CrowdStrike cracks PartyTicket ransomware targeting Ukraine

By Arielle Waldman

Published: 2022-03-02 · Archived: 2026-04-06 00:46:54 UTC

By

- Arielle Waldman, Features Writer, Dark Reading

Published: 02 Mar 2022

While a new ransomware strain was used in "destructive attacks" that targeted Ukrainian organizations hours before the Russian invasion, CrowdStrike determined it is decryptable.

On Feb. 23, antimalware vendor ESET uncovered a new data-wiping malware it dubbed HermeticWiper used in a campaign hours after a series of DDoS attacks kicked several websites associated with the Ukrainian government offline. ESET researchers also observed a Go-based ransomware it tracks as HermeticRansom deployed during the campaign. Following reports from ESET and other vendors, CrowdStrike began tracking the "sophisticated wiper" under the name DriveSlayer.

While analyzing DriveSlayer, CrowdStrike uncovered new insight into HermeticRansom, which it is tracking as PartyTicket.

CrowdStrike provided further analysis in a blog post Tuesday where the security vendor said PartyTicket ransomware "superficially encrypts files" due to implementation errors that make "its encryption breakable and slow." While CrowdStrike did not attribute PartyTicket to a specific threat group, it did provide further insight into the developer.

"This flaw suggests that the malware author was either inexperienced writing in Go or invested limited efforts in testing the malware, possibly because the available development time was limited," the blog post said.

CrowdStrike published a script in the blog post that will decrypt files that have been locked by PartyTicket. "Due to the previously discussed implementation errors in the AES key generation, it is possible to recover the AES key used for encryption by PartyTicket," it explained.

A sample analysis revealed many symbols referencing the U.S. political system, such as President Joe Biden and the White House. CrowdStrike observed that prior to encryption, the ransomware renamed the file using a format that included the letters JB, which "very likely stands for the initials of the United States president Joseph Biden."

Based on the three factors including the deployment timing, political messaging and "relative immaturity" of the ransomware, CrowdStrike said the primary use of PartyTicket is as an "additional payload alongside DriveSlayer activity, rather than as a legitimate ransomware extortion attempt."

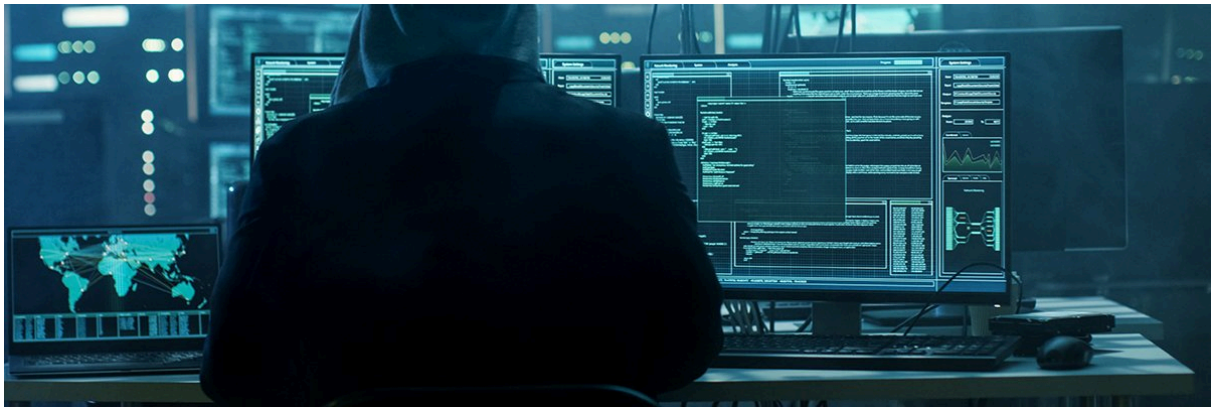
Similarly, ESET researchers determined that the ransomware was potentially used to hide the actions of the data-wiping malware and did not mention any extortion motives. Several security vendors and threat analysts have tracked destructive malware attacks against various targets in Ukraine since Russia's invasion of the country began last week.

Dig Deeper on Threats and vulnerabilities

- 

  Top open source and commercial threat intelligence feeds

By: Karen Kent



CrowdStrike: Europe second only to North America for cyber attacks

By: Brian McKenna

News brief: KillSec, Yurei score successful ransomware attacks

By: Staff report

- 

How ESET is using AI PCs to boost endpoint security

By: Gabe Knuth
