ID: 431672
Sample Name: #RFQ ORDER484475577797.exe
Cookbook: default.jbs
Time: 06:00:18
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report #RFQ ORDER484475577797.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 6
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: 7
Networking: 7
E-Banking Fraud: 7
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 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 19
General 19
File Icon 19
Static PE Info 20
General 20
Entrypoint Preview 20
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Network Behavior 20
Network Port Distribution 20
TCP Packets 20
Code Manipulations 20
Statistics 20
Behavior 20

System Behavior 21
Analysis Process: #RFQ ORDER484475577797.exe PID: 4364 Parent PID: 5700 21
General 21
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: powershell.exe PID: 5616 Parent PID: 4364 21
General 21
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: conhost.exe PID: 4884 Parent PID: 5616 22
General 22
Analysis Process: powershell.exe PID: 6052 Parent PID: 4364 22
General 22
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Analysis Process: conhost.exe PID: 5460 Parent PID: 6052 23
General 23
Analysis Process: schtasks.exe PID: 5728 Parent PID: 4364 23
General 23
File Activities 23
File Read 23
Analysis Process: conhost.exe PID: 5916 Parent PID: 5728 23
General 23
Analysis Process: powershell.exe PID: 3292 Parent PID: 4364 23
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Analysis Process: conhost.exe PID: 1968 Parent PID: 3292 24
General 24
Analysis Process: #RFQ ORDER484475577797.exe PID: 1048 Parent PID: 4364 24
General 24
Disassembly 26
Code Analysis 26

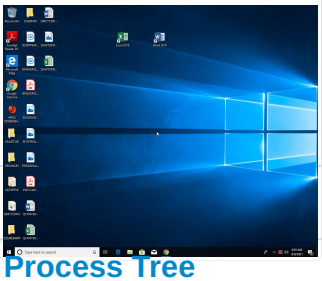
Analysis Report #RFQ ORDER484475577797.exe

Overview

General Information

Sample Name:	#RFQ ORDER484475577797.exe
Analysis ID:	431672
MD5:	18e38261e8ea6a..
SHA1:	bbfaf42987014ba..
SHA256:	3cb5c285d5e7f16..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

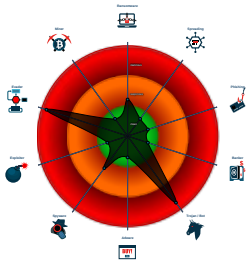
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- #RFQ ORDER484475577797.exe (PID: 4364 cmdline: 'C:\Users\user\Desktop\#RFQ ORDER484475577797.exe' MD5: 18E38261E8EA6AE0077C5448F809CCB6)
  - powershell.exe (PID: 5616 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\#RFQ ORDER484475577797.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6052 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5728 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LNSXWuepjsOA' /XML 'C:\Users\user\AppData\Local\Temp\tmp5439.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 3292 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - #RFQ ORDER484475577797.exe (PID: 1048 cmdline: C:\Users\user\Desktop\#RFQ ORDER484475577797.exe MD5: 18E38261E8EA6AE0077C5448F809CCB6)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "44a4f7d4-4e07-4399-aab5-6ba6b60e",
  "Group": "bb",
  "Domain1": "194.5.98.120",
  "Domain2": "joseedward5001.ddns.net",
  "Port": 1604,
  "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
0000000A.00000002.494989235.000000000653 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
0000000A.00000002.494989235.000000000653 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
00000000.00000002.234685013.000000000261 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000A.00000002.491944391.000000000448 3000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x55dd7:$a: NanoCore • 0x55ec1:$a: NanoCore • 0x56d38:$a: NanoCore • 0x5fee2:$a: NanoCore • 0x5ff43:$a: NanoCore • 0x5ff86:$a: NanoCore • 0x5ffc6:$a: NanoCore • 0x60202:$a: NanoCore • 0x602a2:$a: NanoCore • 0x60a7a:$a: NanoCore • 0x6106d:$a: NanoCore • 0x611be:$a: NanoCore • 0x62018:$a: NanoCore • 0x6227f:$a: NanoCore • 0x62294:$a: NanoCore • 0x622b3:$a: NanoCore • 0x6b1b6:$a: NanoCore • 0x6b1df:$a: NanoCore • 0x76f58:$a: NanoCore • 0x76f81:$a: NanoCore • 0x9be44:$a: NanoCore

Source	Rule	Description	Author	Strings
0000000A.00000002.484331798.0000000002C1C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x7aa6a:$a: NanoCore • 0x7aa8f:$a: NanoCore • 0x7aae8:$a: NanoCore • 0x8accf:$a: NanoCore • 0x8acf5:$a: NanoCore • 0x8ad51:$a: NanoCore • 0x97beb:$a: NanoCore • 0x97c44:$a: NanoCore • 0x97c77:$a: NanoCore • 0x97ea3:$a: NanoCore • 0x97f1f:$a: NanoCore • 0x98538:$a: NanoCore • 0x98681:$a: NanoCore • 0x98b55:$a: NanoCore • 0x98e3c:$a: NanoCore • 0x98e53:$a: NanoCore • 0xa1d37:$a: NanoCore • 0xa1db3:$a: NanoCore • 0xa4696:$a: NanoCore • 0xa9ca1:$a: NanoCore • 0xa9d1b:$a: NanoCore
Click to see the 51 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.#RFQ ORDER484475577797.exe.2c91ed4.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
10.2.#RFQ ORDER484475577797.exe.2c91ed4.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
10.2.#RFQ ORDER484475577797.exe.6560000.32.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
10.2.#RFQ ORDER484475577797.exe.6560000.32.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x16e3:$x2: NanoCore.ClientPluginHost • 0x1800:$s4: PipeCreated • 0x16fd:$s5: IClientLoggingHost
10.2.#RFQ ORDER484475577797.exe.5e14629.29.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 159 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

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:

Found malware configuration

Yara detected Nanocore RAT

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)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

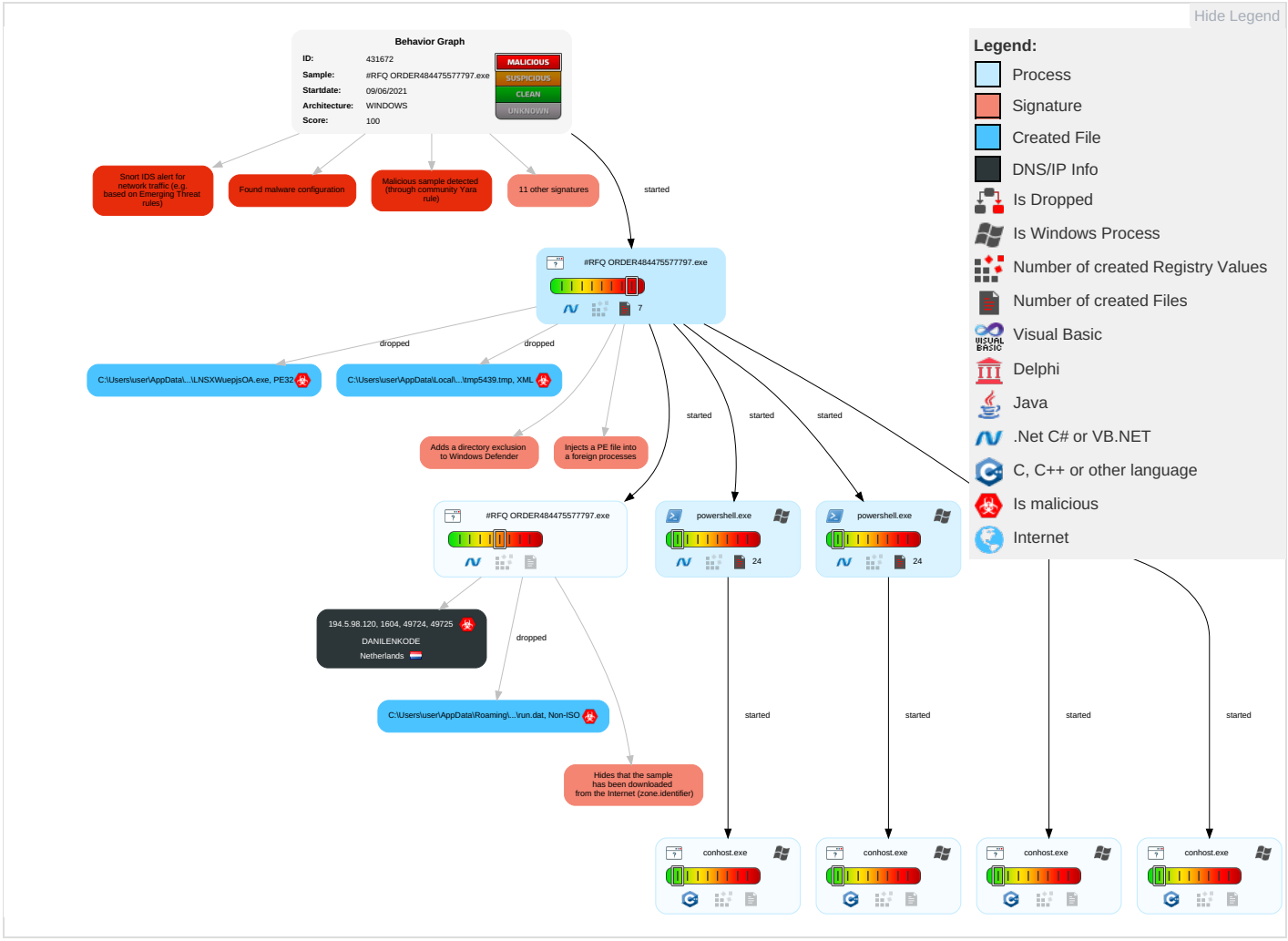
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

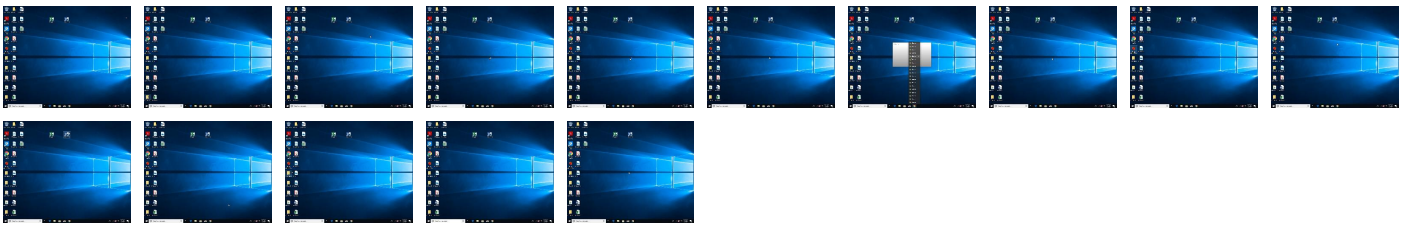
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe	4%	ReversingLabs	Win32.Trojan.GenericML	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.#RFQ ORDER484475577797.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.#RFQ ORDER484475577797.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.#RFQ ORDER484475577797.exe.5e10000.30.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.0.#RFQ ORDER484475577797.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.microsoft.co	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/siv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/4	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTFu	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/uet;	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasv	0%	Avira URL Cloud	safe	
http://www.fontbureau.com4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/j	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.com;	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com_	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fonts.comic)	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	URL Reputation	safe	
194.5.98.120	0%	Avira URL Cloud	safe	
http://www.fontbureau.comica	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
joseedward5001.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
194.5.98.120	true	• Avira URL Cloud: safe	unknown
joseedward5001.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.120	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431672
Start date:	09.06.2021
Start time:	06:00:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#RFQ ORDER484475577797.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:	33
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@15/21@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 43.8% • Quality standard deviation: 34.6%
HCA Information:	• Successful, ratio: 96% • 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
06:01:10	API Interceptor	968x Sleep call for process: #RFQ ORDER484475577797.exe modified
06:01:50	API Interceptor	97x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.120	Purchase_Order_Form_4667ROO3.exe	Get hash	malicious	Browse	
	IMG-06-05-345678909876543.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61
	DHL_file.exe	Get hash	malicious	Browse	• 194.5.98.145
	BBS FX.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	GpnPv433gb.exe	Get hash	malicious	Browse	• 194.5.98.11
	Kj7tTd1Zimp0cil.exe	Get hash	malicious	Browse	• 194.5.97.197
	Resume.exe	Get hash	malicious	Browse	• 194.5.98.8
	SecuriteInfo.com.Trojan.DownLoader39.38629.28832.exe	Get hash	malicious	Browse	• 194.5.98.145
	SecuriteInfo.com.Variant.Razy.840898.18291.exe	Get hash	malicious	Browse	• 194.5.98.144
	8LtwhjD2Qm.exe	Get hash	malicious	Browse	• 194.5.98.107
	Receiptn.exe	Get hash	malicious	Browse	• 194.5.98.180
	soa5.exe	Get hash	malicious	Browse	• 194.5.98.48
	soa5.exe	Get hash	malicious	Browse	• 194.5.98.48
	68Aj4oxPok.exe	Get hash	malicious	Browse	• 194.5.98.144
	Ysur2E8xPs.exe	Get hash	malicious	Browse	• 194.5.97.61
	HI4B6mZPHx.exe	Get hash	malicious	Browse	• 194.5.98.55

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#RFQ ORDER484475577797.exe.log	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

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

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
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-Scri pt.....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):	22432
Entropy (8bit):	5.601026317548112
Encrypted:	false
SSDEEP:	384:BtCDFL9zhSggIRkGnTnRel4KnOsIiP7Y9gFSJUeRe1BMrmKZ1AV7nD2He64I+qzg:KkG+4KOsdrFXeNT4e4V
MD5:	D441FECFBC90075FAD33775038F0095C
SHA1:	55927F378AE17EC0A7DF2DDAE83D7848FB2F041B
SHA-256:	293AC01B9F1A15C9CCE0E416EE3DF851C39475E82DE6014A22847EB21BF28068
SHA-512:	027A8FFD08983312AB767AE0537D800E890ECB4F71423231AE98A487D3A38526455C9B3FB6945421A3830AA5C1DE484AF3A8E961845B6DE104A0CEC780EC534C
Malicious:	false
Reputation:	low
Preview:	@...e.....X.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]..... %.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5tg0nxmy.vv5.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a4oghqwf.k1g.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_a4oghqwf.k1g.ps1	
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hjifbzqp.is4.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ugjy2ffl.kar.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\Local\Temp__PSScriptPolicyTest_xagkqtsl.tds.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\Local\Temp__PSScriptPolicyTest_zpenzzls.5ci.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zpenzzls.5ci.psm1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmp5439.tmp	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.19563600381544
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBatn:cbh47TlNQ//rydbz9l3YODOLNdq3+
MD5:	9446876F31244201872510015A7EA95E
SHA1:	CB825B2C983C682796CF98AAB272F0ADEC79F18D
SHA-256:	CD02449A4809FA4ED344985993AA17AB08E25B76F70C75B84FEC26BEFA36B8B5
SHA-512:	2639393CDE51B79BA31DD5666E341A14AD76DED15E169BF98A517DFDC0E34AFBD792F819D7EE1A51F6281FD482DFFF85B31929A5094CF6A84B98AC69EB90A7 8
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
File Type:	data
Category:	dropped
Size (bytes):	3480
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	96:flC0IIC0IIC0IIC0IIC0IIC0IIC0IIC0IIC0IIC0IIC0IIC08:f8L8L8L8L8L8L8L8L8L8L8L8L8L8L8r
MD5:	E1AFCDE67424226B8B4FC4209A77391C
SHA1:	B66E69ED31F39B8B0EFB652C514C43BCB42B5D28
SHA-256:	72826C35B0442BC1ACA3EE1C0CAA2DE87A694FC344BBF47A853082D26D6906F8
SHA-512:	313502CC6AF6482EF66C3CC10A65CBC60DBCF4C5EA4DA344833198902EE08996175FA60B12D05E7B5B887E08341B0468D47CD4CC578DF5D265E70CDE4F33F3 5
Malicious:	false
Preview:	 Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:M:M
MD5:	94F847755D0DE54CF6CA9961C9C969EE
SHA1:	B63BC791DB5FDE76F962C652F651E4461B797BED
SHA-256:	071211A30D041059B4C4E674D2F22C953645E3FE5C09171202CE1B5267D36870
SHA-512:	957E701B2177E95E41722AAF63F5AFA480C8363681865AA0540DAD2937F48C3D74E8E0E43253EDC9AB95D8236E3110FD57961D4E6AE73EC082BFD67F5687BA3E
Malicious:	**true**
Preview:	 .].F+.H

C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe	
Size (bytes):	800768
Entropy (8bit):	7.563112762527505
Encrypted:	false
SSDEEP:	12288:qB4w15tyPvHv4nO1eklMV40J4o9MBfpXjgp6PSPxM6Grfs768VN21zX4y8:qY4O1ekULCXgp6PSPxMtE768VN2J
MD5:	18E38261E8EA6AE0077C5448F809CCB6
SHA1:	BBFAF42987014BA9571C75D1982843D7AD7155AC
SHA-256:	3CB5C285D5E7F163C9764EF3E99467F5460B7F704C996FFA8E5E2982A2A86693
SHA-512:	8E2FFA93BFDCA6E2B4A362FA85A21963A5C7425DC37C82D0259F522289EC4CFF515DB5899C03887FC0B0F83F4947BFBB97F509C2AC0806F38EBAD2AC46B9A3B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.`.....P.....N..... ... ....@.. ..... ..@.....h...O.... ..hK.....0..... ..... ..H.....text..... ..... ..`.rsrc...hK... ...L.....@..@.rel oc.....6.....@..B.....H.....d<.....x....".....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(. ...oS...('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*..(3...*6. .o4...(5...*&...o6...*.0.....,..+...(7...s8.....*&..(3....*.

C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\#RFQ ORDER484475577797.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210609\PowerShell_transcript.138727.QzgMIEIQ.20210609060115.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):	5797
Entropy (8bit):	5.415713008653414
Encrypted:	false
SSDEEP:	96:BZ+hENktqDo1ZzZ3PhENktqDo1ZddsWUjZrhENktqDo1Z7BEEFZy:S
MD5:	CA824DEAD6121491D79217A2C39FD399
SHA1:	73BCD105A1A14FCF1C1A4EDC38D649DA14D553AC
SHA-256:	43ECA14E267592783142ED5926C122025770383F743E346BD2D9D64AEA5A87EF
SHA-512:	4B1EC19081DAAB57743D001801B43ECD5A7D4CA74750C448B5853D577E49C065EE64F05637221BCE1F489A0B080B7EE86E119B39FD32C0A5340728E41837D165
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210609060141..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe..Process ID: 6052..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: 20210609060141..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe..**********..Windows PowerShell transcript start..Start time: 20210609060805..Username: computer\user..RunAs User: computer\

C:\Users\user\Documents\20210609\PowerShell_transcript.138727.X6ZuAXXc.20210609060117.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):	5797
Entropy (8bit):	5.417979553216565
Encrypted:	false
SSDEEP:	96:BZ4hENmyqDo1Z4ZlhENmyqDo1ZxsWUjZ/hENmyqDo1ZkBEEhZa:oFz2
MD5:	5A7AD0849A4D8940ECB0224D99ED685F
SHA1:	BEFB48FDC96A6843CFDBEAB178B4ABAFF24440CF
SHA-256:	FDF27A85345399236C5F8069C8071016A0FCA637B4FBAFB49D1F88DCE305A73A
SHA-512:	0E0765D188913C6A020A32490E71621DE1B43820F5701D30DA838F6456EF5D448F862F1F958DFAE9A836D1CBDE503162A322015E6887035E5D1C14600F9050AF

C:\Users\user\Documents\20210609\PowerShell_transcript.138727.X6ZuAXXc.20210609060117.txt	
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210609060143..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe..Process ID: 3292..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: 20210609060144..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe..**********..Windows PowerShell transcript start..Start time: 20210609060656..Username: computer\user..RunAs User: computer\

C:\Users\user\Documents\20210609\PowerShell_transcript.138727.sxkKCi0R.20210609060114.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):	3587
Entropy (8bit):	5.41331628562482
Encrypted:	false
SSDEEP:	96:BZahENfeqDo1ZlOhZchENfeqDo1ZWqHBW0cBW0cBW0UZn:nk2GWFWFWl
MD5:	5CA658B9BC39C8A62F3C84EDB61C78AA
SHA1:	4975C9EC7BD674BEF41B9B330E4419DCCD4C4A94
SHA-256:	D444FE345A5D102C2962A23E9DB454FE43FC90945C5F16EA144961C549B445CA
SHA-512:	E95C7BD3A3982E643E6752D954905B17CCE040EA64C8C6581DF9F53B64ECD87BE194BE3ABE31A98C9E8F5A9F2B6F102F770817C9C1B303588F8082FF4D7EE60
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210609060134..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 138727 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#RFQ ORDER484475577797.exe..Process ID: 5616..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: 20210609060135..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#RFQ ORDER484475577797.exe..**********..Command start time: 20210609060424..**********..PS>TerminatingError(Add-MpPreference): "A positional parameter

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.563112762527505
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	#RFQ ORDER484475577797.exe
File size:	800768
MD5:	18e38261e8ea6ae0077c5448f809ccb6
SHA1:	bbfaf42987014ba9571c75d1982843d7ad7155ac
SHA256:	3cb5c285d5e7f163c9764ef3e99467f5460b7f704c996ffa8e5e2982a2a86693
SHA512:	8e2ffa93bfdca6e2b4a362fa85a21963a5c7425dc37c82d0259f522289ec4cff515db5899c03887fc0b0f83f4947bfbb97f509c2ac0806f38ebad2ac46b9a3fb
SSDEEP:	12288:qB4w15tyPvHv4nO1eklMV40J4o9MBfpXjgp6PSPxM6Grfs768VN21zX4y8:qY4O1ekULCXgp6PSPxMtE768VN2J
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.`.....P.....N..... ... .@.. .....@.....

File Icon

Icon Hash:	b6f8c8dccce06110

Static PE Info

General

Entrypoint:	0x4c07ba
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C021FC [Wed Jun 9 02:05:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbe7c0	0xbe800	False	0.817270033629	data	7.61659853966	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x4b68	0x4c00	False	0.469161184211	data	4.53099175809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: #RFQ ORDER484475577797.exe PID: 4364 Parent PID: 5700

General

Start time:	06:01:03
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#RFQ ORDER484475577797.exe'
Imagebase:	0x170000
File size:	800768 bytes
MD5 hash:	18E38261E8EA6AE0077C5448F809CCB6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.234685013.0000000002611000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.237223638.0000000003611000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.237223638.0000000003611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.237223638.0000000003611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5616 Parent PID: 4364

General

Start time:	06:01:12
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:\Users\user\Desktop\#RFQ ORDER484475577797.exe'
Imagebase:	0xf30000
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: 4884 Parent PID: 5616

General

Start time:	06:01:12
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

Analysis Process: powershell.exe PID: 6052 Parent PID: 4364

General

Start time:	06:01:13
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:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe'
Imagebase:	0xf30000
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: 5460 Parent PID: 6052

General

Start time:	06:01:13
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6741d0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5728 Parent PID: 4364

General

Start time:	06:01:13
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LNSXWuepjsOA' /XML 'C:\Users\user\AppData\Local\Temp\tmp5439.tmp'
Imagebase:	0x60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5916 Parent PID: 5728

General

Start time:	06:01:14
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

Analysis Process: powershell.exe PID: 3292 Parent PID: 4364

General

Start time:	06:01:14
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:\Users\user\AppData\Roaming\LNSXWuepjsOA.exe'
Imagebase:	0xf30000
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: 1968 Parent PID: 3292

General

Start time:	06:01:15
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

Analysis Process: #RFQ ORDER484475577797.exe PID: 1048 Parent PID: 4364

General

Start time:	06:01:15
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\#RFQ ORDER484475577797.exe
Imagebase:	0x7f0000
File size:	800768 bytes
MD5 hash:	18E38261E8EA6AE0077C5448F809CCB6
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: 0000000A.00000002.494989235.0000000006530000.00000004.00000001.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.494989235.0000000006530000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.491944391.0000000004483000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.484331798.0000000002C1C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495585675.00000000065F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495585675.00000000065F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.222827759.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.222827759.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.222827759.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495314337.00000000065A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495314337.00000000065A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495206933.0000000006580000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495206933.0000000006580000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495261079.0000000006590000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495261079.0000000006590000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495369457.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495369457.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.483639790.0000000002BB1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495737204.0000000006630000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495737204.0000000006630000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.223631637.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.223631637.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.223631637.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495530552.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495530552.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495151540.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495151540.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.493841988.0000000005430000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.493841988.0000000005430000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.489457795.0000000003BF9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.489457795.0000000003BF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.489186804.00000000030DC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.467232540.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.467232540.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.467232540.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495415659.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495415659.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.494542186.0000000005E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.494542186.0000000005E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.494542186.0000000005E10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.491386366.0000000004223000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.491386366.0000000004223000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.491745715.00000000043D6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.491745715.00000000043D6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.492065013.000000000456E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.492065013.000000000456E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.495101158.0000000006560000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.495101158.0000000006560000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

Disassembly

Code Analysis