ID: 559231
Sample Name: Payment confirmation .exe
Cookbook: default.jbs
Time: 05:29:25
Date: 25/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

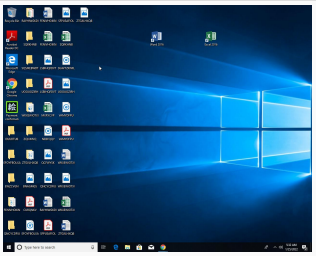
Windows Analysis Report

Payment confirmation .exe

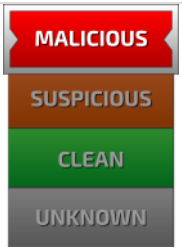
Overview

General Information

Sample Name:	Payment confirmation .exe
Analysis ID:	559231
MD5:	0d98108aa5a338.
SHA1:	e08d7ba0bf0ac4..
SHA256:	796f57da16fa76b.
Tags:	exe nanocore
Infos:	



Detection



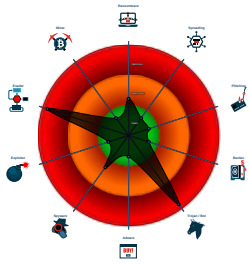
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a…
- Connects to many ports of the same…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Payment confirmation .exe (PID: 4540 cmdline: "C:\Users\user\Desktop\Payment confirmation .exe" MD5: 0D98108AA5A3383C2C3152CF2CD5AE9A)
  - powershell.exe (PID: 5776 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\iBGUhLU.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4688 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iBGUhLU" /XML "C:\Users\user\AppData\Local\Temp\tmp2497.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Payment confirmation .exe (PID: 5116 cmdline: C:\Users\user\Desktop\Payment confirmation .exe MD5: 0D98108AA5A3383C2C3152CF2CD5AE9A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "2616a878-9933-42e4-9fe0-3b57e29b",
  "Domain1": "naki.airdns.org",
  "Domain2": "37.120.210.211",
  "Port": 56281,
  "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": "faff0000",
  "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
00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000015.00000002.615775430.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000015.00000002.615775430.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x69457:$a: NanoCore • 0x694b0:$a: NanoCore • 0x694ed:$a: NanoCore • 0x69566:$a: NanoCore • 0x694b9:$b: ClientPlugin • 0x694f6:$b: ClientPlugin • 0x69df4:$b: ClientPlugin • 0x69e01:$b: ClientPlugin • 0x863c8:$b: ClientPlugin • 0x5f6e6:$e: KeepAlive • 0x69941:$g: LogClientMessage • 0x698c1:$i: get_Connected • 0x5f7cc:$j: #=q • 0x5f7e8:$j: #=q • 0x5f804:$j: #=q • 0x5f820:$j: #=q • 0x5f83c:$j: #=q • 0x5f86c:$j: #=q • 0x5f89c:$j: #=q • 0x5f8b8:$j: #=q • 0x5f8d4:$j: #=q
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
21.2.Payment confirmation .exe.6800000.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d3db:$x1: NanoCore.ClientPluginHost • 0x1d3f5:$x2: IClientNetworkHost
21.2.Payment confirmation .exe.6800000.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1d3db:$x2: NanoCore.ClientPluginHost • 0x20718:$s4: PipeCreated • 0x1d3c8:$s5: IClientLoggingHost
21.2.Payment confirmation .exe.6804c9f.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a53c:$x1: NanoCore.ClientPluginHost • 0x1a556:$x2: IClientNetworkHost
21.2.Payment confirmation .exe.6804c9f.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1a53c:$x2: NanoCore.ClientPluginHost • 0x1d879:$s4: PipeCreated • 0x1a529:$s5: IClientLoggingHost
21.0.Payment confirmation .exe.400000.10.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 69 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

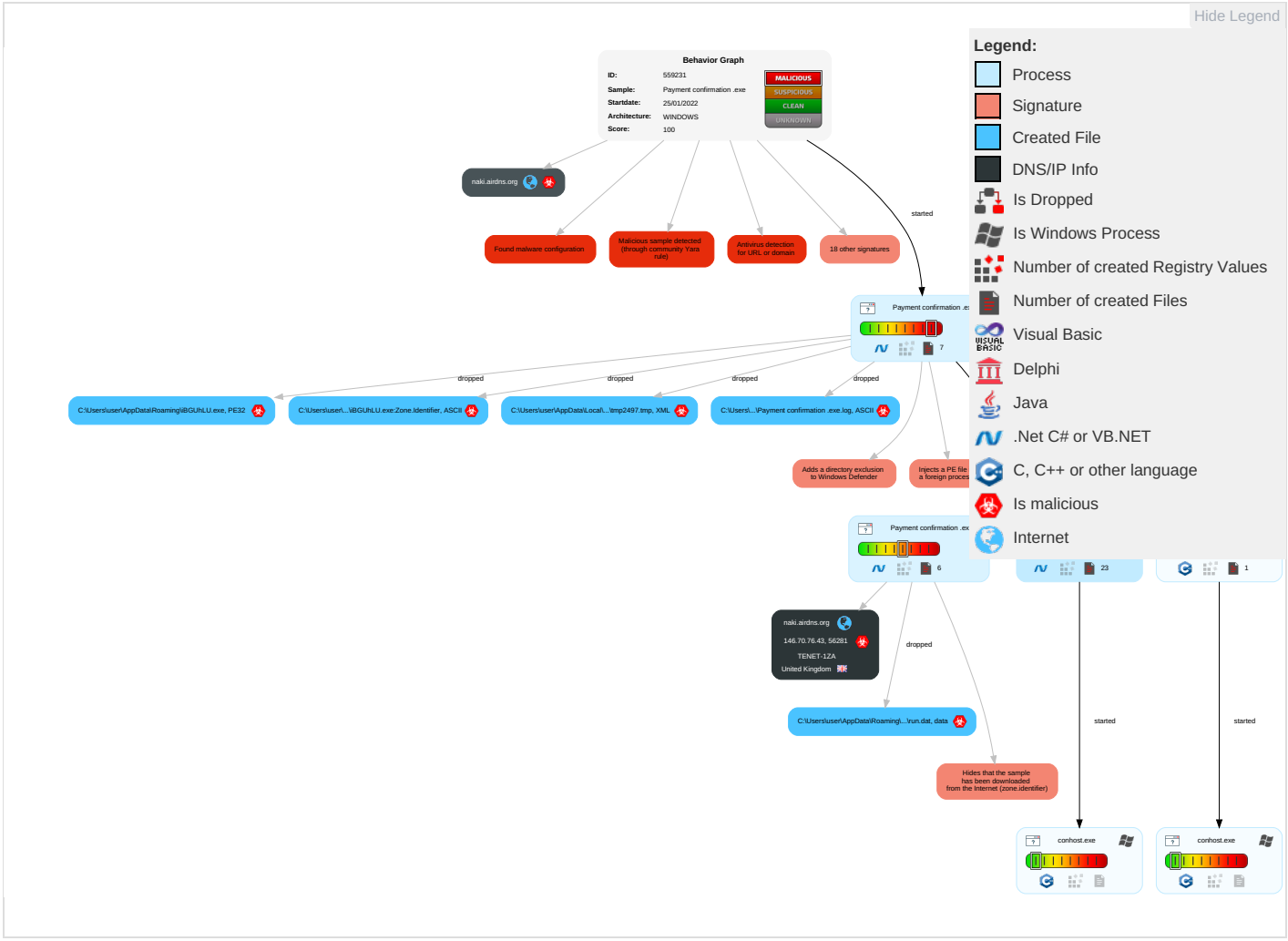
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	1 Masquerading	1 1 Input Capture	1 Query Registry	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

