن وجود البرنامج الخبيث في هذه الأجهزة، ويتم ذلك بعد تحميل هذه الأدوات من مصادر موثوقة في شبكة الانترنت.

مصادر البحث

دراسات وأبحاث شركة CISCO والمؤسسات البحثية التابعة لها.

==========