Dataminr

WHITEPAPER

Weaponizing the Neutral Web

Reviewing Adversary Botnets for Cyber Operations

Joseph Slowik, Director, Cybersecurity Alerting Strategy

Introduction

Offensive and defensive cyber operations, much like their kinetic associations, remain in a constant state of co-development and responsive evolution. Within the cyber realm, the past ten years have witnessed an explosion in both offensive tradecraft and defensive countermeasures, and with this, various shifts in operations. With every defensive response to adversary activity, a reaction emerges to overcome mitigations and controls.

The above evolution is well-tracked in initial access and on-host operations. For example, with respect to the former, the past decade has witnessed first an emphasis on system vulnerability exploitation for access, then a shift towards end-user targeting via mechanisms such as phishing, only for exploitation to roar back as a critical ingress mechanism in the early 2020s.[1] For the latter, adversaries from state-directed actors to criminal entities increasingly migrate from custom, specific tools and malware to "living off the land" binaries (LOLBINs) and similar mechanisms in response to the increasing deployment of endpoint detection and response (EDR) in host visibility.[2]

Aligned with the above observations, cyber defense has rapidly evolved to incorporate the rapid sharing and actioning of technical indicators (frequently referred to as "indicators of compromise," or IOCs) for defensive purposes. For example, an entity may rapidly share information about a current intrusion or related activity with peers or other entities to allow other organizations to rapidly move toward alerting or blocking on the items. Examples of such sharing include technical indicators such as domain names or IP addresses associated with command and control (C2) activity. While this approach has significant limitations,[3] increased and rapid information sharing has nonetheless allowed for various organizations to quickly identify or mitigate against threat actors based on effective communication.

Such activity does not take place in a vacuum. As seen with endpoint and initial intrusion trends, threat actors have not remained static in the face of defender responses. To avoid effective indicator-based defenses, threat actors increasingly work in an "indicator-less" fashion,

[1] "2024 Data Breach Investigations Report," Verizon Business, accessed November 2, 2024, https://www.verizon.com/business/resources/T5d7/reports/2024-dbir-data-breach-investigations-report.pdf

[2] "Identifying and Mitigating Living Off the Land Techniques," US Cybersecurity and Infrastructure Security Agency (CISA), accessed November 2, 2024, https://www.cisa.gov/sites/default/files/2024-02/Joint-Guidance-Identifying-and-Mitigating-LOTL_V3508c.pdf

[3] "The Pyramid of Pain," David Bianco, accessed November 2, 2024, https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

clearly seen in LOLBIN methodologies but also in network infrastructure. Whereas threat actors may have traditionally created network infrastructure in manners that could be tracked or that reveal patterns,[4] [5] various entities now increasingly leverage third-party, compromised infrastructure to proxy communications in a way that makes traditional indicator-centric defense and tracking difficult.

The result of this activity is the increasing weaponization of the "neutral" Internet. Any device connected to and accessible from the Internet is now a potential node for incorporation into malicious infrastructure. Such infrastructure may be used in persistent fashion, or be leveraged in a more ephemeral way allowing for adversaries to rapidly move hosts to confound defenders and evade static alerting and blocking methodologies. Additionally, such actions raise issues as to how to respond to activity, as taking direct action against maliciously-used infrastructure can also impact the legitimate users of otherwise innocent network space. Defenders face a challenge in how to respond to adversary C2 migration – but this problem has existed for quite some time.

Defining Botnets and Reviewing Their Legacy

Botnets are roughly defined as networks of computers infected by malware or some other controlling program that allow a single party to control certain actions on or through infected devices.[6] Historically, these networks of compromised machines have been used for purposes ranging from spam origination or relay to distributed denial of service (DDoS) activity. The value proposition of botnets historically has been scale, in allowing a controlling entity to rapidly expand their footprint and increase the scope and velocity of malicious campaigns.

Proxied communication or the use of "neutral" devices or servers for malicious purposes following compromise is not new. The first widely acknowledged and publicly recognized botnet emerged roughly concurrent with the emergence of the popular Internet: the EarthLink spammer botnet from 2000.

[4] "A case study tracking adversary infrastructure through SSL certificate use featuring Fancy Bear/APT28/Sofacy," ThreatConnect, accessed November 2 2024, https://threatconnect.com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/

[5] "Analyzing Network Infrastructure as Composite Objects," Joe Slowik, DomainTools, accessed November 2 2024

[6] "What is a Botnet?" Palo Alto Networks, accessed November 2 2024, https://www.paloaltonetworks.com/cyberpedia/what-is-botnet

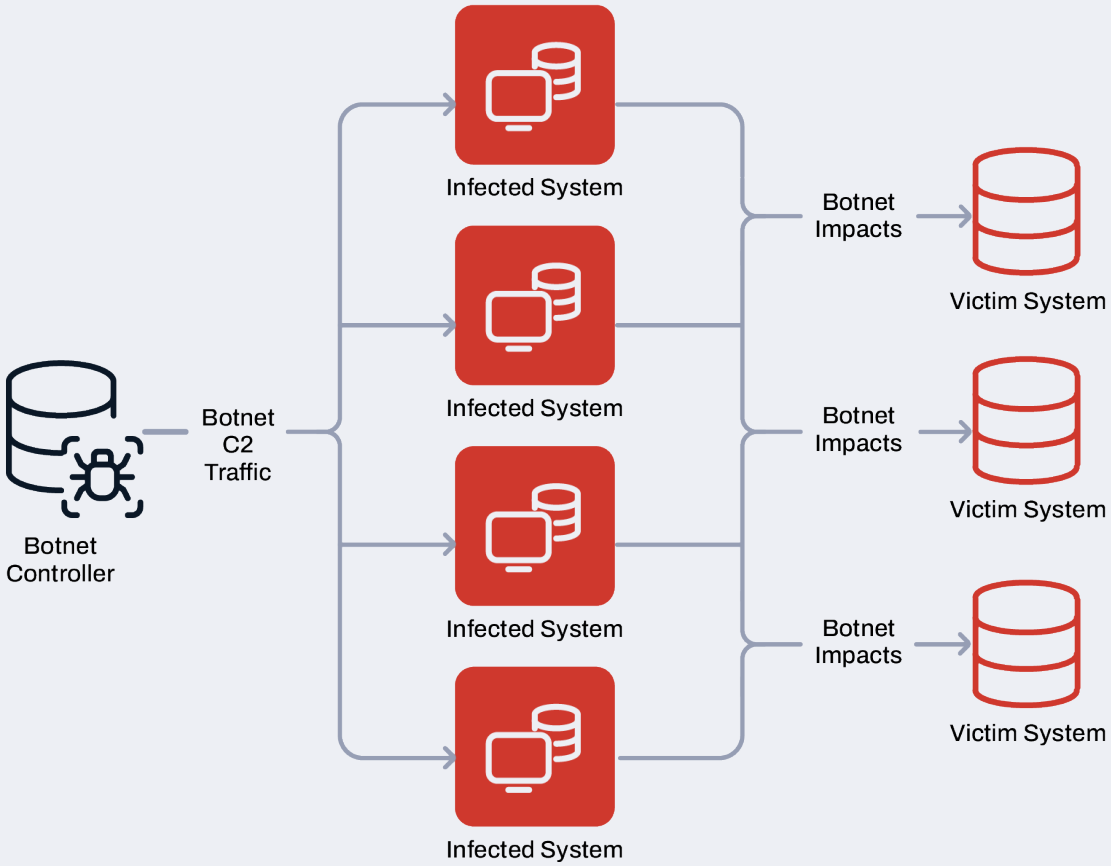

Figure 1: Simplified Botnet Example

This botnet was used for typical criminal purposes such as collecting credit card and other financial information by leveraging compromised systems to send spam messages.[7] [8] In this sense, the EarthLink spammer hews to a common conception of botnet activity: leveraging compromised systems to further various sorts of monetizing activity for criminal purposes.

Criminal botnets would continue to exist and expand with multiple monetization strategies emerging to leverage these distributed networks. Examples such as the Zeus botnet to multiple dropper-based botnets used for ransomware staging and operations emerged through the present to continue this element of botnet operations, coopting end user machines into networks of criminal activity.[9] [10]

However, not long after the emergence of botnets as a mechanism for scaled, amplified cyber operations for criminal purposes, other entities noticed the possibilities inherent in such methodology. Thus emerged increased weaponization of perceived "commodity" or "primitive" mechanisms for the pursuit of more interesting, strategic objectives.

[7] "9 of History's Notable Botnet Attacks," Human Security White Ops, accessed November 2 2024, https://www.humansecurity.com/learn/blog/9-of-the-most-notable-botnets

[8] "Bots Gone Bad, An ascending DDoS threat," Gary Sockrider, Netscout, accessed November 2, 2024, https://www.netscout.com/blog/bots-gone-bad

[9] "US Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator," US Department of Justice, accessed November 3, 2024, https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware

[10] "Largest ever operation against botnets hits dropper malware ecosystem," Europol, accessed November 2, 2024, https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

The Emergence of State-Directed Botnet Activity

On April 27, 2007, various external-facing websites and other resources in Estonia experienced degrees of disruption or denial of service, not long after Estonian authorities relocated a monument to Soviet troops from the Second World War from a high-visibility location in Tallinn to a military cemetery.[11] [12] While some of the activity in question appears linked to specific individuals in Russia, the overwhelming volume of activity for the likely politically-motivated disruptive event appears to have emerged from botnets managed by entities sympathetic to Russian views during this crisis.[13]

While Russian state direction of the Estonian activity remains unproven, subsequent activity in 2008 against Georgia appears more firmly linked with Russian state control. In August 2008, following Georgian military responses to Russian provocations, Russia initiated an invasion of the Georgian region of South Ossetia. Concurrent (and potentially coordinated) with physical hostilities, Georgian internet resources faced an onslaught similar to that experienced by Estonia in 2007.[14] Like Estonia, Georgian resources were largely rendered inert or inaccessible due to DDoS activity emanating from various botnets.

The two events above represent instances where a state entity at minimum benefited from, if not actively controlled and directed, botnet operations for DDoS activity against civilian targets. In both instances, government and civilian communications were severely impacted resulting in loss of services and degradation in information dissemination at times of high political tension, and in the case of Georgia, active, physical hostilities. While the overall impact of these events is debatable compared to traditional kinetic operations, the disruptive element introduced through these operations in conjunction with other information operations effectively "boosted" these events in terms of psychological impact on respective populations.[15]

[11] "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," Rain Ottis, Cooperative Cyber Defense Centre of Excellence https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[12] Herzog, Stephen, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Journal of Strategic Security 4 no. 2 (2011), 49-60

[13] "2007 cyber attacks on Estonia," NATO, accessed November 4, 2024, https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

[14] Hollis, Davis, "Cyberwar Case Study: Georgia 2008, Small Wars Journal (2011)

[15] Slowik, Joseph. "Full-Spectrum Information Operations for Critical Infrastructure Attacks." Presentation, CYBERWARCON, Arlington, VA, November 2019. (https://www.youtube.com/watch?v=n7XqxRXwFZ4)

Following these events in the Russian "near abroad," another botnet-boosted DDoS attack took place, this time against the financial sector in the United States from late 2011 to early 2013.[16] The incidents resulted in tens of millions of dollars in damages and mitigation costs. These events were linked to Iranian government proxies, specifically individuals working for two Islamic Revolutionary Guard Corps-affiliated companies, ITSecTeam and Mersad Company.[17] While not technically sophisticated, the events represent a likely state-directed effort to inflict costs on a key element of U.S. critical infrastructure during a time of heightened U.S.-Iran tensions.

While the U.S. financial sector events were largely mitigated, such efforts came at significant cost in boosting the ability of resources to handle ever-higher volumes of traffic. More "root cause" efforts to combat these botnets were simply unavailable as the primary mechanisms for defeating these networks would be either elimination of the transmitting nodes or severing links to the botnet controllers. The former would involve interacting with notionally innocent devices coopted into the botnet, with the potential for unanticipated and unwanted side effects, while the latter might violate rules of engagement in attacking or mitigating infrastructure in foreign (and hostile) states.

Throughout these examples, the scale of botnets was leveraged to enable disruption and induce a denial of service condition for targeted (often critical) infrastructure. While potentially shrugged off as "just DDoS activity," such operations can significantly impair communication and government functionality in times of crisis. As a result, it is not surprising that likely state-directed DDoS activity leveraging botnets for signal amplification has continued through the present, as seen in Russian actions targeting Ukraine prior to and following the most recent phase of hostilities in 2022.[18]

[16] "US indicts Iranians for hacking dozens of banks, New York dam," Dustin Volz and Jim Finkle, Reuters, accessed November 3, 2024, https://www.reuters.com/article/technology/us-indicts-iranians-for-hacking-dozens-of-banks-new-york-dam-idUSKCN0WQ1JF/

[17] "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against US Financial Sector," US Department of Justice, accessed November 3, 2024, https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[18] "Attribution of Russia's Malicious Cyber Activity Against Ukraine," Antony J. Blinken, US Department of State, accessed November 4, 2024, https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/

Expanding Attack Surface

The campaigns against Estonia, Georgia, and the U.S. financial sector leveraged traditional networks of compromised computers to achieve scale and mass. However, the potential scope of botnets began to increase dramatically around the same time as these events due to the increasing connectivity of various devices, appliances, and other equipment as part of the emerging "Internet of Things" (IoT) ecosystem. Frequently based on outdated operating systems, running vulnerable software, or using hard-coded credentials enabling third parties to access exposed devices, IoT botnets rapidly emerged to take advantage of systematic weaknesses.

Most notable in this space is the Mirai botnet. First emerging in 2016, the Mirai botnet focused on IoT device compromise to build botnets of hundreds of thousands of endpoints including DVRs, IP cameras, small-office home-office (SOHO) networking equipment, and similar devices.[19] The Mirai botnet was rapidly weaponized for extortion operations via DDoS activity against commercial entities. While the original creators of the Mirai botnet were arrested in 2017,[20] variants of Mirai operate to this day for various objectives given the permissiveness of the IoT environment for malicious activity. The most notable example at the time of writing is the Kimwolf botnet, responsible for infecting millions of devices yet still using portions of the original Mirai framework.[21]

Like the original botnets, IoT botnets initially emerged for criminal operations, particularly "DDoS-for-hire" activity for extortion purposes. However, it would not take very long for other entities to take note of the opportunities available in IoT and other (largely residential) devices featuring less defender and administrator visibility, poor configuration or vulnerable software, and other enticing factors in building networks of compromised systems.

[19] M. Antonakakis et al, "Understanding the Mirai Botnet," Proceedings of the 26th USENIX Security Symposium, 1093-1110. https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

[20] "Justice Department Announces Charges and Guilty Pleas in Three Computer Crime Cases Involving Significant DDoS Attacks," US Department of Justice, accessed November 3, 2024, https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

[21] "What is the Aisuru-Kimwolf botnet?," Cloudflare, accessed February 15, 2026, https://www.cloudflare.com/learning/ddos/glossary/aisuru-kimwolf-botnet/

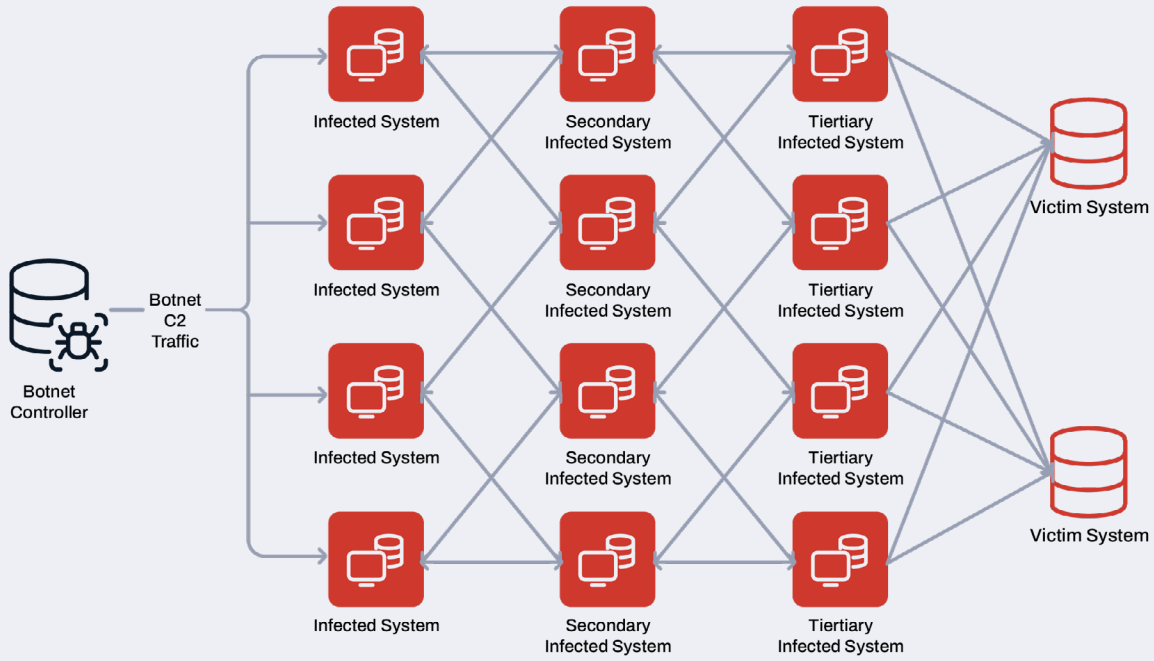

Figure 2: Complex Botnet Example

Current Botnet Operations

Since their emergence, botnet operations have grown in scope and complexity. Notably for state-sponsored or -directed operations are more complex frameworks leveraging multiple "hops" between infrastructure in the form of proxy chains to further complicate tracing network traffic from victims to originating controllers. The benefits of this more complicated setup are obscuring controlling infrastructure from identification (and disruption) while also marshalling multiple, sacrificial endpoints in the "neutral web" for use as traffic relays.

At times referred to as "operational relay boxes" or "ORBs," these more complicated botnets will blend various systems into a mesh network, combining features of traditional botnets with virtual private network (VPN) functionality.[22] Although not replacing more traditional botnet topologies, ORB-like networks are increasingly common for complicated espionage and intrusion campaigns associated with state-sponsored or -directed operations.

Thus, the current landscape of botnet operations continues to leverage "neutral" or otherwise benign devices for malicious purposes, but doing so in increasingly complicated fashion. As a result, the ability to trace back communication and map these environments becomes increasingly difficult, especially as threat actors have become increasingly adept in rotating infrastructure so that nodes are ephemeral in their use, swapped out for alternatives before defenders can identify and map links.

These advantages and applications have led to various entities migrating operations to proxy networks of varying degrees of sophistication. Moving beyond DDoS activity, threat actors observe the opportunities in C2 hardening and obfuscation, building both more resilient and deniable platforms for various operations.

[22] "An Introduction to Operational Relay Box (ORB) Networks - Unpatched, Forgotten, and Obscured," S2 Research Team, Team Cymru, accessed November 3, 2024, https://www.team-cymru.com/post/an-introduction-to-operational-relay-box-orb-networks-unpatched-forgotten-and-obscured

Russian Operations: VPNFilter and Cyclops Blink

In May 2018, public reporting emerged on a malware family referred to as "VPNFilter." Targeting a variety of SOHO devices and network attached storage (NAS) appliances, VPNFilter compromised up to a half million endpoints across over 50 countries at the time of reporting.[23] VPNFilter notably combined stealthy intrusion, intelligence collection, and persistence mechanisms on victim devices with the ability of herding infected devices into coordinated action, either for tunneling communication for deniability or executing a built-in "kill" command for potential widespread disruption.

Concurrent with public disclosure, the U.S. Federal Bureau of Investigation (FBI) announced a takedown effort targeting VPNFilter.[24] This effort leveraged a take-over of domains associated with VPNFilter C2 infrastructure to redirect communication to FBI-controlled devices, allowing for victim identification. As such, the takedown left actual device remediation to end users and operators following disclosure to them by cooperating parties, emphasizing the difficulty in combatting botnets since they are effectively installed on "innocent" devices across multiple countries and locations.

Based on these considerations, it is unsurprising that researchers identified continued VPNFilter activity over two years after the initial takedown campaign.[25] Due to the reliance on end-users to remediate devices (including equipment such as ISP-provided networking gear over which end-users may have little if any ability to operate or control), "latent infections" persisted enabling VPNFilter controllers to regain access to some devices.

While VPNFilter infections persisted, the entity behind this botnet (assessed by various intelligence agencies to ultimately be the Russia-linked Sandworm threat actor) retooled, leading to the discovery of a replacement malware called Cyclops Blink in 2022.[26]

[23] "New VPNFilter malware targets at least 500K networking devices worldwide," William Largent, Cisco Talos, accessed November 4, 2024, https://blog.talosintelligence.com/vpnfilter/

[24] "Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," US Department of Justice, accessed November 4, 2024, https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected

[25] "VPNFilter Two Years Later: Routers Still Compromised," Stephen Hilt & Fernando Merces, TrendMicro, accessed November 4, 2024, https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html

[26] "New Sandworm Malware Cyclops Blink Replaces VPNFilter," US Cybersecurity and Infrastructure Security Agency, accessed November 4, 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-054a

Assessed to be active since 2019 and emerging as a replacement for VPNFilter, Cyclops Blink continued the modular nature of VPNFilter but focused infections initially on WatchGuard networking equipment. Subsequent research identified Cyclops Blink variants targeting other SOHO networking gear as well.[27]

Like VPNFilter, Cyclops Blink was the subject of an FBI takedown operation shortly after initial public disclosure.[28] The disruption again focused initially on the C2 infrastructure managing the bot infections rather than remediating the bots themselves, leaving this to the owners of infected devices. However, following the initial March 2022 takedown, FBI officials acknowledged that initial actions failed resulting in something surprising and more robust.

Based on the Department of Justice's press release, it appears the FBI directly communicated with intermediate controller devices within the Cyclops Blink botnet, removed the relevant malware, and applied (non-persistent) device configuration changes to prevent reinfection.[29]

While not directly communicating with individual "bots" at the very end of the communication chain, this action represents an escalation in takedown operations against ostensibly "neutral" devices to impair the operation of an adversary-controlled communication network.

Following Cyclops Blink disruption, public reporting on Russian-managed botnets decreased. However, botnet applications still appear to be robust, with a variety of amplified DDoS actions affecting Ukraine (and supporting countries) from early 2022 onward.[30]

Additionally, while VPNFilter and Cyclops Blink related to Sandworm (the public term for cyber operations emanating from the GRU's Unit 74455), other Russian-linked entities such as APT28 (a public term for cyber operations emanating from the GRU's Unit 26165) have also leveraged widespread exploitation of SOHO devices to build botnets for follow-on activity.[31] Thus botnet operations, tuned to intelligence collection and C2 proxying along with directly disruptive operations such as DDoS activity, appear to be a foundational element of Russian-nexus threat actors through the present.

[27] "Cyclops Blink Sets Sights on Asus Routers," Feike Hacquebord, Stephen Hilt, & Fernando Merces, TrendMicro, accessed November 4, 2024, https://www.trendmicro.com/en_us/research/22/c/cyclops-blink-sets-sights-on-asus-routers--.html

[28] "Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)," US Department of Justice, accessed November 4, 2024,

[29] "Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)."

[30] "Attribution of Russia's Malicious Cyber Activity Against Ukraine."

[31] "Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU)," US Department of Justice, accessed November 4, 2024, https://www.justice.gov/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian

Volt Typhoon and PRC-Linked Proxy Networks

Unlike Russian-related (or directed) operations, there is no substantial documented evidence of state-directed botnet-based disruptive activity linked to the People's Republic of China (PRC). While there have been DDoS actions against entities in Taiwan and elsewhere over the years, these appear to be more "patriotic" in origin than explicitly state-controlled and directed. While there may be no Estonia or Georgia event related to PRC weaponization of botnets, the last several years have identified extensive investment by PRC-associated threat actors in botnets used for proxy network purposes.

Multiple PRC-linked threat actors are assessed to leverage botnets as proxy networks for engaging in cyber operations. Notably, there is an apparent division of labor between the entities using these networks to facilitate operations, and the entities responsible for building and maintaining the communication environments.[32] [33] For example, U.S. government actions worked to disrupt a botnet under the control of an entity labeled Flax Typhoon, but where the named entity (linked to PRC entity Integrity Technology Group) was merely building out and providing access to this network for other malicious activity.[34] As such there is a complex and difficult to untangle ecosystem of operations and relationships between infrastructure providers and infrastructure users or clients.

Among the most notable instances of botnet-based proxy network use associated with PRC threat actors are activities linked to an entity referred to as Volt Typhoon.[35] This entity is linked to multiple proxy networks to facilitate initial access operations targeting critical infrastructure entities in the U.S. and elsewhere, such as the KV Botnet.[36]

---

[32] "IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders," Michael Raggi, Mandiant, accessed November 6, 2024, https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

[33] "Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network," Microsoft Threat Intelligence, accessed November 8, 2024, https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/

[34] "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers," US Department of Justice, accessed November 11, 2024, https://www.justice.gov/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

[35] "Determining Volt Typhoon Next Steps & Defensive Responses," Joseph Slowik, Dataminr, accessed February 15, 2026.

[36] "Routers Roasting on an Open Firewall: the KV-botnet Investigation," Black Lotus Labs by Lumen, accessed November 8, 2024, https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/

This botnet was assessed by U.S. officials to facilitate Volt Typhoon operations, leading to a disruption effort in late 2023 and early 2024.[37] [38] Consisting mostly of end-of-life SOHO routers, the KV Botnet takedown went further than earlier botnet disruption events in that the FBI actively removed malware from devices and disconnected devices from botnet controllers. While the KV Botnet may have recovered to some degree and Volt Typhoon-related actions continue to leverage botnets for proxying purposes,[39] [40] the perceived threat of Volt Typhoon actions against U.S. critical infrastructure networks appears to have prompted a far more active and intrusive response.

Volt Typhoon (and related) operations are perceived in U.S. defense and intelligence circles as uniquely threatening as initial target and access development for potential future disruptive activity against critical infrastructure. U.S. officials have consistently labeled Volt Typhoon a unique and concerning threat to U.S. national security, with the possibility that this entity may be preparing the way for inducing "societal panic" through its operations.[41] As such, this PRC-linked group is assessed to be a direct threat to U.S. national security whereas previous Russian-linked operations such as Cyclops Blink appear to be assessed as tangential or non-critical to direct U.S. interests. This perception has likely driven a far more active pursuit of Volt Typhoon infrastructure, such as the attempted KV Botnet takedown. But as noted above, such actions appear to be ephemeral in nature as Volt Typhoon (or, more accurately, the entities through which Volt Typhoon sources proxy infrastructure) has rapidly reconstituted communication networks in response to disruption.

Nonetheless, the willingness of authorities to engage directly with the "neutral web" supporting and sustaining these botnets signals a shift in perspective. Whereas the Iranian entities launching DDoS attacks against the U.S. financial sector acted with apparent impunity based on public reporting, the various botnets enabling Volt Typhoon operations have faced a far more active and provocative response. While the actual efficacy of this response is debatable, the willingness to directly intervene and actively modify devices coopted into malicious proxy networks represents a change, one that is arguably necessary to combat these networks but also with significant risks should remediating actions result in device malfunction or similar adverse impact.

[37] "Court-Authorized Operation Removed Malware from US-Based Victim Routers and Took Steps to Prevent Reinfection," US Department of Justice, accessed November 11, 2024, https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical

[38] "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to US Critical Infrastructure," US Cyber Security & Infrastructure Security Agency (CISA) et al, accessed November 11, 2024, https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

[39] "KV-Botnet: Don't call it a Comeback," Black Lotus Labs by Lumen, accessed November 11, 2024, https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/

[40] "Taking the Crossroads: The Versa Director Zero-Day Exploitation," Black Lotus Labs by Lumen, accessed November 11, 2024, https://blog.lumen.com/taking-the-crossroads-the-versa-director-zero-day-exploitation/

[41] "Any number given of Volt Typhoon victims 'likely an underestimate,' CISA says," Jonathan Grieg & Martin Matishak, The Record, accessed November 11, 2024, https://therecord.media/volt-typhoon-targets-underestimated-cisa-says

Botnet Identification and Defense

The increasingly aggressive actions by authorities against botnets, especially proxy networks, combined with rapid network recovery highlights both the criticality of responding to these networks and the difficulty in doing so. Furthermore, botnets present interesting defensive problems because of their weaponization of ostensibly neutral (or benign) infrastructure for malicious purposes.

Acting directly against botnet and proxy relays raises significant legal (and potentially ethical) questions. For example, if the FBI's KV Botnet takedown resulted in the "bricking" of victim systems at scale, very interesting questions concerning fault, liability, and responsibility would emerge, along with horrific public relations issues. Yet the alternative of botnet controller targeting is inhibited by the increasing complexity of proxy networks and similar infrastructures, making target identification increasingly difficult without potentially divulging sources and methods or escalating matters to more direct disruptive actions.

Nonetheless, options exist that network defenders and asset owners must consider, along with national and legal authorities, to counteract these networks. While the cybercrime element of botnet use is increasingly expensive and disruptive, the use of botnet-like infrastructure by state-directed operations targeting entities in critical infrastructure or government represents a potentially existential problem. As a result, "something" must be done to counteract these networks, pushing beyond traditional cyber actions such as indicator sharing to more robust actions that can adapt alongside the creation and evolution of proxy networks.

Botnet Defense and Mitigation

The most effective mechanism to defend against or mitigate botnet operations is to prevent their formation in the first place. The profusion of SOHO network device and IoT botnets for both criminal and state-directed operations is founded upon easily accessing vulnerable, unpatched, or otherwise insecure devices. Until this fundamental issue is addressed, botnet defense will continue to represent a Sisyphean task.

Initiatives such as the U.S. government's Secure by Design push attempt to address these items from a "forward looking" perspective for future or in-development applications.[42] Alternatively, efforts such as the European Union's NIS2 Directive extends prior guidance for critical sectors to a much broader space to include items such as regulatory actions to include actions such as mandatory patch management.[43]

[42] "Secure by Design," US CISA, accessed November 11, 2024, https://www.cisa.gov/securebydesign

[43] "NIS2 Directive: securing network and information systems," European Commission, accessed February 15 2026, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

These efforts are laudable in attempting to drive improved development and management practices to close off multiple pathways to device subversion or exploitation. Given the increasing number of identified and weaponized vulnerabilities in external-facing applications and devices, and the speed at which identified vulnerabilities are weaponized, such action is not merely desirable but necessary to combat the botnet problem.

Unfortunately, efforts such as Secure by Design, even if achieved, will do little to impact the long-tail of legacy systems and unpatched (or effectively "unpatchable") devices at the mercy of adversaries. The profusion of IoT devices and lightly (if ever) managed SOHO networking gear has provided a robust landscape for malicious actors to operate within, as these devices have lengthy lifespans and often feature little support or little effort to apply updates when they are available. As seen in the reconstitution of botnets such as VPNFilter infections and the KV Botnet, even increasingly robust and aggressive takedown actions will fail if underlying vulnerabilities and systemic weaknesses are not addressed.

A future-oriented policy towards designing and deploying more secure devices is necessary to reduce the scope of future botnet concerns. Essentially, a combination of technical and potentially legal levers must be used to "drain the swamp" of persistent vulnerability that allows for botnets to so easily emerge. Controversially, such actions may include greater responsibility (or recognition of liability) on the part of asset owners, even for residential devices, when these items are coopted into malicious networks through inattention or negligence.

Even if achieved, which would be a daunting task given legal and other hurdles, this effort of Secure by Design or even imposing penalties on various infrastructure owners will fail to address near and immediate term problems. The sheer volume of existing, vulnerable equipment provides adversaries plenty of targets for potential operations. As a result, future preventative actions must be combined with other more immediate strategies to address issues as they exist today.

Counter-Botnet Operations

Given the cost of operations facilitated by botnets, from ransomware to items with potential national security implications, waiting on long-term ecosystem changes to reduce the number of vulnerable devices in a permissive environment is unacceptable. More active strategies are required to counter the use and creation of botnets for a variety of purposes. By applying a mixture of steadily improving product security and active counter-botnet operations, immediate and longer term security concerns can be addressed together.

As seen in the KV Botnet takedown, authorities are increasingly able and willing to actively counter botnets by removing tools and similar actions. However, these actions are notable as they still represent the minority of events compared to more traditional domain capture or infrastructure sink-holing for botnet takedown operations. The latter may be reasonably effective for a time, but the resurgence of multiple botnets, both criminal and state-sponsored, after such disruption shows the limited utility of such actions.

Critical to this discussion is the area where botnets operate: on devices that are also victims (if intermediate ones) of the botnet controllers. The weaponization of "neutral" devices for malicious purposes presents significant problems in scoping the possibilities of counter-botnet operations. As seen in the KV Botnet example, action is possible, but the U.S. government announcement emphasized significant testing and other considerations (including making no changes to devices that would survive a reboot) as part of this operation.[44]

[44] "Court-Authorized Operation Removed Malware from US-Based Victim Routers and Took Steps to Prevent Reinfection."

Had this action resulted in disruption or even damage to victim devices, even if they had been (unwillingly) part of an adversary's proxy communication network, the legal (as well as ethical) implications would be very interesting. Such actions become more interesting when the victim devices are outside of the jurisdiction of the acting entity – for example, if the botnet devices are in another country.

The above represent real and thorny problems, but they are issues that must be addressed. Given that botnet operations have become a scourge across the connected world, stakeholders in their eradication should work together to develop norms and best practices for how to actively counter and neuter such networks to prevent greater harm. In this sense, consensus must be built not only within jurisdictions such as the U.S., but also across countries and blocs identifying rules and norms for offensive remediation of botnet nodes.

Such discussions can and must deal with the risk of inadvertent device harm and similar consequences, as well as identifying when an entity can start engaging in counter-botnet operations that cross jurisdictions.

For example, while a legal and government entity forcibly remediating devices within its own jurisdiction may be complex and potentially problematic, it also takes place within a well-defined Westphalian norm of local law enforcement and security decision making. Extending these actions to incorporate devices that are impacting that jurisdiction but reside outside it presents a very complex case.

Should the responding jurisdiction first gain the positive assent of the second before acting? If so, how could this information be shared, and what would be the potential risks for divulging critical information that may be captured by a hostile entity when dealing with state-directed efforts? If the activity concerns access or attacks on critical infrastructure, can an entity be justified in acting against botnet nodes outside of its jurisdiction unilaterally for reasons of self-defense?

None of the above are easy questions to answer – but we are long past the point when such items must be decided. Given the long-term nature of reducing the possibility of botnet formation, active, offensive counter-botnet operations are a necessity to reduce the twin harms of significant financial loss due to criminal activity and potential societal disruption from state-sponsored entities using complex proxy networks.

Dataminr

Conclusions

Botnets are a persistent problem in information security concerns, but their use and application have increasing national security implications as well. Some of the original "cyber warfare" examples in public reporting concern the use of botnets to enable DDoS activity against government and critical infrastructure targets. Since these events, adversaries have become only more aggressive in weaponizing neutral systems to enable actions against victims for either financial or strategic purposes.

Unfortunately, the problem of botnet use remains difficult because of the emphasis of weaponizing neutral systems to enable subsequent attacks. As a result, botnet mitigations place defenders in a position where an otherwise justifiable action to mitigate a threat may end up doing harm to an otherwise innocent entity. Such concerns are very real and require consideration, but further review of the potential harm involved in such networks (particularly those associated with entities like Volt Typhoon or Sandworm) indicate that greater flexibility is required.

Countering the threat of botnets used for strategic cyber operations thus demands greater willingness to actively engage the neutral web. While long-term solutions must also be considered to effectively build more robust and defensible systems, immediate concerns increasingly justify a more active posture with respect to these networks. Relevant leaders, policy makers, and decision makers are therefore urged to identify the means and guidance necessary to facilitate more active botnet disruption in the face of increasingly aggressive adversary actions.