WEDNESDAY, JUNE 6, 2018

VPNFilter Update - VPNFilter exploits endpoints, targets new devices

INTRODUCTION

Cisco Talos, while working with our various intelligence partners, has discovered additional details regarding "VPNFilter." In the days since we first published our findings on the campaign, we have

Search Blog

SUBSCRIBE TO OUR FEED

Posts

Comments

Subscribe via Email

BLOG ARCHIVE

▼ 2018 (81)

▼ JUNE (3)

VPNFilter Update - VPNFilter exploits endpoints, t...

Talos Threat Research Summit Guide and Cisco Live ...

Vulnerability Spotlight: TALOS-2018-0535 - Oculari...

► MAY (15)

► APRIL (21)

► MARCH (10)

► FEBRUARY (14)

seen that VPNFilter is targeting more makes/models of devices than initially thought, and has additional capabilities, including the ability to deliver exploits to endpoints. Talos recently published a blog about a broad campaign that delivered VPNFilter to small home-office network devices, as well as network-attached storage devices. As we stated in that post, our research into this threat was, and is, ongoing. In the wake of that post, we have had a number of partners step forward with additional information that has assisted us in our work. This post is an update of our findings over the past week.

First, we have determined that additional devices are being targeted by this actor, including some from vendors that are new to the target list. These new vendors are ASUS, D-Link, Huawei, Ubiquiti, UPVEL, and ZTE. New devices were also discovered from Linksys, MikroTik, Netgear, and TP-Link. Our research currently shows that no Cisco network devices are affected. We've provided an updated device list below.

We have also discovered a new stage 3 module that injects malicious content into web traffic as it passes through a network device. At the time of our initial posting, we did not have all of the information regarding the suspected stage 3 modules. The new module allows the actor to deliver exploits to endpoints via a man-in-the-middle capability (e.g. they can intercept network traffic and inject malicious code into it without the user's knowledge). With this new finding, we can confirm that the threat goes beyond what the actor could do on the network device itself, and extends the threat into the networks that a compromised network device supports. We provide technical details on this module, named "ssler" below.

Additionally, we've discovered an additional stage 3 module that provides any stage 2 module that lacks the kill command the capability to disable the device. When executed, this module specifically removes traces of the VPNFilter malware from the device and then renders the device unusable. Analysis of this module, called "dstr," is also provided below.

Finally, we've conducted further research into the stage 3 packet sniffer, including in-depth analysis of how it looks for Modbus traffic.

Technical details

► JANUARY (18)

► 2017 (172)
► 2016 (98)
► 2015 (62)
► 2014 (67)
► 2013 (30)
► 2012 (53)
► 2011 (23)
► 2010 (93)
► 2009 (146)
► 2008 (37)

'ssler' (Endpoint exploitation module — JavaScript injection)

The ssler module, which we pronounce as "Esler," provides data exfiltration and JavaScript injection capabilities by intercepting all traffic passing through the device destined for port 80. This module is expected to be executed with a parameter list, which determines the module's behavior and which websites should be targeted. The first positional parameter controls the folder on the device where stolen data should be stored. The purpose of the other named parameters are as follows:

- dst: — Used by the iptables rules created to specify a destination IP address or CIDR range that the rule should apply to.
- src: — Used by the iptables rules created to specify a source IP address or CIDR range that the rule should apply to.
- dump: — Any domain passed in a dump parameter will have all of its HTTP headers recorded in the reps_*.bin file.
- site: — When a domain is provided in the "site" parameter, this domain will have its web pages targeted for JavaScript injection.
- hook: — This parameter determines the URL of the JavaScript file for injection.

The first action taken by the ssler module is to configure the device's iptables to redirect all traffic destined for port 80 to its local service listening on port 8888. It starts by using the insmod command to insert three iptables modules into the kernel (ip_tables.ko, iptable_filter.ko, iptable_nat.ko) and then executes the following shell commands:

- 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

Note: To ensure that these rules do not get removed, ssler deletes them and then adds them back approximately every four minutes.

