TALOS
Cisco Security Research

SolarMarker tries to take victims around the galaxy

VIEW BLOG POST

This information-stealer is adding new tools, including the recently discovered “Mars” and “Uranus”

SUMMARY

Cisco Talos has observed new activity from Solarmarker, a highly modular .NET-based information stealer and keylogger. A previous staging module, “d.m,” used with this malware has been replaced by a new module dubbed “Mars.” Another previously unreported module named “Uranus” has been identified.

WHAT’S NEW?

Cisco Talos has observed new activity from Solarmarker, a highly modular .NET-based information stealer and keylogger. A previous staging module, “d.m,” used with this malware has been replaced by “Mars.”

HOW DID IT WORK?

Victims usually download Solarmarker’s parent malicious PE files through generic-looking, fake file-sharing pages hosted across free site services, but many of the dummy accounts had become inactive between the time we found the filenames used by Solarmarker’s droppers in our telemetry and attempting to find their download URLs. These links direct the victim to a page offering the ability to download the file as either a PDF or Microsoft Word file. Following the download link sends the victim through multiple redirects across varying domains before landing on a final download page.

SO WHAT?

Organizations should be particularly concerned about the modular nature and information stealing capabilities of this malware family. Using its staging DLL, the malware can then execute whichever payload module they choose, some of which may be previously undiscovered. The modules already observed make potential victims vulnerable to having sensitive information stolen, including employees' browser usage, such as if they enter their credit card number or other personal information. These attackers may also look to steal login credentials, which could then be used for lateral movement into other systems or to access and steal even more enticing data, such as a customer or patient medical information database.

COVERAGE

PRODUCT	PROTECTION
Cisco Secure Endpoint	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS	✓
Cisco Secure Network Analytics	N/A
Cisco Secure Cloud Analytics	N/A
Cisco Secure Malware Analytics	✓
Umbrella	N/A
Cisco Secure Web Appliance	N/A

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org. SIDs 50447 has been released to detect this threat.

The following ClamAV signatures have been released to detect this threat as well as tools and malware related to these campaigns:

- Win.Trojan.Solarmarker-9832983-0
- Win.Dropper.SolarMarker-9867952-0
- Win.Trojan.Jupiter-9858780-0

Cisco Secure Endpoint (AMP) users can use Orbital Advanced Search to run complex OSqueries to see if their endpoints are infected with this specific threat.