ID: 831166
Sample Name: RFQ_31362.exe
Cookbook: default.jbs
Time: 07:26:09
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

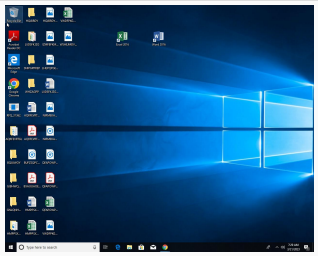
Windows Analysis Report

RFQ_31362.exe

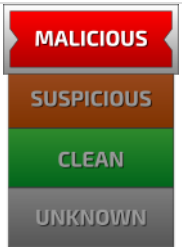
Overview

General Information

Sample Name:	RFQ_31362.exe
Analysis ID:	831166
MD5:	c3c291b38d05…
SHA1:	86411ff9d41eb…
SHA256:	9fcf0a498b86fc…
Tags:	AveMariaRAT exe RAT
Infos:	



Detection



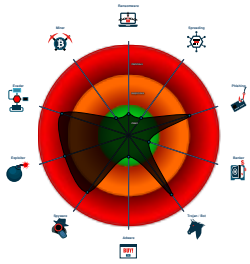
AveMaria, UACMe

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected UACMe UAC Bypass…
- Yara detected AveMaria stealer
- Snort IDS alert for network traffic
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- Increases the number of concurrent…
- Contains functionality to hide user a…
- Machine Learning detection for sam…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- RFQ_31362.exe (PID: 1964 cmdline: C:\Users\user\Desktop\RFQ_31362.exe MD5: C3C291B38D054D5E71FE17A10D737249)
  - powershell.exe (PID: 5228 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\RFQ_31362.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RFQ_31362.exe (PID: 2300 cmdline: C:\Users\user\Desktop\RFQ_31362.exe MD5: C3C291B38D054D5E71FE17A10D737249)
    - cmd.exe (PID: 4272 cmdline: C:\Windows\System32\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Ave Maria, AveMariaRAT, avemaria	Information stealer which uses AutoIT for wrapping.	• Anunak	**http://** blog.morphisec.com/threat-alert-ave-maria-infostealer-on-the-rise-with-new-stealthier-deliveryhttps://asec.ahnlab.com/en/36629/https://blog.morphisec.com/syk-crypter-discordhttps://blog.talosintelligence.com/2020/09/salfram-robbing-place-without-removing.htmlhttps://blog.talosintelligence.com/2020/12/2020-year-in-malware.html	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria

Name	Description	Attribution	Blogpost URLs	Link
UACMe	A toolkit maintained by hfiref0x which incorporates numerous UAC bypass techniques for Windows 7 - Windows 10. Typically, components of this tool are stripped out and reused by malicious actors.	No Attribution	**http://** https://securelist.com/scarcruft-continues-to-evolve-introduces-bluetooth-harvester/90729/https://github.com/hfiref0x/UACME	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.uacme

Malware Configuration

Threatname: AveMaria


```
{
  "C2 url": "panchak.duckdns.org",
  "port": 5050
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.510449817.000000000054F000.00000040.00000400.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth (Nextron Systems)	• 0xdf0:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0xdf0:$c1: Elevation:Administrator!new:
0000000C.00000002.510449817.000000000054F000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth (Nextron Systems)	• 0x150e8:$a1: \Opera Software\Opera Stable\Login Data • 0x15410:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x14d58:$a3: \Google\Chrome\User Data\Default\Login Data
0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AveMaria	Yara detected AveMaria stealer	Joe Security	
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.3.RFQ_31362.exe.12087c0.6.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth (Nextron Systems)	• 0x5f8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
12.3.RFQ_31362.exe.12087c0.6.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth (Nextron Systems)	• 0x5f8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x5f8:$c1: Elevation:Administrator!new: • 0x3400:$c1: Elevation:Administrator!new:
12.3.RFQ_31362.exe.12087c0.6.unpack	JoeSecurity_UACMe	Yara detected UACMe UAC Bypass tool	Joe Security	
12.3.RFQ_31362.exe.12087c0.2.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth (Nextron Systems)	• 0x5f8:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
12.3.RFQ_31362.exe.12087c0.2.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth (Nextron Systems)	• 0x5f8:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x3400:$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} • 0x5f8:$c1: Elevation:Administrator!new: • 0x3400:$c1: Elevation:Administrator!new:
Click to see the 30 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Ave Maria/Warzone RAT BeaconResponse - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502852327 03/21/23-07:28:20.459629
SID:	2852327
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsCommand - Source IP: 193.42.33.160 - Destination IP: 192.168.2.3

Timestamp:	193.42.33.160192.168.2.35050496982852330 03/21/23-07:28:21.036418
SID:	2852330
Source Port:	5050
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 193.42.33.160 - Destination IP: 192.168.2.3

Timestamp:	193.42.33.160192.168.2.35050496982036735 03/21/23-07:28:20.393972
SID:	2036735
Source Port:	5050
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502036734 03/21/23-07:28:20.459629
SID:	2036734
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT PingResponse - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502852328 03/21/23-07:28:41.267270
SID:	2852328
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT RemoteModuleLoadResponse - Source IP: 193.42.33.160 - Destination IP: 192.168.2.3

Timestamp:	193.42.33.160192.168.2.35050496982852335 03/21/23-07:28:21.246341
SID:	2852335
Source Port:	5050
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT InitializePacket - Source IP: 193.42.33.160 - Destination IP: 192.168.2.3

Timestamp:	193.42.33.160192.168.2.35050496982852326 03/21/23-07:29:04.187918
SID:	2852326
Source Port:	5050
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT DownloadAndExecuteCommand - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502852332 03/21/23-07:28:21.039150
SID:	2852332
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsResponse - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502852331 03/21/23-07:28:25.813962
SID:	2852331
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT PingCommand - Source IP: 193.42.33.160 - Destination IP: 192.168.2.3

Timestamp:	193.42.33.160192.168.2.35050496982852329 03/21/23-07:28:41.266781
SID:	2852329
Source Port:	5050
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Ave Maria/Warzone RAT VNCGetModule - Source IP: 192.168.2.3 - Destination IP: 193.42.33.160

Timestamp:	192.168.2.3193.42.33.160469850502852334 03/21/23-07:28:21.039150
SID:	2852334
Source Port:	49698
Destination Port:	5050
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Machine Learning detection for sample

Exploits

Yara detected UACMe UAC Bypass tool

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected AveMaria stealer

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings

Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information

Yara detected AveMaria stealer

Tries to steal Mail credentials (via file / registry access)

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

Remote Access Functionality

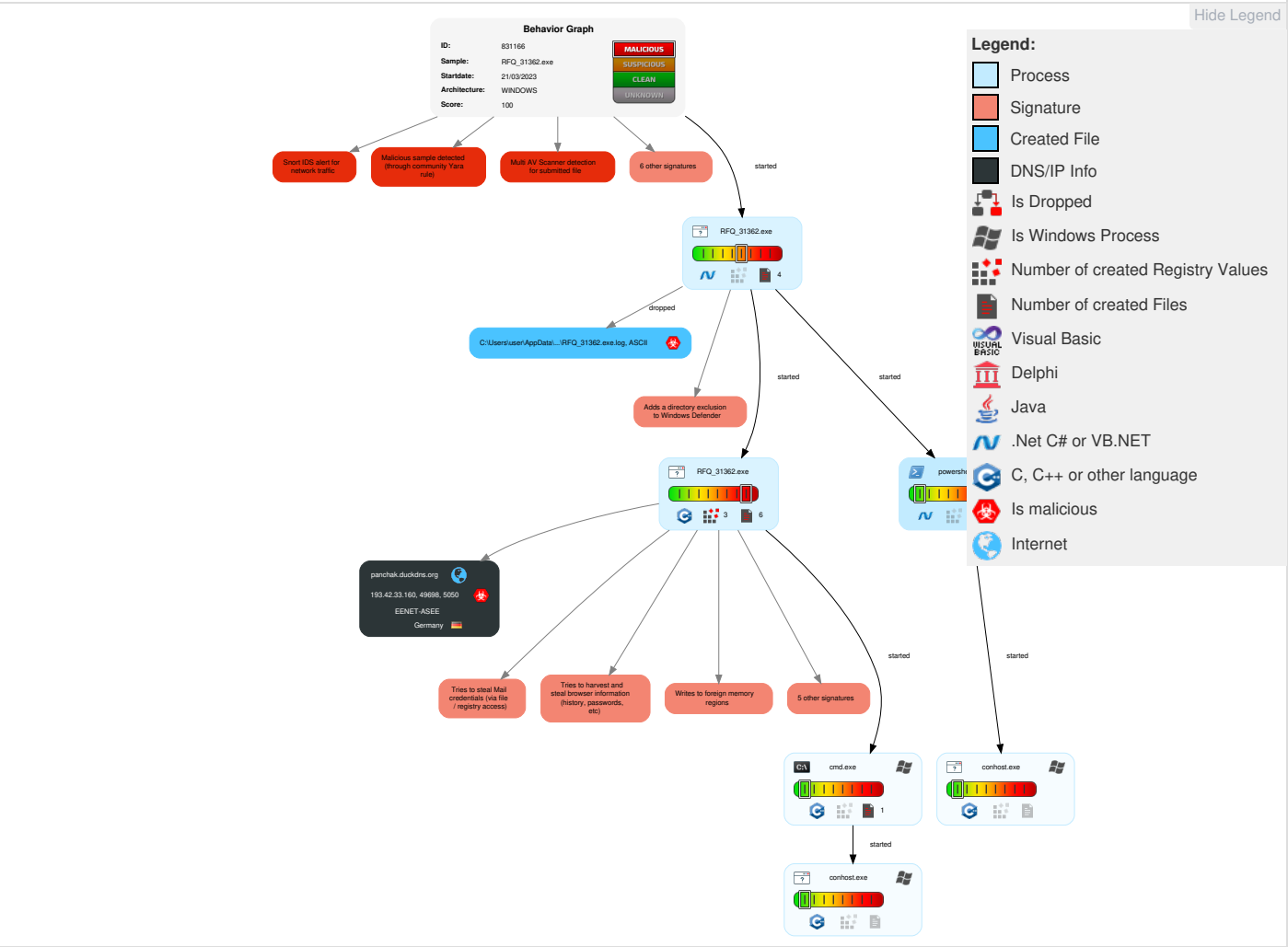
Yara detected AveMaria stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	3 1 2 Process Injection	3 Masquerading	1 OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Endpoint Denial of Service
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Disable or Modify Tools	1 1 1 Input Capture	2 Process Discovery	Remote Desktop Protocol	1 1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	2 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Users	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
RFQ_31362.exe	28%	ReversingLabs	Win32.Trojan.Generic	
RFQ_31362.exe	30%	Virustotal		Browse
RFQ_31362.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.RFQ_31362.exe.400000.1.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
panchak.duckdns.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
panchak.duckdns.org	193.42.33.160	true	true		unknown

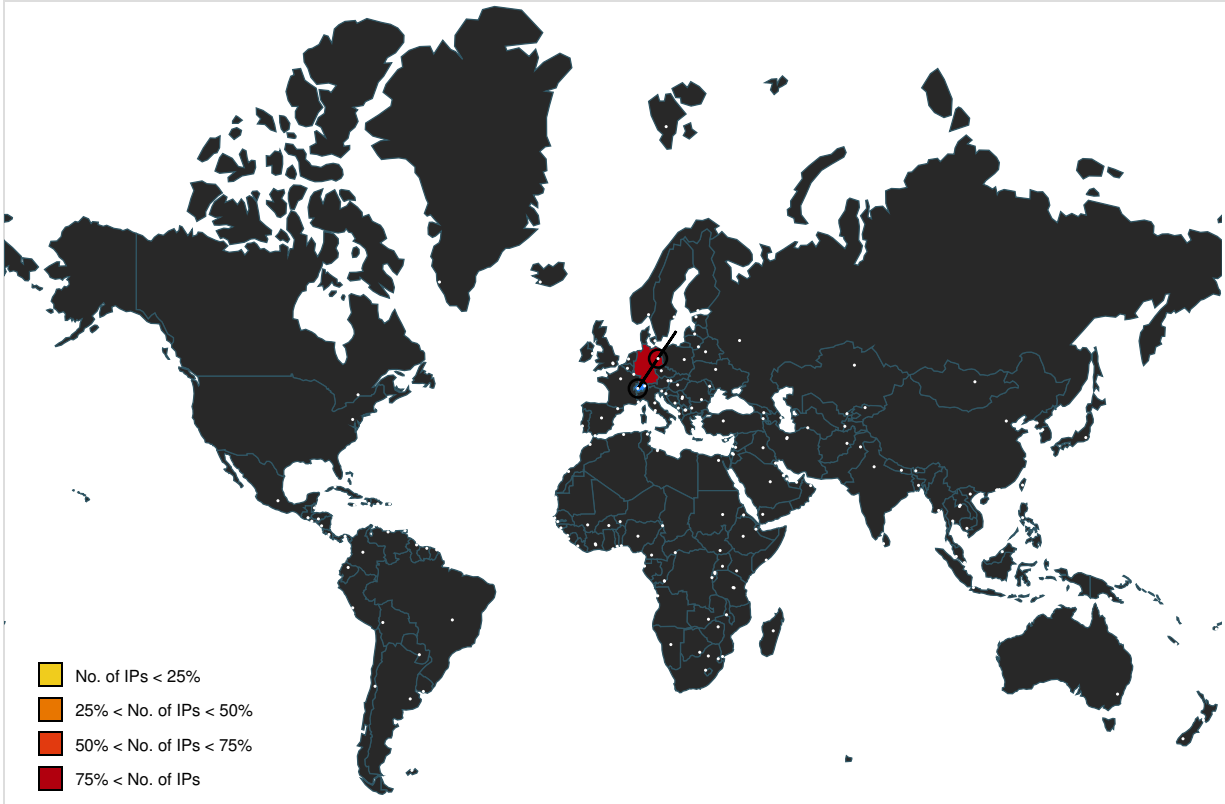
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
panchak.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/syohex/java-simple-mine-sweeperC:	RFQ_31362.exe, 0000000C.00000002.5104498 17.0000000000400000.00000040.00000400.00 020000.00000000.sdmp, RFQ_31362.exe, 000 0000C.00000003.405873618.00000000011FA00 0.00000004.00000020.00020000.00000000.sdmp, RFQ_31362.exe, 0000000C.00000003.406 416749.00000000011F5000.00000004.0000002 0.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs						
IP	**Domain**	**Country**	**Flag**	**ASN**	**ASN Name**	**Malicious**
193.42.33.160	panchak.duckdns.org	Germany		3221	EENET-ASEE	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831166
Start date and time:	2023-03-21 07:26:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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
Sample file name:	RFQ_31362.exe
Detection:	MAL
Classification:	mal100.phis.troj.spyw.expl.evad.winEXE@9/6@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 81% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:28:14	API Interceptor	1x Sleep call for process: RFQ_31362.exe modified
07:28:16	API Interceptor	26x Sleep call for process: powershell.exe modified
07:28:19	API Interceptor	402x Sleep call for process: cmd.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ_31362.exe.log

Process:	C:\Users\user\Desktop\RFQ_31362.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	21952
Entropy (8bit):	5.597899480556724
Encrypted:	false
SSDEEP:	384:8tCRdM07+eANV8M27bynHSBxn0uhbiV9gpSJ3uyVQ+m021AVrd/+7OA+ifYb:zAJ27AH4x0uhbpcuWXtb
MD5:	BB89DC902E4077587FAB7D3C7D4184EA
SHA1:	0936AC18F194EA069D74D3B2330D967F0DD858D4
SHA-256:	5620FABE4F1498BDA6CC3D5A1B235327377338D8E81A5829A4450CD7F2FFF43E
SHA-512:	FBD9AD13DD578094022CD47512C3FB4C1B16A4CD1D8C6F349CE37AEBDDDA0F2B166B7A0DFABF5B8A85B25AAEB064A9F1B7404A27B533828815D5295B5E52367A

Malicious:	false
Reputation:	low
Preview:	@...e.....(....._.Q.F.$...9.y.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'...L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qyfxnjpd.w3d.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rbm4cgs3.iyc.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
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\rEJHIjC.tmp

Process:	C:\Users\user\Desktop\RFQ_31362.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Roaming\yrqKmyp.tmp	
Process:	C:\Users\user\Desktop\RFQ_31362.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	61356
Entropy (8bit):	6.071946363928989
Encrypted:	false
SSDEEP:	1536:kX71LMtANJaRBOHK5KvtgBhqQ0HTgHImA01exhi8qjyDKly2:g711NyBTOgd0HhmAnhqj3L
MD5:	A4F10AC4E9DF2BEBE496AE2386BC7B8C
SHA1:	2D457ECEAA0501744A3A0E86436C435A2973C5EE
SHA-256:	BAED8CDB4BE43EBABE614B0ED48D042F0C8B80D834995284144F808579FDB55B
SHA-512:	FA6203B19B3CFAA2BF4B6DA732DF340AA59B91AF3979CFB8A7FA3D2E7834656A7843755967390BD46DB96052AE6DF0F8F2CA7FC90CE23A60C12ABD37D7FDC252
Malicious:	false
Preview:	{"browser":{"last_redirect_origin":"","last_whats_new_version":104,"shortcut_migration_version":"104.0.5112.81"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"invalidation":{"per_sender_topics_to_handler":{}},"legacy":{"profile":{"name":{"migrated":true}}},"management":{"platform":{"azure_active_directory":0,"enterprise_mdm_win":0}},"network_time":{"network_time_mapping":{"local":1.660685744940254e+12,"network":1.660653319e+12,"ticks":922844395.0,"uncertainty":1339796.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAABL95WKt94zTZq03WydzHLcAAAAAAIAAAAAABBmAAAAAQAAIAAAABAL2tyan+lsWtxhoUVdUYrYiwg8iJkppNr2ZbBFie9UAAAAAA6AAAAAAgAAIAAAABDv4gjLq1dOS7lkRG21YVXojnHhsRhNbP8/D1zs78mXMAAAAB045Od5v4BxiFP4bdRYJjDXn4W2fxYqQj2xfYeAnS1vCL4JXAsdfljw4oXIE4R7l0AAAABlt36FqChftM9b7EtaPw98XRX5Y944rq1WsGWcOPFyXOajfBL3GXBUhMXghJbDGb5WCu+JEdxa

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4286325944521066
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:	RFQ_31362.exe
File size:	865280
MD5:	c3c291b38d054d5e71fe17a10d737249
SHA1:	86411ff9d41eb140c80753873b943d80be323130
SHA256:	9fcf0a498b86fc20af3cc28a984135f0cc202f6577af79f96ec63ca6cb227c3c
SHA512:	3b1b4f937b51d6bef403e44cc4b92ab52c0c5e2b7b503aea46030e9f5f058f77a5b9266c24565bfe18671e666b701c097dac3df089621ec8572f277415f2cdf6
SSDEEP:	12288:2nmIb3fNeH++znVXoW87FqKqi13U3mWxw7DG0mCuT7Yeg4firr:2m03fY+WnVX18BqBAU3e5mnn3
TLSH:	EF0508425EBB5085E8B70F2C547B76880B34E953BEC9903B7CC9B61A4FFA69364063D1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....d.....0..*.....I... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d490e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x64191306 [Tue Mar 21 02:14:30 2023 UTC]
TLS Callbacks:	

CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd48c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x5d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd4882	0x1c	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd2914	0xd2a00	False	0.7573778282640949	SysEx File - Victor	7.432792399181768	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x5d8	0x600	False	0.4309895833333333	data	4.1609318281960155	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd60a0	0x34c	data		
RT_MANIFEST	0xd63ec	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

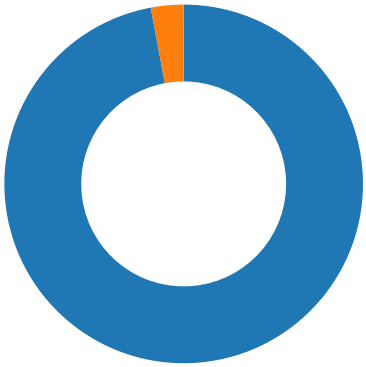
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.42.33.160 4969850502852327 03/21/23-07:28:20.459629	TCP	2852327	ETPRO TROJAN Ave Maria/Warzone RAT BeaconResponse	49698	5050	192.168.2.3	193.42.33.160
193.42.33.160192.168.2.3 5050496982852330 03/21/23-07:28:21.036418	TCP	2852330	ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsCommand	5050	49698	193.42.33.160	192.168.2.3
193.42.33.160192.168.2.3 5050496982036735 03/21/23-07:28:20.393972	TCP	2036735	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	5050	49698	193.42.33.160	192.168.2.3
192.168.2.3193.42.33.160 4969850502036734 03/21/23-07:28:20.459629	TCP	2036734	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin	49698	5050	192.168.2.3	193.42.33.160
192.168.2.3193.42.33.160 4969850502852328 03/21/23-07:28:41.267270	TCP	2852328	ETPRO TROJAN Ave Maria/Warzone RAT PingResponse	49698	5050	192.168.2.3	193.42.33.160
193.42.33.160192.168.2.3 5050496982852335 03/21/23-07:28:21.246341	TCP	2852335	ETPRO TROJAN Ave Maria/Warzone RAT RemoteModuleLoadResponse	5050	49698	193.42.33.160	192.168.2.3
193.42.33.160192.168.2.3 5050496982852326 03/21/23-07:29:04.187918	TCP	2852326	ETPRO TROJAN Ave Maria/Warzone RAT InitializePacket	5050	49698	193.42.33.160	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.42.33.160 4969850502852332 03/21/23-07:28:21.039150	TCP	2852332	ETPRO TROJAN Ave Maria/Warzone RAT DownloadAndExecuteCommand	49698	5050	192.168.2.3	193.42.33.160
192.168.2.3193.42.33.160 4969850502852331 03/21/23-07:28:25.813962	TCP	2852331	ETPRO TROJAN Ave Maria/Warzone RAT ListPasswordsResponse	49698	5050	192.168.2.3	193.42.33.160
193.42.33.160192.168.2.3 5050496982852329 03/21/23-07:28:41.266781	TCP	2852329	ETPRO TROJAN Ave Maria/Warzone RAT PingCommand	5050	49698	193.42.33.160	192.168.2.3
192.168.2.3193.42.33.160 4969850502852334 03/21/23-07:28:21.039150	TCP	2852334	ETPRO TROJAN Ave Maria/Warzone RAT VNCGetModule	49698	5050	192.168.2.3	193.42.33.160

Network Port Distribution



Total Packets: 34

- 53 (DNS)
- 5050 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:28:19.142501116 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:19.174215078 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:19.174313068 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:20.393971920 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:20.459629059 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:20.552443981 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:20.552617073 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:20.652137041 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.036417961 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.039150000 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.152304888 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246340990 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246397972 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246442080 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246484041 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246526003 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246566057 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246591091 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.246608973 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246651888 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246660948 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.246715069 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246726990 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.246758938 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.246845007 CET	49698	5050	192.168.2.3	193.42.33.160

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:28:21.277149916 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277200937 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277246952 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277291059 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277302027 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277338982 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277343988 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277384996 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277430058 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277439117 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277498007 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277544022 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277558088 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277589083 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277636051 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277647018 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277683020 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277728081 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277736902 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277775049 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277820110 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277832985 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277867079 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277915001 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.277925014 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.277961016 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.278007984 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.278017044 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.278059006 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.278112888 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308291912 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308355093 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308402061 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308445930 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308449030 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308512926 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308515072 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308566093 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308614969 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308625937 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308662891 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308708906 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308734894 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308756113 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308804989 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308820963 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308851957 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308898926 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308906078 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.308944941 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308990955 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.308996916 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309039116 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309084892 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309114933 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309130907 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309178114 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309202909 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309226990 CET	5050	49698	193.42.33.160	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:28:21.309272051 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309314013 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309317112 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309365988 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309381962 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309412003 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309459925 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309478045 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309508085 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309556961 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309570074 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309604883 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309652090 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309684992 CET	49698	5050	192.168.2.3	193.42.33.160
Mar 21, 2023 07:28:21.309699059 CET	5050	49698	193.42.33.160	192.168.2.3
Mar 21, 2023 07:28:21.309746027 CET	5050	49698	193.42.33.160	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:28:18.979588032 CET	62704	53	192.168.2.3	8.8.8.8
Mar 21, 2023 07:28:19.090074062 CET	53	62704	8.8.8.8	192.168.2.3

DNS Queries

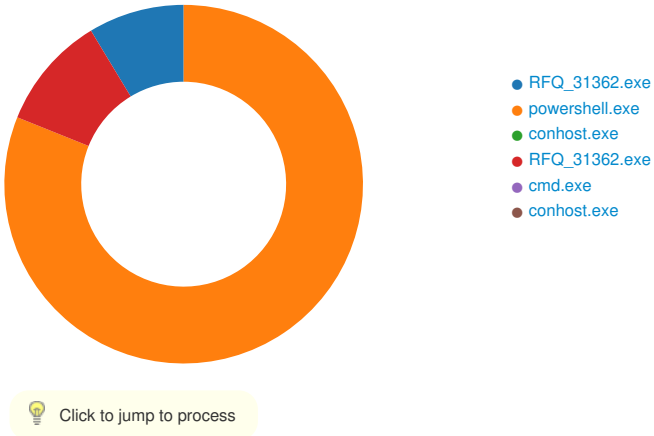
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 07:28:18.979588032 CET	192.168.2.3	8.8.8.8	0x4e01	Standard query (0)	panchak.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 07:28:19.090074062 CET	8.8.8.8	192.168.2.3	0x4e01	No error (0)	panchak.duckdns.org		193.42.33.160	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: RFQ_31362.exe PID: **1964**, Parent PID: **3452**

General

Target ID:	0
Start time:	07:27:01
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\RFQ_31362.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ_31362.exe
Imagebase:	0x270000
File size:	865280 bytes
MD5 hash:	C3C291B38D054D5E71FE17A10D737249
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Analysis Process: powershell.exe PID: **5228**, Parent PID: **1964**

General

Target ID:	10
Start time:	07:28:14
Start date:	21/03/2023
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:\Users\user\Desktop\RFQ_31362.exe
Imagebase:	0x9e0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71745B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qyfxnjpd.w3d.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rbm4cgs3.iyc.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	717E1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qyfxnjpd.w3d.ps1	success or wait	1	717E6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rbm4cgs3.iyc.psm1	success or wait	1	717E6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	16	19	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	35	21	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	56	16	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	72	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	80	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	89	8	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
unknown	97	9	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71745B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_qyfxnjpd.w3d.ps1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_rbm4cgs3.iyc.psm1	0	1	31	1	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 28 14 00 00 19 00 00 00 fd 0e 5f 06 51 08 46 08 24 08 00 00 39 01 79 00 0b 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e(_QF$9y@	success or wait	1	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	72C676FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	72C676FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 09 06 fd 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 09 0c fd 00 21 4d 40 01 58 64 40 01 56 64 40 01 fd 2a 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40	T@>@@V@H@X@#)@\d@Zd@[d@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@ M@!M@Xd@Vd@*@;M@D@D@@M@<M@$M@8M@?M@;@;@;@<@	success or wait	11	72C676FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7297CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72981F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22416	success or wait	1	7298203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	142	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	717E1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72975705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: conhost.exe PID: **2092**, Parent PID: **5228**

General

Target ID:	11
Start time:	07:28:15

Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RFQ_31362.exe PID: **2300**, Parent PID: **1964**

General

Target ID:	12
Start time:	07:28:15
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\RFQ_31362.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ_31362.exe
Imagebase:	0x940000
File size:	865280 bytes
MD5 hash:	C3C291B38D054D5E71FE17A10D737249
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000002.510449817.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000002.510449817.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_RegKeyComb_IExecuteCommandCOM, Description: Detects executables embedding command execution via IExecuteCommand COM object, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_WarzoneRAT, Description: Detects AveMaria/WarzoneRAT, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: AveMaria_WarZone, Description: unknown, Source: 0000000C.00000002.510449817.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.406416749.00000000011F5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.406416749.00000000011F5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 0000000C.00000003.406416749.00000000011F5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 0000000C.00000003.405873618.00000000011FA000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 0000000C.00000003.405873618.00000000011FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000003.405873618.00000000011FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000C.00000003.405873618.00000000011FA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 0000000C.00000003.405873618.00000000011FA000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4135ED	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	402E05	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft Vision\21-03-2023_07.28.20	read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	1	408932	CreateFileW
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	40C5C5	CopyFileW
C:\Users\user\AppData\Roaming\yrqKmyp.tmp	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	40C5D1	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yrqKmyp.tmp	success or wait	1	40FF18	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	0	49152	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 17 00 00 00 00 00 00 00 00 00 00 00 19 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 5b 35 05 00 00 00 01 07 fd 00 00 00 00 10 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .[5	success or wait	1	40C5C5	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yrqKmyp.tmp	0	61356	7b 22 62 72 6f 77 73 65 72 22 3a 7b 22 6c 61 73 74 5f 72 65 64 69 72 65 63 74 5f 6f 72 69 67 69 6e 22 3a 22 22 2c 22 6c 61 73 74 5f 77 68 61 74 73 5f 6e 65 77 5f 76 65 72 73 69 6f 6e 22 3a 31 30 34 2c 22 73 68 6f 72 74 63 75 74 5f 6d 69 67 72 61 74 69 6f 6e 5f 76 65 72 73 69 6f 6e 22 3a 22 31 30 34 2e 30 2e 35 31 31 32 2e 38 31 22 7d 2c 22 64 61 74 61 5f 75 73 65 5f 6d 65 61 73 75 72 65 6d 65 6e 74 22 3a 7b 22 64 61 74 61 5f 75 73 65 64 22 3a 7b 22 73 65 72 76 69 63 65 73 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 2c 22 75 73 65 72 22 3a 7b 22 62 61 63 6b 67 72 6f 75 6e 64 22 3a 7b 7d 2c 22 66 6f 72 65 67 72 6f 75 6e 64 22 3a 7b 7d 7d 7d 2c 22 68 61 72 64 77 61 72 65 5f 61 63 63 65 6c 65 72	{"browser": {"last_redirect_origin":"","last_whats_new_version":104,"shortcut_migration_version":"104.0.5112.81"},"data_use_measurement": {"data_used":{"services": {"background":{},"foreground":{}},"user": {"background": {},"foreground":{}}}},"hardware_acceler	success or wait	1	40C5D1	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\RFQ_31362.exe	unknown	865280	success or wait	1	411E78	ReadFile
C:\Users\user\Desktop\RFQ_31362.exe	unknown	865280	success or wait	1	411E78	ReadFile
C:\Windows\SysWOW64\user32.dll	unknown	1626536	success or wait	1	411E78	ReadFile
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	unknown	100	success or wait	1	49F7887	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	61356	success or wait	1	40CC2B	ReadFile
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	unknown	2048	success or wait	1	49F7887	ReadFile
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	unknown	2048	success or wait	1	49F7887	ReadFile
C:\Users\user\AppData\Roaming\rEJHIjC.tmp	unknown	2048	success or wait	1	49F7887	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\6POVCP500L	success or wait	1	410F94	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	413550	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	413565	RegSetValueExA

Analysis Process: cmd.exe

PID: **4272**, Parent PID: **2300**

General

Target ID:	13
Start time:	07:28:17
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\System32\cmd.exe
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1916**, Parent PID: **4272**

General

Target ID:	14
Start time:	07:28:17
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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

No disassembly