Threat Bulletin

ZuoRAT

July 2022

What is ZuoRAT?

On June 29, 2022, Black Lotus Labs, the threat intelligence arm of Lumen Technologies, revealed the existence of the ZuoRAT threat. The code appears to be a heavily modified version of the code behind the Mirai botnet. The source code for Mirai was leaked in 2016.

ZuoRAT is a multi-stage Remote Access Trojan (RAT) developed for small office/home office (SOHO) routers leveraging known vulnerabilities which allows the threat actor to compromise routers gathering credentials, configuration data, browsing behavior, and hijack DNS and HTTP internet traffic. In the next stage, enabled by a port scan of the adjacent network, the attacker would pivot to Windows workstations loading another RAT that masquerades as a legitimate application.

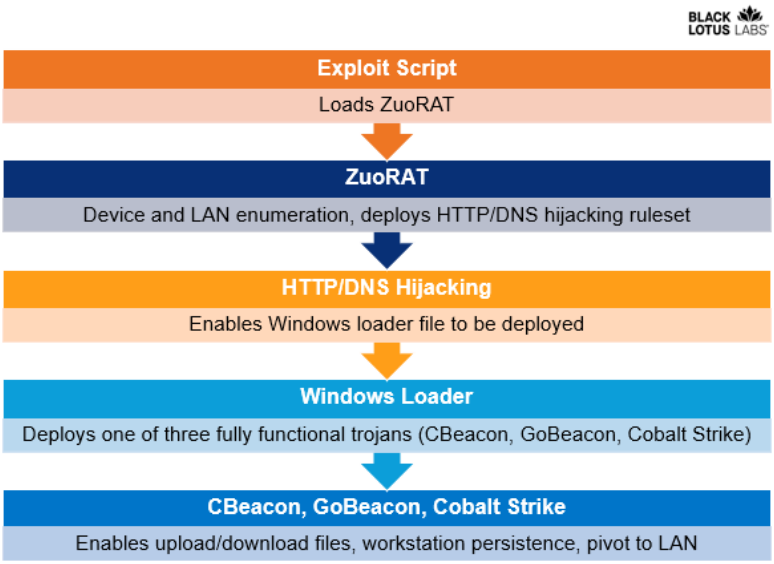
According to security researchers, the threat may have remained undetected for two years. Compromised routers were also used to further hide malicious activity.

The attacks started in October 2020 and targeted known vulnerabilities in routers from ASUS, Cisco, DrayTek, and NETGEAR . Attackers were then able to identify more devices on the network and move laterally (east-west) to attack additional devices within the network.

Given the timing, it is likely that the attackers took advantage of the rapid shift to work-from-home brought upon by the COVID-19 pandemic. Researchers note, “The sudden shift to remote work spurred by the pandemic allowed a sophisticated adversary to seize this opportunity to subvert the traditional defense-in-depth posture of many well-established organizations. The capabilities demonstrated in this campaign – gaining access to SOHO devices of different makes and models, collecting host and LAN information to inform targeting, sampling and hijacking network communications to gain potentially persistent access to in-land devices and intentionally stealth C2 infrastructure leveraging multistage siloed router to router communications – points to a highly sophisticated actor that we hypothesize has been living undetected on the edge of targeted networks for years.”

Allot Secure blocks this attack.

How are users infected?



According to Black Lotus Labs, "ZuoRAT is a MIPS file compiled for SOHO routers that can enumerate a host and internal LAN, capture packets being transmitted over the infected device, and perform person-in-the-middle attacks (DNS and HTTPS hijacking based on predefined rules)."

The ZuoRAT attack begins by exploiting known vulnerabilities CVE-2020-26878 and CVE-2020-26879 using a Python-compiled Windows Portable Executable file to target SOHO routers such as ASUS, Cisco, DrayTek, and NETGEAR. However, as of this writing, the researchers have only been able to gain access to the exploit script for JCG-Q20 model routers. Therefore, there may be additional exploits that are not yet known.

