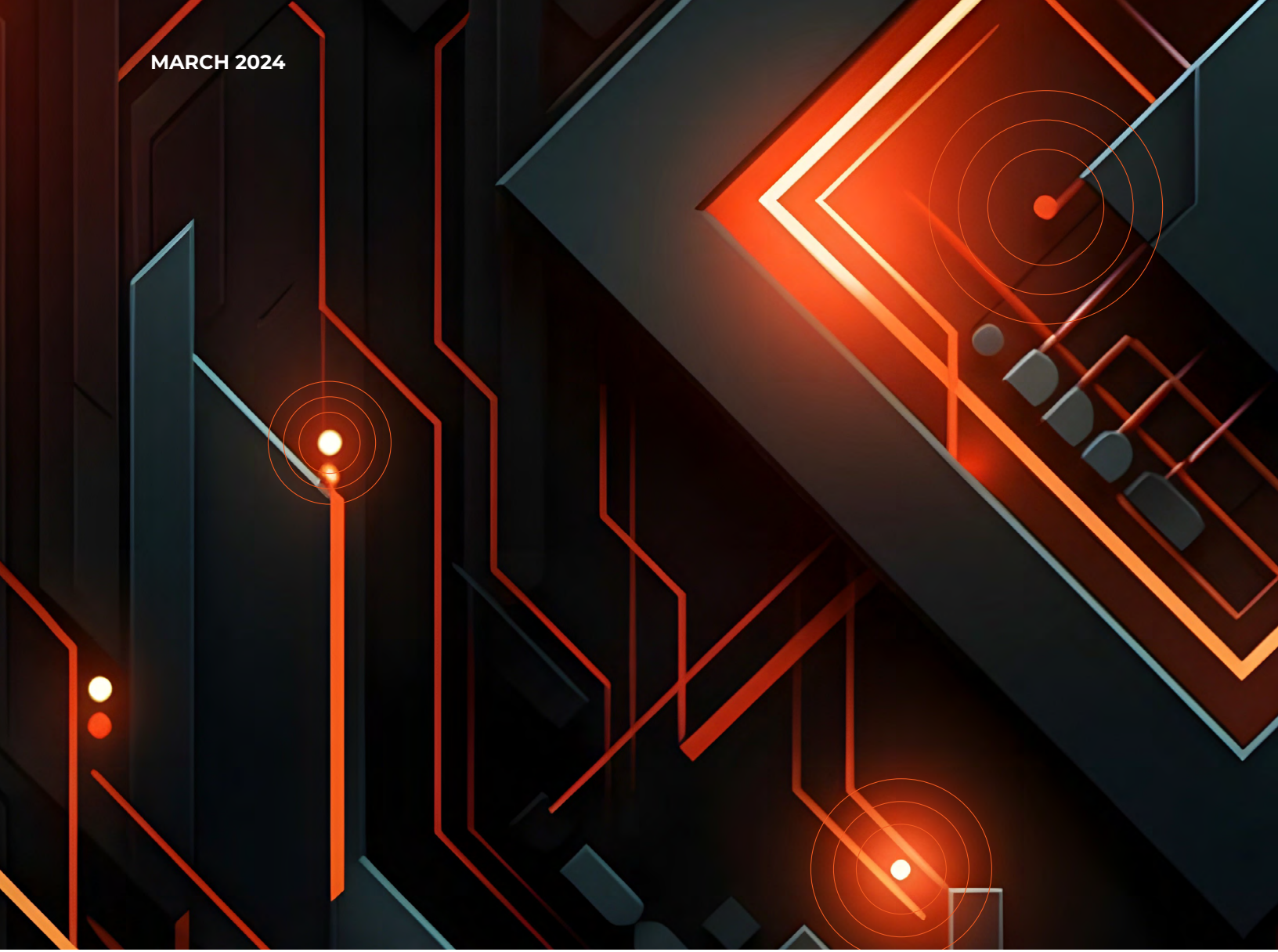


# USTELECOM **BOTNET AND IOT SECURITY TRENDS** 2024

MARCH 2024



# USTELECOM BOTNET AND IOT SECURITY TRENDS 2024

## Table of Contents

<b>Introduction: Summary of 2023 Botnet Trends and Initiatives</b> .....	<b>2</b>
<b>1: Volt Typhoon, Foreign Adversaries, and Major Botnet Takedowns</b> .....	<b>2</b>
Volt Typhoon’s KV-botnet .....	2
Qakbot .....	3
Moobot .....	4
IPStorm .....	4
<b>2: IoT Device and Botnet Security</b> .....	<b>5</b>
New 2023 Mirai Botnet Variants.....	5
Consumer Device Labeling .....	5
Secure by Design and Anti-Botnet Practices .....	6
<b>3: Artificial Intelligence</b> .....	<b>7</b>
Fox8.....	7
<b>Conclusion</b> .....	<b>8</b>
<b>Endnotes</b> .....	<b>9</b>

## Introduction: Summary of 2023 Botnet Trends and Initiatives

2023 saw another record year in the world of botnet activity.

- ▶ In January 2024, FBI Director Christopher Wray warned Congress about Chinese hackers targeting US infrastructure. CISA followed with a related advisory.
- ▶ Attackers are increasingly targeting critical infrastructure, even beyond Volt Typhoon.
- ▶ Botnets saw a 25% year-over-year increase in activity, with Torpig Mebroot comprising 56% of all botnet detections in 2023.
- ▶ There was a noticeable uptick in the activity of other botnets like TorrentLocker, which quadrupled its activity in Q4.<sup>1</sup>
- ▶ IoT and AI are increasingly popular avenues for carrying out botnet activity and attractive target vectors for attackers to exploit.

**As US government agencies unite to combat threats from nation-state advisories and other APTs, USTelecom continues to lend its efforts and support in this space.** In response to these trends, USTelecom members contribute to the following three initiatives.

### 1: Volt Typhoon, Foreign Adversaries, and Major Botnet Takedowns

The United States communications sector is increasingly confronted with significant geopolitical threats posed by foreign adversaries. China stands out prominently among them, demonstrating both its expansive cyber capabilities and strategic ambitions, making it a particularly formidable adversary in this arena. Russia, Iran, and North Korea, among others present challenges, employing a variety of tactics, from cyber espionage to disruptive attacks, posing a multifaceted threat to the integrity and security of communications networks. As the communications sector continues to play a vital role in facilitating global communication and commerce, safeguarding against these threats is paramount to national security and economic stability.

#### **VOLT TYPHOON'S KV-BOTNET**

In December 2023, CISA, the NSA, the FBI, and partner Five Eyes agencies announced a joint advisory that the Volt Typhoon Chinese cyber-espionage group infiltrated US critical infrastructure networks and remained undetected for at least five years before being discovered. The advisory included a technical guide with information on how to detect Volt Typhoon techniques and determine if they were used to compromise their organization's networks, as well as mitigation measures to secure them against attackers using Living Off the Land techniques.<sup>2</sup>

The KV-botnet used by Volt Typhoon was composed of hundreds of US-based small office/home offices (SOHO) routers to hide their malicious activity and evade detection. Volt Typhoon primarily targeted the communications, transportation, energy, and water sectors.<sup>3,4</sup> Authorities believe that the group aimed to position itself within networks that provide them with access to Operational Technology (OT) assets with the end goal of disrupting critical infrastructure, particularly amidst potential military conflicts or geopolitical tensions.

The FBI partnered with industry to disrupt the KV-botnet and the hackers failed to rebuild the dismantled infrastructure after Lumen's Black Lotus Labs dismantled all remaining C2 and payload servers.<sup>5</sup> Lumen has claimed to not have detected any net new C2 servers being activated since January 2024. The lack of an active C2 server combined with the FBI court-authorized action against KV-botnet and Lumen Technologies persistent null-routing of current and new KV cluster infrastructure provides a good indication that the KV activity cluster is no longer effectively active.

**USTelecom members continue to contribute and engage in ongoing efforts with government and industry partners to secure networks from botnet exploitation.<sup>6</sup> Industry contributions took the form of USTelecom member security teams disclosing vulnerabilities and IoCs affecting small and home office routers, and null-routing IP addresses and proxy servers to impede efforts to reinfect the SOHO devices and further hamper communications between the bots and their C2.** The KV-botnet disruption yet again portrays that swift and effective cooperation between industry and law enforcement to take down high profile botnets has yielded notable results.

Lumen predicts that this trend of exploiting compromised firewalls and routers, both to enable access to high-profile targets and to establish covert infrastructure, will continue to emerge and persist as a fundamental aspect of threat actor operations. The abundance of outdated and end-of-life edge devices on the internet, no longer eligible for patches yet still operational, presents an attractive target for attackers. They will continue to target medium to high-bandwidth devices in the geographical regions of their targets, exploiting users' limited awareness of any impact or the absence of monitoring tools to detect infections.<sup>7</sup>

## QAKBOT

In August 2023, the FBI undertook a significant operation as part of an international cybercrime investigation, resulting in the disruption and dismantling of one of the largest active botnets. FBI Director Christopher Wray disclosed that the bureau had infiltrated and redirected traffic flowing through servers belonging to the Qakbot botnet. Qakbot allegedly enabled hackers to target financial institutions, government contractors and other critical infrastructure. The DOJ reported seizing over \$8.6 million in cryptocurrency profits from Qakbot operations, and that the botnet's administrators had received roughly \$58 million in ransoms paid by victims during attacks between October 2021 and April 2023.

The FBI claimed to have identified more than 700,000 computers worldwide that actors infected with the Qakbot malware, including over 200,000 in the US. The FBI said it infiltrated Qakbot's servers, redirected their traffic to FBI-controlled servers and downloaded a malware uninstaller file onto each device as part of the operation, which also prevented any further malware installations. The disruption campaign spanned devices in the US, the UK, the Netherlands, France, Germany, Romania, and Latvia. Wray highlighted that this marks the first instance of the FBI employing this technique in its operations, underscoring the collaboration between the bureau, private sector entities, and international law enforcement agencies in executing the takedowns. Before Qakbot, only the Pentagon's US Cyber Command had conducted out a botnet disruption of this kind.<sup>8</sup>

## MOOBOT

A January 2024 court-authorized operation neutralized a network of hundreds of small office/home office (SOHO) routers that GRU Military Unit 26165, also known as APT 28, Sofacy Group, Forest Blizzard, Pawn Storm, Fancy Bear, and Sednit, used to conceal and enable various crimes. The GRU botnet relied on the “Moobot” malware, which is known to be used by other criminal groups. Non-GRU cybercriminals installed the Moobot malware on Ubiquiti Edge OS routers that still used publicly known default administrator passwords. GRU hackers subsequently used the Moobot malware to install their own custom scripts and files, repurposing the botnet into a global cyber espionage platform.

The DOJ’s court-authorized operation leveraged the Moobot malware to copy and delete stolen and malicious data and files from compromised routers. In addition, to thwart GRU’s access to the routers until victims could mitigate the compromise and regain full control, the operation temporarily modified the routers’ firewall rules to block remote management access and, during the operation, allowed the temporary collection of non-content routing data to detect GRU attempts to obstruct the operation.

The Moobot takedown portrays the DoJ’s accelerating efforts to disrupt Russian cyber campaigns against the US and its allies. This marks the second time in two months that the DoJ disrupted state-sponsored hackers from launching cyber-attacks under the disguise of compromised US routers and the third time since Russia’s invasion of Ukraine that the DoJ has hampered malicious Russian intelligence service activities. Special Agent in Charge Jodi Cohen of the FBI Boston Field Office cited the “FBI’s strong partnerships with the private sector” as “critical to identifying and addressing this threat which targeted our national security interests here and abroad. This operation should make it crystal clear to our adversaries that we will not allow anyone to exploit our technology and networks.”

The FBI continues to emphasize that “the court-authorized steps to disconnect the routers from the Moobot network are temporary in nature; users can roll back the firewall rule changes by undertaking factory resets of their routers or by accessing their routers through their local network (e.g., via the routers’ web-based user interface). However, a factory reset that is not accompanied by a change of the default administrator password will return the router to its default administrator credentials, leaving the router open to reinfection or similar compromises.

To better protect themselves, the FBI advises all victims to conduct the following remediation steps:

1. Perform a hardware factory reset to flush the file systems of malicious files;
2. Upgrade to the latest firmware version;
3. Change any default usernames and passwords; and
4. Implement strategic firewall rules to prevent the unwanted exposure of remote management services.

The FBI strongly encourages router owners to avoid exposing their devices to the internet until they change the default passwords.”<sup>9</sup>

## IPSTORM

In November 2023, The FBI dismantled the IPStorm botnet proxy network and its infrastructure following a September plea deal with the hacker behind the operation. The botnet was used to power

various cybercriminal activities by renting it as a proxy as a service system over infected IoT devices. This investigation is another primary example of law enforcement and the private cybersecurity sector working together to shut down illegal online activities and bring those responsible to justice.<sup>10</sup>

## 2: IoT Device and Botnet Security

IoT botnet DDoS traffic, originating from a large number of insecure IoT devices with the aim of disrupting communications network services for millions of users, reportedly grew 25% year-over-year, following Russia's invasion of Ukraine and stemming from the growing increase in profit-driven hacking collectives operated by cybercriminals.

This sharp increase, also supplemented by the increased use of IoT devices by consumers around the world, was first noticed at the beginning of the Russia-Ukraine conflict but has since spread to other parts of the world, with botnet-driven DDoS attacks being used to disrupt communications networks as well as other critical infrastructure and services. The number of IoT devices participating in these attacks has soared from approximately 200,000 a year ago to around 1 million, constituting over 40% of all DDoS traffic today.

The most common malware in communications networks was found to be bot malware that scans for vulnerable devices, a tactic associated with a variety of IoT botnets. There are billions of IoT devices worldwide, ranging from smart refrigerators, medical sensors, and smart watches; many of which have lax security protections.<sup>11</sup>

### NEW 2023 MIRAI BOTNET VARIANTS

Botnets like Mirai continue to pose threats, exploiting the increasing number of IoT devices. Several new botnet variant families developed based on Mirai are accelerating their spread, and are widely deployed, constituting a considerable threat.<sup>12</sup> Researchers discovered that Mirai was exploiting a new zero-day vulnerability CVE-2023-1380 to attack TP-Link routers and add them to its botnet, which has been used to facilitate some of the most disruptive distributed DDoS attacks on record.<sup>13</sup>

### CONSUMER DEVICE LABELING

The proliferation of IoT devices and IoT-related cybersecurity threats has catalyzed several public-private partnership initiatives. **USTelecom members notably collaborate with NIST and industry groups to develop baseline IoT cybersecurity requirements, as well as support the White House-backed FCC labeling initiatives.**<sup>14, 15, 16</sup>

Given the rising threat of foreign adversaries, **USTelecom has strongly supported and is encouraged by the FCC's recent order prohibiting use of the IoT Label on products produced by entities on any of the following federal restricted lists:**

- ▶ FCC's Covered List
- ▶ The Department of Commerce's Entity List
- ▶ The Department of Defense's List of Chinese Military Companies.

- ▶ Products produced by any entity owned or controlled by or affiliated with any person or entity that has been suspended or debarred from receiving federal procurements or financial awards, to include all entities and individuals published as ineligible for award on the General Service Administration's System for Award Management.

## SECURE BY DESIGN AND ANTI-BOTNET PRACTICES

**In collaboration with stakeholders across the information and communications technology (ICT) ecosystem, including US government agencies, broadband providers have developed the below guidelines to tackle the threat of botnets.** These guidelines emphasize basic security practices and advanced capabilities. The key to controlling this growing threat in the long term lies in adopting these practices and encouraging the development of secure devices. This approach necessitates that manufacturers build security into their products from the ground up, following Secure by Design principles.

- ▶ NIST IR 8259A, IoT Device Cybersecurity Capability Core Baseline<sup>17</sup>
- ▶ NIST IR 8425, Profile of the IoT Core Baseline for Consumer IoT Products<sup>18</sup>
- ▶ ANSI/CTA-2088-A, Baseline Cybersecurity Standard for Devices and Device Systems<sup>19</sup>
- ▶ ISO/IEC 27402:2023, Cybersecurity—IoT security and privacy—Device baseline requirements<sup>20</sup>
- ▶ CSDE, International Botnet and IoT Security Guide<sup>21</sup>

The National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA) have been especially pivotal in promoting Secure by Design, and advocates for integrating security measures into the very fabric of technology products and systems from their inception, rather than applying them as an afterthought. NIST has been instrumental in developing guidelines and standards to enhance the security posture of IoT devices and networks. Their publication, NIST IR 8259A, outlines the core cybersecurity capabilities essential for IoT devices, providing a baseline for manufacturers to follow. Similarly, NIST IR 8425 offers a profile of the IoT Core Baseline specifically tailored for consumer IoT

CISA, on the other hand, plays a crucial role in coordinating cybersecurity efforts across various sectors, including communications. Through initiatives like the Secure by Design framework, CISA provides guidance and resources to organizations to bolster their cybersecurity defenses. By emphasizing proactive measures such as risk assessments, threat modeling, and secure coding practices, CISA empowers organizations to identify and mitigate vulnerabilities early in the development lifecycle, thereby reducing the likelihood of exploitation by malicious actors.

Together, NIST and CISA collaborate closely with industry stakeholders to advance the principles of Secure by Design and foster a culture of cybersecurity awareness and resilience. By promoting best practices, facilitating information sharing, and offering technical assistance, these agencies contribute significantly to enhancing the security posture of the communications sector and safeguarding critical infrastructure from evolving threats.

The ONCD, led by Harry Coker, has emerged as a key player in coordinating and implementing national cybersecurity strategies. Tasked with defending critical infrastructure and coordinating responses to cyber incidents, the ONCD plays a pivotal role in safeguarding the nation's digital assets against a myriad of threats. Through collaboration with government agencies, private sector partners, and international allies, the ONCD works tirelessly to enhance the resilience of the nation's cyber defenses.

Coker's leadership has been instrumental in driving innovation and resilience in cybersecurity practices. By advocating for the adoption of emerging technologies and best practices, such as Secure by Design principles and AI-driven threat detection, the ONCD endeavors to stay ahead of evolving cyber threats and protect the nation's critical infrastructure from potential vulnerabilities. Coker's strong leadership at the ONCD exemplifies a commitment to excellence in cybersecurity and national defense and emphasizes the importance of addressing the complex and evolving cyber threats faced by the communications sector and critical infrastructure as a whole. Through strategic vision, collaboration, and innovation, the ONCD continues to play a vital role in safeguarding the nation's digital infrastructure and bolstering its resilience against cyber threats.

### 3: Artificial Intelligence

Attackers are continuing to develop more sophisticated botnets, using AI and machine learning to evade detection and automate attacks. There are also positive AI uses cases for botnet mitigation, including AI-enabled classification and detection of botnet activity.

#### FOX8 CHATGPT BOTNET

In May 2023, Indiana University Bloomington researchers discovered the Fox8 botnet powered by ChatGPT operating on X and consisting of 1,140 accounts. The bot accounts appeared to use ChatGPT to create and reply to each other's posts. The auto-generated content was apparently intended to entice unsuspecting humans into clicking promotional cryptocurrency website links. Despite the botnet's extensive reach, its use of ChatGPT was not particularly sophisticated. Researchers detected the botnet by searching the platform for the "As an AI language model ..." distinctive phrase often used by ChatGPT when prompted on sensitive topics. Although ChatGPT's usage policy for its AI models prohibits using them for scams or disinformation, the apparent ease with which OpenAI's artificial intelligence was apparently harnessed for the scam suggests more advanced chatbots could potentially be operating other undetected botnets. Social media algorithms are designed to amplify popular posts, regardless of whether that engagement originates from bot accounts. Moreover, the researchers wagered that governments interested in conducting disinformation campaigns are likely already developing and deploying such tools. Researchers have long expressed concerns about the potential for misuse of ChatGPT technology, leading OpenAI to delay the release of a predecessor system over such apprehensions. However, to date, there are few documented examples of large language models being systematically abused at scale. Nonetheless, some political campaigns have begun using AI, with notable figures sharing deep fake videos aimed at undermining their opponents.<sup>22</sup>

On the defensive side, AI has also been used to detect botnets.<sup>23</sup> Looking forward, the advent of AI will enhance both offensive and defensive capabilities for botnet activity.



## Conclusion

In 2023 the communications sector witnessed an alarming increase in threats, particularly from foreign adversaries such as China. FBI Director Christopher Wray's warning to Congress about Chinese hackers targeting US infrastructure, followed by related advisories from CISA, underscored the gravity of the situation. **Notably, Volt Typhoon's infiltration of US critical infrastructure and the subsequent joint efforts by USTelecom members and international law enforcement agencies to disrupt their activities exemplified the magnitude of the threat posed by state-sponsored cyber-espionage groups.** Additionally, the dismantling of botnets like Qakbot and Moobot showcased the collaborative efforts between law enforcement agencies and industry partners to combat cybercrime. As botnets evolve and become more sophisticated, leveraging technologies like AI, the need for robust cybersecurity measures and international cooperation has never been more urgent.

**While it is too early to declare victory or concede defeat, we are delivering serious and debilitating blows to our adversaries, with the hope of deterring future criminal and malicious botnet activity and protecting civilians and critical infrastructure. Moving forward, it is imperative for communications companies and government agencies to remain vigilant and proactive in defending against emerging threats to ensure the integrity and security of global communication networks.**

## Endnotes

- 1 <https://www.prnewswire.com/news-releases/botnets-evolve-as-malware-increases-and-exploits-skyrocket-in-2023-302047892.html>
- 2 <https://www.cisa.gov/resources-tools/resources/identifying-and-mitigating-living-land-techniques>
- 3 <https://www.bleepingcomputer.com/news/security/chinese-hackers-hid-in-us-infrastructure-network-for-5-years/>
- 4 <https://www.bleepingcomputer.com/news/security/chinese-hackers-breach-us-critical-infrastructure-in-stealthy-attacks/>
- 5 <https://www.bleepingcomputer.com/news/security/fbi-disrupts-chinese-botnet-by-wiping-malware-from-infected-routers/>
- 6 <https://www.cisa.gov/news-events/alerts/2024/01/31/cisa-and-fbi-release-secure-design-alert-urging-manufacturers-eliminate-defects-soho-routers>
- 7 <https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/>
- 8 <https://www.axios.com/2023/08/29/fbi-qakbot-botnet-network-ransomware>
- 9 <https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian>
- 10 <https://therecord.media/fbi-takes-down-ipstorm-malware-botnet>
- 11 <https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/>
- 12 <https://securityboulevard.com/2023/10/mirai-botnets-new-wave-hailbotkiraibot-catddos-and-their-fierce-onslaught/>
- 13 <https://www.checkpoint.com/press-releases/april-2023s-most-wanted-malware-qbot-launches-substantial-malspam-campaign-and-mirai-makes-its-return/>
- 14 <https://www.nist.gov/publications/iot-device-cybersecurity-capability-core-baseline>
- 15 <https://csrc.nist.gov/pubs/ir/8425/final>
- 16 <https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-devices>
- 17 <https://csrc.nist.gov/pubs/ir/8259/a/final>
- 18 <https://csrc.nist.gov/pubs/ir/8425/final>
- 19 <https://shop.cta.tech/products/https-cdn-cta-tech-cta-media-media-shop-standards-2020-ansi-cta-2088-a-final-pdf>
- 20 <https://www.iso.org/standard/80136.html>
- 21 <https://kvh31b.p3cdn1.secureserver.net/wp-content/uploads/2021/03/CSDE-2021-Botnet-Report-March-24-2021.pdf>
- 22 <https://www.wired.com/story/chat-gpt-crypto-botnet-scam/>
- 23 <https://www.linkedin.com/pulse/battling-botnets-ai-new-era-cybersecurity-majd-aldeen-masriah/>