ID: 433312
Sample Name: OUTSTANDING INVOICE.pdf.scr
Cookbook: default.jbs
Time: 16:09:16
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report OUTSTANDING INVOICE.pdf.scr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Signature Overview 6
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Persistence and Installation Behavior: 7
Hooking and other Techniques for Hiding and Protection: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
Private 12
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 19
Imports 19
Version Infos 19
Possible Origin 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19

Code Manipulations 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: OUTSTANDING INVOICE.pdf.exe PID: 6484 Parent PID: 6132 20
General 20
File Activities 21
File Created 21
File Written 21
File Read 21
Registry Activities 21
Analysis Process: windows update.exe PID: 5072 Parent PID: 6484 21
General 21
File Activities 21
File Created 21
File Written 21
File Read 21
Registry Activities 21
Analysis Process: windows update.exe PID: 4552 Parent PID: 3424 21
General 21
File Activities 22
File Created 22
File Written 22
File Read 22
Analysis Process: InstallUtil.exe PID: 6684 Parent PID: 4552 22
General 22
File Activities 23
File Created 23
File Written 23
File Read 23
Analysis Process: windows update.exe PID: 4648 Parent PID: 4552 23
General 23
Analysis Process: windows update.exe PID: 6548 Parent PID: 4648 24
General 24
Analysis Process: windows update.exe PID: 4484 Parent PID: 4552 24
General 24
Analysis Process: windows update.exe PID: 5472 Parent PID: 4484 24
General 24
Analysis Process: windows update.exe PID: 5604 Parent PID: 4552 24
General 25
Analysis Process: windows update.exe PID: 6460 Parent PID: 5604 25
General 25
Analysis Process: windows update.exe PID: 4868 Parent PID: 4552 25
General 25
Analysis Process: windows update.exe PID: 6648 Parent PID: 4868 25
General 25
Analysis Process: windows update.exe PID: 6956 Parent PID: 4552 26
General 26
Analysis Process: windows update.exe PID: 6820 Parent PID: 6956 26
General 26
Analysis Process: windows update.exe PID: 4944 Parent PID: 4552 26
General 26
Analysis Process: windows update.exe PID: 4672 Parent PID: 4944 27
General 27
Analysis Process: windows update.exe PID: 1364 Parent PID: 4552 27
General 27
Analysis Process: windows update.exe PID: 6128 Parent PID: 1364 27
General 27
Analysis Process: windows update.exe PID: 684 Parent PID: 4552 27
General 27
Analysis Process: windows update.exe PID: 4856 Parent PID: 684 28
General 28
Analysis Process: windows update.exe PID: 5504 Parent PID: 4552 28
General 28
Analysis Process: windows update.exe PID: 5448 Parent PID: 5504 28
General 28
Analysis Process: windows update.exe PID: 5796 Parent PID: 4552 29
General 29
Analysis Process: windows update.exe PID: 6384 Parent PID: 5796 29
General 29
Analysis Process: windows update.exe PID: 5664 Parent PID: 4552 29
General 29
Analysis Process: windows update.exe PID: 1316 Parent PID: 5664 29
General 29
Analysis Process: windows update.exe PID: 7076 Parent PID: 4552 30
General 30
Disassembly 30
Code Analysis 30

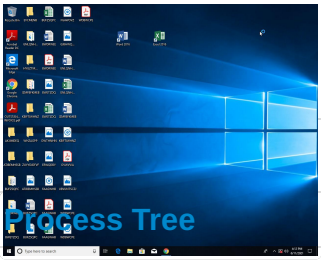
Analysis Report OUTSTANDING INVOICE.pdf.scr

Overview

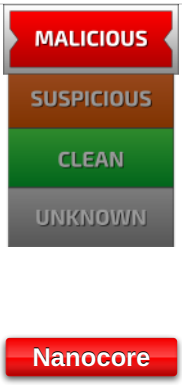
General Information

Sample Name:	OUTSTANDING INVOICE.pdf.scr (renamed file extension from scr to exe)
Analysis ID:	433312
MD5:	416ccd703aff884..
SHA1:	1db05b7beda1a9..
SHA256:	e1b2ca52707d72..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

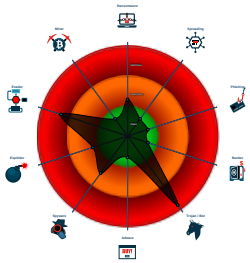


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Yara detected Nanocore RAT
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Drops PE files to the document folde…
- Hides that the sample has been dow…

