U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0294

HINATABOT BOTNET EXPLOITS SERVERS

DATE ISSUED:20 20th March 2023

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

An old security flaw in Realtek SDK, Huawei routers, and Hadoop YARN servers are being exploited by a new Go-Language-based botnet to stage Distributed-Denial-of-Service (DDoS) attacks. The malware can contact a command-and-control (C2) server to listen for incoming instructions and initiate attacks against a target IP address.

BREAKDOWN

Security researchers at Akamai discovered a new botnet dubbed as 'HinataBot' that is distributed by exploiting unpatched vulnerabilities and weak credentials. Security flaws in Hadoop YARN servers, Realtek SDK devices, and Huawei HG532 routers are being utilised to spread the malware. Once the device is infected, the malware waits silently for further instructions from the Command and Control (C2) servers. The malware supports HTTP and UDP floods to perform DDoS attacks. The HTTP packet size ranges between 484 and 589 bytes. The UDP packets generated by HinataBot are particularly large (65,549 bytes) and consist of null bytes capable of overwhelming the target with a large volume of traffic. DDoS attacks are predicted to rise due to the arrival of new malware strains that are capable of targeting IoT devices and taking over accounts to gain unauthorized access to resources.

REMEDIATION STEPS

- Activate multi-factor authentication (MFA) to secure your accounts. This adds another layer of protection, even if the credentials are compromised.
- Reduce the attack surface by using firewalls or Access Control Lists (ACLs) to control what traffic reaches your applications.
- Deploy detection and prevention tools throughout your organisation to identify anomalous network behaviour.
- Use a Web Application Firewall (WAF) to protect your application against attacks.

REFERENCES & RESOURCES

The Bleeping Computer	https://www.bleepingcomputer.com/news/security/new-hinatabot-botnet-could-launch-massive-33-tbps-ddos-attacks/