Shadowserver Special Reports – Cyclops Blink

shadowserver.org/news/shadowserver-special-reports-cyclops-blink/

February 23, 2022

UPDATE 2022-04-21: Fifth special report sent overnight containing 511 IPs likely still infected with Cyclops Blink, corresponding to 270 ASNs in 60 countries. Remediation continuing.

UPDATE 2022-04-13: Overnight 2022-04-12/13 we sent out a fourth special report with 537 IPs likely infected with Cyclops Blink, corresponding to 281 ASNs in 61 countries. The top countries were still United States (154), Canada (58), Sweden (38), Russia (26), Germany (25). A mix of Watchguard and ASUS devices. Remediation continuing, but more patching required.

UPDATE 2022-04-08: Overnight 2022-04-07/08 we sent out a third special report with an additional 553 IPs likely infected with Cyclops Blink, corresponding to 285 ASNs in 61 countries. The top countries were United States (157), Canada (58), Sweden (38), Russia (27), Germany (26).

UPDATE 2022-04-06: US DoJ announcement about disruption action against Cyclops Blink infected devices.

UPDATE 2022-04-01: ASUS released updated firmware for devices impacted by Cyclops Blink.

UPDATE 2022-03-25: ASUS released a security advisory about Cyclops Blink impacting ASUS devices.

UPDATE 2022-03-17: Trend Micro published research detailing ASUS devices also being impacted by Cyclops Blink (some ASUS device IPs were included in our second special report, but not explicitly called out at that time, since details were not public).

UPDATE 2022-03-03: On 2022-03-03 we sent out a second special report with an additional 673 IPs likely infected with Cyclops Blink, observed on 2022-02-24. These IPs are different to those sent out in the first report. Countries with top infections: USA (188), France (92), Italy (65), Canada (55), Germany (39).

Original Article

On May 23rd 2018, the US Department of Justice (DoJ), Federal Bureau of Investigation (FBI) and Cisco Talos publicly announced the disruption of a novel multi-stage modular malware platform called **VPNFilter**. This was designed to infect small office and home office

(SOHO) routers and other network devices. At the time, VPNFilter was believed to be operated by the threat actor known as APT28 (also known as Fancy Bear, Pawn Storm, Sandworm, Sofacy Group, Sednit X-Agent, STRONTIUM and Tsar Team), which was allegedly associated with the Russian military intelligence agency (GRU). You can read more about that sinkholing effort in our original 2018 blog post, which includes links to supporting technical information.

Since then, we have continued notifying VPNFilter victims about infected devices worldwide via Shadowserver's free daily network reports.

In January 2021, we collaborated with partner Trend Micro on a joint analysis of the remaining global VPNFilter victim population. This added some further scan-based insights about third stage victim prevalence into our daily datasets.

From our vantage point as sinkhole operators, the peak day for VPNFilter infections globally was 2018-07-24, which saw 14,966 unique IP addresses being observed hitting the sinkhole. After the initial fairly rapid (by global Internet response standards) remediation of infected devices, a typical long tail of not yet remediated victims still remains today:

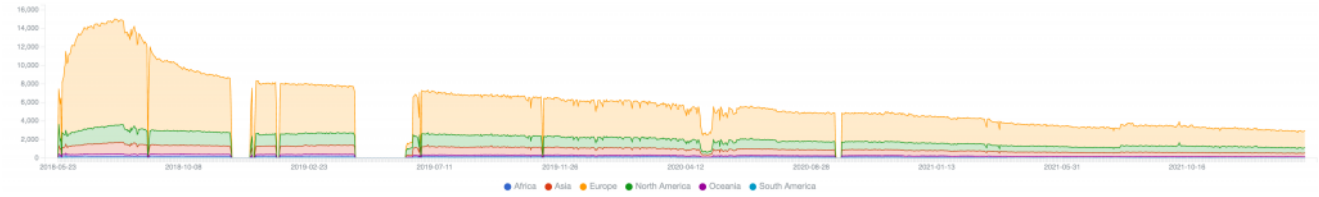

Figure 1 – Unique sinkholed VPNFIlter IP address per day

Note the lack of variation in the daily/weekly number of detected IP addresses. As expected, this suggests that the infected devices are always-on routers (which is unlike the typical overnight or weekend patterns of change we usually see in sinkholed home or office PCs).

The IP-geolocated distribution of sinkholed VPNFilter unique IP addresses on that peak day was:

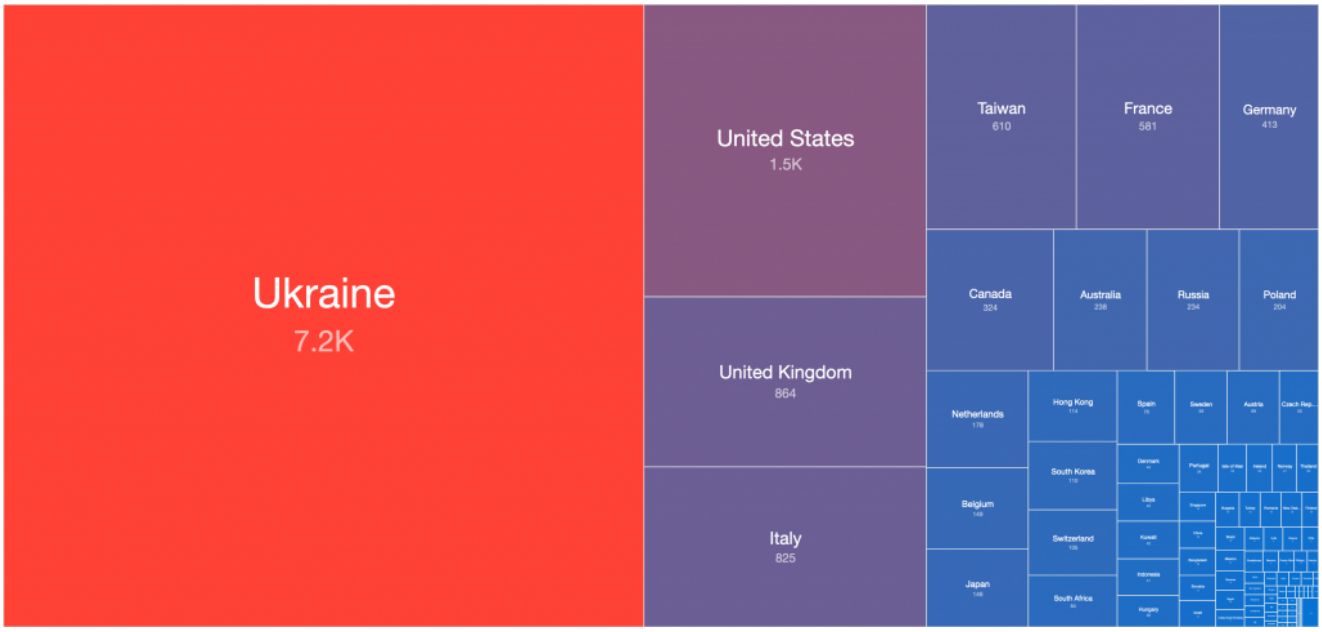

Figure 2 – Unique sinkholed VPNFIlter geolocated IP addresses (2018-07-24)

With Ukraine having by far and away the most infected victim devices.

This compares to the current sinkholed VPNFilter IP address distribution observed yesterday:

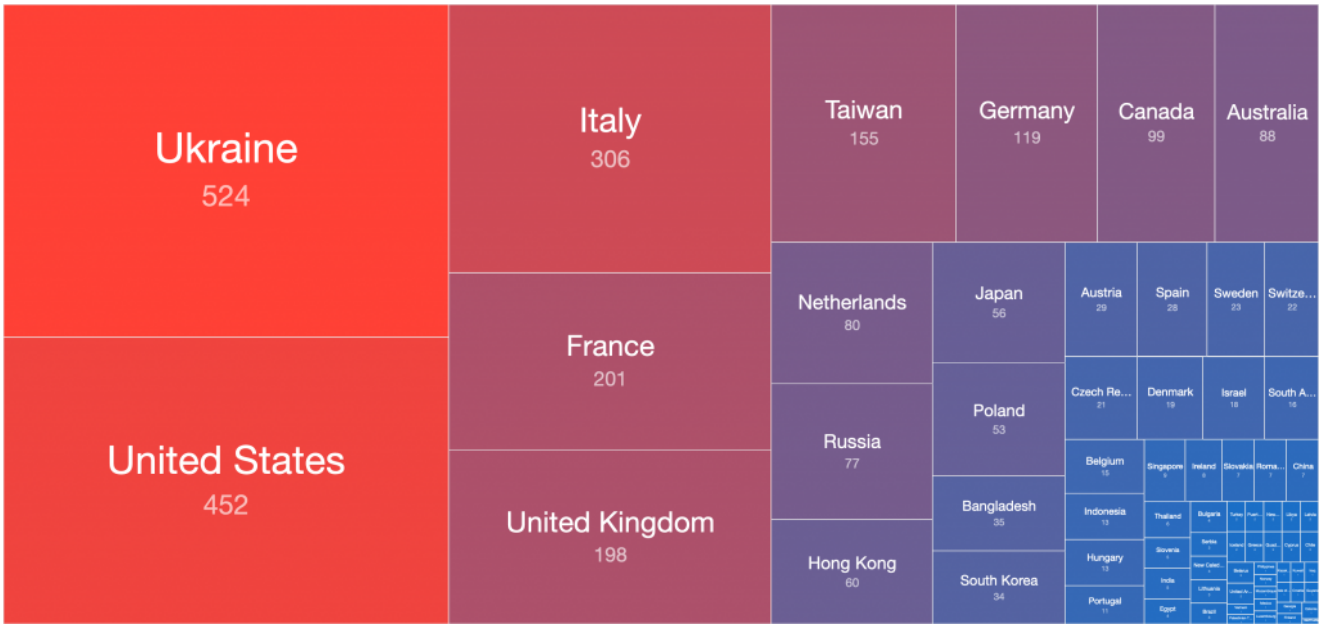

Figure 3 – Unique sinkholed VPNFIlter geolocated IP addresses (2022-02-22)

Cyclops Blink replaces VPNFilter

On February 23rd 2022, the UK National Cyber Security Centre (NCSC), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) jointly announced that they had identified that the

threat actor known as Sandworm or Voodoo Bear has deployed a new, large-scale modular malware framework which is affecting network devices. They have named the malware **Cyclops Blink**. The NCSC, CISA, FBI and NSA have previously attributed the Sandworm threat actor to the Russian GRU's Main Centre for Special Technologies GTsST.

The Cyclops Blink malware is believed to be a more advanced replacement for VPNFilter. It is installed on exploited network devices as part of a legitimate firmware upgrade, allowing persistence between reboots. The UK NCSC's analysis explains that it is possible to recalculate the Hash-based Message Authentication Code (HMAC) value for the modified firmware image because the WatchGuard FireBox devices use a hard-coded key to initialize the hash calculation. This allows their malware to pass checks and appear to be legitimate, vendor-supplied firmware updates.

Infected victims' devices are grouped into clusters, each with a list of Command and Control (C2) servers. They communicate with their operators using Transport Layer Security (TLS) running over The Onion Router (Tor) network. To date, Cyclops Blink malware is believed to have been primarily deployed onto WatchGuard firewall devices (which are Linux ELF 32-bit PowerPC big-endian platforms), and all C2 servers identified to date have been for WatchGuard firewalls. However, the assessment published today indicates that it is likely that the Cyclops Blink malware could also be compiled and deployed onto other architectures and firmware. This botnet appears to have been active since at least June 2019.

A detailed technical analysis of Cyclops Blink by the UK NCSC can be found here, which includes Indicators of Compromise (IoCs) and YARA signatures to assist in detection.

Cyclops Blink Malware Remediation

WatchGuard have provided remediation information for system owners infected with the Cyclops Blink malware:

https://detection.watchguard.com

WatchGuard estimate that Cyclops Blink malware may have infected approximately 1% of WatchGuard firewall devices. They advise that the default configuration is to prevent access to their management interface from the Internet, so this configuration must be manually enabled by the system administrator.

All WatchGuard device owners should follow each step in these instructions to ensure that devices are patched to the latest version and that any infection is removed.

- If your device is identified as infected with Cyclops Blink, you should assume that any passwords present on the device have been compromised and replace them immediately.
- You should ensure that the management interfaces of your network devices are not exposed to the Internet.

UPDATES 2022-03-25 and 2022-04-01: Asus have also provided remediation information and updated firmaware for impacted customers.

Shadowserver Cyclops Blink Special Report

We send out Special Reports whenever we are able to share one-time, high value datasets that we feel should be reported responsibly for maximum public benefit. Although the events included in these Special Reports sometimes fall outside of our usual 24-hour daily reporting window, we believe that there would still be significant benefit to our constituents in receiving and hopefully acting on the data.

On February 23rd 2022, we sent out a new Special Report covering network devices that are believed to be likely infected with the Cyclops Blink malware. This one off Cyclops Blink Special Report contained:

- **1,573** unique victim IP addresses in **495** different Autonomous System Numbers (ASNs) across **70** different countries
- **25** Command and Control (C2) server IP addresses in **19** different Autonomous System Numbers (ASNs) in **7** different countries

A direct link to the Cyclops Blink Special Report format is here.

Cyclops Blink Data Visualisation

The data contained in this new Cyclops Blink Special Report was provided to Shadowserver to disseminate rapidly to National CERTs/CSIRTs and network owners globally, to maximise remediation efforts.

Of the 1,573 IPv4 addresses included in the Cyclops Blink Special Report, the majority of likely infected network devices IP-geolocate as being located in the United States, Canada and Central Europe:

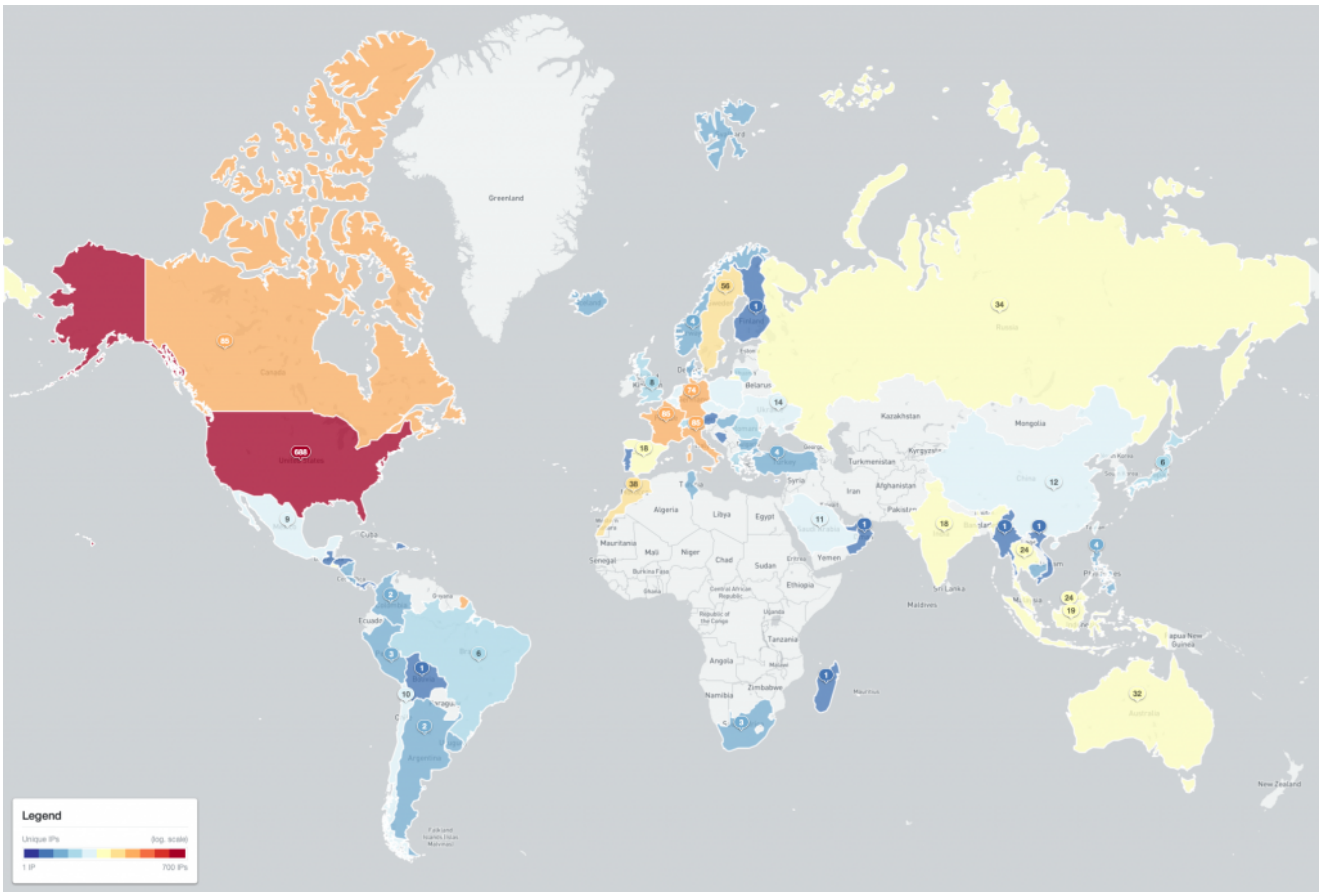

Figure 4 – Map of likely Cyclops Blink infected devices (2022-02-23)

Looking at the data in another way, more than half of the network devices believed to be infected with Cyclops Blink malware are located in the United States, France, Italy, Canada and Germany:

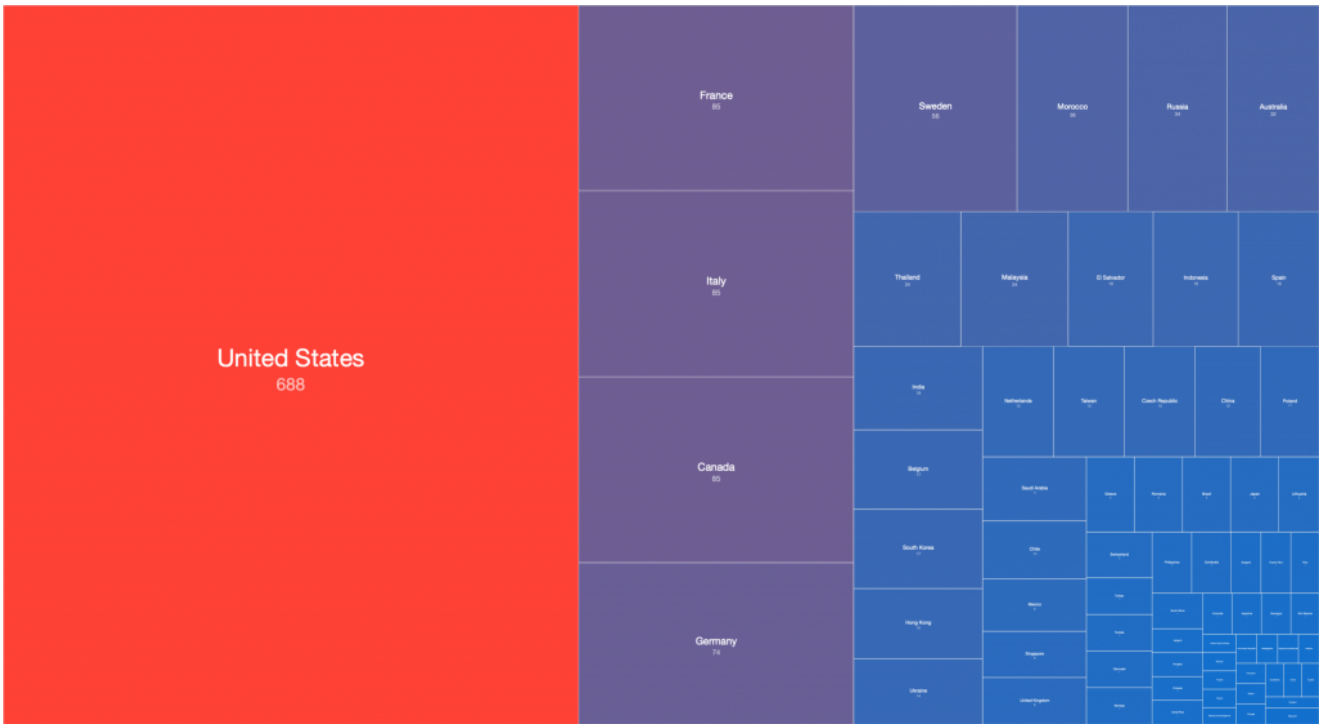

Figure 5 – Tree Map of likely Cyclops Blink infected devices (2022-02-23)

Shadowserver conducts daily Internet-wide scanning of all IPv4 /0, which includes identification of Internet facing devices, where possible, thanks to the EU HaDEA VARIoT project. We began making this information available to National CERT/CSIRTs and Network Owners who subscribe to our free daily network reports in the form of our Daily Device Identification Report in September 2021, which can be used to establish your exposed attack surface. We highly recommend subscribing and reviewing this report for your network, since this is the same profile an attacker scanning to perform reconnaissance from the outside will also see.

The location of the likely Cyclops Blink infected devices generally matches our scan-based understanding of the global distribution WatchGuard firewall devices which are currently exposed to the Internet:

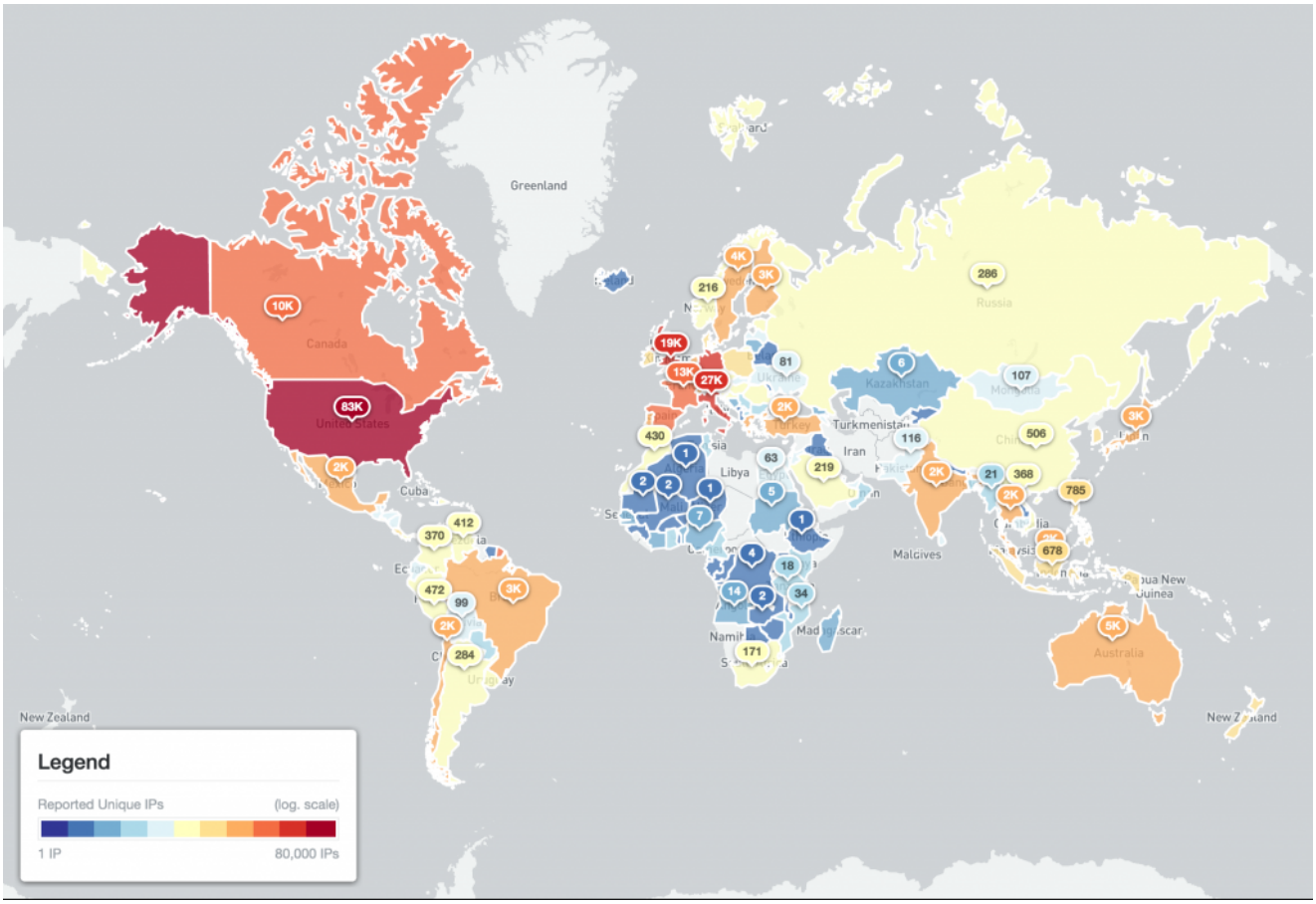

Figure 6 – Identified WatchGuard firewall devices detected – World (2022-02-22 IPv4 /0 scan)

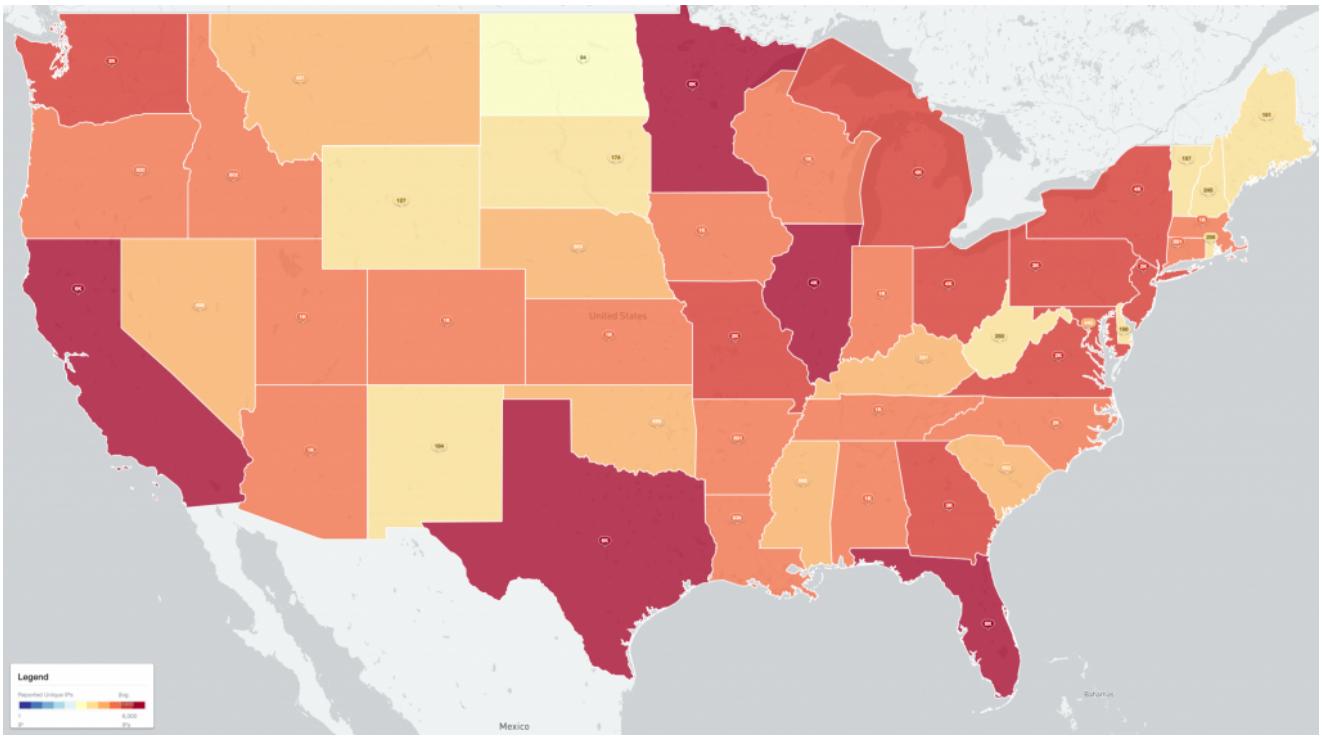

Figure 7 – Identified WatchGuard firewall devices detected – US States (2022-02-22 IPv4 /0 scan)

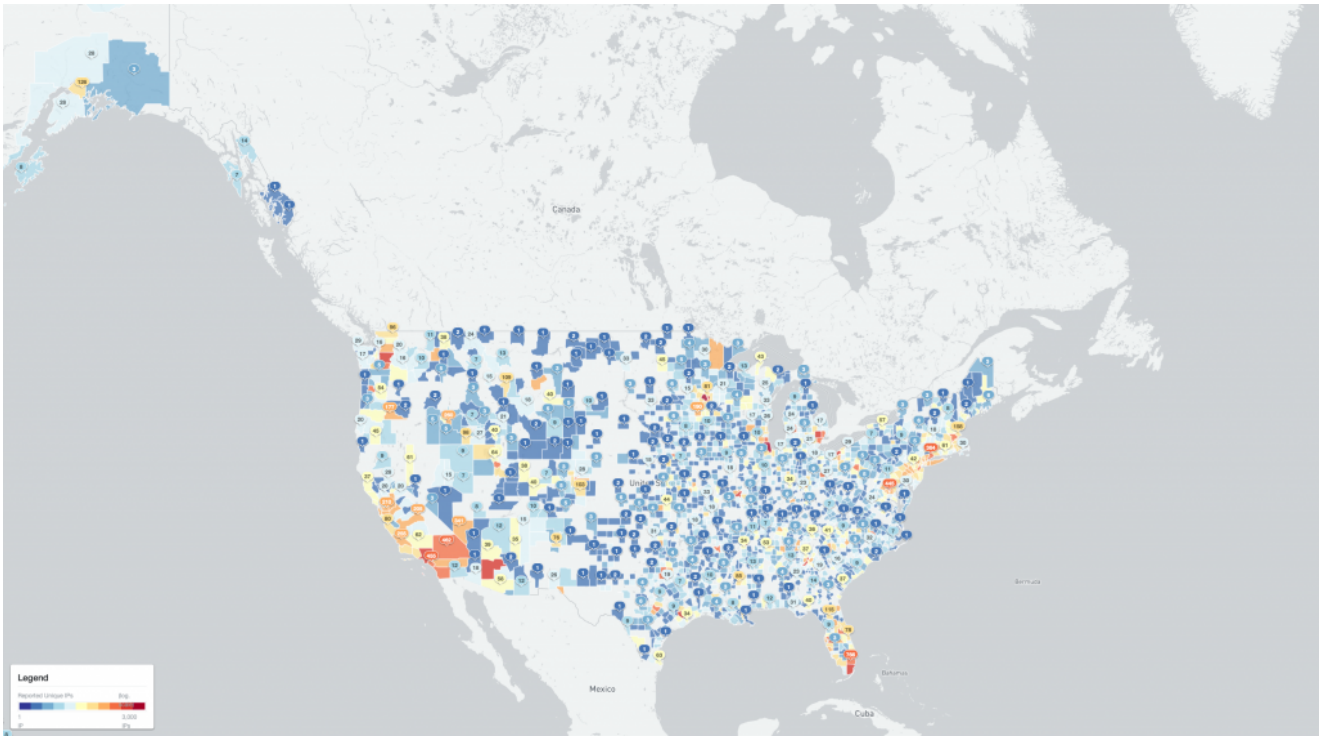

Figure 8 – Identified WatchGuard firewall devices detected – US Counties (2022-02-22 IPv4 /0 scan)

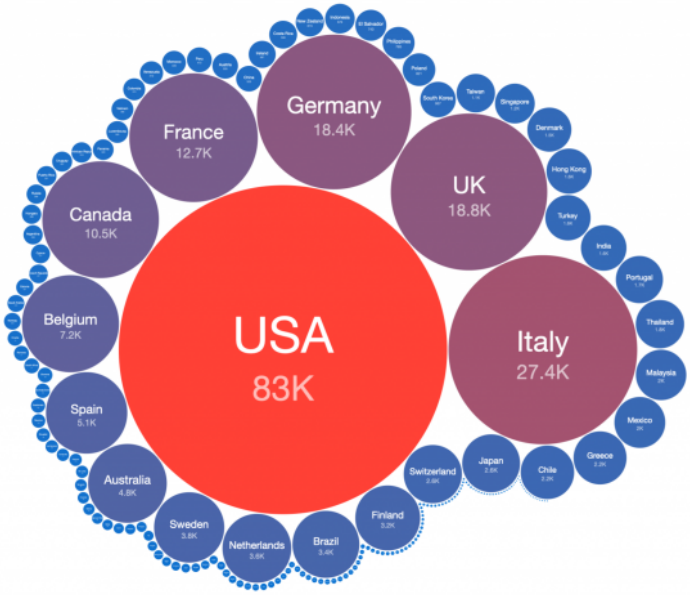

Figure 9 – Identified WatchGuard firewall devices detected – World (2022-02-22 IPv4 /0 scan)

Figure 10 – Identified WatchGuard firewall device models – World (2022-02-22 IPv4 /0 scan)

Shadowserver's daily scanning will obviously not detect all WatchGuard devices. However, comparing the 1,573 unique IP addresses reported out as potentially infected with Cyclops Blink malware to the number of publicly exposed systems identified through scanning, does represent similar orders of magnitude to the 1% infection ratio suggested by WatchGuard.

Cyclops Blink C2 Server Distribution

In addition to the 1,573 IPv4 addresses corresponding to likely infected victim network devices included in our Cyclops Blink Special Report, 25 Cyclops Blink C2 servers have also been identified:

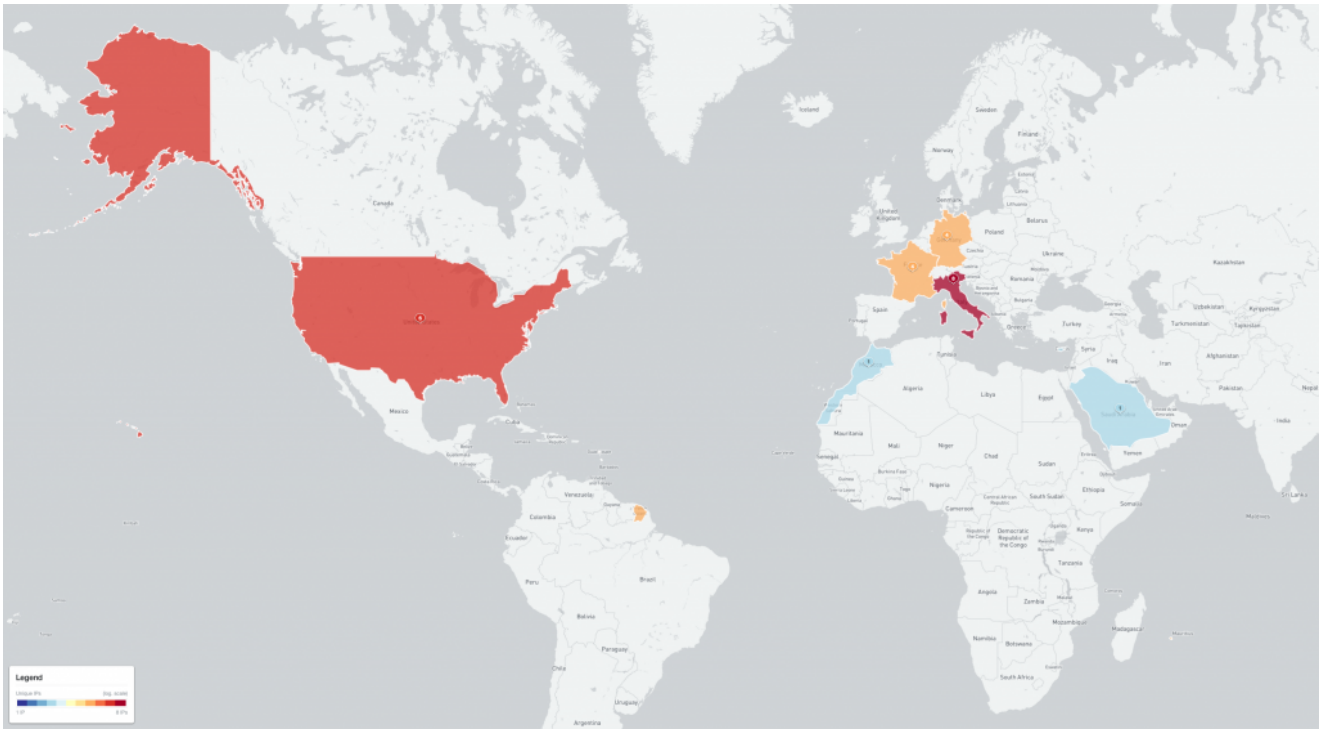

Figure 11 – Cyclops Blink C2 Server Location Map (2022-02-23)

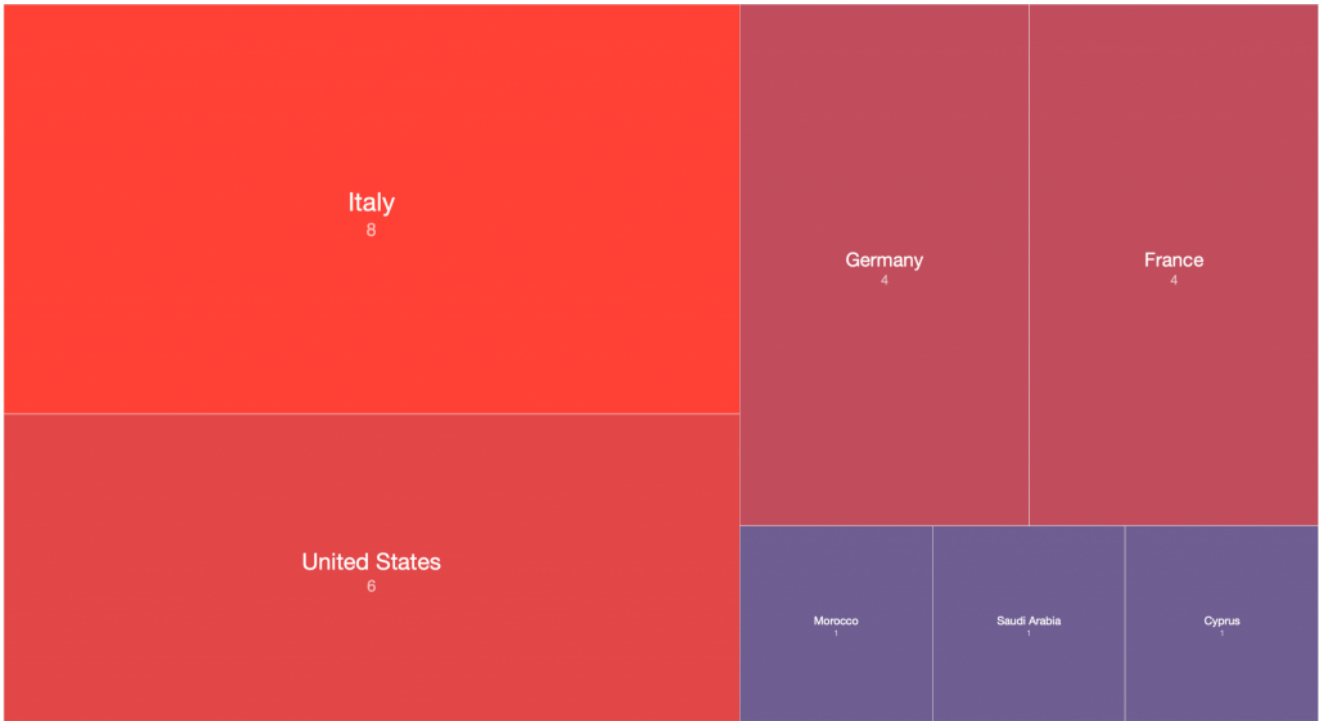

Figure 12 – Cyclops Blink C2 Server Location Countries (2022-02-23)

Not Yet Subscribed to Shadowserver's Free Daily Reports?

If you missed this Special Report because you were not yet a subscriber to our free daily network reports, do not worry: simply subscribe for your network or country now and specifically request all recent Shadowserver Special Reports. We will resend the Special Report specifically for your network or country (for National CERT/CSIRTs).

If you have a data set which you feel could also be of benefit to National CERT/CSIRTs and network owners world-wide to help protect victims of cybercrime, please get in touch and discuss the options for using Shadowserver's proven reporting systems for distribution and remediation.

« Back to News & Insights