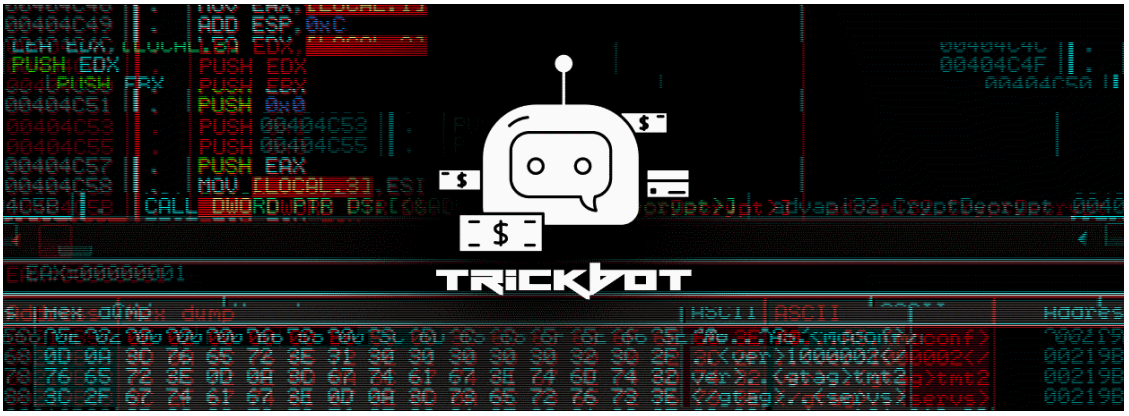
TrickBot turns 100: Latest malware released with new features

By Lawrence Abrams

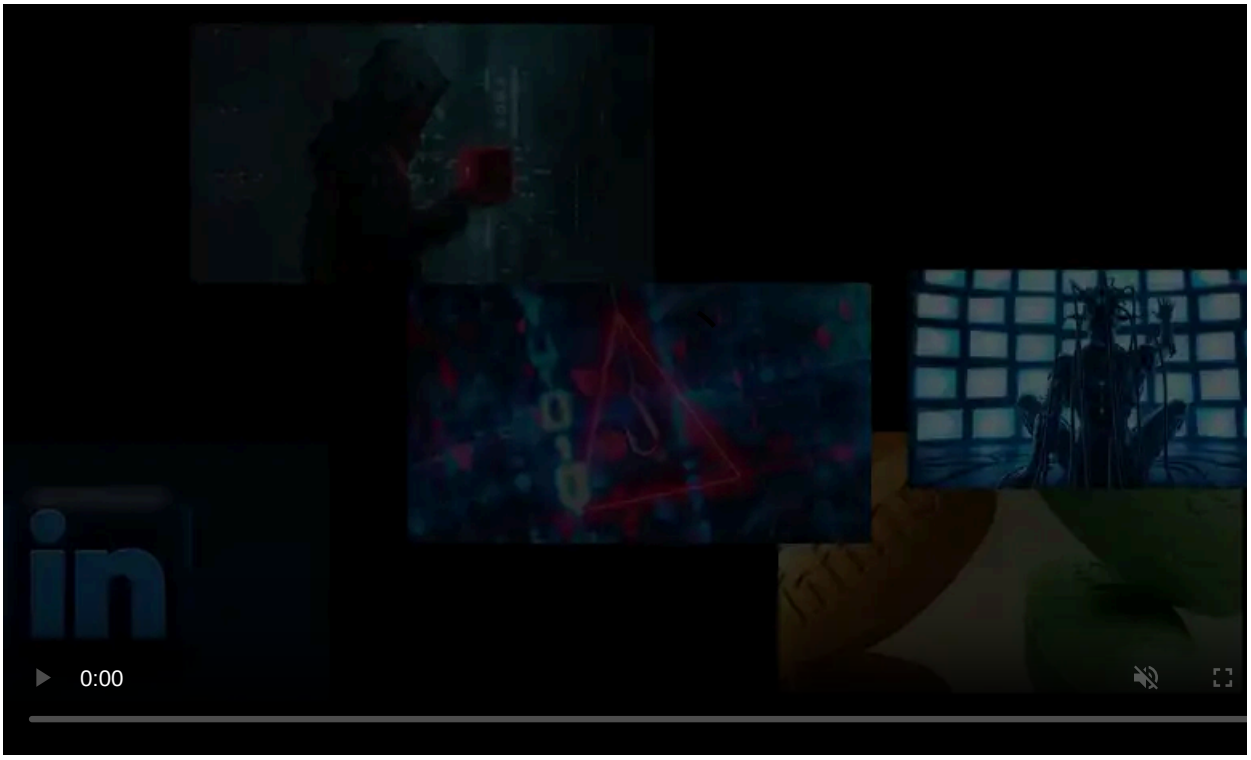
Published: 2020-11-21 · Archived: 2026-04-05 18:22:33 UTC

