ID: 623786
Sample Name: Ki8WlC0ddA.exe
Cookbook: default.jbs
Time: 20:20:48
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

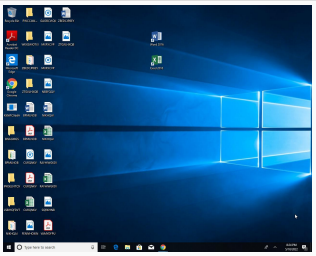
Windows Analysis Report

Ki8WlC0ddA.exe

Overview

General Information

Sample Name:	Ki8WlC0ddA.exe
Analysis ID:	623786
MD5:	0f8819270f26188.
SHA1:	7473c2e2683725..
SHA256:	42bc81c2809d6a..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

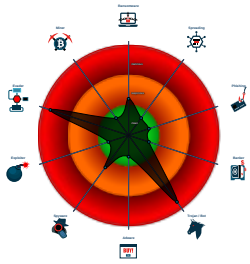
Nanocore

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 dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Ki8WlC0ddA.exe (PID: 4340 cmdline: "C:\Users\user\Desktop\Ki8WlC0ddA.exe" MD5: 0F8819270F261881BDFDBB15FE4F4D7C)
  - powershell.exe (PID: 6620 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nbbxvA.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2892 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2896 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nbbxvA" /XML "C:\Users\user\AppData\Local\Temp\tmp39F4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Ki8WlC0ddA.exe (PID: 5072 cmdline: C:\Users\user\Desktop\Ki8WlC0ddA.exe MD5: 0F8819270F261881BDFDBB15FE4F4D7C)
  - Ki8WlC0ddA.exe (PID: 6192 cmdline: C:\Users\user\Desktop\Ki8WlC0ddA.exe MD5: 0F8819270F261881BDFDBB15FE4F4D7C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6d38b3f5-33a1-41b7-a7f2-d8fe2b39",
  "Group": "happy man",
  "Domain1": "91.193.75.221",
  "Domain2": "",
  "Port": 4040,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000C.00000002.624692987.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000002.624692987.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 30 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.Ki8WlC0ddA.exe.53b4629.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
12.2.Ki8WlC0ddA.exe.53b4629.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
12.2.Ki8WlC0ddA.exe.53b4629.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.Ki8WlC0ddA.exe.53b4629.7.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xb14f:$x2: NanoCore.ClientPlugin • 0xb184:$x3: NanoCore.ClientPluginHost • 0xb143:$i2: IClientData • 0xb165:$i3: IClientNetwork • 0xb174:$i5: IClientDataHost • 0xb19e:$i6: IClientLoggingHost • 0xb1b1:$i7: IClientNetworkHost • 0xb1c4:$i8: IClientUIHost • 0xb1d2:$i9: IClientNameObjectCollection • 0xb1ee:$i10: IClientReadOnlyNameObjectCollection • 0xaf41:$s1: ClientPlugin • 0xb158:$s1: ClientPlugin • 0x10179:$s6: get_ClientSettings
12.2.Ki8WlC0ddA.exe.53b0000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 91 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

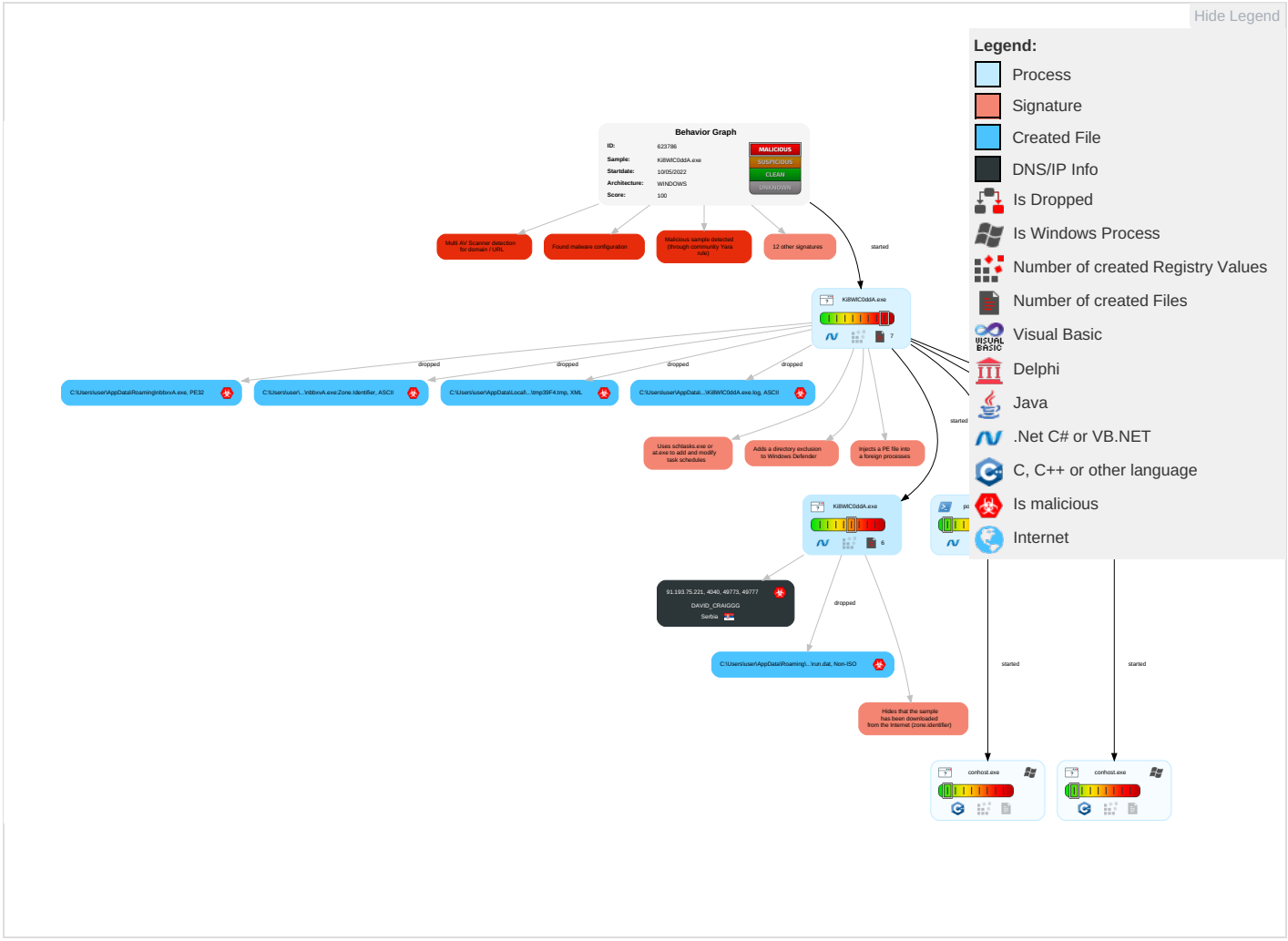
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 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	Fallback Channels	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	1 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

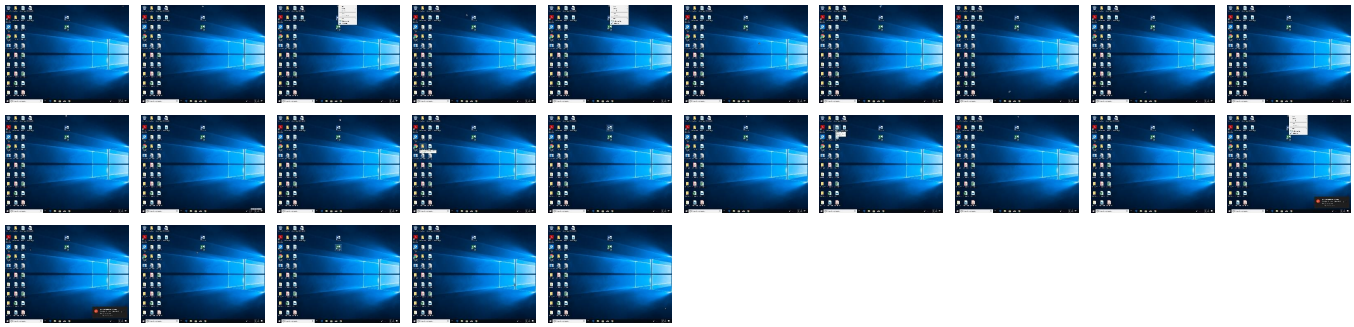
Behavior Graph



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
Ki8WIC0ddA.exe	63%	Virustotal		Browse
Ki8WIC0ddA.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Ki8WIC0ddA.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\nbbxvA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nbbxvA.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.Ki8WIC0ddA.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.Ki8WIC0ddA.exe.53b0000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
12.0.Ki8WlC0ddA.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.Ki8WlC0ddA.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.Ki8WlC0ddA.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.Ki8WlC0ddA.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.Ki8WlC0ddA.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.carterandcone.compor	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krttp://w	0%	Avira URL Cloud	safe	
91.193.75.221	8%	Virustotal		Browse
91.193.75.221	100%	Avira URL Cloud	malware	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.carterandcone.comUI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/a	0%	URL Reputation	safe	
http://www.fontbureau.comalsv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comaK	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.goodfont.co.krm	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comC	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn-s	0%	Avira URL Cloud	safe	
http://www.fontbureau.comicv	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Lodi	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comonyF(	0%	Avira URL Cloud	safe	
http://www.agfamonotype.Y	0%	Avira URL Cloud	safe	
http://www.fontbureau.com.TTFY	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.sandoll.co.krc	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.goodfont.co.krF	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.carterandcone.como.2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/iv	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comt;	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnicr	0%	URL Reputation	safe	
http://www.carterandcone.com-s	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comok	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnG	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/C	0%	URL Reputation	safe	
http://www.fontbureau.comitudC	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnM	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnUI	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/3	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnF	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn%	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.v	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiono(	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cnn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.comu	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl	0%	URL Reputation	safe	
http://www.sandoll.co.krFo	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comce2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/k-s	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCy	0%	Avira URL Cloud	safe	
http://www.carterandcone.comorm	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.carterandcone.comue~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comdC	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krn-u	0%	URL Reputation	safe	
http://www.fontbureau.comlic3	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
91.193.75.221	true	• 8%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.compor	Ki8WIC0ddA.exe, 00000000.00000003.370994517.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krttp://w	Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Ki8WIC0ddA.exe, 00000000.00000003.379402399.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	Ki8WIC0ddA.exe, 00000000.00000003.361655494.00000000054B2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371707918.00000000054CC000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378195328.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comUI	Ki8WIC0ddA.exe, 00000000.00000003.370994517.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/3	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/a	Ki8WIC0ddA.exe, 00000000.00000003.366859147.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.366705899.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsv	Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381204043.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380842783.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380465527.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380552548.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380167449.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comaK	Ki8WIC0ddA.exe, 00000000.00000003.361655494.00000000054B2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krm	Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Ki8WIC0ddA.exe, 00000000.00000002.435002351.00000000024C1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comC	Ki8WIC0ddA.exe, 00000000.00000003.375925606.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn-s	Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comicv	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377187088.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378872487.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378684255.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377000583.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378195328.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376374552.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376318651.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376779662.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378287930.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378450907.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Lodi	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/	Ki8WIC0ddA.exe, 00000000.00000003.382572076.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comonyF(	Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379926306.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380465527.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379817883.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380552548.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380069589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380842783.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379542986.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380465527.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379402399.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380552548.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380167449.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.agfamonotype.Y	Ki8WIC0ddA.exe, 00000000.00000003.395751162.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.395884258.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.395670428.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com.TTFY	Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380465527.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380552548.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.t	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/C	Ki8WIC0ddA.exe, 00000000.00000003.371707918.00000000054CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krc	Ki8WIC0ddA.exe, 00000000.00000003.366501762.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://en.w	Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.krF	Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Ki8WIC0ddA.exe, 00000000.00000003.367879789.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367594620.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367775102.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368109204.00000000054D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378773035.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377613113.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377907580.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378618291.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378378752.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377755305.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377461785.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378216379.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377405776.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378116495.00000000054E3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377284810.00000000054E3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.2	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/t	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372776835.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372572237.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372663553.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372973754.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373048058.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/r	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/iv	Ki8WIC0ddA.exe, 00000000.00000003.371707918.00000000054CC000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comt;	Ki8WIC0ddA.exe, 00000000.00000003.361655494.00000000054B2000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnicr	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368531585.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367879789.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367594620.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367775102.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367376622.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368638844.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368109204.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368395220.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com-s	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comok	Ki8WIC0ddA.exe, 00000000.00000003.381734424.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.382272498.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.382092130.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381834849.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381349447.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.382462785.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.382572076.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381204043.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379926306.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379065859.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379817883.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378872487.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380069589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnG	Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/C	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comitudC	Ki8WIC0ddA.exe, 00000000.00000003.378872487.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnM	Ki8WIC0ddA.exe, 00000000.00000003.367326593.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367144392.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnUI	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368320050.00000000009DC000.00000004.00000020.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368109204.00000000054D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/3	Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnF	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368531585.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367879789.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367594620.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367775102.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367376622.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368638844.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368109204.00000000054D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn%	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.como.v	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiono(	Ki8WIC0ddA.exe, 00000000.00000003.396815587.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396519860.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396425870.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.397001492.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396295063.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396346589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438648214.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396600351.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.typography.netD	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnn	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370994517.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368531585.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367879789.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367594620.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367775102.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367376622.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368638844.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369008885.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Ki8WIC0ddA.exe, 00000000.00000003.382966537.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.393199530.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.393959605.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	Ki8WIC0ddA.exe, 00000000.00000003.364222229.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.364443941.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363651716.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.364147023.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.364089454.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363616640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363932125.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.364045961.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.364363138.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363844392.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comu	Ki8WIC0ddA.exe, 00000000.00000003.363490557.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363651716.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363616640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363685426.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.363844392.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnl	Ki8WIC0ddA.exe, 00000000.00000003.367376622.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krFo	Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersw	Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376374552.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376318651.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.366501762.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designerso	Ki8WIC0ddA.exe, 00000000.00000003.379926306.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379817883.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379542986.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersn	Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368638844.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Ki8WIC0ddA.exe, 00000000.00000003.380167449.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379926306.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377187088.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379065859.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379817883.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378872487.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380069589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380842783.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379542986.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376229750.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377000583.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comL.TTF	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378684255.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378195328.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378287930.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378450907.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Ki8WIC0ddA.exe, 00000000.00000003.373508650.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372776835.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373405020.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373230539.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373729462.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371707918.00000000054CC000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372572237.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372663553.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373563351.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373470016.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373668116.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373438207.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373111641.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372973754.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373048058.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

