NOBELIUM Campaigns and Malware

Cyber Intel Unit ⋮⋮ 6/3/2021

Author: James Barnett

TLP: WHITE

1. Executive Summary

Between 27 and 28 May, Microsoft published two reports on NOBELIUM, the threat actor behind the December 2020 supply chain attacks[1] on SolarWinds' Orion platform. The first report detailed an ongoing spearphishing campaign that leveraged a variety of techniques to distribute a Cobalt Strike Beacon payload that allows NOBELIUM to remotely control the targeted system through an encrypted network tunnel.[2] The second report detailed four tools that were part of NOBELIUM's unique infection chain in that campaign: EnvyScout, BoomBox, NativeZone, and VaporRage.[3]

2. Analysis

2.1. Spearphishing Campaigns

Microsoft reports that NOBELIUM has been conducting a new malicious email campaign since February 2021. It differs significantly from their previous operations that ran from September 2019 to January 2021 and that led to the breach of the SolarWinds Orion platform. In this new campaign, NOBELIUM distributed multiple waves of spearphishing emails, each revealing an evolution of their malware delivery techniques.

The first wave of the campaign, discovered in February, leveraged the legitimate Google Firebase platform to stage an ISO file containing a malicious payload, as well as to record attributes of visitors who accessed the URLs included in the phishing emails. This wave included a brief reconnaissance period starting on 28 January, during which NOBELIUM sent the Firebase tracking URL to targets and recorded when they clicked on the URL. They did not deliver the malicious ISO payload at this stage.

The next waves of the campaign began in March and used a malicious HTML file attached to a spearphishing email in an attempt to compromise targeted users. This HTML file used JavaScript to write an ISO file containing a malicious payload directly to the target's disk, including a message that encouraged the target to open the ISO. If the target did so, the ISO file would then be mounted in the same manner as an external drive. This allowed a shortcut file (LNK) within the ISO to execute an included dynamic-link library (DLL) that ultimately resulted in the delivery and execution of a Cobalt Strike Beacon payload. During these waves, NOBELIUM began to experiment with a distribution method that involved embedding the ISO file within the HTML attachment rather than the previous method of hosting the ISO on Firebase.

The next waves of the campaign began in April and involved NOBELIUM completely abandoning Firebase for both its ISO distribution and victim tracking. They shifted to distributing the ISOs using the aforementioned HTML embedding method and began to use a new method of victim tracking. The campaign evolved again in May when NOBELIUM added a custom .NET module to perform reconnaissance and download additional payloads that they had stored on Dropbox.

On 25 May, NOBELIUM's campaign began using the legitimate mass-mailing service Constant Contact to target roughly 3,000 unique accounts across more than 150 organizations. This new wave of spearphishing emails used several different types of lures, one of which imitated a special alert from the United States Agency for International Development (USAID), stating that Donald Trump had published new documents regarding election fraud, and included a link where these documents would purportedly be found. In reality, this link used Constant Contact's legitimate redirector service to send victims to a different URL that would deliver NOBELIUM's malicious ISO file.

On 1 June, the U.S. Department of Justice announced that they had seized two of the domains involved in NOBELIUM's spearphishing campaign (theyardservice[.]com and worldhomeoutlet[.]com) pursuant to a court order on 28 May.[8]

2.2. EnvyScout

EnvyScout is a malicious HTML file that deobfuscates and writes a malicious ISO file to disk. In this campaign, the threat actors delivered the file *NV.html* as an attachment to the campaign's spearphishing emails. The body of this HTML file included tracking and credential harvesting URLs, an encoded ISO payload, an embedded JavaScript to decode the payload, and another embedded JavaScript to allow the HTML file to write the decoded ISO file to disk.

2.3. BoomBox

BoomBox is a malicious downloader distributed as an executable named *BOOM.exe* contained within the ISO dropped by EnvyScout. When executed, it checks to ensure that a directory named *NV* is present in its working directory and terminates if it does not find this directory. BoomBox also performs another check to ensure that the system does not contain a file named *%AppData%\Microsoft\NativeCache\NativeCacheSvc.dll* and will terminate if it finds the file.

After performing these checks, BoomBox proceeds to gather information about the infected system, including its hostname, domain name, IP address, and the victim's username. It encrypts this information using the Advanced Encryption Standard (AES) with a hardcoded encryption key *123do3y4r378o5t34onf7t3o573tfo73* and initialization vector (IV) value *1233t04p7jn3n4rg*. After encryption, BoomBox adds PDF file signatures to the beginning and end of the data so that the encrypted data appears to be a valid PDF file, and then uploads the file to Dropbox.

Once BoomBox has uploaded information about the victim's system, it proceeds to download the NativeZone and VaporRage payloads from Dropbox. It then decrypts and executes these payloads to start the next stage of the attack chain.

2.4. NativeZone

NativeZone is Microsoft's name for NOBELIUM's wide variety of custom Cobalt Strike Beacon loaders. These loaders were previously tracked under unique names including TEARDROP[4] and Raindrop, but Microsoft is now tracking them under the single name NativeZone due to their disposable nature and similar purpose within NOBELIUM's attack chain. All variants of NativeZone are malicious DLLs that decrypt and load a malicious payload from an embedded code buffer or from another accompanying file.

2.5. VaporRage

VaporRage is a malicious DLL file that acts as a shellcode downloader. It contains functions that are called by NativeZone in order to download, decode, and execute arbitrary shellcode from the attacker's command and control (C&C) servers. The most common shellcode payload that VaporRage currently delivers is Cobalt Strike Beacon, as observed in NOBELIUM's previous campaigns.

2.6. Cobalt Strike

Cobalt Strike is a legitimate penetration testing tool that has become increasingly popular amongst threat actors due to its many powerful features. Its capabilities include keylogging, taking screenshots, deploying additional payloads, exploiting system vulnerabilities to facilitate additional attacks, evading detection with various countermeasures, rapidly exfiltrating data through encrypted tunnels, and more.[5]

3. Prevention and Mitigation

The Cybersecurity and Infrastructure Security Agency (CISA) provides the following list of best practices to strengthen the security of an organization.[6] In addition, CISA references the publication from the National Institute of Standards and Technology (NIST), "Guide to Malware Incident Prevention & Handling for Desktops and Laptops" for more information on malware incident prevention and handling.[7]

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

4. Indicators of Compromise

Indicator	Description
boom[.]exe	BoomBox EXE filename
0acb884f2f4cfa75b726cb8290b20328c8ddbcd49f95a1d761b7d131b95bafec	BoomBox EXE SHA256s
8199f309478e8ed3f03f75e7574a3e9bce09b4423bd7eb08bb5bff03af2b7c27	
cf1d992f776421f72eabc31d5afc2f2067ae856f1c9c1d6dc643a67cb9349d8c	
74d6b7b2[.]app[.]giftbox4u[.]com	Cobalt Strike C&C domains
aimsecurity[.]net	
cityloss[.]com	
content[.]pcmsar[.]net	
cross-checking[.]com	
giftbox4u[.]com	
hanproud[.]com	
newstepsco[.]com	
stockmarketon[.]com	
stsnews[.]com	
tacomanewspaper[.]com	
trendignews[.]com	
139[.]99[.]167[.]177	Cobalt Strike C&C IP
desktop[.]dll	Cobalt Strike DLL filenames
diassvcs[.]dll	
dxgim[.]dll	
GraphicalComponent[.]dll	
imgmountingservice[.]dll	
information[.]exe	
Java_SRE_runtime_update[.]dll	
msch[.]dll	
msdiskmountservice[.]dll	
mshost[.]dll	
mstu[.]dll	

WRAR600[.]EXE	
0c14a791f8a48d2944a9fa842f45becb7309ad004695e38f48fca69135d327c6 1f5a915e75ad96e560cee3e24861cf6f8de299fdf79e1829453defbfe2013239 292e5b0a12fea4ff3fc02e1f98b7a370f88152ce71fe62670dd2f5edfaab2ff8 2a352380d61e89c89f03f4008044241a38751284995d000c73acf9cad38b989e 2ebbb99b8dae0c7b0931190fa81add987b44d4435dafcf53a9cde0f19bb91398 776014a63bf3cc7034bd5b6a9c36c75a930b59182fe232535bb7a305e539967b 88c95954800827cb68e1efdacd99093f7f9646d82613039472b5c90e5978444d a4f1f09a2b9bc87de90891da6c0fca28e2f88fd67034648060cef9862af9a3bf bca5560a9a9dd54be76e4a8d63a66e9cfd731b0bd28524db05cc498bb5b56384 c4ff632696ec6e406388e1d42421b3cd3b5f79dcb2df67e2022d961d5f5a9e78	Cobalt Strike DLL SHA256s
f9a74ac540a6584fc3ba7ccc172f948c6b716cceea313ce1d9e7b735fa2a5687	
reply slip[.]rtf Reply slip[.]rtf	Cobalt Strike encrypted payload filenames
7a3b27cf04b7f8110fc1eee5f9c4830d38ac00467fc856330115af4bffaf35b6 7bf3457087ea91164f86f4bb50ddb46c469c464c300228dba793f7bfe608c83e	Cobalt Strike encrypted payload SHA256s
enpport[.]com	EnvyScout C&C domain
Attachment[.]html attachment[.]html cert[.]html information[.]html Invitation[.]html NV[.]html nv[.]html Reply slip[.]html	EnvyScout HTML attachment filenames
065e9471fb4425ec0b3a2fd15e1546d66002caca844866b0764cbf837c21a72a 279d5ef8f80aba530aaac8afd049fa171704fc703d9cfe337b56639732e8ce11 2836e5553e1ae52a1591545b362d1a630e3fef7e6b7e8342a84008fe4a6473a9 6df1d7191f6dd930642cc5c599efb54bfcc964b7a2e77f6007787de472b22a6a 9059c5b46dce8595fcc46e63e4ffbceeed883b7b1c9a2313f7208a7f26a0c186	EnvyScout HTML attachment SHA256s

9301e48ea3fa7d39df871f04072ee47b9046d76aa378a1c5697f3b2c14aef1d6 ca83d7456a49dc5b8fe71007e5ac590842b146dd5c45c9a65fe57e428a8bd7c6 cfb57906cf9c5e9c91bc4aa065f7997b1b32b88ff76f253a73ee7f6cfd8fff2f dcf48223af8bb423a0b6d4a366163b9308e9102764f0e188318a53f18d6abd25 f5bc4a9ffc2d33d4f915e41090af71544d84b651fb2444ac91f6e56c1f2c70d5 f7e8c9d19efd71f5c8217bf12bdd3f6c88d5f56ab65fea02dc2777c5402a18f1	
cdn[.]theyardservice[.]com dailydews[.]com dataplane[.]theyardservice[.]com doggroomingnews[.]com email[.]theyardservice[.]com emergencystreet[.]com smtp2[.]theyardservice[.]com static[.]theyardservice[.]com theyardservice[.]com usaid[.]theyardservice[.]com worldhomeoutlet[.]com	NativeZone C&C domains
documents[.]dll KM[.]FileSystem[.]dll NativeCacheSvc[.]dll RtlSvcMicro[.]dll Wbtr[.]dll	NativeZone DLL filenames
136f4083b67bc8dc999eb15bb83042aeb01791fc0b20b5683af6b4ddcf0bbc7d 3b94cc71c325f9068105b9e7d5c9667b1de2bde85b7abc5b29ff649fd54715c4 4fbfeb7a0bb6b9841b92fa4e6b5a7bdb69c2a12ed39691c9495ff88cd6f58836 6d08b767117a0915fb86857096b4219fd58596b42ccf61462b137432abd3920e b295c5ad4963bdffa764b93421c3dd512ca6733b79bdff2b99510e7d56a70935 ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330	NativeZone DLL SHA256s
manual[.]pdf	NativeZone PDF filename
656384c4e5f9fe435d51edf910e7ba28b5c6d183587cf3e8f75fb2d798a01eeb	NativeZone PDF SHA256
financialmarket[.]org	NOBELIUM C&C

pcmsar[.]net techiefly[.]com theadminforum[.]com	domains
185[.]158[.]250[.]239 195[.]206[.]181[.]169 37[.]120[.]247[.]135 45[.]135[.]167[.]27 51[.]254[.]241[.]158 51[.]38[.]85[.]225	NOBELIUM C&C IPs
ica-declass[.]pdf Meeting info[.]docx nv[.]pdf state ellection changes[.]docx	NOBELIUM decoy document filenames
574b7a80d8b9791cb74608bc4a9fcba4e4574fafef8e57bdee340728445ebd16 73ca0485f2c2c8ba95e00188de7f5509304e1c1eb20ed3a238b0aa9674f9104e 7d34f25ad8099bd069c5a04799299f17d127a3866b77ee34ffb59cfd36e29673 d37347f47bb8c7831ae9bb902ed27a6ce85ddd9ba6dd1e963542fd63047b829c	NOBELIUM decoy document SHA256s
cdnappservice[.]firebaseio[.]com eventbrite-com-default-rtdb[.]firebaseio[.]com humanitarian-forum-default-rtdb[.]firebaseio[.]com security-updater-default-rtdb[.]firebaseio[.]com supportcdn-default-rtdb[.]firebaseio[.]com	NOBELIUM ISO download domains
AktualizC!ciu[.]img Attachment[.]img attachment[.]img attachment[.]iso dppy_empty[.]iso ica-declass[.]img ICA-declass[.]iso information[.]iso Invitation Document[.]iso	NOBELIUM ISO filenames

nv[.]img	
NV[.]img	
Reply slip[.]iso	
SMM_Report[.]img	
topics_of_discussion[.]iso	
2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252	NOBELIUM ISO SHA256s
5f7d08eb2039a9d2e99ebf3d0ef2796b93d0a01e9b8ec403fec8fcdf46448693	
60e20576b08a24cdaeaabc4849011885fb7517713226e2663031d9533d2187bc	
6e2069758228e8d69f8c0a82a88ca7433a0a71076c9b1cb0d4646ba8236edf23	
749bf48a22ca161d86b6e36e71a6817b478a99d935cd721e8bf3dba716224c84	
7ed1b6753c94250ad3c1c675eb644940c8104ff06a123252173c33cc1be5e434	
873717ea2ea01ae6cd2c2dca9d6f832a316a6e0370071bb4ee6ecff3163f8d18	
89016b87e97a07b4e0263a18827defdeaa3e150b1523534bbdebe7305beabb64	
94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916	
98473e1b8f7bedd5cfa3b83dad611db48eee23faec452e62797fb7752228c759	
a45a77ad5c138a149aa71fb323a1e2513e7ac416be263d1783a7db380d06d2fc	
d19ff098fe0f5947e08ec23be27d3a3355e14fb20135d8c4145126caa8be4b05	
e41a7616a3919d883beb1527026281d66e7bcdaff99600e462d36a58f1bdc794	
f006af714379fdd63923536d908f916f4c55480f3d07adadd53d5807e0c285ee	
AKTUALIZ[.]LNK	NOBELIUM LNK filenames
Attachment[.]lnk	
attachment[.]lnk	
information[.]txt[.]lnk	
Integrated Review[.]lnk	
NV[.]lnk	
nv[.]lnk	
Plending forms[.]lnk	
Programme outline[.]lnk	
reply slip[.]lnk	
Reply slip[.]rtf[.]lnk	

reports[.]lnk	
ScanClientUpdate[.]lnk	
0585ed374f47d823f8fcbb4054ad06980b1fe89f3fa3484558e7d30f7b6e9597	NOBELIUM LNK SHA256s
112f92cfecdc4e177458bc1caebcc4420b5879840f137f249fac360ddac64ddd	
194f4d1823e93905ee346d7e1fffc256e0befd478735f4b961954df52558c618	
24caf54e7c3fe308444093f7ac64d6d520c8f44ea4251e09e24931bdb72f5548	
3c86859207ac6071220976c52cef99abf18ae37ae702c5d2268948dda370910b	
48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0	
6866041f93141697ec166fe64e35b00c5fcd5d009500ecf58dd0b7e28764b167	
69f0d85119123f3c2e4c052a83671732aced07312a05a3abf4ab0360c70f65de	
74202eed181e2b83dd0ab6f791a34a13bd94e63e86b82395f9443cb5aeddc891	
b81beb17622d4675a1c6f4efb358cc66903366df75eb5911bca725465160bdb6	
d7c05bd68e8bde3d13aa7dbd6911461104d06715da15d3ee7f75136fa8330cc2	
eae312c5ec2028a2602c9654be679ecde099b2c0b148f8d71fca43706efe4c76	
f88530bc87cf2c133c0a50e434ce0428694901fe7860abb42737097fdea56b30	
cdnappservice[.]web[.]app	NOBELIUM spearphish URL domains
eventbrite-com-default-rtdb[.]firebaseio[.]com	
humanitarian-forum[.]web[.]app	
logicworkservice[.]web[.]app	
security-updater[.]web[.]app	
supportcdn[.]web[.]app	
ScanClientUpdate[.]zip	NOBELIUM ZIP attachment filename
ca66b671a75bbee69a4a4d3000b45d5dc7d3891c7ee5891272ccb2c5aed5746c	NOBELIUM ZIP attachment SHA256
holescontracting[.]com	VaporRage C&C domains
newsplacec[.]com	
CertPKIProvider[.]dll	VaporRage DLL filenames
mswsc[.]dll	
117317d623003995d639975774edd1bfe38cec7d24b22d3e48d22c91cf8636bb	VaporRage DLL SHA256s
1c17c39af41a5d8f54441ce6b1cf925f6727a2ee9038284a8a7071c984d0460f	
b0bfe6a8aa031f7f5972524473f3e404f85520a7553662aaf886055007a57db5	

readme[.]pdf	VaporRage PDF filename
23e20d630a8fd12600c2811d8f179f0e408dcb3e82600456db74cbf93a66e70f	VaporRage PDF SHA256

Endnotes

1. https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory-solarwinds-supply-chain-attack/
2. https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
3. https://www.microsoft.com/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/
4. https://blogs.infoblox.com/cyber-threat-intelligence/teardrop-malware/
5. https://www.cobaltstrike.com/features
6. https://us-cert.cisa.gov/ncas/analysis-reports/ar21-039b
7. https://csrc.nist.gov/publications/detail/sp/800-83/rev-1/final
8. https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-used-furtherance-spear