EMPM686-0201

Samridha Murali

02/28/20222

<center>Current Event 5</center>

On February 23, 2022 Ukrainian government websites were hit by a massive Distributed Denial of Service attack. Websites for the Ukrainian Ministry of Foreign affairs, Cabinet of Ministers and Rada, the country's parliament were down on Wednesday. On February 24 2022, some major organizations faced a ransomware attack. The diabolical hacker organization behind this attack, deployed this ransomware attack as distraction from a dangerous wiper attack. This new form of disk-wiping malware attack has been launched to attack organizations in Ukraine. Organizations in the financial, defence, aviation and IT services sector were targeted. The attackers appear to have used a known vulnerability in Microsoft SQL server. Shortly after this Russia invaded Ukraine.

The impact of Denial of Service attack is not released yet, but Ukrainians' cell phones were flooded with text messages that ATMs no longer worked in the country (but whether bank accounts were affected is not known still). The exact number of computers affected by the wiper attack is not known still, but more than hundreds of computers are affected. When the wiper malware is executed, it will damage the Master Boot Record (MBR) of the infected computer, making it inoperable. It is still not found if it has any additional functionality other than wiping.

Government should have an army of specialized cyber security experts to handle cyber warfare. Organizations must review their security policies and operations during war and tighten their security protocols. Organizations can block traffic based on IP location. Given this situation where organizations are planned and targeted, to prevent any disastrous outcome important assets could be kept offline or at least kept internal only to a particular region.

References :

1. Threat Hunter team (2022, Feb 24) https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia
2. Lauren Feiner (2022, Feb 23) https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html