ID: 800441
Sample Name:
cRC31pEDkr.exe
Cookbook: default.jbs
Time: 13:58:11
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

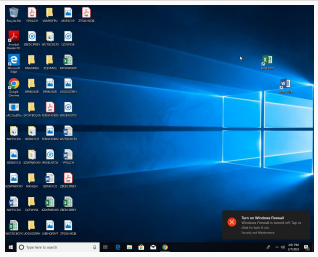
Windows Analysis Report

cRC31pEDkr.exe

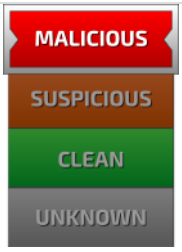
Overview

General Information

Sample Name:	cRC31pEDkr.exe
Analysis ID:	800441
MD5:	ac2609d2181f7..
SHA1:	2ac2462013be…
SHA256:	9730aee1d4d0…
Tags:	exe NanoCore
Infos:	



Detection



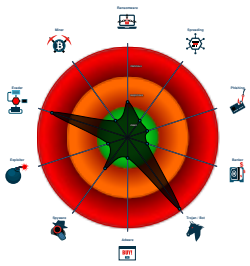
Nanocore, zgRAT

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- cRC31pEDkr.exe (PID: 4064 cmdline: C:\Users\user\Desktop\cRC31pEDkr.exe MD5: AC2609D2181F756550E3C180329B121C)
  - powershell.exe (PID: 3492 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\cRC31pEDkr.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4332 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4724 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KgZEfacljaFey" /XML "C:\Users\user\AppData\Local\Temp\tmp5E04.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cRC31pEDkr.exe (PID: 4980 cmdline: C:\Users\user\Desktop\cRC31pEDkr.exe MD5: AC2609D2181F756550E3C180329B121C)
  - cRC31pEDkr.exe (PID: 4556 cmdline: C:\Users\user\Desktop\cRC31pEDkr.exe MD5: AC2609D2181F756550E3C180329B121C)
  - cRC31pEDkr.exe (PID: 1876 cmdline: C:\Users\user\Desktop\cRC31pEDkr.exe MD5: AC2609D2181F756550E3C180329B121C)
- KgZEfacljaFey.exe (PID: 6040 cmdline: C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe MD5: AC2609D2181F756550E3C180329B121C)
  - schtasks.exe (PID: 5600 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KgZEfacljaFey" /XML "C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - KgZEfacljaFey.exe (PID: 5196 cmdline: C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe MD5: AC2609D2181F756550E3C180329B121C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "e971e6b5-1c8b-4bb4-a1a3-7f94e076",
  "Group": "Ebube",
  "Domain1": "elzy.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 2000,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x42f0d:$a: NanoCore • 0x42f66:$a: NanoCore • 0x42fa3:$a: NanoCore • 0x4301c:$a: NanoCore • 0x566c7:$a: NanoCore • 0x566dc:$a: NanoCore • 0x56711:$a: NanoCore • 0x6f183:$a: NanoCore • 0x6f198:$a: NanoCore • 0x6f1cd:$a: NanoCore • 0x42f6f:$b: ClientPlugin • 0x42fac:$b: ClientPlugin • 0x438aa:$b: ClientPlugin • 0x438b7:$b: ClientPlugin • 0x56483:$b: ClientPlugin • 0x5649e:$b: ClientPlugin • 0x564ce:$b: ClientPlugin • 0x566e5:$b: ClientPlugin • 0x5671a:$b: ClientPlugin • 0x6ef3f:$b: ClientPlugin • 0x6ef5a:$b: ClientPlugin
0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x42fa3:$a1: NanoCore.ClientPluginHost • 0x56711:$a1: NanoCore.ClientPluginHost • 0x6f1cd:$a1: NanoCore.ClientPluginHost • 0x42f66:$a2: NanoCore.ClientPlugin • 0x566dc:$a2: NanoCore.ClientPlugin • 0x6f198:$a2: NanoCore.ClientPlugin • 0x4333a:$b1: get_BuilderSettings • 0x5b657:$b1: get_BuilderSettings • 0x74113:$b1: get_BuilderSettings • 0x42ff1:$b4: IClientAppHost • 0x433ab:$b6: AddHostEntry • 0x4341a:$b7: LogClientException • 0x5b5c6:$b7: LogClientException • 0x74082:$b7: LogClientException • 0x4338f:$b8: PipeExists • 0x42fde:$b9: IClientLoggingHost • 0x5672b:$b9: IClientLoggingHost • 0x6f1e7:$b9: IClientLoggingHost
0000000A.00000002.562803290.00000000026D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.562803290.00000000026D1000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x36139:$a1: NanoCore.ClientPluginHost • 0x360fc:$a2: NanoCore.ClientPlugin • 0x364d0:$b1: get_BuilderSettings • 0x36187:$b4: IClientAppHost • 0x36541:$b6: AddHostEntry • 0x365b0:$b7: LogClientException • 0x36525:$b8: PipeExists • 0x36174:$b9: IClientLoggingHost
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.cRC31pEDkr.exe.5290000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
10.2.cRC31pEDkr.exe.5290000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
10.2.cRC31pEDkr.exe.5290000.3.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
10.2.cRC31pEDkr.exe.5290000.3.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
14.2.KgZEfacljaFey.exe.3b8ff64.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 93 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

