Unmasking the new XorDDoS controller and infrastructure

blog.talosintelligence.com/unmasking-the-new-xorddos-controller-and-infrastructure/

April 17, 2025

By Joey Chen

Thursday, April 17, 2025 06:00

Threat Spotlight

- Cisco Talos observed an existing distributed denial-of-service (DDoS) malware known as XorDDoS, continuing to spread globally between November 2023 and February 2025.
- A significant finding shows that over 70 percent of attacks using XorDDoS targeted the United States from Nov. 2023 to Feb. 2025.
- The language settings of the muti-layer controller, XorDDoS builder and controller binding tool strongly suggest that the operators are Chinese-speaking individuals.
- Talos discovered the latest version of the XorDDoS controller, called the “VIP version,” and its corresponding central controller were used to build the DDoS bot network for more sophisticated and widespread attacks.
- Talos' analysis exposes the network connection between central controller, sub-controller and XorDDoS malware in order to highlight the XorDDoS trojan network pattern. This may help victims identify when they are targeted by these trojans.

Linux XorDDoS trojan trend and victimology

The XorDDoS trojan is a well-known DDoS malware that targets Linux machines, turning them into "zombie bots" that carry out attacks. First identified in 2014, its sub-controller was uncovered in 2015. Based on the simplified Chinese user interface and instructions of the XorDDoS controllers and builder, Talos assess with high confidence that the operators are Chinese-speaking individuals.

From 2020 to 2023, the XorDDoS trojan has increased significantly in prevalence. This trend is not only due to the widespread global distribution of the XorDDoS trojan but also an uptick in malicious DNS requests linked to its command-and-control (C2) infrastructure. In addition to targeting commonly exposed Linux machines, the trojan has expanded its reach to Docker servers, converting infected hosts into bots. It employs a strategy of Secure Shell

(SSH) brute-force attacks to gain remote access to target devices. Once it obtains valid SSH credentials, the attacker leverages root privileges to execute a script that downloads and installs XorDDoS on the compromised device.

Even though numerous security vendors have already provided solutions and detection methods to capture them, Talos continues to observe attempts to deliver XorDDoS malware.

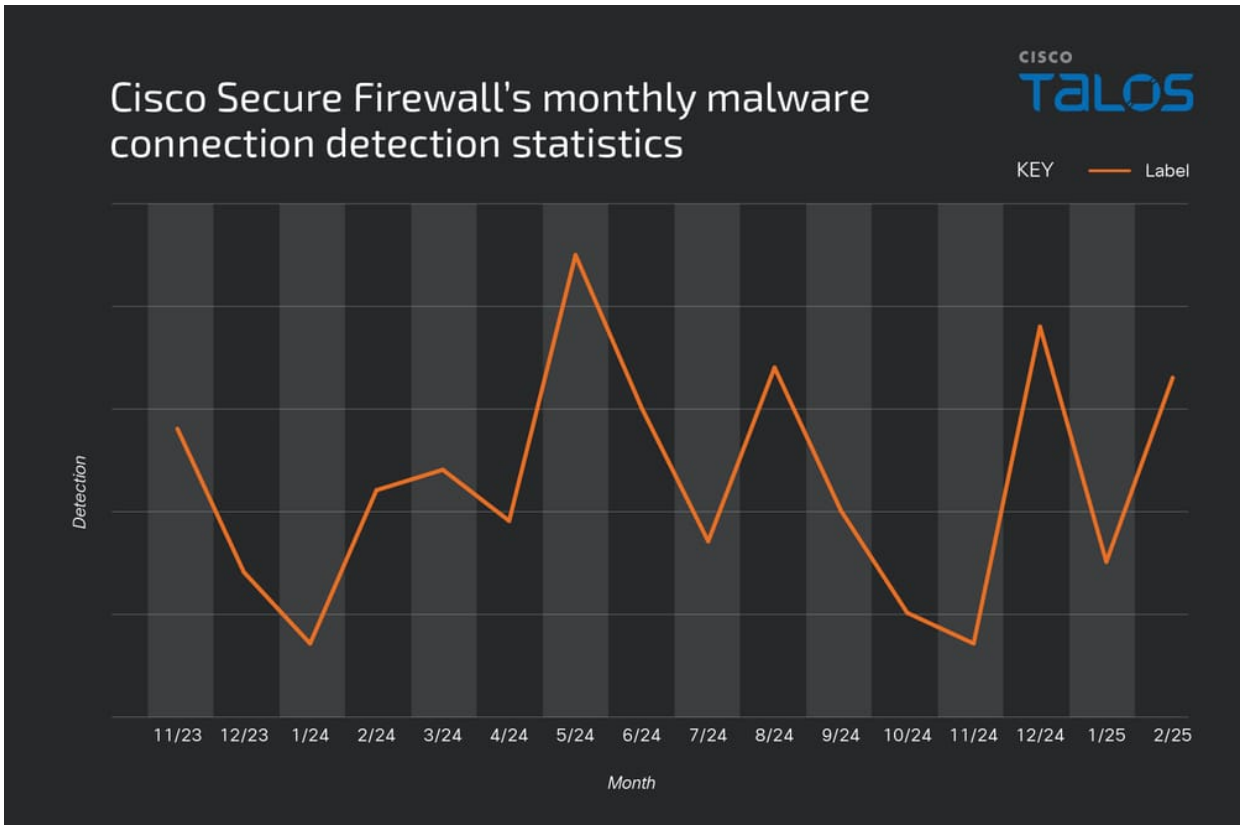

Figure 1. Cisco Secure Firewall's monthly malware connection detection statistics.

