Disrupting cyberattacks targeting Ukraine

blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/

April 7, 2022

Today, we're sharing more about cyberattacks we've seen from a Russian nation-state actor targeting Ukraine and steps we've taken to disrupt it.

We recently observed attacks targeting Ukrainian entities from Strontium, a Russian GRU-connected actor we have tracked for years. This week, we were able to disrupt some of Strontium's attacks on targets in Ukraine. On Wednesday April 6th, we obtained a court order authorizing us to take control of seven internet domains Strontium was using to conduct these attacks. We have since re-directed these domains to a sinkhole controlled by Microsoft, enabling us to mitigate Strontium's current use of these domains and enable victim notifications.

Strontium was using this infrastructure to target Ukrainian institutions including media organizations. It was also targeting government institutions and think tanks in the United States and the European Union involved in foreign policy. We believe Strontium was attempting to establish long-term access to the systems of its targets, provide tactical support for the physical invasion and exfiltrate sensitive information. We have notified Ukraine's government about the activity we detected and the action we've taken.

This disruption is part of an ongoing long-term investment, started in 2016, to take legal and technical action to seize infrastructure being used by Strontium. We have established a legal process that enables us to obtain rapid court decisions for this work. Prior to this week, we had taken action through this process 15 times to seize control of more than 100 Strontium controlled domains.

The Strontium attacks are just a small part of the activity we have seen in Ukraine. Before the Russian invasion, our teams began working around the clock to help organizations in Ukraine, including government agencies, defend against an onslaught of cyberwarfare that has escalated since the invasion began and has continued relentlessly. Since then, we have observed nearly all of Russia's nation-state actors engaged in the ongoing full-scale offensive against Ukraine's government and critical infrastructure, and we continue to work closely with government and organizations of all kinds in Ukraine to help them defend against this onslaught. In the coming weeks we expect to provide a more comprehensive look at the scope of the cyberwar in Ukraine.

Tags: cyberattacks, cybersecurity, cyberwar, Russia, strontium, Ukraine