# New sLoad malware downloader being leveraged by APT group TA554 to spread Ramnit

cyware.com/news/new-sload-malware-downloader-being-leveraged-by-apt-group-ta554-to-spread-ramnit-7d03f2d9

- sLoad comes packed with sophisticated reconnaissance capabilities and has also been distributing other malware variants like Gootkit, Ursniff and more.
- The new campaign has been targeting financial institutions across Italy, Canada, and the UK.

A new malware downloader dubbed sLoad has been discovered active in the wild. The malware downloader comes packed with sophisticated reconnaissance capabilities and has been distributing the notorious Ramnit banking trojan.

The malware duo is being leveraged by a threat group called TA554, who has been targeting financial institutions across Italy, Canada and the UK. TA554 has been active since 2017. However, its latest campaign began in May 2018.

## sLoad capabilities

sLoad is capable of conducting reconnaissance operations such as gathering system information like a list of running processes, the presence of Outlook, and the presence of Citrix-related files. sLoad is also capable of checking the DNS cache for a particular domain, such as that of a targeted bank. What is more, the malware downloader can also take screenshots and load external binaries.

“After the initial beacon, sLoad enters a loop in which it pushes extensive information about the victim’s system to the C&C, expects and executes commands from the server, and sends screenshots to the server. In this loop, it first performs a request to “captcha.php” and sends information about the infected system via the URL parameters,” security researchers at Proofpoint, who discovered the new campaign, wrote in a blog.

## Modus operandi

TA554’s campaign involves sending victims cleverly crafted emails, which contain language that is native to the targeted country. The phishing emails also often mention the target’s name and address in various parts of the email, such as the email subject and body. The threat group generally uses package delivery or order notification as lures.

The phishing emails contain malicious URLs that link to zipped LNK files, which, in turn, download the final payloads, which could either be a PowerShell script or another malware downloader.

“Geofencing -- restricting access to content based on the user’s location, determined via the source IP address -- is performed at all steps of the infection chain,” Proofpoint researchers said.

Apart from Ramnit, sLoad has so far also been used to distribute other malware variants such as Gootkit, Ursnif, DarkVNC, PsiXBot, and more. The researchers said that since May, they have observed multiple new versions of sLoad, all of which contained some minor modifications.

“sLoad, like other downloaders we have profiled recently, fingerprints infected systems, allowing threat actors to better choose targets of interest for the payloads of their choice. In this case, that final payload is generally a banking Trojan via which the actors can not only steal additional data but perform man-in-the-browser attacks on infected individuals,” Proofpoint researchers added. “Downloaders, though, like sLoad, Marap, and others, provide high degrees of flexibility to threat actors, whether avoiding vendor sandboxes, delivering ransomware to a system that appears mission critical, or delivering a banking Trojan to systems with the most likely return.”

SLoad Reconnaissance Malware Ramnit Trojan Ursnif Banking Malware

Malware Downloader

Publisher

**Cyware**