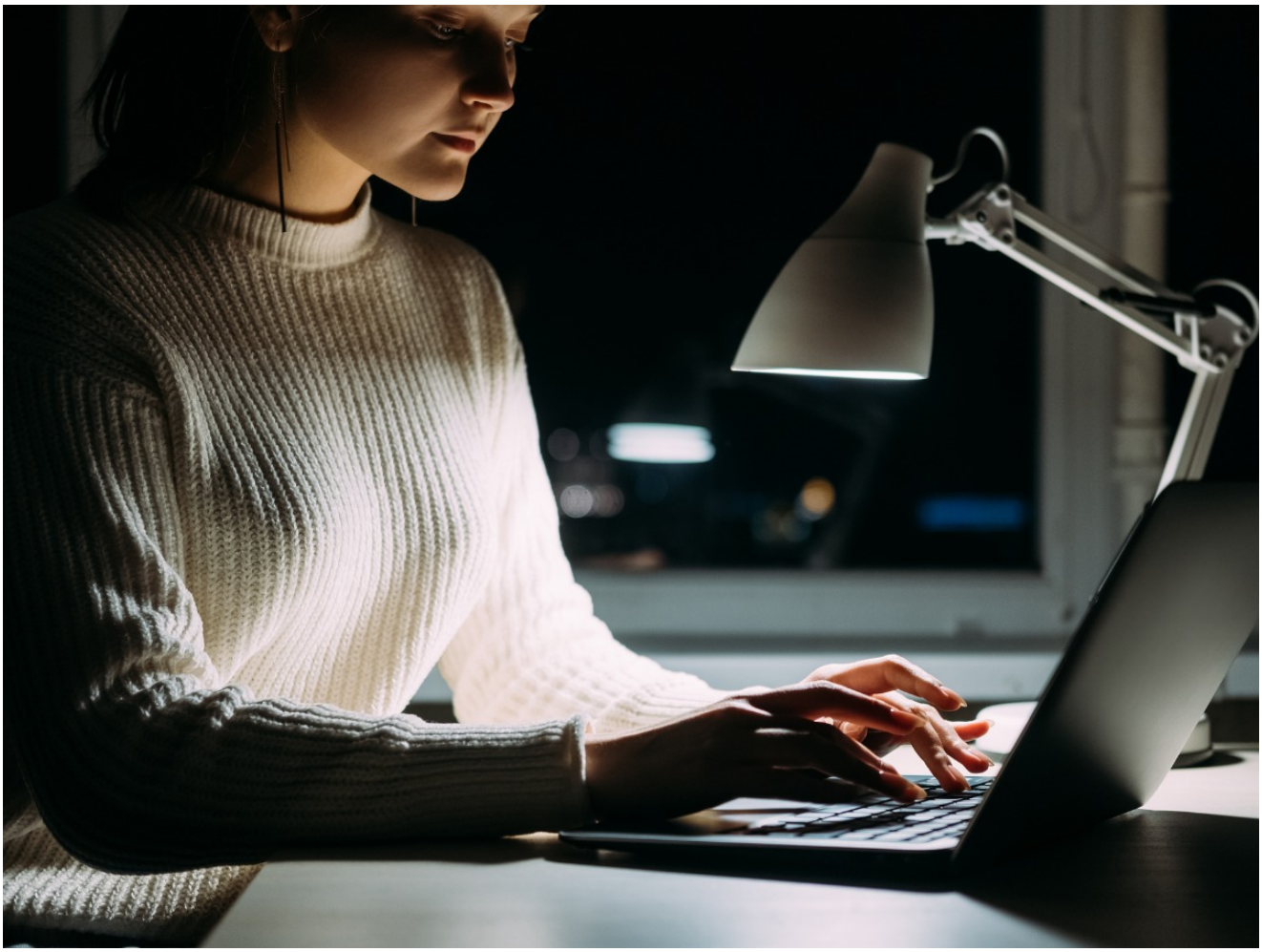
Nobelium Returns to the Political World Stage

fortinet.com/blog/threat-research/nobelium-returns-to-the-political-world-stage

February 24, 2022



Nobelium, also known as APT29 and Cozy Bear, is a highly sophisticated group of Russian-sponsored cybercriminals. Approximately two years ago, countless system administrators and IT teams were forced to work around the clock to address Nobelium's attack on SolarWinds. And last year, they similarly targeted numerous IT supply chains in the hopes of being able to embed themselves once again deep inside IT networks. But fast forward to today, and the Nobelium group seems to have shifted their focus. This time, rather than targeting software solutions, they have begun targeting embassies. While these attacks may not impact the average Windows computer user, they do have potentially larger political ramifications.

FortiGuard Labs has uncovered evidence that the Nobelium group is impersonating someone associated with the Turkish embassy in targeted email-based attacks. We will be analyzing one such attack that uses Omicron/Covid-19 as a lure. Those working in or around embassies are urged to be extra diligent when opening emails.

In this blog, we will highlight techniques and code reuse by Nobelium. We will also highlight the usage of JARM, which is a widely used technology created by Salesforce to fingerprint and track malicious servers.
Affected Platforms: Windows
Impacted Users: Windows users associated with the targeted embassies
Impact: Compromised machines are under the control of the threat actor
Severity Level: Medium

Figure 1: Embassy email

The source email address seems to be a legitimate, albeit compromised email account of a government department focused on social affairs. In tracing this, however, this email comes from a French-speaking country in Africa. It is disguised as coming from a Turkish embassy and sent to a Portuguese-speaking nation, although it is written in English.

The email itself comes with a .HTML file attachment. This file contains malicious JavaScript designed to create an .ISO file on the user's computer. Figure 2 shows some similarities between a previous Nobelium attack and this current version.

Figure 2: Malicious Javascript

The original HTML Smuggling attack conducted by Nobelium used EnvyScout to convert a text blob into an .ISO file. EnvyScout is one of the toolsets used as a dropper in spearphishing attacks by this APT group. As seen in Figure 2, both samples used an application type of "x-cd-image." This part of the attack has changed very little. However, Figure 3 below shows the function used to create the .ISO file has been streamlined from previous iterations.

Figure 3: ISO creation

Once the .ISO file has been created on the user's machine, the attack requires a user to open the file. By default, opening an .ISO file on modern versions of Windows causes it to mount the file on the next available drive letter. Once mounted, the files can be seen. Figure 4 below shows this part of the attack chain.

Figure 4: Mounted ISO files

One of the previous variants of the Nobelium attack was dated almost exactly one year prior to the current attack. Both versions contain malicious shortcuts that point to a DLL file. In the current version, the DLL file inside the bin folder is named "DeleteDateConnectionPosition.dll."

In the past, one of the payloads used was a Cobalt Strike beacon, and this is the case in this current version. Given the current political situation, it is clearly in Russia's best interest to know what other governments are thinking, planning, and doing, and successful installation

of a Cobalt Strike beacon provides a foothold into the embassies they are interested in monitoring. To achieve this objective, the shortcut launches the DLL using an export named "DeleteDateConnectionPosition."

Figure 5: DLL Exports

Many of the exports inside the DLL contain junk code. As such, debugging the malware is faster than statically analyzing it. Once completed we discovered a C2 server, as shown below.

Figure 6: Debugging the malicious DLL

According to our sources, this server is not a shared server and the IP address only contains the sinitude[.]com domain.

JARM Fingerprinting

For those unfamiliar with JARM, it is a technology developed by Salesforce to fingerprint servers for the purposes of clustering. Specifically, JARM revolves around a server's TLS implementation. As further explained by Salesforce, it is not a secure crypto function, and as a result, it may produce false positives. Nevertheless, it has been a fairly accurate way to group malicious servers into relevant clusters.

The JARM signature for sinitude[.]com has been found on numerous servers. Many of these servers have also acted as Cobalt Strike beacon C2 servers. During the course of our investigation, we found that this JARM signature was also found on C2 servers associated with the malware family BazarLoader. BazarLoader, among other things, contains code and application guardrails that makes sure it is not running on a Russian computer.

By looking at network traffic since the beginning of this year, we found that several IP addresses are connected to sinitude[.]com. However, our data indicates that only one IP address (back in January) actually created a full connection to communicate with the C2. This IP address is located in Kharkiv, the second largest city in Ukraine. This Kharkiv IP address itself has communicated with unique malware families and is part of the TOR network.

Conclusion

In this latest attack, Nobelium has used techniques similar to those they have used in the past. Malicious emails remain the predominant way to infiltrate organizations, and Nobelium takes advantage of that attack vector. The biggest difference now is the political landscape. While previous attacks carried out by Nobelium may have been more technical in nature, this latest round has far more consequences on the political world stage.

Fortinet Protections

The FortiGuard Antivirus Service detects and blocks both the .ISO and DLL files as W64/CobaltStrike_Beacon.A!tr.

The FortiGuard Antivirus Service detects and blocks the malicious html email attachment as JS/Agent.ONO!tr.

All relevant network IOCs are blocked by the WebFiltering client.

MITRE TTPs

Initial Access	
Phishing: Spearphishing Attachment	T1566.001
Execution	
Command and Scripting Interpreter: JavaScript	T1059.007
User Execution: Malicious File	T1204.002
Defense Evasion	
Build Image on Host	T1612
Deobfuscate/Decode Files or Information	T1140
Obfuscated Files or Information: HTML Smuggling	T1027.006
Command and Control	
Application Layer Protocol: Web Protocols	T1071.001
Impact	
Resource Hijacking	T1496

IOCs

File IOCs

Covid.html (SHA2:
A896C2D16CADCDEDD10390C3AF3399361914DB57BDE1673E46180244E806A1D0)

Covid.iso (SHA2:
3CB0D2CFF9DB85C8E816515DDC380EA73850846317B0BB73EA6145C026276948)

DeleteDateConnectionPosition.dll (SHA2:
6EE1E629494D7B5138386D98BD718B010EE774FE4A4C9D0E069525408BB7B1F7)

Network IOCs

Sinitude[.]com

JARM Signature:
2ad2ad0002ad2ad0002ad2ad2ad2ade1a3c0d7ca6ad8388057924be83dfc6a

Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.