ID: 526551
Sample Name: PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Cookbook: default.jbs
Time: 18:39:26
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

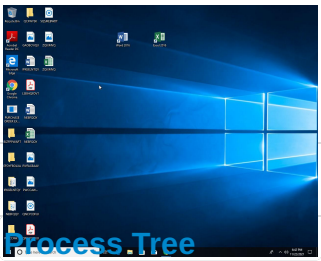
Windows Analysis Report PURCHASE ORDER EXPORT…

Overview

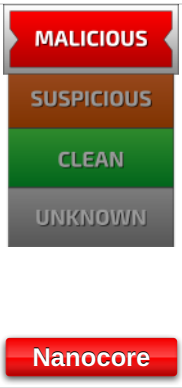
General Information

Sample Name:	PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Analysis ID:	526551
MD5:	7ba9068de522fce.
SHA1:	9a7b48eb459863..
SHA256:	3a247872a0d5d1..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

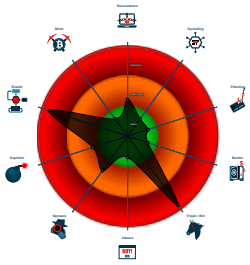


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…

Classification



- **System is w10x64**
- PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe (PID: 6904 cmdline: "C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe" MD5: 7BA9068DE522FCEF76DD98DC7E1D6F4E)
  - powershell.exe (PID: 7164 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3296 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 1364 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\rEyeIgLUX.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6348 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rEyeIgLUX" /XML "C:\Users\user\AppData\Local\Temp\tmp467D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe (PID: 2800 cmdline: C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe MD5: 7BA9068DE522FCEF76DD98DC7E1D6F4E)
- dhcpmon.exe (PID: 7040 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 7BA9068DE522FCEF76DD98DC7E1D6F4E)
  - powershell.exe (PID: 7116 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4876 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\rEyeIgLUX.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5540 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5912 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rEyeIgLUX" /XML "C:\Users\user\AppData\Local\Temp\tmpA8E1.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 4596 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 7BA9068DE522FCEF76DD98DC7E1D6F4E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7bac51af-6e1b-49a6-b8e9-5df85863",
  "Group": "Ziba",
  "Domain1": "james12.ddns.net",
  "Domain2": "",
  "Port": 6327,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 50,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "james12.ddns.net",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.713495925.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000000.713495925.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000000.713495925.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000A.00000000.709764931.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000000.709764931.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.3.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe.43a9b21.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x18dbe:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x18de8:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
10.3.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe.43a9b21.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x18dbe:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x1ac6e:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
10.3.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe.43a9b21.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.dhcpmon.exe.43995b0.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.dhcpmon.exe.43995b0.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
Click to see the 110 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

