ID: 431812
Sample Name:
ZVFVY7NwZ7.exe
Cookbook: default.jbs
Time: 11:09:18
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report ZVFVY7NwZ7.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 13
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 19
UDP Packets 19
DNS Queries 19

DNS Answers 19
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 20
Analysis Process: ZVFVY7NwZ7.exe PID: 2220 Parent PID: 5828 20
General 20
File Activities 20
File Created 20
File Written 20
File Read 20
Registry Activities 20
Key Value Modified 20
Analysis Process: wscript.exe PID: 1784 Parent PID: 2220 20
General 20
File Activities 21
Analysis Process: ZVFVY7NwZ7.exe PID: 5612 Parent PID: 2220 21
General 21
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 23
Analysis Process: powershell.exe PID: 3016 Parent PID: 1784 23
General 23
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Analysis Process: conhost.exe PID: 4180 Parent PID: 3016 23
General 23
Disassembly 23
Code Analysis 23

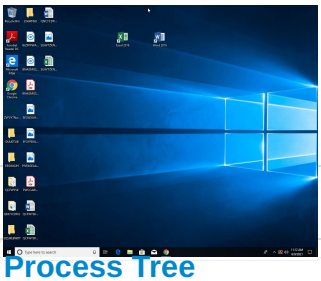
Analysis Report ZVFVY7NwZ7.exe

Overview

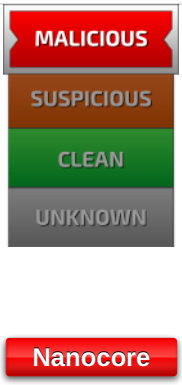
General Information

Sample Name:	ZVFVY7NwZ7.exe
Analysis ID:	431812
MD5:	8e87de15cd3da1..
SHA1:	80830909ec859e..
SHA256:	ec850202f17a8e7.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



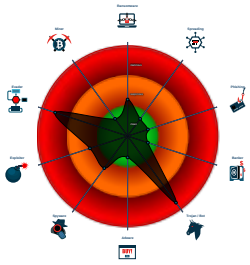
Nanocore

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- ZVFVY7NwZ7.exe (PID: 2220 cmdline: 'C:\Users\user\Desktop\ZVFVY7NwZ7.exe' MD5: 8E87DE15CD3DA1245B9C7B0E48C0F126)
  - wscript.exe (PID: 1784 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp_Lzqtfofnnzmk.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - powershell.exe (PID: 3016 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath C:\,'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ZVFVY7NwZ7.exe (PID: 5612 cmdline: C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe MD5: 8E87DE15CD3DA1245B9C7B0E48C0F126)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "4614bd42-26c0-4da0-8e09-16890d37",
  "Group": "Default",
  "Domain1": "wekeepworking.sytes.net",
  "Domain2": "wekeepworking12.sytes.net",
  "Port": 1144,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1049d:$x1: NanoCore.ClientPluginHost • 0x104da:$x2: IClientNetworkHost • 0x1400d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10205:$a: NanoCore • 0x10215:$a: NanoCore • 0x10449:$a: NanoCore • 0x1045d:$a: NanoCore • 0x1049d:$a: NanoCore • 0x10264:$b: ClientPlugin • 0x10466:$b: ClientPlugin • 0x104a6:$b: ClientPlugin • 0x1038b:$c: ProjectData • 0x10d92:$d: DESCrypto • 0x1875e:$e: KeepAlive • 0x1674c:$g: LogClientMessage • 0x12947:$i: get_Connected • 0x110c8:$j: #=q • 0x110f8:$j: #=q • 0x11114:$j: #=q • 0x11144:$j: #=q • 0x11160:$j: #=q • 0x1117c:$j: #=q • 0x111ac:$j: #=q • 0x111c8:$j: #=q
0000000D.00000002.484283906.0000000006400000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
0000000D.00000002.484283906.0000000006400000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.ZVFVY7NwZ7.exe.6400000.14.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
13.2.ZVFVY7NwZ7.exe.6400000.14.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost
13.2.ZVFVY7NwZ7.exe.674e8a4.25.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10937:$x1: NanoCore.ClientPluginHost • 0x10951:$x2: IClientNetworkHost
13.2.ZVFVY7NwZ7.exe.674e8a4.25.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x10937:$x2: NanoCore.ClientPluginHost • 0x13c74:$s4: PipeCreated • 0x10924:$s5: IClientLoggingHost
13.2.ZVFVY7NwZ7.exe.6480000.19.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
Click to see the 105 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: WScript or CScript Dropper