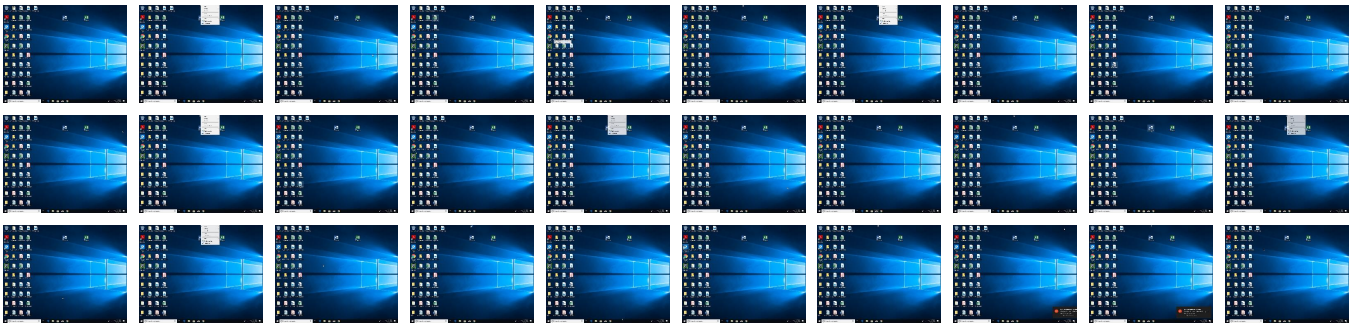
Behavior Graph



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
Payment confirmation .exe	32%	Virustotal		Browse
Payment confirmation .exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
Payment confirmation .exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\iBGUhLU.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\iBGUhLU.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.0.Payment confirmation .exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.Payment confirmation .exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
21.0.Payment confirmation .exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.Payment confirmation .exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.0.Payment confirmation .exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.Payment confirmation .exe.6070000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
21.0.Payment confirmation .exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
naki.airdns.org	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comces	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cnK	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.goodfont.co.kr-c	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnrm	0%	Avira URL Cloud	safe	
37.120.210.211	4%	Virustotal		Browse
37.120.210.211	100%	Avira URL Cloud	malware	
naki.airdns.org	0%	Avira URL Cloud	safe	
http://www.carterandcone.com3	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.urwpp.de~	0%	Avira URL Cloud	safe	
http://www.carterandcone.comt0	0%	Avira URL Cloud	safe	
http://www.carterandcone.comypo	0%	URL Reputation	safe	
http://www.founder.com.cn/cnno	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comdia	0%	URL Reputation	safe	
http://www.sandoll.co.krs-c	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.sandoll.co.krTF	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comncyl	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnls(	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnsof0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.carterandcone.com9	0%	URL Reputation	safe	
http://fontfabrik.comug	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html%	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comac	0%	Avira URL Cloud	safe	
http://www.sakkal.comd	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://fontfabrik.como	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.krmn-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.comth	0%	Avira URL Cloud	safe	
http://www.carterandcone.comcyK	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comno.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.coms	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.V	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnmpa	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmo	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comlg	0%	Avira URL Cloud	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.sandoll.co.kr_	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comhly	0%	URL Reputation	safe	
http://www.founder.com.cn/cnls(	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.urwpp.deg	0%	Avira URL Cloud	safe	
http://www.carterandcone.comesH	0%	Avira URL Cloud	safe	
http://www.carterandcone.comr-t	0%	Avira URL Cloud	safe	
http://www.carterandcone.comso	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva&	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
naki.airdns.org	146.70.76.43	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
37.120.210.211	true	• 4%, Virustotal, Browse • Avira URL Cloud: malware	unknown
naki.airdns.org	true	• Avira URL Cloud: safe	unknown
0,0,343003226,0000000000A68000,00000002,00000001,01000000,00000003,3,D7A61577F9C39F0C	true		low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comces	Payment confirmation .exe, 00000000.0000 0003.365623717.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365155998.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 546838.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365769728.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365290423.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comn-u	Payment confirmation .exe, 00000000.0000 0003.365155998.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365290423.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365423276.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnK	Payment confirmation .exe, 00000000.0000 0003.362608382.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362684991.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.362259718.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 098396.0000000005CD0000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362442942.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr-c	Payment confirmation .exe, 00000000.0000 0003.360704375.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersB	Payment confirmation .exe, 00000000.0000 0003.383170261.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Payment confirmation .exe, 00000000.0000 0003.365546838.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362814594.0 0000000012CC000.00000004.00000020.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365769728.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnrm	Payment confirmation .exe, 00000000.0000 0003.362098396.0000000005CD0000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	Payment confirmation .exe, 00000000.0000 0003.393018990.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.373895893.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.380893532.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.374 935499.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.382778780.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.376425938.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.381168425.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://www.carterandcone.com3	Payment confirmation .exe, 00000000.0000 0003.364863222.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365010134.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.360704375.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Payment confirmation .exe, 00000000.0000 0003.365423276.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de~	Payment confirmation .exe, 00000000.0000 0003.372633234.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.372433937.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.372152219.0000000005CD3000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comt0	Payment confirmation .exe, 00000000.0000 0003.366147501.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365623717.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365906076.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366 744577.0000000005CCC000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366465674.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366265697.0000000005CD4000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366935086.0000000005CCC000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 546838.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.367218271.000000000 5CD3000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.367116516.0000000005CCC000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366030122.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 769728.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366668074.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365290423.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366592843.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comypo	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364016052.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnno	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362608382.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364507204.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 684991.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363185032.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.363495280.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362259718.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364863222.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 016052.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363634963.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.363056742.0000000005CD4000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362098396.0 000000005CD0000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.363356203.0000000005CCD000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 442942.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.364641374.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.361861660.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365546838.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 900001.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364361805.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365010134.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Payment confirmation .exe, 00000000.0000 0003.353514887.0000000005CB2000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000002.567198922.0 000000006EC2000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdia	Payment confirmation .exe, 00000000.0000 0002.559399340.00000000012C7000.00000004 .00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krs-c	Payment confirmation .exe, 00000000.0000 0003.360528445.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.360704375.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersh	Payment confirmation .exe, 00000000.0000 0003.376137586.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.376425938.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krTF	Payment confirmation .exe, 00000000.0000 0003.360704375.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Payment confirmation .exe, 00000000.00000002.567198922.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Payment confirmation .exe, 00000000.00000002.567198922.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.356117157.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.356378144.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.356305451.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comncyl	Payment confirmation .exe, 00000000.00000003.363863872.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364016052.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363634963.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnls(	Payment confirmation .exe, 00000000.00000003.363863872.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363495280.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364016052.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363634963.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363356203.0000000005CCD000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364641374.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364361805.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365010134.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364219785.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnsof0	Payment confirmation .exe, 00000000.00000003.362608382.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362684991.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362259718.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362098396.0000000005CD0000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362442942.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl	Payment confirmation .exe, 00000000.00000003.362608382.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362684991.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362259718.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362098396.0000000005CD0000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362442942.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com9	Payment confirmation .exe, 00000000.0000 0003.364507204.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364016052.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 155998.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364641374.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.364361805.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365010134.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364219785.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 290423.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comug	Payment confirmation .exe, 00000000.0000 0003.356378144.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersc	Payment confirmation .exe, 00000000.0000 0003.376830096.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.376667085.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.376425938.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersb	Payment confirmation .exe, 00000000.0000 0003.383170261.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html%	Payment confirmation .exe, 00000000.0000 0003.367709317.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.com	Payment confirmation .exe, 00000000.0000 0002.559797997.0000000002D01000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	Payment confirmation .exe, 00000000.0000 0003.367855914.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Payment confirmation .exe, 00000000.0000 0003.360911622.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000002.567198922.0 000000006EC2000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.361056673.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.360 528445.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.360704375.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comac	Payment confirmation .exe, 00000000.0000 0003.364361805.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.comd	Payment confirmation .exe, 00000000.0000 0003.368239598.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.368365048.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.368048501.0000000005CD3000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.367 781250.0000000005CD3000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.367855914.000000000 5CD3000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Payment confirmation .exe, 00000000.0000 0003.372633234.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.383309388.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.383712360.0000000005CD8000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.383 422790.0000000005CD7000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.372433937.000000000 5CD3000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.383830654.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.372152219.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.383630749.0000000005CD8000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.383 516270.0000000005CD8000.00000004.0000080 0.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Payment confirmation .exe, 00000000.0000 0003.363356203.0000000005CCD000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Payment confirmation .exe, 00000000.0000 0002.559797997.0000000002D01000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.367781250.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.como	Payment confirmation .exe, 00000000.0000 0003.357825255.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.357302229.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.357469019.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.357 024345.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.357977143.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.356575956.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.356445695.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.356700406.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.356 887648.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.357619118.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.357149641.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	Payment confirmation .exe, 00000000.00000002.567198922.0000000006EC2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.krmn-u	Payment confirmation .exe, 00000000.00000003.360704375.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comth	Payment confirmation .exe, 00000000.00000003.363863872.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366147501.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365623717.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364016052.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363634963.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366265697.0000000005CD4000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364641374.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365546838.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364361805.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366030122.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365769728.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365010134.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364219785.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365290423.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comcyK	Payment confirmation .exe, 00000000.00000003.364507204.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comno.	Payment confirmation .exe, 00000000.00000003.353514887.0000000005CB2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comc	Payment confirmation .exe, 00000000.00000003.365155998.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365290423.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comslnt	Payment confirmation .exe, 00000000.00000003.365623717.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365546838.0000000005CCB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.coms	Payment confirmation .exe, 00000000.00000003.362814594.00000000012CC000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cno.V	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.363495280.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 863222.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364016052.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.363634963.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363356203.0 000000005CCD000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364641374.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 361805.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365010134.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.364219785.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers~	Payment confirmation .exe, 00000000.0000 0003.376667085.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.376137586.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.374935499.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.376 425938.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnmpa	Payment confirmation .exe, 00000000.0000 0003.362608382.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362684991.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.362259718.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 098396.0000000005CD0000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362442942.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmo	Payment confirmation .exe, 00000000.0000 0003.386807451.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.386605316.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.387075190.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.387 222007.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.386931372.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmle	Payment confirmation .exe, 00000000.0000 0003.382357060.0000000005CEE000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.382554954.0 000000005CEE000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.382497875.0000000005CEE000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://en.w	Payment confirmation .exe, 00000000.0000 0003.357486991.0000000005CD8000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.357630236.0 000000005CD8000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.357683121.0000000005CDA000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comlg	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366147501.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 623717.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.363495280.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364016052.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363 634963.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366265697.000000000 5CD4000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365155998.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364641374.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365546838.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 361805.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366030122.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365769728.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365010134.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 219785.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365290423.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365423276.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comm	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366147501.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 623717.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366744577.0000000005CCC000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364016052.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366 465674.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366265697.000000000 5CD4000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365155998.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364641374.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365546838.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 361805.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366030122.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365769728.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366668074.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 010134.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364219785.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365290423.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr_	Payment confirmation .exe, 00000000.0000 0003.360704375.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

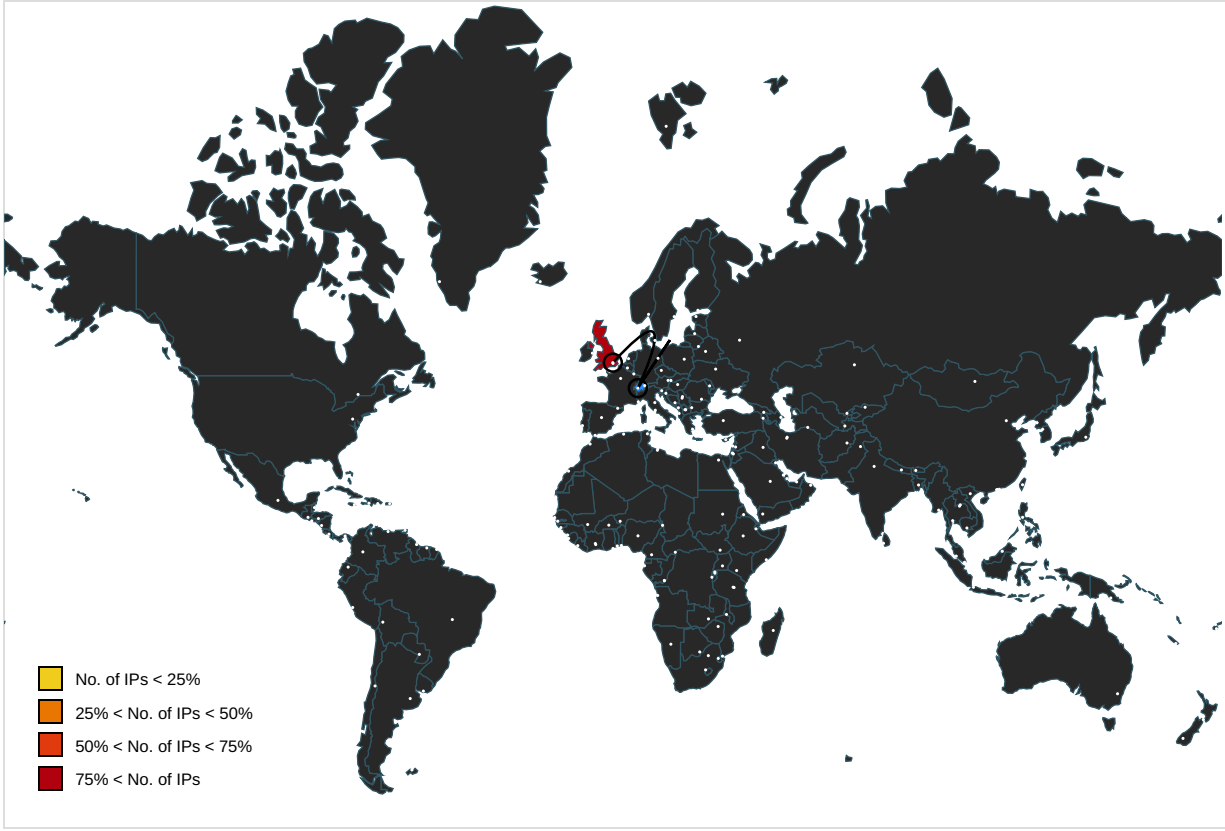
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnk	Payment confirmation .exe, 00000000.0000 0003.363863872.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364507204.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366147501.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 623717.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.363495280.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364016052.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363 634963.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363356203.000000000 5CCD000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366265697.0000000005CD4000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364641374.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 546838.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364361805.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366326585.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366030122.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365769728.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 010134.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364219785.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365290423.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Payment confirmation .exe, 00000000.0000 0003.362259718.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362098396.0 000000005CD0000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.362442942.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	Payment confirmation .exe, 00000000.0000 0003.361861660.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362900001.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364219785.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	Payment confirmation .exe, 00000000.0000 0003.380972243.0000000005CEE000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.381322016.0 000000005CEE000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.381187839.0000000005CEE000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.381 501028.0000000005CEE000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000002.567198922.000000000 6EC2000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.381061897.0000000005CEE000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.380504872.0 000000005CEE000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.380770592.0000000005CEE000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.380 416970.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp	false		high
http://www.carterandcone.comhly	Payment confirmation .exe, 00000000.0000 0003.365623717.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365906076.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365546838.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 769728.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnls(	Payment confirmation .exe, 00000000.0000 0003.362608382.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362684991.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.363185032.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362 259718.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.363056742.000000000 5CD4000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.362098396.0000000005CD0000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.362442942.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.362900001.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	Payment confirmation .exe, 00000000.0000 0003.386028171.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers%	Payment confirmation .exe, 00000000.0000 0003.380694836.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.393018990.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.393142180.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Payment confirmation .exe, 00000000.0000 0002.567198922.0000000006EC2000.00000004 .00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deg	Payment confirmation .exe, 00000000.0000 0003.372633234.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.372433937.0 000000005CD3000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.372152219.0000000005CD3000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comesH	Payment confirmation .exe, 00000000.0000 0003.365155998.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365290423.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365423276.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comr-t	Payment confirmation .exe, 00000000.0000 0003.364507204.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366147501.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365623717.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 906076.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366265697.0000000005CD4000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.364641374.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 546838.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366030122.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365769728.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365010134.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 290423.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Payment confirmation .exe, 00000000.0000 0003.373895893.0000000005CD3000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.374545461.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.374384052.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comso	Payment confirmation .exe, 00000000.0000 0003.364863222.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365155998.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365010134.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 290423.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365423276.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comva&	Payment confirmation .exe, 00000000.0000 0003.364507204.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366147501.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365623717.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 906076.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364863222.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.366465674.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366265697.0 000000005CD4000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365155998.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364 641374.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365546838.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.364361805.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366326585.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.366030122.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 769728.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366668074.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp, Payment confirmation .exe, 00000000.0000 0003.365010134.0000000005CCB000.00000004 .00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.364219785.0 000000005CCB000.00000004.00000800.000200 00.00000000.sdmp, Payment confirmation .exe, 00000 000.00000003.365290423.0000000005CCB000. 00000004.00000800.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.365 423276.0000000005CCB000.00000004.0000080 0.00020000.00000000.sdmp, Payment confirmation .exe, 00000000.00000003.366592843.000000000 5CCB000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/cabarga.htmlH	Payment confirmation .exe, 00000000.0000 0003.382357060.0000000005CEE000.00000004 .00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.70.76.43	naki.airdns.org	United Kingdom		2018	TENET-1ZA	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	559231
Start date:	25.01.2022
Start time:	05:29:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment confirmation .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:	24
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@9/9@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 2.1%) • Quality average: 78.9% • Quality standard deviation: 25.7%

HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:30:52	API Interceptor	157x Sleep call for process: Payment confirmation .exe modified
05:31:58	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859

Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
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\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22308
Entropy (8bit):	5.601222598067954
Encrypted:	false
SSDEEP:	384:ptCDFC0Nr/0968S0nAjultISD7Y9glSJ3xKT1MaXZlbAV7evWLSZBDI+9g:I/YfTACltt3lclCefwy5Vs
MD5:	D08243BF44C39C230E13DE5552CFC229
SHA1:	C05BE7254C2075C784DD4B232BFF0B6EA7B48BBD
SHA-256:	3851DD96A08B0E86AC34F1FCB2D5A24F0A9AC75B9F1462C1072CBB5B8A38A13A
SHA-512:	3801C6FCB595213D3C85E5DE6E0B0B7F6A8E536B02559440FF93986A7B77DA530B583898A5729FEB916BE73C68826C9D79DC92E3FDB744C4F2A2B77D4A2D938
Malicious:	false
Reputation:	low
Preview:	@...e.....h...a.Y.V.....I.....@.....H.....<@.^.L."My...:X..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bf0tqcoi.ti0.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fw12uc5a.y50.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U

MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2497.tmp

Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1606
Entropy (8bit):	5.116364367259849
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLi7xvn:cgea6YrFdOFzOzN33ODOiDdKrsuT0v
MD5:	9A2AE254726CA1E04F7FD2936BC67727
SHA1:	AC650650400D0E16BB0096603F4FDB882EA30A5C
SHA-256:	8B745FC3F6B96C0FFF0D79A1F2E19CED30436F4D52C5E6948D35D9A6B9CC0A6B
SHA-512:	54C37099355A397324B26FD6C5361DC365F5890267240F5E4D74F8FCA4572A4FBE7980DA3CCC15A86D1AAC0F35DEE515C5B59D72B1970185843ABC523796C5D
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:D+8tn:a8tn
MD5:	94BD220310AF83D117DA8CA8A3BBCA0B
SHA1:	DCFE8F5B801F13E2D95BC41546A55A75A3EAEB10
SHA-256:	4D8124FCE210AED26231BA07B7540B0AD6ED3F43A27B3A2C92DF26C7FBE0AF74
SHA-512:	F2BCDFC397913F3C1A3CC16419AC2F8B57660B2FC28225600B2C4CEB961F6C2C23AACBBC56248EE65CA436D1891233BA453A59183FB82F76C71BCA48AFEF75 3C
Malicious:	**true**
Preview:	.kK....H

C:\Users\user\AppData\Roaming\iBGUhLU.exe

Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	993280
Entropy (8bit):	7.851238509161969
Encrypted:	false
SSDEEP:	24576:1MJS/fy8oTImIQoM46ayaad63/85GFnhZ5AVU7wsh6I:1MQ/fYJIvmFEZCUxh6I
MD5:	0D98108AA5A3383C2C3152CF2CD5AE9A
SHA1:	E08D7BA0BF0AC4F93D17E71D27A82DFB22058626
SHA-256:	796F57DA16FA76BD10AFB6A16F9F75B78673F47556CE4D93D93EC34B5D898F61
SHA-512:	8018995A3768CA9C91C4837E82167BB386ADBBE7A06054034A10A21AA07C1D2BFD4D62A58CED067AFC232B4A91CCB8E9988FF70F9A4B2A44553030D7D88966A 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I?.a.....>(... ...@....@.. ....@..... '..K...`. ..... ..... ..H.....text...D.... ..... ..`.sdata.....@.....@....rsrc... ....` .....@..@.reloc.....&.....@..B..... ....

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

Process:	C:\Users\user\Desktop\Payment confirmation .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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220125\PowerShell_transcript.928100.EGNDur5V.20220125053156.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5807
Entropy (8bit):	5.378693775721289
Encrypted:	false
SSDEEP:	96:BZkTLGN7qDo1ZOZFTLGN7qDo1ZPrpDjZsTLGN7qDo1ZOWTTQZ3:m
MD5:	EED916291A2BFA3A57D4F776CD15D542
SHA1:	290FE8AB5F6D45987BBC4F488990B236CE80ECEA
SHA-256:	9D914FC076BB34E47CA55D9920B38C72BD785D25971B2CD430E5F276C450BB08
SHA-512:	B0102F73A0C9E73B58F65360450C0ED327432E54B1FCB7E341F7C36DB8E9F219EE6A8759E3CBFA8D156634EB9F9A0F583282DBB0885E0D9AA14DD37702D517F1
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220125053158..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\iBGUhLU.exe..Process ID: 5776..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220125053158..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\iBGUhLU.exe..**********..Windows PowerShell transcript start..Start time: 20220125053539..Username: computer\user..RunAs User: DESKTOP-716

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.851238509161969
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	Payment confirmation .exe
File size:	993280
MD5:	0d98108aa5a3383c2c3152cf2cd5ae9a
SHA1:	e08d7ba0bf0ac4f93d17e71d27a82dfb22058626
SHA256:	796f57da16fa76bd10afb6a16f9f75b78673f47556ce4d93d93ec34b5d898f61
SHA512:	8018995a3768ca9c91c4837e82167bb386adbbe7a06054034a10a21aa07c1d2bfd4d62a58ced067afc232b4a91ccb8e9988ff70f9a4b2a44553030d7d88966a0
SSDEEP:	24576:1MJS/fy8oTImIQoM46ayaad63/85GFnhZ5AVU7wsh6l:1MQ/fYJlvmFEZCUxh6l
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I?.a.....>(... ...@....@.. ..... @.....

File Icon

Icon Hash:	192d555d6d45650b

Static PE Info

General

Entrypoint:	0x4f283e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61EF3F6C [Tue Jan 25 00:08:12 2022 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf27f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf6000	0x1520	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xf0844	0xf0a00	False	0.917583198052	data	7.86642009336	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xf4000	0x1e8	0x200	False	0.861328125	data	6.61807085145	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf6000	0x1520	0x1600	False	0.273970170455	data	3.59842284173	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf6130	0xea8	data		
RT_GROUP_ICON	0xf6fd8	0x14	data		
RT_VERSION	0xf6fec	0x348	data		
RT_MANIFEST	0xf7334	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

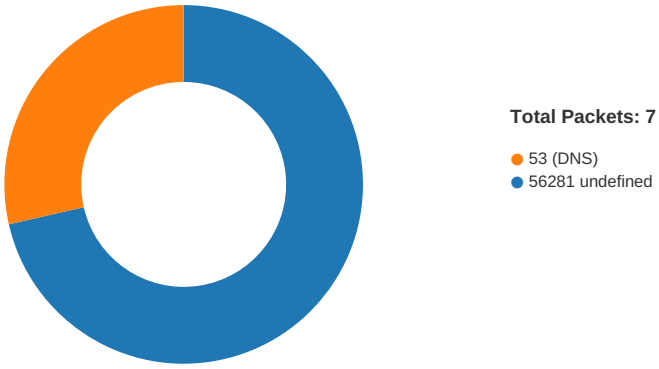
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2010

Description	Data
Assembly Version	1.0.0.0
InternalName	ObjRefSurroga.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	CSMDown
ProductVersion	1.0.0.0
FileDescription	CSMDown
OriginalFilename	ObjRefSurroga.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2022 05:32:17.356909037 CET	49811	56281	192.168.2.6	146.70.76.43
Jan 25, 2022 05:32:20.364269972 CET	49811	56281	192.168.2.6	146.70.76.43
Jan 25, 2022 05:32:26.380498886 CET	49811	56281	192.168.2.6	146.70.76.43
Jan 25, 2022 05:32:34.445142031 CET	49838	56281	192.168.2.6	146.70.76.43
Jan 25, 2022 05:32:37.443854094 CET	49838	56281	192.168.2.6	146.70.76.43

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2022 05:32:17.074172974 CET	50010	53	192.168.2.6	8.8.8.8
Jan 25, 2022 05:32:17.347052097 CET	53	50010	8.8.8.8	192.168.2.6
Jan 25, 2022 05:32:34.326653957 CET	62116	53	192.168.2.6	8.8.8.8
Jan 25, 2022 05:32:34.432260036 CET	53	62116	8.8.8.8	192.168.2.6

DNS Queries

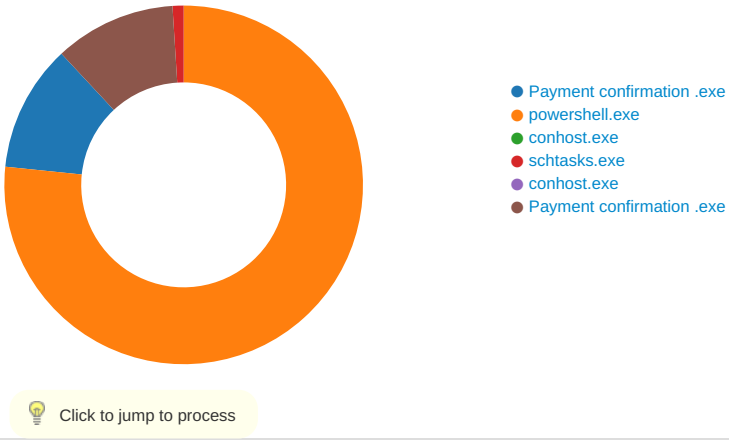
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 25, 2022 05:32:17.074172974 CET	192.168.2.6	8.8.8.8	0x6641	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 25, 2022 05:32:34.326653957 CET	192.168.2.6	8.8.8.8	0x5d8	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 25, 2022 05:32:17.347052097 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 25, 2022 05:32:34.432260036 CET	8.8.8.8	192.168.2.6	0x5d8	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Payment confirmation .exe PID: **4540**, Parent PID: **4280**

General

Start time:	05:30:23
Start date:	25/01/2022
Path:	C:\Users\user\Desktop\Payment confirmation .exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Payment confirmation .exe"
Imagebase:	0x970000
File size:	993280 bytes
MD5 hash:	0D98108AA5A3383C2C3152CF2CD5AE9A
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: 00000000.00000002.562434427.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.562434427.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.562434427.0000000003D0C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.559797997.0000000002D01000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.563113379.0000000003EF5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.563113379.0000000003EF5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.563113379.0000000003EF5000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Roaming\iBGUhLU.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6DE3DD66	CopyFileW
C:\Users\user\AppData\Roaming\ iBGUhLU.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6DE3DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2497.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment confirmation .exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F2FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2497.tmp	success or wait	1	6DE36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ iBGUhLU.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 6c 3f fd 61 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 0a 0f 00 00 1a 00 00 00 00 00 00 3e 28 0f 00 00 20 00 00 00 40 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0f 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELI?a>(@@ @	success or wait	4	6DE3DD66	CopyFileW
C:\Users\user\AppData\Roaming\ iBGUhLU.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6DE3DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2497.tmp	0	1606	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment confirmation .exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6F2FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EFC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EF203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DE31B4F	ReadFile

Analysis Process: powershell.exe PID: **5776**, Parent PID: **4540**

General

Start time:	05:31:53
Start date:	25/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\iBGUhLU.exe
Imagebase:	0xd30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bf0tqcoi.ti0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fw12uc5a.y50.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW
C:\Users\user\Documents\20220125	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3BEFF	CreateDirectoryW
C:\Users\user\Documents\20220125\PowerShell_transcript.928100.EGNDur5V.20220125053156.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bf0tqcoi.ti0.ps1	success or wait	1	6DE36A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fw12uc5a.y50.psm1	success or wait	1	6DE36A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bf0tqcoi.ti0.ps1	0	1	31	1	success or wait	1	6DE31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fw12uc5a.y50.psm1	0	1	31	1	success or wait	1	6DE31B4F	WriteFile
C:\Users\user\Documents\20220125\PowerShell_transcript.928100.EGNDur5V.20220125053156.txt	0	3	ff		success or wait	1	6DE31B4F	WriteFile
C:\Users\user\Documents\20220125\PowerShell_transcript.928100.EGNDur5V.20220125053156.txt	3	683	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 35 30 35 33 31 35 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 32 38 31 30 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a	**********Windows PowerShell transcript startStart time: 20220125053158Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 928100 (Microsoft Windows NT 10.0.17134.0)Host Application:	success or wait	44	6DE31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 fd 14 00 00 18 00 00 00 68 0d 06 04 61 09 59 09 56 09 00 00 fd 00 fd 00 17 00 49 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehaYVI@	success or wait	1	6F2B76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 58 00 00 00 0e 00 20 00	H<@^L"My:X	success or wait	17	6F2B76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6F2B76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6F2B76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6F2B76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 fd 01 40 00 02 54 40 01 55 00 40 00 47 00 40 00 56 00 40 00 fd 01 40 00 fd 00 40 00 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@ S@\@T@@T@U@G@V@@@@X@? X@T@S@S@T @T@xT@zT@T@=M@ DM@:M@"M@ M@!M@g @@@;M@D@D@@M@ <M@$M@8M@? M@;@;@;@	success or wait	11	6F2B76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EFC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EF203DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFCCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFCCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EF203DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EFC5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6EFD1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6EFD203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EF203DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	6	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	141	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6DE31B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EF203DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6EFC5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6DE31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6DE31B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6DE31B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6DE31B4F	ReadFile

Analysis Process: conhost.exe PID: **5732**, Parent PID: **5776**

General

Start time:	05:31:54
Start date:	25/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **4688**, Parent PID: **4540**

General

Start time:	05:31:58
Start date:	25/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\iBGUhLU" /XML "C:\Users\user\AppData\Local\Temp\tmp2497.tmp
Imagebase:	0x12c0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2497.tmp	unknown	2	success or wait	1	12CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2497.tmp	unknown	1607	success or wait	1	12CABD9	ReadFile

Analysis Process: conhost.exe PID: **5004**, Parent PID: **4688**

General

Start time:	05:31:59
Start date:	25/01/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Payment confirmation .exe PID: **5116**, Parent PID: **4540**

General

Start time:	05:31:59
Start date:	25/01/2022
Path:	C:\Users\user\Desktop\Payment confirmation .exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment confirmation .exe
Imagebase:	0x8f0000
File size:	993280 bytes
MD5 hash:	0D98108AA5A3383C2C3152CF2CD5AE9A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.553341686.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.615775430.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.615775430.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.552240141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.552240141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.552240141.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.621380442.0000000006070000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.621380442.0000000006070000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.621380442.0000000006070000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.617626488.0000000003DF9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.617626488.0000000003DF9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.554000137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.554000137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.554000137.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.612866743.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.612866743.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.612866743.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.621567698.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.621567698.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.620905175.0000000005390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000015.00000002.620905175.0000000005390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000000.554553035.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000000.554553035.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000000.554553035.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EFECF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6DE31E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DE3BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Payment confirmation .exe:Zone.Identifier	success or wait	1	5377C7E	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 6b 4b 15 07 fd fd 48	kKH	success or wait	1	6DE31B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EFC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EF203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EF203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EF203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EFC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6DE31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6DE31B4F	ReadFile
C:\Users\user\Desktop\Payment confirmation .exe	unknown	4096	success or wait	1	6EFAD72F	unknown
C:\Users\user\Desktop\Payment confirmation .exe	unknown	512	success or wait	1	6EFAD72F	unknown

Disassembly

No disassembly