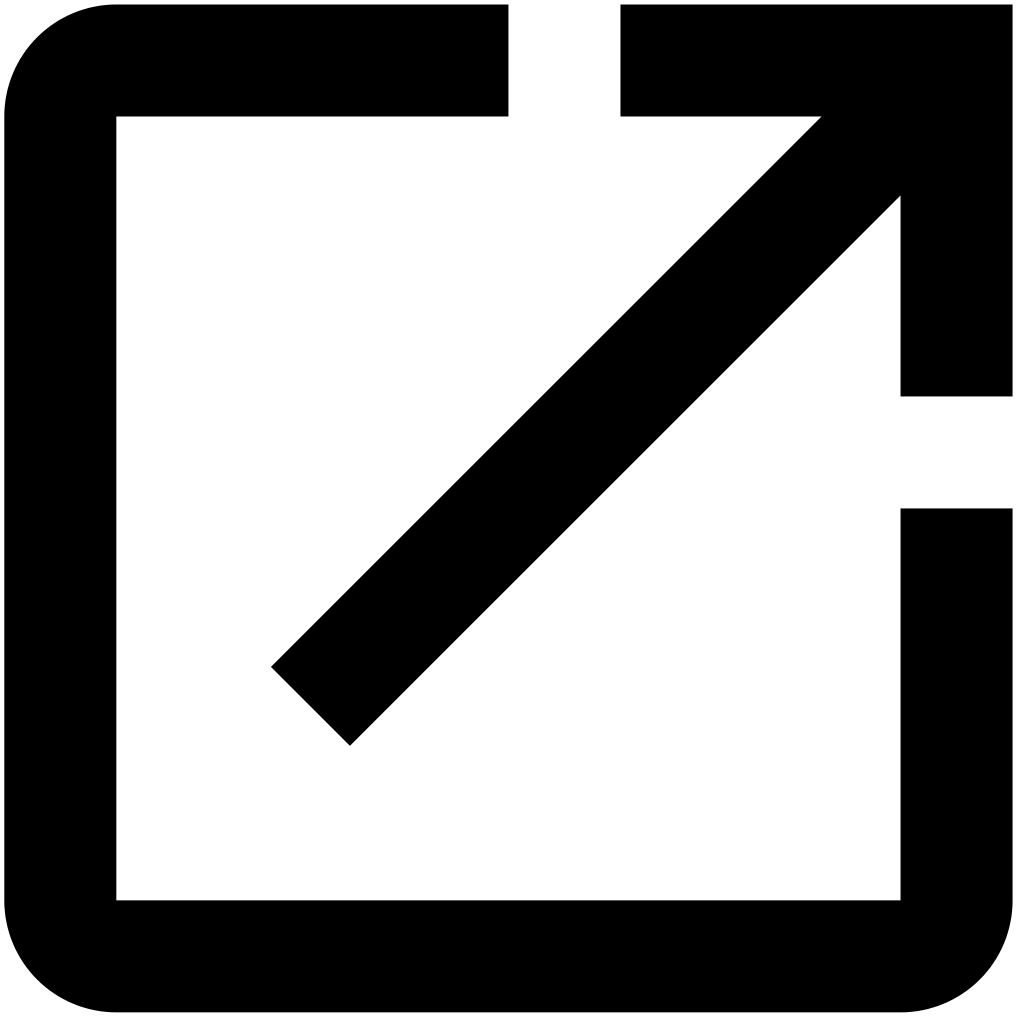


The TrickBot cybercrime gang has released the hundredth version of the TrickBot malware with additional features to evade detection.

TrickBot is a malware infection commonly installed via malicious phishing emails or other malware. When installed, TrickBot will quietly run on a victim's computer while it downloads other modules to perform different tasks.

These modules perform a wide range of malicious activity, including stealing a domain's Active Directory Services database, spreading laterally on a network, screenlocking, stealing cookies and browser passwords, and stealing OpenSSH keys.


0:00



TrickBot is known to finish an attack by giving access to the threat actors behind the Ryuk and Conti ransomware to make matters worse.

