IsaacWiper Followed HermeticWiper Attack on Ukraine Orgs

By Teri Robinson

Published: 2022-03-11 · Archived: 2026-04-05 20:08:48 UTC

In the hours before Russia invaded Ukraine, a destructive malware campaign used HermeticWiper to attack several Ukrainian organizations and, just a day after the invasion began, another wiper, dubbed IsaacWiper by ESET, was pressed into service against a Ukraine government network.

The attackers were not finished, though; perhaps because they could not wipe some of the targeted machines, a WeLiveSecurity blog reported they dropped another version of IsaacWiper that included debug logs.

“With regard to IsaacWiper, we are currently assessing its links, if any, with HermeticWiper,” said ESET head of threat research Jean-Ian Boutin. “It is important to note that it was seen in a Ukrainian governmental organization that was not affected by HermeticWiper.”

The initial wiper attack leveraged HermeticWiper to wipe data, HermeticWizard to spread through the local network and HermeticRansom as decoy ransomware.

The malware artifacts examined seemed to suggest the attacks, which the researchers have not been able to attribute to a particular actor, likely had been planned for several months. “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,” Boutin said.

The HermeticWiper overwrites its own file with random bytes to wipe itself from disk in what researchers feel is an attempt to prevent the wiper from being analyzed. The wiper is spread via a custom worm that ESET calls HermeticWizard, they wrote.

Organizations can expect even more attacks and with greater frequency. “Information warfare, which we refer to as cyberwarfare, is a major component of the Russian doctrine. This explains why, whenever there is a conflict related to Russia, you should expect to see force being applied on the cyber domain as well to create disorientation, lack of trust and fear,” said Mitiga co-founder and CEO Ariel Parnes, former head of the Cyber Department for the Israeli Intelligence Service. “Russia has significant offensive cybersecurity capabilities, including institutional and criminal elements.”

While “the increase in operations will result in smaller-scale impacts as targeting is rushed … for those affected, it won’t be smaller,” said Parnes. “Companies should therefore be ready to increase their ability to detect, patch and remediate against an increase in zero-day vulnerabilities.”

But deploying new defensive cybersecurity capabilities may not be enough to quickly or fully protect organizations. “There is only so much you can do now to prevent a cyberattack in the immediate future,

particularly if you are targeted by Russia or a state-sponsored attacker," said Parnes. "There is a good chance that your organization was already attacked, and they have a backdoor to your network."

Under Russia's doctrine, it has already "conducted cyber operations for quite a while, silently preparing the access needed so they can choose which one to activate and when, by deleting or encrypting data, conducting a distributed denial-of-service attack, or carrying out another attack that will impact business operations," said Parnes.

Organizations should strive to bolster resilience. "Increasingly, geopolitical events have global impact, highlighting the importance of focusing on resilience so that organizations are ready, prepared to recover rapidly and resilient if they get caught up in a wave of state-sponsored cyberattacks," said Parnes.

Recent Articles By Author

Source: https://securityboulevard.com/2022/03/isaacwiper-followed-hermeticwiper-attack-on-ukraine-orgs/