Really, How Bad Do Routers Have It?

Author: Jesse Schibilia

Abstract

In recent years, the United States government has warned the public that state-sponsored cyber actors conduct worldwide exploitation of network devices, particularly small business and home office routers, to support their campaigns. Quantitative analysis of ten years of Internet Storm Center data and current Shodan data was conducted to explore the scope of the router attack surface compared to that of host devices. This investigation determined that hosts are targeted more than twice as much as routers on average, even when controlled for relative number of devices. While the data shows that routers are not targeted as often as hosts, router security must be scrutinized from the early stages of research and development through field deployment. Recommendations for device manufacturers, Internet Service Providers, and cyber security practitioners are provided.

**1. Introduction**

On 06 September 2016, the United States government warned the public about an increasing threat to network infrastructure devices. A router attack campaign called SYNful Knock, which was disclosed 12 months earlier, was of particular concern in this advisory. This campaign didn’t exploit a high-profile router vulnerability but rather gave attackers backdoor access to targeted networks through the exploitation of weak security configurations on commercial and home/small office routers running Cisco IOS. Attackers primarily used default or weak credentials to gain a foothold on poorly secured routers, then installed their own extensible operating system that provided persistent access to all communications traversing the compromised devices (Cybersecurity & Infrastructure Security Agency [CISA], 2016.

This sinister implant was difficult to detect but simple to avoid. Public and private entities moved swiftly to provide effective mitigation guidance for network defenders. Despite the grave security implications for this intrusion vector and the simplicity of mitigation guidance, the security community did not seem to pay heed. Two years later, and despite warnings to batten down the router hatches, a Russian statesponsored group exploited poor router security configurations to deploy VPNFilter malware on hundreds of thousands of routers worldwide (CISA, 2018b). Around the same time, the United States government released a second public warning about SYNful Knock, stating that the campaign continued to be a security concern. It also attributed the activity to Russian state-sponsored cyber actors (CISA, 2018a).

Practitioners appear to lower their guard regarding router security despite these warnings. Oversights are particularly prevalent in-home office and small business settings wherein customers must often use the commodity router or gateway model supplied by the ISP. Some ISPs even prohibit customers from making certain configuration changes that could enhance the security of their edge device (Horowitz, 2022). What’s more, a report by the United States Departments of Commerce and Homeland Security found that when it comes to routers and other network infrastructure devices, “product developers, manufacturers, and vendors are motivated to minimize cost and time to market, rather than to build in security or offer efficient security” (Secretary of Commerce & Secretary of Homeland Security, 2018).

If there are no clear incentives for manufacturers to bring more secure routing devices to market or for ISPs and network defenders to ensure that their equipment is secured against known vulnerabilities, perhaps the threat to edge routers is less significant than the United States government claims. Maybe network defenders should ignore their guidance and expend more effort to improve security on devices behind the network boundary.

Is it possible to quantify the relative volume of malicious traffic targeting routers compared to hosts? Such information could help network defenders prioritize their efforts. The goal of this research is to show that malicious traffic targeting boundary routers is as prevalent as that targeting hosts inside the network. It will also attempt to prove that network defenders focus relatively less effort on their boundary routers compared to hosts within their network.

**2. Research Method**

Two datasets were used to explore the questions outlined above. The Internet

Storm Center’s port history dataset was first queried to investigate relationships between the volume of malicious traffic targeting network devices versus that of hosts. The Internet of Things search engine, Shodan, was then queried to quantify the number of routers versus hosts connected to the Internet. Ten ports were selected to identify devices likely to be hosts, and six ports were selected to identify devices likely to be routers:

|  |  |
| --- | --- |
| **Likely host services** | FTP (21), SSH (22), SMTP (25), DNS (53), HTTP/HTTPS (80/443), SMB (445), MSSQL (1433), 3306 (MySQL), RDP (3389) |
| **Likely router services** | Telnet (23), TFTP (69), SNMP (161), UPnP (1900), Cisco IOS (4786), TR-069 (7547) |

**2.1. Definitions**

Hosts were defined as any physical or virtual workstations or servers that appeared to be running common host operating systems or were running services commonly associated with host systems. This analysis excluded printers, tablets, mobile handsets, Internet of Things devices, and embedded devices. Devices that reasonably appeared to be operated by a cloud service or hosted by a content delivery network were also excluded.

Routers were defined as any wired, Wi-Fi, or mobile customer edge router. Devices were categorized as routers if they appeared to be running operating systems or services commonly associated with networking equipment and reasonably appeared to be connected to the Internet via an ISP. The analysis focused on routers at the customer’s network boundary and did not intentionally include carrier equipment. Other network devices, such as switches, firewalls, and VPNs, were excluded from the analysis.

**2.2. Internet Storm Center dataset**

The Internet Storm Center (ISC) runs a distributed intrusion detection system called DShield to collect data about malicious network activity worldwide. The system ingests volunteer submissions from firewalls covering upwards of 500,000 IP addresses in over 50 countries. The ISC aggregates the volunteered data, anonymizes it, and publishes simplified perspectives of the raw data for public use (ISC, n.d.).

ISC’s port history perspective quantified the daily number of reported records, sources, and targets indicating potentially malicious activity directed at specific network ports. 120 months of ISC’s port history data for each of the 16 selected ports was ingested into Microsoft Excel.

Quantitative analysis was conducted on the data to explore relationships in traffic volume between hosts and routers. The data was visualized in various ways to identify outliers, trends, and further analysis needs.

**2.3. Shodan dataset**

Shodan is a search engine that indexes Internet-connected devices around the world and provides various publicly available information about each of the hundreds of millions of devices it observes (Shodan, n.d.a). Queries of the Shodan search engine were designed for the following purposes:

1. To determine a ratio of hosts to routers among devices indexed by Shodan

2. To quantify the number of devices on which any of the 16 selected ports are open

3. To quantify the number of devices that may be vulnerable to known exploits

**3. Findings and Discussion**

The graphed ISC and Shodan data were first reviewed for relevant trends and data reliability. Visually identified data trends were explored through further analysis. Hostto-router ratios were extracted from ISC target data and Shodan query return data. The host-to-router ratios were then applied to the ISC traffic volume data to normalize it for the relative number of hosts and routers identified in each dataset. Finally, the adjusted traffic volume figures were graphed for comparison to charts from the original ISC

record dataset.

**3.1. Review of ISC daily record scatter plots**

When graphed, the ISC data immediately showed explicit trends. The ten selected host ports were generally targeted with a greater volume of anomalous traffic than the six selected router ports. This was most obvious when looking at the y-axis scales for each scatter plot visualizing the daily number of records for each port. Throughout the ten-year analysis period, most of the selected host ports experienced intermittent or sustained periods where malicious or suspicious traffic was measured in the millions of records. In contrast, most of the router ports only received average traffic volume peaks in the tens or hundreds of thousands of daily records.

**3.2. Telnet protocol suitability**

One notable exception to the low traffic volume trend among the six selected router ports was Telnet protocol (port 23). Over the course of the ten-year analysis period, this service received sustained traffic volumes comparable to many of the highestvolume host ports. Much of the ISC data for Telnet protocol appeared to suffer from wide variation across the ten-year analysis period, which could cause it to be excluded from the overall analysis. Telnet’s data anomalies are likely to be natural variations, however. There was likely an elevated traffic volume targeting Telnet because it has long been known to be an inherently insecure protocol (Software Engineering Institute, 1994).

Telnet is also a strong representative of devices likely to be routers. In support of this assessment, a Shodan query for the top 10 reported products on any device with port 23 open yielded the following results:

**1. Cisco router telnetd 50,600**

2. OpenSSH 13,558

**3. Cisco catalyst switch telnetd 6,088**

4. Microsoft ftpd 1,048

**5. Dropbear sshd 937**

6. Ricoh maintenance telnetd 548

**7. SMC SMC2870W Wireless Ethernet Bridge 435**

8. Hikvision IP Camera 411

9. CCProxy telnet configuration 190

10. Pure-FTPd 189

The bolded products are either routers or have a direct connection to them: Cisco’s Catalyst line of switches has had Layer 3 routing capabilities since the release of the 3550 series (Cisco, 2003), and the Dropbear toolset is a core component of the OpenWRT router operating system distribution (OpenWRT, 2023). One could make the case that Telnet is also a host protocol. While it is true that Telnet is installed on most current host operating systems, it is not enabled by default and is unlikely to be active on most host systems.

**3.3. Review of ISC monthly median record volume**

The ten selected host ports received a reasonably even distribution of malicious or suspicious traffic over the ten-year analysis period, whereas the router protocols varied widely. Four of the six selected router protocols (TFTP, SNMP, UPnP, and IOS) barely registered any traffic. Telnet protocol traffic volume tracked very tightly with FTP (port 21), SSH (port 22), DNS (port 53), and HTTP (port 80) between January 2013 through October 2013, then inexplicably broke away from the group. Traffic peaks between September 2019 and July 2020 for Telnet and TR-069 (port 7547) correlated with surges in traffic to host protocols SSH, HTTP, HTTPS (port 443), and SMB (port 445). These surges were likely related to a high-profile vulnerability, but no specific exploit or campaign targeting all these protocols was identified.

Throughout the ten-year analysis period, the average volume of monthly median malicious or suspicious traffic targeting the ten selected host ports was approximately 2.47 times greater than that targeting the six selected router ports. One notable exception to this trend was Telnet protocol, which averaged about the same volume of malicious traffic over the ten-year analysis period as SMB protocol. The Telnet record data appears to be a true outlier, as there are no apparent measurement or data entry errors.

**Review of ISC monthly median target counts**

The ten host ports were targeted on a greater number of devices during the analysis period when compared to the six router ports. The average number of targeted devices across the host ports was approximately 1.89 times greater than the average number for router ports. Telnet and SNMP (port 161) stood out from this trend. The average number of devices targeted on those two services was greater than all but one of the ten selected host services.

One anomaly emerged when comparing the average monthly median traffic volume to the monthly median target count over the ten-year analysis period. SNMP ranked 10th out of the 16 selected ports for traffic volume, but the protocol was targeted on the second greatest number of devices. Further calculations indicated that for every SNMP target, only 1.6 average monthly records were generated, and each source generated 109.2 records on average per month. This implied that an exceedingly small number of sources (3% of average for all ports) sent relatively small volumes of malicious traffic (13% of average) to a significant number of targets (171% of average). The high average for SNMP targets was influenced almost entirely by prolonged surges between February 2014 and March 2017, after which the number of SNMP targets slowed to a trickle. It’s possible that these peaks resulted from massive scanning campaigns against the protocol, emanating from a small number of attackers or researchers.

SSH protocol was strongly represented in the target data. It saw malicious or suspicious activity on 2.6 times more devices than average for the ten selected host ports. This is likely because attackers instantly stand to gain system administration privileges on devices accessed via SSH. While SSH is an inherently secure protocol, administrators

can easily hamstring defenses through poor security configurations (Unit 42, 2019).

**3.5. Review of ISC monthly median source counts**

In a departure from the ratios observed with the record and target data, the average number of malicious traffic sources for hosts was almost even with that of routers over the ten-year analysis period. In fact, the six selected router ports were targeted from a slightly greater number of malicious sources than were the ten selected host ports. The router ports were targeted by approximately 1.17 times more malicious source devices than the host ports. This reversed ratio was due almost entirely to a sizeable spike in the median number of monthly sources targeting Telnet between January 2016 and June 2017. This massive spike in attackers targeting Telnet can almost certainly be attributed to the Mirai botnet and its variants, which were rampant from mid- 2016 through at least 2021 (Bursztein, 2017). The 18-month-long surge in sources targeting Telnet correlated with a loosely contemporaneous spike in sources targeting DNS and TR-069. These source spikes were also likely related to the Mirai botnet. Each node in the botnet had to regularly conduct a DNS lookup to resolve its C2 domain (Bursztein, 2017), and Mirai’s spreader mechanism began targeting TR-069 at some point in late 2016 (Ullrich, 2016). While this highprofile botnet heavily influenced the monthly median source data, it is a true outlier that remains accurate to events and will be included in the overall analysis.

Telnet boasted the greatest average number of sources across the 16 selected ports, meaning that the largest number of attackers over the ten-year analysis period targeted a router port the most. Telnet’s spot at the top of the podium was facilitated in large part by the spike in Telnet targeting during the Mirai era, but the number of Telnet sources was notable before and after that period as well. The next greatest number of sources targeted SMB protocol, which received a sustained boost of interest beginning in May 2017, just one month after the Shadow Brokers leaked the Eternal Blue exploit