Between November 2023 and February 2025, Talos observed that the XorDDoS trojan continued to have a global impact, with nearly 50 percent of its successfully compromised victims located in the United States. Additionally, we noted that the compromised systems attempted to target and attack several countries, including Spain, the United States, Taiwan, Canada, Japan, Brazil, Paraguay, Argentina, the United Kingdom, the Netherlands, Italy, Ukraine, Germany, Thailand, China, India, Israel, Venezuela, Switzerland, Singapore, Finland, Australia, Saudi Arabia, France, Turkey, the United Arab Emirates and South Korea.

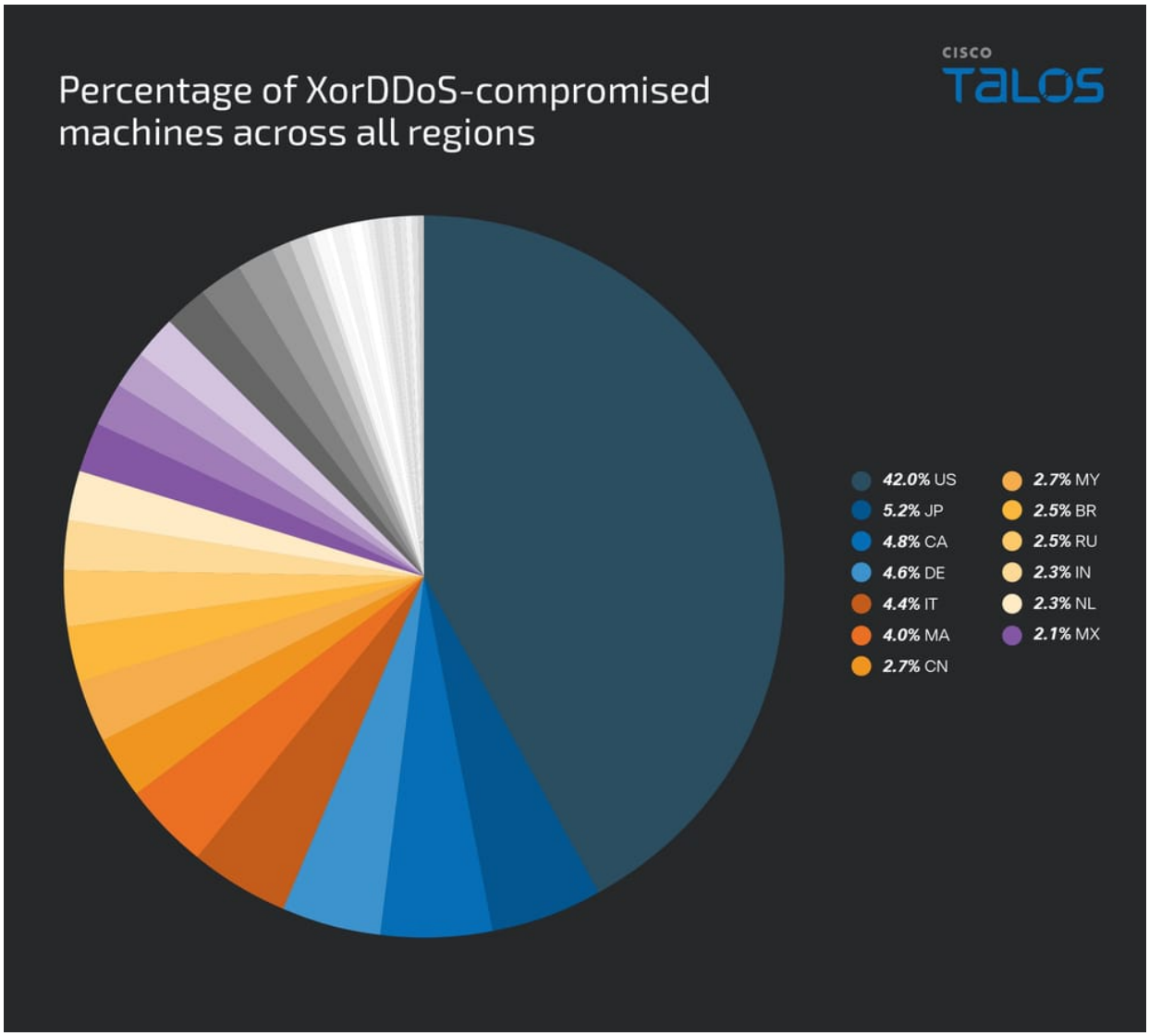

Figure 2. Percentage of XorDDoS successfully-compromised machines across all regions.

Talos also used our Cisco Secure Network/Cloud Analysis to observe actors using those compromised machines to launch DDoS attack and the attacks are globalized. Notably, we found that the United States accounted for over 70 percent of attempted attacks employing XorDDoS.

