# Siloscape malware a risk to Windows containers, Kubernetes

A newly identified malware, dubbed Siloscape by the threat researcher who first spotted it, appears to be the first-recorded malware to target Windows containers, and presents a potential risk to badly configured enterprise clouds.


Trust no one

Zero trust is a security model that eliminates the traditional perimeter and assumes that no user or device can be trusted until proven otherwise. In this handbook, get expert advice on how your organisation can take a zero-trust approach to securing its network, devices and workforce.

Prizmant of Palo Alto's Unit 42 research unit in March 2021, Siloscape is an obfuscated malware that targets Windows containers and from there, attempts to open a backdoor into poorly configured Kubernetes clusters where it runs malicious containers.

Prizmant said the emergence of a malware targeting Windows containers was unsurprising given the surge in cloud adoption in the past few years. He named it Siloscape because its primary goal is to escape the container, which in Windows is implemented mainly by a server silo.

He said that compromising an entire Kubernetes cluster was much more damaging than a single container, as it can run multiple cloud apps, whereas a single container would more usually run just one.

"The attacker might be able to steal critical information such as usernames and passwords, an organisation's confidential and internal files or even entire databases

hosted in the cluster. Such an attack could even be leveraged as a ransomware attack by taking the organisation's files hostage," said Prizmant in a newly published disclosure blog.

"Even worse, with organisations moving to the cloud, many use Kubernetes clusters as their development and testing environments, and a breach of such an environment can lead to devastating software supply chain attacks."

The malware works thus: it first targets common cloud apps such as web servers and accesses them via known vulnerabilities, uses the Windows container escape technique to escape from there to gain code execution on the underlying node, then attempts to abuse the node's credentials to spread further through the Kubernetes cluster.

It then uses the Tor proxy and a .onion domain to connect back to its command and control (C2) server to receive further commands. In the course of his research, Prizmant also gained access to this server, where he and the Unit 42 team found evidence of 23 active victims, and found that the server was hosting a total of 313 users, which may imply Siloscape sits as just one element of a much broader, long-running campaign of cyber-attacks.

Prizmant reiterated that unlike most cloud malwares that confine themselves to activities such as resource hijacking or denial of service (DoS), Siloscape should be considered especially dangerous because it is not limited to specific goals and can be used for many other kinds of attack.

"Any process running in Windows Server containers should be assumed to have the same privileges as admin on the host, which in this case is the Kubernetes node. If you are running applications in Windows Server containers that need to be secured, we recommend moving these applications to Hyper-V containers.

"Furthermore, administrators should make sure their Kubernetes cluster is securely configured. In particular, a secured Kubernetes cluster won't be as vulnerable to this specific malware as the nodes' privileges won't suffice to create new deployments. In this case, Siloscape will exit," he added.

https://www.computerweekly.com/news/252501997/Siloscape-malware-a-risk-to-Windows-containers-Kubernetes

https://www.bankinfosecurity.com/siloscape-malware-reportedly-targeting-windows-containers-a-16820