The threat actor likely used unpatched vulnerabilities to steal credentials from the targeted routers. Although patches for these vulnerabilities exist, it is not uncommon for device administrators never to apply these patches.

The malware queries several web services to gain the router's public IP address. If it does not obtain the public IP address, then ZuoRAT deletes itself.

Once the threat actors got information about DNS settings and the internal host, they were able to perform DNS hijacking. The cybercriminal was also able to specify which client or subnet to hijack, engaging in HTTP hijacking.

The cybercriminals engaged in sophisticated attempts to try to cover their tracks. They handed off the initial exploit from a dedicated VPS that hosted benign content. They leveraged routers as proxy Command & Control servers, hiding in plain sight and rotated proxy routers to avoid detection.

According to Black Lotus Lab's researchers, "Likely to make the staging server appear more legitimate, the threat actor uploaded some content written in Arabic script on the hard-coded IP address's [hosting the threat sample] default page. We did not find any subsequent malicious activity associated with the webpage and suspect it was uploaded as a ruse to avert suspicion. This

type of action is a TTP [tactic, technique, and procedure] of a highly sophisticated actor to evade detection.”

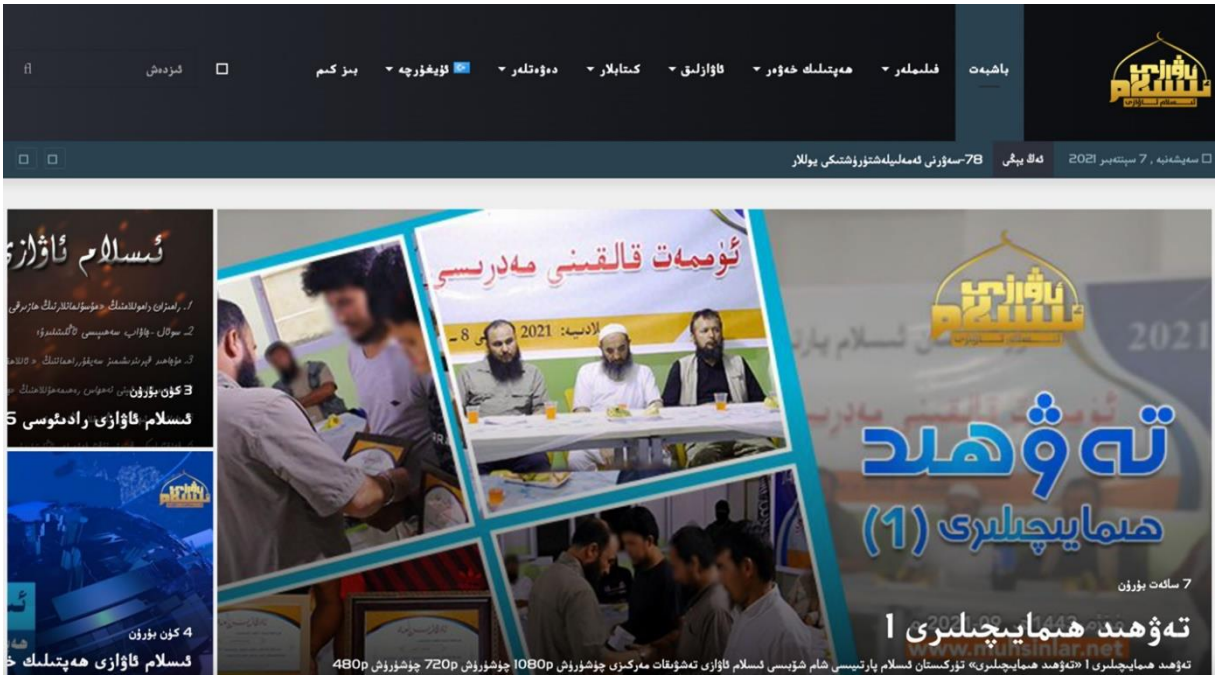


Figure 1 Content hosted on the default landing page

Who is behind the attack?

While the threat technique of compromising SOHO routers as an access vector to gain access to an adjacent LAN is not unique, it is infrequently reported. According to the researchers, “reports of person-in-the-middle style attacks, such as DNS and HTTP hijacking, are even rarer and a mark of a complex and targeted operation. The use of these two techniques congruently demonstrated a high level of sophistication by a threat actor, indicating that this campaign was possibly performed by a state-sponsored organization.”

How service providers can protect their customers

While there have always been many ways for malicious actors to target networks, there is only a handful of router-based malware specifically designed to target the router. ZuoRAT’s behavior points to a highly sophisticated attempt.

To protect their customers, many communication service providers are turning to network-based security which stops the attacks on the network level before they even reach their customers’ devices.

The good news is that customers using Allot Secure, including the router-based HomeSecure and BusinessSecure, are protected from this attack.

How Allot blocks the effects of ZuoRAT

Allot HomeSecure and BusinessSecure solutions, part of the Allot Secure family of cybersecurity solutions, address this attack at multiple stages of the attack chain:

- **Router allowed list:** CSPs can define the destinations a router is allowed to communicate with. These are normally a well-defined set of services that include the CSP ACS, DNS, and NTP servers.

  It is important to note that this first layer blocks the attack in 100% of cases since ZuoRAT is built to identify if it can connect to the Internet. If it cannot connect – which would be the case here due to the protection – it automatically deletes itself and that is the end of the story.

- Even though the attack is blocked with the first layer, there are many other protection layers that address the rest of the exhibited behavior:
  - DNS anti-tampering, redirecting DNS requests to safe DNS servers defined by the CSP.
  - Port scan detection, identifying this stage of the attack too.
  - Domain and IP address filtering -- Blocking even direct IP-based communication is becoming a common tactic used by threat actors to avoid DNS-based filtering.
- Allot HomeSecure and BusinessSecure provide security for IoT, smart appliances, and all devices connected to the home or small office network. They integrate into the existing home/SOHO router with the addition of a thin software client that sits on the router and provides zero-touch network visibility, cybersecurity, and parental/content controls to the subscriber without the need for any installation or configuration by the end-user. Using AI, HomeSecure and BusinessSecure identify and profile connected home/SOHO devices, preventing malware and other threats from infecting the network and detecting and acting upon anomalous behavior.

Protect Subscribers with Allot Secure

Allot Secure is the world's largest network-based security-as-a-service solution built for Communication Service Providers (CSPs), protecting more than 20 million subscribers worldwide. It delivers effortless, device-independent security, achieving high adoption rates. Allot Secure merges

network-based, gateway, and client security into a unified service offering a seamless customer experience for event handling, policy setting, and reporting. It is the only platform protecting end-user and IoT devices simultaneously in the core network, home network, and off-network with a transparent and unified end-user experience. Allot Secure protects mobile, fixed, and converged customers at home, at work, and on the go.

About Allot

Allot Ltd. (NASDAQ: ALLT, TASE: ALLT) is a provider of leading innovative network intelligence and security solutions for service providers and enterprises worldwide, enhancing value to their customers. Our solutions are deployed globally for network and application analytics, traffic control and shaping, network-based security services, and more. Allot's multi-service platforms are deployed by over 500 mobile, fixed, and cloud service providers and over 1000 enterprises. Our industry-leading network-based security as a service solution is already used by over 20 million subscribers globally.
Allot. See. Control. Secure.

For more information, visit www.allot.com

Want to learn more about Security as a Service?
We can assist.

Contact Allot.

Source: ZuoRAT Hijacks SOHO Routers To Silently Stalk Networks, June 28, 2022, https://blog.lumen.com/zuorat-hijacks-soho-routers-to-silently-stalk-networks/