ID: 796220
Sample Name: kcnXZ6yXoo.exe
Cookbook: default.jbs
Time: 18:23:13
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

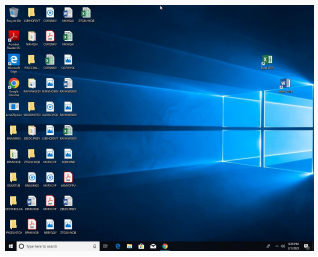
Windows Analysis Report

kcnXZ6yXoo.exe

Overview

General Information

Sample Name:	kcnXZ6yXoo.exe
Analysis ID:	796220
MD5:	cffcaceccd0c0…
SHA1:	45fbb9ddf062f8..
SHA256:	bdfc24d604f25…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

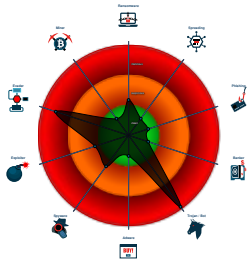
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- kcnXZ6yXoo.exe (PID: 5256 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - kcnXZ6yXoo.exe (PID: 5764 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - kcnXZ6yXoo.exe (PID: 3396 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
    - schtasks.exe (PID: 6084 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp908E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5768 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 1092 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp9283.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - MpCmdRun.exe (PID: 1092 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
      - conhost.exe (PID: 3300 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kcnXZ6yXoo.exe (PID: 5800 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe 0 MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - kcnXZ6yXoo.exe (PID: 5872 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - kcnXZ6yXoo.exe (PID: 2004 cmdline: C:\Users\user\Desktop\kcnXZ6yXoo.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
- dhcpmon.exe (PID: 5920 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - dhcpmon.exe (PID: 2284 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
- dhcpmon.exe (PID: 5904 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: CFFCACECCD0C05762DC335F58A2F0932)
  - dhcpmon.exe (PID: 1364 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: CFFCACECCD0C05762DC335F58A2F0932)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "be28fce4-4930-4ffe-96ed-0110cf99",
  "Group": "SecureKMT",
  "Domain1": "tzitziklishop.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 1665,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x227f:$x2: NanoCore.ClientPlugin • 0x2205:$x3: NanoCore.ClientPluginHost • 0x2295:$i3: IClientNetwork • 0x221f:$i6: IClientLoggingHost • 0x223e:$i7: IClientNetworkHost • 0x1f9f:$s1: ClientPlugin • 0x2288:$s1: ClientPlugin
00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2205:$a1: NanoCore.ClientPluginHost • 0x227f:$a2: NanoCore.ClientPlugin • 0x29a0:$b7: LogClientException • 0x221f:$b9: IClientLoggingHost
00000008.00000002.376686559.0000000002EB0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 106 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.kcnXZ6yXoo.exe.3135440.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
2.2.kcnXZ6yXoo.exe.3135440.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated

Source	Rule	Description	Author	Strings
2.2.kcnXZ6yXoo.exe.3135440.3.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x2d96:$x2: NanoCore.ClientPlugin • 0x2dbb:$x3: NanoCore.ClientPluginHost • 0x2d87:$i3: IClientNetwork • 0x2dac:$i4: IClientAppHost • 0x2dd5:$i5: IClientDataHost • 0x2de5:$i7: IClientNetworkHost • 0x2df8:$i9: IClientNameObjectCollection • 0x2e1d:$i10: IClientReadOnlyNameObjectCollection • 0x2bce:$s1: ClientPlugin • 0x2d9f:$s1: ClientPlugin
2.2.kcnXZ6yXoo.exe.3135440.3.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2dbb:$a1: NanoCore.ClientPluginHost • 0x2d96:$a2: NanoCore.ClientPlugin • 0x6758:$b1: get_BuilderSettings • 0x2dac:$b4: IClientAppHost
2.2.kcnXZ6yXoo.exe.5b40000.26.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
Click to see the 308 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

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26 −

Timestamp:	192.168.2.545.12.253.264972516652816766 02/01/23-18:26:06.563289
SID:	2816766
Source Port:	49725
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26 −

Timestamp:	192.168.2.545.12.253.264971916652816766 02/01/23-18:25:38.356322
SID:	2816766
Source Port:	49719
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264972216652816766 02/01/23-18:25:51.759928
SID:	2816766
Source Port:	49722
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264971516652816766 02/01/23-18:25:18.162168
SID:	2816766
Source Port:	49715
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264972616652816718 02/01/23-18:26:14.335036
SID:	2816718
Source Port:	49726
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264970116652816766 02/01/23-18:24:35.085073
SID:	2816766
Source Port:	49701
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264971616652816718 02/01/23-18:25:24.426541
SID:	2816718
Source Port:	49716
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264970316652816766 02/01/23-18:24:53.542008
SID:	2816766
Source Port:	49703
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264972116652816766 02/01/23-18:25:45.484001
SID:	2816766
Source Port:	49721
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264972616652816766 02/01/23-18:26:14.335036
SID:	2816766
Source Port:	49726

Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.12.253.26 - Destination IP: 192.168.2.5	
Timestamp:	45.12.253.26192.168.2.51665497042810290 02/01/23-18:25:00.449651
SID:	2810290
Source Port:	1665
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264971316652816766 02/01/23-18:25:12.038226
SID:	2816766
Source Port:	49713
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264971616652816766 02/01/23-18:25:24.426541
SID:	2816766
Source Port:	49716
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264972316652816766 02/01/23-18:25:58.538683
SID:	2816766
Source Port:	49723
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264971816652816766 02/01/23-18:25:32.163358
SID:	2816766
Source Port:	49718
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264970416652816766 02/01/23-18:25:02.005236
SID:	2816766
Source Port:	49704
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.545.12.253.264970216652816766 02/01/23-18:24:42.851032
SID:	2816766
Source Port:	49702
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

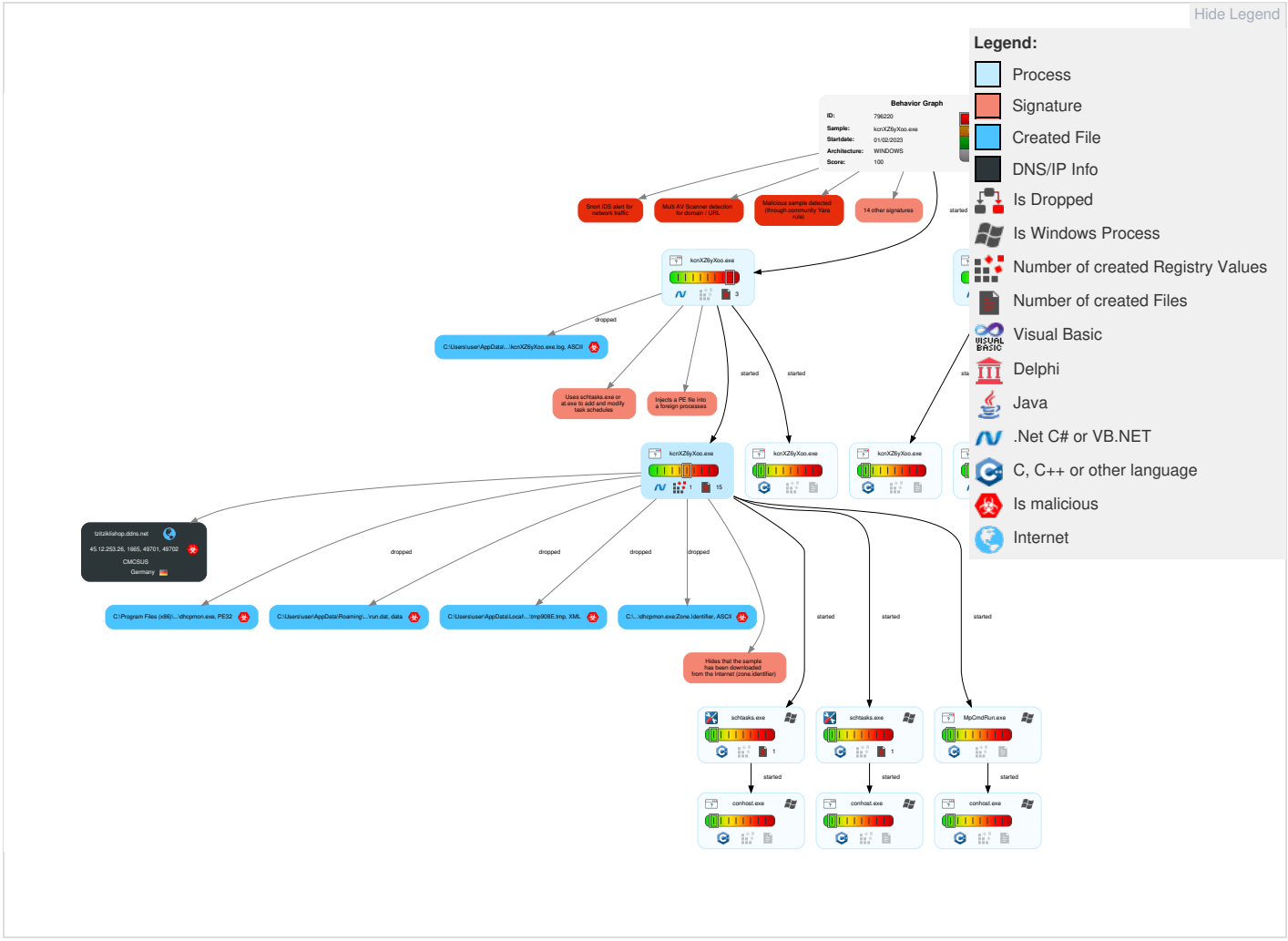
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	1 1 Input Capture	2 1 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	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	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 2 System Information 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	System Owner/User 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	3 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

