CSDE

Council to Secure the Digital Economy

INTERNATIONAL BOTNET AND IOT SECURITY GUIDE 2022

USTELECOM
THE BROADBAND ASSOCIATION

Consumer Technology Association™

CSDE BOTNET Year in Review

THROUGHOUT 2021 AND INTO THE CURRENT YEAR, industry leaders fought back aggressively against botnet attacks and related cyber threats and innovated to bolster defenses against future attacks. Many of the key innovators leading the charge make up the Council to Secure the Digital Economy: Akamai, AT&T, Cisco, Ericsson, IBM, Intel, Lumen, NEC, NTT, Oracle, Panasonic, Samsung, SAP, Telefónica, and Verizon.

Since CSDE first published its guide to fighting botnets and securing IoT, we have seen increased focus on security assurance and technology solutions to combat botnets, holistically, as well as awareness of the importance of equipping devices with baseline security capabilities. A recent report found that in 2021 companies scanned software for vulnerabilities 20 times more often than a decade ago, and they scanned three times as many applications.[1] Moreover, vulnerable libraries have been reduced by two-thirds and the half-life of vulnerabilities within libraries is now three times faster.[2] Technology solutions that help combat botnets evolve continuously and we have seen increased adoption of these capabilities in the market, including in the IoT ecosystem. Automatic onboarding capabilities that remove the need for default passwords, using embedded cryptographic credentials, have developed, and so did the adoption of trusted onboarding mechanisms for IoT Devices.[3]

As technological capabilities advanced, cooperation between industry and law enforcement to take down high-profile botnets has yielded notable results. In early 2021, law enforcement disrupted Emotet — referred to as the “world’s most dangerous malware” by Interpol[4] and Europol[5] — with an international takedown operation. In October, a Russian national was arrested in connection with the TrickBot malware and extradited by the U.S. Department of Justice.[6] These are just some examples of the numerous efforts taking place across the globe to combat the threat of botnets.

Despite these continuing advances, we face challenges as a global connected community. In February 2022, as the geopolitical conflict between Russia and Ukraine escalated, DDoS attacks were launched against Ukrainian government websites[7] and also by hacktivists in defense of Ukraine.[8] Meanwhile, the COVID-19 pandemic’s shift to remote and hybrid work arrangements has drastically expanded the attack surface for botnets. In mid-2021, a team of security researchers found that 51% of organizations reported botnet activity.[9] With IoT devices estimated to reach 30.9 billion by 2025,[10] the potential arsenal of botnets will continue to grow.

CSDE’s recommendations for fighting botnets should be widely adopted in countries across the globe to mitigate against the botnet threat. Below are specific trends that garnered members’ attention and illustrate the changing threat landscape:

Cyclops Blink Botnet

On February 23, the U.S. and U.K. governments issued advisories warning that Russia’s Sandworm hacking group has built a botnet out of firewall devices.[11] Researchers discovered the botnet has been amassing resources since 2019 and appears capable of compiling malware for various types of architectures and firmware besides those it actively exploits.[12] A notable feature of Cyclops Blink is that it persists when a system is rebooted because it is deployed as part of the legitimate firmware update process.

The Sandworm hacking group has previously been implicated in attacking Ukrainian private and government institutions, causing blackouts by disrupting electrical infrastructure, and unleashing NotPetya destructive malware on the world — causing more than 10 billion dollars in damage.[13] For information on how industry leaders can coordinate in case of major attacks on critical infrastructure, including DDoS attacks driven by botnets, see CSDE's Cyber Crisis Report[14] available at CSDE.org.

Mirai Continues Spawning Variants; BotenaGo Source Code Leaks

With many dozens of Mirai variants in existence and new ones constantly being discovered, the notorious IoT botnet family continues to prove its staying power. Mirai's popularity among malicious actors is due, in no small part, to its source code having been leaked back in 2016, enabling hackers of many different skill levels to utilize and modify it as they see fit. The different Mirai variants are controlled by operators who compete among themselves for dominance of vulnerable IoT devices. As can be expected given the technological arms race that botnet operators fight on multiple fronts — against law enforcement and against each other — the newer botnets are increasingly resourceful. Of course, Mirai is far from the only botnet on the IoT attack scene. Mirai faces competition from other botnets such as BoenaGo, Echobot, Gafgyt, and Mozi, among a great number of others.[15]

In January 2022, AT&T Alien Labs reported that the source code of BotenaGo, which shares some similarities to Mirai but is written in a different programming language, was leaked online — meaning it is available for free to any hacker or malware developer.[16] BotenaGo can target potentially millions of IoT devices, and AT&T's researchers warn that "[w]ith only 2,891 lines of code, BotenaGo has the potential to be the starting point for many new variants and new malware families using its source code."[17]

Botnets Exploiting Log4j Vulnerability

The Log4j vulnerability (CVE-2021-44228) — "Log4Shell" — impacts a wide range of systems that make use of Apache Log4j versions 2.0 to 2.14.1. As CSDE noted in its recent paper on Cyber Crisis Response and Handling, Log4Shell "has triggered the highest levels of concern" because of "the likelihood of injected malware in affected systems, and the many reports of malicious scans."[18]

Botnet campaigns are currently exploiting the Log4Shell to infect vulnerable systems. A January 2022 Akamai blog noted that Log4Shell is spreading the infamous Mirai botnet.[19] AT&T's blog highlights a number of botnet families exploiting Log4Shell in addition to Mirai — including Muhstik, Elknot, m8220, SitesLoader, xmrig, and Meterpreter[20]

Cisco Talos Intelligence Group also noted the role of Log4Shell in spreading botnets and expects "many actors with different objectives, ranging from financial to espionage, will rapidly adopt this exploit… to secure access for immediate use, resale or long-term footholds."[21] Early attempts to exploit Log4Shell have frequently involved coin

miners, such as the Kinsing botnet, among a variety of others.[22] Log4Shell will continued to pose a problem for at least months, but quite possibly years.[23]

Ransom DDoS Attacks on the Rise

Ransom DDoS attacks — where malicious actors attempt to extort payment from victims to stop an ongoing DDoS attack or avoid a future DDoS attack — have been on the rise. In Q4 2021, there was 29% year-over-year and 175% quarter-over-quarter increase in these types of attacks.[24] Actors also discovered additional services, such as Voice over IP, where existing countermeasures were not as effective and they had significant success taking some key providers offline such as bandwidth.com and voip.ms; with one actor demanding upward of $4.2 million to stop the attack.[25]

Ransomware attacks in general have become increasingly complex, especially when combined with DDoS attacks. IBM Security Intelligence recently described some of these higher-complexity schemes:[26]

- Attackers steal victim's data before encrypting it and demand two ransoms: one for decrypting the data, another for deleting the stolen data from the attackers' servers.
- Attackers victimize third parties. For example, they may demand ransom victims' clients and suppliers. Or they may target employees, customers, business partners, and others with spear-phishing attacks
- DDoS attacks, often enabled by botnets are used to increase pressure on victims. High-profile ransomware groups such as HelloKitty have been using this technique
- Ransomware such as Yanluowang instructs victims not to contact law enforcement or third parties such as ransomware negotiators. Victims who do not comply with these instructions risk becoming targets of DDoS attacks

Meris Botnet Shatters DDoS Records

The Meris botnet has gained attention of security researchers because it targets routers and networking hardware with great processing power than Mirai's targets — resulting in larger scale attacks. Specifically, Meris infects MikroTik networking gear.

In summer of 2021, Meris was responsible for a DDoS attack that reached 17.2 million requests per second (RPS), which Cloudflare described as "the largest ever reported".[27] Days later, Meris broke this record with a DDoS attack against Yandex that reached 21.8 million RPS.[28] The technique attackers used to launch such a massive DDoS attacks is called HTTP pipelining, which allows the botnet to send multiple requests to a server using a single connection.

Meris has certain limitations. For starters, it relies on a MikroTik vulnerability, which was rapidly patched. However, if a router is already infected, merely updating is not enough to protect the routers. Additional steps are needed such as changing the password, configuring the firewall, and checking for scripts that weren't created by the legitimate user.[29] Another limitation of Meris is that the DDoS technique it uses makes IP spoofing highly unlikely — which means the locations of infected devices are discoverable. However, the Meris botnet uses proxies to hide the attack source.[30]

Despite the limitations of Meris, the botnet has plenty of room to grow. Some researchers estimate the maximum capacity of Meris is about 110 million RPS, which is about five times larger than the current record — leading to speculation that attacks seen so far were "equipment testing events, not meant to take down their targets."[31] It is also conceivable that an as-of-yet unknown zero-day vulnerability could increase the Meris botnet's currently estimated reach. Even if these concerns never manifest, Meris provides a window into potential future threats, as botnets leverage high computational power to carry out attacks.

Mozi Not Dead: Botnets Built to Survive Post-Takedown

When the operator behind the Mozi botnet was arrested in China in summer 2021, some security researchers prematurely proclaimed Mozi was dead.[32] However, as CSDE anticipated in our 2020 Botnet Year in Review, this botnet has tremendous survivability. This is because Mozi is a peer-to-peer (P2P) botnet. P2P botnets distribute control among all nodes on a network, making it much harder for security experts to truly take these botnets down — even after an arrest is made. The only way a botnet like Mozi can disappear permanently is if every one of its targets is updated or altogether replaced. A process that normally takes years. As more P2P botnets are developed, security experts brace for a future where bots — often analogized to zombies — wander through the ecosystem long after their proclaimed "death".

Government Services Targeted

While attribution is still unknown, a DDoS attack launched using a CLDAP reflection vector against Belnet was so successful it knocked nearly the entire Belgium government offline. This not only impacted over 200 Belgium government agencies but interfered with the ability for citizens to reserve time slots for COVID-19 vaccinations.[33] This is an alarming trend that shows the true cost of reflective DDoS attacks and impact they can achieve.[34]

Data Theft and Credential Stuffing Attacks on the Rise

Akamai recently described "a global credential stuffing bonanza" enabled by botnets.[35] Credential stuffing refers to when malicious actors attempt to break into services using credentials stolen during data breaches. Nowadays, malicious actors trade and sell large databases of stolen credentials on the black market. Credential stuffing attacks often target financial services. The trend toward online banking and mobile transactions, accelerated by the pandemic, has incentivized even more of these types of attacks. Verizon's 2021 Data Breach Investigation Report found, however, that the amount of credential stealing botnet breaches targeting information organizations overtook the finance sector last year.[36]

The researchers at Akamai noted that "credential stuffing attracts some of the most sophisticated hackers, resulting in highly sophisticated bots…Sophisticated bots mutate. Many bot management solutions can detect most bots initially, but then lose that ability as the bots start mutating. This happens when attackers see that

you’ve identified their bot and immediately figure out how to circumvent your solution by updating their software. The mutated bots now can avoid the original detection and be deployed again.”[37]

Behavior analysis, one of the advanced capabilities in CSDE’s International Botnet and IoT Security Guide, is one possible way that organizations can keep up with the ever-changing threat of botnets. Behavioral analysis is analogized to the medical profession: a doctor can often tell when someone is sick even before knowing exactly what the problem is.

Conclusion

The challenges posed by botnets are constantly evolving. Industry is engaged in a continuous effort to innovate and outmaneuver highly motivated, well-financed adversaries in collaboration with law enforcement and government partners across the globe. The good news is that many of the trends we are seeing could be mitigated with broader implementation of the guidance CSDE has already published. Therefore, we urge stakeholders in the digital economy to implement the practices necessary to safeguard important interests and bolster security.

Endnotes

[1] https://www.darkreading.com/application-security/vulnerability-scanning-triples-leading-to-two-third-fewer-flaws

[2] Id.

[3] https://www.intel.com/content/www/us/en/developer/tools/secure-device-onboard/overview.html

[4] https://www.tripwire.com/state-of-security/security-data-protection/emotet-botnet-named-most-wanted-malware-for-july-2020/

[5] https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[6] https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal

[7] https://www.zdnet.com/article/ukrainian-govt-sites-banks-disrupted-by-ddos-amid-invasion-fears/

[8] https://www.politico.eu/article/hacktivists-come-to-ukraines-defense/

[9] https://www.fortinet.com/blog/industry-trends/fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware

[10] https://www.zdnet.com/article/mirai-splinter-botnets-dominate-iot-attack-scene/

[11] https://www.cisa.gov/uscert/ncas/alerts/aa22-054a

[12] Id.

[13] https://www.wired.com/story/sandworm-cyclops-blink-hacking-tool/

[14] https://csde.org/projects/ict-mobilization/

[15] https://www.zdnet.com/article/mirai-splinter-botnets-dominate-iot-attack-scene/

[16] https://cybersecurity.att.com/blogs/labs-research/botenago-strike-again-malware-source-code-uploaded-to-github

[17] https://cybersecurity.att.com/blogs/labs-research/botenago-strike-again-malware-source-code-uploaded-to-github

[18] https://csde.org/wp-content/uploads/2022/01/CSDE-Cyber-Handout_Final.pdf

[19] https://www.akamai.com/blog/security/mirai-botnet-abusing-log4j-vulnerability

[20] https://cybersecurity.att.com/blogs/labs-research/global-outbreak-of-log4shell

[21] https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html

[22] https://www.zdnet.com/article/log4j-update-experts-say-log4shell-exploits-will-persist-for-months-if-not-years/

[23] Id.

[24] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/

[25] https://www.bleepingcomputer.com/news/security/bandwidthcom-is-latest-victim-of-ddos-attacks-against-voip-providers/

[26] https://securityintelligence.com/news/hellokitty-ransomware-group-ddos-extortion/

[27] https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/

[28] https://threatpost.com/yandex-meris-botnet/169368/

[29] https://blog.mikrotik.com/security/meris-botnet.html

[30] https://blog.cloudflare.com/meris-botnet/

[31] https://cybernews.com/security/weve-seen-just-the-tip-of-the-meris-botnet-iceberg/

[32] https://securityboulevard.com/2022/01/2021-year-in-review-denial-of-service/

[33] https://news.softpedia.com/news/belgium-was-hit-by-a-massive-cyberattack-532812.shtml

[34] https://blog.lumen.com/tracking-udp-reflectors-for-a-safer-internet/

[35] https://www.akamai.com/blog/trends/keeping-up-with-the-botnets

[36] https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf

[37] https://www.akamai.com/blog/trends/keeping-up-with-the-botnets

For additional information on the Council to Secure the Digital Economy (securingdigitaleconomy.org) or information on this report, please contact:

Robert Mayer
Senior Vice President - Cybersecurity and Innovation
USTelecom
rmayer@ustelecom.org

Mike Bergman
Vice President - Technology & Standards
Consumer Technology Association
mbergman@cta.tech

CSDE
Council to Secure the
Digital Economy