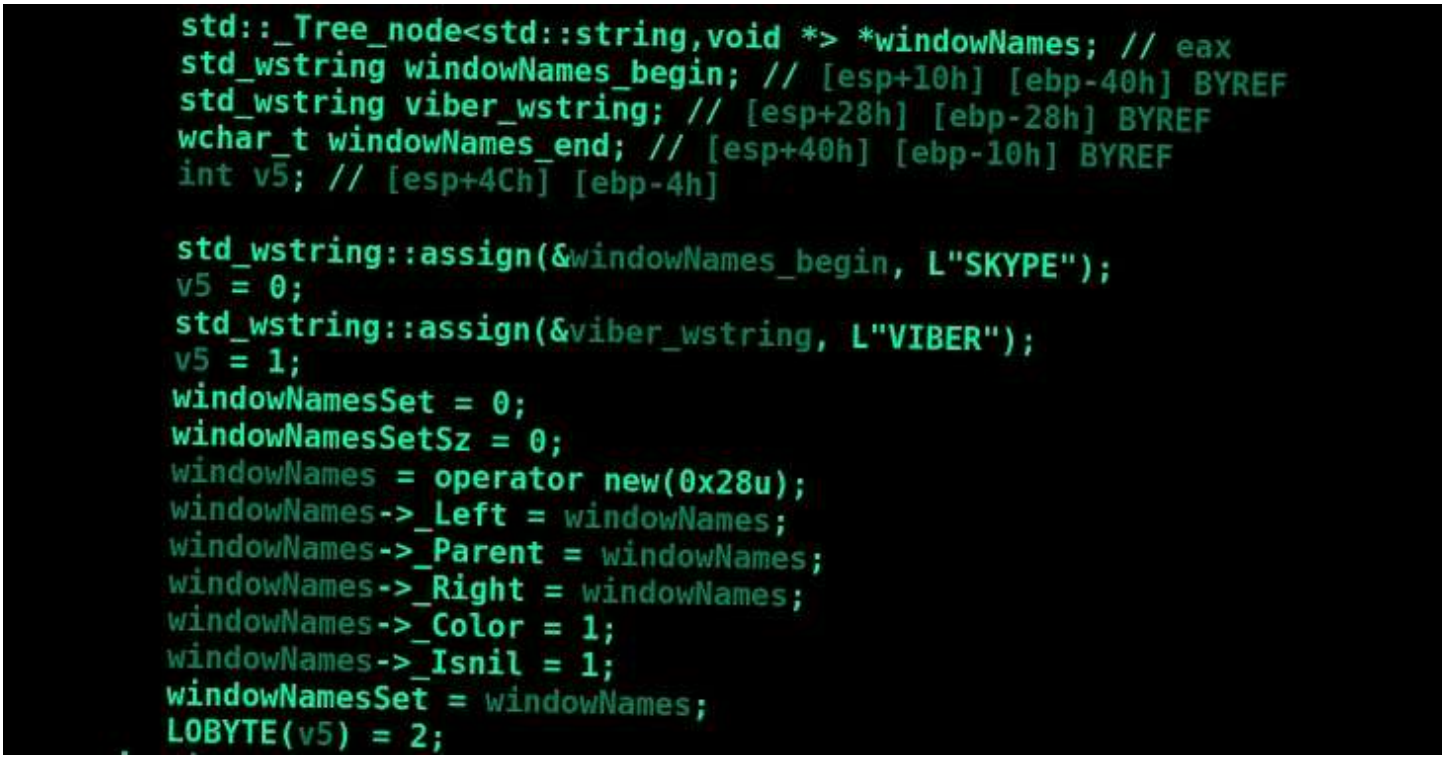
Bad Magic's Extended Reign in Cyber Espionage Goes Back Over a Decade

May 22, 2023 Ravie Lakshmanan



New findings about a hacker group linked to cyber attacks targeting companies in the Russo-Ukrainian conflict area reveal that it may have been around for much longer than previously thought.

The threat actor, tracked as **Bad Magic** (aka Red Stinger), has not only been linked to a fresh sophisticated campaign, but also to an activity cluster that first came to light in May 2016.

