UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00153

SILOSCAPE MALWARE TARGETS CONTAINERS

DATE ISSUED: 8th June 2021

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Microsoft is warning of the first malware specifically designed to target Windows containers using known vulnerabilities in web servers and databases in an effort to target and compromise Kubernetes nodes and plant back doors in clusters.

BREAKDOWN

A heavily obfuscated new malware is targeting the popular Windows containers to "escape the silo" and crack into poorly configured Kubernetes clusters, add a backdoor and run malicious containers on the servers. Discovered by Unit 42 researchers with evidence suggesting the malware campaign was launched on victims over a year ago, the malware seeks known vulnerabilities in popular cloud applications, such as web servers, escape from the Windows cluster in Kubernetes by hunting down credentials and spreading throughout the entire cluster. Each new attack features a uniquely compiled version of the code with a unique set of keys and researchers also noted that there were almost no "readable strings in the entire binary" making reverse engineering tricky. It is also impossible to detect or search for using the hash alone or signature-based malware detection tools. Once established, it reaches out to the Command and Control (C2) server via Tor browser to import further malware and carry out other malicious activities. As this is a cloud-based malware, it is suspected that it would likely be used for resource mining such as cryptojacking and Denial of Service (DoS) style attacks.

REMEDIATION STEPS

- Use Hyper-V containers for containers when using containerisation as a security boundary according to Microsoft's guidance.
- Check configuration of Kubernetes clusters to ensure their security.
- Remove any credentials stored in plain text.

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/windows-containers-malware-targets-kubernetes/166692/
Unit 42 – Palo Alto	https://unit42.paloaltonetworks.com/siloscape/
Computer Weekly	https://www.computerweekly.com/news/252501997/Siloscape-malware-a-risk-to-Windows-containers-Kubernetes
Security Week	https://www.securityweek.com/siloscape-malware-targets-windows-server-containers