Exploring the Depths of SolarMarker's Multi-tiered Infrastructure

recordedfuture.com/exploring-the-depths-of-solarmarkers-multi-tiered-infrastructure

Research (Insikt)

Posted: 13th May 2024

By: Insikt Group®

SolarMarker, a malware known for stealing information, utilizes an evolving, multi-tiered infrastructure that has been active since 2021. This malware, also known as Yellow Cockatoo and Jupyter Infostealer, targets sectors such as education, healthcare, and SMEs. To avoid detection, it employs advanced evasion techniques like Authenticode certificates and large zip files.

SolarMarker's Multi-tiered Infrastructure and its Impact

The SolarMarker malware, also referred to as Yellow Cockatoo, Polazert, and Jupyter Infostealer, has steadily evolved since 2020. The sophisticated and resilient threat actor behind SolarMarker has constructed a multi-tiered infrastructure that swiftly rebuilt infrastructure post-compromise and employs tactics to avoid detection or disruption by law enforcement.

SolarMarker uses advanced evasion techniques such as Authenticode certificates, which lend an air of legitimacy to its malicious payloads, and uses large zip files to bypass antivirus software.

The core of SolarMarker's operations is its layered infrastructure, which consists of at least two clusters: a primary one for active operations and a secondary one likely used for testing new strategies or targeting specific regions or industries. This separation enhances the malware's ability to adapt and respond to countermeasures, making it particularly difficult to eradicate.

Recorded Future Network Intelligence has revealed a substantial number of victims across multiple sectors, including education, healthcare, government, hospitality, and small and medium-sized enterprises. The malware targets both individuals and organizations, stealing vast amounts of data that could be sold on criminal forums, leading to further exploitation and attacks.

In the short term, defense against SolarMarker should include enforcing application allow-lists to prevent downloading seemingly legitimate files containing malware. If allow-lists aren't viable, businesses should conduct thorough security training for employees to recognize signs of a potential breach, such as unexpected file downloads or redirects that could indicate malvertising.

As detailed in the report's appendix, the use of YARA and Snort rules is crucial for detecting current and historical infections. Given the malware's evolving nature, regular updates to these rules, combined with additional detection methods like analyzing network artifacts, are essential.

In the long term, monitoring the cybercriminal ecosystem is important for anticipating new threats. Organizations should refine their security policies and enhance their defense mechanisms to stay ahead of threat actors like those behind SolarMarker. This includes better regulatory measures targeting the cybercriminal infrastructure and law enforcement efforts to tackle these threats at their source.

To read the entire analysis, click here to download the report as a PDF.

Related