FBI links Diavol ransomware to the TrickBot cybercrime group

bleepingcomputer.com/news/security/fbi-links-diavol-ransomware-to-the-trickbot-cybercrime-group/

Lawrence Abrams

By
Lawrence Abrams

- January 20, 2022
- 01:37 PM
- 0

The FBI has formally linked the Diavol ransomware operation to the TrickBot Group, the malware developers behind the notorious TrickBot banking trojan.

The TrickBot Gang, aka Wizard Spider, are the developers of malware infections that have played havoc on corporate networks for years, commonly leading to Conti and Ryuk ransomware attacks, network infiltration, financial fraud, and corporate espionage.

The TrickBot Gang is most known for its namesake, the TrickBot banking trojan, but is also behind the development of the BazarBackdoor and Anchor backdoors.

Prior analysis linked Diavol to TrickBot Group

In July 2021, researchers from FortiGuard Labs released an analysis of a new ransomware called Diavol (Romanian for Devil) that was seen targeting corporate victims.

The researchers saw both Diavol and Conti ransomware payloads deployed on a network in the same ransomware attack in early June 2021.

After analyzing the two ransomware samples, similarities were discovered, such as their use of asynchronous I/O operations for file encryption queuing and almost identical command-line parameters for the same functionality.

At the time, there was not enough evidence to formally link the two operations.

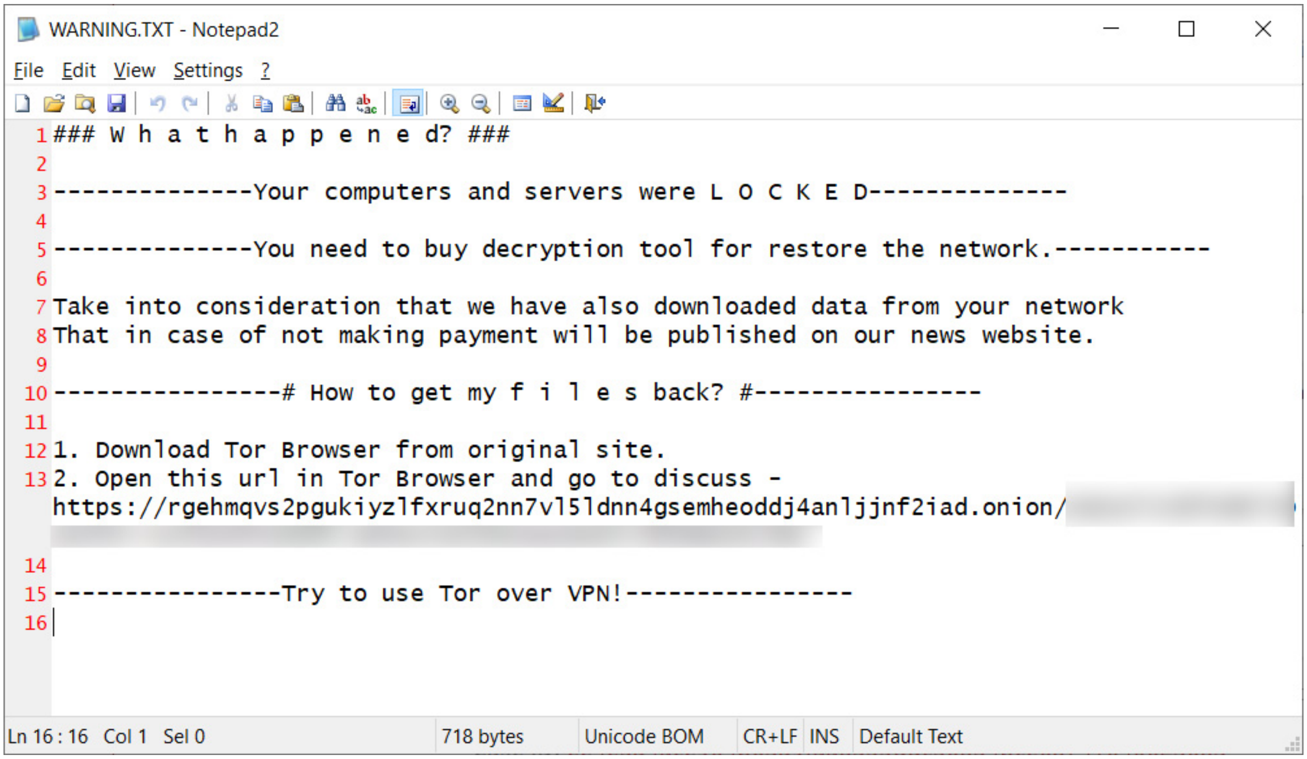
However, a month later, IBM X-Force researchers established a stronger connection between Diavol ransomware and other TrickBot Gang's malware, such as Anchor and TrickBot.

