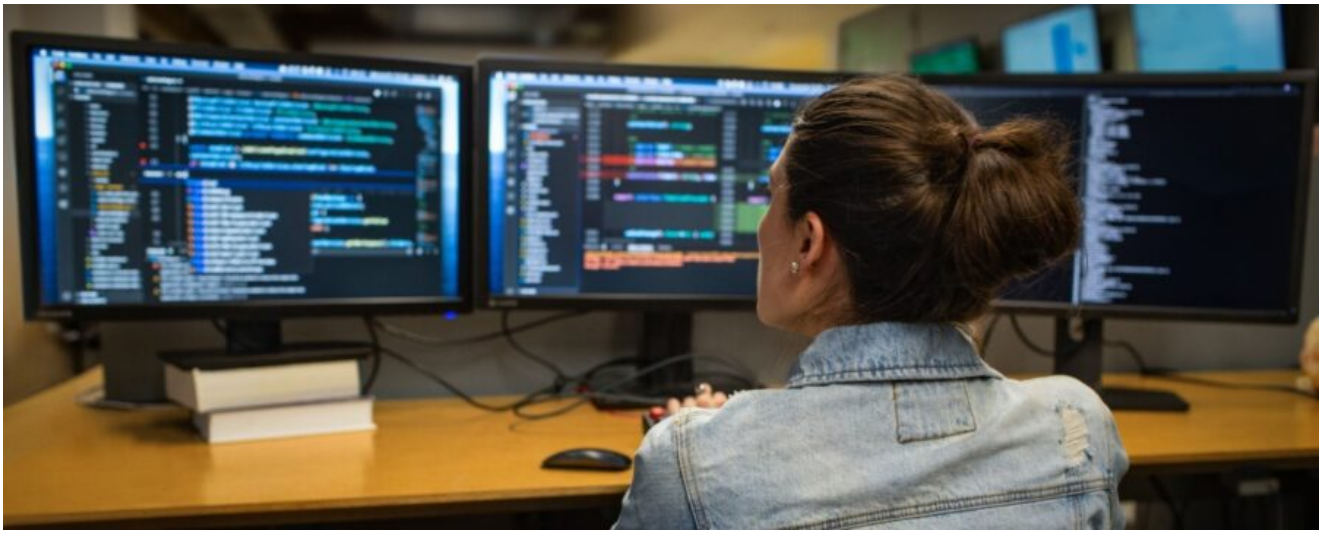
The hunt for NOBELIUM, the most sophisticated nation-state attack in history

microsoft.com/security/blog/2021/11/10/the-hunt-for-nobelium-the-most-sophisticated-nation-state-attack-in-history/

November 10, 2021



This is the second in a four-part blog series on the NOBELIUM nation-state cyberattack. In December 2020, Microsoft began sharing details with the world about what became known as the most sophisticated nation-state cyberattack in history. Microsoft's four-part video series "Decoding NOBELIUM" pulls the curtain back on the NOBELUM incident and how world-class threat hunters from Microsoft and around the industry came together to take on the most sophisticated nation-state attack in history. In this second post, we'll explore the investigation in the second episode of the docuseries.

The threat hunters had but weeks to unravel a global attack that had been planned and executed by an advanced adversary for over a year. The early days of a cyberattack investigation can feel like joining a high-stakes chess match after your opponent has already made a series of moves. You must figure out what your adversary has done while anticipating their next step, and launching a counterplay—all simultaneously. Instead of on a chessboard, your clues are found in the code, logs, and responses to your counterattacks. In the case of the NOBELIUM nation-state attack, this was a highly skilled chess player, but we came together as a company and as an industry to take on this shared adversary. This all started when one security company, Mandiant (formerly known as FireEye), spotted an anomaly in its own environment and shared the evidence with Microsoft for additional analysis, but this story would eventually involve thousands of defenders across the industry to uncover the full picture and help protect organizations.

As explained in our first post in this series, How nation-state attackers like NOBELIUM are changing cybersecurity, nation-state attacks are malicious cyberattacks that originate from a particular country and are an attempt to further that country's interests. The nation-state attack from NOBELIUM, a Russia-sponsored group of hackers, is widely recognized as the most sophisticated in history. The group gained access to multiple enterprises before their actions were detected. This second episode of "Decoding NOBELIUM" explores how the group was detected and how defenders responded in the weeks that followed.

How was NOBELIUM detected?

It was late November 2020 when a security analyst at cybersecurity company Mandiant detected something unusual in its environment. While reviewing sign-in logs for the previous day, she noticed an event for a user with a different registered device. Intuition told her something was off so she called the user to ask if they'd registered a new device. The answer would set off an unprecedented, industry-wide hunt to catch a cybercriminal. The user said, "No."

The security professional alerted her colleagues, including her supervisor, Charles Carmakal, Mandiant Senior Vice President and Chief Technology Officer. While they didn't yet know the identity of the adversary, they would come to realize the importance of this initial detection.

Recognizing that his company needed more collaboration and telemetry to better understand the nature of the attack, Carmakal quickly turned to Microsoft. It was about 9:00 PM when Microsoft Detection and Response Team (DART) Lead Dan Taylor received the call asking for help. Dan initially thought Carmakal was joking and when he realized it was serious, he called Microsoft DART Lead Investigator Roberto, who was taking his dog for the last walk of the day, to ask him if he recognized the anomalous code Mandiant had found. Roberto confirmed that he had seen this anomaly during a previous nation-state investigation.

How did the defense team come together?

Every second counts when responding to large-scale cyberattacks like this. NOBELIUM had a year-long advantage on the defenders. A global threat-hunting effort was formed around the Microsoft Threat Intelligence Center, which defends Microsoft and its customers from advanced threat actors around the world. They immediately activated Microsoft's team of global security experts, who are on-call for major incidents.

Microsoft Security Analyst Joanne was lacing up her hiking boots on a Saturday when she received a text from her supervisor to the entire team that read, "We need all hands on deck for an active incident." The hike would have to wait as she and her teammates began studying the available data for indicators of an attack.

As Microsoft continued to partner with Mandiant, it quickly became clear that this attack extended well beyond one security company. The Microsoft response team grew along with this knowledge. With every meeting, another 50 to 100 Microsoft threat experts joined in—everyone came together to help. And the industry-wide collaboration grew as well. “Many different partners across the industry came together with a common goal,” said Ramin, Senior Malware Reverse Engineer with the Microsoft Threat Intelligence Center.

The biggest challenge was the sophisticated tradecraft of the attacker. They practiced extreme variability. “It became very clear to us that we were dealing with a highly capable, highly clandestine, and advanced adversary,” said Carmakal. NOBELIUM would never use the same IP address across organizations—even going so far as to change it every time the group re-entered the same organization’s network. That meant that traditional markers—including hashes, file names, and IP addresses—were all brittle indicators and less helpful for tracking the attacker’s path. Over time, they began identifying subtle markers of malicious activity.

The team’s relentless investigation led to a breakthrough—they discovered that the unknown threat actor was stealing credentials and moving through the networks undetected. During the ongoing investigation, the team uncovered that anomalous activity was happening within the SolarWinds platform. After decompiling 50,0000 lines of SolarWind’s code, Mandiant and Microsoft’s reverse engineers identified NOBELIUM malware carefully obfuscated within layers of code, designed to easily spread undetected to thousands of target organizations. “When we found that scope, it was a combination of exciting and scary,” said Pete, Senior Software Engineer of the Microsoft Threat Intelligence Center.

“You got a sense that this attacker could start in hundreds of customer networks, very deep into them with elevated rights,” said John Lambert, General Manager of the Microsoft Threat Intelligence Center. “When you realize how many enterprise customers and government departments use [SolarWinds], you knew that this attacker had achieved a place to have major impact, across the globe.”

Over weeks, the hunters uncovered a sophisticated, advanced threat with a scale and scope beyond anything they could have initially guessed. Now, it was time to use that hard-won knowledge to find and repel the current threat from NOBELIUM and prepare for future attacks.

NOBELIUM lessons

How did cybersecurity professionals identify NOBELIUM as the threat actor behind the attack and what can your organization do to detect and respond to nation-state attacks? In the second episode of our four-part video series “Decoding Nobelium,” security professionals talk about the investigation that followed the discovery of NOBELIUM’s attack. Watch the episode for tips on how to protect your organization against cyberattacks.

Microsoft is committed to helping organizations stay protected from cyberattacks, whether cybercriminal or nation-state. In particular, nation-state adversaries have significant expertise and resources and will develop new attack patterns to further their geopolitical objectives. Consistent with our mission to provide security for all, Microsoft will use our leading threat intelligence and global team of dedicated cybersecurity defenders to help protect our customers and the world. Just two recent examples of Microsoft's efforts to combat nation-state attacks include a September 2021 discovery, an investigation of a NOBELIUM malware referred to as FoggyWeb, and our May 2021 profiling of NOBELIUM's early-stage toolset compromising EnvyScout, BoomBox, NativeZone, and VaporRage.

For immediate support, reach out to the Microsoft Security Response Center. Keep an eye out for future posts in the Nobelium nation-state attack series where we share how we fought the NOBELIUM threat and predict the future of cybersecurity. Read our previous post in this series:

> How nation-state attackers like NOBELIUM are changing cybersecurity

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us at @MSFTSecurity for the latest news and updates on cybersecurity.