TrickBot: New attacks see the botnet deploy new banking module, new ransomware

therecord.media/trickbot-new-attacks-see-the-botnet-deploy-new-banking-module-new-ransomware/

July 2, 2021

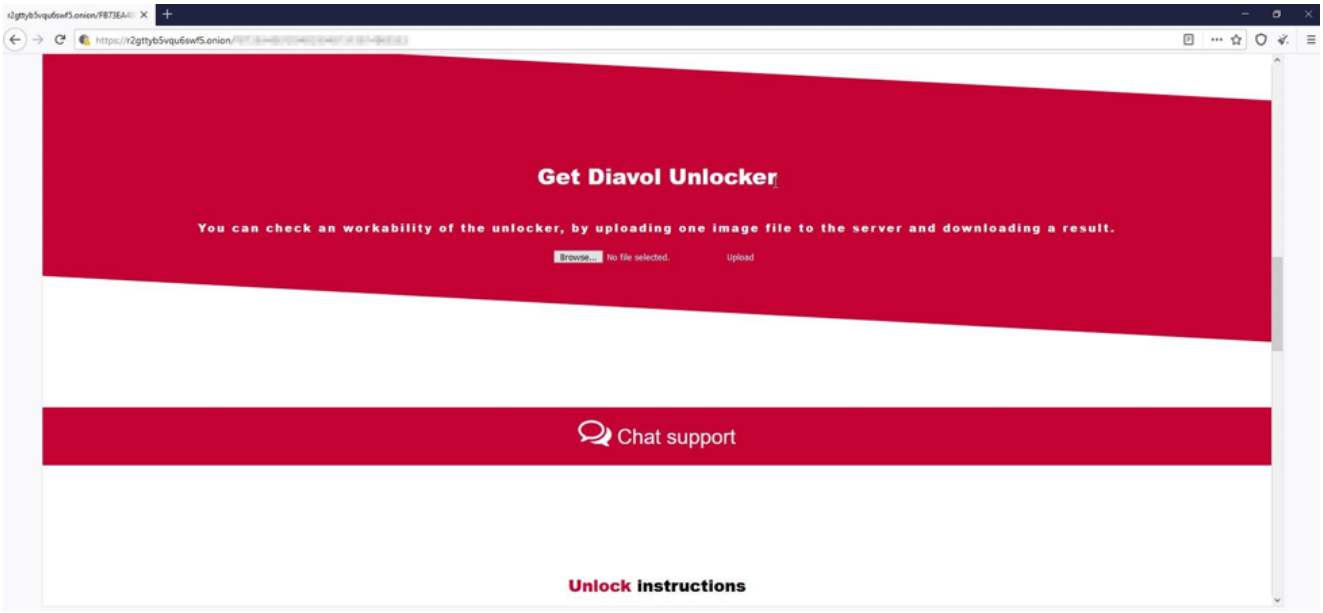

Image: Fortinet

Over the course of the past few weeks, new activity has been observed from TrickBot, one of today's largest malware botnets, with reports that its operators have helped create a new ransomware strain called **Diavol** and that the TrickBot gang is returning to its roots as a banking trojan with a new and updated banking module.

In a report from cybersecurity firm Fortinet, malware researchers Dor Neeamni and Asaf Rubinfeld detailed the TrickBot gang's newest work, the Diavol ransomware:

- Per Fortinet, Diavol was seen in the wild in only one incident, deployed alongside a version of the Conti ransomware in what appeared to have been a test run.
- The Diavol code also contained multiple similarities with the code for the Conti ransomware.
- Following this discovery, Fortinet said it believed Diavol was the work of the Wizard Spider gang, an industry codename for the operators of the TrickBot botnet and the Conti ransomware.
- The Diavol ransomware also reused some language from Egregor ransom notes, but no other connection has been seen between the two.
- No leak site has been discovered for Diavol yet.
- Surprisingly, Diavol did not come with code to prevent the ransomware from running inside former Soviet states, something that is found in almost all major ransomware strains today.

- The ransomware's name, Diavol, means "devil" in Romanian.

But while Diavol has been linked to the TrickBot creators, in a report published yesterday, security firm Kryptos Logic said it spotted changes to the TrickBot malware code itself.

- Since June 2021, TrickBot has been seen pushing a new module on infected computers. The new module contains a revamped version of its old banking component that tries to intercept credentials for e-banking websites.
- Called a "webinject" module, this component has been rewritten to include new methods to inject malicious code inside banking websites.
- Per Kryptos Logic, this new code appears to have been copied from the old Zeus banking malware, different from the two webinject techniques TrickBot had used in previous years.
- Zeus-style injects work by proxying traffic through a local SOCKS server. If the web traffic matches a list of banking login URLs, the traffic is modified accordingly with malicious code to record credentials or carry out other operations.
- Per Kryptos Logic, this new banking/webinject module shares substantial code with IcedID's webinject module.
- The move to support Zeus-style web injects may be an attempt from the TrickBot gang to muscle into the territory of other Malware-as-a-Service banking trojans and steal some of their customers in the underground cybercrime market.

> The resumption of development of the webinject module indicates that TrickBot intends to revive its bank fraud operation, which appears to have been shelved for over a year. The addition of Zeus-style webinjects may suggest expansion of their Malware-as-a-Service platform, enabling users to bring their own webinjects.
>
> *Kryptos Logic Vantage Team.*

> TrickBot has brought back their bank fraud module, which has been updated to support Zeus-style webinjects. This could suggest they are resuming their bank fraud operation, and plan to expand access to those unfamiliar with their internal webinject format. https://t.co/YrS2bVZ0Xt
>
> — MalwareTech (@MalwareTechBlog) July 1, 2021

Tags

- banking trojan
- botnet
- Diavol
- malware
- Ransomware
- Trickbot
- webinject

- Wizard Spider

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.