Any outgoing web requests on port 80 are now intercepted by ssler and can be inspected and manipulated before being sent to the legitimate HTTP service. All HTTP requests are sslstripped. That is, the following changes are made to requests before being sent to the true HTTP server:

- Any instances of the string https:// are replaced with http://, converting requests for secure HTTP resources to requests for insecure ones so sensitive data such as credentials can be extracted from them.
- If the request contains the header Connection: keep-alive, it is replaced with Connection: close
- If the request contains the header Accept-Encoding with the gzip value, this is converted to Accept-Encoding: plaintext/none so no responses will be compressed with gzip (exceptions are made for certain file types, such as images).

If the host is in one of the dump: parameters, the details of the request are saved to the disk for exfiltration, including the URL, port and all of the request headers. If the host is not in a dump: parameter, it will only dump requests with an Authorization header or URLs that have credentials in them. URLs are determined to have credentials if they contain either the string assword= or ass= and one of the following strings in them:

- sername=
- ser=
- ame=
- ogin=
- ail=
- hone=
- session%5Busername
- session%5Bpassword

- session[password

Any POST requests to accounts.google.com containing the string signin will also be dumped.

After these modifications are made, a connection to the true HTTP server is made by ssler using the modified request data over port 80. Ssler receives the response from the HTTP server and makes the following changes to the response before passing it on to the victim:

- A response with an https:// in its Location header value is converted to http://
- The following headers are ignored, i.e. not sent to the client:
    - Alt-Scv
    - Vary
    - Content-MD5
    - content-security-policy
    - X-FB-Debug
    - public-key-pins-report-only
    - Access-Control-Allow-Origin
- The entire response is sslstripped — that is, all instances of https:// with \x20http://.
- If parameter site: is provided a domain (or part of a domain, e.g. "google"), it will attempt to inject JavaScript into all Content-Type: text/html or Content-Type: text/javascript responses. The requirement is that the string <meta name= … > be present and long enough to fit the string from the hook: parameter. The <meta name= … > tag will be replaced with <script type="text/javascript" src="[hook value]">. The victim IP combined with the site is then added to an internal whitelist in ssler and will not be targeted for injection again until the whitelist is cleared (which occurs every four days).

Each domain that is sslstripped in the responses (e.g. domains found in links) is then added to a list of stripped domains. Subsequent requests that are intercepted by the ssler module to domains in this list will occur via HTTPS over port 443, instead of HTTP over port 80. By default, four domains are on this list, so ssler will always connect to these domains via HTTPS over port 443: www.google.com, twitter.com, www.facebook.com, or www.youtube.com.

'dstr' (device destruction module)

The dstr modules are used to render an infected device inoperable by deleting files necessary for normal operation. It deletes all files and folders related to its own operation first before deleting the rest of the files on the system, possibly in an attempt to hide its presence during a forensic analysis.

The x86 version of the dstr module was analyzed in-depth. This module first deleted itself from the disk and then stops the execution of the parent Stage 2 process. It will then search all running process for ones named vpnfilter, security, and tor and terminate them. Next, it explicitly deletes the following files and directories:

