VIRUS ALERTS

"Siloscape" Malware

Original Issue Date:June 14, 2021

Virus Type: Malware Targeting Windows Containers

It has been reported that a new category of malware is targeting misconfigured Kubernetes clusters through Windows containers to compromise cloud environments. The malware variant gains initial access by exploiting vulnerabilities in common cloud applications or a vulnerable web page or database and then utilizes windows container escape techniques, executes code on underlying node and then spreads in poorly configured Kubernetes clusters to open a backdoor in order to run/deploy malicious containers. Once cluster is compromised, the attacker might be able to steal critical information such as usernames and passwords, an organization¿s confidential and internal files or even entire databases hosted in the cluster. This malware can leverage the computing resources in a Kubernetes cluster for cryptojacking and potentially exfiltrate sensitive data from hundreds of applications running in the compromised clusters.

Behaviour:

- Uses Windows container escape techniques to escape the container and gain code execution on the underlying node.
- Attempts to abuse the node's credentials to spread in the cluster.
- Siloscape uses the Tor proxy and an ".onion" domain to anonymously connect to its command and control (C2) server.

Indicators of Compromise:

SHA 256:

- 5B7A23676EE1953247A0364AC431B193E32C952CF17B205D36F800C270753FCB
- 81046F943D26501561612A629D8BE95AF254BC161011BA8A62D25C34C16D6D2A
- 010859BA20684AEABA986928A28E1AF219BAEBBF51B273FF47CB382987373DB7

Best practices and Countermeasures:

1. Kubernetes cluster configuration should restrict node privileges such that creation of new deployments is not possible. (It means that any process running in Windows Server containers should not have the same privileges as admin). Malware is ineffective in this case.
2. It is advised to follow Microsoft's recommendation of discarding use of Windows containers as a security feature. Hyper-V containers should be employed for operations that rely on containerization as a security boundary and it is recommended to move applications running in Windows Server containers to Hyper-V containers.
3. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
4. Check regularly for the integrity of the information stored in the databases.
5. Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
6. If not required consider disabling, PowerShell / windows script hosting.
7. Restrict users' abilities (permissions) to install and run unwanted software applications.
8. Enable personal firewalls on workstations.
9. Enable Windows Defender Application Guard with designated the trusted sites as whitelisted, so that rest all sites will be open in container to block the access to memory, local storage, other installed applications or any other resources of interest to the attacker.
10. Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers. Repeat audits at regular intervals.
11. Maintain updated Antivirus software on all systems.

References

https://unit42.paloaltonetworks.com/siloscape/
https://www.securityweek.com/siloscape-malware-targets-windows-server-containers
https://docs.microsoft.com/en-us/troubleshoot/windows-server/containers/support-for-windows-containers-docker-on-premises-scenarios

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email:info@cert-in.org.in
Phone: +91-11-24368572

Postal Address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India