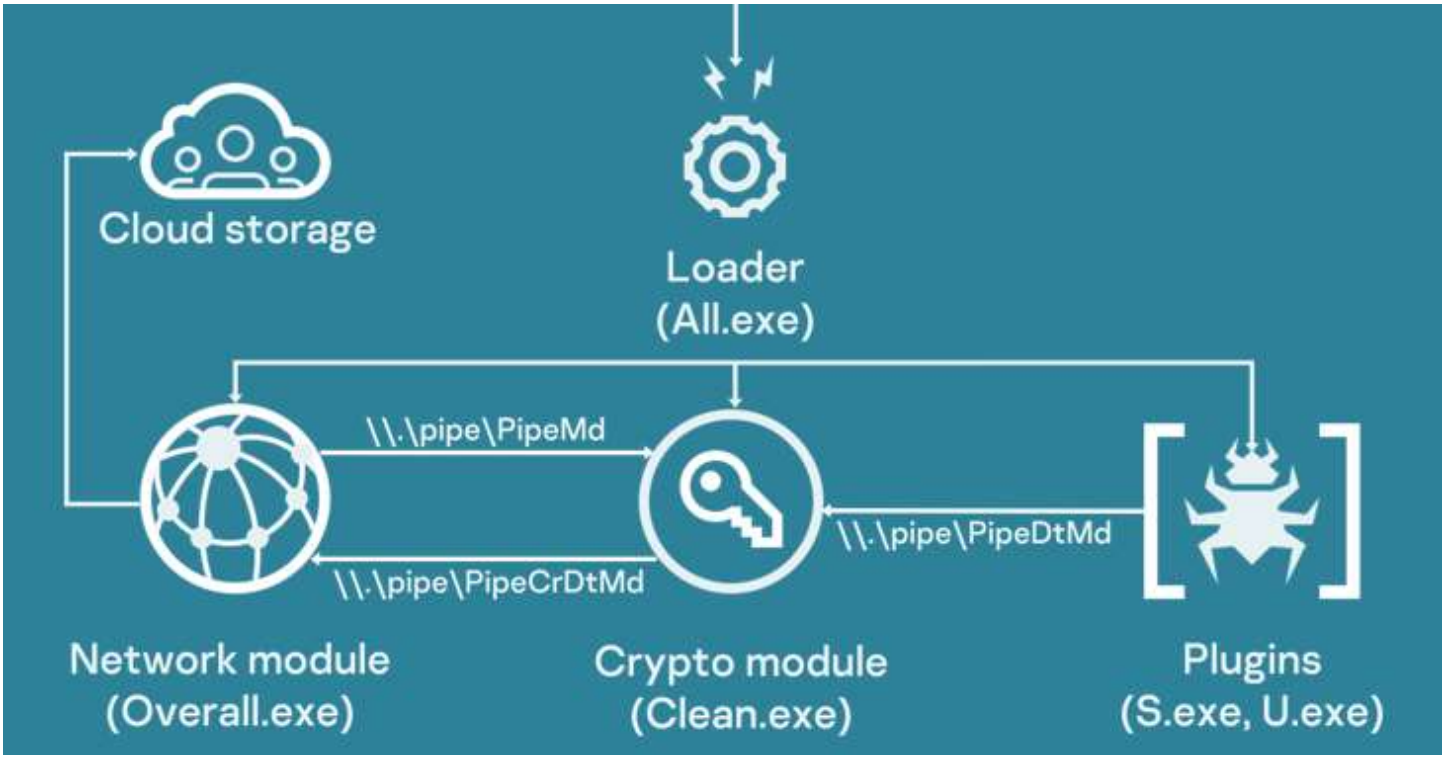
New 'Bad Magic' Cyber Threat Disrupts Ukraine's Key Sectors Amid War

Mar 21, 2023 Ravie Lakshmanan



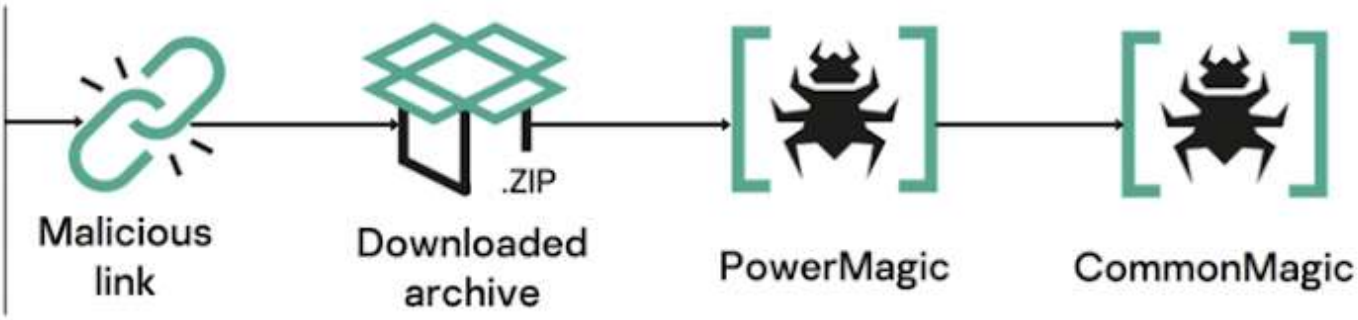
Amid the ongoing war between Russia and Ukraine, government, agriculture, and transportation organizations located in Donetsk, Lugansk, and Crimea have been attacked as part of an active campaign that drops a previously unseen, modular framework dubbed **CommonMagic**.

"Although the initial vector of compromise is unclear, the details of the next stage imply the use of spear phishing or similar methods," Kaspersky said in a new report.

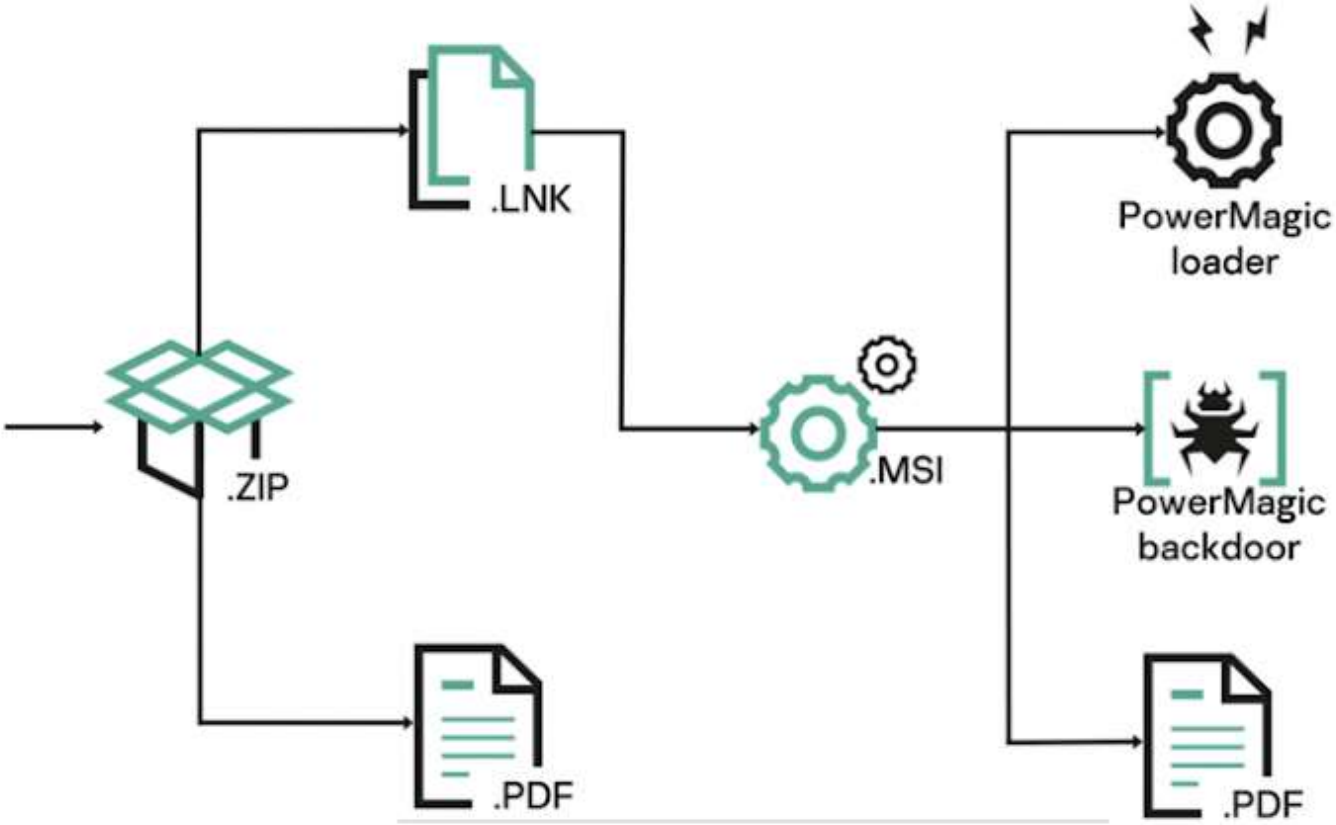
The Russian cybersecurity company, which detected the attacks in October 2022, is tracking the activity cluster under the name "Bad Magic."

Attack chains entail the use of booby-trapped URLS pointing to a ZIP archive hosted on a malicious web server. The file, when opened, contains a decoy document and a malicious LNK file that culminates in the deployment of a backdoor named PowerMagic.

Written in PowerShell, PowerMagic establishes contact with a remote server and executes arbitrary commands, the results of which are exfiltrated to cloud services like Dropbox and Microsoft OneDrive.



Infection chain



Installation workflow

PowerMagic also serves as a conduit to deliver the CommonMagic framework, a set of executable modules that are designed to carry out specific tasks such as interacting with the command-and-control (C2) server, encrypting and decrypting C2 traffic, and executing plugins.

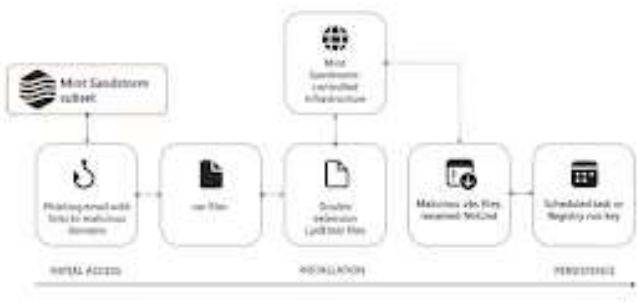
Two of the plugins discovered so far come with capabilities to capture screenshots every three seconds and gather files of interest from connected USB devices.

Kaspersky said it found no evidence linking the operation and its tooling to any known threat actor or group. The earliest ZIP archive attachment dates back to September 2021, indicating that the campaign may have flown under the radar for more than 1.5 years.

"Geopolitics always affect the cyberthreat landscape and lead to the emergence of new threats," Kaspersky's Leonid Besverzhenko said. "Although the malware and techniques employed in the CommonMagic campaign are not particularly sophisticated, the use of cloud storage as the command-and-control infrastructure is noteworthy."

Found this article interesting? Follow us on Twitter and LinkedIn to read more exclusive content we post.

Breaking News



Iranian Hackers Masquerade as Journalists to Spy on Israel-Hamas War Experts...

PAX PoS Terminal Flaw Could Allow Attackers to Tamper with Transactions...

Combating IP Leaks into AI Applications with Free Discovery and Risk Reduction Automation...

Feds Warn of AndroxGh0st Botnet Targeting AWS, Azure, and Office 365 Credentials...

Cybersecurity Resources

ThreatLocker® Redefines Incident Response with Zero Trust

Empower Your Defense with SMB Threat Insights

MSPs & MSSPs: Start Your vCISO Journey Here

Earn a Master's in Cybersecurity Risk Management

Your e-mail address

Connect with us!






Company

About THN
Advertise with us
Contact

Pages

Webinars
Deals Store
Privacy Policy

Contact Us