- /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/

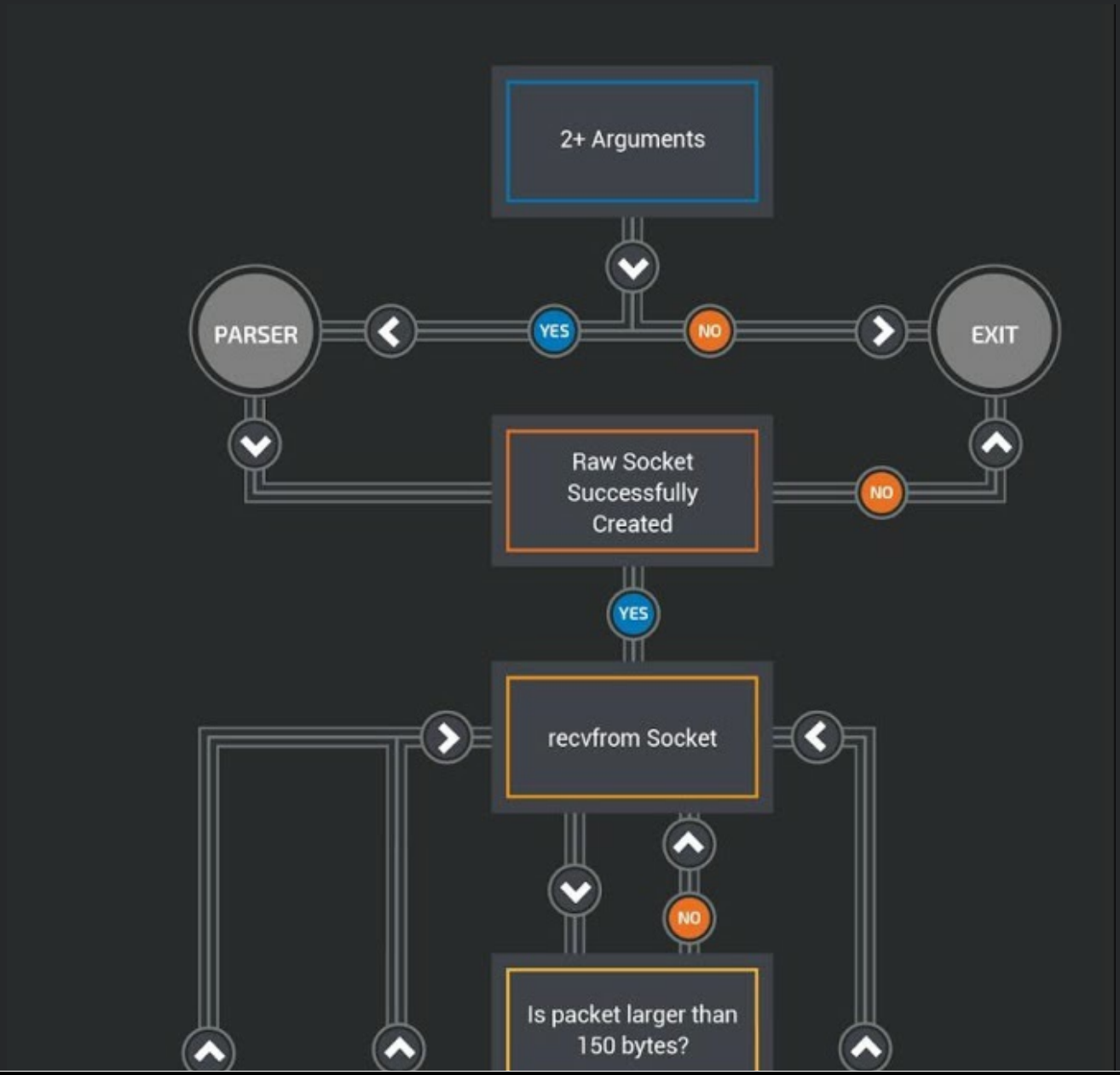
The dstr module clears flash memory by overwriting the bytes of all available /dev/mtdX devices with a 0xFF byte. Finally, the shell command rm -rf /* is executed to delete the remainder of the file system and the device is rebooted. At this point, the device will not have any of the files it needs to operate and fail to boot.

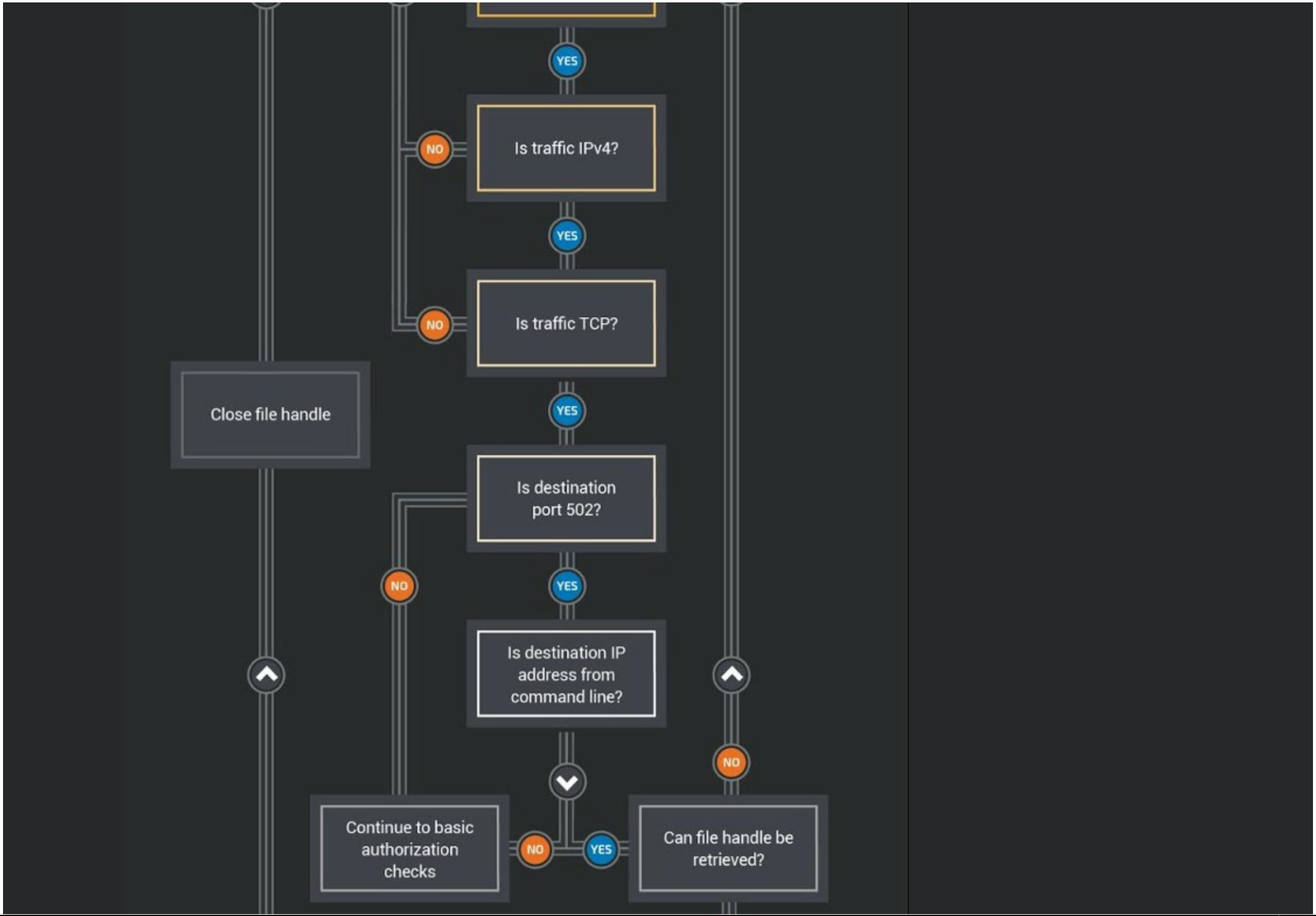
Additional research on the third stage packet sniffer

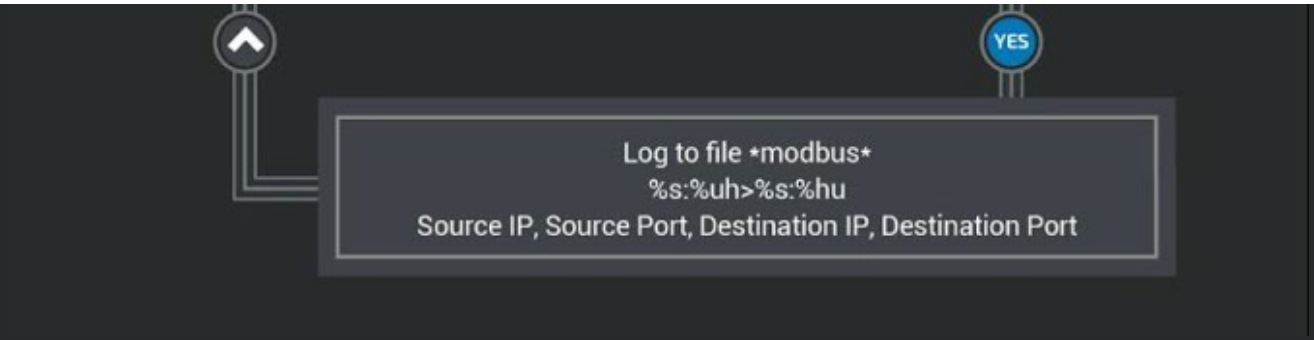
'ps' (stage 3 packet sniffer)

One of stage 3 packet sniffer module samples we have is the R600VPN MIPS-like (Lexra architecture) sample. This sample is a packet sniffer that is looking for basic authentication as well as monitoring ICS traffic, and is specific to the TP-LINK R600-VPN. The malware uses a raw socket to look for connections to a pre-specified IP address, only looking at TCP packets that are 150 bytes or larger (note: This is the full packet size, with headers. Depending on the size of the TCP header,

or larger. (Note: This is the full packet size, with headers. Depending on the size of the TCP header, the PDU could be approximately 56 to 96 bytes and still meet the criteria to get logged). It has the ability to view, but not modify, the network traffic. Very significant changes would be required to implement functionality that could modify traffic.







Packets that are not on port 502, are scanned for BasicAuth, and that information is logged.

- Else: (non-Modbus traffic): sniffing HTTP basic auth credentials
  - 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=

- Logging: Logs on IPs and ports, but not the packet contents on port 502. It does not validate the traffic as Modbus.
    - Modbus - Logs SourceIP, SourcePort, DestinationIP, DestinationPort and labels it *modbus*
    - All Other - write full packet to log file if and only if it passes basic auth check

Conclusion

These new discoveries have shown us that the threat from VPNFilter continues to grow. In addition to the broader threat surface found with additional targeted devices and vendors, the discovery of the malware's capability to support the exploitation of endpoint devices expands the scope of this threat beyond the devices themselves, and into the networks those devices support. If successful, the actor would be able to deploy any desired additional capability into the environment to support their goals, including rootkits, exfiltration capability and destructive malware.

Talos would like to thank all of the individual researchers, companies and intelligence partners from around the world who have stepped forward to share information and address this threat. Your actions have helped us gain a greater understanding of this campaign, and in some cases, have directly improved the situation. We recognize this is a team sport, and truly appreciate your assistance.

We will continue to monitor VPNFilter and work with our partners to understand the threat as it continues to evolve in order to ensure that our customers remain protected and the public is informed.

Updated List of IOCs

As stated previously, we highly suspect that there are additional IOCs and versions of this malware that we are not currently aware of. The following list of IOCs comprises what we know as of this date. News IOCs are in BOLD below.

Known C2 Domains and IPs

ASSOCIATED WITH THE 1ST STAGE

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

ASSOCIATED WITH THE 2ND STAGE

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
94.185.80[.]82
62.210.180[.]229
91.200.13[.]76
23.111.177[.]114

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

Known File Hashes

1ST STAGE MALWARE

50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec
0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92
b9770ec366271dacdae8f5088218f65a6c0dd82553dd93f41ede586353986124
51e92ba8dac0f93fc755cb98979d066234260eafc7654088c5be320f431a34fa
6a76e3e98775b1d86b037b5ee291ccfcffb5a98f66319175f4b54b6c36d2f2bf
313d29f490619e796057d50ba8f1d4b0b73d4d4c6391cf35baaaace71ea9ac37

2ND STAGE 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
5d94d2b5f856e5a1fc3a3315d3cd039403841034815 84b80e9d95e29431f5f7a
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

3RD STAGE PLUGINS

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

78fee8982625d125f17cf802d9b597605d02e5ea431e903f7537964883cf5714
3bd34426641b149c40263e94dca5610a9ecfcbce69bfdd145dff1b5008402314

