Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

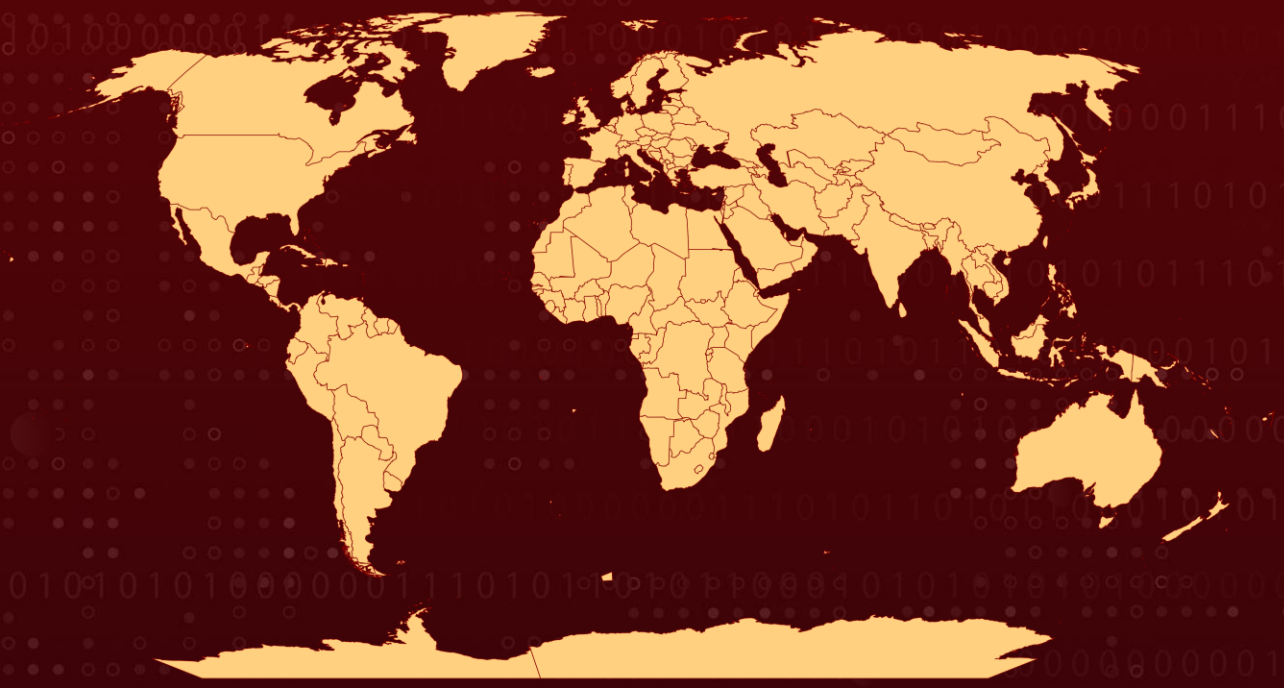
A new botnet called the "Medusa Botnet" is emerging via Mirai Botnet targeting Linux users

Date of Publication	Admiralty Code	TA Number
February 6, 2023	A1	TA2023064

Summary

First appeared: 2016
Attack Region: Worldwide
Impacted Platform: Linux
Attack: The "Medusa Botnet" is a newly discovered botnet that is capable of carrying out DDoS, ransomware, and brute force attacks.

Attack Regions



Attack Details

#1

Mirai is a botnet that has been active since 2016 and exploits vulnerabilities in Linux-based networking devices like routers and IoT devices to gain control and perform malicious activities like DDoS attacks and downloading additional malware. The Mirai botnet has recently been seen downloading and spreading a new botnet called the "Medusa Botnet."

#2

The Medusa Botnet is written in Python and can perform various malicious activities like DDoS attacks, Ransomware attacks, and brute force attacks. The Ransomware aspect of the botnet encrypts targeted files and displays a ransom note, although the code appears to be faulty. The botnet uses a Python library to encrypt files with AES 256-bit encryption and can launch attacks on different levels of the network hierarchy.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	**TA0007** Discovery	**TA0010** Exfiltration	**TA0040** Impact
T1518.001 Security Software Discovery	**T1518** Software Discovery	**T1499** Endpoint Denial of Service	**T1571** Non-Standard Port
T1027 Obfuscated Files or Information	**T1110** Brute Force	**T1486** Data Encrypted for Impact	**T1095** Non-Application Layer Protocol
T1071 Application Layer Protocol	**T1055** Process Injection		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2491bb75c8a3d3b8728ab46a933cd81f8176c1f9d7292faeecea67d71ce87b5c 87b5ba7da8aa64721baca0421a01e01bb1f1ca8a2f73daa3ca2f5857e353c182 2f2759b5933f06c9fdbc87ea941e8ef53ea0e3b715afd57de52ed2927d197c33 bce94b214a6bae00b03ada34c66210d9143895d6c0be9e21c10e9951cc469fbf 48f5f09ddd7089a9397d26e219eb1a1a937c3238f7ecdc7cdfc5383141d77ad9 5799ee35a334f839bb666a0136ca2615390d0b7fb6a14875bafbfab3414045e9
SHA1	54c67bb062d73ae9fabf5f0e1e2136e05cb6e69b c059eec897c48b81cfc6a6765e176cc88231c31e 088332f4ff6b6a12f094a429d6f60ec500d3d85b dc6ea04feb31eb9539f577d7965d0fb925dd7e52 3bcbc498de18d91a1d05e428fa94e4145959fbd2 B2134b18e827402378da09a8dcd9da92509e8131
URLs	medusa-stealer[.]cc hxxp://45.145.167[.]117/medusa_stealer.sh

TYPE	VALUE
MD5	ed64d941fd8603196c0e31ae58c1992d e3a08ffb7106ece9612d3aa8078a8287 336674857b5ede1e09daeff1a14adedc ed24c7c0b73887e35f1c12ab0dda98fe 14655930fab2319ff9cd5187a0caa242 1eee2293e51b01300c75b649715e472d

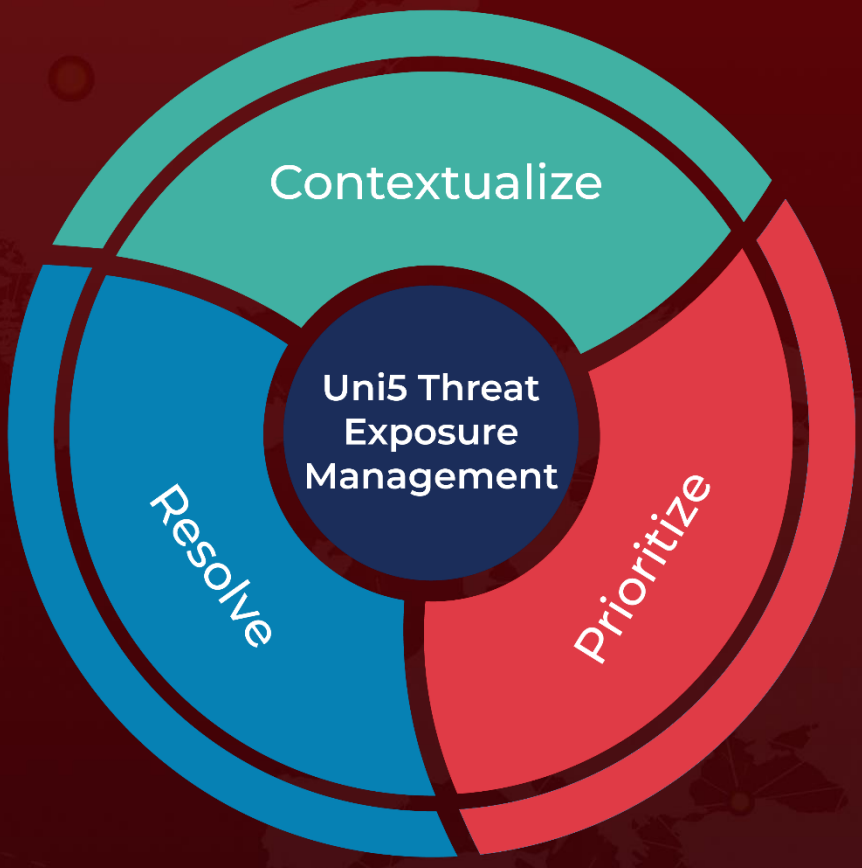
References

https://blog.cyble.com/2023/02/03/new-medusa-botnet-emerging-via-mirai-botnet-targeting-linux-users/

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

February 6, 2023 • 11:45 PM

More at www.hivepro.com