Malware attacks targeting Ukraine government

blogs.microsoft.com/on-the-issues/2022/01/15/mstic-malware-cyberattacks-ukraine-government/

January 16, 2022

Today, we're sharing that we've observed destructive malware in systems belonging to several Ukrainian government agencies and organizations that work closely with the Ukrainian government. The malware is disguised as ransomware but, if activated by the attacker, would render the infected computer system inoperable. We're sharing this information to help others in the cybersecurity community look out for and defend against these attacks.

At this time, we have not identified notable overlap between the unique characteristics of the group behind these attacks and groups we've traditionally tracked but we continue to analyze the activity.

The organizations affected by this malware include government agencies that provide critical executive branch or emergency response functions and an IT firm that manages websites for public and private sector clients, including government agencies whose websites were recently defaced.

The Microsoft Threat Intelligence Center (MSTIC) has published a technical blog post detailing Microsoft's ongoing investigation and how the security community can detect and defend against this malware. We have also notified each of the impacted organizations we have identified so far, partnered with other cybersecurity providers to share what we know, and notified appropriate government agencies in the United States and elsewhere. It is possible more organizations have been infected with this malware and the number of impacted organizations could grow. We will continue to work with the cybersecurity community to identify and assist targets and victims.

We first detected this malware on January 13 2022. We have already built and deployed protections for this malware into Microsoft 365 Defender Endpoint Detection (EDR) and Anti-virus (AV) protections wherever these products are deployed, both on-premises and in the cloud. We see no indication so far that these attacks utilize any vulnerability in Microsoft products and services.

Tags: cyberattacks, cybercrime, cybersecurity, malware, Microsoft Threat Intelligence Center, MSTIC