Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

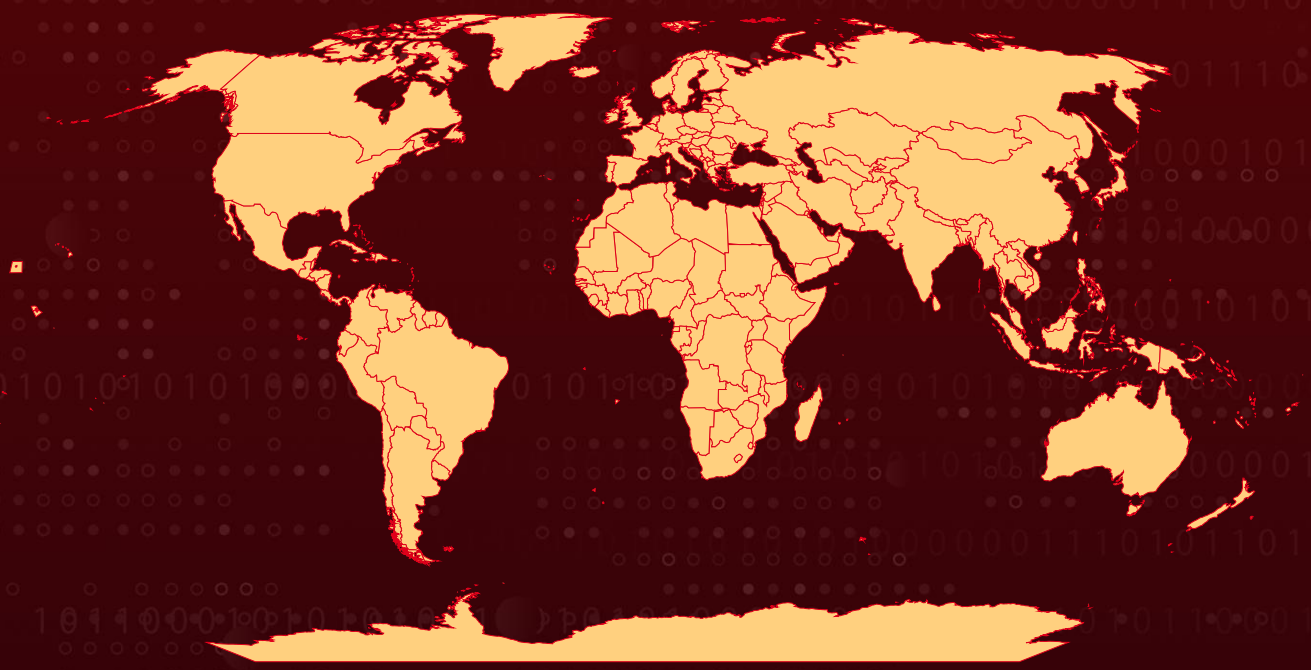
GorillaBot: A Rising Threat in Global DDoS Attacks

Date of Publication	Admiralty Code	TA Number
October 9, 2024	A1	TA2024384

Summary

Attack Began: September 4, 2024
Malware: GorillaBot
Targeted Industries: Universities, Government websites, Telecoms, Banks, Gaming
Targeted Region: Worldwide
Attack: GorillaBot is a new and advanced botnet that has executed over 300,000 DDoS attacks between September 4 to 27, 2024, targeting over 113 countries, including China and the U.S. It uses a variety of attack vectors, including UDP and TCP ACK floods, and exploits vulnerabilities in devices and systems. The botnet's sophisticated encryption techniques, linked to the KekSec group, make it highly persistent and difficult to detect, posing a serious threat to critical sectors. Enhanced security measures are essential to mitigate its impact globally.

Attack Regions



Attack Details

#1

A new botnet, GorillaBot, has surfaced as a significant threat in the realm of DDoS (Distributed Denial of Service) attacks, issuing over 300,000 commands within a few weeks between September 4 and 27, 2024. GorillaBot primarily targets countries such as China and the U.S., but its impact extends globally, affecting over 113 nations. GorillaBot is based on the leaked Mirai botnet code, which leverages compromised IoT (Internet of Things) devices for large-scale cyberattacks.

#2

The botnet employs a variety of DDoS attack vectors, including UDP Flood, TCP ACK Flood, and ACK Bypass Flood, all designed to overwhelm systems and cause service outages. Its use of the connectionless UDP protocol allows for arbitrary source IP spoofing, generating substantial traffic volumes. The botnet supports multiple CPU architectures ARM, MIPS, x86_64, and x86 enhancing its ability to compromise a wide range of devices. Notably, it exploits a vulnerability in Apache Hadoop YARN RPC for remote code execution, highlighting its capability to leverage existing security weaknesses.

#3

GorillaBot uses five built-in C&C servers, randomly connecting to one upon execution. Its use of encryption algorithms similar to those of the KekSec group enhances its resistance to detection and remediation efforts. The persistence mechanisms are particularly concerning, as GorillaBot creates a service file that ensures its operations resume automatically upon system startup. This service is responsible for downloading and executing malicious scripts from remote servers, embedding the botnet deeper into compromised systems.

#4

Additionally, the botnet also checks for the presence of the /proc filesystem to avoid detection by honeypots. The GorillaBot botnet represents a significant escalation in DDoS threats worldwide. Its advanced methods and widespread reach underscore the urgent need for enhanced security measures across all sectors.

Recommendations

Patch Devices Regularly: Ensure all IoT devices, servers, and critical infrastructure systems are updated to protect against vulnerabilities like the Apache Hadoop YARN flaw that GorillaBot exploits.

Implement Rate Limiting and IP Filtering: Rate Limiting involves throttling traffic to prevent sudden surges that could indicate a DDoS attack. This technique helps mitigate the impact of volumetric attacks by restricting the rate of incoming requests. Coupled with IP Filtering, which blocks traffic from known malicious IP addresses, this approach can significantly reduce the risk of successful attacks.

Use Anomaly Detection: Integrate AI-powered detection systems that monitor unusual traffic patterns and behaviors in real time, allowing early identification of potential botnet activity. Honeypots should also be refined to evade botnet evasion techniques like GorillaBot's /proc checks.

Utilize Content Delivery Networks (CDNs): Deploying Content Delivery Networks can enhance resilience against DDoS attacks by distributing traffic across multiple geographically dispersed servers. This makes it harder for attackers to overwhelm a single point of failure, thereby improving scalability and availability during high traffic periods. CDNs also provide additional layers of caching and load balancing, which can further mitigate the effects of an attack.

Continuous Monitoring and Threat Detection: Establishing a system for continuous monitoring is crucial for early detection of suspicious activity. Organizations should utilize specialized tools that analyze network traffic patterns to identify anomalies that may indicate an impending DDoS attack. This proactive approach enables swift responses, minimizing potential damage

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0011 Command and Control
TA0040 Impact	TA0005 Defense Evasion	T1588 Obtain Capabilities	T1588.006 Vulnerabilities

T1498 Network Denial of Service	T1547 Boot or Logon Autostart Execution	T1584 Compromise Infrastructure	T1027 Obfuscated Files or Information
T1543.002 Systemd Service	T1543 Create or Modify System Process	T1584.005 Botnet	T1059 Command and Scripting Interpreter

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	276adc6a55f13a229a5ff482e49f3a0b, 63cbfc2c626da269c67506636bb1ea30, 7f134c477f307652bb884cafe98b0bf2, 3a3be84df2435623132efd1cd9467b17, 03a59780b4c5a3c990d0031c959bf7cc, 5b37be51ee3d41c07d02795a853b8577, 15f6a606ab74b66e1f7e4a01b4a6b2d7
URL	hxxp[://]pen.gorillafirewall[.]su/
SHA256	22a545fdb6ebbc5ba351c97d32cd008a1550a49891ae6112ddc8a6370376f053, 4cac6023b760e1fdae8c096a4db425eae3bbfe0d2554551efb76fc2f2d3a6b1b, e8320657b9ff24198170e6b30188304555b43281b654075052721717f66fb4df, 42845557a515bc05c290b3ab9d1ad291303691d472db9e09863bfc782b803ed2, d99d10559f1ad6bba1b59913604e261a613daa94af01ade8276effd692b5c03f, 826f9c8153c14a66ba730291e5f78d71d958c08cde45e2119afa227211ee5132, 6d10e4da8d8090e0e7e077ef4aead8b8720d1bd4f9b86d34ae66eac0e17e659c, b4a2a1900bab5b6e405cc78b72c5d1706c789b309bc1fa27ad746153ccb84004, 3905126f5f9f7430dee31c207706852e56292291449b563781bc6ee0b540343a,

TYPE	VALUE
SHA256	d4007f1ac2cb3a48db4bde7dbab7255421bf64f768a06492b81087f67a2e6c9c, e03580729f2f09dbd937d685fc9229959e84c9f329bee7eee16536bb8f9e60cf, 81c775f9540a66fded643fe4ec53dbbf35742bd3b069d95d689da313fc9b80a9

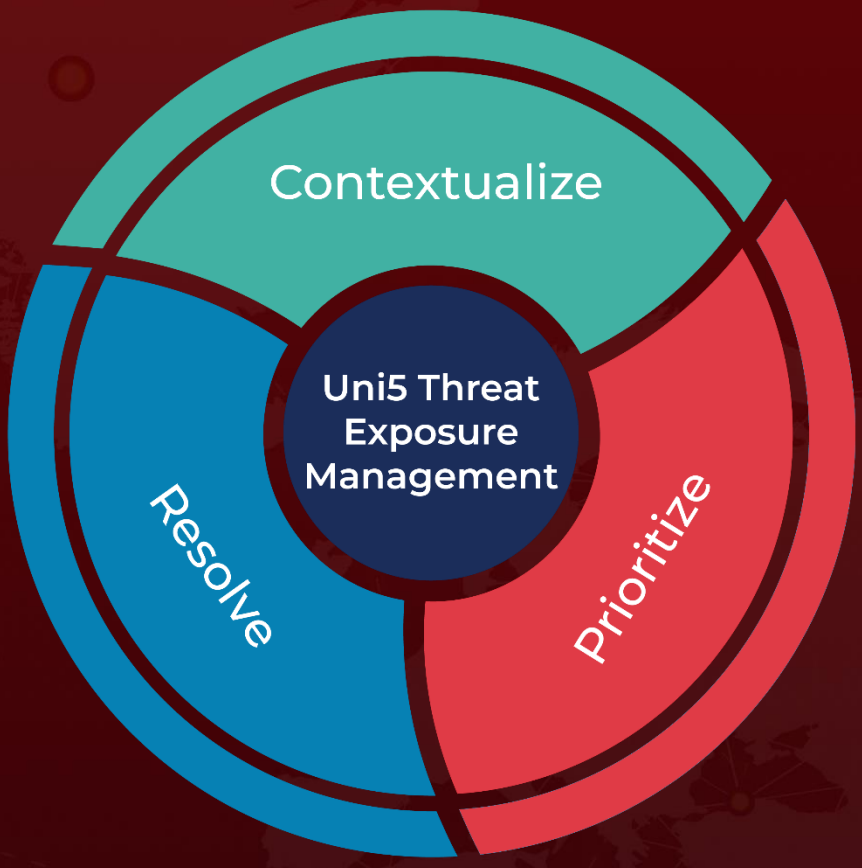
References

https://nsfocusglobal.com/over-300000-gorillabot-the-new-king-of-ddos-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 9, 2024 . 5:30 AM

More at www.hivepro.com