OWASP
Open Web Application Security Project

Be Warned of this evolving Autom Crypto-mining Malware Attacks Using upgraded evasion Tactics

LEARN MORE

The early attacks...
1:12 PM techniques,...
Notes

The early attacks...
1:11 PM a vanilla ima...
Notes

A crypto mining c...
1:10 PM evolving def...
Notes

17 January 2022 at 1:10 PM

A crypto mining campaign has been ongoing for years and is continuously evolving defence evasion tactics to stay undetected. The campaign is named Autom owing to the shell script that started the attack.

According to researchers, the campaign has been ongoing for the past three years and evolved to stay hidden.

- It was first detected in 2019 and since then 84 attacks have been discovered using the same shell script.
- In 2020, cybercriminals were evading defence by bypassing security features and then started using an obfuscating script in 2021.
- Attackers launched at least 125 attacks only in the third quarter of 2021.

The early attacks...
1:12 PM techniques,...
Notes

The early attacks...
1:11 PM a vanilla ima...
Notes

A crypto mining c...
1:10 PM evolving def...
Notes

17 January 2022 at 1:11 PM

The early attacks were executing a malicious command while running a vanilla image named as alpine: latest that eventually downloaded a shell script, autom[.]sh.

- The command that was added to the official image to perform the attack has hardly changed in the past years. However, the shell script is now downloaded from a different server.
- The shell script starts the attack, allows the attackers to create a new user account, (akay), and upgrade privileges to a root user for running arbitrary commands to mine cryptocurrency.

The early attacks...
1:12 PM techniques,...
Notes

The early attacks...
1:11 PM a vanilla ima...
Notes

A crypto mining c...
1:10 PM evolving def...
Notes

17 January 2022 at 1:12 PM

The early attacks of the campaign in 2019 had no special obfuscating techniques, which it later developed.

- The malware can disable security mechanisms and obtain an obfuscated mining shell script that was Base64-encoded around five times to avoid security tools.
- Further, the attacker added concealment capabilities involving downloading log_rotate[.]bin script to launch crypto-mining activity by creating a new cron job to start mining every 55 minutes.

Threat actors driving the Autom campaign have displayed a high level of expertise in launching attacks while staying under the radar. Security teams must up their guards before such threats infect them.