

New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions

By Lawrence Abrams

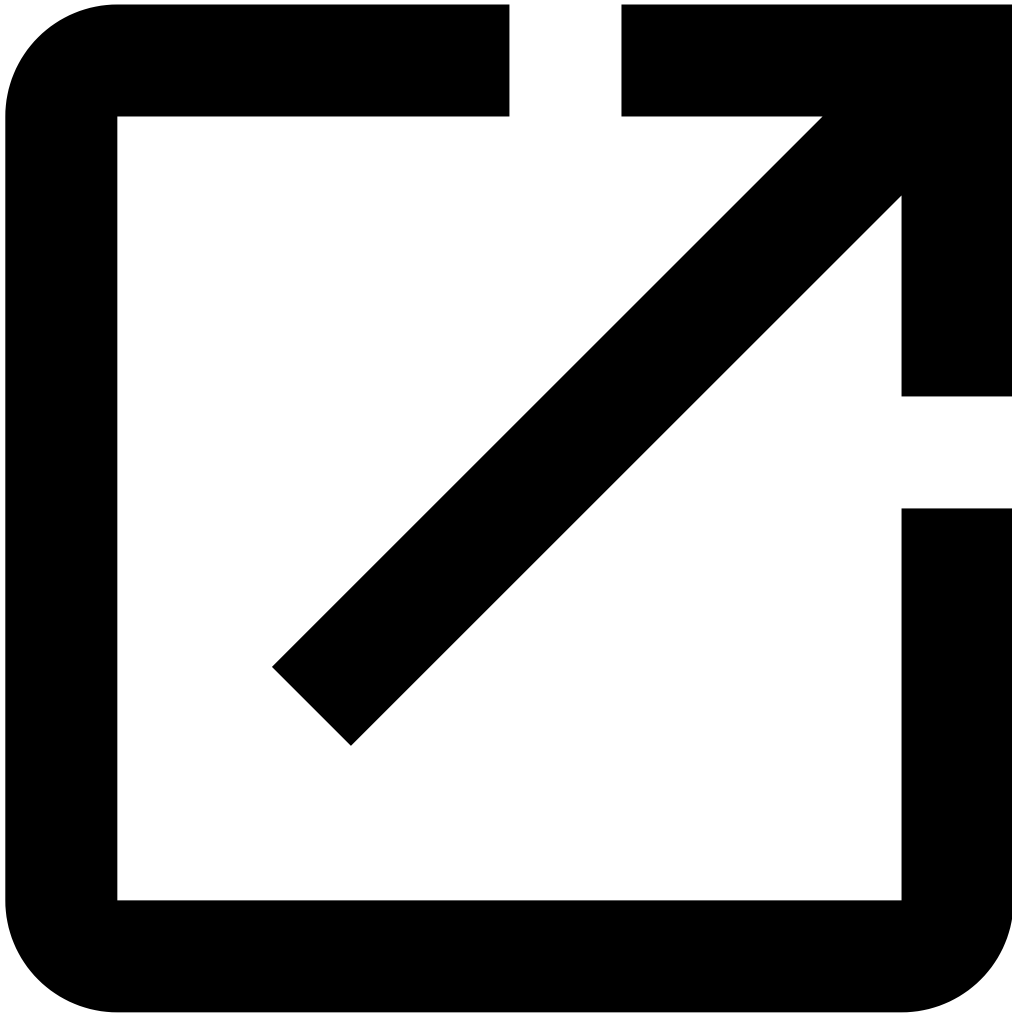