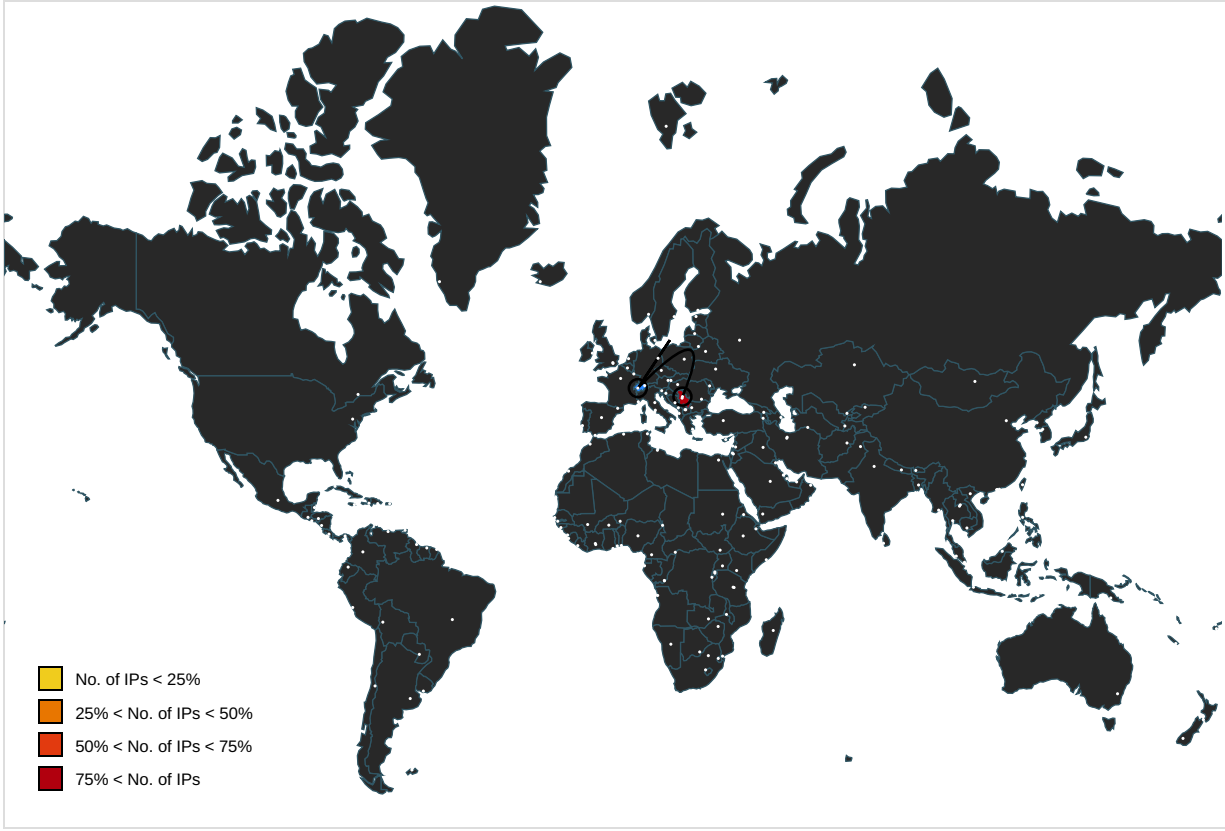
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377187088.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378872487.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378684255.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377000583.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378195328.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376374552.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376779662.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378287930.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378450907.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comce2	Ki8WIC0ddA.exe, 00000000.00000003.396815587.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396519860.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396425870.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.397001492.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396346589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438648214.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.396600351.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/k-s	Ki8WIC0ddA.exe, 00000000.00000003.372036060.00000000054CE000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372180731.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371707918.00000000054CC000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.371925042.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372327843.00000000054D2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369325878.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370994517.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368531585.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367879789.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367594620.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367775102.00000000054D1000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367326593.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368839959.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369524251.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.367144392.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369220038.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368638844.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.368138951.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/.	Ki8WIC0ddA.exe, 00000000.00000003.382572076.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTCy	Ki8WIC0ddA.exe, 00000000.00000003.370994517.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370802204.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370928366.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comorm	Ki8WIC0ddA.exe, 00000000.00000003.370294710.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369716108.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.369976743.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370152722.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.	Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377187088.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377000583.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376374552.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376318651.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376779662.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comue~	Ki8WIC0ddA.exe, 00000000.00000003.370548701.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.370421646.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comm	Ki8WIC0ddA.exe, 00000000.00000003.396600351.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Ki8WIC0ddA.exe, 00000000.00000003.372483656.00000000054D4000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373438207.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373111641.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.372973754.00000000054D3000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.373048058.00000000054D3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	Ki8WIC0ddA.exe, 00000000.00000003.375925606.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.375811643.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Ki8WIC0ddA.exe, 00000000.00000002.438805105.00000000066C2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdC	Ki8WIC0ddA.exe, 00000000.00000003.378051983.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377714029.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377528969.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377187088.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377828569.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376639491.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377265560.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377000583.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376434741.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.378195328.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376374552.00000000054D0000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377444886.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.377341586.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.376779662.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krn-u	Ki8WIC0ddA.exe, 00000000.00000003.366638740.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.366501762.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlic3	Ki8WIC0ddA.exe, 00000000.00000003.380737640.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379926306.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380650301.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.381062648.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380349987.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379817883.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380069589.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380842783.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.379542986.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380465527.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380552548.00000000054CB000.00000004.00000800.00020000.00000000.sdmp, Ki8WIC0ddA.exe, 00000000.00000003.380167449.00000000054CB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Ki8WIC0ddA.exe, 00000000.00000003.375811643.00000000054D0000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.221	unknown	Serbia		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623786
Start date and time: 10/05/202220:20:48	2022-05-10 20:20:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ki8WlC0ddA.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@11/9@0/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target Ki8WlC0ddA.exe, PID 5072 because there are no executed function
- 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
20:22:22	API Interceptor	713x Sleep call for process: Ki8WlC0ddA.exe modified
20:22:29	API Interceptor	41x 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\Ki8WlC0ddA.exe.log

Process:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false

SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
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):	22188
Entropy (8bit):	5.598160129279729
Encrypted:	false
SSDEEP:	384:9tCDe0wtHZHCIiYS0nIjultIA47nv3g3hInAML+6fmAV7ROidGZQvnI+++g:J5HCI7TIClt7c667KepNG+g
MD5:	E415DB43B45288B4347C4C3A5CFD1DA2
SHA1:	3C015F553C4D8A12D6AF92C59E1AD0780277CEAC
SHA-256:	62414F327822AF8C2CF75394C9E38227D812D42902619E22A93A02B917937A6B
SHA-512:	85DE19317306C8FA24153CAD13F9A1DD538A4D95C34EE4B1479B5AA2DB9539C2632FAA29F316CD3FEBBB2C9904AA908AD1F755433B27F595104C4045C1996AEC
Malicious:	false
Reputation:	low
Preview:	@...e.....d.....K...D.<.9.....X...-.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e5mvax22.jet.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r1la5k4g.tlc.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
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp39F4.tmp

Process:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1609
Entropy (8bit):	5.126414460395903
Encrypted:	false
SSDEEP:	24:2di4+S2qh/dp1Kd+y1modHUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtqxvn:cgeHMYrFdOFzOzN33ODOiDdKrsuT+v
MD5:	D817721B3222A81D668B278F4C7FB15E
SHA1:	D9E3B938D94E3C4168E5595893B86DF03D1D62BE
SHA-256:	0C94818867E19163C0A62116BB70A70D3265E0F43FD1FEEF41C98D38EF82AFB3
SHA-512:	36D16F4F18A2EFC43A0EA3C74D87AEDE9017F2977ADF223B417ABBF8695971396AC541933CB23252E714E90DF2727F2FA8A105FBF12406CA80D1247A71FD92CA
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</StartWhenAvai

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

Process:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:VUt:V0
MD5:	923A7A6E01C3242596B4D950D6B20EFA
SHA1:	330D952A60F1ECE84AE8A4881E3EA1BA35DBAE3D
SHA-256:	9BDC8A1B234E8533091289DB12DFFA06A876EE6B7252DDD52D0AE593029A258A
SHA-512:	C1BD44A61BFD0690C8BA754BD9BED08B276A56FF304A994C0B22901AA3F0F9DB00F14852142EC56895E7C0BA2B1E7AE3A0B6E8DA7CC90914FDC82D13D7952CB6
Malicious:	**true**
Preview:	h.*..2.H

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

Process:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	657920
Entropy (8bit):	7.935629638737511
Encrypted:	false
SSDEEP:	12288:tYV82L2IIafm7N8VVfcYKMrc/nQPnEuBTVFKNFgq/TDm7r3:mu2KafmIfcY3Y/qHBZ8zlmH
MD5:	0F8819270F261881BDFDBB15FE4F4D7C
SHA1:	7473C2E2683725955A0E9ACE00FA1DEA2A884A4C
SHA-256:	42BC81C2809D6AE05C7EAC0F21374E297F21ACB00D3BAEE3A2C6A14B963A058A
SHA-512:	473808E146741876941FD96557FB290E707D645636AB039FD873C21023EC97345474D4272D20CBA63AC2F22097B2734DB0EB8817C3430907861CF60040DFD984
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 57%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....xb.....0.....B.... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text...H.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....$.....H.....d...$O.....hF.....^..}.....(.....(.....*.0..+.....,..{.....+....,...{....o.....(.....*...s....}.....(.....r...po. ....*....0.....{.....+..*&...}....*..s....}.....(.....}.....(.....*..s....}.....(.....r...p}.....(.....*.0..`.....{....s.....+:....7...%..;.o.....{.....sw...o.....o ...%.....-..o!....*...{.....o"...(# ...($...(%.....{.....o.....*.0..?.....7...o.....7..

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

Process:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220510\PowerShell_transcript.849224.GF_mjD2U.20220510202227.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):	5813
Entropy (8bit):	5.3818582682762255
Encrypted:	false
SSDEEP:	96:BZA65NQqDo1Z9ZO65NQqDo1ZJEq8jZyx65NQqDo1ZkN5MMxZe:jT
MD5:	1DA29D1894E77B9BA3977D096D10811E
SHA1:	D0DD941D535DD09DF3E4278C416BFECA0B1A5AEA
SHA-256:	6E785EE9F4562FC8CF7C81AA9DEC1A10B2A45CE3F5F2B978792E185926E2C106
SHA-512:	06A35D253A194C207E4B2045EDB577E18040835EAEC5F7632896E011EEE2F374F85EC01A63FB00F8F05CB9E3E5E0DD89822CC982862646584D9D48036A1A7671
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220510202229..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 849224 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\AppData\Roaming\nbbxvA.exe..Process ID: 6620..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: 20220510202229..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\ AppData\Roaming\nbbxvA.exe..**********..Windows PowerShell transcript start..Start time: 20220510202546..Username: computer\user..RunAs User: DESKTO P-

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.935629638737511
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Ki8WlC0ddA.exe
File size:	657920
MD5:	0f8819270f261881bdfdbb15fe4f4d7c
SHA1:	7473c2e2683725955a0e9ace00fa1dea2a884a4c
SHA256:	42bc81c2809d6ae05c7eac0f21374e297f21acb00d3baee3a2c6a14b963a058a
SHA512:	473808e146741876941fd96557fb290e707d645636ab039fd873c21023ec97345474d4272d20cba63ac2f22097b2734db0eb8817c3430907861cf60040dfd984
SSDEEP:	12288:tYV82L2IIafm7N8VVfcYKMrc/nQPnEuBTVFKNFgq/TDm7r3:mu2KafmIfcY3Y/qHBZ8zlmH
TLSH:	74E42228AB784B63CB3953F2A251429403F73B6C7021FF595D9128EE29D3F421662F93

File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....xb..............0.............B.... ... .@.. ....`............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a1e42
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6278C699 [Mon May 9 07:45:29 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

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
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	0xa1df0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa4000	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	0x9fe48	0xa0000	False	0.938734436035	data	7.94239606201	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x5bc	0x600	False	0.425130208333	data	4.12036037241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	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_VERSION	0xa2090	0x32c	data		
RT_MANIFEST	0xa23cc	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 2017
Assembly Version	1.0.0.0
InternalName	TYPEFL.exe
FileVersion	1.0.0.0

Description	Data
CompanyName	
LegalTrademarks	
Comments	
ProductName	ProjektOkienka
ProductVersion	1.0.0.0
FileDescription	ProjektOkienka
OriginalFilename	TYPEFL.exe

Network Behavior

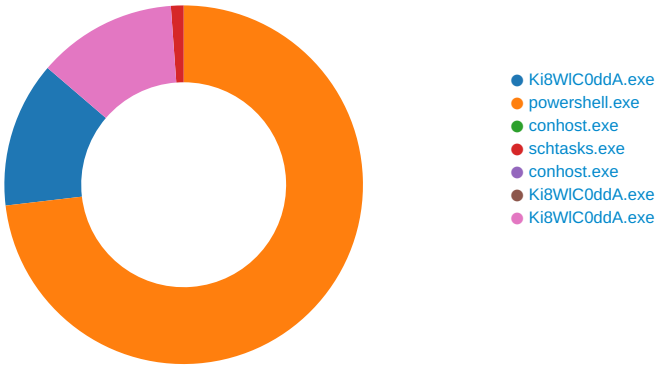
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:22:42.503998041 CEST	49773	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:42.545831919 CEST	4040	49773	91.193.75.221	192.168.2.7
May 10, 2022 20:22:43.080039978 CEST	49773	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:43.122967005 CEST	4040	49773	91.193.75.221	192.168.2.7
May 10, 2022 20:22:43.673918009 CEST	49773	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:43.715069056 CEST	4040	49773	91.193.75.221	192.168.2.7
May 10, 2022 20:22:47.804563999 CEST	49777	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:47.845561028 CEST	4040	49777	91.193.75.221	192.168.2.7
May 10, 2022 20:22:48.439953089 CEST	49777	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:48.480900049 CEST	4040	49777	91.193.75.221	192.168.2.7
May 10, 2022 20:22:49.130536079 CEST	49777	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:49.171638966 CEST	4040	49777	91.193.75.221	192.168.2.7
May 10, 2022 20:22:53.175615072 CEST	49782	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:53.216734886 CEST	4040	49782	91.193.75.221	192.168.2.7
May 10, 2022 20:22:53.737314939 CEST	49782	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:53.778502941 CEST	4040	49782	91.193.75.221	192.168.2.7
May 10, 2022 20:22:54.440404892 CEST	49782	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:54.481309891 CEST	4040	49782	91.193.75.221	192.168.2.7
May 10, 2022 20:22:58.527121067 CEST	49784	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:58.568022013 CEST	4040	49784	91.193.75.221	192.168.2.7
May 10, 2022 20:22:59.128285885 CEST	49784	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:59.169106960 CEST	4040	49784	91.193.75.221	192.168.2.7
May 10, 2022 20:22:59.737725019 CEST	49784	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:22:59.778687000 CEST	4040	49784	91.193.75.221	192.168.2.7
May 10, 2022 20:23:03.798732042 CEST	49791	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:03.840225935 CEST	4040	49791	91.193.75.221	192.168.2.7
May 10, 2022 20:23:04.441392899 CEST	49791	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:04.482343912 CEST	4040	49791	91.193.75.221	192.168.2.7
May 10, 2022 20:23:05.128849983 CEST	49791	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:05.169980049 CEST	4040	49791	91.193.75.221	192.168.2.7
May 10, 2022 20:23:09.196000099 CEST	49793	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:09.240170956 CEST	4040	49793	91.193.75.221	192.168.2.7
May 10, 2022 20:23:09.941673994 CEST	49793	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:09.985274076 CEST	4040	49793	91.193.75.221	192.168.2.7
May 10, 2022 20:23:10.629247904 CEST	49793	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:10.670150995 CEST	4040	49793	91.193.75.221	192.168.2.7
May 10, 2022 20:23:15.073534012 CEST	49796	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:15.115176916 CEST	4040	49796	91.193.75.221	192.168.2.7
May 10, 2022 20:23:15.645334959 CEST	49796	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:15.686187029 CEST	4040	49796	91.193.75.221	192.168.2.7
May 10, 2022 20:23:16.239181042 CEST	49796	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:16.280177116 CEST	4040	49796	91.193.75.221	192.168.2.7
May 10, 2022 20:23:20.570420027 CEST	49797	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:20.611356974 CEST	4040	49797	91.193.75.221	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 20:23:21.302205086 CEST	49797	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:21.343199968 CEST	4040	49797	91.193.75.221	192.168.2.7
May 10, 2022 20:23:21.895936966 CEST	49797	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:21.936805964 CEST	4040	49797	91.193.75.221	192.168.2.7
May 10, 2022 20:23:25.944119930 CEST	49801	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:25.985007048 CEST	4040	49801	91.193.75.221	192.168.2.7
May 10, 2022 20:23:26.505623102 CEST	49801	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:26.546449900 CEST	4040	49801	91.193.75.221	192.168.2.7
May 10, 2022 20:23:27.208856106 CEST	49801	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:27.249741077 CEST	4040	49801	91.193.75.221	192.168.2.7
May 10, 2022 20:23:31.266387939 CEST	49804	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:31.307337999 CEST	4040	49804	91.193.75.221	192.168.2.7
May 10, 2022 20:23:31.972084045 CEST	49804	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:32.012989998 CEST	4040	49804	91.193.75.221	192.168.2.7
May 10, 2022 20:23:32.709341049 CEST	49804	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:32.750113964 CEST	4040	49804	91.193.75.221	192.168.2.7
May 10, 2022 20:23:36.799782991 CEST	49810	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:36.840713978 CEST	4040	49810	91.193.75.221	192.168.2.7
May 10, 2022 20:23:37.346612930 CEST	49810	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:37.387509108 CEST	4040	49810	91.193.75.221	192.168.2.7
May 10, 2022 20:23:38.036809921 CEST	49810	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:38.077678919 CEST	4040	49810	91.193.75.221	192.168.2.7
May 10, 2022 20:23:42.136236906 CEST	49838	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:42.177123070 CEST	4040	49838	91.193.75.221	192.168.2.7
May 10, 2022 20:23:42.687381029 CEST	49838	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:42.728276968 CEST	4040	49838	91.193.75.221	192.168.2.7
May 10, 2022 20:23:43.235841990 CEST	49838	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:43.278156996 CEST	4040	49838	91.193.75.221	192.168.2.7
May 10, 2022 20:23:47.293898106 CEST	49858	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:47.334815025 CEST	4040	49858	91.193.75.221	192.168.2.7
May 10, 2022 20:23:47.852050066 CEST	49858	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:47.892920017 CEST	4040	49858	91.193.75.221	192.168.2.7
May 10, 2022 20:23:48.398979902 CEST	49858	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:48.439848900 CEST	4040	49858	91.193.75.221	192.168.2.7
May 10, 2022 20:23:52.450114012 CEST	49864	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:52.493285894 CEST	4040	49864	91.193.75.221	192.168.2.7
May 10, 2022 20:23:53.149414062 CEST	49864	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:53.190282106 CEST	4040	49864	91.193.75.221	192.168.2.7
May 10, 2022 20:23:53.836975098 CEST	49864	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:53.878005981 CEST	4040	49864	91.193.75.221	192.168.2.7
May 10, 2022 20:23:58.045922041 CEST	49865	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:58.086949110 CEST	4040	49865	91.193.75.221	192.168.2.7
May 10, 2022 20:23:58.587449074 CEST	49865	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:58.628504992 CEST	4040	49865	91.193.75.221	192.168.2.7
May 10, 2022 20:23:59.134346008 CEST	49865	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:23:59.175266027 CEST	4040	49865	91.193.75.221	192.168.2.7
May 10, 2022 20:24:03.182952881 CEST	49866	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:24:03.223838091 CEST	4040	49866	91.193.75.221	192.168.2.7
May 10, 2022 20:24:03.729336977 CEST	49866	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:24:03.770442009 CEST	4040	49866	91.193.75.221	192.168.2.7
May 10, 2022 20:24:04.275322914 CEST	49866	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:24:04.316310883 CEST	4040	49866	91.193.75.221	192.168.2.7
May 10, 2022 20:24:08.323231936 CEST	49867	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:24:08.364171982 CEST	4040	49867	91.193.75.221	192.168.2.7
May 10, 2022 20:24:08.869493008 CEST	49867	4040	192.168.2.7	91.193.75.221
May 10, 2022 20:24:08.910485029 CEST	4040	49867	91.193.75.221	192.168.2.7

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Ki8WlC0ddA.exe PID: **4340**, Parent PID: **5200**

General

Target ID:	0
Start time:	20:22:01
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Ki8WlC0ddA.exe"
Imagebase:	0x110000
File size:	657920 bytes
MD5 hash:	0F8819270F261881BDFDBB15FE4F4D7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.435002351.00000000024C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.437559429.00000000036A5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.437559429.00000000036A5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.437559429.00000000036A5000.00000004.00000800.00020000.00000000.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	6DC1CF06	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	6DC1CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nbbxvA.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	6CA6DD66	CopyFileW
C:\Users\user\AppData\Roaming\nbbxvA.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CA6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp39F4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CA67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ki8WlC0ddA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF2C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp39F4.tmp	success or wait	1	6CA66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nbbxvA.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 03 00 fd fd 78 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 00 0a 00 00 08 00 00 00 00 00 00 42 1e 0a 00 00 20 00 00 00 20 0a 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 60 0a 00 00 02 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.$PELxb0B @ `@	success or wait	3	6CA6DD66	CopyFileW
C:\Users\user\AppData\Roaming\nbbxvA.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	6CA6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp39F4.tmp	0	1609	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 66 72 6f 6e 74 64 65 73 6b 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	<?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> </RegistrationInf	success or wait	1	6CA61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Ki8WIC0ddA.exe.log	0	1308	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	6DF2C907	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	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	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	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile

Analysis Process: powershell.exe PID: **6620**, Parent PID: **4340**

General

Target ID:	4
Start time:	20:22:26
Start date:	10/05/2022
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\nbbxvA.exe
Imagebase:	0xf0000
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	6DC1CF06	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	6DC1CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r1la5k4g.tlc.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5mvax22.jet.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CA61E60	CreateFileW
C:\Users\user\Documents\20220510	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CA6BEFF	CreateDirectoryW
C:\Users\user\Documents\20220510\PowerShell_transcript.849224.GF_mjD2U.20220510202227.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CA61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r1la5k4g.tlc.ps1	success or wait	1	6CA66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5mvax22.jet.psm1	success or wait	1	6CA66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_r1la5k4g.tlc.ps1	0	1	31	1	success or wait	1	6CA61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_e5mvax22.jet.psm1	0	1	31	1	success or wait	1	6CA61B4F	WriteFile
C:\Users\user\Documents\20220510\PowerShell_transcript.849224.GF_mjD2U.20220510202227.txt	0	3	ff		success or wait	1	6CA61B4F	WriteFile
C:\Users\user\Documents\20220510\PowerShell_transcript.849224.GF_mjD2U.20220510202227.txt	3	685	2a 2a 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 35 31 30 32 30 32 32 32 39 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 66 72 6f 6e 74 64 65 73 6b 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 66 72 6f 6e 74 64 65 73 6b 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 38 34 39 32 32 34 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	**********Windows PowerShell transcript startStart time: 20220510202229Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 849224 (Microsoft Windows NT 10.0.17134.0)Host Applicatio	success or wait	44	6CA61B4F	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 64 14 00 00 18 00 00 00 4b 0c 06 05 44 07 3c 07 39 07 00 00 fd 01 58 00 08 00 2d 0c 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@edKD<9X-@	success or wait	1	6DEE76FC	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 50 00 00 00 0e 00 20 00	H<@^L"My:P	success or wait	17	6DEE76FC	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	6DEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6DEE76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6DEE76FC	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 16 3b 40 01 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 02 54 40 01 40 58 40 01 3f 58 40 01 1b 3b 40 01 1c 54 40 01 19 3b 40 01 fd 53 40 01 fd 53 40 01 fd 3c 40 01 1e 54 40 01 19 54 40 01 fd 3c 40 01 78 54 40 01 fd 3c 40 01 57 03 40 01 4d 03 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 fd 45 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 00 01 38 4d 00 01 3f 4d 00 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@;@[@NT@HT@S@S@hT@ S@ S@S@\@T@T@@X@? X@;@T@;@S@S@<@ T@ T@<@xT@<@W@M@z T@T@=M@DM@:M@" M@E@ M@!M@;M@D@D@@M @<M@$M8M?MBMDmE	success or wait	11	6DEE76FC	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	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6DC01F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23120	success or wait	1	6DC0203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	62	success or wait	1	6CA61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	2	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6DBF5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6DBF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	12	6CA61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6CA61B4F	ReadFile

Analysis Process: conhost.exe PID: **2892**, Parent PID: **6620**

General

Target ID:	5
Start time:	20:22:26
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: **2896**, Parent PID: **4340**

General

Target ID:	6
Start time:	20:22:26
Start date:	10/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nbbxvA" /XML "C:\Users\user\AppData\Local\Temp\tmp39F4.tmp
Imagebase:	0xcf0000
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\tmp39F4.tmp	unknown	2	success or wait	1	CFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp39F4.tmp	unknown	1610	success or wait	1	CFABD9	ReadFile

Analysis Process: conhost.exe PID: **5288**, Parent PID: **2896**

General	
Target ID:	7
Start time:	20:22:28
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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: Ki8WlC0ddA.exe PID: **5072**, Parent PID: **4340**

General	
Target ID:	9
Start time:	20:22:30
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
Imagebase:	0x430000
File size:	657920 bytes
MD5 hash:	0F8819270F261881BDFDBB15FE4F4D7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Ki8WlC0ddA.exe PID: **6192**, Parent PID: **4340**

General	
Target ID:	12
Start time:	20:22:32
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Ki8WlC0ddA.exe
Imagebase:	0x5a0000
File size:	657920 bytes
MD5 hash:	0F8819270F261881BDFDBB15FE4F4D7C
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: 0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.427017575.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.624692987.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.624692987.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.624692987.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.632329502.0000000005130000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.632329502.0000000005130000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.632329502.0000000005130000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.424343119.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.424343119.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.424343119.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.424852171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.424852171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.424852171.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.425529951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.425529951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.425529951.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.630145120.00000000039B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.630145120.00000000039B9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.632605760.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.632605760.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.632605760.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000C.00000002.632605760.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
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	6DC1CF06	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	6DC1CF06	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	6CA6BEFF	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	6CA61E60	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	6CA6BEFF	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	6CA6BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Ki8WlC0ddA.exe:Zone.Identifier	success or wait	1	6C9E2935	unknown

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	68 fd 2a fd fd 32 fd 48	h*2H	success or wait	1	6CA61B4F	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	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA61B4F	ReadFile
C:\Users\user\Desktop\Ki8WlC0ddA.exe	unknown	4096	success or wait	1	6DBDD72F	unknown
C:\Users\user\Desktop\Ki8WlC0ddA.exe	unknown	512	success or wait	1	6DBDD72F	unknown

Disassembly

No disassembly