FBI links Diavol ransomware to TrickBot gang

Today, the FBI has formally announced that they have linked the Diavol Ransomware operation to the TrickBot Gang in a new advisory sharing indicators of compromise seen in previous attacks.

"The FBI first learned of Diavol ransomware in October 2021. Diavol is associated with developers from the Trickbot Group, who are responsible for the Trickbot Banking Trojan," the FBI states in a new FBI Flash advisory.

Since then, the FBI has seen ransom demands ranging between $10,000 and $500,000, with lower payments accepted after ransom negotiations.



```
### W h a t h a p p e n e d? ###

--------------Your computers and servers were L O C K E D--------------

--------------You need to buy decryption tool for restore the network.-----------

Take into consideration that we have also downloaded data from your network
That in case of not making payment will be published on our news website.

----------------# How to get my f i l e s back? #----------------

1. Download Tor Browser from original site.
2. Open this url in Tor Browser and go to discuss -
https://rgehmqvs2pgukiyzlfxruq2nn7vl5ldnn4gsemheoddj4anljjnf2iad.onion/[redacted]

----------------Try to use Tor over VPN!----------------

```

Warning.txt ransom note from Diavol ransomware

These amounts are in stark contrast to the higher ransoms demanded by other ransomware operations linked to TrickBot, such as Conti and Ryuk, who have historically asked for multi-million dollar ransoms.

For example, in April, the Conti ransomware operation demanded $40 million from Florida's Broward County School district and $14 million from chip maker Advantech.

The FBI was likely able to formally link Diavol to the TrickBot Gang after the arrest of Alla Witte, a Latvian woman involved in the development of ransomware for the malware gang.

Vitali Kremez, CEO of AdvIntel, who has been tracking the TrickBot operations, told BleepingComputer that Witte was responsible for the development of the new TrickBot-linked ransomware.

"Alla Witte played a critical role for the TrickBot operations and based on the previous AdvIntel deep adversarial insight she was responsible for the development of the Diavol ransomware and frontend/backend project meant to support TrickBot operations with the specific tailored ransomware with the bot backconnectivity between TrickBot and Diavol," Kremez told BleepingComputer in a conversation.

"Another name for the Diavol ransomware was called "Enigma" ransomware leveraged by the TrickBot crew before the Diavol re-brand."

The FBI's advisory contains numerous indicators of compromise and mitigations for Diavol, making it an essential read for all security professionals and Windows/network administrators.

It should be noted that the Diavol ransomware originally created ransom notes named 'README_FOR_DECRYPT.txt' as pointed out by the FBI advisory, but BleepingComputer has seen the ransomware gang switch in November to ransom notes named 'Warning.txt.'

The FBI also urges all victims, regardless of whether they plan to pay a ransom, to promptly notify law enforcement of attacks to collect fresh IOCs that they can use for investigative purposes and law enforcement operations.

If you are affected by a Diavol attack, it is also important to notify the FBI before paying as they "may be able to provide threat mitigation resources to those impacted by Diavol ransomware."

Related Articles:

TrickBot cybercrime group linked to new Diavol ransomware

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Google exposes tactics of a Conti ransomware access broker

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

- Anchor
- BazarLoader
- Diavol
- Enigma
- Ransomware
- TrickBot
- Wizard Spider

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: