BLACKSWAN CYBERSECURITY

THREAT ADVISORY

December 8, 2023

Krasue RAT Linux Malware

SUMMARY

Krasue is a remote access trojan (RAT) designed for Linux systems, specifically within telecommunications companies in Thailand. Krasue was identified by security researchers at Group-IB and has been seen successfully evading detection since 2021. Analyzing the Krasue binary found seven different variants of a rootkit that supports various versions of the Linux kernel. This RAT appears to be constructed with code derived from three distinct open-source projects.

TECHNICAL DETAILS

Group-IB provided details of their analysis of Krasue, including its primary function of ensuring persistent access to the infected host system. This persistence may also indicate potential deployment via a botnet or distribution by initial access brokers for threat actors looking for specific targets. Although the method of distribution remains unclear, potential vectors include exploiting vulnerabilities, credential brute force attacks, or disguising itself as a legitimate product when downloaded from untrusted sources. Krasue seems to be concentrating its efforts on targeting telecommunications companies in Thailand.

Group-IB's analysis of the rootkit embedded within the Krasue binary found that it operates as a Linux Kernel Module (LKM), presenting itself as an unsigned VMware driver upon execution and at the same security level as the underlying operating system. The rootkit's compatibility with Linux Kernel versions 2.6x/3.10.x allows it to go undetected, exploiting the limited Endpoint Detection and Response coverage on older Linux servers. All seven iterations of the embedded rootkit have consistent system call and function call hooking capabilities. Examination of the code found that Krause is derived from three open-source LKM rootkits—Diamorphine, Suterusu, and Rooty—all of which have been available since 2017.

Capabilities of Krasue include port manipulation, process invisibility, root privilege provision, execution of the kill command for any process ID, and adept concealment of malware-related files and directories. When communicating with a command and control (C2), Krasue responds to commands that include ping responses, master configuration settings, information retrieval requests, restart and respawn processes, and even self-termination commands.

Group-IB's investigation found 9 distinct C2 IP addresses hardcoded into the malware, with address utilizing port 554 that is associated with Real Time Streaming Protocol (RTSP) connections. The utilization of RTSP for C2 communication adds a distinctive characteristic to Krasue's behavior.

Though Krasue's origin is still unclear, researchers have observed overlaps with XorDdos Linux malware, suggesting a potential common author or operator. It is also plausible that the Krasue developer had access to the code of XorDdos.

RECOMMENDATIONS

- Consider reviewing the Group-IB provided indicators of compromise (IOCs) and YARA rules for detection, potentially encouraging collaborative research efforts among the cybersecurity community.
- Implement network traffic monitoring to detect and analyze unusual patterns, especially on port 554, as Krasue utilizes this uncommon approach for communication.

- Strengthen EDR solutions to ensure comprehensive coverage, especially on older Linux servers where Krasue exploits potential vulnerabilities.
- Conduct regular security audits to identify and address vulnerabilities promptly. Implement robust patch management practices to ensure that systems are up-to-date and protected against known exploits.
- Employ behavioral analysis tools and anomaly detection mechanisms to identify suspicious activities, particularly those associated with rootkit functionalities such as process invisibility and port manipulation.
- Enforce multi-factor authentication (MFA) to mitigate the risk of credential brute force attacks, a potential avenue for Krasue's distribution.
- Educate users about the risks associated with downloading software from untrusted sources, emphasizing the importance of obtaining applications from reputable repositories.

INDICATORS OF COMPROMISE

Hashes:

- 902013bc59be545fb70407e8883717453fb423a7a7209e119f112ff6771e44cc
- b6db6702ca85bc80599d7f1d8b1a9b6dd56a8e87c55fc831dc9c689e54b8205d
- ed38a61a6b7af436120465d352baa4cdf4ed8f01a7db7245b6254353e52f818f
- afbc79dfc4c7c4fd9b71b5fea23ef12adf0b84b1af22a993ecf91f3d829967a4
- 97f08424b14594a5a39d214bb97823690f1086c78fd877558761afe0a032b772
- 38ba7790697da0a736c80fd9a04731b8b0bac675cca065cfd42a56dde644e353
- e0748b32d0569dfafef6a8ffd3259edc6785902e73434e4b914e68fea86e6632
- 4428d7bd7ae613ff68d3b1b8e80d564e2f69208695f7ab6e5fdb6946cc46b5e1
- c9552ba602d204571b9f98bd16f60b6f4534b3ad32b4fc8b3b4ab79f2bf371e5
- 3e37c7b65c1e46b2eb132f98f65c711b4169c6caeeaecc799abbda122c0c4a59
- 8a58dce7b57411441ac1fbff3062f5eb43a432304b2ba34ead60e9dd4dc94831

IP Address(es):

- 128.199.226[.]11:554

REFERENCES

- https://www.group-ib.com/blog/krasue-rat/
- https://thehackernews.com/2023/12/new-stealthy-krasue-linux-trojan.html
- https://www.bleepingcomputer.com/news/security/krasue-rat-malware-hides-on-linux-servers-using[1]embedded-rootkits