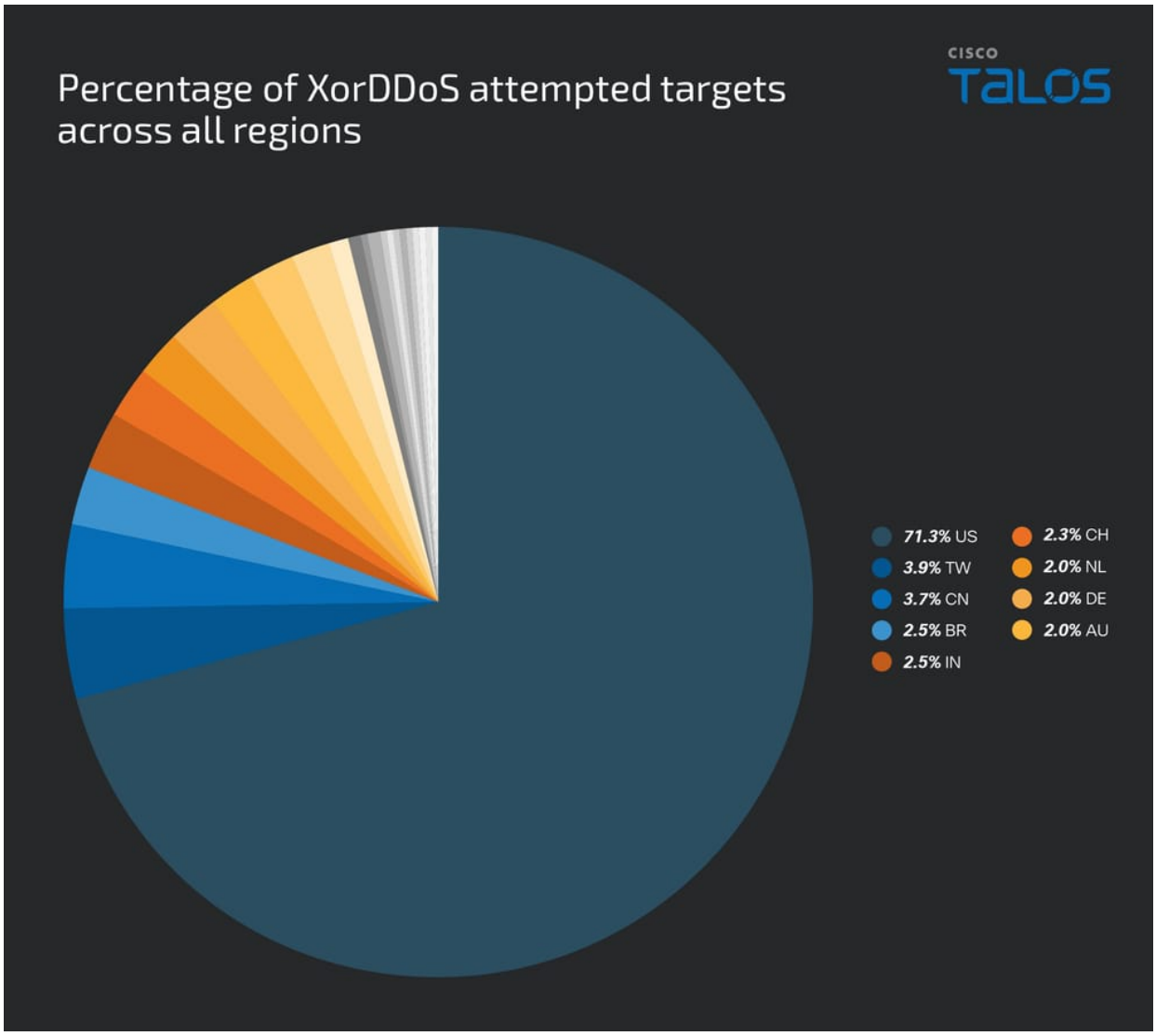

Figure 3. Percentage of XorDDoS attempted targets across all regions.

Infection chain

XorDDoS has long relied on SSH brute-force attacks to spread. It deploys a malicious shell script that attempts numerous root credential combinations across thousands of servers until it successfully accesses a target Linux device. Once inside the machine, XorDDoS implements persistence mechanisms to ensure it launches automatically at system startup, therefore evading detection and termination by security products. To maintain persistence, the malware installs an init script and a cron job script. These scripts are embedded within the malware and perform actions consistent with those outlined in previous reports.

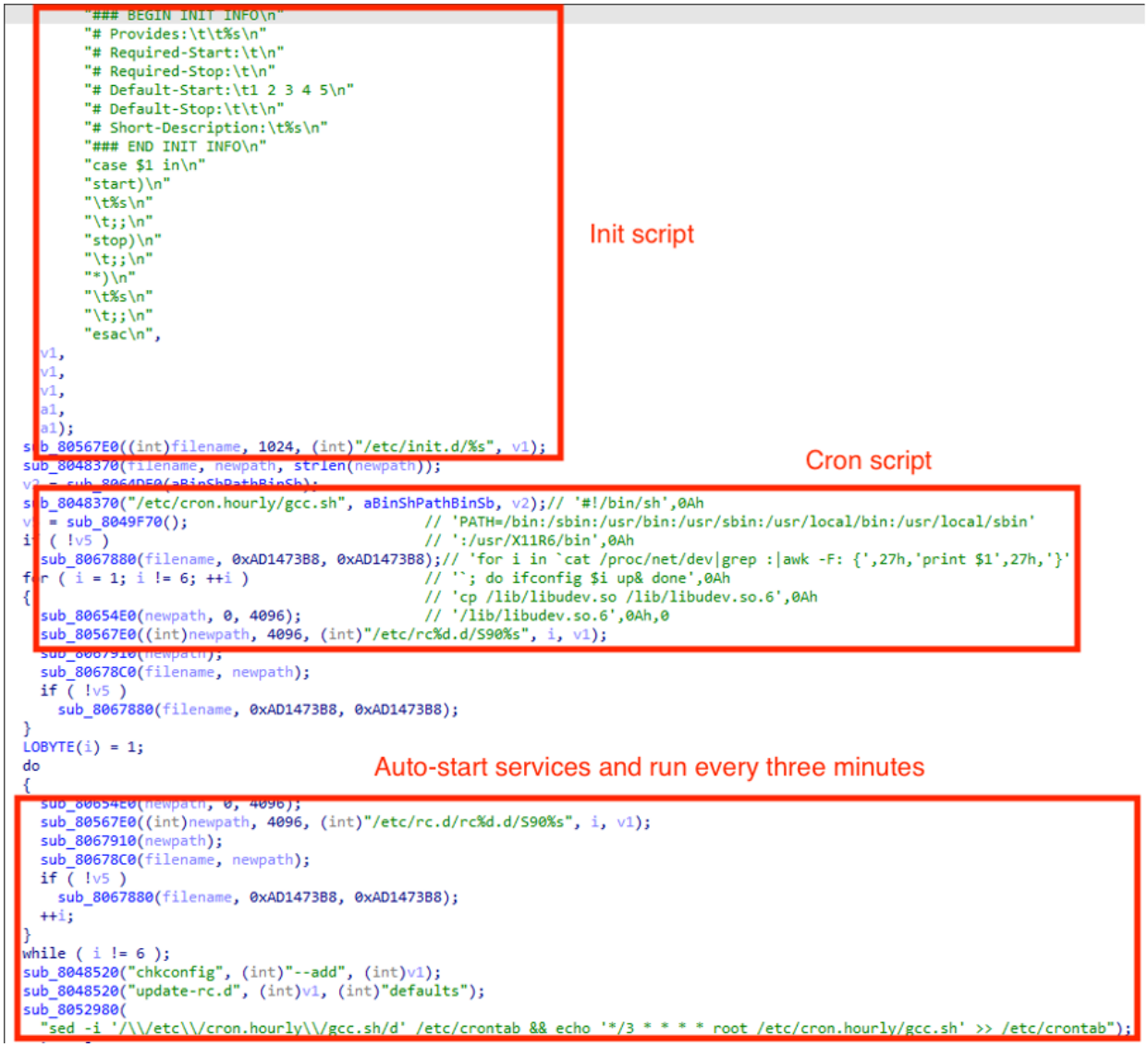

Figure 4. Inint script and cron script embedded in trojan.

The latest version of XorDDoS malware continues to use the same decryption function and the XOR key "BB2FA36AAA9541F0" to decrypt its embedded configuration. Once the URLs or IPs are decrypted, they are added to a remote list. This list is then used to establish communication and retrieve commands from the C2 server. Talos used CyberChef to successfully decrypt one of the examples.

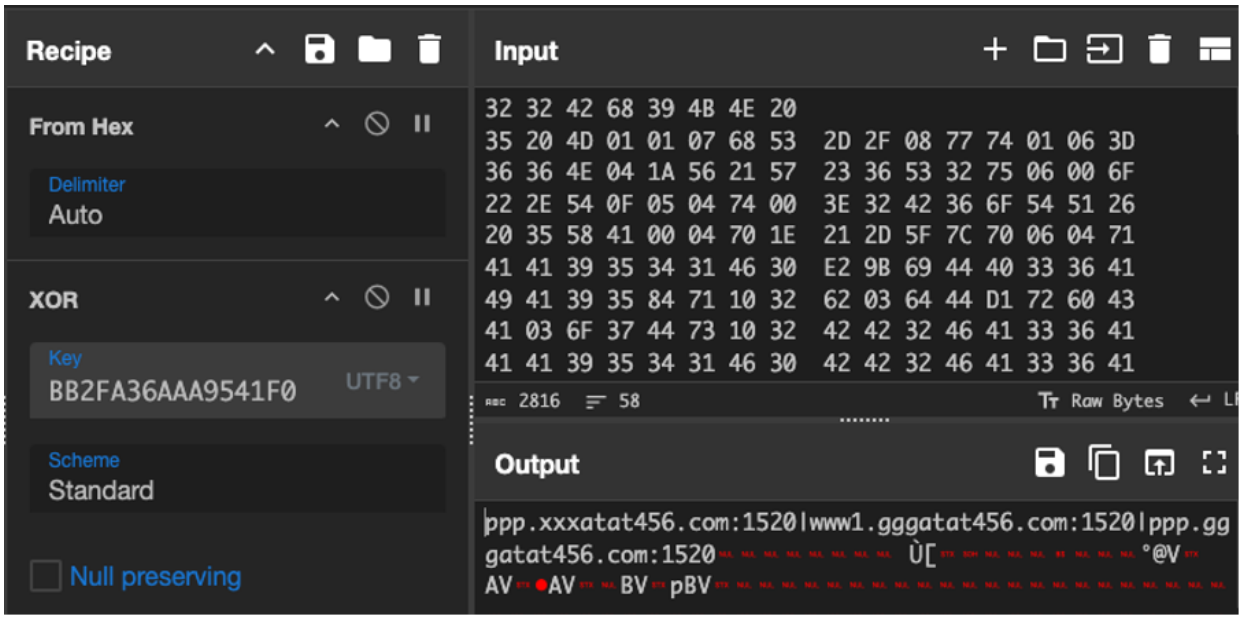

Figure 5. Talos CyberChef decryption.

XorDDoS new sub-controller and central controller

Although the sub-controller for XorDDoS was exposed in 2015, attacks have persisted over the last decade. The panel from 2015 was for version 1.4, the oldest version, which we believe is no longer in use by threat actors. In 2024, Talos discovered a new “VIP” version of the XorDDoS sub-controller, which can control the "VIP version” of the XorDDoS trojan, the first instance of which we traced back to 2017. With the newest version of the XorDDoS sub-controller and trojan builder, Talos believes that this collection is a product suite developed for sale.

Figure 6 shows translated screenshots of the XorDDoS trojan sub-controller and builder. The builder also contains new feature descriptions, which strengthens Talos’ assessment that this is a product meant to be sold. The VIP version of the XorDDoS trojan builder includes new feature descriptions. When translated, the description in Figure 7 reads, "Stable Anti-Kick, 100% Packet Sending, Fixes for Over Ten Thousand Online Without Lag. Supports Domain Online, IP Online, with New Packet Sending Code and Wall-Penetration Optimization. Can Send 1024 Packets with Resource Utilization Optimization."

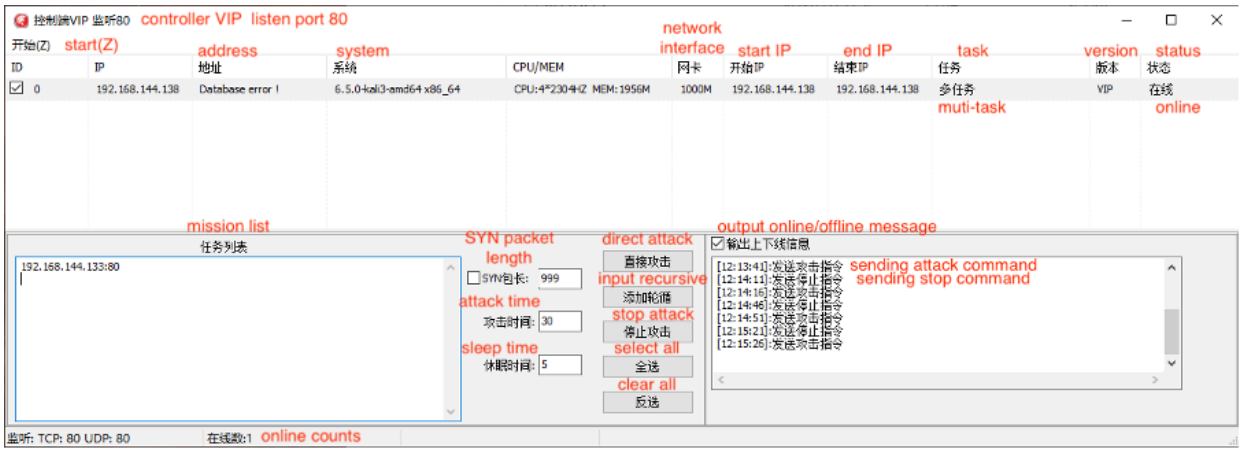

Figure 6. VIP version sub-controller.

Figure 7. Feature description in the VIP version of the XorDDoS trojan builder.

Talos observed a new version of the sub-controller, which we call the "central controller." Specifically created for the XorDDoS trojan, the central controller enables threat actors to manage multiple XorDDoS controllers simultaneously. This updated central controller enhances cybercriminals' ability to coordinate and execute attacks more efficiently, indicating an evolution in their tactics and capabilities.

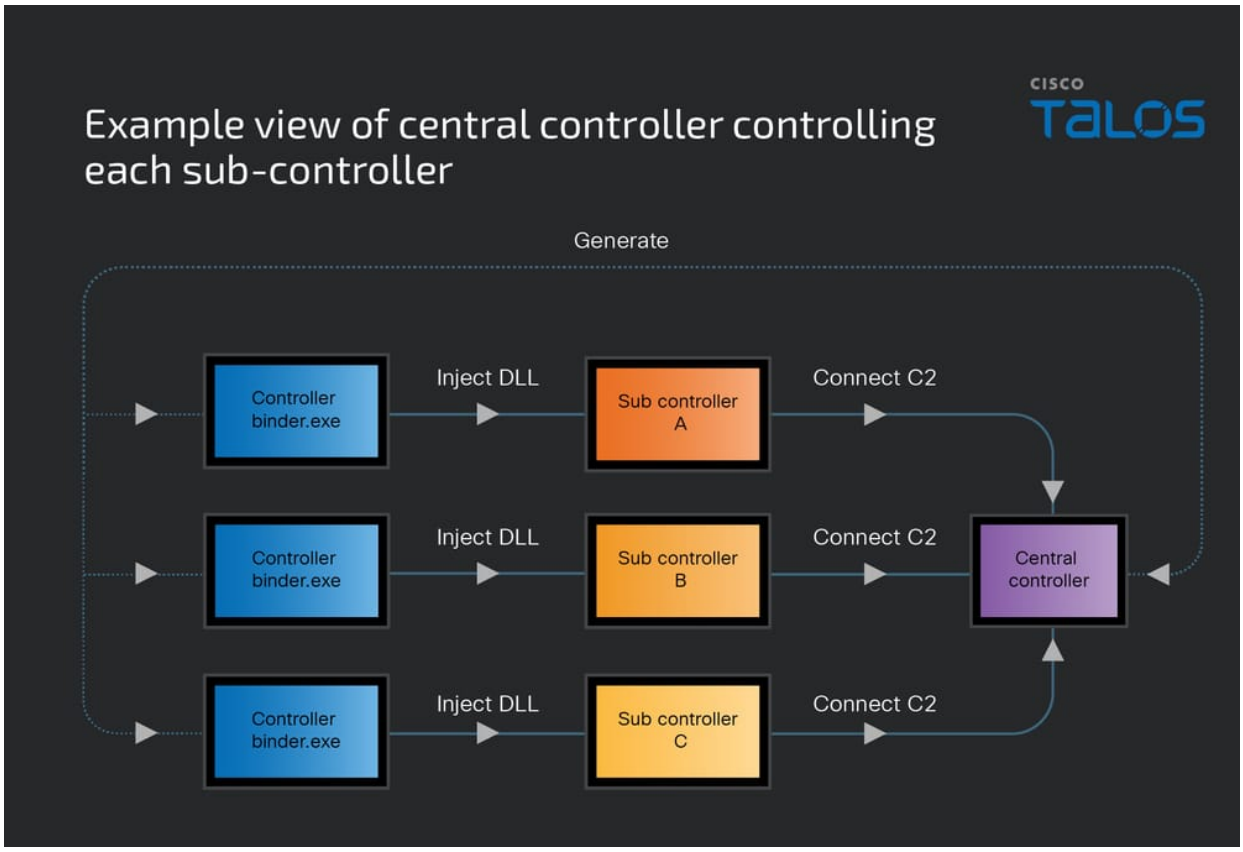

Figure 8. Example view of central controller controlling each sub-controller.