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

Uses dynamic DNS services

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

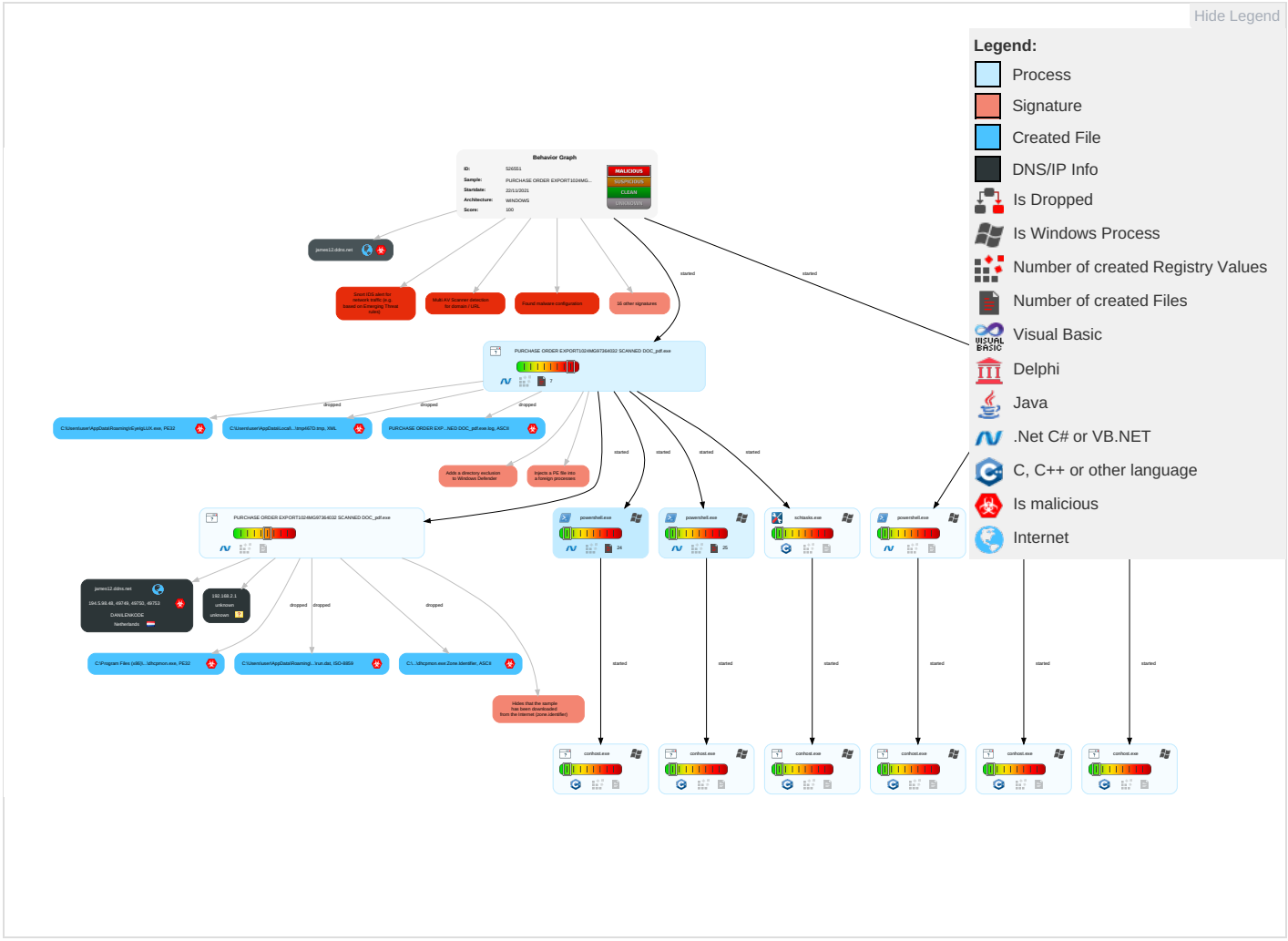
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	En Cha

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Nor Por
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 4	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rer Sof
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Nor App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	App Lay Pro
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 3 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

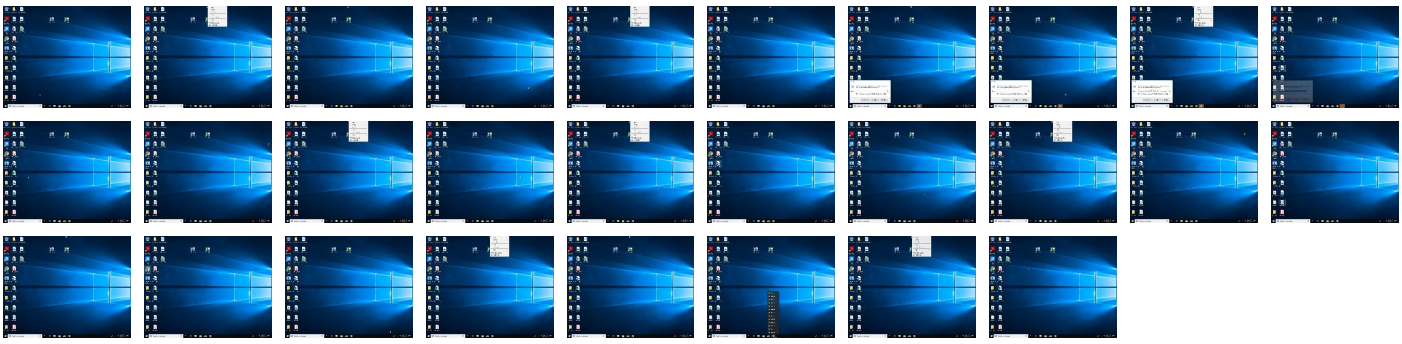
Behavior Graph



Screenshots

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
PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe	27%	Virustotal		Browse
PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\rEyeIgLUX.exe	29%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.0.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe .400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe .400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe .400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe .400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe .400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
james12.ddns.net	9%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com6	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnJ-9	0%	Avira URL Cloud	safe	
http://www.carterandcone.com6	0%	Avira URL Cloud	safe	
http://www.tiro.com8o	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.sandoll.co.krimale	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb-n	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC;	0%	Avira URL Cloud	safe	
http://www.urwpp.deBU	0%	Avira URL Cloud	safe	
http://www.fonts.comcoo	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comter	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
james12.ddns.net	0%	Avira URL Cloud	safe	
http://www.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.comgy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/gHAV9-	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.sandoll.co.kr201	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.comLo	0%	Avira URL Cloud	safe	
http://www.carterandcone.comint	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnb-/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comalsFSL	0%	Avira URL Cloud	safe	
http://www.tiro.comyo	0%	Avira URL Cloud	safe	
http://www.carterandcone.com?-e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
james12.ddns.net	194.5.98.48	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
james12.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.48	james12.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526551
Start date:	22.11.2021
Start time:	18:39:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.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:	29
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@24/25@17/2
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
18:40:32	API Interceptor	830x Sleep call for process: PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe modified
18:40:37	API Interceptor	144x Sleep call for process: powershell.exe modified
18:40:50	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:40:59	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.48	ESTADO+10+DE+NOVIEMBRE+DE+2021-101121.pdf.js	Get hash	malicious	Browse	
	PURCHASE ORDER EXPORT1024 SCANNED DOC_pdf.exe	Get hash	malicious	Browse	
	XdZ4ad8GpU.exe	Get hash	malicious	Browse	
	we-ship-SNE-9874657.xlsx	Get hash	malicious	Browse	
	XnQ8NBKkhW.exe	Get hash	malicious	Browse	
	YdACOWCggQ.exe	Get hash	malicious	Browse	
	Import order764536.xlsx	Get hash	malicious	Browse	
	Bill of Lading, Invoice, & Packing LIsts.exe	Get hash	malicious	Browse	
	Quotation Price - Double R Trading b.v.exe	Get hash	malicious	Browse	
	Nizi International S.A. #New Order.exe	Get hash	malicious	Browse	
	DHL Import Clearance #U2013 Consignment #6225954602.exe	Get hash	malicious	Browse	
	soa5.exe	Get hash	malicious	Browse	
	soa5.exe	Get hash	malicious	Browse	
	PO SKP 149684.jar	Get hash	malicious	Browse	
	TECHNICAL OFFERS.exe	Get hash	malicious	Browse	
	17New P.O_signed.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
james12.ddns.net	PURCHASE ORDER EXPORT1024 SCANNED DOC_pdf.exe	Get hash	malicious	Browse	• 194.5.98.48
	PURCHASE ORDER EXPORTO52022 IMG00987066 SCANNED DOC_PDF.exe	Get hash	malicious	Browse	• 91.193.75.132
	qd9HIAs3XV.exe	Get hash	malicious	Browse	• 91.193.75.132
	wDIaJji4Vv.exe	Get hash	malicious	Browse	• 79.134.225.7
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	PURCHASE ORDER EXPORT0022355048 SCAN DOC_PDF.exe	Get hash	malicious	Browse	• 79.134.225.7

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	purchase order NI32855 (1).exe	Get hash	malicious	Browse	• 194.5.98.139
	8mTwU7uNFV.exe	Get hash	malicious	Browse	• 194.5.97.131
	KNpmkMT5f3.exe	Get hash	malicious	Browse	• 194.5.98.12
	scvRj4lo1E.exe	Get hash	malicious	Browse	• 194.5.98.11

