

Second New 'IsaacWiper' Data Wiper Targets Ukraine After Russian Invasion

[H thehackernews.com/2022/03/second-new-isaacwiper-data-wiper.html](https://thehackernews.com/2022/03/second-new-isaacwiper-data-wiper.html)

March 1, 2022



A new data wiper malware has been observed deployed against an unnamed Ukrainian government network, a day after destructive cyber attacks struck multiple entities in the country preceding the start of Russia's military invasion.

Slovak cybersecurity firm ESET dubbed the new malware "[IsaacWiper](#)," which it said was detected on February 24 in an organization that was not affected by [HermeticWiper](#) (aka FoxBlade), another data wiping malware that targeted several organizations on February 23 as part of a sabotage operation aimed at rendering the machines unusable.

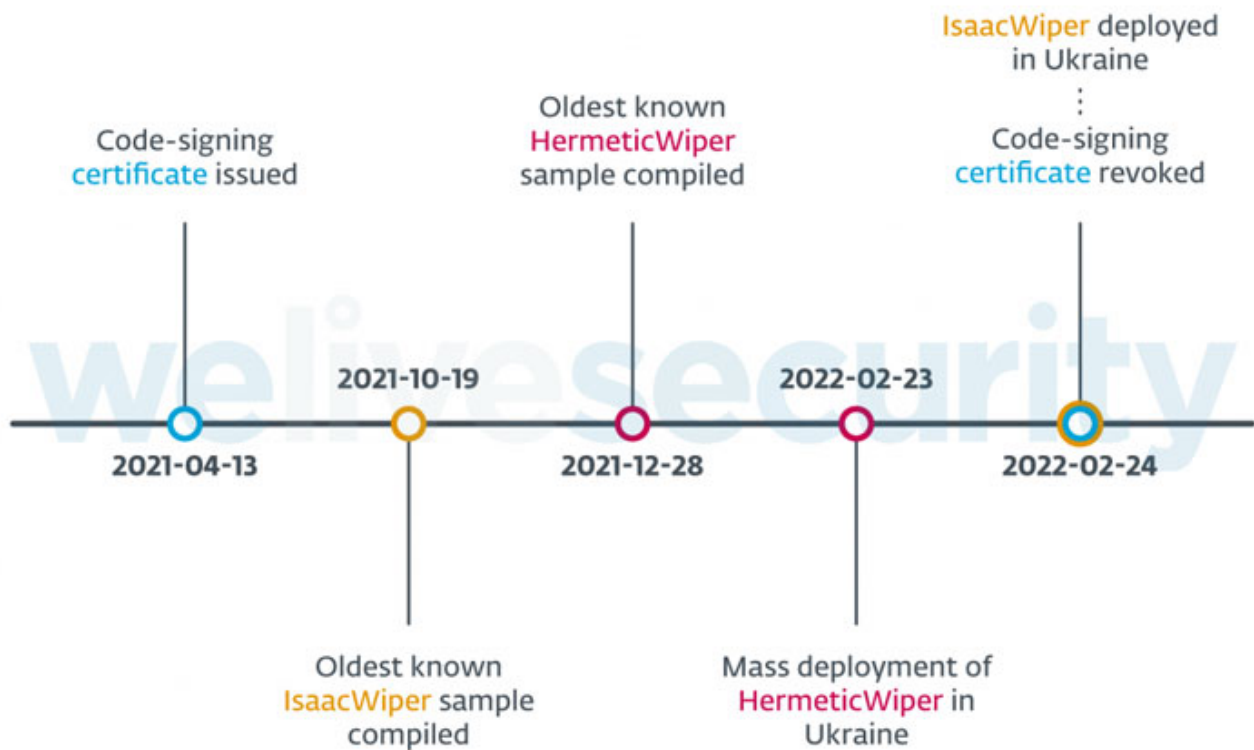
Further analysis of the HermeticWiper attacks, which infected at least five Ukrainian organizations, have revealed a worm constituent that propagates the malware across the compromised network and a ransomware module that acts as a "distraction from the wiper attacks," corroborating a [prior report](#) from Symantec.



"These destructive attacks leveraged at least three components: HermeticWiper for wiping the data, HermeticWizard for spreading on the local network, and HermeticRansom acting as a decoy ransomware," the company said.


In a separate analysis of the new Golang-based ransomware, Russian cybersecurity company Kaspersky, which codenamed the malware "Elections GoRansom," characterized it as a last-minute operation, adding it was "likely used as a smokescreen for the HermeticWiper attack due to its non-sophisticated style and poor implementation."

As an anti-forensic measure, HermeticWiper is also designed to hinder analysis by erasing itself from the disk by overwriting its own file with random bytes.



ESET said it hasn't been able to find "any tangible connection" to attribute these attacks to a known threat actor. But the malware artifacts unearthed so far make it clear that the intrusions had been planned for several months, with the targeted entities suffering compromises well in advance of the wiper's deployment.

"This is based on several facts: the HermeticWiper PE compilation timestamps, the oldest being December 28, 2021; the code-signing certificate issue date of April 13, 2021; and the deployment of HermeticWiper through the default domain policy in at least one instance, suggesting the attackers had prior access to one of that victim's Active Directory servers," said Jean-Ian Boutin, ESET head of threat research.

 CyberSecurity

Also unknown are the initial access vectors used to deploy both the wipers, although it's suspected that the attackers leveraged tools like Impacket and RemCom, a remote access software, for lateral movement and malware distribution.

Furthermore, IsaacWiper shares no code-level overlaps with HermeticWiper and is substantially less sophisticated, even as it sets out to enumerate all the physical and logical drives before proceeding to carry out its file wiping operations.

"On February 25, 2022, attackers dropped a new version of IsaacWiper with debug logs," the researchers said. "This may indicate that the attackers were unable to wipe some of the targeted machines and added log messages to understand what was happening."

Update: Microsoft, which is tracking HermeticWiper under the name FoxBlade (and HermeticRansom as SonicVote), said the "intended objective of these attacks is the disruption, degradation, and destruction of targeted resources" in Ukraine.

The infections impacted "hundreds of systems spanning multiple government, information technology, financial sector, and energy organizations predominantly located in or with a nexus to Ukraine," it noted.

The tech giant's Threat Intelligence Center (MSTIC) has attributed the attacks to an emerging threat cluster designated as DEV-0665, pointing out its lack of affiliation to a previously known threat activity group. It's worth noting here that the actor responsible for the WhisperGate wiper attacks in January is known as DEV-0586.

Assigning IsaacWiper-related intrusions the moniker Lasainraw, Microsoft also characterized them as a "limited destructive malware attack," adding it's "continuing to investigate this incident and has not currently linked it to known threat activity."

SHARE     

SHARE 