New Wiper Malware Targeting Ukraine Amid Russia's Military Operation

thehackernews.com/2022/02/new-wiper-malware-targeting-ukraine.html

February 23, 2022

Cybersecurity firms ESET and Broadcom's Symantec said they discovered a new data wiper malware used in fresh attacks against hundreds of machines in Ukraine, as Russian forces formally launched a full-scale military operation against the country.

The Slovak company dubbed the wiper "**HermeticWiper**" (aka **KillDisk.NCV**), with one of the malware samples compiled on December 28, 2021, implying that preparations for the attacks may have been underway for nearly two months.

"The wiper binary is signed using a code signing certificate issued to Hermetica Digital Ltd," ESET said in a series of tweets. "The wiper abuses legitimate drivers from the EaseUS Partition Master software in order to corrupt data. As a final step the wiper reboots [the] computer."

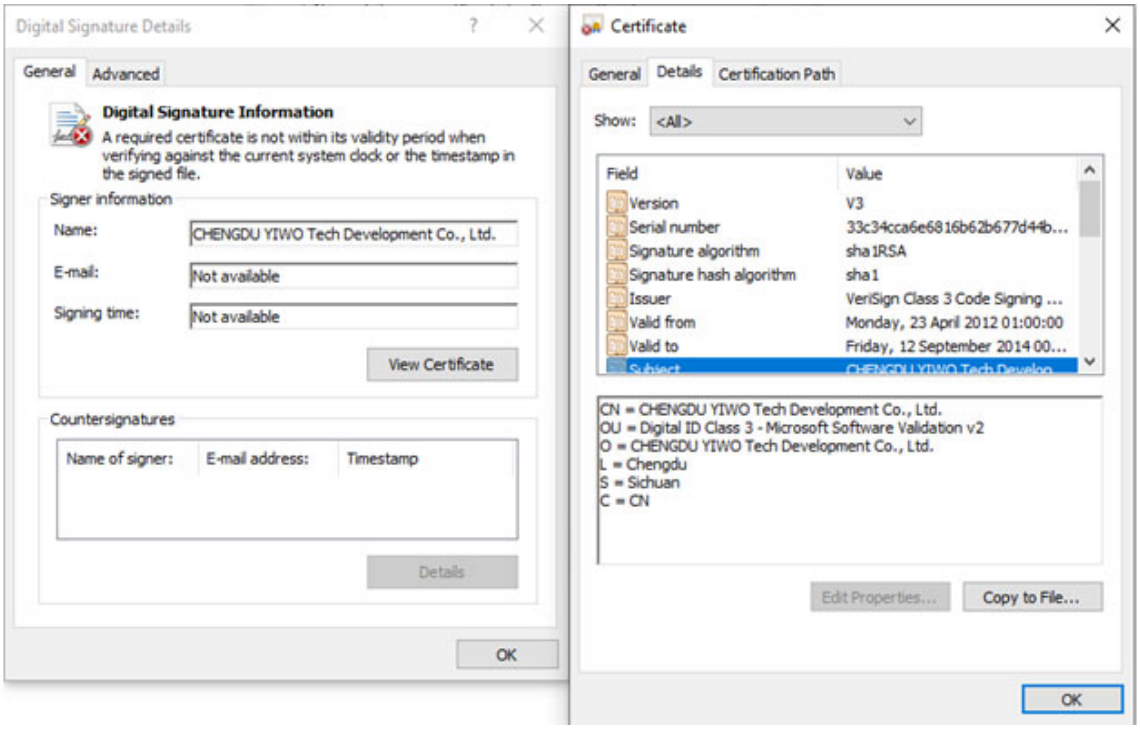
Specifically, HermeticWiper is delivered via the benign but signed EaseUS partition management driver that then proceeds to impair the first 512 bytes, the Master Boot Record (MBR) for every physical drive, before initiating a system shutdown and effectively rendering the machine inoperable.

"After a week of defacements and increasing DDoS attacks, the proliferation of sabotage operations through wiper malware is an expected and regrettable escalation," SentinelOne's principal threat researcher Juan Andres Guerrero-Saade said in a report analyzing the new malware.

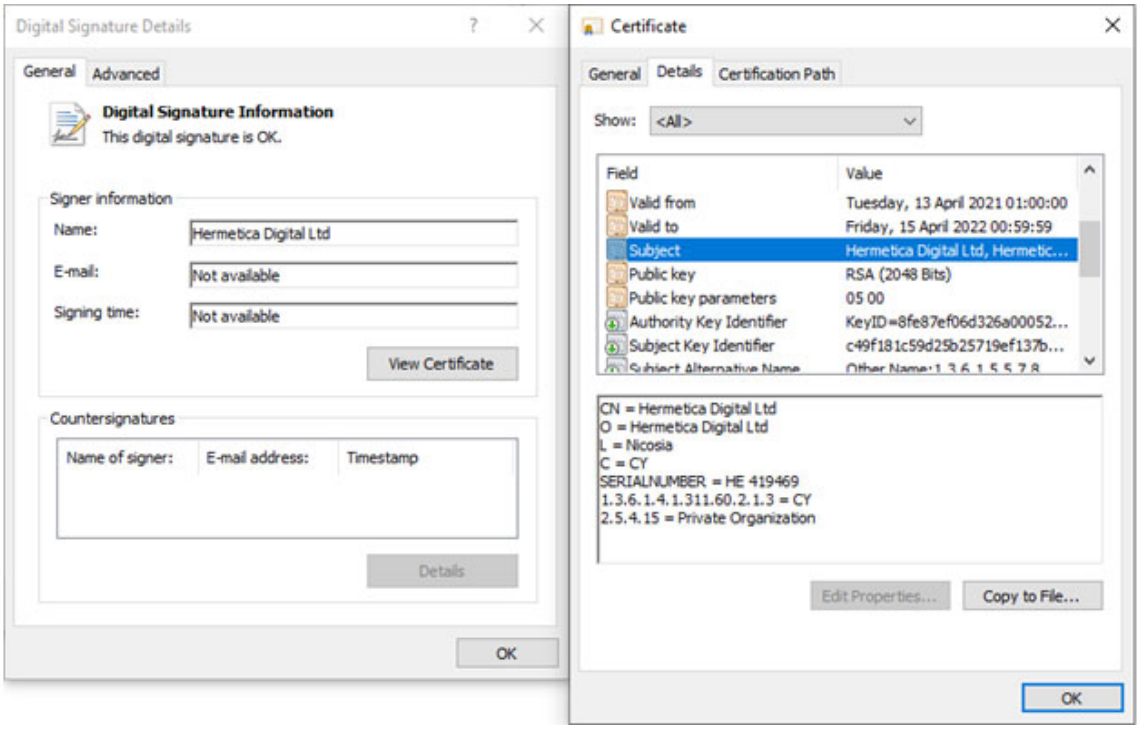
At least one of the intrusions involved deploying the malware directly from the Windows domain controller, indicating that the attackers had taken control of the target network.

The scale and the impact of the data-wiping attacks remains unknown as yet, as is the identity of the threat actor behind the infections. But the development marks the second time this year that a destructive malware has been deployed on Ukrainian computer systems after the WhisperGate operation in mid-January.

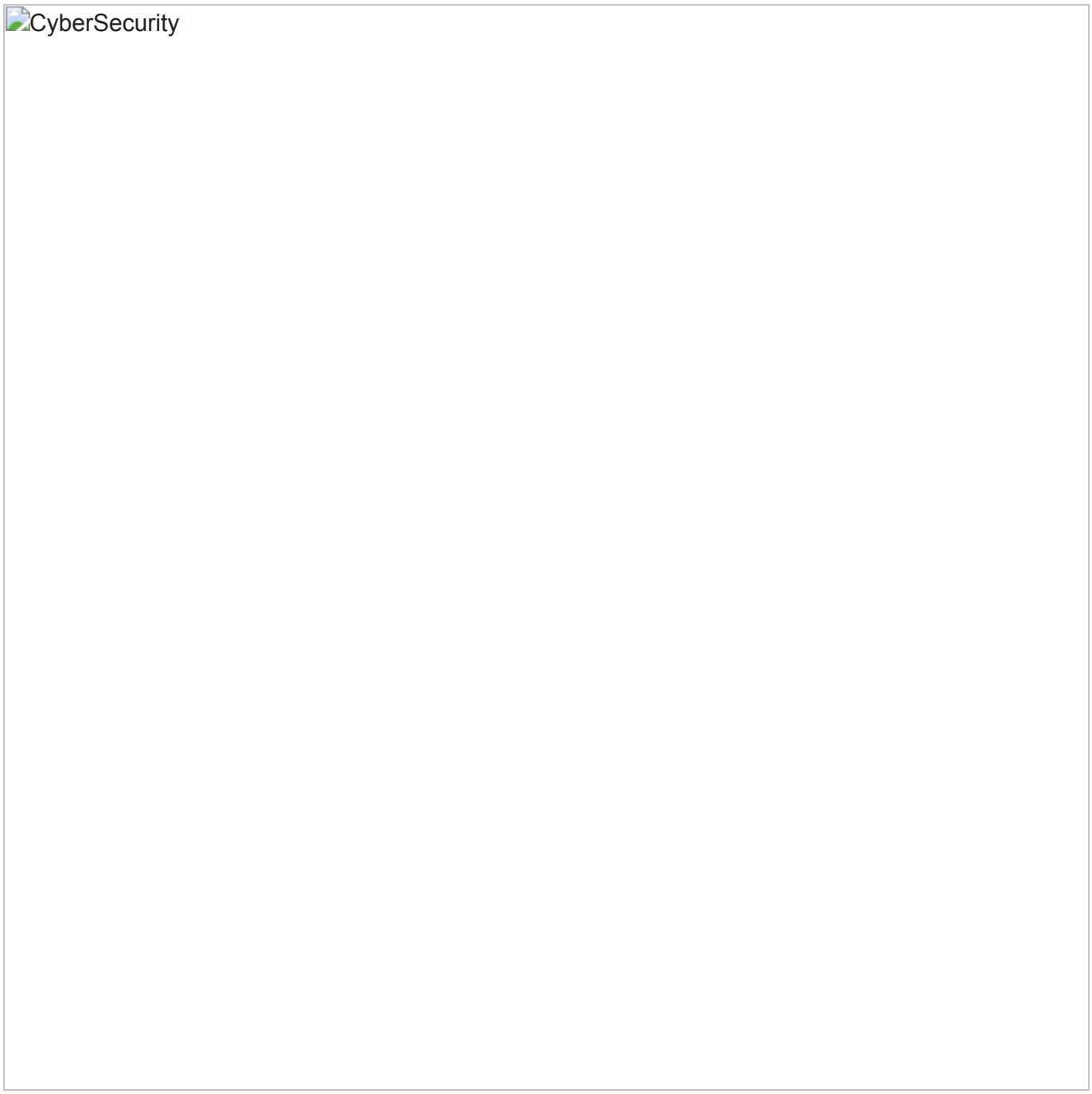
The wiper attacks also follow a third "massive" wave of distributed denial-of-service (DDoS) attacks that hit several Ukrainian government and banking institutions on Wednesday, knocking out online portals for the Ministry of Foreign Affairs, Cabinet of Ministers, and Rada, the country's parliament.



Last week, two of the largest Ukrainian banks, PrivatBank and Oschadbank, as well as the websites of the Ukrainian Ministry of Defense and the Armed Forces suffered outages as a result of a DDoS attack from unknown actors, prompting the U.K. and U.S. governments to point the fingers at the Russian Main Intelligence Directorate (GRU), an allegation the Kremlin has denied.



Campaigns that use DDoS attacks deliver torrents of junk traffic that are intended to overwhelm targets with the goal of rendering them inaccessible. A subsequent analysis of the February 15 incidents by the CERT-UA found that they were carried out using botnets such as Mirai and Mēris by leveraging compromised MikroTik routers and other IoT devices.



What's more, information systems belonging to Ukraine's state institutions are said to have been unsuccessfully targeted in as many as 121 cyber attacks in January 2022 alone.

That's not all. Cybercriminals on the dark web are looking to capitalize on the ongoing political tensions by advertising databases and network accesses containing information on Ukrainian citizens and critical infra entities on RaidForums and Free Civilian marketplaces in "hopes of gaining high profits," according to a report published by Accenture earlier this week.

The continuous onslaught of disruptive malicious cyber acts since the start of the year has also led the Ukrainian law enforcement authority to paint the attacks as an effort to spread anxiety, undermine confidence in the state's ability to defend its citizens, and destabilize its unity.

"Ukraine is facing attempts to systematically sow panic, spread fake information and distort the real state of affairs," the Security Service of Ukraine (SSU) said on February 14. "All this combined is nothing more than another massive wave of hybrid warfare."

SHARE □ □ □ □ □
SHARE □