January, 2023

MULTIPLE CVEs

DragonSpark Attack | SparkRAT

Context

The DragonSpark Attack is a sophisticated attack that utilizes a tool called SparkRAT. SparkRAT is a Remote Access Trojan that can run on multiple platforms and is developed using the Go programming language. The attack was first discovered by SentinelLabs and is carried out by compromising infrastructure located in China, Hong Kong, Taiwan, Singapore, and the United States. The attacker uses this compromised infrastructure to deploy malware and a variety of other tools. To execute code from the malware binaries, the attackers use a technique called Golang source code interpretation, which allows them to create a reverse shell for remote code execution. This technique makes it difficult to detect the attack because most endpoint security software assesses the behavior of compiled code, rather than the source code itself.

Mitigation

To prevent DragonSpark Attack, it is recommended to follow the below mitigation actions:

- Review and restrict external access to exposed services.
- Keep all software up-to-date, including anti-virus and anti-malware software.
- Use application allowlisting to prevent installation of unauthorized applications and to control how authorized applications and tools interact with their environment and the Internet.
- Block traffic to and from high risk infrastructures using both tactical and operational threat intelligence.

Technical Details

Tactics, Techniques and Procedures

The attackers are exploiting web servers and MySQL database servers that are publicly accessible on the internet to gain initial entry. To achieve this, they utilize a tool called China Chopper to deploy webshells on these servers. The webshells are injected into the servers using various methods such as SQL injection, cross-site scripting, or exploiting vulnerabilities within the web server software.

BadPotato and SharpToken are tools that allow an attacker to escalate their privileges on Windows machines and execute commands with the highest level of access, SYSTEM privileges.

GotoHTTP is a tool that can be used to remotely access and control computers, regardless of the operating system they are running on. It includes features such as file transfer, screen view, and the ability to establish persistence.

The threat group used a custom-built malware called ShellCode_Loader to execute malicious code on the targeted systems. This malware is written in Python and packaged using PyInstaller.

Another custom-built malware used by the group is called m6699[.]exe. It is written in the programming language Golang and uses a technique called source code interpretation at runtime. This technique makes it harder for static analysis mechanisms to detect the malware, allowing the threat actors to evade detection.

Cyber Threat Intelligence

While there is no conclusive evidence linking DragonSpark to other hacking groups, it is likely that the threat actor behind DragonSpark is of Chinese origin. This is based on the fact that SparkRAT and several other tools used in the attacks were developed by Chinese-speaking developers.

The threat actor behind SparkRAT is continuously adding new features to the tool, and is able to leverage various other tools. Moreover, it has the ability to upgrade itself automatically, which indicates that it will likely continue to be used by multiple threat actor groups. While there is evidence that these threat actors are sharing such tools, there is no evidence of any direct linkage between them.

References

Related IOC's

https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/

Public Intelligence

https://www.sentinelone.com/labs/dragonspark-attacks-evade-detection-with-sparkrat-and-golang-source-code-interpretation/

https://www.bleepingcomputer.com/news/security/hackers-use-golang-source-code-interpreter-to-evade-detection/

https://en.wikipedia.org/wiki/Go_(programming_language)

https://github.com/golang/go

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.