Evil Corp switches to Hades ransomware to evade sanctions

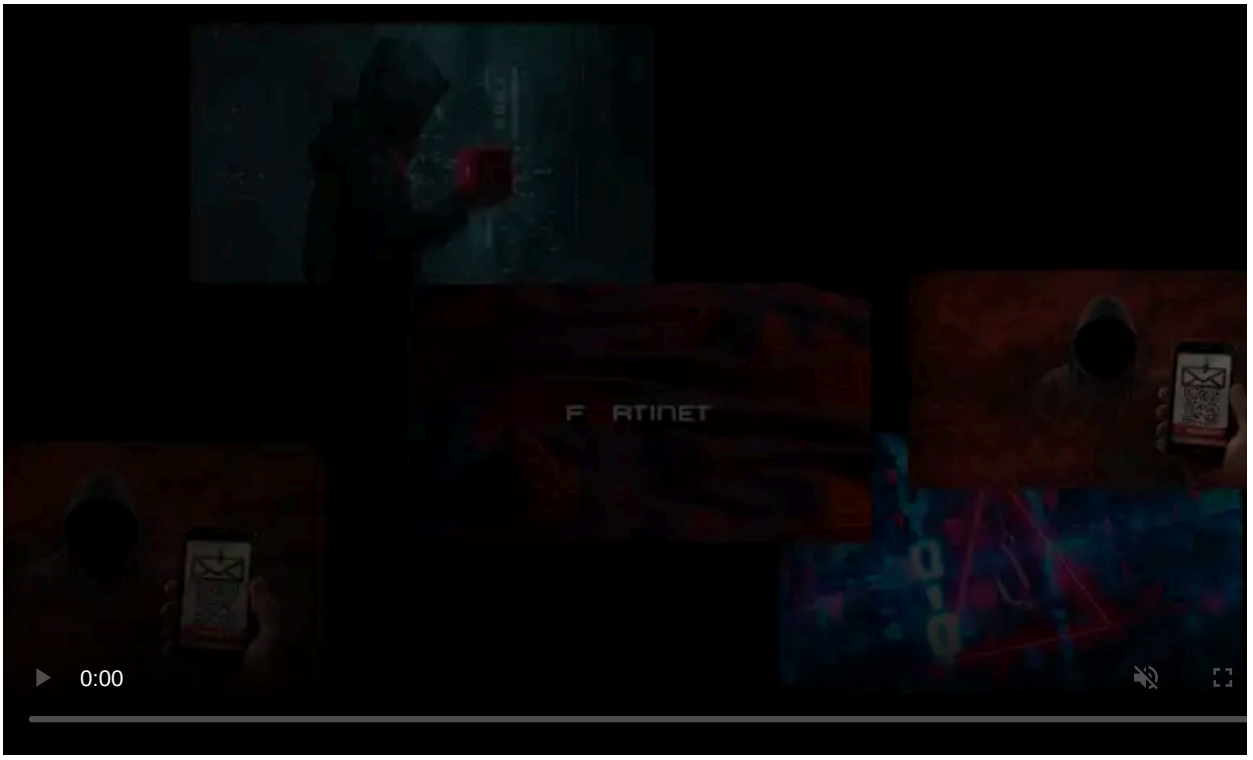
By Sergiu Gatlan

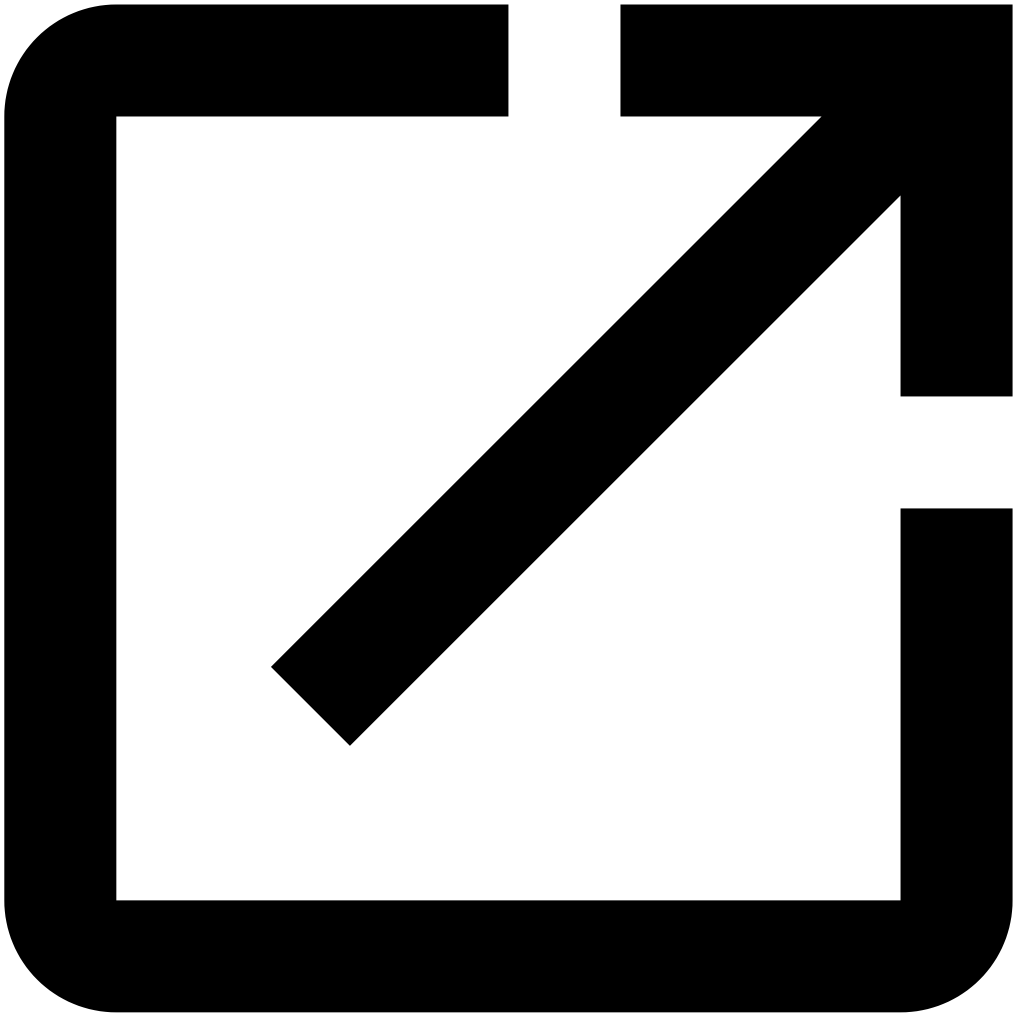
Published: 2021-03-25 · Archived: 2026-04-06 01:36:53 UTC

Hades ransomware has been linked to the Evil Corp cybercrime gang who uses it to evade sanctions imposed by the Treasury Department's Office of Foreign Assets Control (OFAC).

Evil Corp (aka the Dridex gang or INDRIK SPIDER) has been active since at least 2007 and it is known for distributing the Dridex malware.

They later shifted to the ransomware "business," first using Locky ransomware and then their own ransomware strain known as BitPaymer, deployed in attacks until 2019.


F RTINET
0:00



US sanctions for financial damages of more than $100 million

The U.S. Treasury Department sanctioned Evil Corp gang members in December 2019 after being charged for using Dridex to cause over $100 million in financial damages.

Because of this, their victims face a tricky situation if they want to pay Evil Corp's ransom as they would also violate the sanctions.

OFAC also warned in October 2020 that orgs assisting ransomware victims in making ransom payments to sanctioned threat actors also face risks as their actions could violate regulations.

Starting with June 2020, Evil Corp refreshed its tactics to circumvent the sanctions, deploying its new WastedLocker ransomware in attacks targeting enterprise orgs.

Wearable device maker Garmin is one of the high-profile targets Evil Corp hit with its WastedLocker ransomware. The company had to shut down some of its connected services and call centers following the attack.

New tooling helps bypass sanctions

CrowdStrike now linked the cybercrime gang to Hades ransomware based on "significant code overlap." This new, previously unattributed malware tooling is helping Evil Corp bypass sanctions to monetize their attacks.

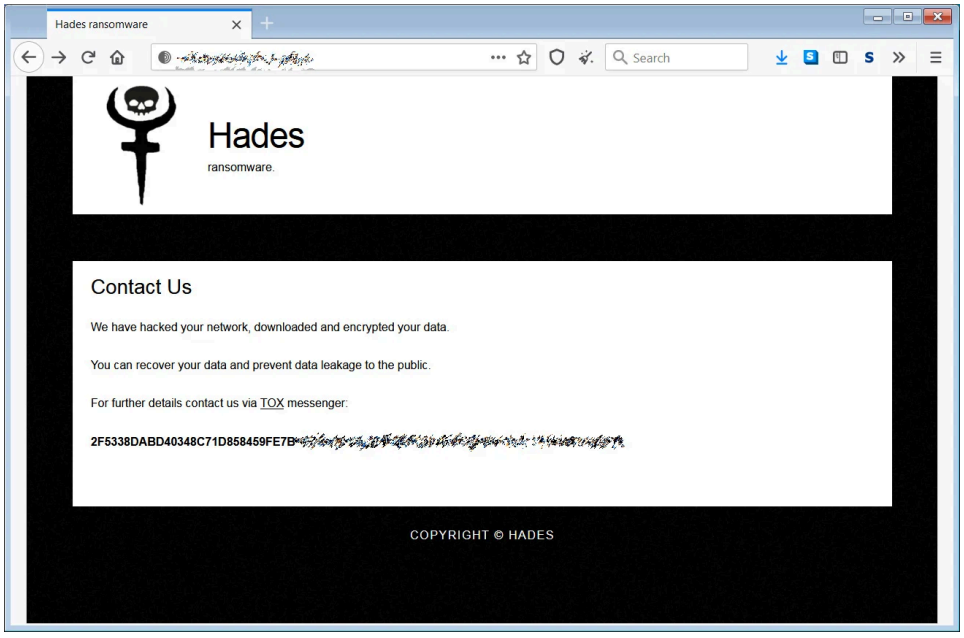
Hades ransomware is a 64-bit compiled variant of WastedLocker upgraded with supplementary code obfuscation and a few minor feature changes.

"Hades ransomware shares the majority of its functionality with WastedLocker; the ISFB-inspired static configuration, multi-staged persistence/installation process, file/directory enumeration, and encryption functionality are largely unchanged," CrowdStrike said.

"Hades did receive minor modifications, and the removed features included those that were uniquely characteristic of INDRIK SPIDER’s previous ransomware families — WastedLocker and BitPaymer."

When encrypting a victim's systems, Hades creates a ransom note named 'HOW-TO-DECRYPT-[extension].txt' resembling ransom notes dropped by REvil ransomware.

The ransom notes contain a URL that directs the victims to a Tor site with info about the attack and a Tox messenger address they can use to contact Evil Corp's operators.



Hades Tor site (*BleepingComputer*)

"INDRIK SPIDER's move to this ransomware variant also came with another shift in tactics: the departure from using email communication and the possibility of exfiltrating data from victims to elicit payments," CrowdStrike added.

BleepingComputer reported that Hades ransomware was used to encrypt trucking giant Forward Air's systems in December 2020.

While there aren't many Hades ransomware attacks being reported by affected organizations, Evil Corp victims have been using the ID-Ransomware service to check if their systems were hit by Hades ransomware since the group started using the new strain.

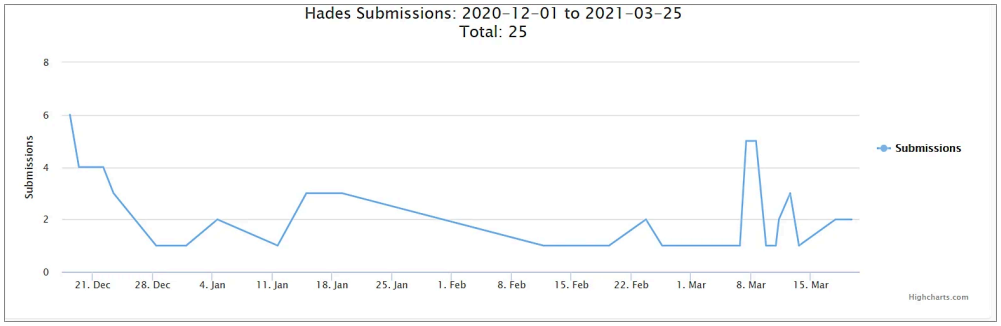


Image: ID-Ransomware

"The continued development of WastedLocker ransomware is the latest attempt by the notorious adversary to distance themselves from known tooling to aid them in bypassing the sanctions imposed upon them," CrowsStrike concluded.

"The sanctions and indictments have undoubtedly significantly impacted the group and have made it difficult for INDRIK SPIDER to successfully monetize their criminal endeavors."

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
