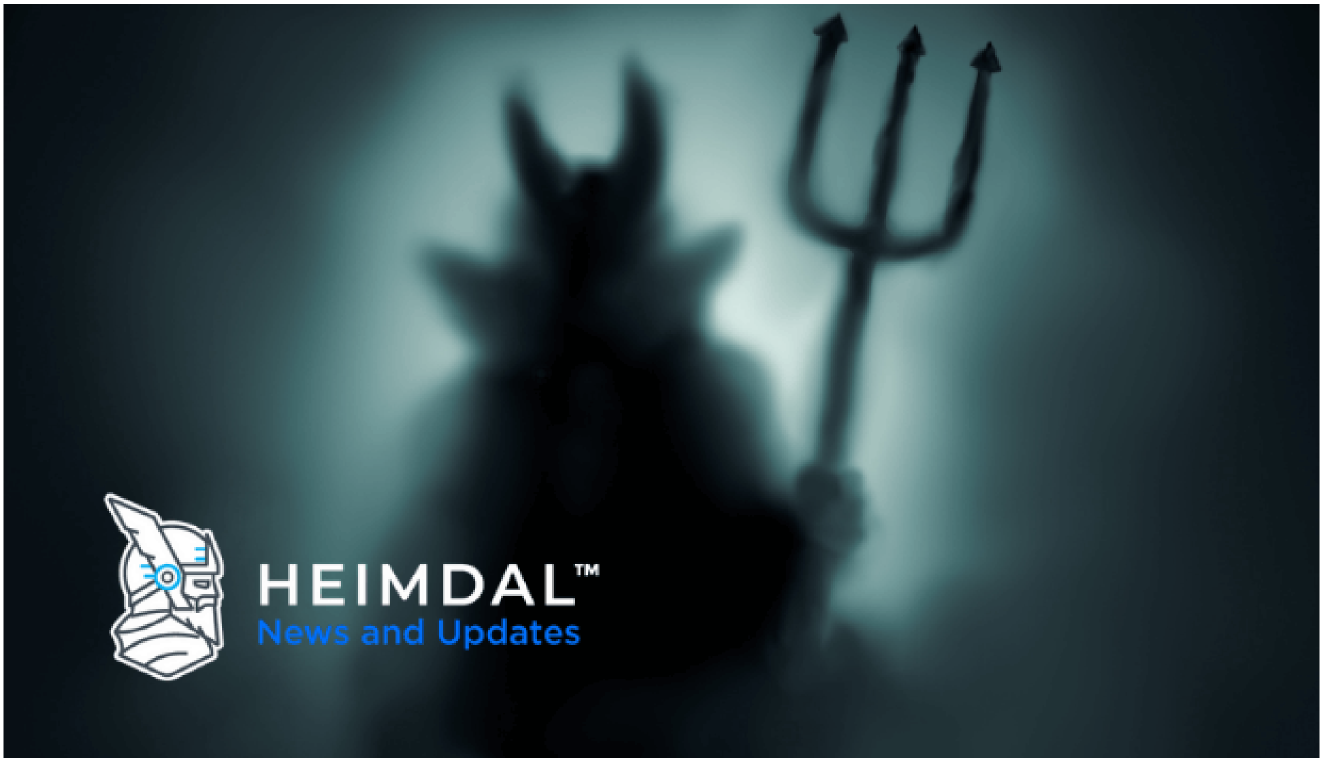
Is Diavol Ransomware Connected to Wizard Spider?

heimdalsecurity.com/blog/is-diavol-ransomware-connected-to-wizard-spider/

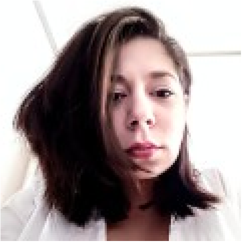
Dora Tudor

July 6, 2021



As Diavol Ransomware Is New on the Threat Landscape Researchers Weren't Sure Where it Would Fit.

LAST UPDATED ON JULY 6, 2021



QUICK READ

2 min

Let's get started!

We recently witnessed the appearance of a new ransomware strain that was dubbed as Diavol ransomware by the security researchers from FortiGuard Lab.

Diavol ransomware could be linked to the Wizard Spider threat actor as the researchers discovered a few similarities in the M.O. used by the malware. Wizard Spider is a cybercrime group from Russia that uses Trickbot, Ryuk, and Conti ransomware as their primary tools.

It is believed that the Health Service Executive cyberattack in Ireland could've been conducted by this very organization. The cybercrime group has been known to have a tendency towards wire fraud previously when they also used Diavol and Conti threat payloads in ransomware attacks back in early June this year.

What's New?

As Diavol ransomware is a relatively new actor in the threat landscape, researchers weren't sure where it would fit, but a recent report indicates a strong connection with Wizard Spider.

- Both Diavol and Conti ransomware families' samples use the same asynchronous I/O operations for file encryption queuing, along with virtually identical command-line parameters.
- However, despite similarities, the researchers couldn't find a strong connection between Diavol and Wizard Spider. Some notable differences, making the attribution impossible have been identified.
- There are no built-in checks in Diavol that stop the payloads from running on Russian targets' systems, as Conti does. Additionally, there is no evidence of data exfiltration abilities before encryption.

