Hildegard: TeamTNT’s New Feature-Rich Malware Targeting Kubernetes

cyware.com/news/hildegard-teamtnts-new-feature-rich-malware-targeting-kubernetes-6587eb45

With consistently improved abilities, TeamTNT has been observed employing a new malware, Hildegard, which carries stealth and persistence capabilities.

TeamTNT’s new trump card

Palo Alto Networks researchers have observed TeamTNT’s Hildegard malware targeting Kubernetes systems at its reconnaissance and weaponization stage in January.

- The attackers have predominantly leveraged misconfigured kubelet agents to gain access to the Kubernetes environments for cryptojacking and potentially exfiltrating sensitive data from tens of thousands of applications running in the clusters.
- The Hildegard malware uses a tmate reverse shell and an IRC channel to establish C&C connections. To disguise the malicious process, it uses a known Linux process name (bioset).
- In addition, for defense evasion, the malware hides malicious processes using library injection and encrypts the malicious payload inside a binary to make the automated static analysis more difficult.

Recent attacks

- In the last month, the group was using a detection evasion tool named libprocesshider, copied from open source repositories.

- TeamTNT hackers had used malicious shell scripts to exfiltrate Docker API logins, along with AWS credentials, and deployed cryptocurrency miners.
- In another research, Palo Alto researchers found an Ezuri loader in the group's recently developed arsenal.
- In December, the TeamTNT group was deploying a distributed denial of service (DDoS) capable IRC bot called TNTbotinger.

Wrapping up

TeamTNT has been continuously expanding its capabilities and arsenal with new tools and malware. Targeting a Kubernetes cluster can be more profitable than a hijacked Docker host. With more sophisticated tactics for initial intrusion, execution, defense evasion, and command and control, the threat actor can be expected to launch a larger-scale attack in the near future.

TeamTNT Palo Alto Hildegard Malware Cryptojacking Cryptojacking Attacks

Publisher

Cyware