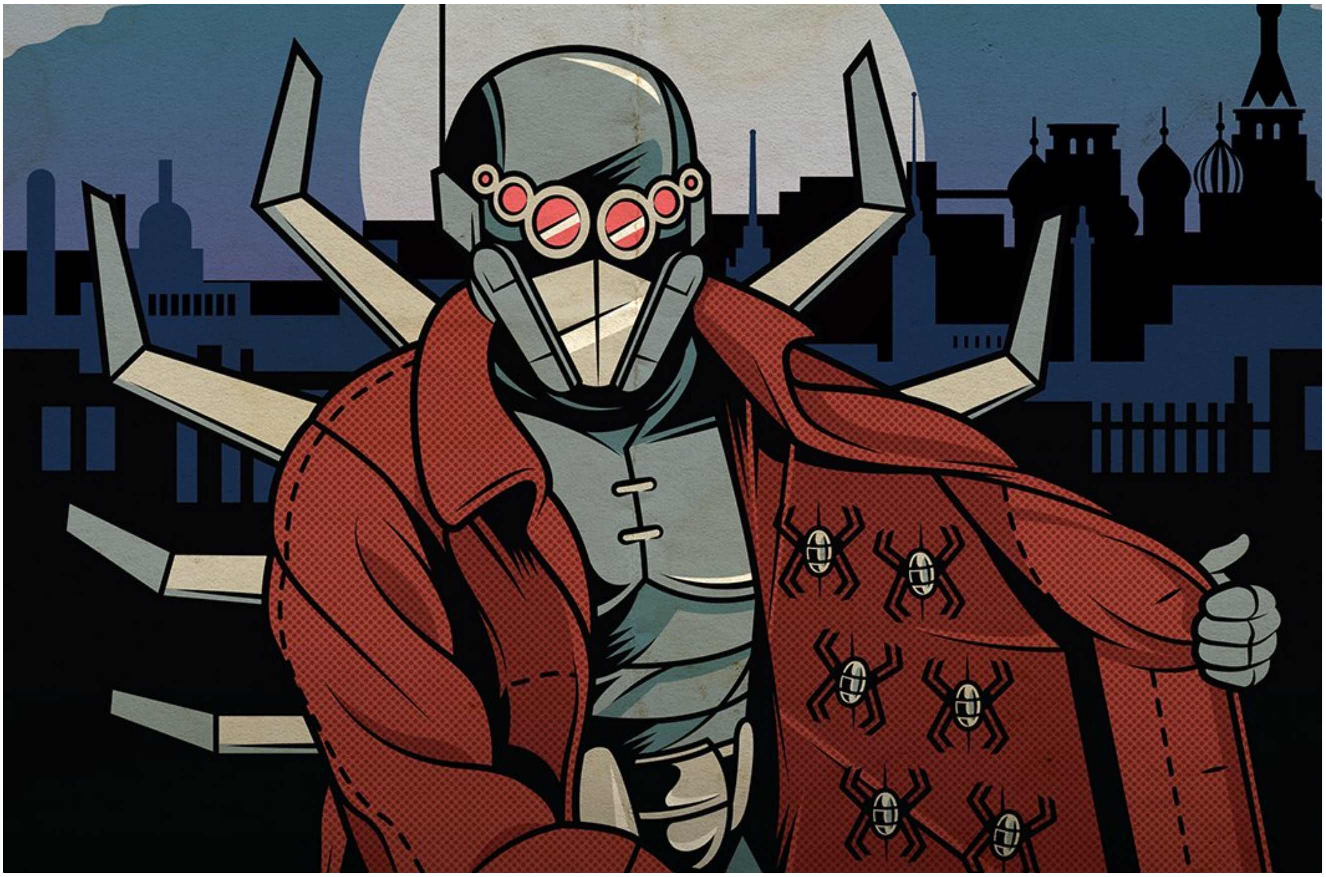
WastedLocker Superseded by Hades Ransomware

crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/

Adam Podlosky - Brendon Feeley

March 17, 2021



Introduction

In December 2019, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) took action against the Russia-based cybercriminal group INDRIK SPIDER, also known as Evil Corp, a sophisticated eCrime (ECX 357.19) adversary notorious for conducting numerous schemes against a variety of targets beginning in 2014. This adversary is best known for their Dridex banking trojan, which was prolific from June 2014 through early 2020, and their Bitpaymer crypter used in big game hunting (BGH) attacks beginning in 2017. The OFAC action consisted of sanctions that prohibit the facilitation of significant payments to the organization, such as those involved in BGH ransom payments.

In addition to OFAC's action against INDRIK SPIDER, the U.S. Department of Justice (DOJ) charged two key members of the group — Maksim Yakubets and Igor Turashev — with criminal infringements, and the U.S. Department of State announced a reward of up to $5 million USD for any information leading to the capture or conviction of INDRIK SPIDER's leader.

Following the OFAC sanctions and the unsealing of the indictment, INDRIK SPIDER went through significant periods of downtime and continued to develop their MO, TTPs and tradecraft in an attempt to evade the sanctions placed upon them — the latest evolution is Hades, which first reared its head after the OFAC action was announced.

INDRIK SPIDER’s Reaction

Subsequent to the announcement of the sanctions against the group, INDRIK SPIDER disappeared for a short while until reappearing in January 2020, when BitPaymer was once again observed being used in a BGH operation against a victim conglomerate spanning multiple verticals. This BitPaymer operation was one of the first identified examples of INDRIK SPIDER using a variant of Gozi ISFB as a part of their toolset instead of their Dridex banking trojan.

Following a short hiatus from March to May 2020, INDRIK SPIDER significantly increased their efforts to move away from their existing tools and introduced WastedLocker — the successor to their BitPaymer ransomware. Approximately six months after the OFAC sanctions and the unsealing of the indictment against Yakubets and Turashev, WastedLocker was used in the first BGH campaign, marking a new era for INDRIK SPIDER, as they also began using a variant of Gozi ISFB in their operations. This further operational shift was highly likely an attempt to distance themselves from their infamous Dridex and BitPaymer tools.

In June 2020, the trend of moving away from their typical infection chain continued, and INDRIK SPIDER began using fake browser updates to deliver the Cobalt Strike red-teaming tool. INDRIK SPIDER extensively used Cobalt Strike to establish an initial foothold and move laterally within the victim network. Once control over the enterprise environment was established, WastedLocker would subsequently be executed in their BGH campaigns. INDRIK SPIDER continued with their usual operational tempo, infecting organizations across more than a dozen sectors — predominantly in the U.S. — until late 2020.

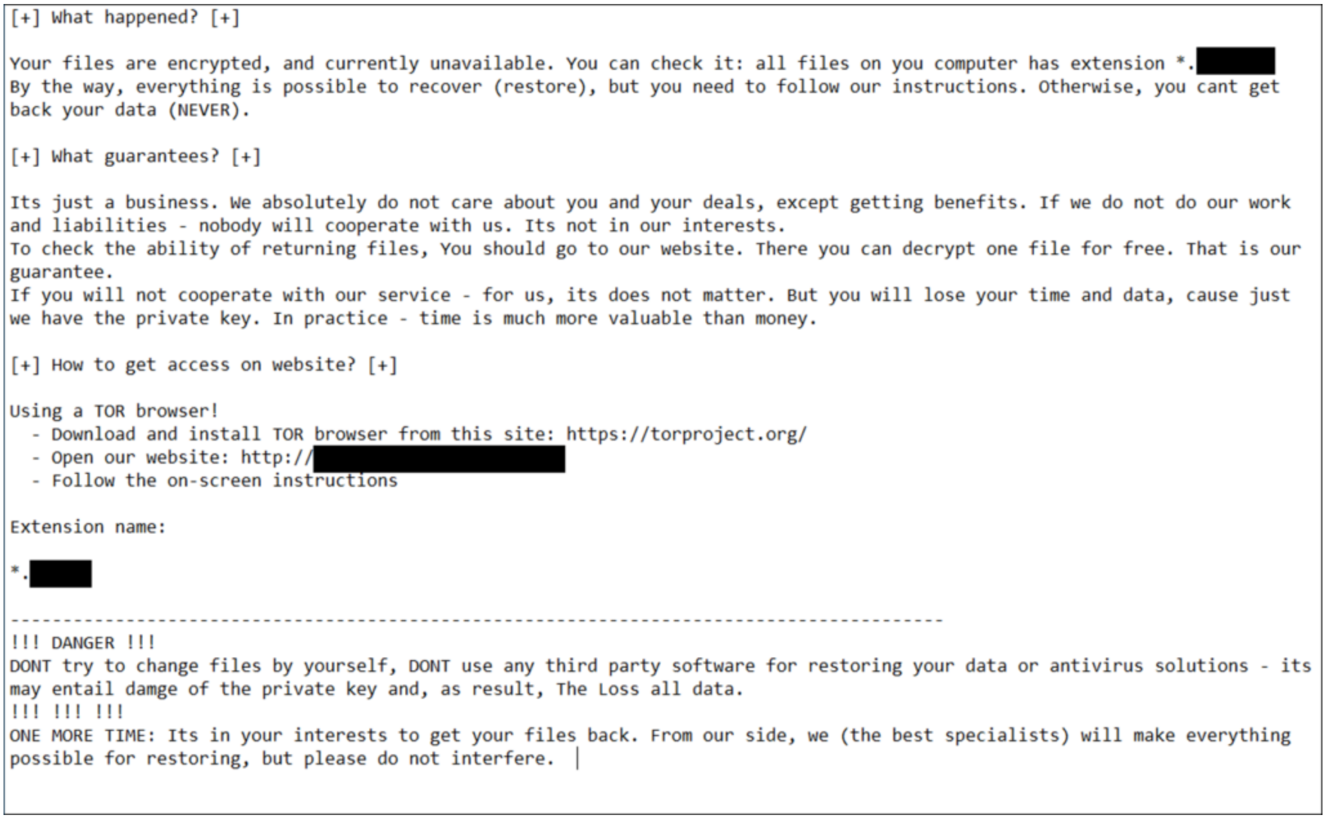
WastedLocker to Hades Evolution

Based on significant code overlap, CrowdStrike Intelligence has identified Hades ransomware as INDRIK SPIDER’s successor to WastedLocker. Hades ransomware — first publicly identified by security researchers in December 2020 — was named for a Tor hidden website that victims are instructed to visit; however, Hades is merely a 64-bit compiled variant of WastedLocker with additional code obfuscation and minor feature changes. The WastedLocker-derived Hades ransomware is unrelated to a similarly named ransomware family, Hades Locker, identified by security firms in 2016.

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. 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. At the time of this publication, CrowdStrike has identified the following changes INDRIK SPIDER made to the WastedLocker-derived Hades ransomware variant:

- Hades is now a 64-bit compiled executable with additional code-obfuscation, likely to disguise the minimal changes, evade existing signature-based detections and hinder reverse engineering efforts.
- The majority of standard file and registry Windows API calls were replaced with their system call counterparts (i.e., the user-mode Native APIs exported from NTDLL).
- Hades employs a different User Account Control (UAC) bypass than WastedLocker; however, both implementations are taken directly from the open-source UACME project (https[:]//github[.]com/hfiref0x/UACME).
- Hades writes a single ransom note named `HOW-TO-DECRYPT-[extension].txt` to traversed directories, as opposed to WastedLocker's and BitPaymer's approach of creating a note for each encrypted file.
- Hades ransomware now stores the key information in each encrypted file rather than the ransom note. Both WastedLocker and BitPaymer stored the encoded and encrypted key information in the file-specific ransom notes.
- While Hades still copies itself to a generated subdirectory in `Application Data`, it no longer uses the `:bin` Alternate Data Stream (ADS). The use of the `:bin` ADS path was characteristic of both WastedLocker and BitPaymer.

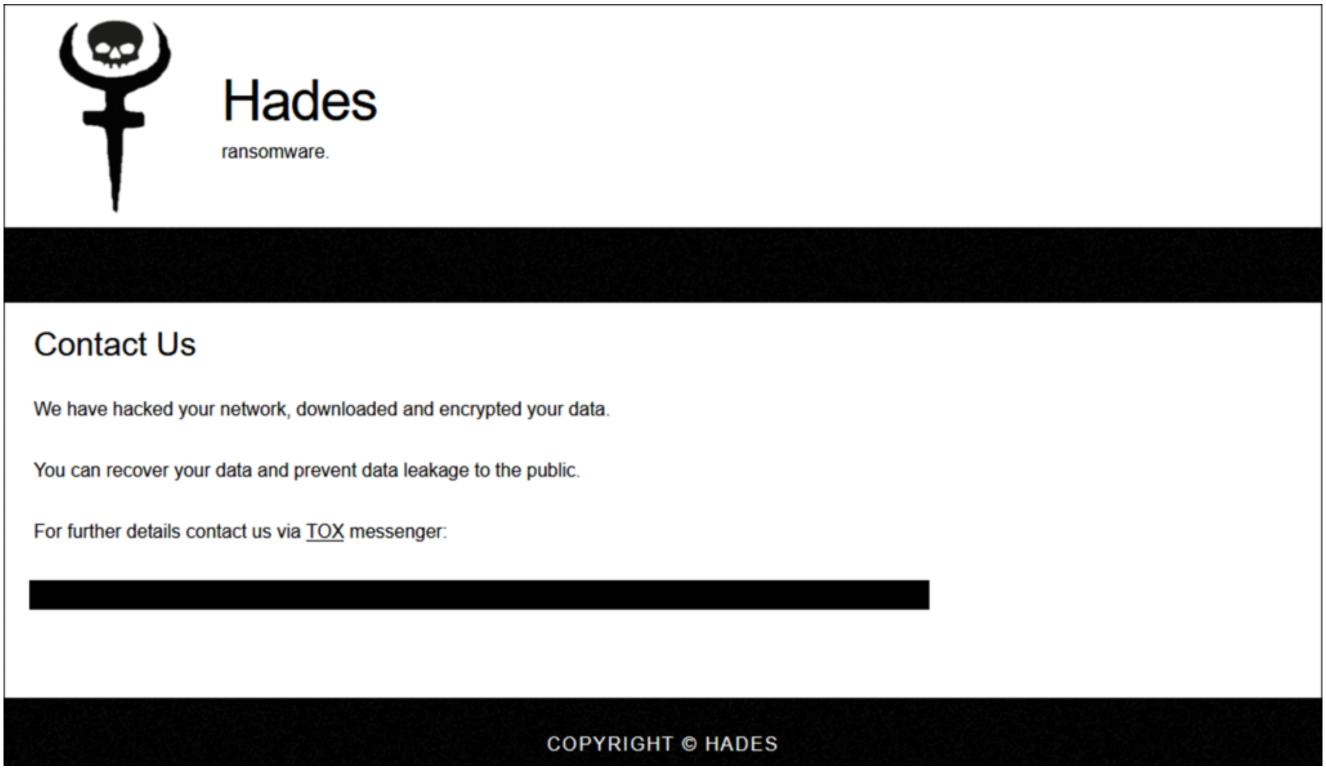
INDRIK SPIDER's move to this ransomware variant also came with another shift in tactics: the departure from using email communication and the possibility of exfiltrating data from victims to elicit payments. The Hades ransom note (shown in Figure 1) directs victims to a Tor hidden site. The identified ransom notes do not identify the victim company, as was often observed with WastedLocker and BitPaymer.



```
[+] What happened? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has extension *.[redacted]
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant get
back your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do our work
and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our
guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just
we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]

Using a TOR browser!
  - Download and install TOR browser from this site: https://torproject.org/
  - Open our website: http://[redacted]
  - Follow the on-screen instructions

Extension name:

*.[redacted]

-----------------------------------------------------------------------------------------
!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its
may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) will make everything
possible for restoring, but please do not interfere.
```

Figure 1. Hades ransomware (WastedLocker variant) ransom note

The Tor website (shown in Figure 2) is unique for each victim and states that data has been exfiltrated from their network. The only provided means of contact is a Tox-identifier for communication with the Tox peer-to-peer instant messenger (https[:]//tox[.]chat/)



Hades

ransomware.

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via TOX messenger:

[redacted]

COPYRIGHT © HADES

Figure 2. Hades ransomware (WastedLocker variant) Tor site

Conclusion

Since the OFAC sanctions and DOJ indictments against the group and its members, INDRIK SPIDER's continued diversification has demonstrated the group's significant resources and operational resilience. INDRIK SPIDER's ability to adapt and overcome adversity has been illustrated in their continual advances in their campaigns, implementation of new tools, and adoption of third-party products and services. The development of their tradecraft has almost certainly been prompted by the legal action taken against them. 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. The sanctions and indictments have undoubtedly significantly impacted the group and have made it difficult for INDRIK SPIDER to successfully monetize their criminal endeavors.

Indicators of Compromise

Description	SHA256 Hash
Hades ransomware, variant of WastedLocker	`fe997a590a68d98f95ac0b6c994ba69c3b2ece9841277b7fecd9dfaa6f589a87`

Additional Resources

- *Read more about big game hunting adversaries tracked by CrowdStrike Intelligence in 2020 in the CrowdStrike 2021 Global Threat Report.*
- *Check out the Global Threat Report resource hub to learn more about today's adversaries.*
- *To find out more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Learn more about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*