Putin Warns Russian Critical Infrastructure to Brace for Potential Cyber Attacks

thehackernews.com/2022/02/putin-warns-russian-critical.html

February 25, 2022

The Russian government on Thursday warned of cyber attacks aimed at domestic critical infrastructure operators, as the country's full-blown invasion of Ukraine enters the second day.

In addition to cautioning of the "threat of an increase in the intensity of computer attacks," Russia's National Computer Incident Response and Coordination Center said that the "attacks can be aimed at disrupting the functioning of important information resources and services, causing reputational damage, including for political purposes."

"Any failure in the operation of [critical information infrastructure] objects due to a reason that is not reliably established, first of all, should be considered as the result of a computer attack," the agency added.

Furthermore, it notified of possible influence operations undertaken to "form a negative image of the Russian Federation in the eyes of the world community," echoing a similar alert released by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) last week about information manipulation efforts from foreign actors to strike critical entities.

The agency, however, didn't share more specifics on the nature of the attacks or their provenance.

The advisory comes as multiple government and banking websites in Russia, including that of military (mil.ru), the Kremlin (kremlin.ru), and the State Duma (duma.gov.ru), were rendered unreachable amid a spate of cyber offensives targeting Ukraine that resulted in the deployment of a data wiper called HermeticWiper on hundreds of machines in the East European nation.

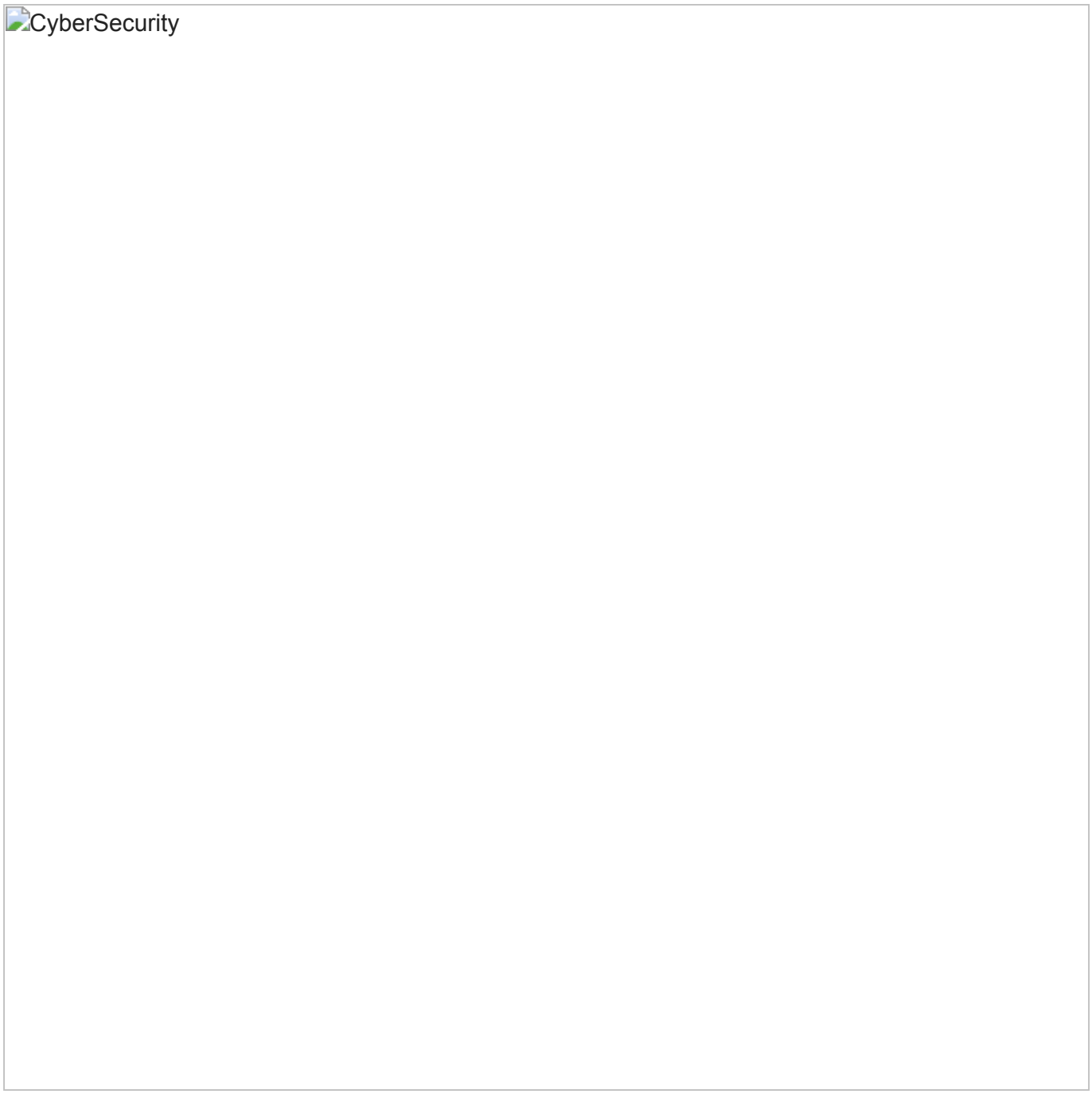
"It's important to note that the wiper leverages high privileges on the compromised host to make the host 'unbootable' by overriding the boot records and configurations, erase device configurations, and delete shadow copies," Lavi Lazarovitz, head of security research at CyberArk Labs, said in a statement shared with The Hacker News.

"The wiper is configured to not encrypt domain controllers – that is to keep the domain running and allow the ransomware to use valid credentials to authenticate to servers and encrypt those. This further highlights that the threat actors use compromised identities to access the network and / or move laterally," Lazarovitz elaborated.

It's not clear how many networks have been affected by the previously unseen data-wiping malware, which targeted organizations in the financial, defense, aviation, and IT industries, according to Symantec. The Broadcom-owned company also said it observed evidence of wiper attacks against machines in Lithuania, implying a spillover effect.

What's more, HermeticWiper shares overlaps with another data wiper called WhisperGate that was first reported as being used against Ukrainian organizations in January. Like the latter, the newly discovered malware is accompanied by the distribution of a ransomware strain on compromised systems.

The ransomware malware is a 64-bit, 3.14 MB .EXE file, written in Golang, per Cybereason's incident response engineer, Chen Erlich, who shared a preliminary analysis of the executable.



"It appears likely that the ransomware was used as a decoy or distraction from the wiper attacks," Symantec said. "This has some similarities to the earlier WhisperGate wiper attacks against Ukraine, where the wiper was disguised as ransomware."

Initial forensic analysis suggests that the attacks may have been in preparation mode for at least three months, what with potentially related malicious activity detected in a Lithuanian organization as early as November 12, 2021. Also, one of the HermeticWiper samples was found to have a compilation timestamp of December 28, 2021.

While the latest disruptive actions are yet to be formally attributed, the U.K. and U.S. governments linked the DDoS attacks on Ukraine in mid-February to Russia's Main Intelligence Directorate (also known as GRU).

As the attacks continue to unfold both on the physical and digital realms, Reuters reported that the Ukrainian government is seeking the help of the underground hacker community in the country to fend off cyber infiltrations aimed at critical infrastructure and conduct covert espionage missions against the invading Russian forces.

SHARE □ □ □ □ □
SHARE □