New features added to TrickBot v100

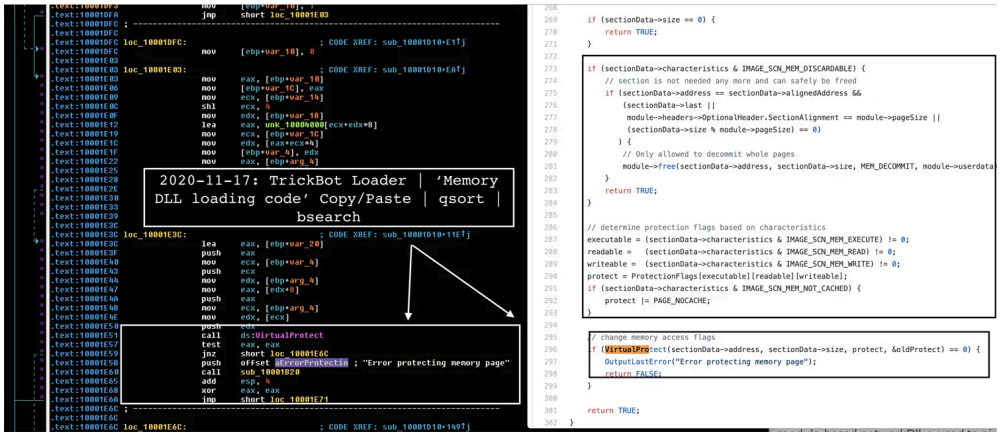
After Microsoft and their partners performed a coordinated attack against TrickBot infrastructure last month, it was hoped that it would take them some time to recover.

Unfortunately, the TrickBot gang is still chugging along, as shown by the release of the TrickBot malware's hundredth build.

This latest build was discovered by Advanced Intel's Vitali Kremez, who found that they added new features to make it harder to detect.

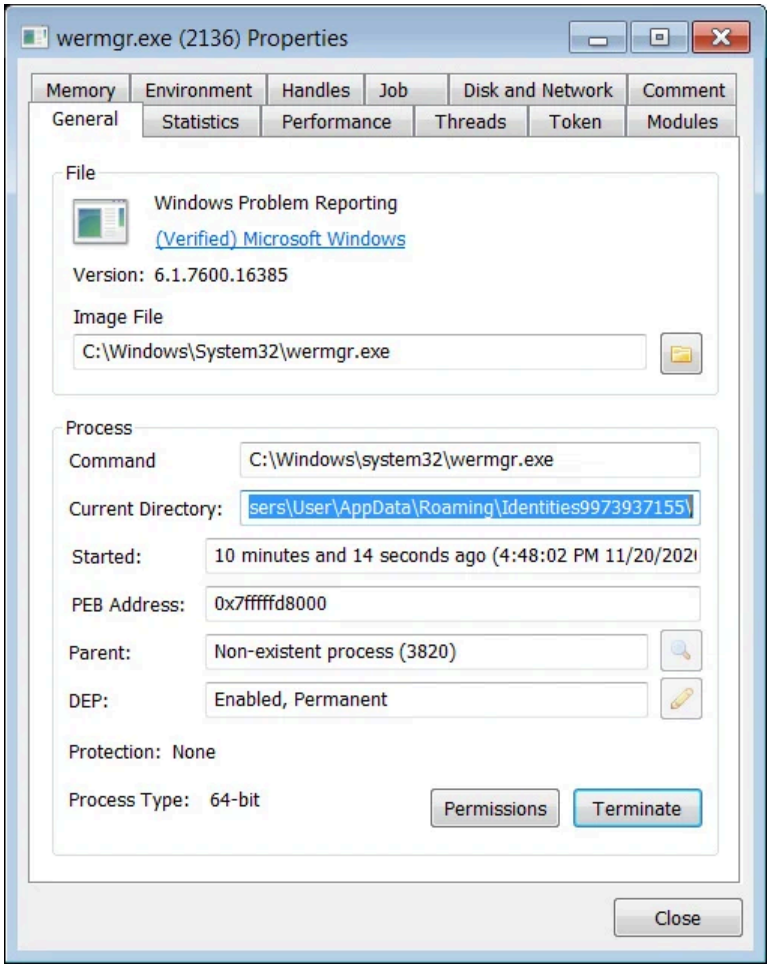
With this release, TrickBot is now injecting its DLL into the legitimate Windows wermgr.exe (Windows Problem Reporting) executable directly from memory using code from the 'MemoryModule' project.

"MemoryModule is a library that can be used to load a DLL completely from memory - without storing on the disk first," explains the project's GitHub page.



'MemoryModule' code in TrickBot
Source: Vitali Kremez

Initially started as an executable, TrickBot will inject itself into wermgr.exe and then terminates the original TrickBot executable.



TrickBot injected into Wermgr.exe

According to Kremez, when injecting the DLL, it will do so using Doppel Hollowing, or process doppelganging, to evade detection by security software.

"This technique makes use of transactions, a feature of NTFS that allows to group together a set of actions on the file system, and if any of those actions fails, a complete rollback occurs. The injector process creates a new transaction, inside of which it creates a new file containing the malicious payload. It then maps the file inside the target process and finally rolls back the transaction. In this way it appears as if the file has never existed, even though its content is still inside the process memory," a writeup on this technique by security researcher Francesco Muronie explains.

As you can see, the TrickBot gang has not allowed the disruption of their infrastructure to hold them back, and they continue to integrate new features to prevent the malware from being undetected.

Unfortunately, this means TrickBot is here to stay for the foreseeable future, and consumers and the enterprise need to remain diligent and be smart about what email attachments they open.