Diavol's encryption uses user-mode Asynchronous Procedure Calls (APCs), a function that executes without synchronization in the context of a particular threat.

The technique is also known as AtomBombing, and is a code injection technique that often goes undetected by antivirus solutions. The APC in question uses an asymmetric encryption algorithm, thus making it stand apart from other ransomware families, and on that very chain of thought, it also speeds up significantly the encryption process.

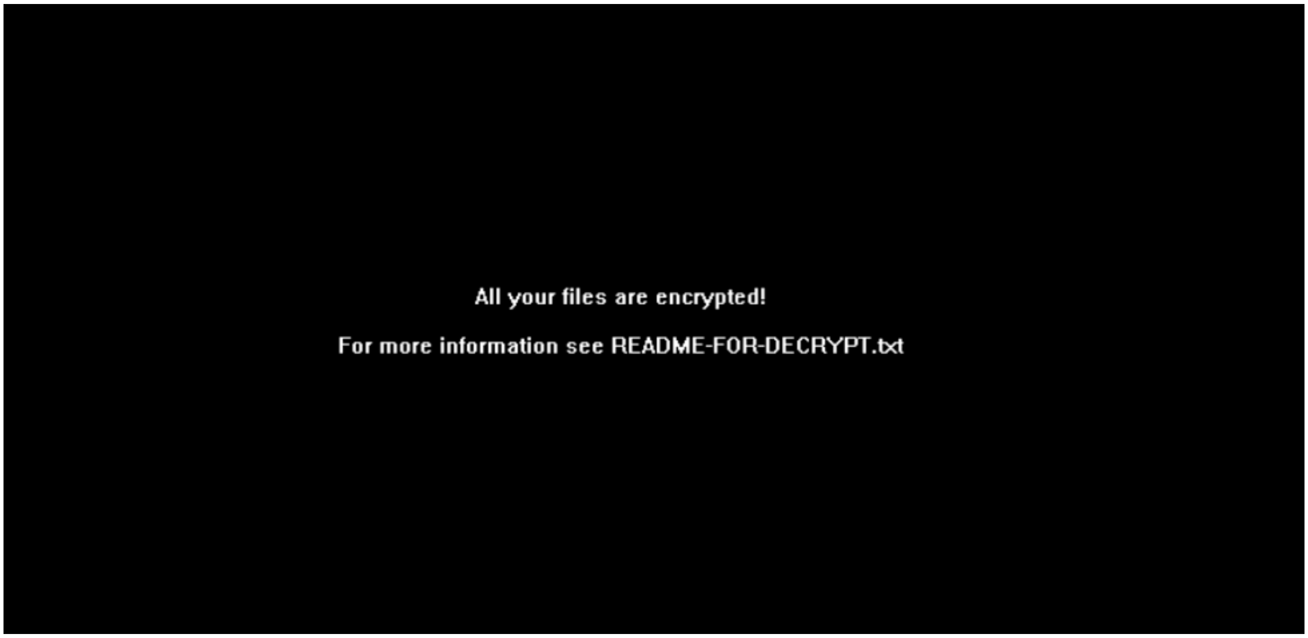
Symmetric algorithms are often used to significantly speed up the encryption process, therefore are being used by the vast majority of ransomware families.

Diavol ransomware also lacks any type of obfuscation as does not use packing or anti-disassembly methods, thus making the analysis harder as the malware gets stored in bitmap images.

Another interesting aspect about Diavol ransomware is the fact that upon execution, the ransomware manages to extract the code from the images' PE resource section in order to then load them within a buffer with permissions to run, with the code extracting 14 different routines that will execute in the following order:

- Create an identifier for the victim
- Initialize configuration
- Register with the C&C server and update the configuration
- Stop services and processes
- Initialize encryption key
- Find all drives to encrypt
- Find files to encrypt
- Prevent recovery by deleting shadow copies
- Encryption
- Change the desktop wallpaper

Right before Diavol ransomware is done, it will change each encrypted Windows device's background to a black wallpaper with the following message: "All your files are encrypted! For more information see README-FOR-DECRYPT.txt"



All your files are encrypted!

For more information see README-FOR-DECRYPT.txt

Source

Conti payloads named *locker.exe* were found in the network, thus strengthening the possibility that the threat actor could indeed be Wizard Spider.

The journalists at CYWARE believe that the connection of this ransomware to already established cybercrime groups shows how ransomware operations are constantly evolving, and it will probably not be a surprise if more of such established cybercrime groups will be joining the list of ransomware operators in the upcoming months.

RELATED

Diavol Ransomware, a New Ransomware in the Cybersecurity Landscape

Conti Ransomware Leaks Police Citations and Forces the City of Tulsa to Issue a Data Breach Warning

Emotet and Trickbot Banking Trojans Acquire Internet Worm Capabilities