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

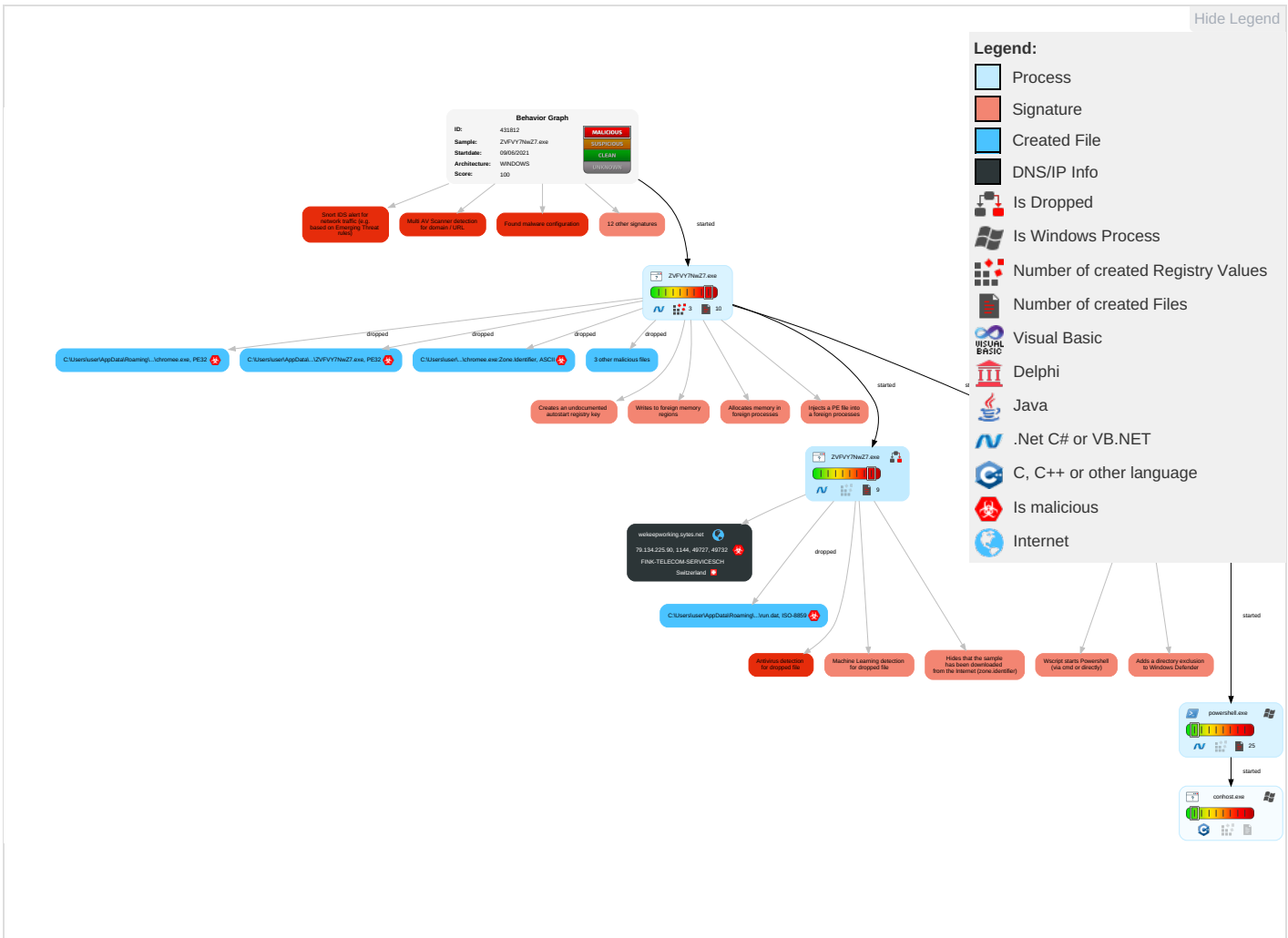
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Valid Accounts	Windows Management Instrumentation 1	Registry Run Keys / Startup Folder 1 1	Process Injection 3 1 2	Disable or Modify Tools 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	En Cha
Default Accounts	Scripting 1 1 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Nor Por
Domain Accounts	PowerShell 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 1 1 1	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rer Sof

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 1 2 1	SSH	Keylogging	Data Transfer Size Limits	App Lay Pro
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
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/Obfuscated Non-C2 Protocol	File Pro

Behavior Graph



Screenshots

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
ZVFVY7NwZ7.exe	100%	Avira	HEUR/AGEN.1129534	
ZVFVY7NwZ7.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe	100%	Avira	HEUR/AGEN.1129534	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe	100%	Avira	HEUR/AGEN.1129534	
C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.ZVFVY7NwZ7.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1129534		Download File
0.0.ZVFVY7NwZ7.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1129534		Download File
13.2.ZVFVY7NwZ7.exe.a40000.1.unpack	100%	Avira	HEUR/AGEN.1129534		Download File
13.0.ZVFVY7NwZ7.exe.a40000.0.unpack	100%	Avira	HEUR/AGEN.1129534		Download File
13.2.ZVFVY7NwZ7.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.ZVFVY7NwZ7.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.ZVFVY7NwZ7.exe.6490000.21.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.0.ZVFVY7NwZ7.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.ZVFVY7NwZ7.exe.a40000.4.unpack	100%	Avira	HEUR/AGEN.1129534		Download File
13.0.ZVFVY7NwZ7.exe.a40000.2.unpack	100%	Avira	HEUR/AGEN.1129534		Download File

Domains

Source	Detection	Scanner	Label	Link
wekeepworking.sytes.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	URL Reputation	safe	
http://schemas.microso	0%	URL Reputation	safe	
http://schemas.microso	0%	URL Reputation	safe	
http://schemas.microso	0%	URL Reputation	safe	
wekeepworking.sytes.net	8%	Virustotal		Browse
wekeepworking.sytes.net	0%	Avira URL Cloud	safe	
wekeepworking12.sytes.net	2%	Virustotal		Browse
wekeepworking12.sytes.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	79.134.225.90	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
wekeepworking.sytes.net	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown
wekeepworking12.sytes.net	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.90	wekeepworking.sytes.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431812
Start date:	09.06.2021
Start time:	11:09:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ZVFVY7NwZ7.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:	31
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.evad.winEXE@8/15@9/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 97% • 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
11:11:09	API Interceptor	524x Sleep call for process: ZVFVY7NwZ7.exe modified
11:11:32	API Interceptor	34x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.90	kylfnzzg3E.exe	Get hash	malicious	Browse	
	Ref 0180066743.xlsx	Get hash	malicious	Browse	
	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	A2PlnLyOA7.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	
	4fn66P5vkl.exe	Get hash	malicious	Browse	
	P_O 00041221.xlsx	Get hash	malicious	Browse	
	LOT_20210526.xlsx	Get hash	malicious	Browse	
	Swift Copy.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wekeepworking.sytes.net	kyIfnzzg3E.exe	Get hash	malicious	Browse	• 79.134.225.90
	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	A2PlnLyOA7.exe	Get hash	malicious	Browse	• 79.134.225.90
	SecuriteInfo.com.Trojan.GenericKD.37013274.28794.exe	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	Q2MAUt4mRO.exe	Get hash	malicious	Browse	• 79.134.225.90
	4fn66P5vkl.exe	Get hash	malicious	Browse	• 79.134.225.90
	P_O 00041221.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	LOT_20210526.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	QI5MR3pte0.exe	Get hash	malicious	Browse	• 185.140.53.40
	5Em2NXNxSt.exe	Get hash	malicious	Browse	• 185.140.53.40
	7Zpsd899Kf.exe	Get hash	malicious	Browse	• 185.140.53.40
	LfgEatrwIF.exe	Get hash	malicious	Browse	• 185.140.53.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	0jyrU2E05S.exe	Get hash	malicious	Browse	• 79.134.225.72
	kyIfnzzg3E.exe	Get hash	malicious	Browse	• 79.134.225.90
	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	MS2106071066.exe	Get hash	malicious	Browse	• 79.134.225.71
	Kangean PO.doc	Get hash	malicious	Browse	• 79.134.225.72
	facture.jar	Get hash	malicious	Browse	• 79.134.225.69
	c3yBu1IF57.exe	Get hash	malicious	Browse	• 79.134.225.92
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 79.134.225.25
	SecuriteInfo.com.Trojan.Win32.Save.a.16917.exe	Get hash	malicious	Browse	• 79.134.225.94
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	H538065217Invoice.exe	Get hash	malicious	Browse	• 79.134.225.9
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	P.I-84512.doc	Get hash	malicious	Browse	• 79.134.225.41
	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	• 79.134.225.92
	Swift [ref QT #U2013 2102001-R2]pdf.exe	Get hash	malicious	Browse	• 79.134.225.10
	PO756654.exe	Get hash	malicious	Browse	• 79.134.225.99
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90
	br.exe	Get hash	malicious	Browse	• 79.134.225.73
	Yeni sipari#U015f _WJO-001, pdf.exe	Get hash	malicious	Browse	• 79.134.225.71
	as.exe	Get hash	malicious	Browse	• 79.134.225.73

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ZVFVY7NwZ7.exe.log	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	847
Entropy (8bit):	5.35816127824051
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MxHKXwYHKhQnoPtHoxHhAHKzva
MD5:	31E089E21A2AEB18A2A23D3E61EB2167
SHA1:	E873A8FC023D1C6D767A0C752582E3C9FD67A8B0
SHA-256:	2DCCE5D76F242AF36DB3D670C006468BEEA4C58A6814B2684FE44D45E7A3F836
SHA-512:	A0DB65C3E133856C0A73990AEC30B1B037EA486B44E4A30657DD5775880FB9248D9E1CB533420299D0538882E9A883BA64F30F7263EB0DD62D1C673E7DBA881
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",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\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22148
Entropy (8bit):	5.6032477905053035
Encrypted:	false
SSDEEP:	384:CtCDLq0D01mp9lro0rvHcOYSBKQulJIai7V9wWSJUeRu1BMkmNZ1AV7ObWT+564u:R59lroCBY4KQulJ1RWXet346zu
MD5:	8496AB6417CE1A827983CF75D1766111
SHA1:	00F94AE48032DDA9B613E657D36948841FB6861B
SHA-256:	162E0F40330B89C783DE280CF40134BBE1A4E653F89B2D4802E242C95BA950FA
SHA-512:	1FFB57D1D1A429B9C87A33D730D55A45A397C4109D38E44BB1C938F907CB4E0E4D4E09A5DA7BA483EF0E7362B9DAE0FA207C0F4FDBF51A14C85941010C85C4A
Malicious:	false
Reputation:	low
Preview:	@...e.....Y.....<.-.....G.5.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	662016
Entropy (8bit):	7.9894013878846275
Encrypted:	false
SSDEEP:	12288:ETQ2c25dc9wH6UvJF0nvekN2rDerJDTQsKIU9JDAccU7jYUL1Xk:52oWksqla711Xk
MD5:	8E87DE15CD3DA1245B9C7B0E48C0F126
SHA1:	80830909EC859ED61811329AE16888CB87E1ED5F
SHA-256:	EC850202F17A8E7F5A04603E9C70AB21D7B39FB3142A79098AEF1D592974702E
SHA-512:	236BDCAE21D29DF979BFEDF650B23FEA04BEBABD4EB79B172D9E4AC2A602494727338E3937C9F9F371DBF0FF78E457BEE138C9A7FDE6351ED9A205888E4EA4A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.*.....0..... ... .@.. .....`..... ..@.....K.... .....@..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....x7.../.....:...xf.....{....*J8....*..}....8.....{....*6..}....8....*..z8....*..(....8.....(....8.....&~.....*...~....*...{. ...*6..}....8....*....{....*J8....*..}....8.....z8.....(....8.....(....8....*.&~.....*...~....*...{....*6..}....8....*....{....*6..}....8....*..f..(....8....*..(....8.....&~.....*...~....*...{....*J8....*..}....8.....{... .*J8....*..}....8.....z8.....(....8.....(....8....*.&~.....*...~..

C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp_Lzqtfofnnzmk.vbs	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	183
Entropy (8bit):	5.011522109824809
Encrypted:	false
SSDEEP:	3:FER/n0eFHgSSJJFkBBVIceGAFddGeWLCXknRAuWXp5cViEaKC5SufyM1K/RFofDe:FER/lFHsQdeGgdEYmRAuWXp+NaZ5SuHm
MD5:	B1B51D4DF85A59A665A8BDB96E5018CF
SHA1:	0F6FE802C29633E900FF2C59A58B759B1DFF01BF
SHA-256:	975B377F5BFECD9542B801DDA6831BD44CCFF88F8C804D3FF42B2161C07A8075
SHA-512:	665151289DDA2AEF11C3626F4DEDBB6D8908898BC25F4AF1D4E91D1B787245D56A3EA82F07BB7C743ADAB5F7D218F5DD7C9C62F3438405CB15CCF27864E1B21
Malicious:	**true**
Reputation:	low
Preview:	CreateObject("WScript.Shell").Run "powershell Add-MpPreference -ExclusionPath C:\,'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe'", 0, False

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jef2jh0v.dlt.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jef2jh0v.dlt.psm1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jorb5u2s.hyr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe
File Type:	data
Category:	dropped
Size (bytes):	1728
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	48:IkR5lkR5lkR5lkR5lkR5lkR5lkR5i:xwwwwwwwk
MD5:	C7F4F5E1BE880A59E49249005C1E301D
SHA1:	EF2AAE2EA249910F3F61B363A7DD0AF70EFE6448
SHA-256:	F7E2318D515B382C2100F5B11F89C7B62B6E75AB8AEE9F684BDFAAF28195858D
SHA-512:	0DFF549B01A00BEE1AF1775AAA551B1DDC9AE7929CE401515956A5F2A6E112F0CCBD78BC3281442DD682CE6F7DD3A467A6E7458BB600D583FF90B13E8A7810 2
Malicious:	false
Preview:	 Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL |XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*.. mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.* ..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1.....r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.' .*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h.P.vY.....S.5.6.C4..E.Y.|.....).zs...w.gl..\.G..J.M.vES.0....P.:..6..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:FcBO8:m48
MD5:	E471DF101ED8DA84A64E823BF7403022
SHA1:	339749BEE39C1AA31386305E2218344B50D106A8
SHA-256:	DA4A09868C322C15D6042F046B60E1FC57D96A1AD055DF1CD79C114B1849C3A3
SHA-512:	3BF4945E5AECCAF5C82671755B152B797B516D527DC0E58F5FCBD9CD755837D41AAA88B99D4433F086EDF024D8A1FB59D14880920645A2E66FBED7DE74B2D6 5
Malicious:	**true**
Preview:	 ..9.q+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	662016
Entropy (8bit):	7.9894013878846275
Encrypted:	false
SSDEEP:	12288:ETQ2c25dc9wH6UvJF0nvekN2rDerJDTQsKlU9JDAccU7jYUL1Xk:52oWksqla711Xk
MD5:	8E87DE15CD3DA1245B9C7B0E48C0F126
SHA1:	80830909EC859ED61811329AE16888CB87E1ED5F
SHA-256:	EC850202F17A8E7F5A04603E9C70AB21D7B39FB3142A79098AEF1D592974702E
SHA-512:	236BDCAE21D29DF979BFEDF650B23FEA04BEBABD4EB79B172D9E4AC2A602494727338E3937C9F9F371DBF0FF78E457BEE138C9A7FDE6351ED9A205888E4EA44A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.*.....0..... ... .@.. .....`..... ..@.....K.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....x7.../.....:...xf.....{....*J8....*..}....8.....{....*6..}....8....*..z8....*..(....8.....(....8.....&~.....*...~....*...{. ...*6..}....8....*....{....*J8....*..}....8.....z8.....(....8.....(....8....*.&~.....*...~....*...{....*6..}....8....*....{....*6..}....8....*..f..(....8....*..(....8.....&~.....*...~....*...{....*J8....*..}....8.....{... .*J8....*..}....8.....z8.....(....8.....(....8....*.&~.....*...~..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe:Zone.Identifier	
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210609\PowerShell_transcript.585948.u328TzvM.20210609111113.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5985
Entropy (8bit):	5.402422714094943
Encrypted:	false
SSDEEP:	96:BZ2uhTN/iqDo1Zog/ZhhTN/iqDo1ZlQ6ljZrhTN/iqDo1Zf944NZq:Y
MD5:	05A8E500125FEEE93AADE0A7C34094DB
SHA1:	1A03B7A62033BBB1E5EF38CEA7690AA6E1FFB108
SHA-256:	2AF2DEBB3DC2A0EF09C5B8598B4A87B8CF88DA50B9A863B31953AD8E43898A73
SHA-512:	DEA849ECC102B52C931BAEA33FC8F46E786CCFEA400187F99D91CA3D909AC360CCFBD67FB94D0B003D98198235335816770 1F6705F1195F7B8555226EFFE7DA
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210609111125..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\,'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe'..Process ID: 3016..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210609111125..**********..PS>Add-MpPreference -ExclusionPath C:\,'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe'..**********..Windows PowerShell transcript st

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9894013878846275
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:	ZVFVY7NwZ7.exe
File size:	662016
MD5:	8e87de15cd3da1245b9c7b0e48c0f126
SHA1:	80830909ec859ed61811329ae16888cb87e1ed5f
SHA256:	ec850202f17a8e7f5a04603e9c70ab21d7b39fb3142a79098aef1d592974702e
SHA512:	236bdcae21d29df979bfedf650b23fea04bebabd4eb79b172d9e4ac2a602494727338e3937c9f9f371dbf0ff78e457bee138c9a7fde6351ed9a205888e4ea44a
SSDEEP:	12288:ETQ2c25dc9wH6UvJF0nvekN2rDerJDTQsKIU9JDAccU7jYUL1Xk:52oWksqla711Xk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.*.....0..... ... .@.. ..... `.....@.....

File Icon

Icon Hash:	10b060d8e070b000

Static PE Info

General

Entrypoint:	0x4a1eee
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xBF2AF027 [Thu Aug 20 02:10:47 2071 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	0x9fef4	0xa0000	False	0.990547180176	data	7.99463093072	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x15f8	0x1600	False	0.431640625	data	5.40076952317	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	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
06/09/21-11:11:14.736138	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:21.395950	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:28.259042	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:35.554623	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:42.576920	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:49.577258	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	1144	192.168.2.3	79.134.225.90
06/09/21-11:11:56.550233	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1144	192.168.2.3	79.134.225.90
06/09/21-11:12:03.578127	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1144	192.168.2.3	79.134.225.90
06/09/21-11:12:09.564033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1144	192.168.2.3	79.134.225.90

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 11:11:13.707573891 CEST	192.168.2.3	8.8.8.8	0x391c	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:21.126924038 CEST	192.168.2.3	8.8.8.8	0xe1db	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:27.948843002 CEST	192.168.2.3	8.8.8.8	0xa73c	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:35.313149929 CEST	192.168.2.3	8.8.8.8	0xef12	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:42.301753998 CEST	192.168.2.3	8.8.8.8	0x78a5	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:49.292023897 CEST	192.168.2.3	8.8.8.8	0xa26	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:56.291692019 CEST	192.168.2.3	8.8.8.8	0x6bc6	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:12:03.304757118 CEST	192.168.2.3	8.8.8.8	0x873c	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)
Jun 9, 2021 11:12:09.290930986 CEST	192.168.2.3	8.8.8.8	0x2439	Standard query (0)	wekeepworking.sytes.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 11:11:13.751946926 CEST	8.8.8.8	192.168.2.3	0x391c	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:21.173408031 CEST	8.8.8.8	192.168.2.3	0xe1db	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:27.993294001 CEST	8.8.8.8	192.168.2.3	0xa73c	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:35.358407021 CEST	8.8.8.8	192.168.2.3	0xef12	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:42.344507933 CEST	8.8.8.8	192.168.2.3	0x78a5	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:49.336129904 CEST	8.8.8.8	192.168.2.3	0xa26	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:11:56.336420059 CEST	8.8.8.8	192.168.2.3	0x6bc6	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:12:03.352278948 CEST	8.8.8.8	192.168.2.3	0x873c	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)
Jun 9, 2021 11:12:09.334048033 CEST	8.8.8.8	192.168.2.3	0x2439	No error (0)	wekeepworking.sytes.net		79.134.225.90	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ZVFVY7NwZ7.exe PID: 2220 Parent PID: 5828

General

Start time:	11:10:05
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\ZVFVY7NwZ7.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ZVFVY7NwZ7.exe'
Imagebase:	0x980000
File size:	662016 bytes
MD5 hash:	8E87DE15CD3DA1245B9C7B0E48C0F126
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: 00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.335459284.0000000003E69000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.333737756.0000000002E9F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.333737756.0000000002E9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.335651817.0000000003EFF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.335651817.0000000003EFF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.335651817.0000000003EFF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.337200878.00000000040C3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.337200878.00000000040C3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.337200878.00000000040C3000.00000004.00000001.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 Modified

Analysis Process: wscript.exe PID: 1784 Parent PID: 2220

General

Start time:	11:11:05
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp_Lzqtfofnnzmk.vbs'
Imagebase:	0x940000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: ZVFVY7NwZ7.exe PID: 5612 Parent PID: 2220

General

Start time:	11:11:06
Start date:	09/06/2021
Path:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\ZVFVY7NwZ7.exe
Imagebase:	0xa40000
File size:	662016 bytes
MD5 hash:	8E87DE15CD3DA1245B9C7B0E48C0F126
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: 0000000D.00000002.484283906.0000000006400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484283906.0000000006400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.331387954.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.331387954.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.331387954.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484696296.0000000006740000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484696296.0000000006740000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484800150.0000000006790000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484800150.0000000006790000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484337930.0000000006420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484337930.0000000006420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.331849695.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.331849695.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.331849695.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.475975321.0000000002E91000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.475975321.0000000002E91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484498956.0000000006480000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484498956.0000000006480000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484317113.0000000006410000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484317113.0000000006410000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.469794004.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.469794004.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.469794004.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484473522.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484473522.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.481077983.0000000004080000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.482916804.0000000005420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.482916804.0000000005420000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484017800.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484017800.0000000006040000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484414885.0000000006450000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484414885.0000000006450000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484531579.0000000006490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484531579.0000000006490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.484531579.0000000006490000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.483489458.0000000005670000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.483489458.0000000005670000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.484260372.00000000063F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.484260372.00000000063F0000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 3016 Parent PID: 1784

General

Start time:	11:11:07
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath C:\,'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\chromee\chromee.exe'
Imagebase:	0x2c0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4180 Parent PID: 3016

General

Start time:	11:11:07
Start date:	09/06/2021
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

Disassembly

Code Analysis