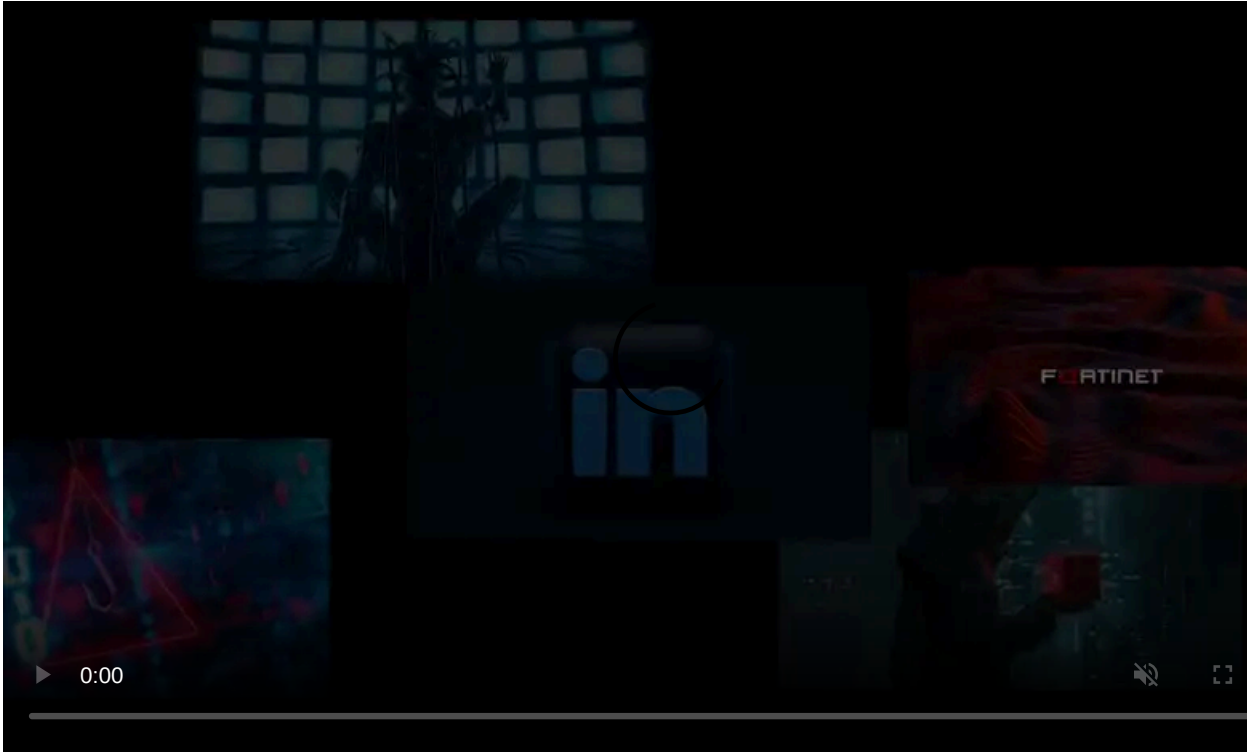
Published: 2021-06-06 · Archived: 2026-04-05 19:33:39 UTC



The new PayloadBIN ransomware has been attributed to the Evil Corp cybercrime gang, rebranding to evade sanctions imposed by the US Treasury Department's Office of Foreign Assets Control (OFAC).

The Evil Corp gang, also known as Indrik Spider and the Dridex gang, started as an affiliate for the ZeuS botnet. Over time, they formed a group that focused on distributing the banking trojan and downloader called Dridex via phishing emails.

As cybergangs started to transition to highly profitable ransomware attacks, Evil Corp launched a ransomware operation called BitPaymer, which was delivered via the Dridex malware in compromised corporate networks.



Visit Advertiser website [GO TO PAGE](#)

After being [sanctioned by the US government in 2019](#), ransomware negotiation firms refused to facilitate ransom payments for Evil Corp ransomware attacks to avoid facing fines or legal action from the Treasury Department.

Evil Corp began renaming their ransomware operations to different names such as [WastedLocker](#), [Hades](#), and Phoenix to bypass these sanctions.

The threat actors used Phoenix in an [attack on insurance firm CNA](#).

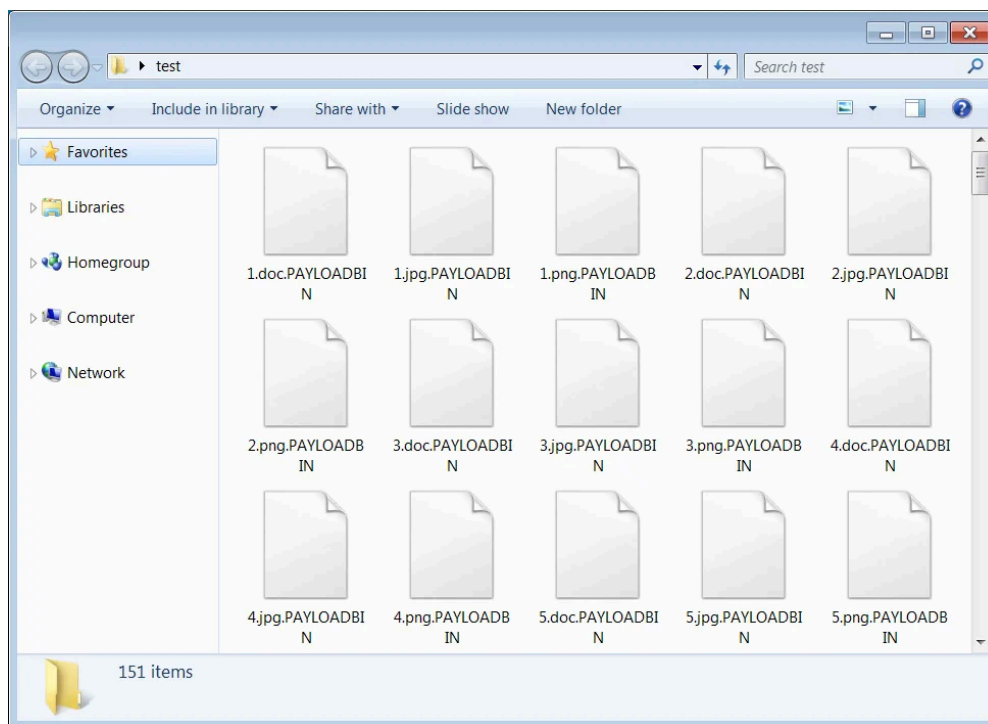
Evil Corp impersonates Payload Bin hacking group

After [breaching the Metropolitan Police Department](#) in Washington, DC, and stealing unencrypted data, the [Babuk gang said they were quitting ransomware encryption](#) and instead focus on data theft and extortion.

At the end of May, the Babuk data leak site had a design refresh where the ransomware gang rebranded as a new group called 'payload bin,' shown below.

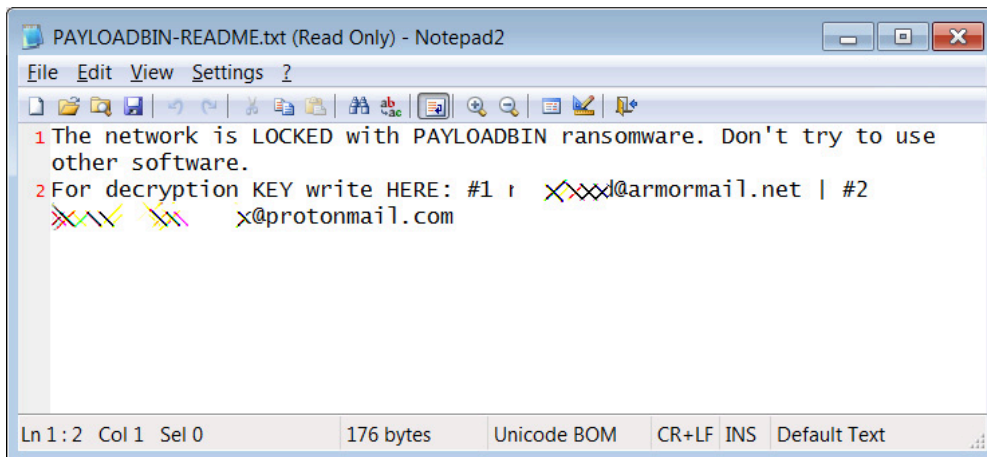
On Thursday, BleepingComputer found a new ransomware sample called PayloadBIN [[VirusTotal](#)] that we immediately assumed was related to the rebranding of Babuk Locker.

When installed, the ransomware will append the **.PAYLOADBIN** extension to encrypted files, as shown below.



Files encrypted by PayloadBIN

Furthermore, the ransom note is named '**PAYLOADBIN-README.txt**' and states that the victim's "networks is LOCKED with PAYLOADBIN ransomware."



PayloadBIN ransom note

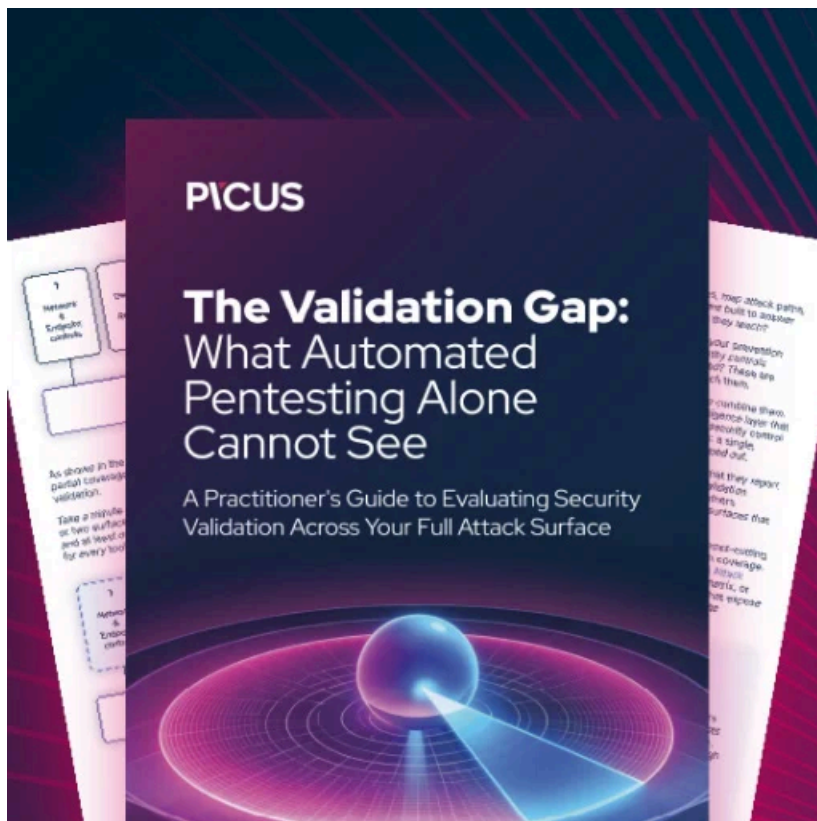
After finding the sample, BleepingComputer thought Babuk was lying about their intentions to move away from ransomware and rebranded to a new name.

However, after analyzing the new ransomware, both [Fabian Wosar](#) of Emsisoft and [Michael Gillespie](#) of ID Ransomware confirmed that the ransomware is a rebranding of Evil Corp's previous ransomware operations.

While discussing why they would have impersonated another cybercrime group, Wosar felt that they saw and took an opportunity to impersonate a hacking group that is not sanctioned.

“Now they had a gang rebranding and just took the opportunity.” - Fabian Wosar.

As the ransomware is now attributed to a sanctioned hacking group, most ransomware negotiation firms will likely not help facilitate payments for victims affected by the PayloadBIN ransomware.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

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.

Source: <https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/>