Talos
Cisco Security Research

ServHelper serves up new victims for Group TA505

VIEW BLOG POST

This threat actor is stealing credit card data with the Raccoon and Amadey malware families

SUMMARY

Group TA505 has been active for at least seven years, making wide-ranging connections with other threat actors involved in ransomware, stealing credit card numbers and exfiltrating data. One of the common tools in TA505's arsenal is ServHelper. In mid-June, Cisco Talos detected an increase in ServHelper's activity. We found that ServHelper is being installed onto the targeted systems using several different mechanisms, including other malware families such as Raccoon and Amadey.

WHAT'S NEW?

Although ServHelper has existed since at least early 2019, we detected the use of other malware families to install it. The installation comes as a GoLang dropper, .NET dropper or PowerShell script. Its activity is generally linked to Group TA505, but we cannot be certain that they are the exclusive users of this RAT.

HOW DID IT WORK?

One path for infection starts with the compromise of a legitimate site that hosts cryptographically signed MSI installers. These install popular software, such as Discord. However, they also launch a variant of the Raccoon stealer, which downloads and installs a ServHelper RAT if instructed by the command and control (C2) server. Attackers also deploy the RAT with a variant of the Amadey malware.

SO WHAT?

Although many threat actors, such as TA505 or its associated groups – to which we attribute these campaigns with moderate confidence – have been affected by the arrests of several CLOP members in Ukraine, they continued to operate using a different set of tools. These attacks are geared toward taking control over the infected systems and stealing confidential data which the group will likely leverage for financial gain later.

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 is ideally suited to prevent the execution of the malware detailed in this post. New users can try Cisco Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Firewall and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Malware Analytics helps identify malicious binaries and build protection into all Cisco Security products.

Cisco Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

The following SNORT® rules have been released to detect this threat:
57693 - 57717.