TrickBot Ravages Customers of Amazon, PayPal and Other Top Brands

By Tara Seals

Published: 2022-02-16 · Archived: 2026-04-06 00:43:40 UTC

The resurgent trojan has targeted 60 top companies to harvest credentials for a wide range of applications, with an eye to virulent follow-on attacks.

Cyberattackers are targeting 60 different high-profile companies with the TrickBot malware, researchers have warned, with many of those in the U.S. The goal is to attack those companies' customers, according to Check Point Research (CPR), which are being cherry-picked for victimization.

According to a Wednesday CPR writeup, TrickBot is targeting well-known brands that include Amazon, American Express, JPMorgan Chase, Microsoft, Navy Federal Credit Union, PayPal, RBC, Yahoo and others.

"Trickbot attacks high-profile victims to steal the credentials and provide its operators access to the portals with sensitive data where they can cause greater damage," researchers noted in their report.

On the technical front, the variant that's being used in the campaign has also added three interesting modules, and new de-obfuscation and anti-analysis approaches, researchers added.

TrickBot's Back with a New Bag

The TrickBot malware was originally a banking trojan, but it has evolved well beyond those humble beginnings to become a wide-ranging credential-stealer and initial-access threat, often responsible for fetching second-stage

binaries such as ransomware.

Since the well-publicized law-enforcement takedown of its infrastructure in October 2020, the threat has clawed its way back, now sporting more than 20 different modules that can be downloaded and executed on demand. It typically spreads via emails, though the latest campaign adds self-propagation via the EternalRomance vulnerability.

“Such modules allow the execution of all kinds of malicious activities and pose great danger to the customers of 60 high-profile financial (including cryptocurrency) and technology companies,” CPR researchers warned. “We see that the malware is very selective in how it chooses its targets.”

It has also been seen working in concert with a similar malware, Emotet, which suffered its own takedown in January 2021.

CPR in just its own telemetry found that TrickBot overall has seen more than 140,000 successful infections since the takedown; and researchers noted that it’s back to taking first place in malware prevalence lists.

Fresh Modules for Rotting Infections

The version of TrickBot that CPR found being used in the current campaign sports three freshened-up modules of note, researchers said:

- injectDll
- tabDll
- pwgrabc

TrickBot’s ‘injectDll’: A Web-Injects Module

Web injects are well-known from the banking-trojan world; they are used to present targets with overlaid facsimiles of real banking log-in sites; when a victim tries to sign on, they steal the credential data, and can pave the way for drained bank accounts and fraudulent wire transfers down the road.

This particular module has added a web-injects format from the infamous Zeus banking trojan, researchers said, which collects information from login actions on targeted sites and sends it to a command-and-control server (C2).

“The injectDll module performs browser data injection, including JavaScript which targets customers of 60 high-profile companies,” according to the writeup. “Add Trickbot’s cherry-picking of victims, and the menace becomes even more dangerous.”

On the anti-analysis front, the payload injected into the banking site’s page is minified (making the code size smaller makes the code unreadable), obfuscated and contains anti-deobfuscation techniques, researchers said. The final payload, which contains the actual code that grabs the victim’s keystrokes and web form submit actions, is also minified and obfuscated and contains a few layers of anti-deobfuscation techniques, they said.

“Usually a researcher tries to analyze minified and obfuscated JavaScript code using tools like JavaScript Beautifiers, deobfuscators like de4js, and so on,” they explained. “After we applied these tools, we noticed that

although the code became more readable, it also stopped working."

Another anti-analysis technique they observed involved researchers sending automated requests to the C2 to get fresh web-injects: "If there is no 'Referer' header in the request, the server will not answer with a valid web-inject," according to CPR.

"We not only see variants created based on more recently successful malware, but we even see threat actors use malware that is even twenty years old to generate new variants," Saryu Nayyar, CEO and founder at Gurucul, said of the Zeus connection, via email. "As can be seen by TrickBot, even when a threat actor group is broken up, their legacy lives on to as other groups can inherent their tools, tactics and procedures with their own modifications and improvements to evade current detection techniques."

TrickBot's 'tabDLL' Module

The second new development is a dynamic link library (DLL), also used to grab user credentials. Its ultimate goal is to spread the malware via network shares, researchers noted.

tabDLL uses a multi-step process, as CPR laid out. In sequence, the module does the following:

1. Enable the storing of user credential information in the LSASS application;
2. Inject the "Locker" module into the legitimate explorer.exe application;
3. From the infected explorer.exe, force the user to enter login credentials to the application, then lock the user's session;
4. Store the credentials in the LSASS application memory;
5. Grab the credentials from the LSASS application memory using Mimikatz, which is an open-source tool for extracting data from an application's memory;
6. Report credentials to the C2;
7. And, use the EternalRomance exploit to spread to other targets inside the network via SMBv1 network shares.

TrickBot's 'pwgrabc' Module

The pwgrabc module, as its name suggests, is a catch-all credential stealer for various applications.

The targeted applications are as follows: AnyConnect; Chrome; ChromeBeta; Edge; EdgeBeta; Filezilla; Firefox; Git; Internet Explorer; KeePass; OpenSSH; OpenVPN; Outlook; Precious; Putty; RDCMan; RDP; TeamViewer; VNC; and WinSCP.

Overall, the campaign is a nice mix of skills, the researchers concluded.

"Based on our technical analysis, we can see that TrickBot authors have the skills to approach the malware development from a very low level and pay attention to small details," they said. "Meanwhile…we know that the operators behind the infrastructure are very experienced with malware development on a high level as well. TrickBot remains a dangerous threat."

Join Threatpost on Wed. Feb 23 at 2 PM ET for a LIVE roundtable discussion, "The Secret to Keeping Secrets," sponsored by Keeper Security, will focus on how to locate and lock down your organization's most sensitive data. Zane Bond with Keeper Security will join Threatpost's Becky Bracken to offer concrete steps to protect your organization's critical information in the cloud, in transit and in storage. REGISTER NOW and please Tweet us your questions ahead of time @Threatpost so they can be included in the discussion.