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#RFQ ORDER484425083-NJ.exe	Get hash	malicious	Browse	• 194.5.98.120
	RzUbuIerbF.exe	Get hash	malicious	Browse	• 194.5.97.207
	SIGNED_COPY_IMG_ORDER_...REQUEST_IMG_123456.exe	Get hash	malicious	Browse	• 194.5.98.5
	NOA MU21S0029729.exe	Get hash	malicious	Browse	• 194.5.97.207
	New purchase order 4940009190,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23
	Fattura_del_cliente_V406307-scan.exe	Get hash	malicious	Browse	• 194.5.97.165
	ML822VOG-R11.doc	Get hash	malicious	Browse	• 194.5.97.131
	6Xzgfme0z6.exe	Get hash	malicious	Browse	• 194.5.97.131
	ESTADO+10+DE+NOVIEMBRE+DE+2021-101121.pdf.js	Get hash	malicious	Browse	• 194.5.98.48
	RTQFHtPW9x.exe	Get hash	malicious	Browse	• 194.5.98.107
	Document#053681.exe	Get hash	malicious	Browse	• 194.5.98.204
	4vo6jE1nlG.exe	Get hash	malicious	Browse	• 194.5.97.54
	ORDEN DE COMPRA-PDF.exe	Get hash	malicious	Browse	• 194.5.97.149
	Confirmation Transfer Copy MT102-Ref No#01018.exe	Get hash	malicious	Browse	• 194.5.98.105
	Confirmation Transfer Copy MT102-Ref No-01018.exe	Get hash	malicious	Browse	• 194.5.98.105
	PAYMENT COPY EXPORT1024 SCANNED DOCUMENT _pdf.exe	Get hash	malicious	Browse	• 194.5.98.30

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	528896
Entropy (8bit):	7.701920893284902
Encrypted:	false
SSDEEP:	12288:/sRtD00gTfhllXbNGMporp7d1tEQE6Zfj:/sRC0gTpXBIp7d3np1
MD5:	7BA9068DE522FCEF76DD98DC7E1D6F4E
SHA1:	9A7B48EB45986398308B356851638545189070B4
SHA-256:	3A247872A0D5D1686D14A0FCDE7143A0F501A3520ABD05DC261DBB4373DE29FB
SHA-512:	DF562F256CD32FEABC8FC764E3D2CD3EE4E1EE2D90FA4C8059DB5E4442EFEF830E99E7D0B4FEEDC8850852FBFF085EE9F4241563D7BE34CAC7C4BE4D25C7 B89
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a.....0.....&... ...@....@.. ....@.....\&..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....&.....H.....xj...F.....k...L....u.....b..}.....}.....(.....*r..}.....}.....r...p(.....**...(3....*...|7...%(.....{....X(.....|7...%(.....{.. ..X(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*....0..A.....A...%...%.. .%...%.....%.r...p.%.rl..p.%.r[..p.(.....+..*^..}.....(.....(.....*....0..,.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.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**

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe.log	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	659
Entropy (8bit):	5.2661344468761735
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2U/N0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2U/Pz2T
MD5:	3C153E5BCCA87FF6E091634EE977299F
SHA1:	6DE85803E7FA00C03CE809243EB8162DF036430A
SHA-256:	F0705BDCE38ADB33CA8B414DDB85718985660BC73E0BE4439E0A94384A37797D
SHA-512:	54BDFFA72A0D4122B5B79B092D7E8C3213EB30AE2858188748E52ADD65ADE2F2F887892C06BB8ED790C19F1ED949176B9A9F0113679EF38B74387A189E6DC74
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Transactions\aa840ffb0dd775d9eb8d66c8a8e8cdd9\System.Transactions.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	5.2661344468761735
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70U2U/N0Ug+9Yz9tv:MLF20NaL329hJ5g522rW2U/Pz2T
MD5:	3C153E5BCCA87FF6E091634EE977299F
SHA1:	6DE85803E7FA00C03CE809243EB8162DF036430A
SHA-256:	F0705BDCE38ADB33CA8B414DDB85718985660BC73E0BE4439E0A94384A37797D
SHA-512:	54BDFFA72A0D4122B5B79B092D7E8C3213EB30AE2858188748E52ADD65ADE2F2F887892C06BB8ED790C19F1ED949176B9A9F0113679EF38B74387A189E6DC74
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Transactions\aa840ffb0dd775d9eb8d66c8a8e8cdd9\System.Transactions.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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):	19672
Entropy (8bit):	5.5736404828152555
Encrypted:	false
SSDEEP:	384:3tjosG0glZCfBm1cS0nujul+O3oIpaeQ99VYcg+M1M0s0UP7zA:4lMQ+TuCln4AatZYFCd0Aw
MD5:	56E80992D0E90DDB7556402340E3887D
SHA1:	66EA823C0A75D9EAD4A59CCB234B180EE6721DCC
SHA-256:	F6FE3B497BDB21DD11F72C27C7978D36CCB5B11121B3F2848B0FF3EEE22F0D56
SHA-512:	DB881E4C11C0C70F6473C1D0F7B38A4F7AA2D6A572D49A94764C494BB80F114E50ABF0777B889DE088D4F033BFFBFF6E423F9B8DE0F82B82EF3736D2B4870A8
Malicious:	false
Preview:	@...e.....~.r.r...T...6.s.....@.....H.....<@.^.L."My...:B..... .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...<.....):gK..G...$.1.q.....System.Configuration<.....~.[L.D.Z.>..m.....System.Transactions.P...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3byeis5t.mkj.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_3byeis5t.mkj.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_cove0s0s.3bl.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_rugwc3rr.lmi.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_t03bphms.jnb.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_tegsgvfz.cq0.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tegsgvfz.cq0.psm1	
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_ujndjznq.u24.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_ziiazx4u.hf1.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_zvqmwook.lku.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\tmp467D.tmp	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe

C:\Users\user\AppData\Local\Temp\tmp467D.tmp	
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1596
Entropy (8bit):	5.136880481438
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta7xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTyv
MD5:	C8A9CED37FE1D102C8DA64F64112F294
SHA1:	B907D3DEE8303EC07A6F2B7B0073D2CDC5CF3BD2
SHA-256:	63E7E5D7B989B28A26CF5BC25499564ECBD960420680EC91184727F40D384A88
SHA-512:	257A9798E335CACF4EF9925311FEE66510B79188A2435FAD6947CEC364CE28A19AA79191DF0FD1BCCE2253B07B35B52110AAAB530F928F55F84520A6F0A4A352
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</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpA8E1.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1596
Entropy (8bit):	5.136880481438
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNta7xvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTyv
MD5:	C8A9CED37FE1D102C8DA64F64112F294
SHA1:	B907D3DEE8303EC07A6F2B7B0073D2CDC5CF3BD2
SHA-256:	63E7E5D7B989B28A26CF5BC25499564ECBD960420680EC91184727F40D384A88
SHA-512:	257A9798E335CACF4EF9925311FEE66510B79188A2435FAD6947CEC364CE28A19AA79191DF0FD1BCCE2253B07B35B52110AAAB530F928F55F84520A6F0A4A352
Malicious:	false
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</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
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.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:zS6Bt:zJb
MD5:	447E56D9F2F69A68280F058717E47720
SHA1:	43084A5985A2B4483F0A04DAF6FEF25282FE75B2

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	981B88BE484260AFF3988F2CB00BF3603454209CB083B15D059468D46207B95D
SHA-512:	8819BBE46FECCDCBC78EB82A5152D3530C40C5121A2162AB3617C66004EA40579C958B676F149F37D620317BEA1D2DB1F70467F8032DA773D9A39F36F0F7B01
Malicious:	**true**
Preview:	oCt7..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=..:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\rEyeIgLUX.exe	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	528896
Entropy (8bit):	7.701920893284902
Encrypted:	false
SSDEEP:	12288:/sRtD00gTfhllXbNGMporp7d1tEQE6Zfj:/sRC0gTpXBIp7d3np1
MD5:	7BA9068DE522FCEF76DD98DC7E1D6F4E
SHA1:	9A7B48EB45986398308B356851638545189070B4
SHA-256:	3A247872A0D5D1686D14A0FCDE7143A0F501A3520ABD05DC261DBB4373DE29FB
SHA-512:	DF562F256CD32FEABC8FC764E3D2CD3EE4E1EE2D90FA4C8059DB5E4442EFEF830E99E7D0B4FEEDC8850852FBFF085EE9F4241563D7BE34CAC7C4BE4D25C7 B89
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a.....0.....&... ...@....@.. ....@.....\&..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....&.....H.....xj...F.....k...L....u.....b..}.....}.....(,.....*r..}.....}.....r...p(,.....**...(3....*...|7...%(.....{....X(.....|7...%(.....{.. ..X(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*...|7...%(.....{....ZX(.....|7...%(.....{....ZX(.....*....0..A.....A...%...%.. .%...%.....%.r...p.%.rI..p.%.r[..p.(.....+..*^..}.....(.....(.....*....0..,.....

C:\Users\user\AppData\Roaming\rEyeIgLUX.exe:Zone.Identifier

C:\Users\user\AppData\Roaming\rEyeIgLUX.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.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\20211122\PowerShell_transcript.849224.0aNFpDSB.20211122184104.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):	5785
Entropy (8bit):	5.395485214371877
Encrypted:	false
SSDEEP:	96:BZzj5NnqDo1ZpZlj5NnqDo1ZsgWojZ6j5NnqDo1ZUd44jZo:6
MD5:	CE31543FC89019B00EDF04B681802872
SHA1:	F5B84C944798AD2AD34E9277332C54A1939C7CC3
SHA-256:	B380E9A7D74681929EEEF91BC19201A5C00EBEF1A604536C75A3D6DF3AE130B0
SHA-512:	114425CB207CDBBECFA65C8E7A8676F87545F42560181D8A189367963F086DEC853B3AD656B5D7D7AF00A4EB9565510220338E6EF9361E5192E7A6BEF25E0FB2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122184106..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (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\rEyeIgLUX.exe..Process ID: 4876..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: 20211122184106..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\rEyeIgLUX.exe..**********..Windows PowerShell transcript start..Start time: 20211122184438..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20211122\PowerShell_transcript.849224.IStSMB+a.20211122184034.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):	3594
Entropy (8bit):	5.405633910560106
Encrypted:	false
SSDEEP:	96:BZOj5NrqDo1Zj7FZIj5NrqDo1Zwqjx0cx0cx0OZp:2YFFR
MD5:	CEE0A42CD1D7EE13BBA3A74641330AE7
SHA1:	72103F998981C24954D90BB61D80345DA749CA9C
SHA-256:	3B90CCABC7B664922F3A0C1E9287B91E7B11EB91D73BC1290A3940EFF15A48E6
SHA-512:	8B88FCA3E064005B007B7007F32DF822643E52081EA1F1490C2BAD6D966620535863F5B4E2D55407A186CD111B81D1125D983DDEBD50924331B7F46AD5C3A8F5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122184037..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe..Process ID: 7164..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..PSR emotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211122184037..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe..**********..Command start time: 20211122184351..**********..PS>T

C:\Users\user\Documents\20211122\PowerShell_transcript.849224.QY1C3Hux.20211122184036.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):	5785
Entropy (8bit):	5.394923057421319
Encrypted:	false
SSDEEP:	96:BZxj5NSqDo1ZfZPj5NSqDo1ZRgWojZRj5NSqDo1Z7d44PZ0:w
MD5:	2A9419D7EC38BD059C90FF679722B004
SHA1:	A74F655BA50DFC10EC477351E96B8A6C7B457149

C:\Users\user\Documents\20211122\PowerShell_transcript.849224.QY1C3Hux.20211122184036.txt	
SHA-256:	A8E583DC9A0B5246E118492D0AB074E75C2840F2F182083C4D804D11DAADC11B
SHA-512:	43F576D8C4B330D0B9E2F1594707ED0D81EDFDA9AC851A2CB13812076DF796647A93C99245F9BE7B7E45746B5FBA57D42DF5E5254691A5E464C401037ED3727
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122184038..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (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\rEyeIgLUX.exe..Process ID: 1364..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: 20211122184038..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData \Roaming\rEyeIgLUX.exe..**********..Windows PowerShell transcript start..Start time: 20211122184506..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20211122\PowerShell_transcript.849224.yB0+MJmL.20211122184103.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):	3691
Entropy (8bit):	5.225781823272133
Encrypted:	false
SSDEEP:	96:BZIj5NEqDo1ZLZjj5NEqDo1ZllzvOzGMzGMzwxZD:SvyGgGgwn
MD5:	947F79D947B2B697AC196E32915D49E4
SHA1:	95320BB3FD390079A0E19061959FEE626FAAF6EC
SHA-256:	030932EA39336FE1895D22316F99790C1143F08BBA8002B4339600F438666F6E
SHA-512:	92B986BC83583F9C6315B1B8EE99711361540C296518FB46EAA5E4D9600E64E1B22C9A0E2D9BAA07A1DA960F4CA69EA6B1E15376EA1936EF2A2224991E6255F2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122184105..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..Process ID: 7116..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: 20211122184105..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..**********..Windows PowerShell transcript start..Start time: 20211122184546..Username: computer\user..RunAs User: co mputer\

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.701920893284902
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:	PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
File size:	528896
MD5:	7ba9068de522fcef76dd98dc7e1d6f4e
SHA1:	9a7b48eb45986398308b356851638545189070b4
SHA256:	3a247872a0d5d1686d14a0fcde7143a0f501a3520abd05c c261dbb4373de29fb
SHA512:	df562f256cd32feabc8fc764e3d2cd3ee4e1ee2d90fa4c80 59db5e4442efef830e99e7d0b4feedc8850852fbff085ee9f 4241563d7be34cac7c4be4d25c71b89
SSDEEP:	12288:/sRtD00gTfhllXbNGMporp7d1tEQE6Zfj:/sRC0gT pXBIp7d3np1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....2.a.....0.....&... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4826ae
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:	0x619B32FA [Mon Nov 22 06:04:42 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x806c4	0x80800	False	0.848606213521	data	7.71310269817	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x5f4	0x600	False	0.430989583333	data	4.18745646157	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	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
11/22/21-18:40:50.223437	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59123	8.8.4.4	192.168.2.4
11/22/21-18:40:50.460878	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	6327	192.168.2.4	194.5.98.48
11/22/21-18:40:56.573634	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:02.432617	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.4.4	192.168.2.4
11/22/21-18:41:03.037286	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:10.212791	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.4.4	192.168.2.4
11/22/21-18:41:10.596063	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:17.075973	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62389	8.8.4.4	192.168.2.4
11/22/21-18:41:17.300188	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	6327	192.168.2.4	194.5.98.48

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/22/21-18:41:23.311968	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49910	8.8.4.4	192.168.2.4
11/22/21-18:41:23.468587	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:29.666241	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.4.4	192.168.2.4
11/22/21-18:41:29.799446	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:36.269051	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:43.646812	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56627	8.8.4.4	192.168.2.4
11/22/21-18:41:43.922060	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:50.327657	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	6327	192.168.2.4	194.5.98.48
11/22/21-18:41:56.541259	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.4.4	192.168.2.4
11/22/21-18:41:57.111015	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	6327	192.168.2.4	194.5.98.48
11/22/21-18:42:03.632540	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	6327	192.168.2.4	194.5.98.48
11/22/21-18:42:09.953892	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	6327	192.168.2.4	194.5.98.48
11/22/21-18:42:16.648975	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	6327	192.168.2.4	194.5.98.48
11/22/21-18:42:29.880554	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49612	8.8.4.4	192.168.2.4
11/22/21-18:42:30.013654	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	6327	192.168.2.4	194.5.98.48
11/22/21-18:42:35.947030	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	6327	192.168.2.4	194.5.98.48

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 18:40:50.200015068 CET	192.168.2.4	8.8.4.4	0x131d	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:40:56.423813105 CET	192.168.2.4	8.8.4.4	0x631a	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:02.410928011 CET	192.168.2.4	8.8.4.4	0xfb51	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:10.181791067 CET	192.168.2.4	8.8.4.4	0xb48a	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:17.054394960 CET	192.168.2.4	8.8.4.4	0x3e13	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:23.290021896 CET	192.168.2.4	8.8.4.4	0xc6d2	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:29.646991968 CET	192.168.2.4	8.8.4.4	0xfbe9	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:35.981303930 CET	192.168.2.4	8.8.4.4	0xcc7b	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:43.626094103 CET	192.168.2.4	8.8.4.4	0x968b	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:50.163022995 CET	192.168.2.4	8.8.4.4	0xa4ec	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:56.512414932 CET	192.168.2.4	8.8.4.4	0x2f36	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:03.480258942 CET	192.168.2.4	8.8.4.4	0x8afc	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:09.781270027 CET	192.168.2.4	8.8.4.4	0x711b	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2021 18:42:16.481969118 CET	192.168.2.4	8.8.4.4	0x7c11	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:22.479844093 CET	192.168.2.4	8.8.4.4	0x35ec	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:29.858758926 CET	192.168.2.4	8.8.4.4	0x9451	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:35.795295000 CET	192.168.2.4	8.8.4.4	0xff88	Standard query (0)	james12.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 18:40:50.223437071 CET	8.8.4.4	192.168.2.4	0x131d	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:40:56.442034006 CET	8.8.4.4	192.168.2.4	0x631a	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:02.432616949 CET	8.8.4.4	192.168.2.4	0xfb51	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:10.212790966 CET	8.8.4.4	192.168.2.4	0xb48a	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:17.075973034 CET	8.8.4.4	192.168.2.4	0x3e13	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:23.311968088 CET	8.8.4.4	192.168.2.4	0xc6d2	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:29.666240931 CET	8.8.4.4	192.168.2.4	0xfbe9	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:35.999191999 CET	8.8.4.4	192.168.2.4	0xcc7b	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:43.646811962 CET	8.8.4.4	192.168.2.4	0x968b	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:50.181020021 CET	8.8.4.4	192.168.2.4	0xa4ec	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:41:56.541259050 CET	8.8.4.4	192.168.2.4	0x2f36	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:03.499874115 CET	8.8.4.4	192.168.2.4	0x8afc	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:09.800605059 CET	8.8.4.4	192.168.2.4	0x711b	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:16.499813080 CET	8.8.4.4	192.168.2.4	0x7c11	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:22.500077009 CET	8.8.4.4	192.168.2.4	0x35ec	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:29.880553961 CET	8.8.4.4	192.168.2.4	0x9451	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)
Nov 22, 2021 18:42:35.814043045 CET	8.8.4.4	192.168.2.4	0xff88	No error (0)	james12.ddns.net		194.5.98.48	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe PID: 6904 Parent PID: 5360

General

Start time:	18:40:27
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe"
Imagebase:	0xd60000
File size:	528896 bytes
MD5 hash:	7BA9068DE522FCEF76DD98DC7E1D6F4E
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: 00000000.00000002.715793394.00000000035A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.717130946.0000000004841000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.717130946.0000000004841000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.717130946.0000000004841000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.716851621.0000000004632000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.716851621.0000000004632000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.716851621.0000000004632000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.716174408.0000000003729000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 7164 Parent PID: 6904

General

Start time:	18:40:33

Start date:	22/11/2021
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\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Imagebase:	0xa80000
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: 3296 Parent PID: 7164

General

Start time:	18:40:34
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 1364 Parent PID: 6904

General

Start time:	18:40:34
Start date:	22/11/2021
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\rEyeIgLUX.exe
Imagebase:	0xa80000
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: 6320 Parent PID: 1364

General

Start time:	18:40:35
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6348 Parent PID: 6904

General

Start time:	18:40:35
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rEyeIgLUX" /XML "C:\Users\user\AppData\Local\Temp\tmp467D.tmp
Imagebase:	0xb80000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 5180 Parent PID: 6348

General

Start time:	18:40:37
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe PID: 2800 Parent PID: 6904

General

Start time:	18:40:39
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe
Imagebase:	0x850000
File size:	528896 bytes
MD5 hash:	7BA9068DE522FCEF76DD98DC7E1D6F4E
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.00000000.713495925.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.713495925.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.713495925.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.709764931.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.709764931.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.709764931.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.755956371.00000000043A4000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.707589363.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.707589363.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.707589363.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.756004455.00000000043DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.756004455.00000000043DB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.713893383.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.713893383.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.713893383.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7040 Parent PID: 3424

General

Start time:	18:40:58

Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xb10000
File size:	528896 bytes
MD5 hash:	7BA9068DE522FCEF76DD98DC7E1D6F4E
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: 0000000E.00000002.775456783.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.775731201.0000000003406000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.777582585.0000000004312000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.777582585.0000000004312000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.777582585.0000000004312000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.778491014.0000000004520000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.778491014.0000000004520000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.778491014.0000000004520000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 29%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 7116 Parent PID: 7040

General

Start time:	18:41:00
Start date:	22/11/2021
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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xa80000
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: conhost.exe PID: 7072 Parent PID: 7116

General

Start time:	18:41:01
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 4876 Parent PID: 7040

General

Start time:	18:41:01
Start date:	22/11/2021
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\rEyeIgLUX.exe
Imagebase:	0xa80000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 5540 Parent PID: 4876

General

Start time:	18:41:02
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5912 Parent PID: 7040

General

Start time:	18:41:03
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\rEyeIgLUX" /XML "C:\Users\user\AppData\Local\Temp\tmpA8E1.tmp
Imagebase:	0xb80000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4648 Parent PID: 5912

General

Start time:	18:41:05
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 4596 Parent PID: 7040

General

Start time:	18:41:07
Start date:	22/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x5d0000
File size:	528896 bytes
MD5 hash:	7BA9068DE522FCEF76DD98DC7E1D6F4E
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: 00000015.00000000.768345508.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.768345508.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.768345508.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.766081622.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.766081622.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.766081622.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.787863880.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.787863880.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.787863880.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.790219362.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.790219362.0000000002D91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.770033827.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.770033827.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.770033827.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.790326430.0000000003D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.790326430.0000000003D91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.766641531.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.766641531.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.766641531.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis