Ransomware is being used as bait in data destruction attacks targeting Ukraine

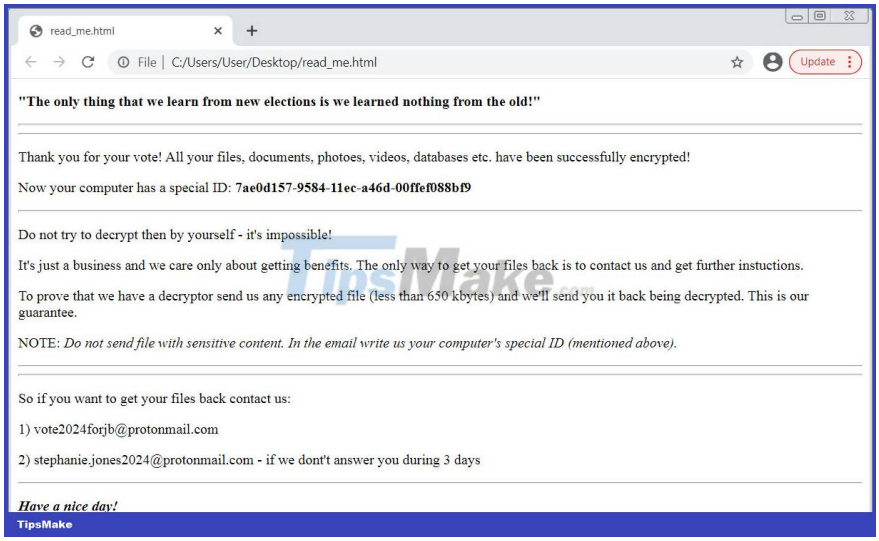
International security researchers have issued a warning about a new type of data erasure malware that is currently being deployed in destructive attacks targeting Ukraine's network infrastructure.

International security researchers have issued a warning about a new type of data erasure malware that is currently being deployed in destructive attacks against Ukraine's network infrastructure. In many cases, the attacks are accompanied by a GoLang-based ransomware.

The Symantec security team said today that it has found a malicious wiper malware program called HermeticWiper that is being deployed in infection campaigns targeting agencies and organizations related to the Ukrainian government. This is basically a type of malicious code designed to erase data in a radical way. After successful infection, HermeticWiper will immediately destroy data on the system, making it unrecoverable and causing local failure.

Symantec also revealed another interesting piece of information, which is that it appears that ransomware has been used as a bait or as a distraction from malicious and potentially dangerous wiper malware attacks. more severe damage. This suggests some similarities to previous WhisperGate attacks that also targeted Ukraine, where wiper malware was disguised as ransomware.

The decoy ransomware also comes with ransom notices on compromised systems, along with political messages. The ransom note instructs victims to contact two email addresses ( and ) to recover encrypted data.



The hacked targets included financial contractors and government organizations from not only Ukraine but also Latvia and Lithuania.

Although the cyberattack was primarily recorded on February 24, cybersecurity firm ESET noted that the HermeticWiper malware has code compiled from December 28, 2021. This suggests that this could be a pre-planned cyber attack. Up to now, thousands of devices operating in Ukraine's cyberspace have been found to be infected with the above malware.

Notably, Symantec also found evidence that attackers gained access to victims' networks long before that, by exploiting Microsoft Exchange vulnerabilities in early November. 2021 and install the web shell before deploying the malware.

The wiper malware uses the EaseUS Partition Manager driver to corrupt the files of the compromised device before rebooting the system. In particular, the data eraser will also wipe the device's Master Boot Record, making all infected devices unbootable.

Along with the malware infection attacks, Ukraine's network infrastructure is also suffering from a series of DDoS attacks targeting a number of key government agencies and banks.