Diavol ransomware sample shows stronger connection to TrickBot gang

bleepingcomputer.com/news/security/diavol-ransomware-sample-shows-stronger-connection-to-trickbot-gang/

Ionut Ilascu

By
Ionut Ilascu

- August 18, 2021
- 07:52 AM
- 0

A new analysis of a Diavol ransomware sample shows a more clear connection with the gang behind the TrickBot botnet and the evolution of the malware.

The recent research is the second one that finds common ground in the code of the two threats, tying them to the same actor.

Early sample comes with hints

Previous analysis of Diavol (Romanian for Devil) ransomware from Fortinet's FortiGuard Labs revealed a set of similarities with the TrickBot malware as well as differences that prevented high-confidence attribution of the code.

Fortinet’s assessment at the beginning of July noted that both Diavol and Conti - a ransomware family strongly connected with TrickBot - used the same command-line parameters for a variety of tasks (logging, encryption, scanning).

A report from the IBM X-Force threat analysts Charlotte Hammond and Chris Caridi provides clues pointing to a stronger connection between Diavol ransomware and the TrickBot gang.

Unlike the sample analyzed by Fortinet, which was a newer, “fully functional and weaponized piece of ransomware,” the one that IBM examined is an older variant closer to a development version used for testing purposes.

The incomplete state of the malware contained the signs that allowed the researchers to reach a more reliable conclusion.

IBM X-Force looked at a sample submitted to Virus Total on January 27, 2021, with a reported compilation date of March 5, 2020. By comparison, the compilation date for the version in Fortinet’s analysis is April 30, 2021.

The researchers noticed that Diavol ransomware collected basic information from the infected system and generated a System or Bot ID that help the attacker track multiple intrusions from affiliates in the ransomware-as-a-service (RaaS) operation.

Diavol ransomware’s Bot ID format includes the hostname, username, and Windows version of the compromised system, and a global unique identifier (GUID). The format is “almost identical” to the one generated by TrickBot malware, the analysts note.

```
[hostname]-[username]_W[windows _version].[guid]
```

A very similar Bot ID pattern has been seen with Anchor DNS, another piece of malware attributed to the TrickBot gang, the researchers say in their report.

The victim IDs are important for malware operators because they can track the success of various campaigns and let affiliates know about it.

“This is why these specific formatting and naming conventions could potentially point to the group responsible for the initial deployment” - IBM X-Force

The researchers also note that the HTTP headers for the command and control (C2) server communication were “set to prefer Russian language content,” also favored by TrickBot operators.

Another clue pointing to the Russian threat actors is code for checking the language on the compromised system to filter out victims in Russia or the Commonwealth of Independent States (CIS) region.

While Fortinet did not find this language check code in the Diavol ransomware sample they analyzed, IBM says that they found indications in the development version that such code “may have been present or intended to be developed, even if it was not activated in the compiled samples.”

“A list of four-character hexadecimal strings was identified in the development sample. These strings are unused within the compiled code but were recognized as potentially being language code identifiers, and further analysis confirmed that all are related to Russian and Commonwealth of Independent States languages” - IBM X-Force

Given the different development stages in the two Diavol ransomware variants and when they were found, it is clear that the malware is evolving.

IBM X-Force did not find definitive evidence to tie Diavol ransomware to the TrickBot gang but discovered new signs suggesting a connection.

But between their report and Fortinet’s finding that the malware functions in a very similar way as Conti, the attribution balance seems to tilt visibly towards TrickBot.

Related Articles:

Google exposes tactics of a Conti ransomware access broker

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

TrickBot cybercrime group linked to new Diavol ransomware

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Conti ransomware shuts down operation, rebrands into smaller units

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.