Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

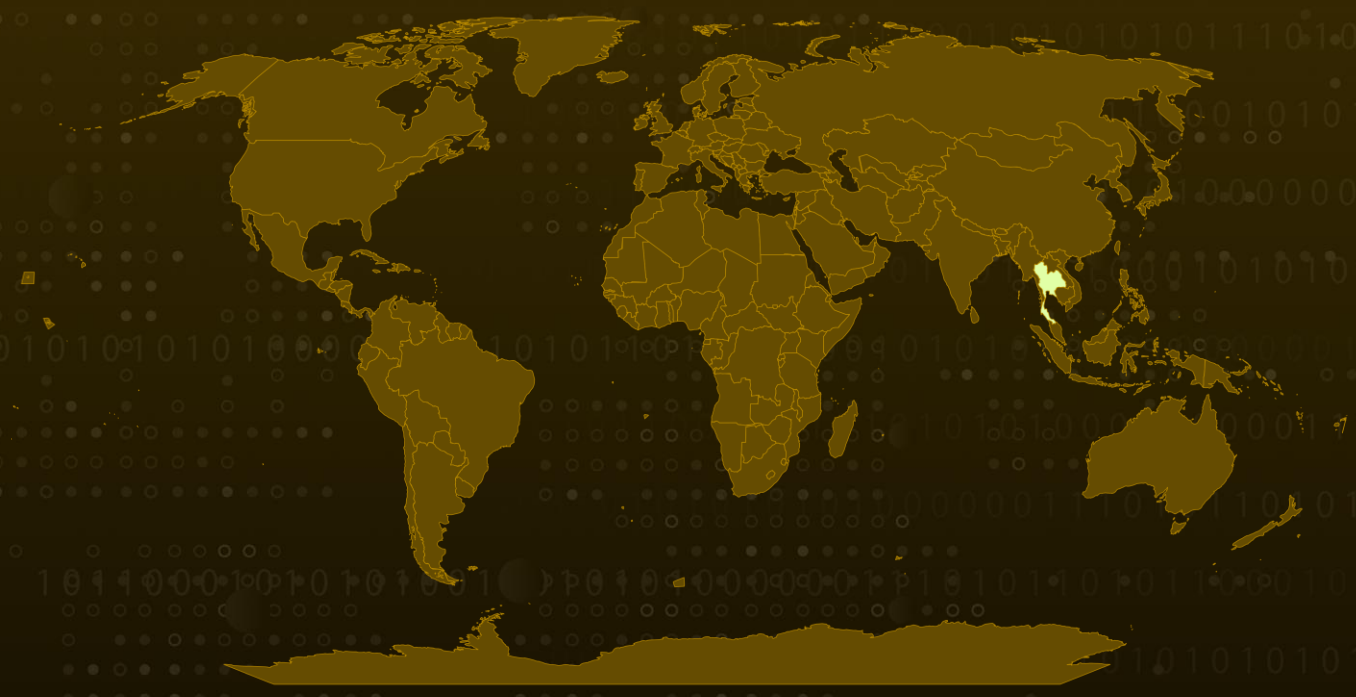
New Linux Krasue RAT Targeting Telecom Companies in Thailand

Date of Publication	Admiralty Code	TA Number
December 8, 2023	A1	TA2023495

Summary

First appeared: 2021
Attack Region: Thailand
Targeted Industry: Telecommunications
Malware : KrasueRAT, XorDdos Trojan
Affected Platform : Linux
Attack: Krasue, a new Linux Remote Access Trojan, targets Thai organizations, primarily in telecommunications, using embedded rootkits and a unique RTSP-based communication tactic. Believed to be connected to XorDdos, it evades detection through various stealth measures, emphasizing the importance of heightened cybersecurity vigilance.

Attack Regions



Attack Details

#1 A newly discovered Linux Remote Access Trojan (RAT), named Krasue, has been targeting organizations in Thailand, particularly in the telecommunications sector, since 2021. This malware enables attackers to gain remote access to targeted networks and employs embedded rootkits for different Linux kernel versions.

#2 Krasue stands out for using Real-Time Streaming Protocol (RTSP) messages as a disguised "alive ping," a rare tactic in the wild. It is believed to be deployed in the later stages of an attack chain, facilitating persistent access to victim hosts, potentially as part of a botnet or sold by initial access brokers.

#3 The RAT has similarities to the XorDdos Linux Trojan, documented by Microsoft in March 2022, suggesting a shared authorship or access to its source code. Krasue has managed to evade detection through tactics such as poor Endpoint Detection & Response coverage on older Linux servers, packed malware samples, and stealth mechanisms, including UPX packing, daemonization, and the disregard of interrupt signals.

#4 The malware establishes communication through a UDP socket server with a command and control (C2) server, utilizing AES-CBC encryption. Its rootkit, based on open-source projects, conceals its presence, hooks system calls, and communicates with the C2 using RTSP messages. While Krasue's core functionalities differ from XorDdos, the rootkit segments exhibit substantial overlaps, indicating a potential connection between the two. The discovery underscores the need for continuous vigilance and enhanced security measures to counter the evolving threat posed by Krasue.

Recommendations

Monitor RTSP Traffic: Pay close attention to Real-Time Streaming Protocol (RTSP) traffic on your network. Anomalies in RTSP communication, especially unexpected patterns or unusual volumes, could be indicative of malicious activity.

Enable Kernel Module Signature Verification: Configure your Linux kernel to load only signed modules. This ensures that modules with valid digital signatures from trusted sources are the only ones allowed to load, preventing the execution of unsigned or tampered modules.

Monitor System and Network Logs: Regularly review system and network logs for any signs of unusual or suspicious activities. Pay attention to unauthorized access attempts, unexpected network traffic, and any anomalies that could indicate a security incident.

Software and System Updates: Regularly update operating systems, software, and applications to patch vulnerabilities. Implement automatic updates to ensure timely patching and security improvements. In case of download software and packages obtain from reputable and official sources only.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0011** Command and Control	**TA0005** Defense Evasion
TA0003 Persistence	**TA0042** Resource Development	**TA0006** Credential Access	**T1573** Encrypted Channel
T1583 Acquire Infrastructure	**T1014** Rootkit	**T1036** Masquerading	**T1110** Brute Force
T1583.005 Botnet	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits
T1027 Obfuscated Files or Information	**T1572** Protocol Tunneling	**T1059.004** Unix Shell	**T1059** Command and Scripting Interpreter
T1027.002 Software Packing	**T1564.001** Hidden Files and Directories	**T1564** Hide Artifacts	**T1071.001** Web Protocols
T1071 Application Layer Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	128.199.226[.]11
MD5	100a5f3875e430f6de03d99752fbb6a7, 5055925b5bcd715d5b70b57fdbeda66b
SHA1	051bc3273a20a53d730a3beaff2fadcd38d6bb85, eddb4476ca610f3c5e895f4811c9744704552d2f
SHA256	38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353, 3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59, 4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1, 8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831, 902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc, 97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772, afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4, b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d, c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5, e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632, ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f

References

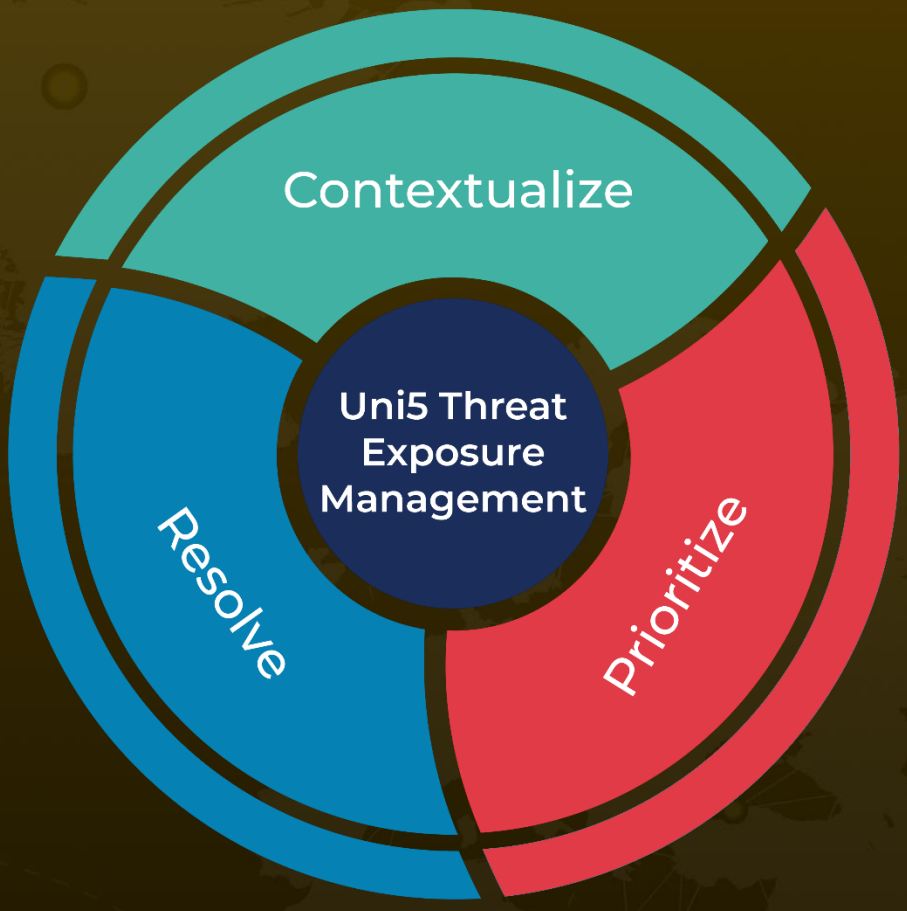
https://www.group-ib.com/blog/krasue-rat/

https://www.hivepro.com/threat-advisory/a-new-xorddos-linux-trojan-that-launches-powerful-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

December 8, 2023 • 5:00 AM

More at www.hivepro.com