Classification



- **System is w10x64**
- OUTSTANDING INVOICE.pdf.exe (PID: 6484 cmdline: 'C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe' MD5: 416CCD703AFF8844F0454E112F663C06)
  - windows update.exe (PID: 5072 cmdline: 'C:\Users\user\Documents\windows update.exe' MD5: 416CCD703AFF8844F0454E112F663C06)
- windows update.exe (PID: 4552 cmdline: 'C:\Users\user\Documents\windows update.exe' MD5: 416CCD703AFF8844F0454E112F663C06)
  - InstallUtil.exe (PID: 6684 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - windows update.exe (PID: 4648 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6548 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 4484 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 5472 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 5604 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6460 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 4868 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6648 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 6956 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6820 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 4944 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 4672 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 1364 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6128 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 684 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 4856 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 5504 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 5448 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 5796 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 6384 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 5664 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - windows update.exe (PID: 1316 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
  - windows update.exe (PID: 7076 cmdline: 'C:\Users\user\AppData\Local\Temp\windows update.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "e7a66d0e-8937-40e7-aaea-a267e5d3",
  "Group": "MAY 09 2021",
  "Domain1": "194.5.98.28",
  "Domain2": "brownhost22.ddns.net",
  "Port": 2021,
  "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
0000000B.00000000.738643631.000000000702000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000000.738643631.000000000702000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000000.738643631.000000000702000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000006.00000002.931537578.00000000037A9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10d8f:$x1: NanoCore.ClientPluginHost • 0x56b8d:$x1: NanoCore.ClientPluginHost • 0x10dcc:$x2: IClientNetworkHost • 0x56bca:$x2: IClientNetworkHost • 0x148ff:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x5a6fd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000002.931537578.00000000037A9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.windows update.exe.36d8222.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
6.2.windows update.exe.36d8222.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
6.2.windows update.exe.36d8222.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.2.windows update.exe.36d8222.5.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
6.2.windows update.exe.37efa00.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 105 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- 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:

- 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)
- .NET source code contains very large array initializations
- Initial sample is a PE file and has a suspicious name

Persistence and Installation Behavior:

- Drops PE files to the document folder of the user

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)
- Uses an obfuscated file name to hide its real file extension (double extension)

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

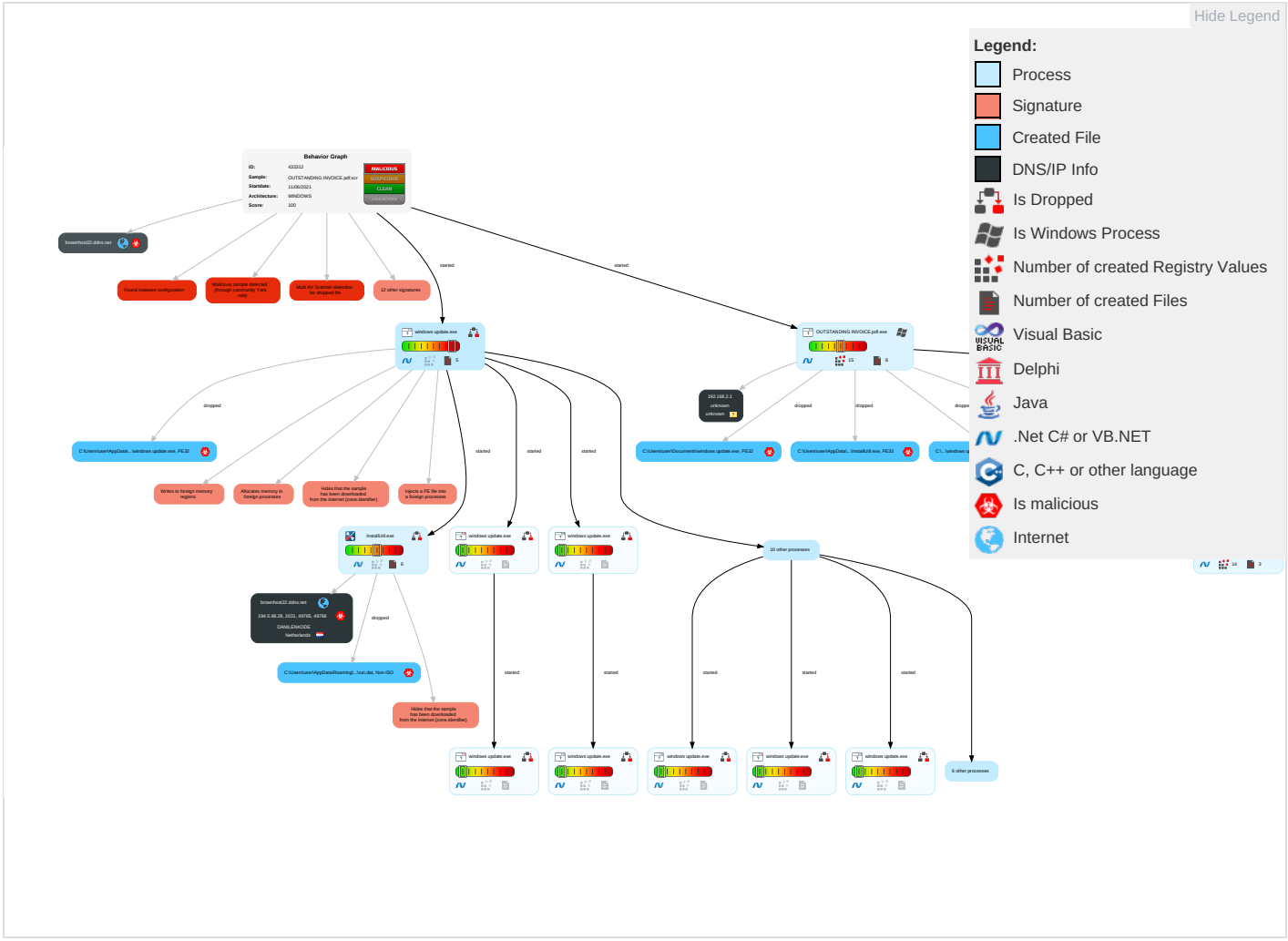
Remote Access Functionality:

- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts 1	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 2 1	File and Directory Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 1 2	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Non-S Port 1
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Software Packing 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Remot Softwa
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Timestomp 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applic Layer Protoc
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Applic Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer I
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
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 Tr Protoc

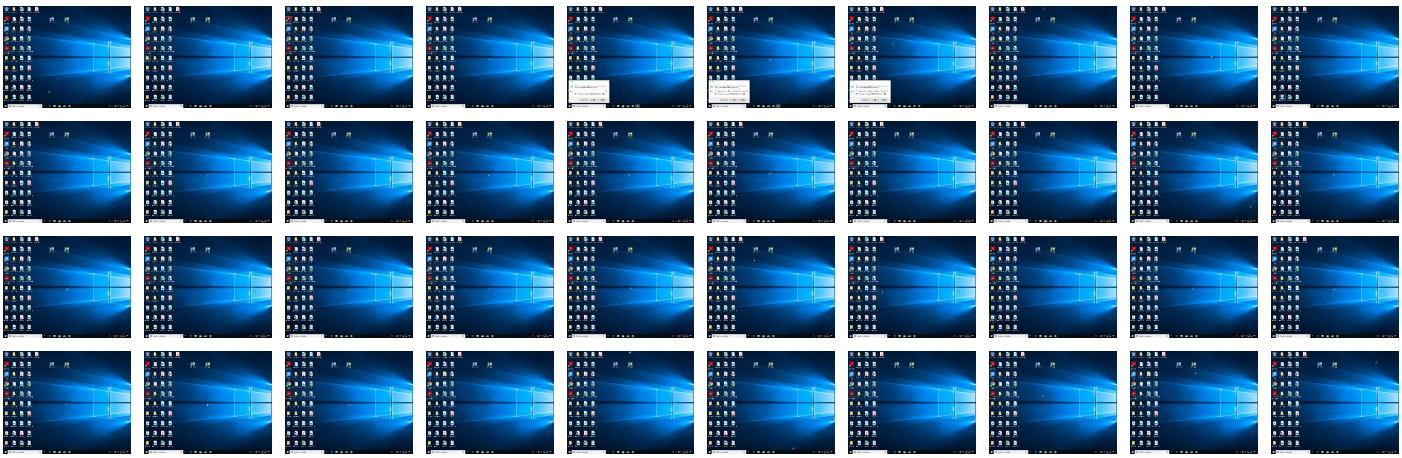
Behavior Graph



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
OUTSTANDING INVOICE.pdf.exe	26%	Virustotal		Browse
OUTSTANDING INVOICE.pdf.exe	52%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
OUTSTANDING INVOICE.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\Documents\windows update.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\windows update.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\windows update.exe	13%	ReversingLabs		
C:\Users\user\Documents\windows update.exe	52%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.InstallUtil.exe.58b0000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.2.InstallUtil.exe.700000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
11.0.InstallUtil.exe.700000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.InstallUtil.exe.700000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
brownhost22.ddns.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://https://www.google.	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ns.adobe.c/gMa	0%	Avira URL Cloud	safe	
brownhost22.ddns.net	1%	Virustotal		Browse
brownhost22.ddns.net	0%	Avira URL Cloud	safe	
http://ns.d	0%	Avira URL Cloud	safe	
http://https://www.google.h	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://www.google.imag	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
194.5.98.28	0%	Avira URL Cloud	safe	
http://https://www.google.$	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
brownhost22.ddns.net	194.5.98.28	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
brownhost22.ddns.net	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
194.5.98.28	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.28	brownhost22.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433312
Start date:	11.06.2021
Start time:	16:09:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OUTSTANDING INVOICE.pdf.scr (renamed file extension from scr to 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:	40
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@54/32@8/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.5%) • Quality average: 49.5% • Quality standard deviation: 38.3%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:10:20	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\windows update.lnk

Time	Type	Description
16:10:27	API Interceptor	1x Sleep call for process: OUTSTANDING INVOICE.pdf.exe modified
16:10:35	API Interceptor	1x Sleep call for process: windows update.exe modified
16:10:52	API Interceptor	648x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.28	Folha de dados de cota#U00e7#U00e3o para nossa empresa doc.exe	Get hash	malicious	Browse	
	Folha de dados de cota#U00e7#U00e3o para nossa empresa doc.exe	Get hash	malicious	Browse	
	27RFQ.exe	Get hash	malicious	Browse	
	32RFQ.exe	Get hash	malicious	Browse	
	3Agent Registration Update on PAGA.xlsx.exe	Get hash	malicious	Browse	
	20New Price list Update On DSTV&GOTV For Easter Bonus.xlsx.exe	Get hash	malicious	Browse	
	46Recently Updated On Our Pricing And Commissions On Paga.xlsx.exe	Get hash	malicious	Browse	
	9PAGA Commission Analysis On Bill Payment And Airtime for the month of march 2019.pdf.exe	Get hash	malicious	Browse	
	31ACTIVATION TEMPLATE.xlsx.exe	Get hash	malicious	Browse	
	3Paga Agent Bonus Activation For The Month Of March 2019.pdf.exe	Get hash	malicious	Browse	
	19Important Verification Information Update On QT Paypoint.xlsx.exe	Get hash	malicious	Browse	
	35Agent price update as at 21st of March 2019.xlsx.exe	Get hash	malicious	Browse	
	54AGENT GUIDE DOCUMENT.pdf.exe	Get hash	malicious	Browse	
	3OFFER LETTER.pdf.exe	Get hash	malicious	Browse	
	612019 DEALERS CONFERENCE REPORT ON DSTVGOTV AGENT.pdf.exe	Get hash	malicious	Browse	
	18new pricing on Quickteller Paypoint & Multi Choice.xlsx.exe	Get hash	malicious	Browse	
	37SWAP TEMPLATE-DEALERS.pdf.exe	Get hash	malicious	Browse	
	1Quickteller Paypoint - Transaction Statement For January 2019.pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Request Letter for Courtesy Call.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	SecuriteInfo.com.Heur.23766.xls	Get hash	malicious	Browse	• 194.5.97.241
	SwiftCopy.pdf.exe	Get hash	malicious	Browse	• 194.5.98.31
	wlCqbMRJ7p.exe	Get hash	malicious	Browse	• 194.5.98.5
	SecuriteInfo.com.Trojan.PackedNET.832.3222.exe	Get hash	malicious	Browse	• 194.5.98.144
	SecuriteInfo.com.Trojan.PackedNET.831.12541.exe	Get hash	malicious	Browse	• 194.5.98.144
	0Cg1YYs1sv.exe	Get hash	malicious	Browse	• 194.5.98.144
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	DEPOSITAR.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	InvoicePOzGlybgcIc1vHasG.exe	Get hash	malicious	Browse	• 194.5.98.87
	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87
	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61
	DHL_file.exe	Get hash	malicious	Browse	• 194.5.98.145

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\windows update.exe	SecuriteInfo.com.Variant.Razy.840898.18291.exe	Get hash	malicious	Browse	
	68Aj4oxPok.exe	Get hash	malicious	Browse	
	Ysur2E8xPs.exe	Get hash	malicious	Browse	
	payment swift copy.exe	Get hash	malicious	Browse	
	I201002X430 CIF #20210604.exe	Get hash	malicious	Browse	
	PO_66202009475352576 62_Arabico.PDF.exe	Get hash	malicious	Browse	
	s.exe	Get hash	malicious	Browse	
	PO_66202009475352576 61_Arabico.PDF.exe	Get hash	malicious	Browse	
	MV.exe	Get hash	malicious	Browse	
	e.exe	Get hash	malicious	Browse	
	RFQ9088QTY.exe	Get hash	malicious	Browse	
	SRESTKM-series.exe	Get hash	malicious	Browse	
	All Details.exe	Get hash	malicious	Browse	
	Property Samples 1.exe	Get hash	malicious	Browse	
	malwa.exe	Get hash	malicious	Browse	
	Sorted Properties.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.jc.exe	Get hash	malicious	Browse	
	47432000083600.xlsx	Get hash	malicious	Browse	
	Mortgage Description.exe	Get hash	malicious	Browse	
	jf6RU7vl5Y.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	qe8V4QGYIK.exe	Get hash	malicious	Browse	
	POD0608.doc	Get hash	malicious	Browse	
	SKM__C20192910887888001990.pdf.exe	Get hash	malicious	Browse	
	http___pbfoa.org_f.exe	Get hash	malicious	Browse	
	DHL_June 2021 at 7.M_9B7290_PDF.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.46369990.8945.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.480664.28948.exe	Get hash	malicious	Browse	
	Halkbank_Ekstre_20210206_080203_744632.exe	Get hash	malicious	Browse	
	Halkbank_Ekstre_20210602_080203_744632.exe	Get hash	malicious	Browse	
	ONS-2_exe.exe	Get hash	malicious	Browse	
	mvJMfkrri8.exe	Get hash	malicious	Browse	
	1X6McyRQlO.exe	Get hash	malicious	Browse	
	Halkbank_Ekstre_20210528_080203_744632.exe	Get hash	malicious	Browse	
	CYGK8igofD.exe	Get hash	malicious	Browse	
	Halkbank_Ekstre_20210526_080203_744632.exe	Get hash	malicious	Browse	
	SKBMT_0052Statement gpj.exe	Get hash	malicious	Browse	
	PO#903_2224_NGUYEN_LINH_SERVICE_AND_TRADINGS_COx.exe	Get hash	malicious	Browse	
	RFQ#1875-ET1-002.eXE	Get hash	malicious	Browse	
	V99tNu1MCy.exe	Get hash	malicious	Browse	
	Patch.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OUTSTANDING INVOICE.pdf.exe.log

Process:	C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\OUTSTANDING INVOICE.pdf.exe.log	
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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.Co

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\windows update.exe.log	
Process:	C:\Users\user\Documents\windows update.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnoe
MD5:	F2152F0304453BCFB93E6D4F93C3F0DC
SHA1:	DD69A4D7F9F9C8D97F1DF535BA3949E9325B5A2F
SHA-256:	5A4D59CD30A1AF620B87602BC23A3F1EFEF792884053DAE6A89D1AC9AAD4A411
SHA-512:	02402D9EAA2DF813F83A265C31D00048F84AD18AE23935B428062A9E09B173B13E93A3CACC6547277DA6F937BBC413B839620BA600144739DA37086E03DD8B4F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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.Co

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: qe8V4QGYIK.exe, Detection: malicious, Browse • Filename: POD0608.doc, Detection: malicious, Browse • Filename: SKM__C20192910887888001990.pdf.exe, Detection: malicious, Browse • Filename: http___pbfoa.org_f.exe, Detection: malicious, Browse • Filename: DHL_June 2021 at 7.M_9B7290_PDF.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.46369990.8945.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.480664.28948.exe, Detection: malicious, Browse • Filename: Halkbank_Ekstre_20210206_080203_744632.exe, Detection: malicious, Browse • Filename: Halkbank_Ekstre_20210602_080203_744632.exe, Detection: malicious, Browse • Filename: ONS-2_exe.exe, Detection: malicious, Browse • Filename: mvJMfkrri8.exe, Detection: malicious, Browse • Filename: 1X6McyRQlO.exe, Detection: malicious, Browse • Filename: Halkbank_Ekstre_20210528_080203_744632.exe, Detection: malicious, Browse • Filename: CYGK8igofD.exe, Detection: malicious, Browse • Filename: Halkbank_Ekstre_20210526_080203_744632.exe, Detection: malicious, Browse • Filename: SKBMT_0052Statement gpj.exe, Detection: malicious, Browse • Filename: PO#903_2224_NGUYEN_LINH_SERVICE_AND_TRADINGS_COx.exe, Detection: malicious, Browse • Filename: RFQ#1875-ET1-002.eXE, Detection: malicious, Browse • Filename: V99tNu1MCy.exe, Detection: malicious, Browse • Filename: Patch.exe, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... ....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Temp\windows update.exe	
Process:	C:\Users\user\Documents\windows update.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	4.369296705546591
Encrypted:	false
SSDEEP:	768:jlU4+MS3Fu0thSOV4GM0SuHk9Oh/1TRIWUk7NlfaNV9KQLxXXSv:l6o03IGMLuHk+Ck5lfaNP7xSv
MD5:	0E362E7005823D0BEC3719B902ED6D62
SHA1:	590D860B909804349E0CDC2F1662B37BD62F7463
SHA-256:	2D0DC6216F613AC7551A7E70A798C22AEE8EB9819428B1357E2B8C73BEF905AD
SHA-512:	518991B68496B3F8545E418CF9B345E0791E09CC20D177B8AA47E0ABA447AA55383C64F5BDACA39F2B061A5D08C16F2AD484AF8A9F238CA23AB081618FBA3AD3
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Variant.Razy.840898.18291.exe, Detection: malicious, Browse • Filename: 68Aj4oxPok.exe, Detection: malicious, Browse • Filename: Ysur2E8xPs.exe, Detection: malicious, Browse • Filename: payment swift copy.exe, Detection: malicious, Browse • Filename: I201002X430 CIF #20210604.exe, Detection: malicious, Browse • Filename: PO_662020094753525766 2_Arabico.PDF.exe, Detection: malicious, Browse • Filename: s.exe, Detection: malicious, Browse • Filename: PO_662020094753525766 1_Arabico.PDF.exe, Detection: malicious, Browse • Filename: MV.exe, Detection: malicious, Browse • Filename: e.exe, Detection: malicious, Browse • Filename: RFQ9088QTY.exe, Detection: malicious, Browse • Filename: SRESTKM-series.exe, Detection: malicious, Browse • Filename: All Details.exe, Detection: malicious, Browse • Filename: Property Samples 1.exe, Detection: malicious, Browse • Filename: malwa.exe, Detection: malicious, Browse • Filename: Sorted Properties.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.BehavesLike.Win32.Generic.jc.exe, Detection: malicious, Browse • Filename: 47432000083600.xlsx, Detection: malicious, Browse • Filename: Mortgage Description.exe, Detection: malicious, Browse • Filename: jf6RU7vI5Y.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y .....P..&.....D... .....@.. ....`.....D..W...`.....hD..... ....H.....text....$... ...&..... ..`.rsrc.....`.....(.....@..@.rel oc.....0.....@..B.....D.....H.....l....%.....).....0..6.....(8...t....&.(8...t....&.....(8...t.....8;....8%.....(8...t....&.(8...t..... .:.....(8...t....:.....(8...t....:....(8...t.....\:@....(8...t....&.)...&8.....(8...t....&(8...t....&.....:.....8x.....:L...88....(8...t....&(8...t....&(8...t....&(8...t.....:....8!..... (8...t....&.....(8...t....&.....(8...t....:8.....(8...t....&.

C:\Users\user\AppData\Local\Temp\windows update.txt	
Process:	C:\Users\user\AppData\Local\Temp\windows update.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.67255728631531
Encrypted:	false
SSDEEP:	3:1RPt+coAl+rpdgyn:jwNADyn
MD5:	B123C14157021A4A8CBB20A6A79CADF2
SHA1:	453A4D2A9D0EE7B92410B61D0EE2B9E376673F66
SHA-256:	135B683A083C792F3BBE477AD0B4387FF52E525AF7B5E9BDEE2DBAEE90415521
SHA-512:	12908F27A937DCA23C6CEB299A57916F5DAFD9BC69ABB195E1CC140BDAE677F6817D40DB90AF56CF56463BD34ED96537127B2050784228A09F73E753CB0E3A2
Malicious:	false
Preview:	4552..C:\Users\user\Documents\windows update.exe..7076..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:OH+n:Oen
MD5:	8E40229D25FAFCE8413383CD73D05F6D
SHA1:	C0B22276D7342D7FFF71039D3F154DEF7CD6C879
SHA-256:	F64C0C11CFD8BF8725860EF9CD54F540A2D1FB3FD807DDAF163DD3C94EB5E529
SHA-512:	DFCFA538CB853142C93834A1DB4F5A114F5418296CCE950CD85EDF1487218EAAD9A79717DEF3030887AA5F53DBB67BD9E04E30798312C027C179917CE647F45
Malicious:	**true**
Preview:	_....,.H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\windows update.lnk	
Process:	C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	886
Entropy (8bit):	3.231105392562601
Encrypted:	false
SSDEEP:	12:8wl0y0sXowAOcuJEIx+0OS503oR9S50XgRN1A4t2Y+xIBjK:8KLgr0Oi0Yri0Xg+7aB
MD5:	7837A5262A520E094F689075739AA11A
SHA1:	C18E43A81700E883BADA63011A13C4FCE1EE76E4
SHA-256:	FAB5A94E97A4424EF7881F1248EC45B8E08196138B01658C2707631D04FEC7C6
SHA-512:	0110EE04C937CE5DF98DBFBBBE33F71DB30277D5C7F73FDB997C9C2639B15E218C60BF93C8C95CC98697369C1F79805A8BE453836611B6FE0CCF9DB853C7CF4
Malicious:	false
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<.....j.o.n.e.s.....\.1.....Documents.D.....D.o.c.u.m.e.n.t.s.....x.2.....windows update.exe..V.....w.i.n.d.o.w.s. .u.p.d.a.t.e...e.x.e..."...1.....\.....\.....\.....\.....\.....\.....\.D.o.c.u.m.e.n.t.s.\.w.i.n.d.o.w.s. .u.p.d.a.t.e...e.x.e.+.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.D.o.c.u.m.e.n.t.s.\.w.i.n.d.o.w.s. .u.p.d.a.t.e...e.x.e.....).....#.F..I.H.i.).....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

C:\Users\user\Documents\windows update.exe	
Process:	C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	759808
Entropy (8bit):	6.605601315429397
Encrypted:	false
SSDEEP:	12288:RjMA4cScHfc4eucIV7B+Aci98+WrWwYPF+h3HjsrGAUyE:RjEkfDxcc7Bud6fPFUz4GlB
MD5:	416CCD703AFF8844F0454E112F663C06
SHA1:	1DB05B7BEDA1A9E4FB0C4CD8E04C512C98EFDF3C
SHA-256:	E1B2CA52707D724682E2C2618EB33899B019E8650E325E800E43E2042231F55D
SHA-512:	D44EC955BE8247D6F6CD4C5AC7DC714142560A5378AF0DA9A3C0A1E0D871A5D12137226657E55B10FE4296CD5BB0EBB64DE8852678CCFBB868FF1C591B66312
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 52%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!..Y.....f...0.....>.... .....@.. .....`.....S.....,..... ..... ..H.....text...Dd... ...f..... ..`.rsrc....,.....h.....@..@.reloc.....@..B..... .....H.....O.....R.....:...%.k...hs.mx!.cQu5..l{K....ynPn..oO.. c...0r.cg.J...O..dX.....4..9*..]....K....gK.]..o\!.<...s.)<....js9!...K.}...|lqr(.....Pd.d(l.\.....4.%.4.1.....H..g.....C..v...h.t.i.....3.l.....,.k.....,.q.....~...N.3.....z..D.....A.....g...E.7.....a...B.*.../...;.;.|..+.>.3.)."]7+.q.)+B.L.D.....0.....p.....5...!.,).

C:\Users\user\Documents\windows update.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\OUTSTANDING INVOICE.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:\Users\user\Documents\windows update.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.605601315429397
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	OUTSTANDING INVOICE.pdf.exe
File size:	759808
MD5:	416ccd703aff8844f0454e112f663c06
SHA1:	1db05b7beda1a9e4fb0c4cd8e04c512c98efdf3c
SHA256:	e1b2ca52707d724682e2c2618eb33899b019e8650e325e800e43e2042231f55d
SHA512:	d44ec955be8247d6f6cd4c5ac7dc714142560a5378af0da9a3c0a1e0d871a5d12137226657e55b10fe4296cd5bb0ebb64de8852678ccfbb868ff1c591b6631a2
SSDEEP:	12288:RjMA4cScHfc4eucIV7B+Aci98+WrWwYPF+h3HjsrGAUyE:RjEkfDxcc7Bud6fPFUz4GlB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!..Y.....f...0.....>.... .....@.. .....` .....

File Icon

Icon Hash:	4e9292f2c88cd3cc

Static PE Info

General

Entrypoint:	0x4b843e
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, HIGH_ENTROPY_VA
Time Stamp:	0x5910BC21 [Mon May 8 18:42:41 2017 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	0xb6444	0xb6600	False	0.63441221513	data	6.6286481102	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xba000	0x2c2e	0x2e00	False	0.143597146739	data	3.22794117168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	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

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:11:10.420857906 CEST	192.168.2.4	8.8.8.8	0xd7af	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:15.808563948 CEST	192.168.2.4	8.8.8.8	0x2041	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:21.331908941 CEST	192.168.2.4	8.8.8.8	0x5a09	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:42.466228008 CEST	192.168.2.4	8.8.8.8	0x5c75	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:47.852722883 CEST	192.168.2.4	8.8.8.8	0x1911	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:53.194025993 CEST	192.168.2.4	8.8.8.8	0x4fc	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:12:14.333482027 CEST	192.168.2.4	8.8.8.8	0xec22	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:12:19.632985115 CEST	192.168.2.4	8.8.8.8	0x4224	Standard query (0)	brownhost2 2.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:11:10.484180927 CEST	8.8.8.8	192.168.2.4	0xd7af	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:15.867630959 CEST	8.8.8.8	192.168.2.4	0x2041	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:21.392391920 CEST	8.8.8.8	192.168.2.4	0x5a09	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:11:42.527839899 CEST	8.8.8.8	192.168.2.4	0x5c75	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:47.914501905 CEST	8.8.8.8	192.168.2.4	0x1911	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:11:53.255685091 CEST	8.8.8.8	192.168.2.4	0x4fc	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:12:14.391980886 CEST	8.8.8.8	192.168.2.4	0xec22	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)
Jun 11, 2021 16:12:19.693648100 CEST	8.8.8.8	192.168.2.4	0x4224	No error (0)	brownhost2 2.ddns.net		194.5.98.28	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: OUTSTANDING INVOICE.pdf.exe PID: 6484 Parent PID: 6132

General

Start time:	16:10:03
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OUTSTANDING INVOICE.pdf.exe'
Imagebase:	0x4e0000
File size:	759808 bytes
MD5 hash:	416CCD703AFF8844F0454E112F663C06
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.698113969.0000000003AAA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.698113969.0000000003AAA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.698113969.0000000003AAA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.697836109.000000000394C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.697836109.000000000394C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.697836109.000000000394C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: windows update.exe PID: 5072 Parent PID: 6484

General

Start time:	16:10:26
Start date:	11/06/2021
Path:	C:\Users\user\Documents\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Documents\windows update.exe'
Imagebase:	0x740000
File size:	759808 bytes
MD5 hash:	416CCD703AFF8844F0454E112F663C06
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 52%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: windows update.exe PID: 4552 Parent PID: 3424

General

Start time:	16:10:28
Start date:	11/06/2021
Path:	C:\Users\user\Documents\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Documents\windows update.exe'
Imagebase:	0xc0000
File size:	759808 bytes
MD5 hash:	416CCD703AFF8844F0454E112F663C06
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: 00000006.00000002.931537578.00000000037A9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.931537578.00000000037A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.931537578.00000000037A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.931420211.000000000364C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.931420211.000000000364C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.931420211.000000000364C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.931144467.0000000003528000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.931144467.0000000003528000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.931144467.0000000003528000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: InstallUtil.exe PID: 6684 Parent PID: 4552

General

Start time:	16:10:46
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x310000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 0000000B.00000000.738643631.0000000000702000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.738643631.0000000000702000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.738643631.0000000000702000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.738992009.0000000000702000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.738992009.0000000000702000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.738992009.0000000000702000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.925828807.0000000003659000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.925828807.0000000003659000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.914832988.0000000000702000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.914832988.0000000000702000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.914832988.0000000000702000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.929762962.0000000004FE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.929762962.0000000004FE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.930250382.00000000058B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.930250382.00000000058B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.930250382.00000000058B0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: windows update.exe PID: 4648 Parent PID: 4552

General

Start time:	16:10:53
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x820000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Antivirus matches:	• Detection: 14%, Metadefender, Browse • Detection: 13%, ReversingLabs
Reputation:	moderate

Analysis Process: windows update.exe PID: 6548 Parent PID: 4648

General

Start time:	16:10:56
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x160000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 4484 Parent PID: 4552

General

Start time:	16:11:00
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xa40000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 5472 Parent PID: 4484

General

Start time:	16:11:01
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xad0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 5604 Parent PID: 4552

General

Start time:	16:11:06
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xf90000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 6460 Parent PID: 5604

General

Start time:	16:11:07
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x920000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 4868 Parent PID: 4552

General

Start time:	16:11:11
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xd50000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 6648 Parent PID: 4868

General

Start time:	16:11:14
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x450000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 6956 Parent PID: 4552

General

Start time:	16:11:18
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xc10000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 6820 Parent PID: 6956

General

Start time:	16:11:20
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x640000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: windows update.exe PID: 4944 Parent PID: 4552

General

Start time:	16:11:23
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x340000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Reputation:	moderate

Analysis Process: windows update.exe PID: 4672 Parent PID: 4944

General

Start time:	16:11:25
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xf50000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 1364 Parent PID: 4552

General

Start time:	16:11:29
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xaa0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 6128 Parent PID: 1364

General

Start time:	16:11:32
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x950000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 684 Parent PID: 4552

General

Start time:	16:11:36
Start date:	11/06/2021

Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x20000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 4856 Parent PID: 684

General

Start time:	16:11:38
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x240000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 5504 Parent PID: 4552

General

Start time:	16:11:41
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x2d0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 5448 Parent PID: 5504

General

Start time:	16:11:43
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xe90000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 5796 Parent PID: 4552

General

Start time:	16:11:47
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xaa0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 6384 Parent PID: 5796

General

Start time:	16:11:50
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x560000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 5664 Parent PID: 4552

General

Start time:	16:11:54
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xc30000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 1316 Parent PID: 5664

General

Start time:	16:11:56
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0xb30000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: windows update.exe PID: 7076 Parent PID: 4552

General

Start time:	16:12:00
Start date:	11/06/2021
Path:	C:\Users\user\AppData\Local\Temp\windows update.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\windows update.exe'
Imagebase:	0x4d0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis