2-The Official Microsoft Blog-Defend and deter

Defend and deter

May 30, 2021 | Tom Burt - Corporate Vice President, Customer Security & Trust

Last week, Microsoft announced that Nobelium, a skilled hacking group associated with the Russian SVR and behind the SolarWinds attack last year, was engaged in phishing attacks targeting thousands of accounts at hundreds of government and human rights agencies. Today, we're providing an update on our continued investigation into these attacks and sharing some important context as we've all had a chance to learn more.

As we have notified our targeted customers and watched closely for other reports, we are still not seeing evidence of any significant number of compromised organizations at this time. 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. We will continue to monitor the situation, but so far this is good news. *[Reinforce]*

We should also start to put last week's wave of attacks into context. Why was it important to disclose these attacks? What is the significance of these attacks? And what do we think should be done?

At Microsoft, we receive more than eight trillion signals every day from our network. Our expert cybersleuths use advanced technology and deep experience to comb this data for signs of attacks so that we can notify and protect our customers. We also share information about attacks we discover with the public so that others in government and the private sector can take steps to defend against adversaries and so that policymakers can be well informed. *[Rebuild, Reinforce]*

Last week’s phishing attacks were important to disclose because they were evidence of a new campaign by a sophisticated adversary. We saw and shared publicly Nobelium’s extensive experimentation in the early stages of its campaign *[Rebuild]* – experiments consistent with Nobelium’s established practice to avoid detection and remain persistent in victim networks. We wanted the defender community in government and in the private sector to have this technical information as soon as possible. Our disclosure has already yielded benefits as CISA, the U.S. agency most responsible for our civil cyberdefense, used our information to identify and help protect more potential victims. *[Rebuild]*

But not every attack is the same, and so not every attack requires the same response. Last week’s phishing attacks were a far cry from the ransomware attacks that, in recent years, have shut down local government agencies across the U.S., interrupted health care and, most recently, stopped the flow of oil in the Colonial Pipeline.

So how, then, should government respond to last week’s attacks? Some argue that governments have engaged in espionage against one another for millennia and will continue to do so in the internet age. They say that last week’s phishing attacks were “espionage as usual” and therefore do not necessitate any significant governmental response. Let’s examine this statement, with which we largely agree, by comparing this past week’s phishing to Nobelium’s SolarWinds attacks last year.

The SolarWinds attacks were also called “espionage as usual” by some. We disagree. The SolarWinds attacks can be distinguished from expected espionage in two important ways. First, the attack corrupted and used the SolarWinds software update process. Online updates are how all vendors keep their customers secure and must be trusted. Using updates for malign purposes destroys that trust and risks the security of the entire digital ecosystem. In addition, the SolarWinds attacks were indiscriminate. Although malware that opened backdoors for the attacker was installed in more than 18,000 networks, the U.S. government has found only about 100 victims that had those backdoors actually used for espionage purposes. This overbroad and indiscriminate attack caused business disruption and imposed significant expense on 18,000 organizations and enterprises needlessly. This is not “espionage as usual.” Last week’s phishing attacks, in contrast, were focused on espionage targets and did not corrupt a core process essential to the security of the digital ecosystem. And, due in part to being caught early and good defensive technology, last week’s attacks were mostly unsuccessful. *[Reinforce]*

More impactful nation-state attacks continue to occur, however. With SolarWinds, the Exchange Server attacks from early this year and now this phishing attack, it is clear we must accelerate the work underway by the private sector and government to address our collective cybersecurity. *[Rebuild]*

First, we must work to better defend. The best defense is to move to the cloud, where the most secure technology from any cloud provider is always up to date, and where the fastest security innovations are occurring *[Rebuild]*. All users should also employ two-factor authentication and other basic cybersecurity hygiene. *[Rebuild]* The Biden Administration has taken an important step forward toward advancing our defense in issuing the recent Cybersecurity Executive Order. That EO, which will require strong collaboration between the public and private sectors to fully implement, will significantly improve the security of government agencies and the technology ecosystem broadly *[Rebuild]*. The EO is a reflection of this Administration’s unprecedented commitment to cybersecurity. During the Hafnium/Exchange Server attacks earlier this year, the White House also led the formation of both an informal task force and a formal Unified Coordination Group that included, for the first time, the private sector together with government agencies, creating coordinated efforts that resulted in only minor impacts from those attacks. We need to continue to work collectively to improve our defense.

[Reinforce]

Second, we must work to deter damaging attacks *[Rebuild]*. Again, this Administration has already taken important steps. It attributed SolarWinds to the Russian SVR intelligence agency more rapidly than the U.S. has ever previously publicly attributed a cyberattack to a foreign nation. It also imposed sanctions for that and other actions – a step essential to deterrence. Yes, more will need to be done. Clearer rules for nation-state conduct need to be defined and agreed to by the international community, and clear and expected sanctions should be communicated for violation of those rules. For example, what exactly is the "espionage as usual" that should be tolerated, and when is this line crossed? Progress is being made through the Paris Call for Trust and Security in Cyberspace, established in 2018, *[Reinforce]* which we hope the U.S. will now join. Recent United Nations processes are also resulting in consensus reports that will further the international effort to define these rules, *[Reinforce]* and the Oxford Process has convened the world's leading international law experts to define how international law applies to cyberspace. These are all encouraging steps. *[Rebuild, Reinforce]*

Progress must continue. At Microsoft we will continue our efforts across all these issues and will continue to work across the private sector *[Rebuild]*, with the Administration and with all other interested governments to make this progress. Achieving stability will take time and work, but it will be time well spent.