Free HermeticRansom Ransomware Decryptor Released

By Lisa Vaas

Published: 2022-03-04 · Archived: 2026-04-06 00:59:27 UTC

Cruddy cryptography means victims whose files have been encrypted by the Ukraine-tormenting ransomware can break the chains without paying extortionists.

A free decryptor is out to unlock a ransomware found piggybacking on the HermeticWiper data wiper malware that ESET and Broadcom's Symantec discovered targeting machines at financial, defense, aviation and IT services outfits in Ukraine, Lithuania and Latvia last week.

The fact that there was ransomware clinging to the data-wiping malware didn't surprise cybersecurity experts, of course. It was predicted by Katie Nickels, director of intel at Red Canary, for one: She tweeted that there was very likely a "broader intrusion chain."

What might have been a bit more surprising was the welcome discovery, made by CrowdStrike's Intelligence Team earlier this week, that HermeticRansom had a lame encryption process that let the ransomware's tentacles be untangled.

Avast Threat Labs had spotted the new ransomware strain last Thursday, Feb. 24. Avast, which named the new strain HermeticRansom, on Thursday released a free decryptor that incorporated a decryption script CrowdStrike released to GitHub, a user-friendly GUI and a set of instructions on its use.

The decryptor can be downloaded here.

Crypto Likely Weakened by Coding Errors

HermeticRansom, aka PartyTicket, was identified at several victimized organizations, among other malware families that included what CrowdStrike called the "sophisticated" HermeticWiper, aka DriveSlayer.

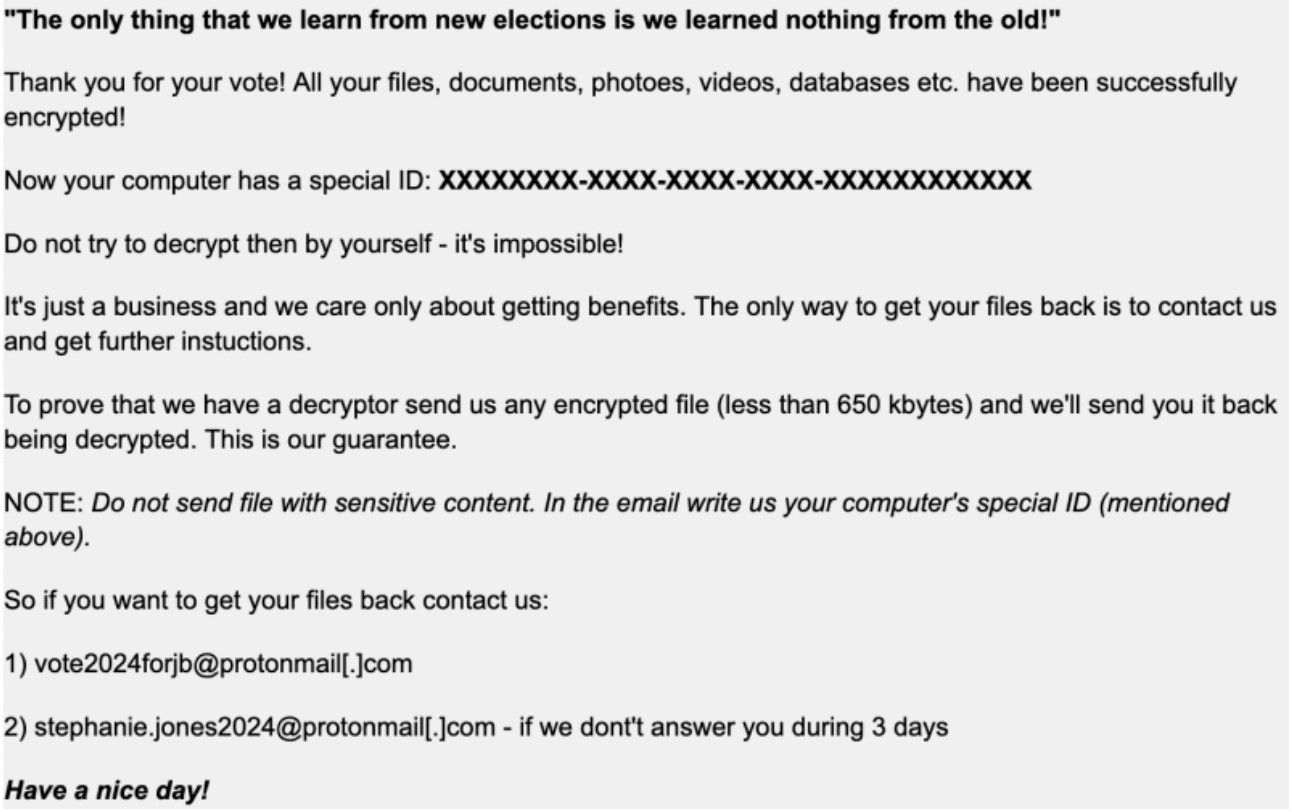
Regardless of how sophisticated the wiper malware was, the ransomware that hopped a ride on it had less-than-stellar encryption, with a logic flaw in the encryption process that enabled researchers to break through, CrowdStrike said: "Analysis of the [PartyTicket/HermeticRansom] ransomware indicates it superficially encrypts files and does not properly initialize the encryption key, making the encrypted file with the associated .encryptedJB extension recoverable."

At the time it published its report, CrowdStrike hadn't traced the ransomware to a known threat actor. It didn't quite seem like a serious attempt at ransomware, at any rate, researchers said, given the coding errors that made its encryption "breakable and slow."

Either the malware author was unfamiliar with writing in Go or rushed its development without thoroughly testing it, analysts surmised.

Either way, it looked to analysts as if extortion wasn't the primary aim: "The relative immaturity and political messaging of the ransomware, the deployment timing and the targeting of Ukrainian entities are consistent with its use as an additional payload alongside DriveSlayer activity, rather than as a legitimate ransomware extortion attempt," they wrote.

Below is a screen capture of HermeticRansom's extortion note:



"The only thing that we learn from new elections is we learned nothing from the old!"

Thank you for your vote! All your files, documents, photoes, videos, databases etc. have been successfully encrypted!

Now your computer has a special ID: **XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX**

Do not try to decrypt then by yourself - it's impossible!

It's just a business and we care only about getting benefits. The only way to get your files back is to contact us and get further instuctions.

To prove that we have a decryptor send us any encrypted file (less than 650 kbytes) and we'll send you it back being decrypted. This is our guarantee.

NOTE: *Do not send file with sensitive content. In the email write us your computer's special ID (mentioned above).*

So if you want to get your files back contact us:

1) vote2024forjb@protonmail[.]com

2) stephanie.jones2024@protonmail[.]com - if we dont't answer you during 3 days

Have a nice day!

HermeticRansom ransomware demand note. Source: CrowdStrike Intelligence Team.

HermeticWiper History

HermeticWiper, discovered last week, has been used against hundreds of machines in Ukraine – attacks that followed distributed denial-of-service (DDoS) attacks launched against Ukraine websites on Feb. 23.

One of the HermeticWiper malware samples was compiled back on Dec. 28, pointing to the wiper attacks having been readied two months before Russia's military assault.

HermeticWiper was only one of an onslaught of cyberattacks and malware that have been unleashed prior to and during the crisis, including the novel FoxBlade trojan, a wave of pre-invasion DDoS attacks in mid-February, plus another campaign of wiper attacks targeting Ukraine and aimed at eroding trust in January – just a few of an ongoing barrage of cyberattacks in the cyber warzone.

Register Today for **Log4j Exploit: Lessons Learned and Risk Reduction Best Practices** – a LIVE **Threatpost event** sked for Thurs., March 10 at 2PM ET. Join Sonatype code **expert Justin Young** as he helps you sharpen code-hunting skills to reduce attacker dwell time. Learn why Log4j is still dangerous and how SBOMs fit into software supply-chain security. Register Now for this one-time FREE event, Sponsored by Sonatype.

Source: https://threatpost.com/free-hermeticransom-ransomware-decryptor-released/178762/