SELF-SIGNED CERTIFICATE FINGERPRINTS

d113ce61ab1e4bfcb32fb3c53bd3cdeee81108d02d3886f6e2286e0b6a006747
c52b3901a26df1680acbfb9e6184b321f0b22dd6c4bb107e5e071553d375c851
f372ebe8277b78d50c5600d0e2af3fe29b1e04b5435a7149f04edd165743c16d
be4715b029cbd3f8e2f37bc525005b2cb9cad977117a26fac94339a721e3f2a5
27af4b890db1a611d0054d5d4a7d9a36c9f52dffeb67a053be9ea03a495a9302
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
fb47ba27dceea486aab7a0f8ec5674332ca1f6af962a1724df89d658d470348f
b25336c2dd388459dec37fa8d0467cf2ac3c81a272176128338a2c1d7c083c78
cd75d3a70e3218688bdd23a0f618add964603736f7c899265b1d8386b9902526
110da84f31e7868ad741bcb0d9f7771a0bb39c44785055e6da0ecc393598adc8
909cf80d3ef4c52abc95d286df8d218462739889b6be4762a1d2fac1adb2ec2b
044bfa11ea91b5559f7502c3a504b19ee3c555e95907a98508825b4aa56294e4
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412
8f1d0cd5dd6585c3d5d478e18a85e7109c8a88489c46987621e01d21fab5095d
d5dec646c957305d91303a1d7931b30e7fb2f38d54a1102e14fd7a4b9f6e0806
c0f8bde03df3dec6e43b327378777ebc35d9ea8cfe39628f79f20b1c40c1b412

Known Affected Devices

The following devices are known to be affected by this threat. Based on the scale of this research, much of our observations are remote and not on the device, so it is difficult to determine specific version numbers and models in many cases.

Given our observations with this threat, we assess that this list may still be incomplete and other devices may be affected.

ASUS DEVICES:

RT-AC66U (new)
RT-N10 (new)
RT-N10E (new)
RT-N10U (new)
RT-N56U (new)
RT-N66U (new)

D-LINK DEVICES:

DES-1210-08P (new)
DIR-300 (new)
DIR-300A (new)
DSR-250N (new)
DSR-500N (new)
DSR-1000 (new)
DSR-1000N (new)

HUAWEI DEVICES:

HG8245 (new)

LINKSYS DEVICES:

E1200
E2500
E3000 (new)
E3200 (new)
E4200 (new)
RV082 (new)
WRVS4400N

MIKROTIK DEVICES:

CCR1009 (new)

CCR1016
CCR1036
CCR1072
CRS109 (new)
CRS112 (new)
CRS125 (new)
RB411 (new)
RB450 (new)
RB750 (new)
RB911 (new)
RB921 (new)
RB941 (new)
RB951 (new)
RB952 (new)
RB960 (new)
RB962 (new)
RB1100 (new)
RB1200 (new)
RB2011 (new)
RB3011 (new)
RB Groove (new)
RB Omnitik (new)
STX5 (new)

NETGEAR DEVICES:
DG834 (new)
DGN1000 (new)
DGN2200
DGN3500 (new)
FVS318N (new)

MBRN3000 (new)
R6400
R7000
R8000
WNR1000
WNR2000
WNR2200 (new)
WNR4000 (new)
WNDR3700 (new)
WNDR4000 (new)
WNDR4300 (new)
WNDR4300-TN (new)
UTM50 (new)

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

TP-LINK DEVICES:
R600VPN
TL-WR741ND (new)
TL-WR841N (new)

UBIQUITI DEVICES:
NSM2 (new)
PBE M5 (new)

UPVEL DEVICES:
Unknown Models* (new)

ZTE DEVICES:

ZXHN H108N (new)

* Malware targeting Upvel as a vendor has been discovered, but we are unable to determine which specific device it is targeting.

POSTED BY WILLIAM LARGENT AT 9:02 AM
LABELS: AMP, CLAMAV, IOT, IOT MALWARE, NEW ROUTER MALWARE, OFFICE ROUTER ATTACK, SNORT RULES, TALOS, THREAT INTELLIGENCE, THREAT RESEARCH, VPN FILTER ATTACK, VPNFILTER, VPNFILTER MALWARE, VULNERABLE ROUTERS

SHARE THIS POST

NO COMMENTS:

POST A COMMENT