Global vision.
Local knowledge.

Cisco Connect City
Country • Day Month Year
VPNFilter

- A multi-stage, modular framework
- Infected at least 500,000 in at least 54 countries
- New functions include data filtering and multiple encrypted tunneling capabilities
- Protocol used by MikroTik networking devices > exploitation methods used by the actor
VPNFilter Code and Victims

- Malware overlaps with versions of the BlackEnergy malware, targeted devices in Ukraine
  - theft of website credentials and monitoring of Modbus SCADA protocols
  - destructive capability that can render an infected device unusable
  - most devices targeted, particularly in older versions, have known public exploits or default credentials

- Victims:
  - ASUS, D-Link, Huawei, Ubiquiti, UPVEL, ZTE, Linksys, MikroTik, Netgear, and TP-Link
  - QNAP network-attached storage (NAS) devices
  - no Cisco network devices
3 Stages

**Stage 1**
- Photobucket or toknowall EXIF metadata used to call out IP
- Backup 1
- Backup 2
- Pulls down photo
- TOKNOWALL.COM: If Photobucket fails, it calls out to toknowall to download a picture

**Stage 2**
- STAGE 2 SERVER
- STAGE 3 SERVER
- Manually pushes Stage 2
- Stage 3 Plugin
- TOR Plugins
- Instructions (if exists)
- If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection

**Stage 3**
- EXPLOITATION

**Command & Control**
VPNFilter Capabilities

- Multiple ways for the threat actor to obfuscate and/or encrypt malicious traffic, including communications used for C2 and data exfiltration.
- Multiple tools that could be utilized to identify additional victims accessible from the actor's foothold on devices compromised by VPNFilter for both lateral movement within a network.
- The capacity to build a distributed network of proxies that could be leveraged in future unrelated attacks to provide a means of obfuscating
VPNFilter Modules

- 'ssler' (Endpoint exploitation module – JavaScript injection)

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Module Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘htpx’</td>
<td>Redirects and inspects the contents of HTTP traffic transmitted through devices.</td>
</tr>
<tr>
<td>‘ndbr’</td>
<td>Multifunctional SSH utility.</td>
</tr>
<tr>
<td>‘nm’</td>
<td>Allows network mapping activities to be conducted from compromised devices.</td>
</tr>
<tr>
<td>‘netfilter’</td>
<td>Denial of service utility.</td>
</tr>
<tr>
<td>‘portforwarding’</td>
<td>Allows the forwarding of network traffic to attacker specified infrastructure.</td>
</tr>
<tr>
<td>‘socks5proxy’</td>
<td>Enables establishment of a SOCKS5 proxy on compromised devices.</td>
</tr>
<tr>
<td>‘tcpvppn’</td>
<td>Enables establishment of a Reverse-TCP VPN on compromised devices.</td>
</tr>
</tbody>
</table>
Cisco Umbrella, Cloud Web Security, and Web Security Appliance can block internet communications of affected devices to known malicious destinations.

Cisco Stealthwatch Enterprise and Stealthwatch Cloud can detect affected devices communicating on the network to known malicious destinations on the internet.

Cisco NGFW and NGIPS can block the communication of affected devices on the network to known malicious destinations on the internet.

AMP and Threat Grid detect known IoCs and file hashes to block Stages 1–3 malware and plug-ins.
Please, complete the survey