Mphasis
The Next Applied

Snake malware steals SSH keys to spread across the network

Date: 22nd February 2024 | Severity: High

Summary

A new version of White Snake Stealer, an information stealer which targets Windows and Linux systems, has been released by cyber security firm, Microsoft, and the University of California, Los Angeles.

A threat actor is using an open-source network mapping tool named SSH-Snake to look for private keys undetected and move laterally on the victim infrastructure.

SSH-Snake was discovered by the Sysdig Threat Research Team (TRT), who describe it as a "self-modifying worm" that stands out from traditional SSH worms by avoiding the patterns typically associated with scripted attacks.

The worm searches for private keys in various locations, including shell history files, and uses them to stealthily spread to new systems after mapping the network.

Attack Vectors

Tactic: Lateral Movement

The researchers say that one particularity of SSH-Snake is the ability to modify itself and make itself smaller when running for the first time. It does this by removing comments, unnecessary functions, and whitespace from its code.

Designed for versatility, SSH-Snake is plug-and-play yet allows customizing for specific operational needs, including adapting strategies to discover private keys and identify their potential use.

Sysdig’s analysts confirmed SSH-Snake’s operational status after discovering a command and control (C2) server used by its operators to store data harvested by the worm, including credentials and victim IP addresses.

This data shows signs of active exploitation of known Confluence vulnerabilities (and possibly other flaws) for initial access, leading to the deployment of the worm on these endpoints.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	Snake malware IOCS.xlsx

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://www.bleepingcomputer.com/news/security/new-ssh-snake-malware-steals-ssh-keys-to-spread-across-the-network/

https://otx.alienvault.com/pulse/64a3e7f5b11f005642279d47