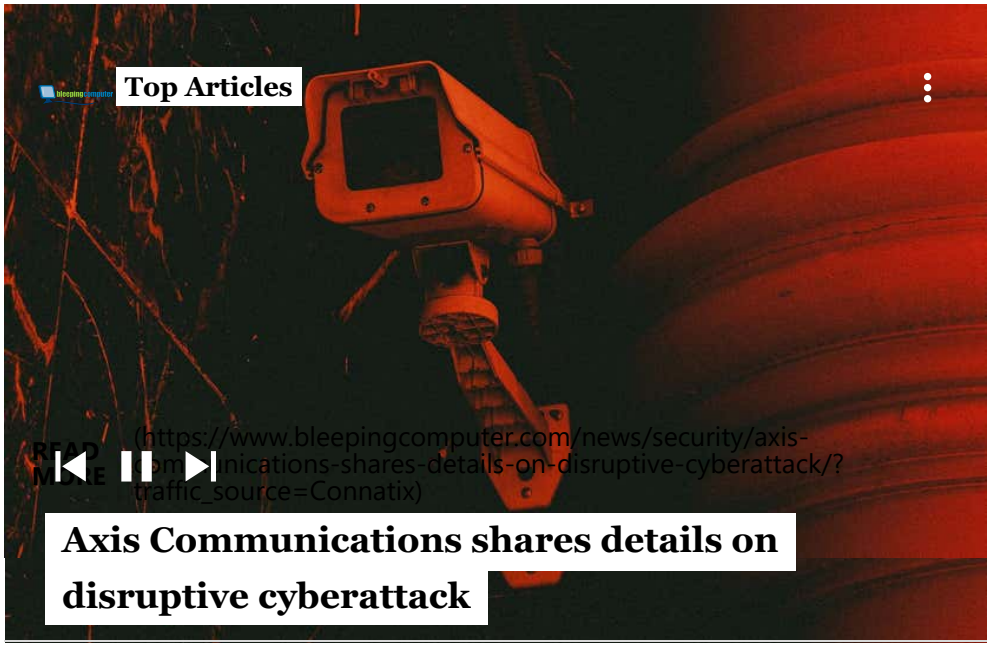
Microsoft: Ukraine hit with new FoxBlade malware hours before invasion

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** February 28, 2022 06:05 PM **0**

Microsoft said that Ukrainian networks were targeted with newly found malware several hours before Russia's invasion of Ukraine on February 24th.

Researchers with the Microsoft Threat Intelligence Center (MSTIC) observed destructive attacks targeting Ukraine and spotted a new malware strain they dubbed FoxBlade.

"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 (https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/).



"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 also said that the company updated its Defender security platform with new signatures to block the FoxBlade malware within three hours of discovering the malicious tool deployed in the wild.

Microsoft describes the malware in a Security Intelligence advisory published on February 23rd as a trojan that can use computers "for distributed denial-of-service (DDoS) attacks" without the owners' knowledge.

These recently spotted and still active cyberattacks "have been precisely targeted," Smith also revealed.

This contrasts to the indiscriminate malware assaults that impacted Ukraine's and other countries' economies during the 2017 NotPetya worldwide attack linked to a Russian GRU Main Intelligence Directorate hacking group known as Sandworm (https://www.bleepingcomputer.com/news/security/us-indicts-russian-gru-sandworm-hackers-for-notpetya-worldwide-attacks/).

Ukrainian networks attacked with destructive malware

The offensive cyberattacks detected by MSTIC researchers right before the Russian invasion followed several other series of malware attacks since the start of 2021.

Earlier this month, newly discovered HermeticWiper malware (https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/) was used to target Ukraine together with ransomware decoys (https://www.bleepingcomputer.com/news/security/ransomware-used-as-decoy-in-data-wiping-attacks-on-ukraine/) to wipe data and render devices unbootable.

In January, the country was struck by another series of malware attacks deploying the WhisperGate wiper (https://www.bleepingcomputer.com/news/security/microsoft-fake-ransomware-targets-ukraine-in-data-wiping-attacks/) disguised as a ransomware payload.

Over the weekend, CISA and the FBI warned US organizations that the data wiping attacks against Ukraine could spill over to other countries (https://www.bleepingcomputer.com/news/security/cisa-and-fbi-warn-of-potential-data-wiping-attacks-spillover/), urging US orgs to "increase vigilance" and reinforce their defenses.

The same day, Ukraine's Vice Prime Minister Mykhailo Fedorov also revealed the creation of an "IT army" (https://www.bleepingcomputer.com/news/security/ukraine-recruits-it-army-to-hack-russian-entities-lists-31-targets/) to help the country "fight on the cyber front."

Right before the war started, the Ukrainian Security Service (SSU) reported that Ukraine was being targeted by a "massive wave of hybrid warfare (https://www.bleepingcomputer.com/news/security/ukraine-says-it-s-targeted-by-massive-wave-of-hybrid-warfare-/)."