ID: 451451
Sample Name: Inv-04_PDF.vbs
Cookbook: default.jbs
Time: 16:41:32
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

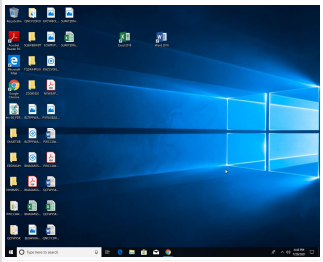
Windows Analysis Report Inv-04_PDF.vbs

Overview

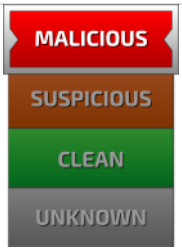
General Information

Sample Name:	Inv-04_PDF.vbs
Analysis ID:	451451
MD5:	457617bb66ce73..
SHA1:	a1e9d7b4f153da6.
SHA256:	ea11c7637e649d..
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection



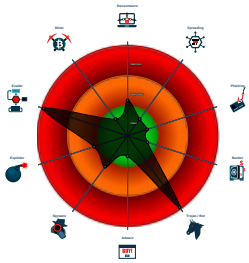
Nanocore AgentTesla

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

Signatures

- Benign windows process drops PE f…
- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- VBScript performs obfuscated calls …
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Creates an undocumented autostart …
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 800 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Inv-04_PDF.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - not.exe (PID: 3288 cmdline: 'C:\Users\user\AppData\Local\Temp\not.exe' MD5: 672E9FDC80F39F27F98A048B9F51AEA0)
    - InstallUtil.exe (PID: 1256 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - pad.exe (PID: 3864 cmdline: 'C:\Users\user\AppData\Local\Temp\pad.exe' MD5: E98879EEEFFC1846AB8765CE44E9E351)
    - pad.exe (PID: 4848 cmdline: C:\Users\user\AppData\Local\Temp\pad.exe MD5: E98879EEEFFC1846AB8765CE44E9E351)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Inv-04_PDF.vbs	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0x6f8ed:$: VFZxUUFBT • 0x1884ec:$: RWcVFBQU

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.377527863.000000000435 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.377527863.000000000435 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000015.00000002.467183565.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000015.00000002.467183565.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000015.00000002.467183565.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
Click to see the 65 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.pad.exe.71d0000.34.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
21.2.pad.exe.71d0000.34.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
21.2.pad.exe.7170000.29.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
21.2.pad.exe.7170000.29.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
21.2.pad.exe.71c0000.33.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
Click to see the 149 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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Networking:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

Yara detected AgentTesla

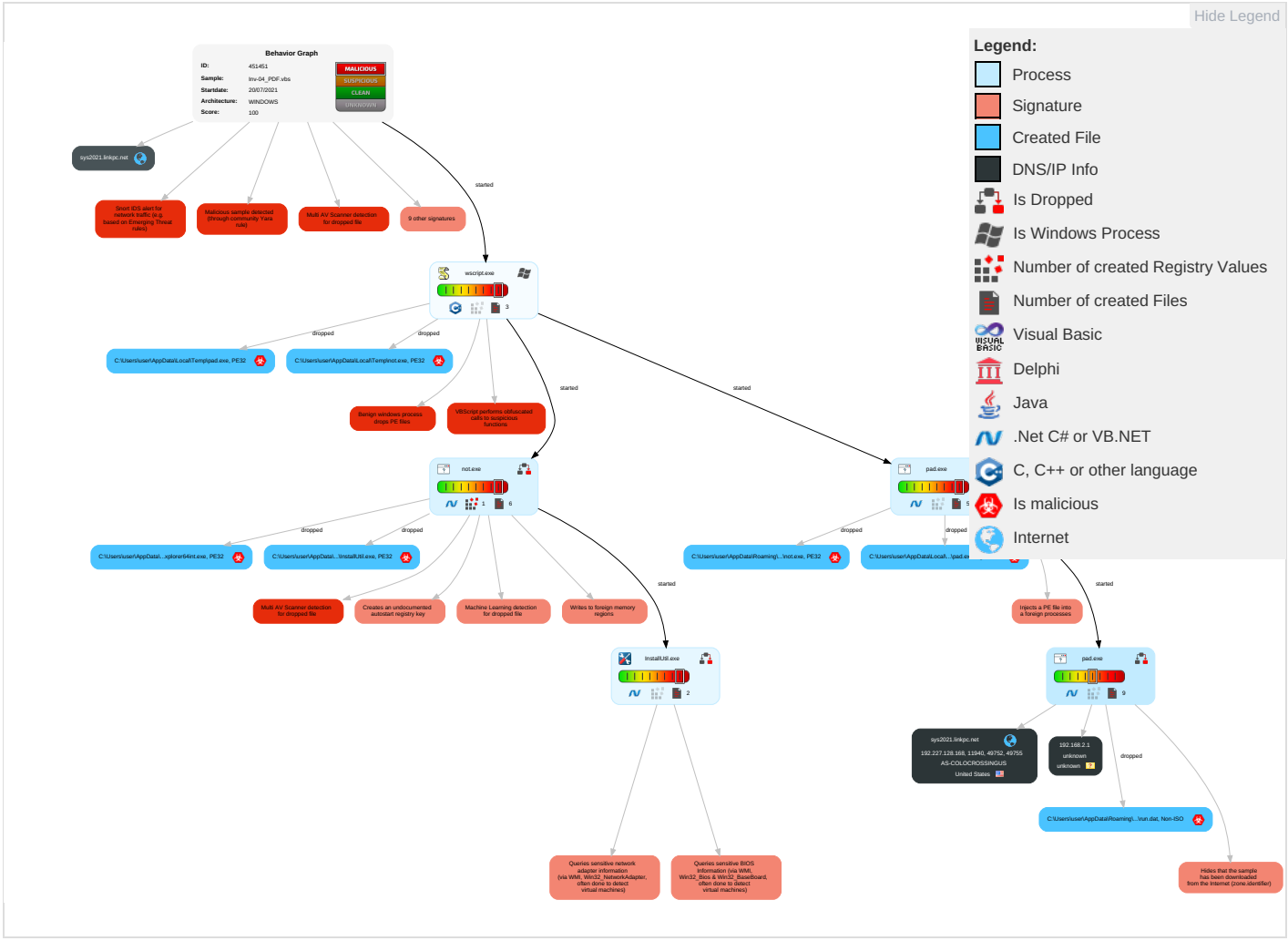
Yara detected AgentTesla

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1 2 1	Registry Run Keys / Startup Folder 1 1	Process Injection 2 1 2	Scripting 1 2 1	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 1	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
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/Obfuscate Non-C2 Protocol

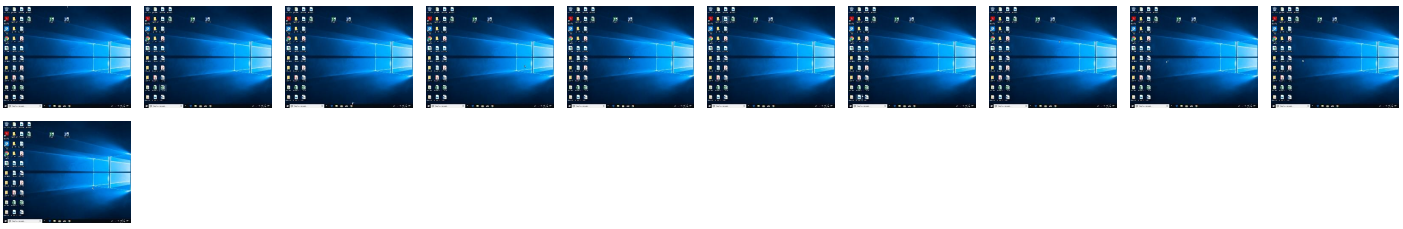
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Inv-04_PDF.vbs	28%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\not.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\eXPLorerInternet64\Explorer64int.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\not.exe	17%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\pad.exe	13%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepad\not.exe	13%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
C:\Users\user\AppData\Roaming\eXPLorerInternet64\Explorer64int.exe	17%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
21.2.pad.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.pad.exe.60e0000.23.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitudE	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsivw	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr8	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/a	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.founder.com.cn/cnm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.sandoll.co.krT	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krcom	0%	Avira URL Cloud	safe	
http://www.fontbureau.comT.TTFh	0%	Avira URL Cloud	safe	
http://gKSfZA.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.sandoll.co.krF	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.comldh	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasa	0%	Avira URL Cloud	safe	
http://www.fontbureau.comL	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.carterandcone.como.U	0%	Avira URL Cloud	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sys2021.linkpc.net	192.227.128.168	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.227.128.168	sys2021.linkpc.net	United States		36352	AS-COLOCROSSINGUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451451
Start date:	20.07.2021
Start time:	16:41:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Inv-04_PDF.vbs
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:	26
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.winVBS@9/11@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.4% (good quality ratio 3.3%) • Quality average: 42% • Quality standard deviation: 32.7%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:43:43	API Interceptor	336x Sleep call for process: pad.exe modified
16:44:03	API Interceptor	182x Sleep call for process: InstallUtil.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\not.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\not.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	5.353835388147306
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	D7428B0428DC5FA72A41122D265CFA0E
SHA1:	F485E2EC6F980F218063AF527724C088617B3B94
SHA-256:	C49B31FB28F5EC1B5A82D45DF4A0A88DBC26E468BA007D8E63C800BA69CC5FFC
SHA-512:	FD5BC965FD28DC219F2703726A34A7156D1B71B9199617136F936DD5DDBB2CA65175FBB4B761243635493D6CABE3069406B4D4473DEEB93FDCDA1F392345683
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\pad.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1299
Entropy (8bit):	5.353835388147306
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4xLE4qE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzg
MD5:	D7428B0428DC5FA72A41122D265CFA0E
SHA1:	F485E2EC6F980F218063AF527724C088617B3B94
SHA-256:	C49B31FB28F5EC1B5A82D45DF4A0A88DBC26E468BA007D8E63C800BA69CC5FFC
SHA-512:	FD5BC965FD28DC219F2703726A34A7156D1B71B9199617136F936DD5DDBB2CA65175FBB4B761243635493D6CABE3069406B4D4473DEEB93FDCDA1F392345683
Malicious:	**true**
Reputation:	unknown

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

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\InstallUtil.exe

Process:	C:\Users\user\AppData\Local\Temp\not.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:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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\not.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	861184
Entropy (8bit):	7.283904937853201
Encrypted:	false
SSDEEP:	24576:N+MOQW87bhQxtVUbJLy5yLlSKElPlHsQ2Ze:N+rQQxtVUREplD
MD5:	672E9FDC80F39F27F98A048B9F51AEA0
SHA1:	506479C1633363F4AC0276E59D6B66F648CF4A33
SHA-256:	A9497517888F5E6E725FA5AFD4FAED80EEC9F218438DBCCF2C9E6E1B37AA8ED1
SHA-512:	EB8BB241076CFBDA03DB01D20341CC73FD7A807CE33442528232941C89C2DA0007E0CEE339D82C27446C9310B00036D1816BE8E5F3A78EE85E37CDD4D9194EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y.....0.....@..... .. ....@.. ....@.....K.... ...<.....`..... ..... ..H.....text..... ..... .. ..`.rsrc....<... ...>.....@..@.reloc.....` .....".....@..B.....H.....1...-.....D_...J.....b.r...p}.....(.....(....*....0..B.....8&.....(....(... ....(.....(....(.....X....?.....{.....o....*..^.{....o.. ..9.....(....*^(.....s....o....*2(.....o....*....0..7.....rI..p(....(.....&.r_..p~....o.....(.....*.....0.....{....o....s....&.....o....(.....(.....*.....9.....{....9.....{....o..... (....*....0.....s....}.....s....}.....s....

C:\Users\user\AppData\Local\Temp\pad.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	910336
Entropy (8bit):	7.23755229212912
Encrypted:	false
SSDEEP:	24576:J+MOQW87bhQxtVUERugTkTicdXxMUjLOuy1B0sK1n:J+rQQxtVUYAfXmfNK
MD5:	E98879EEEFFC1846AB8765CE44E9E351
SHA1:	7E3DEE30D973F77C967275C9295AFB3BCBA8D7C4
SHA-256:	6C83263FC21CD5F86BFED551789EB3CAED34FB557C95EA12A557F400F5C1B043
SHA-512:	A21EF6DC8A390069F14053320402305C202A0D0C7ACFCB89C8D4743D4A53F58DBFDD7F345C62D4B6540A265CAF36AC03FA12432FC3DC99F7AD82BF079C2C1E6
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\pad.exe	
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....@..... .....@.. .....@..... ..@.....W.....<..... ..... ..H.....text..... ..... ..`.rsrc....<.....>.....@..@.reloc..... .....@..B.....H.....x.....(.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..'.....r...p.-.&&.(.....,& +.}....+.(....+.*..0..P.....-.&+7.+...(.....-.& .....-.&..(....(.....X.+.(....+.(....+....2..{.....o....*.0.....{....o....,..-.&+.(....+.*.0..!.....(.....-.&.....s....o....+.&+.*....0.....(.....-. &o....+.&+.*...0..E.....rE..p(...(!....,.&.-.+.&.r[..p~"...o#....-

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe
File Type:	data
Category:	dropped
Size (bytes):	1160
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	24:IQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+dQnybgC4jh+K:IknjhUknjhUknjhUknjhUknjhL
MD5:	7BEBBE1F1511163A3243CD8E0C75CC69
SHA1:	216B3AB5D802FA037A6EC5348B189398D8980B3C
SHA-256:	79A130865E9EFFFAA6C2E453942CE87F652681BCD76AAF987318300CAF5E3778
SHA-512:	4DCCB32411DEF72C938022B8675DA50B2DC4CD2C051B1C0377F63D6AAC42FC3D128B0ED580FB88954AB04A9E9EC8D272EBCCF74EB3F136BEF41ADBB845A1A 530
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:xt4:r4
MD5:	F6CFFA17DBE12B0A078E66EFB573E56C
SHA1:	6951DB8D370A1F3A2BE0BCCF36BCDAC15C59C8B2
SHA-256:	3EA55370EFCD3C4EBA9B95B4C60EF1151A456CABC670A2299DFCB43499B8B4AD
SHA-512:	7D770807274F4A0926A59BD4D3927F05206B2A37AC12C80D76B6A4F519240FA927FBE16889C3A761D52E9952DD4B93437D6082345406B61F42251425AF88CB7D
Malicious:	**true**
Reputation:	unknown
Preview:	...5.K.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe
File Type:	data
Category:	dropped
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
Reputation:	unknown
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wl8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v.'".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../....D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,...]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i.........$....$.......CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\notepad\not.exe	
Process:	C:\Users\user\AppData\Local\Temp\pad.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	910336
Entropy (8bit):	7.23755229212912
Encrypted:	false
SSDEEP:	24576:J+MOQW87bhQxtVUERugTkTicdXxMUjLOuy1B0sK1n:J+rQQxtVUYAfXmfNK
MD5:	E98879EEEFFC1846AB8765CE44E9E351
SHA1:	7E3DEE30D973F77C967275C9295AFB3BCBA8D7C4
SHA-256:	6C83263FC21CD5F86BFED551789EB3CAED34FB557C95EA12A557F400F5C1B043
SHA-512:	A21EF6DC8A390069F14053320402305C202A0D0C7ACFCB89C8D4743D4A53F58DBFDD7F345C62D4B6540A265CAF36AC03FA12432FC3DC99F7AD82BF079C2C1E6
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....@..... .....@.. .....@..... ..@.....W.....<..... ..... ..... ..H.....text..... ..... ..`.rsrc....<.....>.....@..@.reloc..... .....@..B.....H.....x.....(.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..'.....r...p.-.&&.(.....,.& +.}....+.(....+.*..0..P.....-.&+7.+...(.....-.& .....-.&..(....(.....X.+.(....+.(....+....2..{.....o....*.0.....{....o....,...-.&+.(....+.*.0..!.....(.....-.&.....s....o....+.&+.*....0.....(.....-. &o....+.&+.*...0..E.....rE..p(...(!....,.&.-.+.&.r[..p~"...o#....-

C:\Users\user\AppData\Roaming\eXPLorerInternet64\Explorer64int.exe	
Process:	C:\Users\user\AppData\Local\Temp\not.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	861184
Entropy (8bit):	7.283904937853201
Encrypted:	false
SSDEEP:	24576:N+MOQW87bhQxtVUbJLy5yLlSKElPlHsQ2Ze:N+rQQxtVUREplD
MD5:	672E9FDC80F39F27F98A048B9F51AEA0
SHA1:	506479C1633363F4AC0276E59D6B66F648CF4A33
SHA-256:	A9497517888F5E6E725FA5AFD4FAED80EEC9F218438DBCCF2C9E6E1B37AA8ED1
SHA-512:	EB8BB241076CFBDA03DB01D20341CC73FD7A807CE33442528232941C89C2DA0007E0CEE339D82C27446C9310B00036D1816BE8E5F3A78EE85E37CDD4D9194EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y.....0.....@..... .. ....@.. ....@.....K.... ...<.....`..... ..... ..H.....text..... ..... ..`.rsrc....<... ...>.....@..@.reloc.....` ....."..... .....@..B.....H.....1...-.....D_..J.....b.r...p}.....(.....(....*....0..B.....8&.....(....(... ....(.....(....(.....X....?.....{.....o....*..^.{....o.. ..9.....(....*^(.....s....o....*2(.....o....*....0..7.....rI..p(....(.....&.r_..p~....o.....(.....*.....0.,.....{....o....s....&.....o....(.....(.....*.....9.....{....9.....{....o..... (....*....0.....s....}.....s....}.....s....

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.889989493707388
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Inv-04_PDF.vbs
File size:	2456287
MD5:	457617bb66ce73bbc76af8d376469792
SHA1:	a1e9d7b4f153da6d345d6e8dd5d6923a260cff10
SHA256:	ea11c7637e649da3353f4d11ea0c03e95a53284bc57dc0 7f947ceb39e2d24230
SHA512:	0bd228909974157183b20da8825bc144a19274498d5c8d 0a2876b3375907f64b7494dc1566512ed48289a797013c 436ad9aaeb44aaabdee23b5b8e32e512a57c
SSDEEP:	24576:xEqf8Apx7oAYNFynaU4TjUuL42eM1p23LHi6dG Ws8mSrM1bNZYo+USqNcDxWHgGR:X7jsqObR18/zsq GpZP+jRGhyXtWw05p
File Content Preview:	on error resume next..Dim jwQEupTNVJLJrbyZcjRvoijZ OeJkqsMKdJPxclxumqbickVetieYsEYBMqpPgiXcwBgiL BxrlWlyGBxdJeqINnRZkOllvhODTzlaEmSslnnVvauKtL GBrOOJkHyxQLvDIEeHQWZXMyWaAvdKTaskbMLEkc qwoUcasjNrvmuXmiptsolodnepTKbvsaXofcjrVwhRhmP ggUx..'tXSMwTCTAqnHhHSyUPFrJyy

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/20/21-16:43:46.398528	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	11940	192.168.2.3	192.227.128.168
07/20/21-16:43:53.902338	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	11940	192.168.2.3	192.227.128.168
07/20/21-16:44:06.084065	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	11940	192.168.2.3	192.227.128.168
07/20/21-16:44:11.155063	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	11940	192.168.2.3	192.227.128.168
07/20/21-16:44:18.264924	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	11940	192.168.2.3	192.227.128.168
07/20/21-16:44:25.056672	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	11940	192.168.2.3	192.227.128.168

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 16:43:45.657146931 CEST	192.168.2.3	8.8.8.8	0xf809	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 16:43:53.672847986 CEST	192.168.2.3	8.8.8.8	0x677a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:01.179711103 CEST	192.168.2.3	8.8.8.8	0x9c9c	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:05.732892036 CEST	192.168.2.3	8.8.8.8	0x23d	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:10.865714073 CEST	192.168.2.3	8.8.8.8	0xafcb	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:18.043675900 CEST	192.168.2.3	8.8.8.8	0x9f1b	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:24.853782892 CEST	192.168.2.3	8.8.8.8	0x1bab	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 16:43:45.830271006 CEST	8.8.8.8	192.168.2.3	0xf809	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:43:53.734150887 CEST	8.8.8.8	192.168.2.3	0x677a	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:01.342683077 CEST	8.8.8.8	192.168.2.3	0x9c9c	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:05.790107965 CEST	8.8.8.8	192.168.2.3	0x23d	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:10.926053047 CEST	8.8.8.8	192.168.2.3	0xafcb	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:18.103776932 CEST	8.8.8.8	192.168.2.3	0x9f1b	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)
Jul 20, 2021 16:44:24.910593987 CEST	8.8.8.8	192.168.2.3	0x1bab	No error (0)	sys2021.linkpc.net		192.227.128.168	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 800 Parent PID: 3388

General

Start time:	16:42:19
Start date:	20/07/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Inv-04_PDF.vbs'
Imagebase:	0x7ff6ef2f0000

File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000003.204392554.0000024E8ED41000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000003.204019039.0000024E8ED41000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000003.203457786.0000024E8DE11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000003.203069676.0000024E8E011000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

Analysis Process: not.exe PID: 3288 Parent PID: 800

General

Start time:	16:42:24
Start date:	20/07/2021
Path:	C:\Users\user\AppData\Local\Temp\not.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\not.exe'
Imagebase:	0xaa0000
File size:	861184 bytes
MD5 hash:	672E9FDC80F39F27F98A048B9F51AEA0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.377527863.0000000004359000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.377527863.0000000004359000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.374626615.00000000033E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.374626615.00000000033E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.377677715.00000000043E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.377677715.00000000043E9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: pad.exe PID: 3864 Parent PID: 800

General

Start time:	16:42:25
Start date:	20/07/2021
Path:	C:\Users\user\AppData\Local\Temp\pad.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\pad.exe'
Imagebase:	0x160000
File size:	910336 bytes
MD5 hash:	E98879EEEFFC1846AB8765CE44E9E351
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: 00000005.00000002.381230315.000000000383F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.381230315.000000000383F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.381230315.000000000383F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.379844287.00000000035D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.379844287.00000000035D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.379844287.00000000035D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.377434610.0000000002669000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.377434610.0000000002669000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.379650089.0000000003581000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.379650089.0000000003581000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.379650089.0000000003581000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Modified

Analysis Process: InstallUtil.exe PID: 1256 Parent PID: 3288

General

Start time:	16:43:37
Start date:	20/07/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x7ff7488e0000
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: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.467182396.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.467182396.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.473068281.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.473068281.0000000002A11000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: pad.exe PID: 4848 Parent PID: 3864

General

Start time:	16:43:39
Start date:	20/07/2021
Path:	C:\Users\user\AppData\Local\Temp\pad.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\pad.exe
Imagebase:	0xa90000
File size:	910336 bytes
MD5 hash:	E98879EEEFFC1846AB8765CE44E9E351
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: 00000015.00000002.467183565.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.467183565.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.467183565.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482312137.0000000007140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482312137.0000000007140000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.479089175.0000000004299000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482506479.00000000071D0000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482506479.00000000071D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482440711.00000000071A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482440711.00000000071A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482479884.00000000071C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482479884.00000000071C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.478704472.0000000004001000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482402802.0000000007180000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482402802.0000000007180000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482100815.0000000006FA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482100815.0000000006FA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482341087.0000000007150000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482341087.0000000007150000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.478801230.000000000407C000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000015.00000002.478801230.000000000407C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482424636.0000000007190000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482424636.0000000007190000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.480997661.00000000060E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.480997661.00000000060E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.480997661.00000000060E0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482572860.0000000007210000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482572860.0000000007210000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482367619.0000000007160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482367619.0000000007160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.474083544.0000000002FB1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.481484843.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.481484843.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.482385656.0000000007170000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.482385656.0000000007170000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.480380824.0000000005670000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.480380824.0000000005670000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: NanoCore, Description: unknown, Source: 00000015.00000002.474351614.000000000301B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis