04

Botnets Multiply and Level Up

NETSCOUT

Malware and infected bots are used for everything from stealing passwords to launching some of the most disruptive network-based attacks in history. Since their discovery in the 1990s, malware-infected computing resources known as bots have plagued network-connected resources.

Botnets are collections of these bots, and they have grown at a staggering pace. Unfortunately, as technology has improved and innovated, threat actors have as well, scaling botnets in terms of both size and capability.

THE NETSCOUT PERSPECTIVE

In 1H 2022 alone, NETSCOUT's global honeypot network observed more than 67 million connections from 608,000 unique IP addresses, spanning 13,000 ASNs, 30,000 organizations, and 165 countries. Although those numbers are staggering, they don't come as a shock to us. In fact, we previously reported that direct-path attacks were becoming a tool of choice for adversaries—a fact further established by an 11 percent increase in direct-path attacks from 2H 2021 to 1H 2022. This growth largely is due to innovation in the botnet landscape.

In 1H 2022 NETSCOUT observed...

67,000,000 **Total Connections**

608,000 **Unique IP addresses** → 13,000 **ASNs** → 30,000 **Organizations** → 165 **Countries**

KEY FINDINGS

1. Botnet proliferation is growing at an alarming rate: We've gone from tracking tens of thousands to tracking more than 400,000 high-confidence botted nodes.

2. The continuous move to direct-path attacks sourced from botnets translated to more application-layer attacks, a trend on the rise since early last year.

3. Like Meris, Dvinis, and Killnet, Mirai recently integrated the use of SOCKS5 proxy into its communication protocol in a move likely meant to thwart analysis and mitigation of compromised nodes.

Botnets and Their Impact

In the past year, NETSCOUT has noted an uptick in adversaries using DDoS-for-hire providers as part of a triple threat. In these attacks, adversaries exfiltrate data, use ransomware to lock the target out of its own data, and then launch DDoS attacks in hopes of receiving cryptocurrency payouts—meanwhile wreaking havoc on the organization's networks and reputation. These attacks are increasing in frequency driven by botnets being used to take advantage of direct-path attack surfaces.

Layer 7 Direct Path Attacks

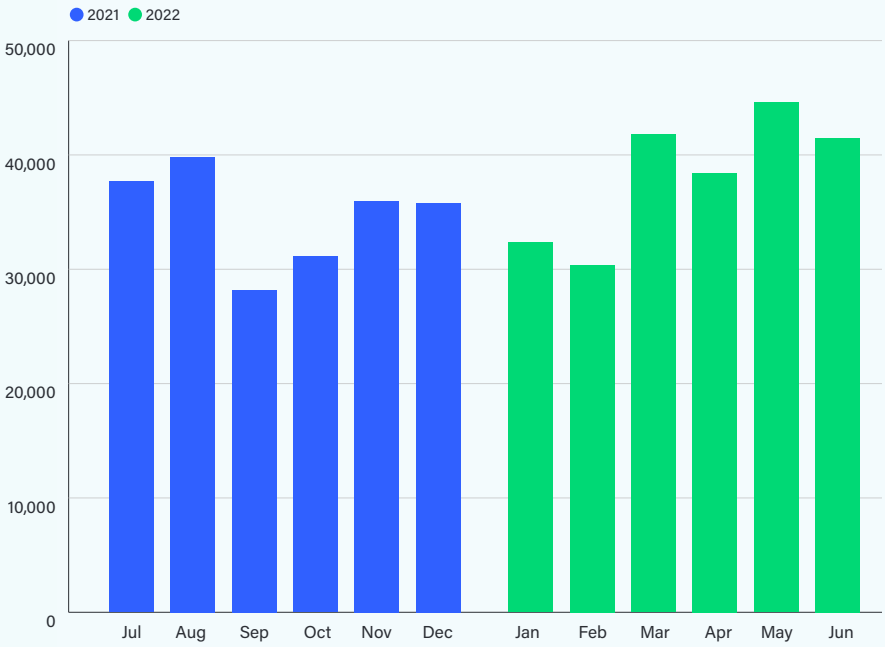


Figure 1: Layer 7 Direct Path Attacks (Data: ATLAS)

In 2H 2021, NETSCOUT reported on a developing trend in which direct-path attacks were starting to supplant reflection/amplification vectors that had long been the norm. We've continued to see this trend in 1H 2022.