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

Multi AV Scanner detection for submitted file

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

Uses dynamic DNS services

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 zgRAT

Yara detected Nanocore RAT

Remote Access Functionality

Yara detected zgRAT

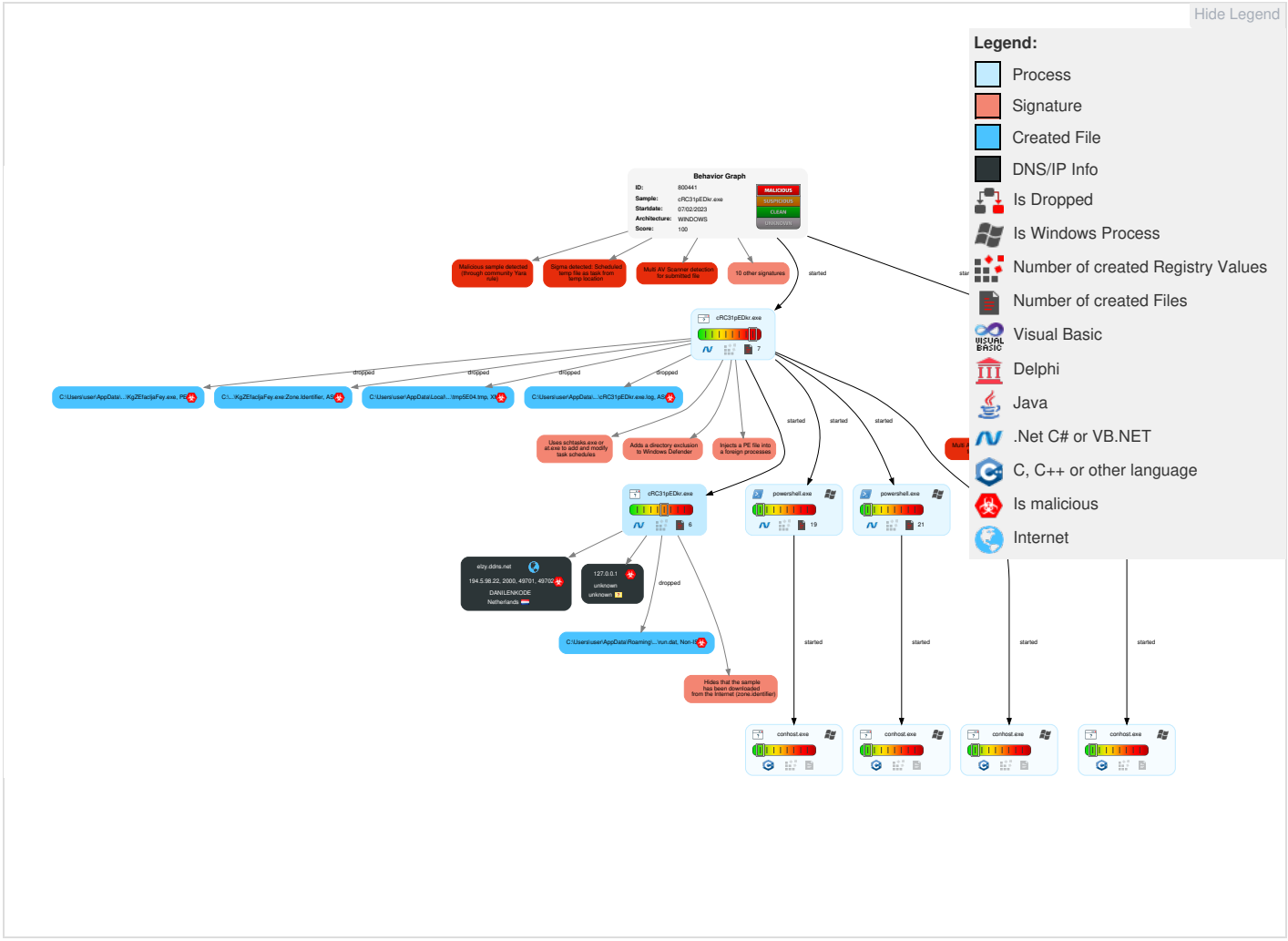
Detected Nanocore Rat

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	2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process 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 1 Virtualization/Sandbox Evasion	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	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information 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	Network Sniffing	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

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
cRC31pEDkr.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.RedLine	
cRC31pEDkr.exe	58%	Virustotal		Browse
cRC31pEDkr.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.RedLine	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.cRC31pEDkr.exe.5a60000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.2.KgZEfacljaFey.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
elzy.ddns.net	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.com9	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.carterandcone.comX	0%	URL Reputation	safe	
http://www.fontbureau.comk:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/K	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.sandoll.co.krUN.TTFq	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn%	0%	URL Reputation	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/B	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/K	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.carterandcone.com/	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/pa	0%	Avira URL Cloud	safe	
http://www.carterandcone.comUI	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdfet	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.sandoll.co.krs-c	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnp	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s_tr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Y	0%	URL Reputation	safe	
http://www.carterandcone.como.T	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnalg	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalicB	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.carterandcone.comorm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0;	0%	Avira URL Cloud	safe	
http://www.carterandcone.comiE	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0MSB	0%	Avira URL Cloud	safe	
http://www.carterandcone.comgU	0%	Avira URL Cloud	safe	
http://www.tiro.com(T	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivdo	0%	Avira URL Cloud	safe	
http://www.agfamonotype.:	0%	Avira URL Cloud	safe	
http://fontfabrik.com(	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnai	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCO	0%	Avira URL Cloud	safe	
http://fontfabrik.comV	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFB	0%	Avira URL Cloud	safe	
elzy.ddns.net	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/q	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF:	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comb-n	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comonyo	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com.l	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsivr	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtur	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomFB	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn%l	0%	Avira URL Cloud	safe	
http://www.fontbureau.comuB	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/H	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elzy.ddns.net	194.5.98.22	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.htmld.	cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061C4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061C3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305483804.00000000061C3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/pa	cRC31pEDkr.exe, 00000000.00000003.298728068.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298967599.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298859286.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298929001.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	cRC31pEDkr.exe, 00000000.00000003.304695105.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304762717.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.295924683.0000000061920000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comk:	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.307034097.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306899940.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.307202697.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.307122475.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comUI	cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgreta	cRC31pEDkr.exe, 00000000.00000003.313368578.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313245718.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.312989584.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313086465.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313567844.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313446406.00000000061AF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krUN.TTFq	cRC31pEDkr.exe, 00000000.00000003.298180772.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298215222.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com9	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306012535.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305740219.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305962193.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305830017.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305783137.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305703104.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdfet	cRC31pEDkr.exe, 00000000.00000003.304814982.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304911562.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304695105.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304762717.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304864258.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	cRC31pEDkr.exe, 00000000.00000002.345847320.0000000003251000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.345847320.00000000033A6000.00000004.00000800.00020000.00000000.sdmp, KgZEfacljaFey.exe, 00000007.00000002.388126518.0000000002C71000.00000004.00000800.00020000.00000000.sdmp, KgZEfacljaFey.exe, 00000007.00000002.388126518.0000000002EED000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 0000000A.00000002.562803290.00000000026D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.como.	cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com=	cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061B4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/	cRC31pEDkr.exe, 00000000.00000003.308327351.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.308403894.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.308132703.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.308242645.00000000061B1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.T	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300300850.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomd	cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305740219.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305703104.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061B4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comX	cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnalg	cRC31pEDkr.exe, 00000000.00000003.298728068.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298967599.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298859286.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298515941.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299115455.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298929001.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/K	cRC31pEDkr.exe, 00000000.00000003.301234096.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302112307.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301955327.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalicB	cRC31pEDkr.exe, 00000000.00000003.305962193.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/B	cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301430204.00000000061AF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	cRC31pEDkr.exe, 00000000.00000003.313368578.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313245718.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313086465.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313567844.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313446406.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355271792.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	cRC31pEDkr.exe, 00000000.00000003.297044710.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296998530.00000000061B7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comiE	cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0;	cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301430204.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	cRC31pEDkr.exe, 00000000.00000003.298215222.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298249561.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0MSB	cRC31pEDkr.exe, 00000000.00000003.301234096.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/t	cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301430204.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comgU	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com(T	cRC31pEDkr.exe, 00000000.00000003.299081793.000000000187C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comsivdo	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.agfamonotype.:	cRC31pEDkr.exe, 00000000.00000003.312291594.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.312434363.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	cRC31pEDkr.exe, 00000000.00000003.305830017.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com(	cRC31pEDkr.exe, 00000000.00000003.296893411.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296871633.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296944042.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296795116.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296850779.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296915043.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296828770.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296755309.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296778637.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.zhongyicts.com.cnF	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnai	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn%	cRC31pEDkr.exe, 00000000.00000003.298728068.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300300850.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298967599.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298859286.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298515941.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299115455.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299194871.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298929001.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comI.TTF	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306012535.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305740219.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305962193.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305830017.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305783137.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306063064.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.comV	cRC31pEDkr.exe, 00000000.00000003.296795116.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296778637.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/B	cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302112307.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301955327.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersL	cRC31pEDkr.exe, 00000000.00000003.304353505.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/K	cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301430204.00000000061AF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comTCO	cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298929001.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299081793.000000000187C000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com/	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comFB	cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300300850.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com.	cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krs-c	cRC31pEDkr.exe, 00000000.00000003.298180772.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298129567.00000000061AF000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	cRC31pEDkr.exe, 00000000.00000003.308242645.00000000061B1000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.309287347.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.309054521.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	cRC31pEDkr.exe, 00000000.00000003.296795116.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296850779.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296828770.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.296726022.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnp	cRC31pEDkr.exe, 00000000.00000003.298437658.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298492392.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/q	cRC31pEDkr.exe, 00000000.00000003.308132703.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF:	cRC31pEDkr.exe, 00000000.00000003.313368578.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313245718.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.312989584.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313086465.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313567844.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313446406.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355271792.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersx	cRC31pEDkr.exe, 00000000.00000003.304597500.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/s_tr	cRC31pEDkr.exe, 00000000.00000003.302453010.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302393161.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302254936.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302112307.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302501034.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301955327.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302344077.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comb-n	cRC31pEDkr.exe, 00000000.00000003.295924683.0000000006192000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	cRC31pEDkr.exe, 00000000.00000003.298180772.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298129567.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298291425.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298215222.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298249561.00000000061B1000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersn	cRC31pEDkr.exe, 00000000.00000003.304353505.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/Y	cRC31pEDkr.exe, 00000000.00000003.304174210.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304255888.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302711504.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302453010.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.303976325.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.303455893.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302393161.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302254936.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.303356467.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304105124.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302112307.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302841481.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301490267.00000000061B0000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302937899.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.303747330.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302501034.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302640559.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.303072404.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comonyo	cRC31pEDkr.exe, 00000000.00000003.304353505.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299194871.00000000061AB000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306012535.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304421291.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304353505.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304556150.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305962193.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305830017.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306899940.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304597500.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304305637.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304506350.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306063064.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	cRC31pEDkr.exe, 00000000.00000003.304814982.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306012535.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305740219.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305962193.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305830017.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305783137.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306899940.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305910322.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306141858.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304911562.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comTC	cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsivr	cRC31pEDkr.exe, 00000000.00000003.304305637.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com.l	cRC31pEDkr.exe, 00000000.00000003.295924683.0000000006192000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/o	cRC31pEDkr.exe, 00000000.00000003.301785059.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301578884.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302112307.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301845055.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301955327.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

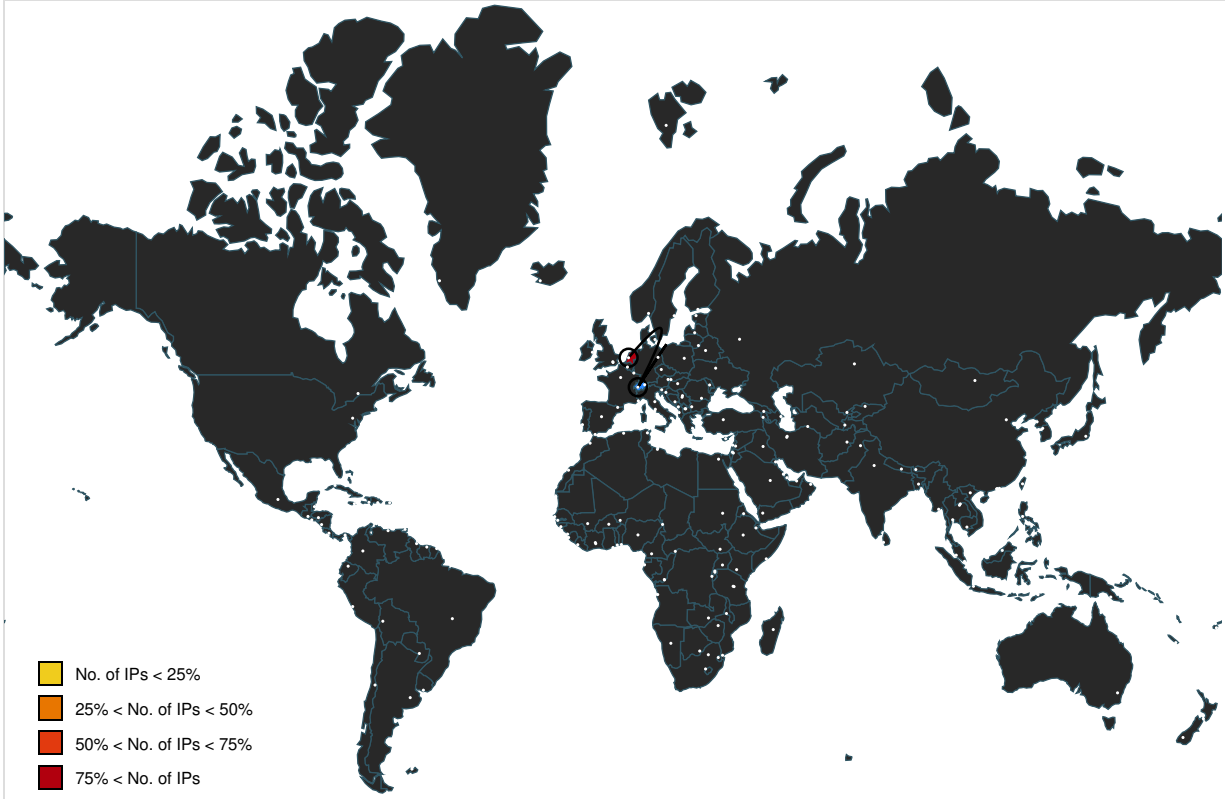
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comcomFB	cRC31pEDkr.exe, 00000000.00000003.306651559.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306765652.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306221985.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306335557.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306899940.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306566595.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.306708081.00000000061B2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtur	cRC31pEDkr.exe, 00000000.00000003.304814982.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304597500.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304911562.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304695105.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304762717.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305703104.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304864258.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/H	cRC31pEDkr.exe, 00000000.00000003.298728068.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299661403.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299622371.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299398041.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300300850.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298967599.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298859286.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299487627.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298515941.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299442136.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299115455.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299194871.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300062616.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299700076.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299806283.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299958934.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.299896606.00000000061B9000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298929001.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	cRC31pEDkr.exe, 00000000.00000003.304814982.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305285674.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305615259.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305740219.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305000246.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304556150.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305570163.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305229705.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304597500.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304911562.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305173293.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305068245.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304695105.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304762717.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305432351.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305703104.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.305526668.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304864258.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn%I	cRC31pEDkr.exe, 00000000.00000003.299274112.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/cabarga.htmlN	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	cRC31pEDkr.exe, 00000000.00000003.298437658.00000000061B8000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298515941.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298663743.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.298492392.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comuB	cRC31pEDkr.exe, 00000000.00000003.313368578.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313245718.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313086465.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.313446406.00000000061AF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comorm	cRC31pEDkr.exe, 00000000.00000003.300199248.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.300143320.00000000061B8000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	cRC31pEDkr.exe, 00000000.00000003.301430204.00000000061AF000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301752812.00000000061B4000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301721227.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.301955327.00000000061B3000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302344077.00000000061B2000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.302191536.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	cRC31pEDkr.exe, 00000000.00000002.355816289.00000000073A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/	cRC31pEDkr.exe, 00000000.00000003.304305637.00000000061BB000.00000004.00000020.00020000.00000000.sdmp, cRC31pEDkr.exe, 00000000.00000003.304305637.00000000061B3000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.22	elzy.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800441

Start date and time:	2023-02-07 13:58:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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
Sample file name:	cRC31pEDkr.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@22/12@10/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe, WmiPrvSE.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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
13:59:13	API Interceptor	784x Sleep call for process: cRC31pEDkr.exe modified
13:59:17	Task Scheduler	Run new task: KgZEfacljaFey path: C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
13:59:18	API Interceptor	55x Sleep call for process: powershell.exe modified
13:59:32	API Interceptor	1x Sleep call for process: KgZEfacljaFey.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\KgZEfacljaFey.exe.log

Process:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cRC31pEDkr.exe.log

Process:	C:\Users\user\Desktop\cRC31pEDkr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
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):	21864
Entropy (8bit):	5.598059944466488
Encrypted:	false
SSDEEP:	384:+tCRLq0+3R2EYf3YSVxnejulrItCiJ9g9SJ3uyV1Im0ZSAVrdt8hqA+iRYg:bDgUxeClrSy9cuG3Uqg
MD5:	F0E335C7015467AA88CB725D1E79D3E3
SHA1:	2CB9B862933DC5AF60596D12EDB1F676C4AD9B6F
SHA-256:	C02AE364FCD84F5B4E478CB668B7F578C55E678AF9EE4C30254FB90B30BD0422
SHA-512:	8CE3A87486B215ABCDB564EBC8489E1D88065F7936D5234E6BCC201A1D34C4845D618CBC04F95F40700170A806881486B2E45E2F161188B9FD19831C24F8EB22
Malicious:	false
Preview:	@...e.....:.X.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.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_l55gaxga.5bu.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wn1bnogj.r25.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xlbtqxm5.ana.ps1

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

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_z0sc0zox.gi0.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp5E04.tmp

Process:	C:\Users\user\Desktop\cRC31pEDkr.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	5.134330559128222
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTuv
MD5:	B60F588C1155AF27B4F7C47D9BA68B63
SHA1:	060A5DB198839D2D4D33E2DA93540D3BD1851042
SHA-256:	4467302D8DE2891402E2EC25B9824333F433D46A306D120E32D93BE4F216C492
SHA-512:	89527F28ED63991D6B1C0D18FDA21F9CF77E0CAB8EEA228359B9781C57FCE2D5EDACDBE5F26C5EB39DEE9C9B0384BD9C89628991D6A5C53B4C87B426410FD 537
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>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp

Process:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1604
Entropy (8bit):	5.134330559128222
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTuv
MD5:	B60F588C1155AF27B4F7C47D9BA68B63
SHA1:	060A5DB198839D2D4D33E2DA93540D3BD1851042
SHA-256:	4467302D8DE2891402E2EC25B9824333F433D46A306D120E32D93BE4F216C492
SHA-512:	89527F28ED63991D6B1C0D18FDA21F9CF77E0CAB8EEA228359B9781C57FCE2D5EDACDBE5F26C5EB39DEE9C9B0384BD9C89628991D6A5C53B4C87B426410FD 537
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

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

Process:	C:\Users\user\Desktop\cRC31pEDkr.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:CS:P
MD5:	76420758AE4C29CAAD2AA6B116E41716
SHA1:	59893B920B4F94B033959DA9C02E6156E8DD98DF
SHA-256:	136D683384EA664828711F6043304C6D2A1E89C3F8DAD346F6007FF13DD5F45D
SHA-512:	892DCB7634396D212CFA50CCA7610683BC01B83743131BE2F700912617F563498EBE2F0450DD59CF46448A298DB2A37C68394DEFF8A00D5480CD68F6A509FB64
Malicious:	**true**
Preview:	of.V..H

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

Process:	C:\Users\user\Desktop\cRC31pEDkr.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	705536
Entropy (8bit):	7.810105998338931
Encrypted:	false
SSDEEP:	12288:VVC66Bm2iNNHOp7HPfublVc1E0cE3UyV5sXoDCnJ8OSTaHlUI1FuH66B:GVM1rut21E0cEkI24D6PSuHlvuHV
MD5:	AC2609D2181F756550E3C180329B121C
SHA1:	2AC2462013BE76E3BB606C7DEAEC5E0E4609CD59
SHA-256:	9730AEE1D4D04BB12E1DF2A5550741EED7266625F8D99443DD0CD0DFFCA07112
SHA-512:	EE9DC08DD3E713FFE4A7FB658A37E8C689A5CDAC7E1CFA6FB3A26A048663FF70B524C49FCEF3B0C033D4DD2EFBE290E2DC62BE74145C461D1E711356C8260DA2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....f...w.....0.....}.....}.....(.....(.....}.....s....}..... ....s....}.....{.....s....}.....{....r...po.....(.....{. ...o.....{.....o.....{....o.....s....s....}.....(.....(.....{....o.....*....0.....{.....X}.....{.....}.....,-..{....(....o.....{....o....(....o....8.....{....(...o.....{....o....(...o.....(.....{.....,{.....+.....,.(..... {.....s....o.....{....o!..

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

Process:	C:\Users\user\Desktop\cRC31pEDkr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.810105998338931

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:	cRC31pEDkr.exe
File size:	705536
MD5:	ac2609d2181f756550e3c180329b121c
SHA1:	2ac2462013be76e3bb606c7deaec5e0e4609cd59
SHA256:	9730aee1d4d04bb12e1df2a5550741eed7266625f8d99443dd0cd0dffca07112
SHA512:	ee9dc08dd3e713ffe4a7fb658a37e8c689a5cdac7e1cfa6fb3a26a048663ff70b524c49fcef3b0c033d4dd2efbe290e2dc62be74145c461d1e711356c826cda2
SSDEEP:	12288:VVC66Bm2iNNHOp7HPfublVc1E0cE3UyV5sXoDCnJ8OSTaHlUI1FuH66B:GVM1rut21E0cEkI24D6PSuHlvuHV
TLSH:	39E401811D64CA58E2F90EBD0F7C5A2D8FF45C9923E3E2B40BE6B4D9A463783C815536
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ad902
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xF2C4F3B5 [Sun Jan 25 03:08:37 2099 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

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
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	0xad8b0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xad894	0x1c	.text
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	0xab908	0xaba00	False	0.8738022350691915	data	7.818047676595979	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x5bc	0x600	False	0.4283854166666667	data	4.10376699366461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

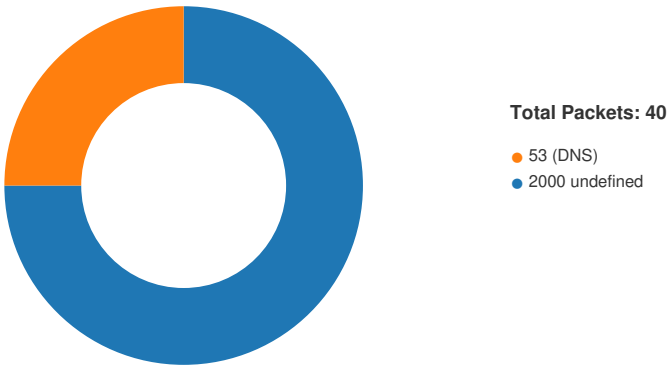
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xae090	0x32c	data		
RT_MANIFEST	0xae3cc	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 13:59:31.713982105 CET	49701	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:31.757090092 CET	2000	49701	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:32.392255068 CET	49701	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:32.435534000 CET	2000	49701	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:33.001553059 CET	49701	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:33.044615030 CET	2000	49701	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:37.180790901 CET	49702	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:37.223854065 CET	2000	49702	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:37.845783949 CET	49702	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:37.888947010 CET	2000	49702	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:38.549042940 CET	49702	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:38.592144012 CET	2000	49702	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:42.792201996 CET	49703	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:42.835329056 CET	2000	49703	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:43.346213102 CET	49703	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:43.389285088 CET	2000	49703	194.5.98.22	192.168.2.5
Feb 7, 2023 13:59:44.049402952 CET	49703	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 13:59:44.092649937 CET	2000	49703	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:04.116805077 CET	49710	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:04.159924030 CET	2000	49710	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:04.660533905 CET	49710	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:04.703702927 CET	2000	49710	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:05.207479000 CET	49710	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:05.250614882 CET	2000	49710	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:09.301789045 CET	49712	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:09.344774961 CET	2000	49712	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:09.848398924 CET	49712	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:09.891593933 CET	2000	49712	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:10.395400047 CET	49712	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:10.438546896 CET	2000	49712	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:14.486471891 CET	49713	2000	192.168.2.5	194.5.98.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 14:00:14.530375004 CET	2000	49713	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:15.036335945 CET	49713	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:15.081300020 CET	2000	49713	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:15.583241940 CET	49713	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:15.626451015 CET	2000	49713	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:35.702507973 CET	49718	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:35.745628119 CET	2000	49718	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:36.256872892 CET	49718	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:36.300020933 CET	2000	49718	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:36.803818941 CET	49718	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:36.846869946 CET	2000	49718	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:41.506460905 CET	49719	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:41.549746990 CET	2000	49719	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:42.054270983 CET	49719	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:42.097364902 CET	2000	49719	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:42.663737059 CET	49719	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:42.708404064 CET	2000	49719	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:46.919289112 CET	49721	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:46.962531090 CET	2000	49721	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:47.476569891 CET	49721	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:47.519581079 CET	2000	49721	194.5.98.22	192.168.2.5
Feb 7, 2023 14:00:48.023495913 CET	49721	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:00:48.066632986 CET	2000	49721	194.5.98.22	192.168.2.5
Feb 7, 2023 14:01:07.652275085 CET	49726	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:01:07.695615053 CET	2000	49726	194.5.98.22	192.168.2.5
Feb 7, 2023 14:01:08.207467079 CET	49726	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:01:08.250525951 CET	2000	49726	194.5.98.22	192.168.2.5
Feb 7, 2023 14:01:08.762331963 CET	49726	2000	192.168.2.5	194.5.98.22
Feb 7, 2023 14:01:08.805807114 CET	2000	49726	194.5.98.22	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 13:59:31.679389000 CET	61893	53	192.168.2.5	8.8.8.8
Feb 7, 2023 13:59:31.699139118 CET	53	61893	8.8.8.8	192.168.2.5
Feb 7, 2023 13:59:37.159048080 CET	60649	53	192.168.2.5	8.8.8.8
Feb 7, 2023 13:59:37.179442883 CET	53	60649	8.8.8.8	192.168.2.5
Feb 7, 2023 13:59:42.715939045 CET	51441	53	192.168.2.5	8.8.8.8
Feb 7, 2023 13:59:42.735929966 CET	53	51441	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:04.092628002 CET	65323	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:04.113540888 CET	53	65323	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:09.282095909 CET	63446	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:09.300489902 CET	53	63446	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:14.467171907 CET	56751	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:14.485213041 CET	53	56751	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:35.679114103 CET	60975	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:35.700711012 CET	53	60975	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:41.407455921 CET	59220	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:41.429548979 CET	53	59220	8.8.8.8	192.168.2.5
Feb 7, 2023 14:00:46.845959902 CET	56682	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:00:46.865693092 CET	53	56682	8.8.8.8	192.168.2.5
Feb 7, 2023 14:01:07.633317947 CET	62659	53	192.168.2.5	8.8.8.8
Feb 7, 2023 14:01:07.651314974 CET	53	62659	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 13:59:31.679389000 CET	192.168.2.5	8.8.8.8	0xb8e1	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false

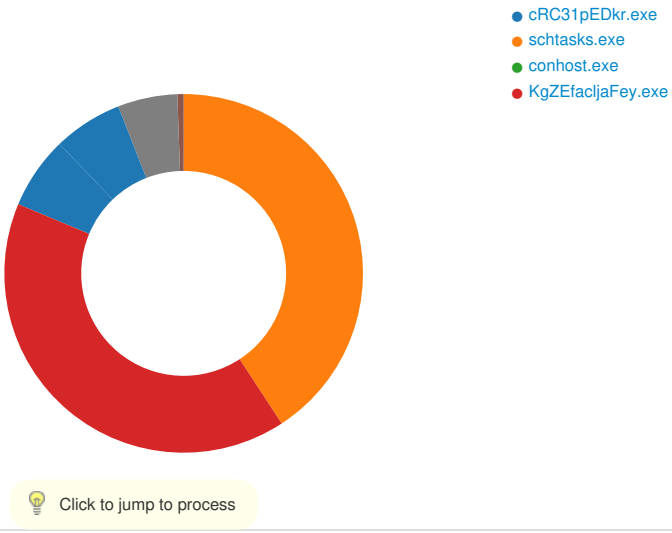
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 13:59:37.159048080 CET	192.168.2.5	8.8.8.8	0xc0cd	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:59:42.715939045 CET	192.168.2.5	8.8.8.8	0xc75e	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:04.092628002 CET	192.168.2.5	8.8.8.8	0x1f49	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:09.282095909 CET	192.168.2.5	8.8.8.8	0x26db	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:14.467171907 CET	192.168.2.5	8.8.8.8	0x8558	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:35.679114103 CET	192.168.2.5	8.8.8.8	0xdfdc	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:41.407455921 CET	192.168.2.5	8.8.8.8	0x1d80	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:46.845959902 CET	192.168.2.5	8.8.8.8	0x7a18	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:01:07.633317947 CET	192.168.2.5	8.8.8.8	0xd446	Standard query (0)	elzy.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 13:59:31.699139118 CET	8.8.8.8	192.168.2.5	0xb8e1	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:59:37.179442883 CET	8.8.8.8	192.168.2.5	0xc0cd	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 13:59:42.735929966 CET	8.8.8.8	192.168.2.5	0xc75e	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:04.113540888 CET	8.8.8.8	192.168.2.5	0x1f49	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:09.300489902 CET	8.8.8.8	192.168.2.5	0x26db	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:14.485213041 CET	8.8.8.8	192.168.2.5	0x8558	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:35.700711012 CET	8.8.8.8	192.168.2.5	0xdfdc	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:41.429548979 CET	8.8.8.8	192.168.2.5	0x1d80	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:00:46.865693092 CET	8.8.8.8	192.168.2.5	0x7a18	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false
Feb 7, 2023 14:01:07.651314974 CET	8.8.8.8	192.168.2.5	0xd446	No error (0)	elzy.ddns.net		194.5.98.22	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: cRC31pEDkr.exe PID: 4064, Parent PID: 3324

General

Target ID:	0
Start time:	13:59:04
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\cRC31pEDkr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\cRC31pEDkr.exe
Imagebase:	0xe60000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.350028595.000000000436A000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.350028595.000000000436A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.350028595.000000000436A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.350028595.000000000436A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.345847320.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.345847320.00000000033A6000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	7222CF06	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	7222CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\KgZEfacljaFey.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	7107DD66	CopyFileW
C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7107DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5E04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cRC31pEDkr.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5E04.tmp	success or wait	1	71076A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\KgZEfacljaFey.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 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0a 00 00 08 00 00 00 00 00 00 02 fd 0a 00 00 20 00 00 00 fd 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 20 0b 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.$PEL0 @ @	success or wait	3	7107DD66	CopyFileW
C:\Users\user\AppData\Roaming\KgZEfacljaFey.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	7107DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5E04.tmp	0	1604	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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cRC31pEDkr.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: powershell.exe PID: **3492**, Parent PID: **4064**

General

Target ID:	1
Start time:	13:59:15
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\cRC31pEDkr.exe
Imagebase:	0xe80000
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\AppData\Local\Temp__PSscriptPolicyTest_z0sc0zox.gi0.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wn1bnogj.r25.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW
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	7222CF06	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	7222CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z0sc0zox.gi0.ps1	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wn1bnogj.r25.psm1	success or wait	1	71076A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_z0sc0zox.gi0.ps1	0	1	31	1	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_wn1bnogj.r25.psm1	0	1	31	1	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 12 14 00 00 19 00 00 00 fd 0e fd 04 fd 09 fd 09 09 00 00 3a 01 58 00 08 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@e:X@	success or wait	1	724F76FC	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	724F76FC	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	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	724F76FC	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	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72211F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	22412	success or wait	1	7221203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	83	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: conhost.exe PID: **4580**, Parent PID: **3492**

General

Target ID:	2
Start time:	13:59:15
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **4332**, Parent PID: **4064**

General

Target ID:	3
Start time:	13:59:15
Start date:	07/02/2023
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\KgZEfacljaFey.exe
Imagebase:	0xe80000
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\AppData\Local\Temp__PSscriptPolicyTest_xlbtqxm5.ana.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l55gaxga.5bu.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW
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	7222CF06	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	7222CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xlbtqxm5.ana.ps1	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l55gaxga.5bu.psm1	success or wait	1	71076A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_xlbtqxm5.ana.ps1	0	1	31	1	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_l55gaxga.5bu.psm1	0	1	31	1	success or wait	1	71071B4F	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 12 14 00 00 19 00 00 00 fd 0e fd 04 fd 09 fd 09 09 00 00 3a 01 58 00 08 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e:X@	success or wait	1	724F76FC	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	724F76FC	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	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	724F76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	724F76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00 01 45 4d 00 01 fd 71 00 01 fd 71 00 01 fd 53 00 01 fd 25 00 01 fd 6e 00 01 34 26 00 01 35 26 00 01 37 26 00	T@>@@V@H@X@[@NT@HT@S@S@hT@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@T@=M@DM@:M@"M@M@!M@;M@D@D@@M@<M@$M@8M@?M@BMDmEEMqqS%n4&5&7&	success or wait	11	724F76FC	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	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	7220CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72211F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	65	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71071B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72205705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: conhost.exe PID: **4592**, Parent PID: **4332**

General	
Target ID:	4
Start time:	13:59:15
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: **4724**, Parent PID: **4064**

General	
Target ID:	5
Start time:	13:59:15
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KgZEfacljaFey" /XML "C:\Users\user\AppData\Local\Temp\tmp5E04.tmp
Imagebase:	0x820000
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\tmp5E04.tmp	unknown	2	success or wait	1	82AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5E04.tmp	unknown	1605	success or wait	1	82ABD9	ReadFile

Analysis Process: conhost.exe PID: **4476**, Parent PID: **4724**

General	
Target ID:	6
Start time:	13:59:15
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: KgZEfacljaFey.exe PID: **6040**, Parent PID: **1084**

General

Target ID:	7
Start time:	13:59:17
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
Imagebase:	0x7ff7fcd70000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.388126518.0000000002C71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.388126518.0000000002EED000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
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	7222CF06	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	7222CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\KgZEfacljaFey.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp	success or wait	1	71076A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp	0	1604	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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationInfo>	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\KgZEfacljaFey.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile

Analysis Process: cRC31pEDkr.exe PID: **4980**, Parent PID: **4064**

General

Target ID:	8
Start time:	13:59:24
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\cRC31pEDkr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\cRC31pEDkr.exe
Imagebase:	0x1a0000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cRC31pEDkr.exe PID: **4556**, Parent PID: **4064**

General

Target ID:	9
Start time:	13:59:24
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\cRC31pEDkr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\cRC31pEDkr.exe
Imagebase:	0x2b0000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cRC31pEDkr.exe PID: **1876**, Parent PID: **4064**

General

Target ID:	10
Start time:	13:59:24
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\cRC31pEDkr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\cRC31pEDkr.exe
Imagebase:	0x450000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.562803290.00000000026D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.562803290.00000000026D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.567364411.0000000005290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.567364411.0000000005290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.567364411.0000000005290000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.567364411.0000000005290000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.566234207.000000000371B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.567497022.0000000005A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.567497022.0000000005A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.567497022.0000000005A60000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.567497022.0000000005A60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.567497022.0000000005A60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
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	7222CF06	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	7222CF06	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	7107BEFF	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	71071E60	CreateFileW
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	7107BEFF	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	7107BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cRC31pEDkr.exe:Zone.Identifier	success or wait	1	70FF2935	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	6f 66 15 56 09 fd 48	ofVH	success or wait	1	71071B4F	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	72205705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Users\user\Desktop\cRC31pEDkr.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\cRC31pEDkr.exe	unknown	512	success or wait	1	721ED72F	unknown

Analysis Process: schtasks.exe PID: **5600**, Parent PID: **6040**

General

Target ID:	12
Start time:	13:59:36
Start date:	07/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KgZEfacljaFey" /XML "C:\Users\user\AppData\Local\Temp\tmpAD4D.tmp
Imagebase:	0x820000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **2056**, Parent PID: **5600**

General

Target ID:	13
Start time:	13:59:36
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: KgZEfacljaFey.exe PID: **5196**, Parent PID: **6040**

General

Target ID:	14
Start time:	13:59:43
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\KgZEfacljaFey.exe
Imagebase:	0x750000
File size:	705536 bytes
MD5 hash:	AC2609D2181F756550E3C180329B121C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.404051124.0000000003B49000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.401166525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.401166525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.401166525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.401166525.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.403629575.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.403629575.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000E.00000002.403629575.0000000002B41000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Disassembly

No disassembly