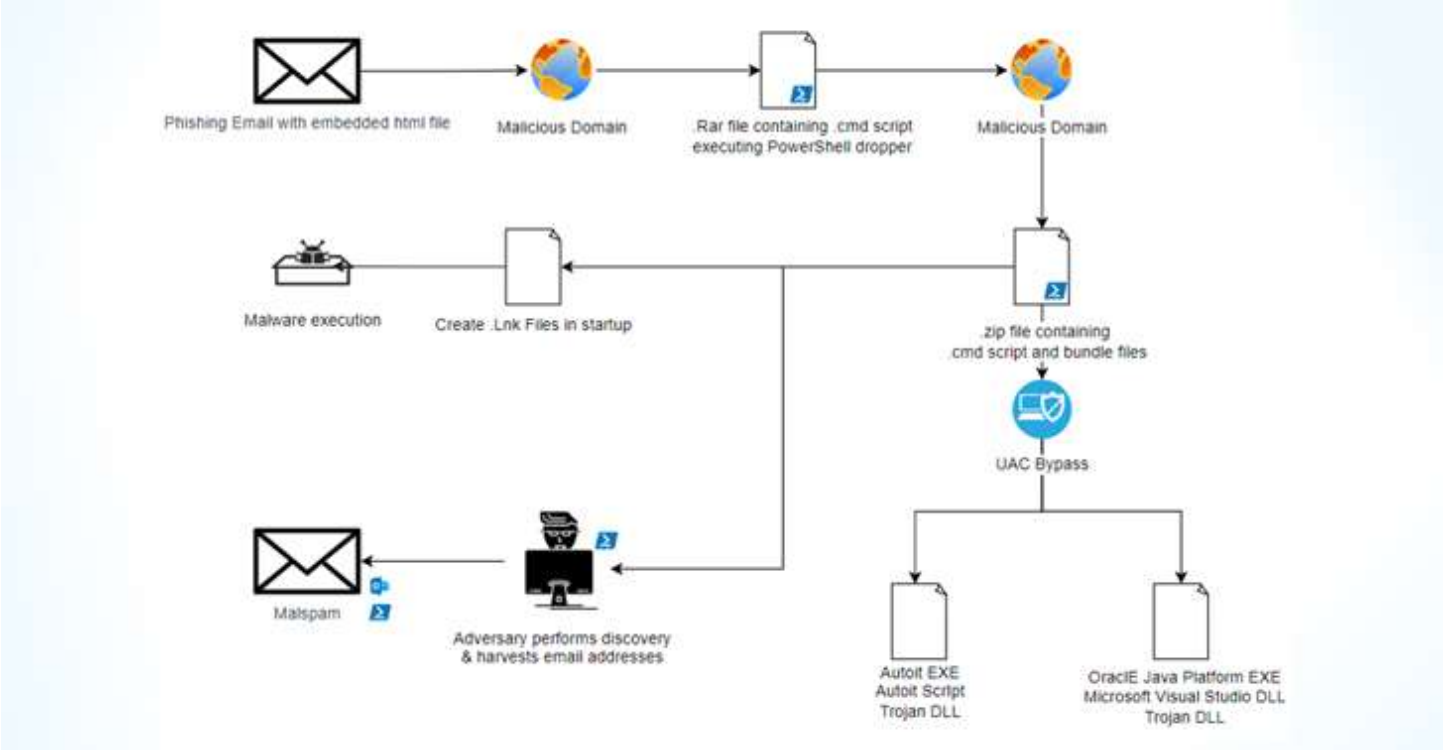
Casbaneiro Banking Malware Goes Under the Radar with UAC Bypass Technique

Jul 25, 2023 THN



The financially motivated threat actors behind the **Casbaneiro** banking malware family have been observed making use of a User Account Control (UAC) bypass technique to gain full administrative privileges on a machine, a sign that the threat actor is evolving their tactics to avoid detection and execute malicious code on compromised assets.

"They are still heavily focused on Latin American financial institutions, but the changes in their techniques represent a significant risk to multi-regional financial organizations as well," Sygnia said in a statement shared with The Hacker News.

Casbaneiro, also known as Metamorfo and Ponteiro, is best known for its banking trojan, which first emerged in mass email spam campaigns targeting the Latin American financial sector in 2018.

Infection chains typically begin with a phishing email pointing to a booby-trapped attachment that, when launched, activates a series of steps that culminate in the deployment of the banking malware, alongside scripts that leverage living-off-the-land (LotL) techniques to fingerprint the host and gather system metadata.

Also downloaded at this stage is a binary called Horabot that's designed to propagate the infection internally to other unsuspecting employees of the breached organization.

"This adds credibility to the email sent, as there are no obvious anomalies in the email headers (suspicious external domains), which would typically trigger email security solutions to act and mitigate," the cybersecurity company said in a previous report published in April 2022. "The emails include the same PDF attachment used to compromise the previous victim hosts, and so the chain is executed once more."

What's changed in recent attack waves is that the attack is kick-started by spear-phishing email embedded with a link to an HTML file that redirects the target to download a RAR file, a deviation from the use of malicious PDF attachments with a download link to a ZIP file.

A second major change to the modus operandi concerns the use of fodhelper.exe to achieve a UAC bypass and attain high integrity level execution.

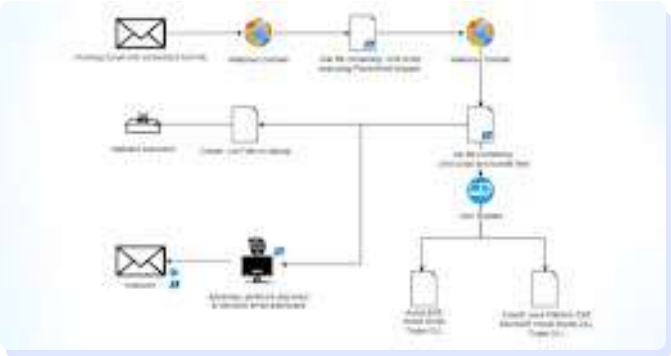
Sygnia said it also observed Casbaneiro attackers creating a mock folder on C:\Windows[space]\system32 to copy the fodhelper.exe executable, although the specially crafted path is said to have never been employed in the intrusion.

"It is possible that the attacker deployed the mock folder to bypass AV detections or to leverage that folder for side-load DLLs with Microsoft-signed binaries for UAC bypass," the company said.

The development marks the third time the mock trusted folder approach has been detected in the wild in recent months, with the method used in campaigns delivering a malware loader called DBatLoader as well as remote access trojans like Warzone RAT (aka Ave Maria).

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

Breaking News



Casbaneiro Banking Malware Goes Under the Radar with UAC B...

macOS Under Attack: Examining the Growing Threat and User ...

TETRA:BURST — 5 New Vulnerabilities Exposed in Widely Used...

How MDR Helps Solve the Cybersecurity Talent Gap...

Cybersecurity Resources

Protect Your Devices – Download McAfee Antivirus Now

Security Controls Tools You Can Use

The Ultimate Guide to Vulnerability Scanning

Earn a Master's in Cybersecurity Risk Management

Join 110,000+ Professionals

Sign up for free and start receiving your daily dose of cybersecurity news, insights and tips.

Your e-mail address

Connect with us!





Company

About THN

Advertise with us

Contact

Pages

Webinars

Deals Store

Privacy Policy

Contact Us