NETSCOUT BOTNET TRACKING

NETSCOUT actively monitors and publishes botnet activity in feed content for our products. Efforts to improve botnet tracking are a perpetual cycle as new botnets and IoT malware emerge. A quick snapshot of the number of botted nodes NETSCOUT tracked during 1H 2022 shows:

Q1 2022

21,226
Nodes

Q2 2022

488,381
Nodes

DDoS-Capable Botnets

It's hard to talk about bots and botnets without mentioning DDoS attacks and the malware families such as Mirai that have catapulted them into the spotlight. Mirai inflected the damage it did by taking advantage of IoT devices, which amounted to about 6.3 billion possible devices when Mirai was first detected in 2016. Mirai has continued to evolve since source code was released. The end result is that it now is used not only to target IoT devices but also to attack vulnerabilities in a wide range of other devices, including cable modems and enterprise-grade routers and servers.

~14 Billion

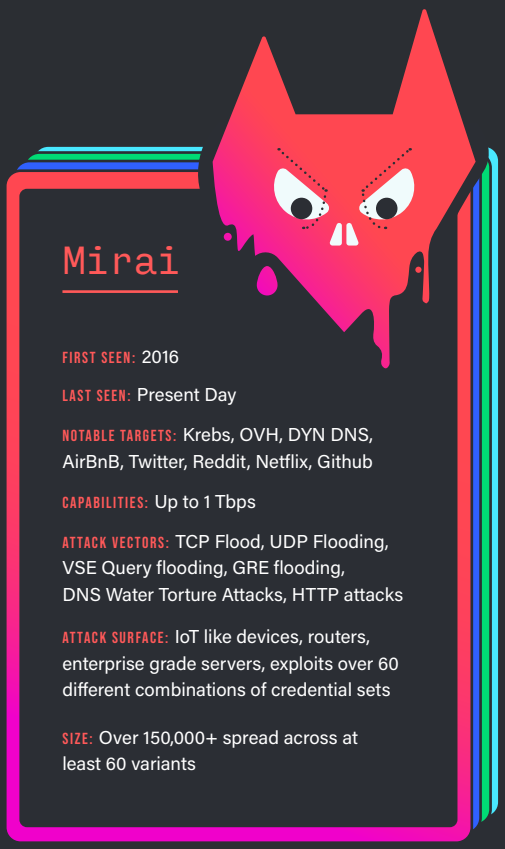
available IoT devices in 1H 2022. These devices have very few security implementations making them very attractive targets.

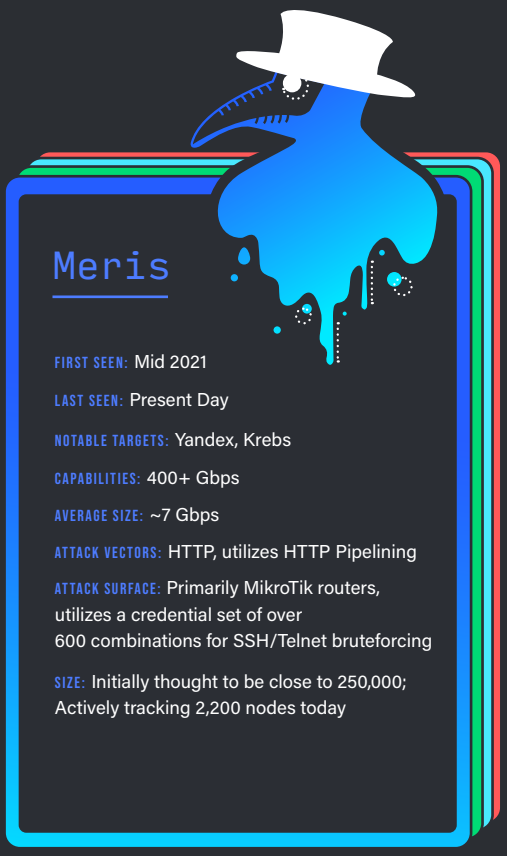
Mirai

Initially, Mirai targeted several prominent websites and services, including Krebs on Security (620 Gbps), OVH (1 Tbps), and DNS service provider DYN. The resulting service interruptions hit high-profile websites such as Airbnb, Twitter, Reddit, and Netflix, as well as code repositories such as GitHub. When Mirai's source code was made public, it birthed a plague of related malware that has since evolved and continues to wreak havoc today.

Mirai has been used to launch DDoS attacks that utilize a variety of common DDoS vectors, including TCP flooding, UDP flooding, valve source exploit (VSE) query flooding, generic routing encapsulation (GRE) flooding, pseudo-random DNS label-prepending attacks (also known as DNS water-torture attacks), and HTTP (GET, POST, and HEAD) attacks. Most recently, Mirai also has started taking advantage of SOCKS proxies.

IoT devices—estimated at 14 billion today—are attractive targets, given the nature of their limited hardware and the fact that very few security implementations are baked into the devices. In fact, it's not uncommon for these devices to have default or hardcoded passwords, and users rarely take basic security steps to protect the devices. Likewise, they're often also incorrectly exposed to the internet at large, making them ripe for exploitation.





Meris

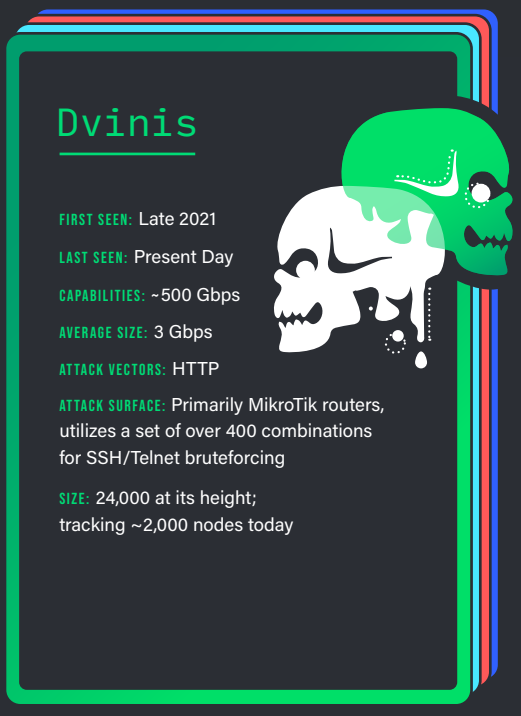
In 2021, another pair of DDoS-capable botnets entered the scene. First came Meris, which first attacked Yandex and Krebs on Security from compromised MikroTik routers. A previously disclosed vulnerability that exposed administrative credentials to the adversary was used. If an admin failed to change the credentials—even with the vulnerability patched—the devices could still be subsumed and added to a botnet. Primarily, Meris launched DDoS attacks by utilizing HTTP-related vectors, especially those leveraging HTTP pipelining.

At its height, Meris was estimated to contain as many as 250,000 compromised devices. The attacks against Krebs on Security accounted for more than 2 million requests per second. By comparison, the attack Mirai launched against Krebs in 2016 was only 450,000 requests per second, illustrating the impressive power of botnets driven by enterprise-class routers.

Dvinis

By analyzing attacks such as Krebs and Yandex, NETSCOUT researchers determined that it wasn't a single botnet leveraging these devices, which led to the discovery of Dvinis. Dvinis has a few key differentiators, such as primarily using MikroTik devices and HTTP-based vectors for DDoS attacks. Unlike Meris, Dvinis forgoes using HTTP pipelining, and earlier versions had a telltale malformed GET request with an extra trailing.

Dvinis also opens and utilizes a different set of ports, and the credential sets that it brute forces for propagation (more than 400 unique) are less substantial than Meris (more than 600). Today, both botnet sources are heavily concentrated in Brazil, Indonesia, Russia, and China.



Killnet

FIRST SEEN: Early 2022

LAST SEEN: Present Day

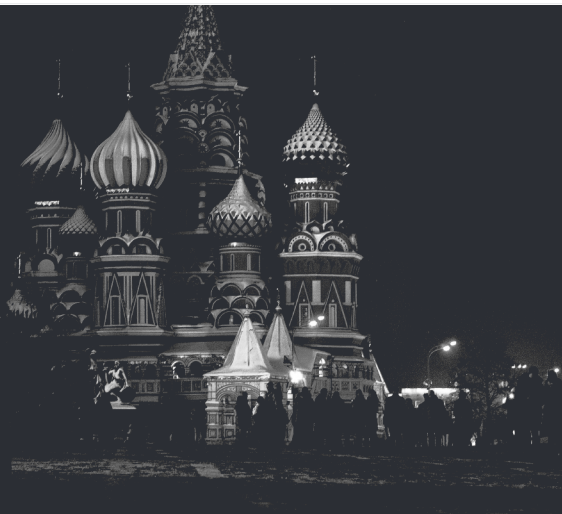
NOTABLE TARGETS: Mainly countries and organizations sympathetic to Ukraine in the ongoing Russia-Ukraine conflict

CAPABILITIES: 40 Gbps

ATTACK VECTORS: Layer 4 and Layer 7 DDoS attacks, ICMP Flood, IP Fragmentation, SYN Floods, RST Floods, SYN/ACK floods, NTP floods, DNS amplification, CLDAP amplification

ATTACK SURFACE: IoT devices, exploitable routers, exploitable enterprise grade servers.

SIZE: ~11,000 nodes



Killnet

Most recently, the Killnet botnet has garnered media attention. Run by a pro-Russian DDoS-for-hire group turned hacktivist, Killnet largely appears to be geopolitically motivated, with a list of attack targets that include the U.S. federal government, as well as Ukrainian and Lithuanian organizations that take opposing viewpoints from the adversary's.

Killnet's primary toolkit includes its own DDoS-capable malware, known as VERA; several off-the-shelf solutions such as Low Orbit Ion Cannon and slowloris; IP-stressor services such as Stresser.ai; and additional toolkits such as Blood Deluxe and CC-attack. Killnet tools also show a preference for utilizing open SOCKS4/SOCKS5 proxies.

Conclusion

Without question, botnets continue to evolve at a frightening pace. Their creators aren't restricted by red tape, internal processes such as Agile, or approval processes. Their capabilities expand with each passing year, and their targets now range from gamers to geopolitical enemies. All of these factors make it imperative for organizations to defend against these attacks or risk massive disruptions to service and reputation.

EXPLORE MORE OF THE 1H2022 DDoS THREAT INTELLIGENCE REPORT

For more expert insight in DDoS global and regional attack statistics, botnet activity, attack vectors and DDoS is used in geopolitical conflicts, revisit the NETSCOUT 1H 2022 DDoS Threat Intelligence Report landing page.

VISIT THE SITE

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) helps assure digital business services against security, availability, and performance disruptions. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our Omnis™ cybersecurity advanced threat detection and response platform offers comprehensive network visibility, threat detection, highly contextual investigation, and automated mitigation at the network edge. NETSCOUT nGenius™ service assurance solutions provide real-time, contextual analysis of service, network, and application performance. And Arbor Smart DDoS Protection by NETSCOUT products help protect against attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

To learn more about improving service, network, and application performance in physical or virtual data centers or in the cloud, and how NETSCOUT's security and performance solutions can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT on Twitter, Facebook, or LinkedIn.

CONTRIBUTORS

Chris Conrad
AUTHOR

Richard Hummel
EDITOR

NETSCOUT

SECR_045_EN 2201 09/2022