# New activity from Russian actor Nobelium

blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/

October 25, 2021


Today, we're sharing the latest activity we've observed from the Russian nation-state actor Nobelium. This is the same actor behind the cyberattacks targeting SolarWinds customers in 2020 and which the U.S. government and others have identified as being part of Russia's foreign intelligence service known as the SVR.

Nobelium has been attempting to replicate the approach it has used in past attacks by targeting organizations integral to the global IT supply chain. This time, it is attacking a different part of the supply chain: resellers and other technology service providers that customize, deploy and manage cloud services and other technologies on behalf of their customers. We believe Nobelium ultimately hopes to piggyback on any direct access that resellers may have to their customers' IT systems and more easily impersonate an organization's trusted technology partner to gain access to their downstream customers. We began observing this latest campaign in May 2021 and have been notifying impacted partners and customers while also developing new technical assistance and guidance for the reseller community. Since May, we have notified more than 140 resellers and technology service providers that have been targeted by Nobelium. We continue to investigate, but to date we believe as many as 14 of these resellers and service providers have been

compromised. Fortunately, we have discovered this campaign during its early stages, and we are sharing these developments to help cloud service resellers, technology providers, and their customers take timely steps to help ensure Nobelium is not more successful.

These attacks have been a part of a larger wave of Nobelium activities this summer. In fact, between July 1 and October 19 this year, we informed 609 customers that they had been attacked 22,868 times by Nobelium, with a success rate in the low single digits. By comparison, prior to July 1, 2021, we had notified customers about attacks from all nation-state actors 20,500 times over the past three years.

This recent activity is another indicator that Russia is trying to gain long-term, systematic access to a variety of points in the technology supply chain and establish a mechanism for surveilling – now or in the future – targets of interest to the Russian government. While we are sharing details here about the most recent activity by Nobelium, the Microsoft Digital Defense Report, published earlier this month, highlights continued attacks from other nation-state actors and cybercriminals. In line with these attacks, we are notifying our customers when they are targeted or compromised by those actors.

The attacks we've observed in the recent campaign against resellers and service providers have not attempted to exploit any flaw or vulnerability in software but rather used well-known techniques, like password spray and phishing, to steal legitimate credentials and gain privileged access. We have learned enough about these new attacks, which began as early as May this year, that we can now provide actionable information which can be used to defend against this new approach.

We've also been coordinating with others in the security community to improve our knowledge of, and protections against, Nobelium's activity, and we've been working closely with government agencies in the U.S. and Europe. While we are clear-eyed that nation-states, including Russia, will not stop attacks like these overnight, we believe steps like the cybersecurity executive order in the U.S., and the greater coordination and information sharing we've seen between industry and government in the past two years, have put us all in a much better position to defend against them.

We have long maintained and evolved the security requirements and policies we enforce with service providers that sell or support Microsoft technology. For example, in September 2020, we updated contracts with our resellers to expand Microsoft's abilities and rights to address reseller security incidents and to require that resellers implement specific security protections for their environments, such as restricting Partner Portal access and requiring that resellers enable multi-factor authentication (MFA) in accessing our cloud portals and underlying services, and we will take the necessary and appropriate steps to enforce these security commitments. We continue to assess and identify new opportunities to drive greater security throughout the partner ecosystem, recognizing the need for continuous

improvement. As a result of what we have learned over the past several months, we are working to implement improvements that will help better secure and protect the ecosystem, especially for the technology partners in our supply chain:

- As noted above, in September 2020, we rolled out MFA to access Partner Center and to use delegated administrative privilege (DAP) to manage a customer environment
- On October 15, we launched a program to provide two years of an Azure Active Directory Premium plan for free that provides extended access to additional premium features to strengthen security controls
- Microsoft threat protection and security operations tools such as Microsoft Cloud App Security (MCAS), M365 Defender, Azure Defender and Azure Sentinel have added detections to help organizations identify and respond to these attacks
- We are currently piloting new and more granular features for organizations that want to provide privileged access to resellers
- We are piloting improved monitoring to empower partners and customers to manage and audit their delegated privileged accounts and remove unnecessary authority
- We are auditing unused privileged accounts and working with partners to assess and remove unnecessary privilege and access

Today, we are also releasing technical guidance that can help organizations protect themselves against the latest Nobelium activity we've observed as the actor has honed its techniques as well as guidance for partners.

These are just the immediate steps that we've taken and, in the coming months, we will be engaging closely with all of our technology partners to further improve security. We will make it easier for service providers of all sizes to access our most advanced services for managing secure log-in, identity and access management solutions for free or at a low cost.

As we said in May, progress must continue. At Microsoft, we will continue our efforts across all these issues and will continue to work across the private sector, with the U.S. administration and with all other interested governments to make this progress.

Tags: cybersecurity, Microsoft Digital Defense Report, Nobelium