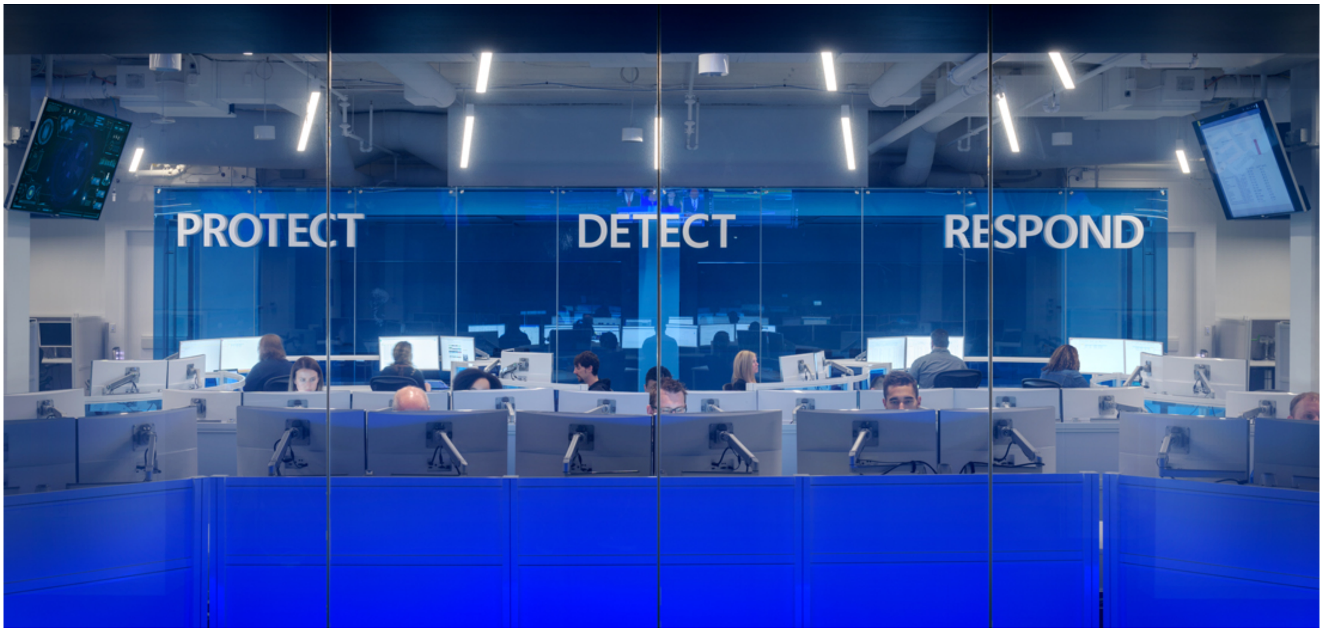
# Protecting people from recent cyberattacks

blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/

December 6, 2021



The Microsoft Digital Crimes Unit (DCU) has disrupted the activities of a China-based hacking group that we call Nickel. In documents that were unsealed today, a federal court in Virginia has granted our request to seize websites Nickel was using to attack organizations in the United States and 28 other countries around the world, enabling us to cut off Nickel's access to its victims and prevent the websites from being used to execute attacks. We believe these attacks were largely being used for intelligence gathering from government agencies, think tanks and human rights organizations.

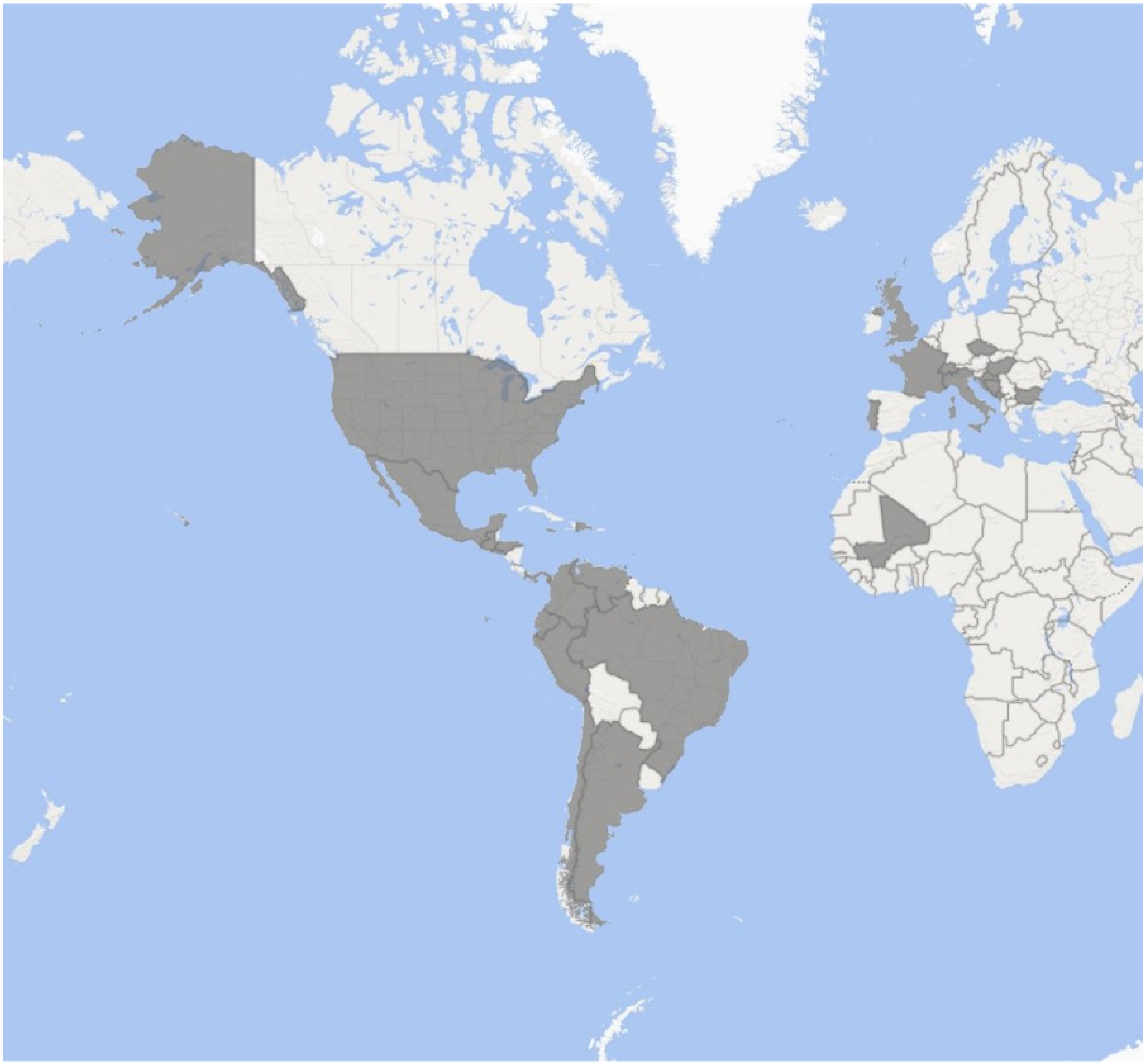
On December 2, Microsoft filed pleadings with the U.S. District Court for the Eastern District of Virginia seeking authority to take control of the sites. The court quickly granted an order that was unsealed today following completion of service on the hosting providers. Obtaining control of the malicious websites and redirecting traffic from those sites to Microsoft's secure servers will help us protect existing and future victims while learning more about Nickel's activities. Our disruption will not prevent Nickel from continuing other hacking activities, but we do believe we have removed a key piece of the infrastructure the group has been relying on for this latest wave of attacks.

Microsoft's DCU has been a pioneer in using this legal strategy against cybercriminals and, more recently, against nation-state hackers. To date, in 24 lawsuits – five against nation-state actors – we've taken down more than 10,000 malicious websites used by cybercriminals and nearly 600 sites used by nation-state actors. We have also successfully blocked the registration of 600,000 sites to get ahead of criminal actors that planned to use them maliciously in the future.

The Microsoft Threat Intelligence Center (MSTIC) has been tracking Nickel since 2016 and analyzing this specific activity since 2019. As with any observed nation-state actor activity, Microsoft continues to notify customers that have been targeted or compromised, when possible, providing them with the information they need to help secure their accounts. The attacks MSTIC observed are highly sophisticated and used a variety of techniques but nearly always had one goal: to insert hard-to-detect malware that facilitates intrusion, surveillance and data theft. Sometimes, Nickel's attacks used compromised third-party virtual private network (VPN) suppliers or stolen credentials obtained from spear phishing campaigns. In some observed activity, Nickel malware used exploits targeting unpatched on-premises Exchange Server and SharePoint systems. However, we have not observed any new vulnerabilities in Microsoft products as part of these attacks. Microsoft has created unique signatures to detect and protect from known Nickel activity through our security products, like Microsoft 365 Defender.

Nickel has targeted organizations in both the private and public sectors, including diplomatic organizations and ministries of foreign affairs in North America, Central America, South America, the Caribbean, Europe and Africa. There is often a correlation between Nickel's targets and China's geopolitical interests. Others in the security community who have researched this group of actors refer to the group by other names, including "KE3CHANG," "APT15," "Vixen Panda," "Royal APT" and "Playful Dragon."

In addition to the U.S., the countries in which Nickel has been active include: Argentina, Barbados, Bosnia and Herzegovina, Brazil, Bulgaria, Chile, Colombia, Croatia, Czech Republic, Dominican Republic, Ecuador, El Salvador, France, Guatemala, Honduras, Hungary, Italy, Jamaica, Mali, Mexico, Montenegro, Panama, Peru, Portugal, Switzerland, Trinidad and Tobago, the United Kingdom and Venezuela.



Nation-state attacks continue to proliferate in number and sophistication. Our goal in this case, as in our previous disruptions that targeted Barium, operating from China, Strontium, operating from Russia, Phosphorus, operating from Iran, and Thallium, operating from North Korea, is to take down malicious infrastructure, better understand actor tactics, protect our customers and inform the broader debate on acceptable norms in cyberspace. We will remain relentless in our efforts to improve the security of the ecosystem and we will continue to share activity we see, regardless of where it originates.

No individual action from Microsoft or anyone else in the industry will stem the tide of attacks we've seen from nation-states and cybercriminals working within their borders. We need industry, governments, civil society and others to come together and establish a new consensus for what is and isn't appropriate behavior in cyberspace. We're encouraged by recent progress. Last month, the United States and the European Union joined the Paris Call for Trust and Security in Cyberspace, the world's largest multistakeholder confirmation of core cybersecurity principles with more than 1,200 endorsers. The Oxford Process has brought together some of the best legal minds to evaluate the application of international law to cyberspace. And the United Nations has taken critical steps to advance dialogue across stakeholders. It is our responsibility, and that of every entity with the relevant expertise and resources, to do whatever we can to help bolster trust in technology and protect the digital ecosystem.

Tags: cyberattacks, cyberfraud, cybersecurity, Digital Crimes Unit, MSTIC, Paris Call for Trust and Security in Cyberspace