The central controller can generate a controller binder that will inject a DLL file to the XorDDoS controller to bind network connection and command operation to the sub-controller, allowing the central controller to fully remote control the sub-controllers.

Figure 9. Generator Setting

The controller binder will establish a connection with the central controller. When running the controller binder on the host, the actor can enter the controller's process name, allowing them to inject into the process and take control. This straightforward strategy allows the actor to send the DDoS commands to multiple controllers simultaneously. There are two notable facts Talos observed from this central controller. First, when the actor opens the central controller, there is a feature description in its mission list column that, when translated, includes the following:

- "Check the SYN packet length to make it a large packet, otherwise it will be a small packet.

- A round-robin attack is a task performed by all online hosts.
- Select the host and click the test mode, which means a single host sends a packet.
- Multiple measurement modes cannot be selected, only one at a time!
- The round-robin attack needs to be stopped manually.
- Supports 1024 packages but requires a corresponding sub-controller.
- The sub-controller of version 1.4 and 1.8 on the underground market cannot use the central controller to send 1024 packages."

Second, the controller's creator left their Tencent QQ instant message contact number and nickname on the central controller, while also mentioning other sub-controller versions available on the underground market. This further supports Talos' assessment that these tools are for sale.

Figure 10. Central controller and controller binder.

Advanced XorDDoS traffic analysis

Talos' detailed analysis of these new tools suggests cybercriminals' continued investment in the development and deployment of the XorDDoS trojan, allowing for more sophisticated and widespread attacks. The entire control flow of these operations demonstrates the adaptability and resilience of these threat actors, emphasizing the ongoing challenge in combating this form of cybercrime. Talos completed a traffic analysis in our sandbox environment, first to analyze how the XorDDoS trojan is connected to the sub-controller, and then to understand how the central controller manages the sub-controller.

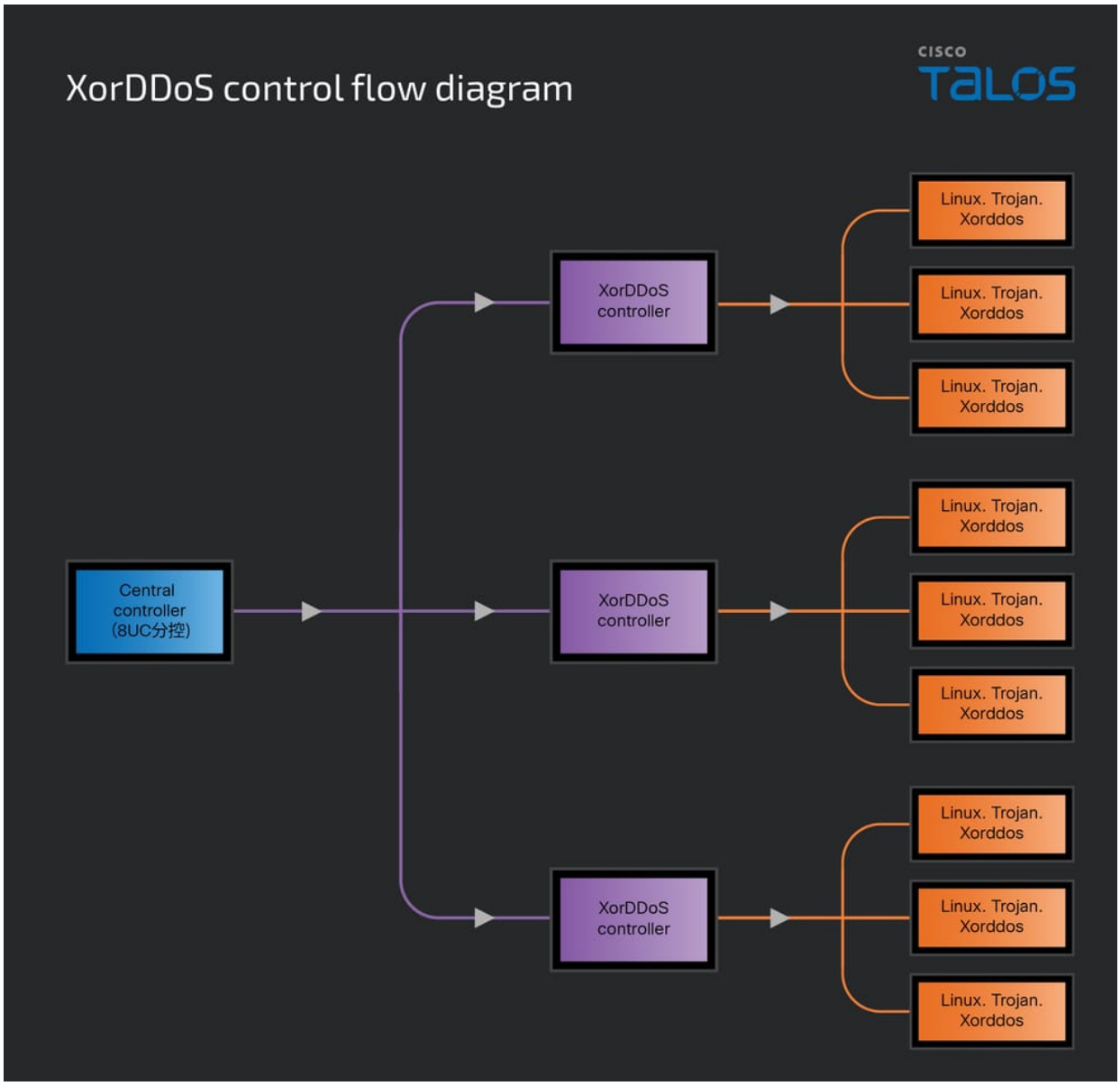

Figure 11. XorDDoS control flow diagram.

The connection between the sub-controller and DDoS trojan is the orange line in Figure 11. When the malware is successfully installed in the target system, it will attempt to send encrypted data, including "phone home," which consists of the CRC Header, uname string release, uname string machine, magic string and hardcoded version string. Talos used CyberChef to provide a decryptor function for this data.

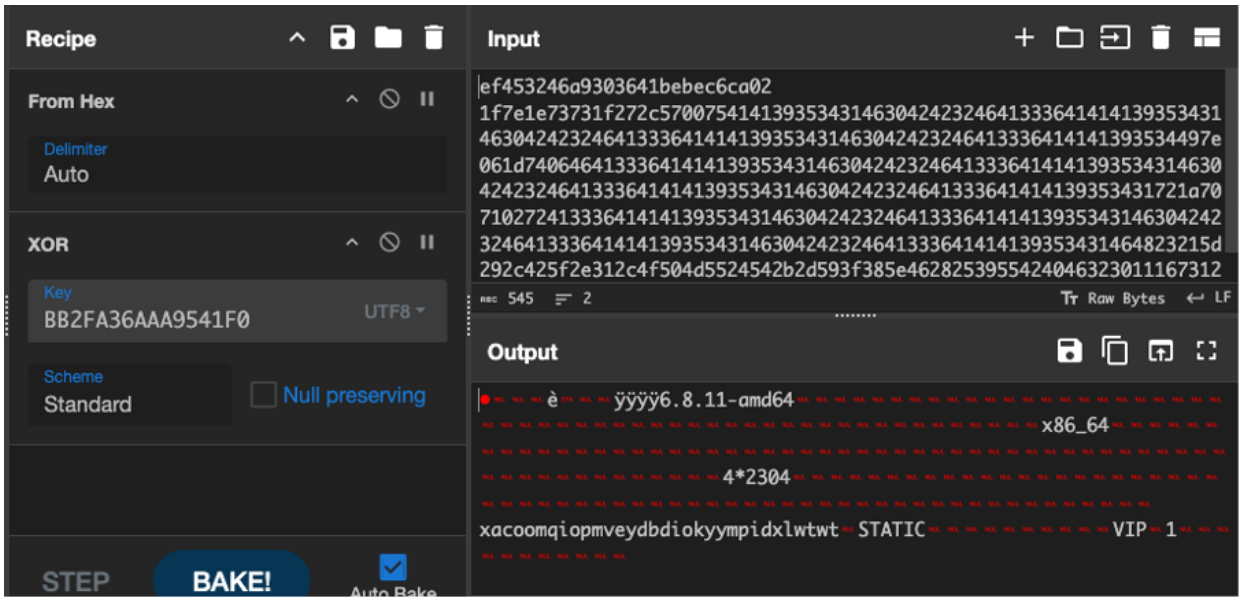

Figure 12. Example of decrypted phone home data.

We noticed that the latest VIP version's "phone home" CRC header remains unchanged from what Unit 42 previously detailed in a blog post. Since the blog post has already covered the encryption of the XorDDoS trojan's phone home data, we will focus here on the behavior of the controller's responses and any modifications in the CRC header.

Once the XorDDoS trojan successfully establishes a connection, the CRC header changes to "5343f0960000000002000000000000000000000000000000000000000000", as shown in Figure 13. This functions similarly to basic client-server authentication for establishing a connection. When the controller issues a command to the XorDDoS trojan, it uses the same CRC header to attach the encrypted command, sending it to the trojan. This process, illustrated in Figure 14, helps the XorDDoS trojan verify that the commands are authorized and safe to execute.

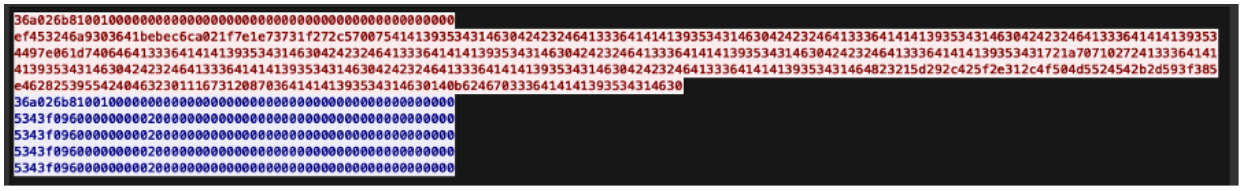

Figure 13. The CRC header changes after successfully establishing a connection.

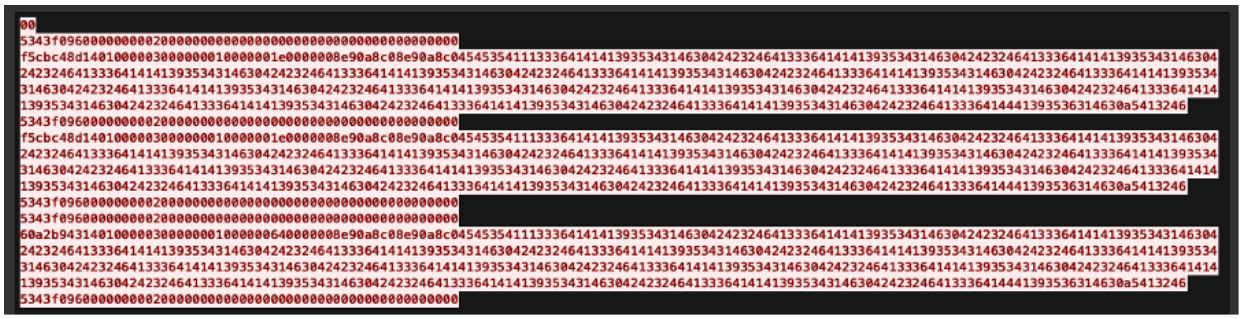

Figure 14. Network flow of sub-controller sending the command to XorDDoS trojan.

Next, Talos explored the connection between the central controller and the sub-controller, represented by the purple line in Figure 11. The central controller can create a controller binder to inject the sub-controller, thereby gaining full access to it. Once the controller binder successfully takes control of the sub-controller, it sends the sub-controller's machine information back to the central controller as a "phone home" beacon. This phone home data uses plaintext to send information, which includes the message number, packet size, IP address, hostname and connection port.

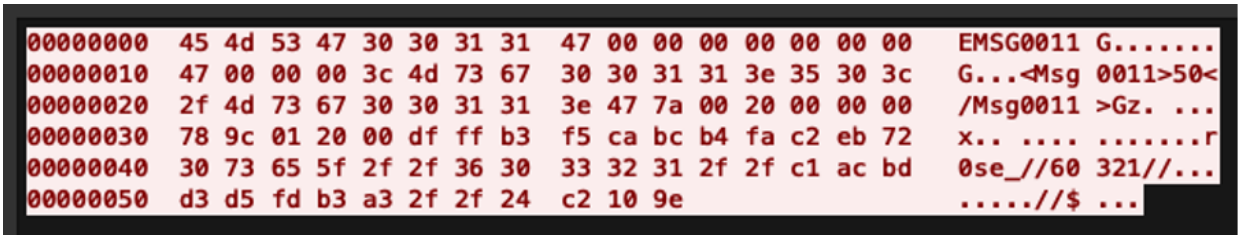

Figure 15. Network flow of the phone home connection.

Talos used the central controller to establish a connection with the sub-controller to monitor network traffic. During this process, we observed that the MSG number in the packets increases with each command sent to either the client controller or back to the central controller. As shown in Figure 16, Talos used the central controller to issue commands to start a SYN DDoS attack, stop the attack, and target specific IPs or domains. For every command sent, the MSG number increments. Similarly, each received packet also sees an increase in its MSG number. However, it's important to note that the MSG numbers for sent packets and received packets are not directly related to each other.

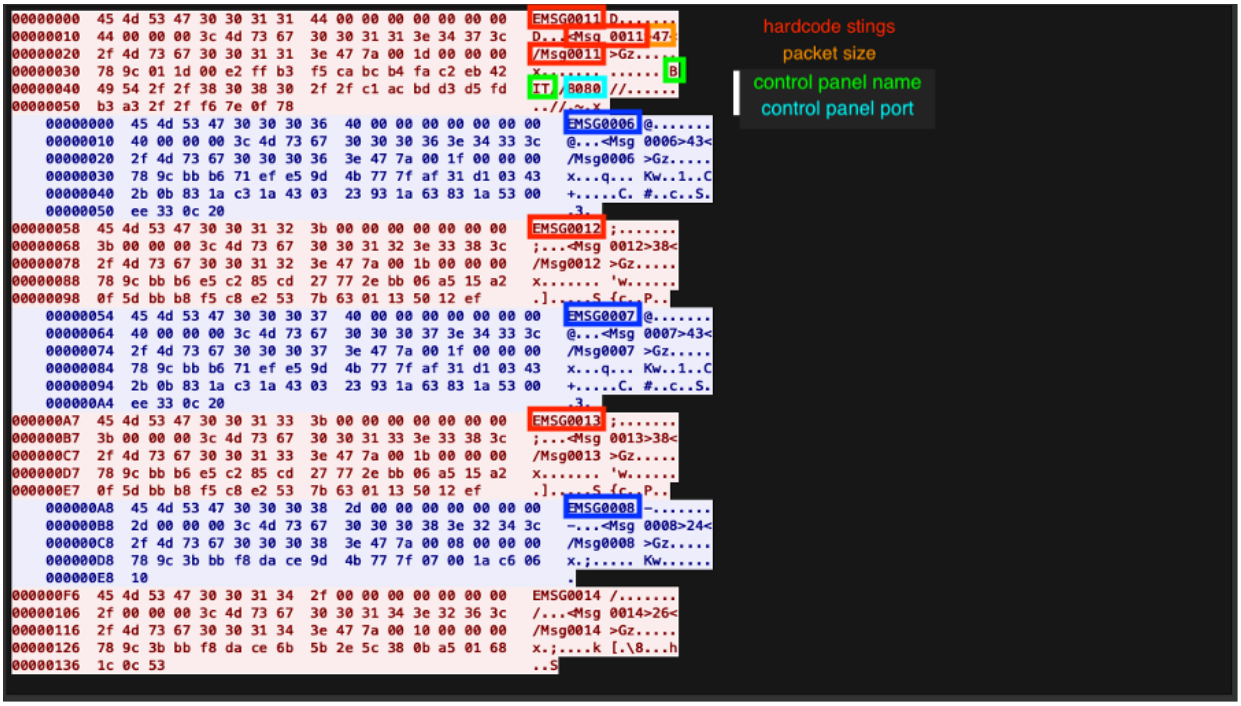

Figure 16. Network flow of central controller sending the command to sub-controller.

Coverage

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them. Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. Snort SIDs for this threat are 64669, 64668 and 64667.

ClamAV detections are also available for this threat: Unix.Dropper.Xorddos::in07.talos

Indicators of Compromise

IOCs for this threat can be found in our GitHub repository here.