Microsoft

Another Nobelium Cyberattack

May 27, 2021

UPDATE (*May 28, 2021, 1pm PT*): Our teams have continued to investigate the latest wave of phishing attacks launched by Nobelium. Based on what we currently know, the security community should feel good about the collective work done to limit the damage done by this wave of attacks. As we have notified our targeted customers and watched closely for other reports, we are not seeing evidence of any significant number of compromised organizations at this time. More importantly, antivirus services, like Microsoft Defender Antivirus, and endpoint detection and response products, such as Microsoft Defender for Endpoint, are identifying and protecting against the malware being used in this wave of attacks and are working in combination with Microsoft Defender for Office 365. It is important for all users to employ basic cybersecurity hygiene, including using multi-factor authentication, using antivirus/antimalware software and being careful not to click on links in email, unless you can confirm reliability to minimize the risk of being phished. We will continue to monitor the situation.

This week we observed cyberattacks by the threat actor Nobelium targeting government agencies, think tanks, consultants, and non-governmental organizations. This wave of

attacks targeted approximately 3,000 email accounts at more than 150 different organizations. While organizations in the United States received the largest share of attacks, targeted victims span at least 24 countries. At least a quarter of the targeted organizations were involved in international development, humanitarian, and human rights work. Nobelium, originating from Russia, is the same actor behind the attacks on SolarWinds customers in 2020. These attacks appear to be a continuation of multiple efforts by Nobelium to target government agencies involved in foreign policy as part of intelligence gathering efforts.

Nobelium launched this week's attacks by gaining access to the Constant Contact account of USAID. Constant Contact is a service used for email marketing. From there, the actor was able to distribute phishing emails that looked authentic but included a link that, when clicked, inserted a malicious file used to distribute a backdoor we call NativeZone. This backdoor could enable a wide range of activities from stealing data to infecting other computers on a network. You can read more about the technical aspects of these attacks in this blog post from the Microsoft Threat Intelligence Center (MSTIC).

Many of the attacks targeting our customers were blocked automatically, and Windows Defender is blocking the malware involved in this attack. We're also in the process of notifying all of our customers who have been targeted. We detected this attack and identified victims through the ongoing work of the MSTIC team in tracking nation-state actors. We have no reason to believe these attacks involve any exploit against or vulnerability in Microsoft's products or services.

These attacks are notable for three reasons.

First, when coupled with the attack on SolarWinds, it's clear that part of Nobelium's playbook is to gain access to trusted technology providers and infect their customers. By piggybacking on software updates and now mass email providers, Nobelium increases the chances of collateral damage in espionage operations and undermines trust in the technology ecosystem.

Second, perhaps unsurprisingly, Nobelium's activities and that of similar actors tend to track with issues of concern to the country from which they are operating. This time Nobelium targeted many humanitarian and human rights organizations. At the height of the Covid-19 pandemic, Russian actor Strontium targeted healthcare organizations involved in vaccines. In 2019, Strontium targeted sporting and anti-doping organizations. And we've previously disclosed activity by Strontium and other actors targeting major elections in the U.S. and elsewhere. This is yet another example of how cyberattacks have become the tool of choice for a growing number of nation-states to accomplish a wide variety of political objectives, with the focus of these attacks by Nobelium on human rights and humanitarian organizations.

Third, nation-state cyberattacks aren't slowing. We need clear rules governing nation-state conduct in cyberspace and clear expectations of the consequences for violation of those rules. We must continue to rally around progress made by the Paris Call for Trust and Security in Cyberspace, and more widely adopt the recommendations of the Cybersecurity Tech Accord, and the CyberPeace Institute. But, we need to do more. Microsoft will continue to work with willing governments and the private sector to advance the cause of digital peace.

Tags: cyberattacks, CyberPeace Institute, cybersecurity, MSTIC, Nobelium