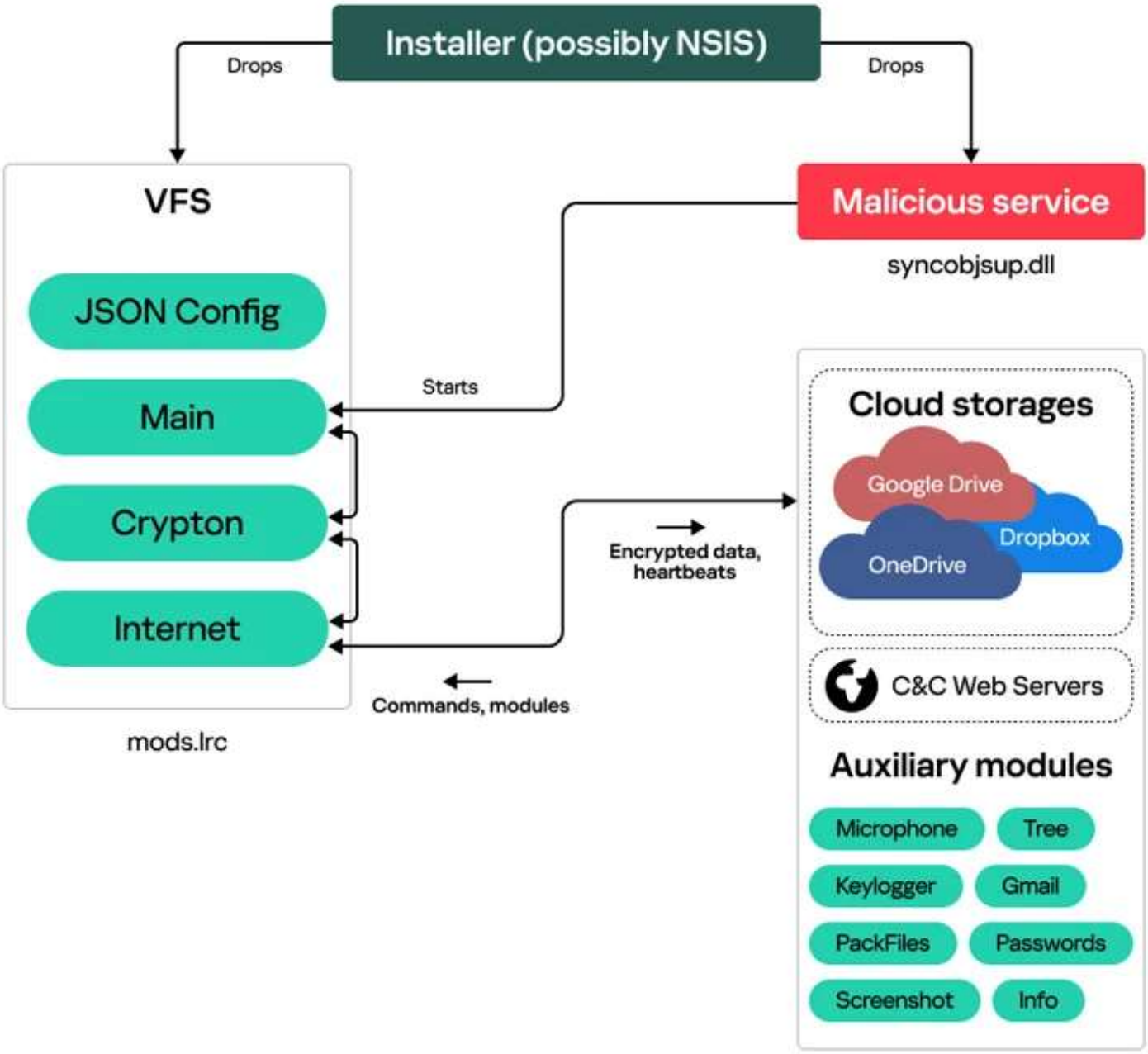
"While the previous targets were primarily located in the Donetsk, Luhansk, and Crimea regions, the scope has now widened to include individuals, diplomatic entities, and research organizations in Western and Central Ukraine," Russian cybersecurity firm Kaspersky said in a technical report published last week.

The campaign is characterized by the use of a novel modular framework codenamed CloudWizard, which features capabilities to take screenshots, record microphone, log keystrokes, grab passwords, and harvest Gmail inboxes.

Bad Magic was first documented by the company in March 2023, detailing the group's use of a backdoor called PowerMagic (aka DBoxShell or GraphShell) and a modular framework dubbed CommonMagic in attacks targeting Russian-occupied territories of Ukraine.

Then earlier this month, Malwarebytes revealed at least five waves of espionage attacks mounted by the group dating back to December 2020.

The deeper insight shared by Kaspersky connects Bad Magic to prior activity based on combing through historical telemetry data, allowing the company to identify various artifacts associated with the CloudWizard framework from 2017 to 2020.



The initial access vector used to drop the first-stage installer is currently unknown. That said, the malware is configured to drop a Windows service ("syncobjsup.dll") and a second file ("mods.lrc"), which, in turn, contains three different modules to harvest and exfiltrate sensitive data.

The information is transmitted in encrypted form to an actor-controlled cloud storage endpoint (OneDrive, Dropbox, or Google Drive). A web server is used as a fallback mechanism in the event none of the services are accessible.

Kaspersky said it identified source code overlaps between an older version of CloudWizard and another malware known as Prikormka, which was discovered by Slovak cybersecurity company ESET in 2016.

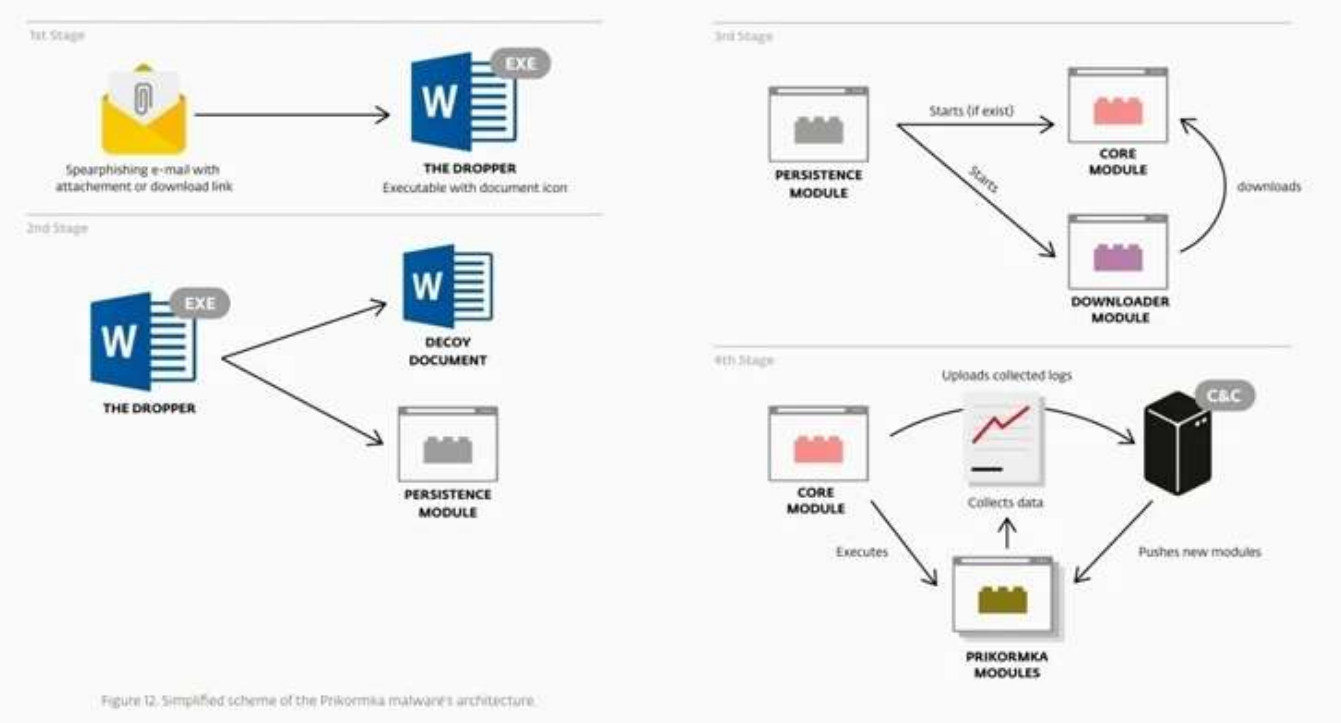


Figure 12. Simplified scheme of the Prikormka malware's architecture

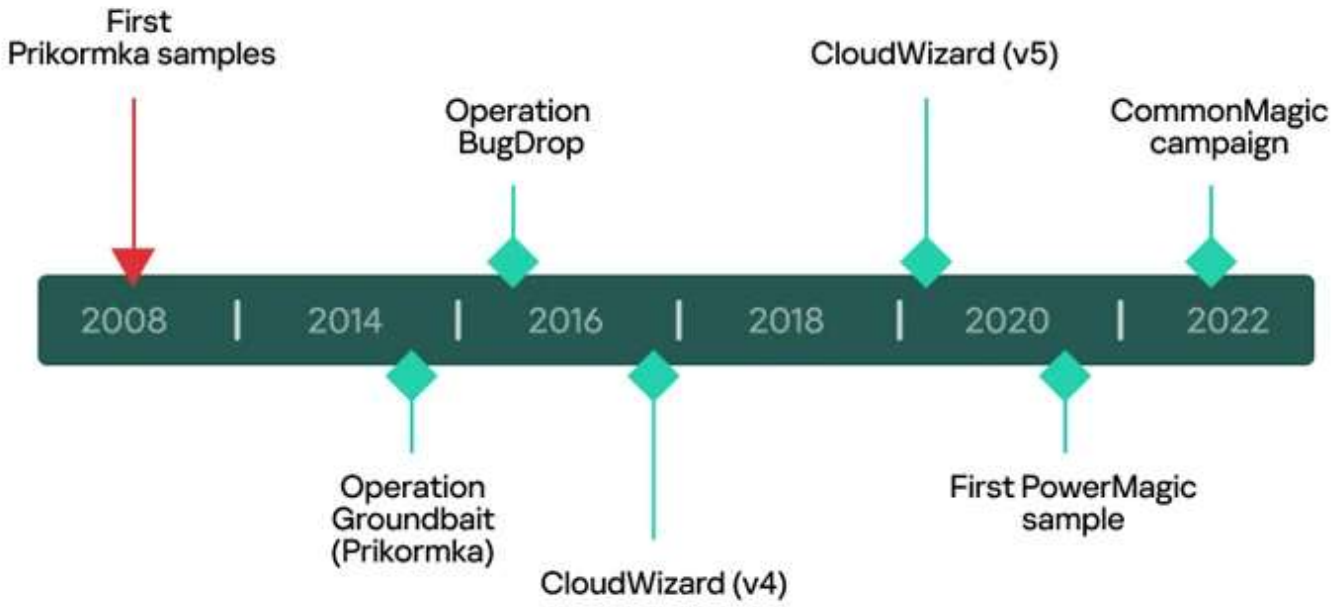
Image Source: ESET

The espionage campaign, monitored by ESET under the moniker Operation Groundbait, primarily singled out anti-government separatists in Donetsk and Luhansk and Ukrainian government officials, politicians, and journalists.

Prikormka is deployed via a dropper contained within malicious email attachments and features 13 different components to harvest various kinds of data from compromised machines. Evidence gathered by ESET shows that the malware has been selectively used since at least 2008.

CloudWizard also exhibits resemblances with a related intrusion set called BugDrop that was disclosed by CyberX (which has since been acquired by Microsoft) in 2017, with the industrial cybersecurity company describing it as more advanced than Groundbait.

Commonalities have also been unearthed between CloudWizard and CommonMagic, including identical source code and victimology patterns, indicating that the threat actor has been repeatedly tweaking its malware arsenal and infecting targets for about 15 years.



The latest development, in attributing the CloudWizard framework to the actor behind Operation Groundbait and Operation BugDrop, provides yet another piece to the puzzle that hopes to eventually reveal the bigger picture of the mysterious group's origins.

"The threat actor responsible for these operations has demonstrated a persistent and ongoing commitment to cyber espionage, continuously enhancing their toolset and targeting organizations of interest for over 15 years," Kaspersky researcher Georgy Kucherin said.

"Geopolitical factors continue to be a significant motivator for APT attacks and, given the prevailing tension in the Russo-Ukrainian conflict area, we anticipate that this actor will persist with its operations for the foreseeable future."

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...

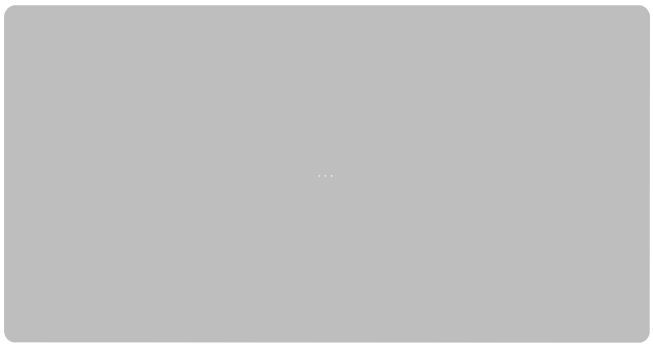
PAX PoS Terminal Flaw Could Allow Attackers to Tamper with Transactions...

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

Contact Privacy Policy

Contact Us