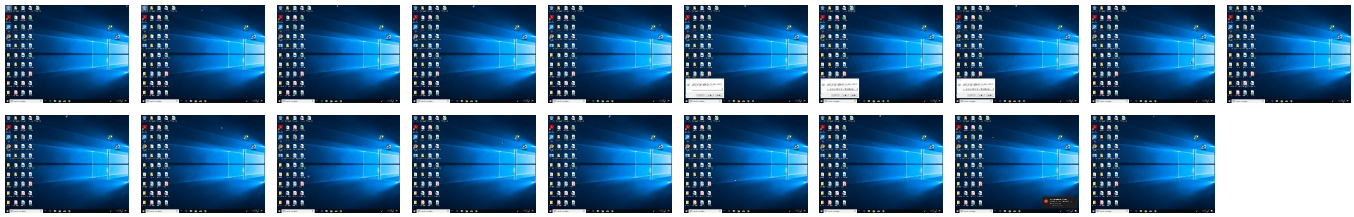
Behavior Graph



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
kcnXZ6yXoo.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	
kcnXZ6yXoo.exe	32%	Virustotal		Browse
kcnXZ6yXoo.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	26%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.kcnXZ6yXoo.exe.58e0000.23.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sakkal.comrm	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/X	0%	URL Reputation	safe	
http://www.founder.com.cn/cnhtRE_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiva	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/A	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.founder.com.cn/cntu	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comals/	0%	URL Reputation	safe	
http://www.fontbureau.comcom.	0%	Avira URL Cloud	safe	
tzitziklishop.ddns.net	100%	Avira URL Cloud	malware	
http://www.fontbureau.comdiaF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFX	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTF/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlvfetf	0%	Avira URL Cloud	safe	
http://www.sakkal.comn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtoedA	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtuo	0%	Avira URL Cloud	safe	
http://www.agfamonotype.Z	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	45.12.253.26	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comFX	kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.comrm	kcnXZ6yXoo.exe, 00000000.00000003.315644708.00000000059F3000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnhtRE_	kcnXZ6yXoo.exe, 00000000.00000003.311803735.00000000059E2000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdiaF	kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom.	kcnXZ6yXoo.exe, 00000000.00000003.318831764.00000000059FA000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comTTF/	kcnXZ6yXoo.exe, 00000000.00000003.317099709.0000000005A02000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	kcnXZ6yXoo.exe, 00000002.00000002.587607897.0000000004CCB000.00000004.00000800.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000002.00000002.587607897.0000000004A86000.00000004.00000800.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000002.00000002.587607897.0000000004B6A000.00000004.00000800.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000002.00000002.578455701.000000000311D000.00000004.00000800.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000002.00000002.603631836.0000000007620000.00000004.08000000.00040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/~	kcnXZ6yXoo.exe, 00000000.00000003.314102705.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comlvfetf	kcnXZ6yXoo.exe, 00000000.00000003.326231202.00000000059FF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	kcnXZ6yXoo.exe, 00000000.00000003.308981659.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comn	kcnXZ6yXoo.exe, 00000000.00000003.316285042.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316444935.00000000059EF000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316031658.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316410028.00000000059EE000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316514139.00000000059EF000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315917112.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316321496.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316162313.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316214959.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316551502.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316368311.00000000059EE000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316124895.00000000059F6000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315960320.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316082284.00000000059F6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	kcnXZ6yXoo.exe, 00000000.00000003.319321867.0000000005A00000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.319384991.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com%	kcnXZ6yXoo.exe, 00000000.00000003.318349413.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318831764.00000000059FA000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318511932.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318276697.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318547414.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318320632.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318631646.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.jiyu-kobo.co.jp/3	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.	kcnXZ6yXoo.exe, 00000000.00000003.318349413.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318511932.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318547414.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318631646.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/.	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/	kcnXZ6yXoo.exe, 00000000.00000003.317495074.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317720307.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317567364.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317368441.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317304521.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317221145.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317147616.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317415466.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317268864.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316162313.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315960320.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316031658.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316082284.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316124895.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315917112.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html:	kcnXZ6yXoo.exe, 00000000.00000003.317767247.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317720307.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.00000000059F4000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.00000000059F4000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.fonts.com	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/%	kcnXZ6yXoo.exe, 00000000.00000003.316321496.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316162313.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315960320.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316285042.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314102705.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316031658.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316082284.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316124895.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315917112.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtoedA	kcnXZ6yXoo.exe, 00000000.00000003.318196897.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318137112.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318276697.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	kcnXZ6yXoo.exe, 00000002.00000002.578455701.00000000030B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/X	kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsiva	kcnXZ6yXoo.exe, 00000000.00000003.318349413.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318831764.00000000059FA000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318511932.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318547414.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318631646.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	kcnXZ6yXoo.exe, 00000000.00000003.312619033.00000000059F9000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318511932.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.326231202.00000000059FF000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318547414.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318631646.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	kcnXZ6yXoo.exe, 00000000.00000003.319447929.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.319321867.0000000005A00000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.319384991.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/X	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314102705.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	kcnXZ6yXoo.exe, 00000000.00000003.318196897.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318349413.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318137112.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318831764.00000000059FA000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318667992.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318511932.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317495074.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318930233.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317720307.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317567364.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317368441.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317304521.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318276697.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318547414.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318320632.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317221145.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.Z	kcnXZ6yXoo.exe, 00000000.00000003.326231202.00000000059E0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

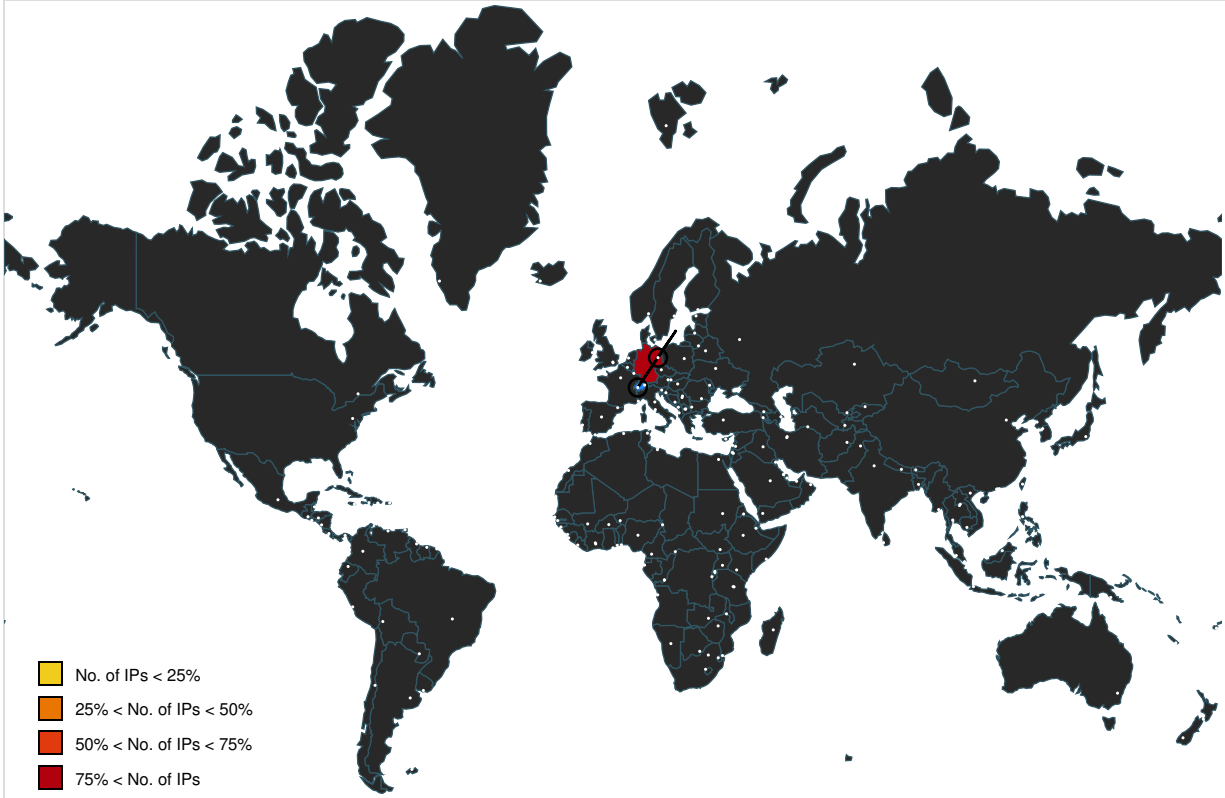
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comtuo	kcnXZ6yXoo.exe, 00000000.00000003.317495074.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317720307.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317567364.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317368441.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317304521.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317221145.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317147616.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317053909.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317099709.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317415466.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317268864.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlP(	kcnXZ6yXoo.exe, 00000000.00000003.318349413.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318276697.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318320632.0000000005A02000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/A	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314102705.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314102705.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314576431.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314305088.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd	kcnXZ6yXoo.exe, 00000000.00000003.317720307.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cntu	kcnXZ6yXoo.exe, 00000000.00000003.311803735.00000000059E2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	kcnXZ6yXoo.exe, 00000000.00000003.311803735.00000000059E2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	kcnXZ6yXoo.exe, 00000000.00000003.311803735.00000000059E2000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/t	kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0/	kcnXZ6yXoo.exe, 00000000.00000003.315020936.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315364448.00000000059F8000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316162313.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315960320.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315865361.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315507955.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316031658.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316082284.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315146785.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315690017.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315428401.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316124895.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315917112.0000000005A04000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.314795179.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315726257.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315644708.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.316214959.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315327758.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comt	kcnXZ6yXoo.exe, 00000000.00000003.317495074.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317720307.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317567364.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317368441.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317304521.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317014695.0000000005A01000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317844075.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317767247.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317955353.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317221145.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317147616.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317053909.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317099709.0000000005A02000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317415466.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.317268864.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	kcnXZ6yXoo.exe, 00000000.00000003.315832173.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	kcnXZ6yXoo.exe, 00000000.00000002.354713070.0000000006BF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals/	kcnXZ6yXoo.exe, 00000000.00000003.318481734.0000000005A03000.00000004.00000020.00020000.00000000.sdmp, kcnXZ6yXoo.exe, 00000000.00000003.318435369.0000000005A03000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.12.253.26	tzitziklishop.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796220
Start date and time:	2023-02-01 18:23:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 28s
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:	20
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:	kcnXZ6yXoo.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@24/12@14/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.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 NtDeviceIoControlFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:24:20	API Interceptor	841x Sleep call for process: kcnXZ6yXoo.exe modified
18:24:26	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\kcnXZ6yXoo.exe" s>$(Arg0)
18:24:28	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
18:24:29	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:24:36	API Interceptor	2x Sleep call for process: dhcpmon.exe modified
18:25:03	API Interceptor	1x Sleep call for process: MpCmdRun.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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	801792
Entropy (8bit):	7.681976997147394
Encrypted:	false
SSDEEP:	24576:yLzyRU5BVftZtPOYkNc9/vgumFRXjVDaqG4yPa:SzyRU/VfbtGpU/vgum7Z7
MD5:	CFFCACECCD0C05762DC335F58A2F0932
SHA1:	45FBB9DDF062F8B64BA3B8ACE48767991517FA50
SHA-256:	BDFC24D604F256170914E2F360D8B6ED30182FE8682FC11AA136DEC7A5FB1876
SHA-512:	D36DE14335FD20C41420E3BFDF69481E3C011F99F4E586E2C91D0B2976F6CB88C9CC63E36F1638D9C647025DF580CAE947E28BB2AEE8206AF4990271941B094
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 26%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....h.c.....0..2.....P... ...`....@.. ..... ..@.....4P..O....`..... ....H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....:.....@..B.....hP.....H.....W...K.....h.....{#...*..{$...*V.(%.....}#....}$...*...0..C.....u.....6..0(&....{#....{#...o'...,.((....{$.... {$...o)...+..+..*. ....)UU.Z(&....{#...o*...X)UU.Z((....{$...o+...X*.0..b.....r...p.....%..{#.....%q.....-.&.+.....o,....%..{$.....%q.....-.&.+.....o,....(-...*&.(%.....*.0..9.....~... .....,".rG..p.....(....o/...s0.....~.....+..*....0.....~.....+..*".....*.0.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.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
Reputation:	unknown

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kcnXZ6yXoo.exe.log

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.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:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp908E.tmp

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.106596988930126
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PLxtn:cbk4oL600QydbQxIYODOLedq3SLj
MD5:	742DC6DB0CE6E76E140A3D4E39B2BA1B
SHA1:	2475B398B66E72F89D6EDEFFAE763F6372D8302E
SHA-256:	54C25E2C914986FC96E3DDFADF625DC44347ACF73C482AB55DE77EF66A9F3548
SHA-512:	7E78EC9672F25D84F9CB02F07798EFBEADD108AFCA22B7062BFCCBCE7C99C5CB9A319B6BFC9643323850980F474A48907A25C70A1B757329443E333DA0FB3EB0
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp9283.tmp

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B

SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3/hwn:Phw
MD5:	E822B6AED0FE7815560B1BC483AB3A36
SHA1:	02CB81F7E45179F377A33BA662D98912C8F2CE2A
SHA-256:	8A059E77296BE8B93CB4C9ADA71F0BF05F7F8522CE66DFBC7DB7550C55F72CDC
SHA-512:	D91B717CF31B0CA96EE66A7B212A4AE8B30FC361569163130C1867CF76E0C163BD979F88A2BDE7D5A71020DCBB60314F830927032C87BD75C71FFFAFBC2A9AAE
Malicious:	**true**
Reputation:	unknown
Preview:	DW.....H

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

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Reputation:	unknown

Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

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

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92 6
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i......~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v."".v.......#..X.a....../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz......(...o......b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O..........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?...........b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i..........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	38
Entropy (8bit):	4.247927513443587
Encrypted:	false
SSDEEP:	3:oNUWJRWOGxANn:oNNJAO+AN
MD5:	BA03B1FDA372E0CEC6CB8137CE0E9F9C
SHA1:	CB6CFCC683ADF187368236200DC03784AF823C2D
SHA-256:	974E48D90CA0A8106A1015DF406414CCF898FB1273048D9C3EFFB170E0EC2080
SHA-512:	0F001690BFB1F2F08AB387FC91E8915B9FEAD54F43042BF4552A739D9E089E62833E3F03792CD5ECD856D38695656884F1E69CC143973AE4C0B61D4145F3D2E(
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\kcnXZ6yXoo.exe

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log

Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	8156
Entropy (8bit):	3.1667968290132404
Encrypted:	false
SSDEEP:	96:cEj+AbCEH+AbuEAc+AbhGEA+AbNEe+Ab/Ee+AbPE6w9+Ab1wTEE+Ab5EA+Ab+:cY+38+DJc+iGr+MZ+65+6tg+ECf+Yb+7
MD5:	69D0BB0FF1440A999D2A62D4E1DDADA2
SHA1:	2C11F6559572A47FB12224B9B2250673B0798542
SHA-256:	A9BEE03B8BA91FC77806EBA39D968711523D9F4B38E56146E1C02F1730256B9A
SHA-512:	E5E4867165319D230C755953FC4D132513A709F6AE53BC085612C9861ED25D88FA15B331BA0F467A58D92B8ECA844E132D0594DE340BED0E2A5A9F68BD26399,
Malicious:	false
Reputation:	unknown
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....-.............-.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.681976997147394
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:	kcnXZ6yXoo.exe
File size:	801792
MD5:	cffcaceccd0c05762dc335f58a2f0932
SHA1:	45fbb9ddf062f8b64ba3b8ace48767991517fa50
SHA256:	bdfc24d604f256170914e2f360d8b6ed30182fe8682fc11aa136dec7a5fb1876
SHA512:	d36de14335fd20c41420e3bfdf69481e3c011f99f4e586e2c91d0b2976f6cb88c9cc63e36f1638d9c647025df580cae947e28bb2aee8206af4990271941b0942
SSDEEP:	24576:yLzyRU5BVftZtPOYkNc9/vgumFRXjVDaqG4yPa:SzyRU/VfbtGpU/vgum7Z7
TLSH:	48058C8777F1A872F6CB10A1142837CD2FE0B103BE55A2579B7B7AC0A7059FB7698241
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....h.c.....0..2.....P... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c5086
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:	0x63DA6893 [Wed Feb 1 13:26:43 2023 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

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
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	0xc5034	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x5c4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc308c	0xc3200	False	0.8482968649903908	data	7.684974410396953	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x5c4	0x600	False	0.4303385416666667	data	4.121702670518778	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc6090	0x334	data		
RT_MANIFEST	0xc63d4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

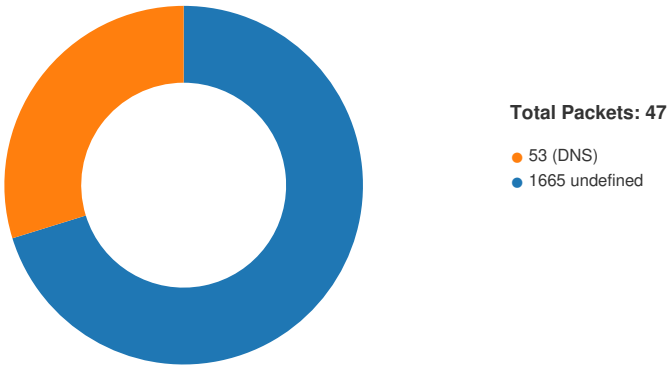
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.545.12.253.264 972516528167660 2/01/23-18:26:06.563289	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49725	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 971916528167660 2/01/23-18:25:38.356322	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 972216528167660 2/01/23-18:25:51.759928	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49722	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 971516528167660 2/01/23-18:25:18.162168	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 972616528167180 2/01/23-18:26:14.335036	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49726	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 970116528167660 2/01/23-18:24:35.085073	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 971616528167180 2/01/23-18:25:24.426541	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49716	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 970316528167660 2/01/23-18:24:53.542008	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 972116528167660 2/01/23-18:25:45.484001	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49721	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 972616528167660 2/01/23-18:26:14.335036	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49726	1665	192.168.2.5	45.12.253.26
45.12.253.26192.168.2.51 665497042810290 2/01/23-18:25:00.449651	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1665	49704	45.12.253.26	192.168.2.5
192.168.2.545.12.253.264 971316528167660 2/01/23-18:25:12.038226	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 971616528167660 2/01/23-18:25:24.426541	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 972316528167660 2/01/23-18:25:58.538683	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	1665	192.168.2.5	45.12.253.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.545.12.253.264 971816652816766 02/01/23-18:25:32.163358	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 970416652816766 02/01/23-18:25:02.005236	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	1665	192.168.2.5	45.12.253.26
192.168.2.545.12.253.264 970216652816766 02/01/23-18:24:42.851032	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	1665	192.168.2.5	45.12.253.26

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 18:24:32.956590891 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:32.983227015 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:32.983406067 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.251296043 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.344775915 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.369502068 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.397341013 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.480207920 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.553070068 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.618894100 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.618937969 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.618963957 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.618989944 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.619014978 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.619076967 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.645889997 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.645936966 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.645963907 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.645992041 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.646007061 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.646023035 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.646051884 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.646059036 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.646083117 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.646112919 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.646117926 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.646148920 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673034906 CET	1665	49701	45.12.253.26	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 18:24:33.673067093 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673086882 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673110962 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673130989 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673145056 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673157930 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673161983 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673171997 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673192978 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673213959 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673214912 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673214912 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673234940 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673242092 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673259020 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673264027 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.673274040 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673289061 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673302889 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673316956 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.673455954 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703617096 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703659058 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703694105 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703716040 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703721046 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703749895 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703761101 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703780890 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703809023 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703824043 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703838110 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703865051 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703891039 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703896046 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703918934 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703931093 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.703947067 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.703974009 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704008102 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704022884 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704060078 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704085112 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704094887 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704106092 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704123020 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704125881 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704148054 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704166889 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704183102 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704185009 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704205990 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704207897 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704227924 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704246998 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704266071 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704271078 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704286098 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704304934 CET	49701	1665	192.168.2.5	45.12.253.26

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 18:24:33.704305887 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704328060 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704340935 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704346895 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704359055 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.704368114 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.704511881 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.705514908 CET	49701	1665	192.168.2.5	45.12.253.26
Feb 1, 2023 18:24:33.731372118 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.731425047 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.731447935 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.731468916 CET	1665	49701	45.12.253.26	192.168.2.5
Feb 1, 2023 18:24:33.731492996 CET	1665	49701	45.12.253.26	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 18:24:32.921785116 CET	61893	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:24:32.938868046 CET	53	61893	8.8.8.8	192.168.2.5
Feb 1, 2023 18:24:42.153881073 CET	60649	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:24:42.174824953 CET	53	60649	8.8.8.8	192.168.2.5
Feb 1, 2023 18:24:51.149646997 CET	51441	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:24:51.167306900 CET	53	51441	8.8.8.8	192.168.2.5
Feb 1, 2023 18:24:59.879889011 CET	49177	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:24:59.899542093 CET	53	49177	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:08.673640966 CET	55039	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:08.691450119 CET	53	55039	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:17.143487930 CET	59220	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:17.161024094 CET	53	59220	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:23.423448086 CET	55068	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:23.442995071 CET	53	55068	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:30.328228951 CET	58532	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:30.348001003 CET	53	58532	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:37.211065054 CET	62659	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:37.230679035 CET	53	62659	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:43.744879007 CET	56263	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:43.764518976 CET	53	56263	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:50.862020969 CET	65513	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:50.881623983 CET	53	65513	8.8.8.8	192.168.2.5
Feb 1, 2023 18:25:56.912189007 CET	56687	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:25:56.931782007 CET	53	56687	8.8.8.8	192.168.2.5
Feb 1, 2023 18:26:04.864137888 CET	52688	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:26:04.883476973 CET	53	52688	8.8.8.8	192.168.2.5
Feb 1, 2023 18:26:13.092663050 CET	61344	53	192.168.2.5	8.8.8.8
Feb 1, 2023 18:26:13.110131979 CET	53	61344	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 1, 2023 18:24:32.921785116 CET	192.168.2.5	8.8.8.8	0xe461	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:42.153881073 CET	192.168.2.5	8.8.8.8	0x6984	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:51.149646997 CET	192.168.2.5	8.8.8.8	0x4d61	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:59.879889011 CET	192.168.2.5	8.8.8.8	0x7513	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:08.673640966 CET	192.168.2.5	8.8.8.8	0x9501	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:17.143487930 CET	192.168.2.5	8.8.8.8	0x62e6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false

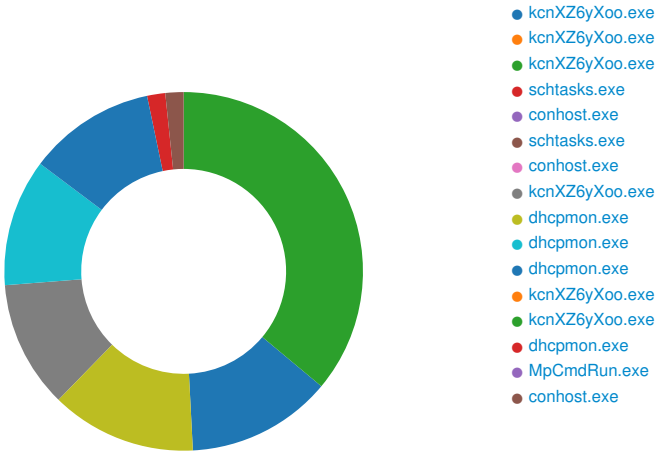
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 18:25:23.423448086 CET	192.168.2.5	8.8.8.8	0x6297	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:30.328228951 CET	192.168.2.5	8.8.8.8	0x6e34	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:37.211065054 CET	192.168.2.5	8.8.8.8	0x607f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:43.744879007 CET	192.168.2.5	8.8.8.8	0x4c0d	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:50.862020969 CET	192.168.2.5	8.8.8.8	0x9fae	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:56.912189007 CET	192.168.2.5	8.8.8.8	0xe12b	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:26:04.864137888 CET	192.168.2.5	8.8.8.8	0xf4e6	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:26:13.092663050 CET	192.168.2.5	8.8.8.8	0x8bd2	Standard query (0)	tzitziklis hop.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 1, 2023 18:24:32.938868046 CET	8.8.8.8	192.168.2.5	0xe461	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:42.174824953 CET	8.8.8.8	192.168.2.5	0x6984	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:51.167306900 CET	8.8.8.8	192.168.2.5	0x4d61	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:24:59.899542093 CET	8.8.8.8	192.168.2.5	0x7513	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:08.691450119 CET	8.8.8.8	192.168.2.5	0x9501	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:17.161024094 CET	8.8.8.8	192.168.2.5	0x62e6	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:23.442995071 CET	8.8.8.8	192.168.2.5	0x6297	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:30.348001003 CET	8.8.8.8	192.168.2.5	0x6e34	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:37.230679035 CET	8.8.8.8	192.168.2.5	0x607f	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:43.764518976 CET	8.8.8.8	192.168.2.5	0x4c0d	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:50.881623983 CET	8.8.8.8	192.168.2.5	0x9fae	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:25:56.931782007 CET	8.8.8.8	192.168.2.5	0xe12b	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:26:04.883476973 CET	8.8.8.8	192.168.2.5	0xf4e6	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 1, 2023 18:26:13.110131979 CET	8.8.8.8	192.168.2.5	0x8bd2	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: kcnXZ6yXoo.exe PID: 5256, Parent PID: 3324

General

Target ID:	0
Start time:	18:24:12
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Imagebase:	0x710000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
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: 00000000.00000002.332268790.0000000003E69000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.332268790.0000000003E69000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.332268790.0000000003E69000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.332268790.0000000003E69000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.328392181.0000000002B80000.00000004.00000800.00020000.00000000.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
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kcnXZ6yXoo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kcnXZ6yXoo.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
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: kcnXZ6yXoo.exe PID: **5764**, Parent PID: **5256**

General

Target ID:	1
Start time:	18:24:21
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Imagebase:	0x20000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: kcnXZ6yXoo.exe PID: **3396**, Parent PID: **5256**

General

Target ID:	2
Start time:	18:24:21
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Imagebase:	0xcc0000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
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: 00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603514529.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004999000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603581661.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603581661.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603581661.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603581661.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.587607897.0000000004CCB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.587607897.0000000004CCB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004CCB000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004BDF000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603254412.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603254412.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603254412.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603254412.0000000007490000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603323053.00000000074A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603323053.00000000074A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603323053.00000000074A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603323053.00000000074A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.587607897.0000000004A86000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.587607897.0000000004A86000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004A86000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.604138192.0000000007A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.604138192.0000000007A10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.604138192.0000000007A10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.604138192.0000000007A10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.602903443.0000000007450000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.602903443.0000000007450000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source:

00000002.00000002.602903443.0000000007450000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.602903443.0000000007450000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.587607897.0000000004C3A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004C3A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.598984140.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.598984140.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.598984140.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.598984140.00000000057E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.599210751.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.599210751.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.599210751.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.599210751.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.599210751.00000000058E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.352344593.0000000001288000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603445677.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603445677.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603445677.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603445677.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.599845120.0000000005B40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.599845120.0000000005B40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.599845120.0000000005B40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.599845120.0000000005B40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603926095.00000000079F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603926095.00000000079F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603926095.00000000079F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603926095.00000000079F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.604219449.0000000007A20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.604219449.0000000007A20000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.604219449.0000000007A20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.604219449.0000000007A20000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.587607897.0000000004B6A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.587607897.0000000004B6A000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004B6A000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.578455701.00000000030B1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.603631836.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.603631836.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.603631836.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.603631836.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.587607897.0000000004B4C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.604565341.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.604565341.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.604565341.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.604565341.0000000007A60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.578455701.000000000311D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.578455701.000000000311D000.00000004.00000800.00020000.00000000.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:\Program Files (x86)\DHCP Monitor	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:\Program Files (x86)\DHCP Monitor\dhcpmon.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:\Program Files (x86)\DHCP Monitor\dhcpmon.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\tmp908E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	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\tmp9283.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	GetTempFileNameW
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
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	71071E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.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\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71071E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp908E.tmp	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp9283.tmp	success or wait	1	71076A95	DeleteFileW
C:\Users\user\Desktop\kcnXZ6yXoo.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	44 57 1b fd fd 04 fd 48	DWH	success or wait	1	71071B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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 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 68 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 32 0c 00 00 08 00 00 00 00 00 00 fd 50 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 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.$PELhc02P `@ @	success or wait	4	7107DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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
C:\Users\user\AppData\Local\Temp\tmp908E.tmp	0	1301	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	38	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 6b 63 6e 58 5a 36 79 58 6f 6f 2e 65 78 65	C:\Users\user\Desktop\kcnXZ6yXoo.exe	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9283.tmp	0	1310	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 0d 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 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	14	71071B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 16 fd fd 20 38 fd 6a fd fd fd fd 7c fd 26 58 fd fd 65 fd 46 fd 2a fd	9iH}Z4f 8j|&XeF*	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
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:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\kcnXZ6yXoo.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Users\user\Desktop\kcnXZ6yXoo.exe	unknown	512	success or wait	1	721ED72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	7107646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **6084**, Parent PID: **3396**

General

Target ID:	3
Start time:	18:24:25
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp908E.tmp
Imagebase:	0xcd0000
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\tmp908E.tmp	unknown	2	success or wait	1	CDAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp908E.tmp	unknown	1302	success or wait	1	CDABD9	ReadFile

Analysis Process: conhost.exe PID: **5768**, Parent PID: **6084**

General

Target ID:	4
Start time:	18:24:25
Start date:	01/02/2023
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: **1092**, Parent PID: **3396**

General

Target ID:	5
Start time:	18:24:25
Start date:	01/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp9283.tmp
Imagebase:	0xcd0000
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\tmp9283.tmp	unknown	2	success or wait	1	CDAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9283.tmp	unknown	1311	success or wait	1	CDABD9	ReadFile

Analysis Process: conhost.exe PID: **1252**, Parent PID: **1092**

General

Target ID:	6
Start time:	18:24:26
Start date:	01/02/2023
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: kcnXZ6yXoo.exe PID: **5800**, Parent PID: **1084**

General

Target ID:	7
Start time:	18:24:27
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe 0
Imagebase:	0xce0000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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 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
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: dhcpmon.exe PID: **5920**, Parent PID: **1084**

General

Target ID:	8
Start time:	18:24:29
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x990000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.376686559.0000000002EB0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, 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\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

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\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.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
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: dhcpmon.exe PID: **5904**, Parent PID: **3324**

General

Target ID:	9
Start time:	18:24:40
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x20000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	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 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
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: dhcpmon.exe PID: **2284**, Parent PID: **5920**

General

Target ID:	10
Start time:	18:24:42
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x730000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
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: 0000000A.00000002.411231497.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.411231497.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.411231497.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.411231497.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.432812642.0000000002AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.432812642.0000000002AE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.432812642.0000000002AE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.434966346.0000000003B2A000.00000004.00000800.00020000.00000000.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

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
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: kcnXZ6yXoo.exe PID: **5872**, Parent PID: **5800**

General

Target ID:	11
Start time:	18:24:43
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Imagebase:	0x2d0000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: kcnXZ6yXoo.exe PID: **2004**, Parent PID: **5800**

General	
Target ID:	12
Start time:	18:24:43
Start date:	01/02/2023
Path:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\kcnXZ6yXoo.exe
Imagebase:	0x5b0000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.435644286.0000000003A6F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.433432436.0000000002A11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.433432436.0000000002A11000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.433432436.0000000002A11000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.435644286.0000000003A84000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.435644286.0000000003A84000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **1364**, Parent PID: **5904**

General	
Target ID:	13
Start time:	18:24:59
Start date:	01/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xb10000
File size:	801792 bytes
MD5 hash:	CFFCACECCD0C05762DC335F58A2F0932
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: MpCmdRun.exe PID: **1092**, Parent PID: **916**

General	
Target ID:	16
Start time:	18:25:02
Start date:	01/02/2023
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff71e280000

File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **3300**, Parent PID: **1092**

General

Target ID:	17
Start time:	18:25:02
Start date:	01/02/2023
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:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly