Ukraine Hit with Novel 'FoxBlade' Trojan Hours Before Invasion

By Lisa Vaas

Published: 2022-03-01 · Archived: 2026-04-05 17:55:02 UTC

Microsoft detected cyberattacks launched against Ukraine hours before Russia's tanks and missiles began to pummel the country last week.

"As tanks rolled into Ukraine, so did malware," summarized humanitarian author Andreas Harsono, referring to the novel malware that Microsoft has named FoxBlade.

On Monday, the company reported that its Threat Intelligence Center (MSTIC) had detected cyberattacks launched against Ukraine's digital infrastructure hours before Russia's tanks and missiles began to pummel the country on Thursday.

"Several hours before the launch of missiles or movement of tanks on February 24, Microsoft's Threat Intelligence Center (MSTIC) detected a new round of offensive and destructive cyberattacks directed against Ukraine's digital infrastructure," Microsoft President and Vice-Chair Brad Smith said.

Infosec Insiders Newsletter! Business Insights Delivered Weekly Subscribe

"We immediately advised the Ukrainian government about the situation, including our identification of the use of a new malware package (which we denominated FoxBlade), and provided technical advice on steps to prevent the malware's success."

Smith said that within three hours of discovering FoxBlade, Microsoft had added new signatures to its Defender anti-malware service to detect the exploit.

FoxBlade Specifics

Microsoft has issued a Security Intelligence advisory about FoxBlade, which is a novel trojan.

While the company shared neither technical specifics nor details about how FoxBlade achieves initial access on targeted machines, the advisory did explain that "This trojan can use your PC for distributed denial-of-service (DDoS) attacks without your knowledge."

Such attacks topped thousands daily in Q3 and were expected to keep growing, Kaspersky researchers reported in November 2021.

Beyond launching DDoS attacks, FoxBlade also downloads and installs other programs – including other malware – onto infected systems, Microsoft advised.

'Precisely Targeted'

The cyberattacks – which were ongoing as of Monday, Smith said – have been "precisely targeted," unlike the indiscriminate malware splattered in the NotPetya attack. The NotPetya cyberattack targeted hundreds of firms and hospitals worldwide in 2017, including Ukraine's power grid.

In 2020, the U.S. Department of Justice (DOJ) charged six Russian nationals for their alleged part in the Ukraine and other cyberattacks.

Regardless of the targeted nature of the current cyberattacks on Ukraine, Smith said Microsoft is still "especially concerned" about recent cyberattacks aimed at Ukrainian civilian digital targets that have been more wide-ranging, including those fired at the financial sector, agriculture sector, emergency response services, humanitarian aid efforts, and energy sector organizations and enterprises.

"These attacks on civilian targets raise serious concerns under the Geneva Convention, and we have shared information with the Ukrainian government about each of them," Smith said.

Microsoft has also advised the Ukrainian government about recent cyber efforts to steal a range of personally identifiable information (PII), including PII related to health, insurance, transportation and other government data.

Microsoft has also passed on threat intelligence and defensive strategies to Ukraine's government so that it could better defend against attacks on military institutions and manufacturers and several other Ukrainian government agencies.

"This work is ongoing," Smith said.

The Ongoing Cyberwar

Microsoft's news about FoxBlade comes as just one of a continuing barrage of cyber assaults targeting both Ukraine and Russia: a barrage that's included the Conti ransomware gang proclaiming that it's pro-Russia. Last week, it, the extortionists blared out a warning on their blog, threatening to use Conti's "full capacity" to retaliate in the face of "Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world."

A pro-Ukraine Conti ransomware gang member subsequently spilled 13 months of the ransomware group's chats, promising more still to come.

As well, ESET and Broadcom's Symantec last week said that they had discovered a new data wiper malware dubbed **HermeticWiper**, that's been used against hundreds of machines in Ukraine. One of the malware samples was compiled back on Dec. 28, pointing to the attacks having been readied two months ago.

Then, on Jan. 13, a destructive wiper malware – posing as ransomware attacks – named WhisperGate began to target Ukrainian organizations: an attack that analysts said was likely part of Russia's wider effort to undermine Ukraine's sovereignty.

As well, in mid-February, institutions central to Ukraine's military and economy – including government and banking websites – were slammed with a wave of DDoS attacks.

CISA's Take-Shelter Advice

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) last week warned that such attacks could spill over Ukraine's borders.

"Destructive malware can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data," CISA said. "Further disruptive cyberattacks against organizations in Ukraine are likely to occur and may unintentionally spill over to organizations in other countries."

Other threats related to the Ukraine/Russia crisis include the typical swarm of threat actors who jump into the fray to exploit the day's headlines, which, in this situation, convey the haze and confusion of war. Case in point: Malwarebytes has uncovered a spate of malicious email bearing the subject line "Microsoft account unusual sign-in activity."

CISA provided this list of "Immediate Shields Up Actions" to protect against this wide range of cyber threats:

- Patch vulnerabilities.
- Use MFA.
- Run antivirus.
- Enable strong spam filters to prevent phishing emails from reaching end users.
- Disable ports and protocols that are not essential.
- Strengthen controls for cloud services.

Moving to the cloud? Discover emerging cloud-security threats along with solid advice for how to defend your assets with our FREE downloadable eBook, "Cloud Security: The Forecast for 2022." We explore organizations' top risks and challenges, best practices for defense, and advice for security success in such a dynamic computing environment, including handy checklists.

Source: https://threatpost.com/microsoft-ukraine-foxblade-trojan-hours-before-russian-invasion/178702/