ID: 451085
Sample Name: #RFQ ORDER7678432213211.exe
Cookbook: default.jbs
Time: 08:12:09
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report #RFQ ORDER7678432213211....

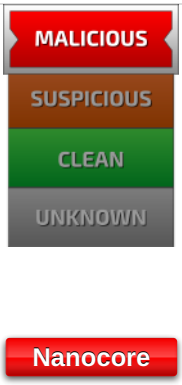
Overview

General Information

Sample Name:	#RFQ ORDER7678432213211.exe
Analysis ID:	451085
MD5:	2f286cd817b368e.
SHA1:	e49beec02d942e..
SHA256:	b291d719522053..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:

Detection

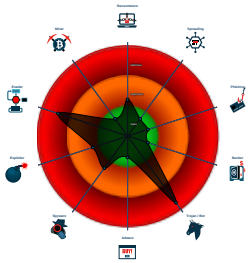


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through ...
- Multi AV Scanner detection for dropp...
- Multi AV Scanner detection for subm...
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e....
- Yara detected Nanocore RAT
- 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



- **System is w10x64**
- #RFQ ORDER7678432213211.exe (PID: 4900 cmdline: 'C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe' MD5: 2F286CD817B368E8A747E8F0D8F28825)
  - powershell.exe (PID: 6052 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2416 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3348 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XgPYsUfalKn' /XML 'C:\Users\user\AppData\Local\Temp\tmpFD92.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1848 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - #RFQ ORDER7678432213211.exe (PID: 1328 cmdline: C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe MD5: 2F286CD817B368E8A747E8F0D8F28825)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-000c0a4c",
  "Group": "oluwa",
  "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
00000012.00000002.493425460.000000000584 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
00000012.00000002.493425460.000000000584 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
00000012.00000002.493258723.00000000057F 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000012.00000002.493258723.00000000057F 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000012.00000002.493293452.000000000580 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost

Click to see the 21 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.#RFQ ORDER7678432213211.exe.6310000 .19.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost
18.2.#RFQ ORDER7678432213211.exe.6310000 .19.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x41ee:$x2: NanoCore.ClientPluginHost • 0x7641:$s4: PipeCreated • 0x4218:$s5: IClientLoggingHost
18.2.#RFQ ORDER7678432213211.exe.57f0000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3deb:$x1: NanoCore.ClientPluginHost • 0x3f48:$x2: IClientNetworkHost
18.2.#RFQ ORDER7678432213211.exe.57f0000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3deb:$x2: NanoCore.ClientPluginHost • 0x4d41:$s3: PipeExists • 0x3fe1:$s4: PipeCreated • 0x3e05:$s5: IClientLoggingHost
18.2.#RFQ ORDER7678432213211.exe.5830000 .11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost

Click to see the 51 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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:

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

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:

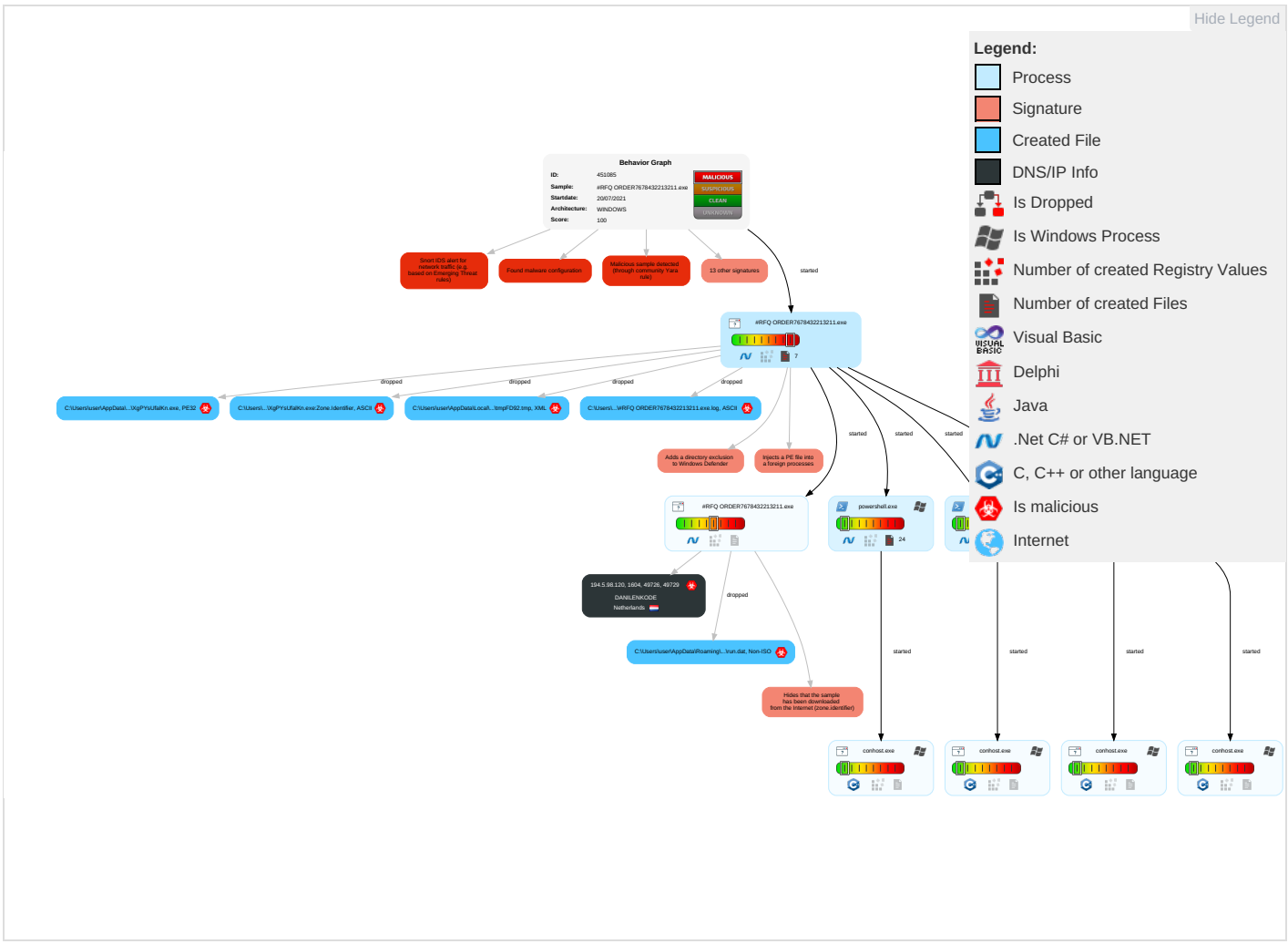
Detected Nanocore Rat

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	Scheduled Task/Job 1	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	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	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	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	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	Software Packing 3	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	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

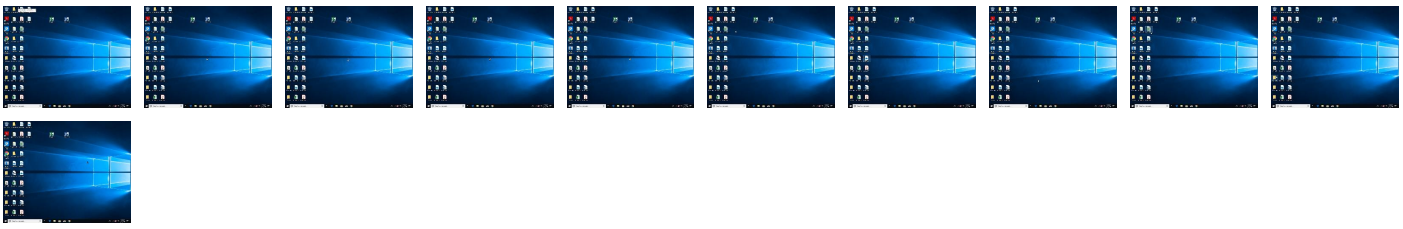
Behavior Graph



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

Source	Detection	Scanner	Label	Link
#RFQ ORDER7678432213211.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	
#RFQ ORDER7678432213211.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe	13%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.#RFQ ORDER7678432213211.exe.5940000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.#RFQ ORDER7678432213211.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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.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.fontbureau.comF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.html;	0%	Avira URL Cloud	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.fonts.comd	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://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//tr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/j.	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/W	0%	Avira URL Cloud	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.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/X.	0%	Avira URL Cloud	safe	
194.5.98.120	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/u.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/O.	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.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comasva	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/X7e	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaV.	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-f	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/n-u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	URL Reputation	safe	
http://www.fonts.comp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/O.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c.U	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/rV.	0%	Avira URL Cloud	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	

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:	33.0.0 White Diamond
Analysis ID:	451085
Start date:	20.07.2021
Start time:	08:12:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#RFQ ORDER7678432213211.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@15/20@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:13:33	API Interceptor	708x Sleep call for process: #RFQ ORDER7678432213211.exe modified
08:13:44	API Interceptor	116x 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	ZwN0lL3CzU.exe	Get hash	malicious	Browse	
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	
	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	ORDER.exe	Get hash	malicious	Browse	• 194.5.98.23
	Q_007880.exe	Get hash	malicious	Browse	• 194.5.97.168
	eQqnH61qiB.exe	Get hash	malicious	Browse	• 194.5.98.207
	B32E407DC3284184684B29FD5235CBEDF2B60F60 AED84.exe	Get hash	malicious	Browse	• 194.5.98.15
	MbBw6XTmif.exe	Get hash	malicious	Browse	• 194.5.98.107
	Jose Luis Ezeiza.cv7-15-2021.exe	Get hash	malicious	Browse	• 194.5.98.8
	t3uss3bjUL.exe	Get hash	malicious	Browse	• 194.5.98.182
	Agree Ment Letter-34222876190544.exe	Get hash	malicious	Browse	• 194.5.98.63
	purestub.exe	Get hash	malicious	Browse	• 194.5.98.63
	RFQ4100003433189994565.exe	Get hash	malicious	Browse	• 194.5.98.195
	Order0045439090.exe	Get hash	malicious	Browse	• 194.5.98.8
	TPJCc3cswr.exe	Get hash	malicious	Browse	• 194.5.97.44
	Proof of payment.exe	Get hash	malicious	Browse	• 194.5.97.181
	Payment Schedule.xlsx	Get hash	malicious	Browse	• 194.5.97.44
	FbJ8HGm3HU.exe	Get hash	malicious	Browse	• 194.5.98.210
	sRXwLQjycE.exe	Get hash	malicious	Browse	• 194.5.98.107
	elmPEd3zO7.exe	Get hash	malicious	Browse	• 194.5.97.131
	proof of payment.scr.exe	Get hash	malicious	Browse	• 194.5.98.5
	4B9CaCxB3Q.exe	Get hash	malicious	Browse	• 194.5.98.207
	yb6le40gR2.exe	Get hash	malicious	Browse	• 194.5.98.210

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#RFQ ORDER7678432213211.exe.log	
Process:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.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:	**true**
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
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22376
Entropy (8bit):	5.6011437476690995
Encrypted:	false
SSDEEP:	384:mtCDtPD3nMSoDHgSBKn0LultIO/7Y9g9SJ3xq1BMrmPZ1AV7HtWwu564I+fJzg:b37os4K6ultR79cZu4q1O
MD5:	59B78DBBB727A10360D42CDD87E4F00B
SHA1:	93AAFD5EAAB8630C2C0414200107BBEE63CB0461
SHA-256:	61E26BCF20A5A4285027EB793DFE60E6D960FEC1CF6988187DF2AFF5A8B0AEFF
SHA-512:	4A9D35BB74092D778AAE430C8A364C678C2264BD694ED401A3C5B69987ACC650EDB60FEA057A1EACE91BE41646ADA192AC3E71B1F0B1655A6574084C7B5A9D C0
Malicious:	false
Preview:	@...e.....R....r.....@.....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_3lbm0dym.0pl.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3lbm0dym.0pl.ps1	
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_5bowk3z4.alr.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_jkmlqmz3.kot.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_mbvx1mrl.nve.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_mjdu1muo.pll.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mjdu1muo.pll.ps1	
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_uwb0ckt4.xfw.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\tmpFD92.tmp	
Process:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.191372227906604
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBFNtn:cbh47TlNQ//rydbz9I3YODOLNdq3P
MD5:	C4BC1F6430E99ECF81752591B68F61E4
SHA1:	EB94AEA189CE6B14A93DBCE1D95216E30C645DF4
SHA-256:	2414C3BBC0BCEACEA13605FDF2BFC30407EDCA1966BC833EBAB1CE2FFF111DE2
SHA-512:	449D433339BC70094DB9FE8C34845235624EF9AB3D0238FC01C47F19674DF6438DDB4BBBCAE46D8FE367CDC018A36212B6BE38FE273DD7C2DC4A886DCAC13(E3
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>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <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 ORDER7678432213211.exe
File Type:	data
Category:	dropped
Size (bytes):	2784
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwZ:flC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	6D2C1BD8306716462108A6A3B4069F75
SHA1:	F46B24F6060F5F15F05CB3C1CFE633E349FFF316
SHA-256:	861DDBD599B4033924CDE39DDA488C7F01F36734489859355F7F419AB75B31C0
SHA-512:	6B231729623A94DC1DED8F6DC21F7B8EC1F109F061A137B037694AAF8013B434654F7893B7B44B4979105A20921BF0C68CA32AA189DFBD85F66AB86A6F64E0ED
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
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 ORDER7678432213211.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:mu8n:mu8
MD5:	F95935841A379CDF26C0AE3A4C0FBBE5
SHA1:	4C11219A155A69DD265A6DBC30B08D75675B88EC
SHA-256:	6248547EF44A01CC92AEEF2DE7A5B1EDDEA0B48D03B1CB020F8087BE1ED22263
SHA-512:	2A28206B5BF60C54AE141DB67175A652A5F1C5FA51C421015D9996DDE29C169565792398DBE409D818CB3BB772C0C76E6DBFDC005BF5174935D919B42EFF2E0
Malicious:	**true**
Preview:	.....K.H

C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe	
Process:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1084928
Entropy (8bit):	7.60637440768652
Encrypted:	false
SSDEEP:	24576:JU3ej57dEAKrvDBhGw4S3hYA0abY7VZ6Iyvv9JQ0NGNPV:ZALX3x0TrS7V
MD5:	2F286CD817B368E8A747E8F0D8F28825
SHA1:	E49BEEC02D942E12B0DAD74D81AB8ED4F02667E2
SHA-256:	B291D719522053A662CADD70B131668A1D953D4C4DD648E8A5647B689EB6341D
SHA-512:	3347116D44099808D4BBC050BC45C6B207ADC8C75E2BCFDFC49D3D535328C9DDEEBC0DED194B0C99E2F4EF021E1CFCA221F6F09EEF7FA77322E103671A400 CC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5.....P.....&.... .....@.. ....@.....O..... ....H.....text...,.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....\|.....0.....(....(.....(.....o!...*.....("......(#.....($.....(%.....(&....*N..(....o....('....*&..((. ...*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*&..(3....*...0..<.....~..... (4.....,!r...p.....(5...o6...s7.....~.....

C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210720\PowerShell_transcript.226546.QECk8fRN.20210720081336.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):	3595
Entropy (8bit):	5.398774077157319

C:\Users\user\Documents\20210720\PowerShell_transcript.226546.QECk8fRN.20210720081336.txt	
Encrypted:	false
SSDEEP:	96:BZGLh/NfctqDo1ZP2wZnh/NfctqDo1Zfq04Y0c4Y0c4Y0YbZei:a32xZYEYEY/Ei
MD5:	74ECE1B3B7B74B56D45D0B249CEA1026
SHA1:	F3262670D2FF79491054B542E1F1FEEDA11795A8
SHA-256:	8C4AE9368E03AEB005387E0ED70E0AF86619C35536D349E7982AC8C75700BC54
SHA-512:	C3F1354E2E164F15242599D81FEEF93865A2BD21251049485E696512A8784CA36D98AB287DAC6FBA6973C78632A44A3DD24D4F19579B77DAB363013CA39F9AA3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210720081403..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226546 (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 ORDER7678432213211.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: 20210720081404..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe..**********..Command start time: 20210720081716..**********..PS>TerminatingError(Add-MpPreference): "A positional paramet

C:\Users\user\Documents\20210720\PowerShell_transcript.226546.u9dWU6FT.20210720081341.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):	5793
Entropy (8bit):	5.412847263408266
Encrypted:	false
SSDEEP:	96:BZNh/NVqDo1ZLZjh/NVqDo1ZDv1HjZAh/NVqDo1ZSaXXpZS:n
MD5:	94A5AE9AD0D8454A4EF076656F8CD28C
SHA1:	121D585258DF4F2E7F6014EDAE62E7B3DBAB28D2
SHA-256:	D772214C85FA0304F10BAE0A6EF2E121D0E178FBCF5D1D5E7E365121C1E0D09C
SHA-512:	540E05271914407E668505658AD2690CA34F146E9488493285559508DFDB7AF27E7CB157DCFEBD5033C5E1DE25490ED4661BDF40856D6F959AE320DB336A8946
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210720081343..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226546 (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\XgPYsUfalKn.exe..Process ID: 1848..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: 20210720081343..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe..**********..Windows PowerShell transcript start..Start time: 20210720081837..Username: computer\user..RunAs User: computer\ha

C:\Users\user\Documents\20210720\PowerShell_transcript.226546.xFvC9uuU.20210720081339.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):	5793
Entropy (8bit):	5.408644517030285
Encrypted:	false
SSDEEP:	96:BZoh/NhqDo1ZGZlSh/NhqDo1Z6v1HjZYh/NhqDo1ZWaXXhZ+:b7
MD5:	B31D920EEB8EE60422F11E5502682C2D
SHA1:	462C3BC549115DD38E47A26E1C7CEC05E57C46DF
SHA-256:	EBDDFEE32AC4653F7D04B6ECA36895358930EE4540BDD228B033CA1C5D582449
SHA-512:	B12784998A80E148D9AA731596F68A2D3075766695473419D6157AF313D7C545B4EBA20E35D17A4134EDA0A64C1D55C49FD62B005472EC1C98ACB7738B0718B9
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210720081405..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 226546 (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\XgPYsUfalKn.exe..Process ID: 2416..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: 20210720081405..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\XgPYsUfalKn.exe..**********..Windows PowerShell transcript start..Start time: 20210720082127..Username: computer\user..RunAs User: computer\ha

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.60637440768652

General

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 ORDER7678432213211.exe
File size:	1084928
MD5:	2f286cd817b368e8a747e8f0d8f28825
SHA1:	e49beec02d942e12b0dad74d81ab8ed4f02667e2
SHA256:	b291d719522053a662cadd70b131668a1d953d4c4dd648e8a5647b689eb6341d
SHA512:	3347116d44099808d4bbc050bc45c6b207adc8c75e2bcfdfc49d3d535328c9ddeebc0ded194b0c99e2f4ef021e1cfca221f6f09eef7fa77322e103671a4009cc
SSDEEP:	24576:JU3ej57dEAKrvDBhGw4S3hYA0abY7VZ6lyvv9JQ0NGNPV:ZALX3x0TrS7V
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....5.....P.....&.... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50a426
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:	0x920335CE [Sat Aug 17 19:45:18 2047 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	0x10842c	0x108600	False	0.76640070922	data	7.61140570465	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x3d0	0x400	False	0.38671875	data	3.0404823065	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/20/21-08:13:47.111506	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	1604	192.168.2.3	194.5.98.120
07/20/21-08:13:54.987776	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:01.086640	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:08.165157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:15.206346	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:22.219133	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:29.166940	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:35.243747	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:41.426450	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:48.432412	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1604	192.168.2.3	194.5.98.120
07/20/21-08:14:54.599567	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	1604	192.168.2.3	194.5.98.120
07/20/21-08:15:01.610024	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1604	192.168.2.3	194.5.98.120
07/20/21-08:15:07.891700	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	1604	192.168.2.3	194.5.98.120

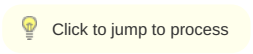
Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: #RFQ ORDER7678432213211.exe PID: 4900 Parent PID: 5592

General

Start time:	08:13:02
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe'
Imagebase:	0x1a0000
File size:	1084928 bytes
MD5 hash:	2F286CD817B368E8A747E8F0D8F28825
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6052 Parent PID: 4900

General

Start time:	08:13:34
Start date:	20/07/2021
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 ORDER7678432213211.exe'
Imagebase:	0x840000
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: 1532 Parent PID: 6052

General

Start time:	08:13:34
Start date:	20/07/2021

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: 2416 Parent PID: 4900

General

Start time:	08:13:35
Start date:	20/07/2021
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\XgPYsUfalKn.exe'
Imagebase:	0x840000
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: schtasks.exe PID: 3348 Parent PID: 4900

General

Start time:	08:13:35
Start date:	20/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XgPYsUfalKn' /XML 'C:\Users\user\AppData\Local\Temp\tmpFD92.tmp'
Imagebase:	0x250000
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: 1844 Parent PID: 2416

General

Start time:	08:13:35
Start date:	20/07/2021
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: conhost.exe PID: 6080 Parent PID: 3348

General

Start time:	08:13:36
Start date:	20/07/2021
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: 1848 Parent PID: 4900

General

Start time:	08:13:37
Start date:	20/07/2021
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\XgPYsUfalKn.exe'
Imagebase:	0x840000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: #RFQ ORDER7678432213211.exe PID: 1328 Parent PID: 4900

General

Start time:	08:13:38
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\#RFQ ORDER7678432213211.exe
Imagebase:	0xa50000
File size:	1084928 bytes
MD5 hash:	2F286CD817B368E8A747E8F0D8F28825
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: 00000012.00000002.493425460.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493425460.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493258723.00000000057F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493258723.00000000057F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493293452.0000000005800000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493293452.0000000005800000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.494090628.0000000006310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.494090628.0000000006310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.477033384.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.477033384.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.477033384.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493236087.00000000057E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493236087.00000000057E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493731765.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493731765.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.493731765.0000000005940000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493399369.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493399369.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.492994566.0000000005630000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.492994566.0000000005630000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.490625846.0000000004081000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493334722.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.493334722.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

Analysis Process: conhost.exe PID: 1260 Parent PID: 1848

General

Start time:	08:13:40
Start date:	20/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis