Russia began preparing for cyberattacks on Ukraine in early 2021

Russian-affiliated hackers were positioning themselves for cyberattacks against Ukraine as early as March 2021, according to researchers at Microsoft Corp.

A handful of hacking groups secured access to Ukrainian organizations — including defense, IT and energy networks — for strategic and battlefield intelligence collection, the technology giant revealed in a report published on Wednesday. The campaigns appeared to be setting the groundwork for attacks before and after the invasion began in February.

These previously unreported reconnaissance operations preceded what has become an aggressive and damaging campaign against Ukraine, which has been hit with more than 237 cyberattacks by at least six Russian-affiliated hacking groups since the invasion began, Tom Burt, Microsoft's vice president for customer security and trust, said in a blog post that accompanied the report.

In addition, Microsoft researchers identified nearly 40 destructive attacks that permanently destroyed files in dozens of organizations across Ukraine. More than 40% of those attacks were aimed at organizations that provide critical infrastructure, according to the report.

While Russia's invasion has been viewed as poorly planned and executed, Microsoft researchers describe a cyber campaign that often coincided with military plans. The report also provides a detailed account of Russia's cyber operations, which some experts have said played a smaller role in the conflict than anticipated.

"Russia's use of cyberattacks appears to be strongly correlated and sometimes directly timed with its kinetic military operations," Burt wrote in a blog post. "For example, a Russian actor launched cyberattacks against a major broadcasting company on March 1, the same day the Russian military announced its intention to destroy Ukrainian 'disinformation' targets and directed a missile strike against a TV tower in Kyiv."

A representative for the Russian embassy in Washington didn't respond to a request for comment.

The state-sponsored hacking groups embedded themselves in the technological scaffolding that keep some of Ukraine's critical infrastructure online, according to Microsoft. They also conducted phishing attacks on the Ukrainian military to collect intelligence which could later be used by the Russian army, the report found.

Microsoft said the cyber operation expanded to a large phishing campaign, by a hacking group it calls Nobelium, against those rallying international support for Ukraine. In early 2021, Nobelium attempted to access IT companies serving governments in NATO member states, including the U.S and Europe. It successfully stole data from Western foreign policy organizations to gauge how NATO would respond to Russian military actions.

Microsoft, which has been working with Ukrainian authorities to help thwart cyberattacks, didn't identify the targeted countries. Nobelium, also known as APT 29 and Cozy Bear and believed to be affiliated with Russian intelligence, has also been accused of the supply chain attack involving SolarWinds Corp., which was made public in December 2020, and the breach of the Democratic National Committee prior to the 2016 U.S. presidential election.

Later in 2021, suspected Russian hackers embedded themselves in the networks of IT and energy providers which would later become targets of destructive attacks. This included the company Kitsoft, an IT service provider for Ukrainian government departments, the websites of which were defaced with threatening text warning Ukrainians to "be afraid and wait for the worst" and claiming their personal data had been stolen.

A representative for Kitsoft couldn't be located for comment.

By 2022, when diplomacy between the two countries had turned sour, hacking groups linked to Russian intelligence appeared to begin exploiting the access to these networks, and began sending malicious "wiper" software, named for its damaging nature, to Ukrainian organizations, according to Microsoft.

Burt warned that cyberattacks in Ukraine would probably increase and that Russian-aligned hacking groups may target NATO members, and he advised

organizations to take alerts published by U.S government agencies seriously.

“Given Russian threat actors have been mirroring and augmenting military actions, we believe cyberattacks will continue to escalate as the conflict rages,” he said.

Source:
https://www.stripes.com/theaters/europe/2022-04-27/russia-cyberattacks-against-ukraine-early-2021-5819876.html

[Disclaimer]