One year later: The VPNFilter catastrophe that wasn't

By Martin Lee

Published: 2019-05-23 · Archived: 2026-04-05 17:56:32 UTC

Thursday, May 23, 2019 16:24

Cisco Talos first disclosed the existence of VPNFilter on May 23, 2018. The malware made headlines across the globe, as it was a sophisticated piece of malware developed by a nation state, infecting half a million devices, and poised to cause havoc. Yet the attack was averted. The attacker's command and control (C2) infrastructure was seized by the FBI, preventing the attacker from broadcasting orders to compromised devices. The attacker lost control of the infected systems, and potential catastrophe was prevented.

This was a wakeup call that alerted the cybersecurity community to a new kind of state-sponsored threat — a vast network of compromised devices across the globe that could stow away secrets, hide the origins of attacks and shut down networks.

This is the story of VPNFilter, and the catastrophe that was averted.

Network as the target

Network infrastructure is a tempting and useful target to attackers. Like any computing system, network devices such as routers and switches may contain vulnerabilities or misconfigurations that allow attackers to compromise the device. Once compromised, the device can be used as a point of incursion to search out and attack additional further systems, or the functionality of the device can be changed to the attacker's will, and network traffic intercepted, modified or rerouted. Unlike many other computing systems, routers and switches are unlikely to be running

anti-virus software, or be under active supervision by eagle-eyed administrators who may notice unusual activity.

In the weeks prior to the disclosure of VPNFilter, it was clear that network infrastructure was increasingly the target of state-sponsored threat actors. The activities of a threat actor associated with Russia had been observed and government agencies across the world published advisories warning organisations to take note[1,2,3].

Traces of VPNFilter

Someone registered the unobtrusive domain toknowall.com in December 2015. On May 4 2017 that domain was changed to point to an IP address hosted in France after it initially pointed at a Bulgarian hosting provider. Although nobody knew it at the time, this was one of the means by which the attackers were communicating with VPNFilter. This domain would remain active until the threat was neutralised on May 23, 2018.

By the end of August 2017, the FBI had been made aware of a home router exhibiting unusual behaviour. The device attempted to connect to a Photobucket account to download an image, behaviour that was clearly being driven by a malware infection[4].

In fact, both the Photobucket accounts and the toknowall.com domain were hosting images in which the IP address of the C2 server, used by the threat actor to issue instructions to the malware were hidden, disguised within the EXIF metadata of the image.

By March 2018, additional malware samples were discovered that also reached out to Photobucket, and used toknowall.com as a backup in case Photobucket was unavailable. Analysing the malware samples showed that the threat actor let an important clue slip.

To keep important data within the malware confidential, the malicious code used encryption, implementing the RC4 encryption algorithm. However, the code implementing this algorithm included a subtle error, a mistake that was identical to exhibited by code used in the BlackEnergy attacks against Ukraine and elsewhere[5]. This code reuse from one attack to another allowed government agencies to identify that this attack originated from the group known as APT28 or “Sofacy.”[6]

BlackEnergy and APT28

Each threat actor group has their own mode of operation, preferences, and characteristics that they display as part of their attacks. For example, Group 123 is known to conduct attacks by distributing documents that reference politics on the Korean peninsula[7]. In contrast, the threat actor Rocke seeks to install cryptocurrency mining software on compromised devices by downloading code from Git repositories[8]. Threat actors frequently reuse code or infrastructure, which allows researchers to identify specific threat actor groups and track their campaigns[9].

APT28, also known as Sofacy or Grizzly Steppe, is one of many threat actors that are followed by analysts. There is little doubt that this threat actor is part of the Russian Intelligence Services, that it is particularly active, and that

it can cause chaos[10,11].

The BlackEnergy attack was one of the most notorious attacks from this group. BlackEnergy disrupted electrical power distributions in Ukraine in December 2015, which caused widespread power outages across the country[7]. A particular characteristic of this attack was a component that wiped disks, rendering infected devices inoperable and destroying forensic evidence which could have been used to understand exactly how the attack was conducted[12].

This intent to destroy systems and prevent recovery was one of the factors that made is so important to respond to VPNFilter swiftly.

Capability and intent

VPNFilter managed to exploit various network devices and affected over 500 000 devices in at least 54 countries. The modular architecture of the malware allowed the threat actor to install various different modules to conduct different malicious activities from the infected devices.

At its simplest, the malware contained the ability to 'brick' or render permanently inoperable the infected devices. Alternatively, the malware could be used as a point of ingress on a network, and subsequently used to discover and attack other systems connected to the affected device. One particular module contained functionality to identify and monitor Modbus network traffic, a protocol widely used in Industrial Control Systems.

A further module allowed the malware to create a giant Tor network comprising the many compromised systems. This network potentially allowed attackers to disguise the ultimate destination of data stolen from other compromised systems, or the country of origin of attacks against systems.

Clearly, capturing data, especially usernames and passwords, was one goal of the attack. The malware was capable of downgrading encrypted https connections to an unencrypted http connection, then saving that traffic for future collection. Similarly, anything that looked like a user credential or authorisation token could be identified, recorded, and subsequently collected.

Since the malware infected routers that direct network traffic to its intended destination, the malware could modify the routing information and create custom destinations for certain traffic; redirecting traffic from the genuine destination to a separate system under the control of the attackers. All of this is achieved without alerting the end user that anything was amiss.

The response

The number of affected systems grew throughout the spring of 2018. However, sharp spikes in the numbers of new infections were observed on May 8 and 17. This sudden growth was almost exclusively within Ukraine which pointed to imminent preparation of an attack.

At this point, Talos worked with partner organisations in the private and public sector to neutralise the threat. The FBI led efforts to seize the C2 infrastructure[6], and in parallel, Talos informed members of the industry coalition group, the Cyber Threat Alliance, to ensure that the whole cyber security industry could act together to neutralise the threat [13].

The response was closely coordinated. Law enforcement took down the C2 infrastructure, cutting the ability of the attacker to send commands to the infected systems. The cyber security industry updated security products to detect and block VPNFilter, and issued advice to users on how to protect themselves.

We will never know the exact nature of the attack that was averted. The timing of the growth of infections suggested that Ukranian Constitution Day on June 29, the anniversary of NotPetya on June 27, or Orthodox Pentecost Monday on May 28 may have been target dates. The Security Service of Ukraine suggested that the attack would have been timed to disrupt the UEFA Champions League Final, which was taking place in Kiev on May 26[14].

Protection

VPNFilter partly resided in memory, and partly on the storage media of the devices it infected. Rebooting the device would clear the memory resident part of the malware, but not stop the malware component residing in the device storage from initiating contact with the command and control systems. However, once that C2 was disabled, the persistent part of the malware could no longer receive instructions.

The remnants of the malware can be cleared by resetting devices to factory settings, followed by patching to the latest version to remove vulnerabilities. Although it is still unclear which vulnerabilities were exploited to install VPNFilter, all the types of devices that were compromised had known existing vulnerabilities.

Given their position in the network topology, perimeter network devices are always going to be exposed to attack. Unpatched devices with known vulnerabilities that are exposed to the internet are ripe for compromise by threat actors such as APT28.

Keeping such devices fully patched and correctly configured are vital parts of network hygiene. However, if this can’t be assured, then devices need to be placed behind next generation firewalls to detect and block the attacks before they impact on the vulnerable device.

Vigilance is also part of good network hygiene. VPNFilter was first detected by identifying the unusual network behaviour of an infected device. The network is ideally placed to be the sensor that detects and informs us of the actions of the bad guys.

Conclusion & Aftermath

Together, Talos and the FBI worked to identify and characterise VPNFilter. The malware’s multi-stage modular platform supported both intelligence-collection and destructive cyber attack operations. The campaign managed to infect over 500 000 devices in at least 54 countries. This malware could have been used to conduct a large-scale destructive attack, which would have rendered infected physical devices unusable and cut off internet access for hundreds of thousands of users. However, identification and characterisation of the threat, coupled with a coordinated response across the public and private sectors, stopped the attack before a catastrophe occurred.

The degree of collaboration across different organisations was unprecedented. There is always a balance to tread between keeping information private in order to maintain operational security, and sharing between partners to act together, maximising the impact against the threat actor to reduce the severity of an attack. There is evidence to suggest that Talos' early engagement of the Cyber Threat Alliance in the case of VPNFilter has had a lasting legacy, helping to encourage others to engage in earlier, and more frequent sharing of data[13].

The various malicious modules identified for VPNFilter give us an insight into the objectives and desires of the threat actor. Notably, infecting routers allows the threat actor to reroute network traffic from the intended legitimate destination to a malicious destination under the control of the attacker. Potentially this ability can be used to collect further usernames and passwords, and also to conduct man-in-the-middle attacks by intercepting and reading network traffic before passing it on to the intended destination.

APT28 is only one example of the many threat actors who continue to attempt destructive attacks. Talos recently discovered the Sea Turtle campaign. Although the unknown threat actor behind the attack is different from APT28, they also sought to reroute internet traffic in order to conduct man-in-the-middle attacks and collect user credentials. However, they achieved their objectives by a completely different approach than VPNFilter, by attacking the internet's DNS infrastructure[15].

Clearly, network infrastructure is in the sights of nation-state threat actors. We can expect that attackers will continue to seek to compromise these systems and continue to refine and develop the malware that they use to achieve their goals. Attackers can only learn from past failures. In the inevitable next wave of attacks, we can expect to see malware that leaves fewer traces in network traffic and has a more sophisticated C2 infrastructure that is more resistant to disruption.

The network is at the heart of our professional and social lives, and increasingly, our physical environment. The little devices that connect us to the network are often overlooked, but it is these systems allow our critical national infrastructure and enterprises to function.

VPNFilter teaches us that attackers have not overlooked the importance of these systems, and that those who may be seeking to disrupt our societies look to strike at the network. However, in attempting to conduct this attack, the threat actors have let slip their technologies and the capabilities that they are trying to develop. These clues help us in knowing where to look and how to search for the next attack in preparation.

Talos continues to use its unparalleled visibility of threats to analyse the changing threat landscape and to act together with partners to protect customers. Nevertheless, cyber security is everyone's concern. We all have our part to play in protecting against the next attack by ensuring that we have adequate security protection, and that all our devices connected to the network are kept updated and fully patched.

We don't know what the next major attack will be, but we continue to search for the hints and clues of an impending attack, so that we can disrupt the activity and stop catastrophes before they happen.

References

[1]. The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations, US Department of Homeland Security. https://cyber.dhs.gov/assets/report/ar-16-20173.pdf

[2]. UK Internet Edge Router Devices: Advisory, UK National Cyber Security Centre. https://www.ncsc.gov.uk/information/uk-internet-edge-router-devices-advisory

[3]. Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices, US Department of Homeland Security. https://www.us-cert.gov/ncas/alerts/TA18-106A

. Affidavit in Support of an Application for a Seizure Warrant, US District Court for the Western District of Pennsylvania. https://www.justice.gov/opa/press-release/file/1066051/download

[5]. New VPNFilter malware targets at least 500K networking devices worldwide, Talos. /VPNFilter

[6]. Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices, US Department of Justice. https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

[7]. Korea In the Crosshairs, Talos. /korea-in-crosshairs

[8]. Rocke: The Champion of Monero Miners, Talos. /rocke-champion-of-monero-miners

[9]. Groups, MITRE ATT&CK. https://attack.mitre.org/groups/

[10]. GRIZZLY STEPPE – Russian Malicious Cyber Activity, US Department of Homeland Security & Federal Bureau of Investigation. https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[11]. Reckless campaign of cyber attacks by Russian military intelligence service exposed, UK National Cyber Security Centre. https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed

[12]. Cyber-Attack Against Ukrainian Critical Infrastructure, US Department of Homeland Security. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[13]. Information Sharing in Action: CTA's Incident Review of VPNFilter, Cyber Threat Alliance. https://www.cyberthreatalliance.org/information-sharing-action-cta-incident-review-vpnfilter/

[14]. The SBU warns of a possible large-scale cyberattack on state structures and private companies ahead of the Champions League final (via Google Translate), Security Service of Ukraine. https://ssu.gov.ua/ua/news/1/category/21/view/4823#.Xa4RX7cc.dpbs

[15]. DNS Hijacking Abuses Trust In Core Internet Service, Talos. /seaturtle

---