Experts Fear Global Impact From Russia's Cyberattacks on Ukraine

HARRAH & ASSOCIATES, INC.

Russia launched a full-scale military assault on Ukraine in the early morning hours of Feb. 24, 2022, accompanied by a series of targeted cyberattacks that experts and officials say could ultimately have a much broader impact.

In the weeks leading up to the invasion, Ukrainian government entities, financial institutions and other key organizations faced website defacements, distributed denial-of-service (DDoS) attacks and destructive malware. Cybersecurity experts around the globe have kept tabs on these cyber events, warning clients and organizations to secure their systems without delay.

On Feb. 23, 2022, researchers at Symantec and ESET first tweeted the discovery of new wiper malware, dubbed "HermeticWiper," that was used against Ukraine. Symantec researchers observed the use of this malware against an organization in Lithuania as early as Nov. 12, 2021. They noted that, with an invasion underway, there remains a high likelihood of further cyberattacks against Ukraine and other countries in the region.

Offering a technical breakdown of the malware, cybersecurity firm SentinelOne commented, "After a week of defacements and increasing DDoS attacks, the proliferation of sabotage operations through wiper malware is an expected and regrettable escalation."

In a recent webcast, experts from Secureworks said they had long expected that any invasion would have a cyber component.

The wiper attacks make no pretense of being ransomware events and aim to destroy data with little hope of recovery. These attacks could contain an element of espionage as well, according to Mike McLellan, director of intelligence at Secureworks.

While the cyberattacks currently appear to be focused on Ukraine, the United States and its allies should be prepared for retaliatory attacks over severe economic sanctions announced by President Joe Biden following the invasion.

In an Axios interview, Sen. Mark Warner (D-VA) said that Russian cyberattacks could trigger expanded conflict with NATO countries.

"If you unleash not one, but five, 10, 50 or 1,000 [cyberattacks] at Ukraine, the chances of them staying within the Ukrainian geographic border are quite small," Warner said. "They could spread to America or the [United Kingdom]. But the more likely effect will be [the attacks] spreading to adjacent geographic territory … [like] Poland."

On Twitter, Warner added, "This is not something to take lightly—cyberattacks don't have borders."

U.S. House Intelligence Chair Rep. Adam Schiff (D-CA) expressed similar concerns in a news briefing.

"We have seen in the past Russia deploy attacks at a particular target—those tools get into the wild, and they cause global damage," Schiff said.

According to McLellan, attacks targeting the United States would require a significant escalation between the West and Russia. However, threat actors unrelated to the situation in Ukraine could take advantage of the unfolding conflict to infiltrate systems.

Jen Easterly, head of the U.S. Cybersecurity and Infrastructure Security Agency (CISA), said on Twitter, "While there are no specific threats to the [United States] at this time, all organizations must be prepared for cyberattacks, whether targeted or not." She cited the 2017 NotPetya attack that brought commerce to a halt and caused billions in damage for corporations around the world.

To help prepare organizations of all sizes, CISA launched Shields Up, a program with guidance for preventing, detecting and minimizing the impact of cyber events.

Cybersecurity firms working closely with the insurance industry advise businesses to protect themselves by reviewing their business continuity plans and ensuring cybersecurity fundamentals are in place. This can include up-to-date patching programs, endpoint threat detection, antivirus programs and multifactor authentication.