GoTitan Botnet Attack

Fernando D. Parra

Metropolitan State University of Denver

Host Security - CSS

Maranda Mulder

February 28th, 2024

GoTitan Botnet Attack

A malicious code from last year called GoTitan is a relatively new botnet based on the Go programming language. GoTitan exploited a critical weakness in Apache systems and is considered a high-level vulnerability with a severity score of 9.8 base score from the National Vulnerability Database in the Common Vulnerability Scoring System Version 3.0 or CVSS v3.0. GoTitan, as stated by NIST, uses the Java Openwire Protocol which can be enabled through port 61616 to use Apache ActiveMQ and apply "Apache ActiveMQ Deserialization of Untrusted Data Vulnerability" (CVE-2023-46604 Detail, 2023). For reference, ActiveMQ allows several applications in different programming languages to communicate, and it is open source.

Utilizing CVSS v3.0 provided by NIST in the same order, the attack vector is through a network, the attack complexity is low, there are now privileges required, the botnet doesn't need user interaction, the scope is unchanged, and it impacts all CIA triad highly. According to *TheHackerNews.com*, "Apache ActiveMQ is being actively exploited by threat actors to distribute a new Go-based botnet called GoTitan as well as a .NET program known as PrCtrl Rat that's capable of remotely commandeering the infected hosts" (Gotitan botnet spotted exploiting recent Apache..., 2023). The vulnerability allows attackers to execute these attacks from a remote location, making it even more dangerous. This could potentially lead to significant disruptions and damage to the targeted organization's operations and the weakness lets attackers execute Distributed Denial-of-Service attacks. For instance, "GoTitan communicates with its C2 server by sending "\xFE\xFE" as a heartbeat signal and waiting for further instructions. When it receives a command, it passes it to a function named "handle_socket_func2" that determines an attack method. GoTitan supports ten different methods of launching distributed denial-of-service

(DDoS) attacks: UDP, UDP HEX, TCP, TLS, RAW, HTTP GET, HTTP POST, HTTP HEAD, and HTTP PUT" (Lin, 2023).

Fortunately, the Cybersecurity and Infrastructure Security Agency was able to identify this exploit and there are no specific companies or organizations that were affected by GoTitan last year. On the other hand, GoTitan is rumored to be in development and could easily spread in a network(s) with outdated or unpatched Apache systems, this opens the opportunity for other devices on the same network to be victims of remote-controlled malware infected by the previously mentioned vulnerable systems. Since this vulnerability was encountered in 2023, the simplest solution to prevent the exploit in most if not all IT infrastructure domains is "to upgrade both brokers and clients to version 5.15.16, 5.16.7, 5.17.6, or 5.18.3 which fixes this issue" (CVE-2023-46604 Detail, 2023). In my perspective, an approach(s) to prevent this exploit is by obviously keeping systems updated, stopping the usage of the Java Openwire Protocol if necessary or is not in use, and/or implementing user authentication and access controls with Apache systems that provide ActiveMQ. Though there are many ways to contain and stop an exploit, using the TPC/IP Model, the access controls can be established in the application layer, security controls like encryption for the transport and network layer can also be enforced, and physical controls for the network access layer could prevent a threat actor to penetrate the network, to begin with.

It is important to recognize that malware threats are constantly evolving and becoming more sophisticated, with GoTitan being one such example. As a resolution, organizations must adopt a robust and proactive security posture to mitigate the risk of these attacks. Botnets like GoTitan can have a devastating impact on businesses, disrupting operations and potentially causing serious harm to the confidentiality, integrity, and availability of other systems and devices. Therefore, it is essential to take a multi-layered approach to security, including measures such as regular software updates, network monitoring, and employee training to ensure that the organization is prepared to defend against these threats.

References

ActiveMQ. (n.d.). https://activemq.apache.org/

CVE-2023-46604 Detail. NVD. (2023, October 27). https://nvd.nist.gov/vuln/detail/CVE-2023-46604

Gotitan botnet spotted exploiting recent Apache ActiveMQ vulnerability. The Hacker News. (2023, November 29). https://thehackernews.com/2023/11/gotitan-botnet-spotted-exploiting.html

Lin, C. (2023, November 28). Gotitan botnet - ongoing exploitation on Apache activemq: Fortiguard Labs. Fortinet Blog. https://www.fortinet.com/blog/threat-research/gotitan-botnet-exploitation-on-apache-activemq?&web_view=true

OpenWire. (n.d.). https://activemq.apache.org/components/artemis/documentation/latest/openwire.html#:~:text=Apache%20ActiveMQ%20Artemis%20supports%20the,OpenWire%20connections%20on%20port%2061616%20