ID: 412751
Sample Name:
03_extracted.exe
Cookbook: default.jbs
Time: 22:39:18
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

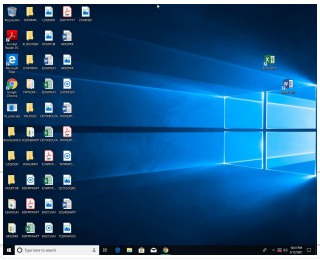
Analysis Report 03_extracted.exe

Overview

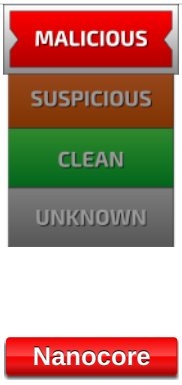
General Information

Sample Name:	03_extracted.exe
Analysis ID:	412751
MD5:	43c4f163196ff02…
SHA1:	f826b410b31cb25.
SHA256:	a585841f956f179..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

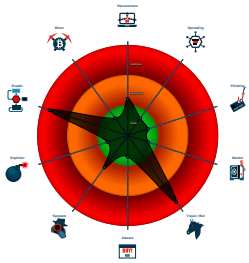


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- 03_extracted.exe (PID: 5976 cmdline: 'C:\Users\user\Desktop\03_extracted.exe' MD5: 43C4F163196FF02E7AA8C5040375FDA4)
  - schtasks.exe (PID: 4652 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LiydYED' /XML 'C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 03_extracted.exe (PID: 5548 cmdline: {path} MD5: 43C4F163196FF02E7AA8C5040375FDA4)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c687c38e-2b2d-4d96-b5eb-9a31ccba",
  "Group": "Sys",
  "Domain1": "sys2021.linkpc.net",
  "Domain2": "",
  "Port": 11940,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.489322816.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000002.489322816.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.489322816.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000006.00000002.496381211.0000000003DE7000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.496381211.0000000003DE7000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x33e5:$a: NanoCore • 0x343e:$a: NanoCore • 0x347b:$a: NanoCore • 0x34f4:$a: NanoCore • 0x16b9f:$a: NanoCore • 0x16bb4:$a: NanoCore • 0x16be9:$a: NanoCore • 0x2f663:$a: NanoCore • 0x2f678:$a: NanoCore • 0x2f6ad:$a: NanoCore • 0x3447:$b: ClientPlugin • 0x3484:$b: ClientPlugin • 0x3d82:$b: ClientPlugin • 0x3d8f:$b: ClientPlugin • 0x1695b:$b: ClientPlugin • 0x16976:$b: ClientPlugin • 0x169a6:$b: ClientPlugin • 0x16bbd:$b: ClientPlugin • 0x16bf2:$b: ClientPlugin • 0x2f41f:$b: ClientPlugin • 0x2f43a:$b: ClientPlugin
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.03_extracted.exe.3dee43c.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28271:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x2829e:$x2: IClientNetworkHost
6.2.03_extracted.exe.3dee43c.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28271:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2934c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x2828b:$s5: IClientLoggingHost
6.2.03_extracted.exe.3dee43c.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.2.03_extracted.exe.5654629.11.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
6.2.03_extracted.exe.5654629.11.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
Click to see the 37 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

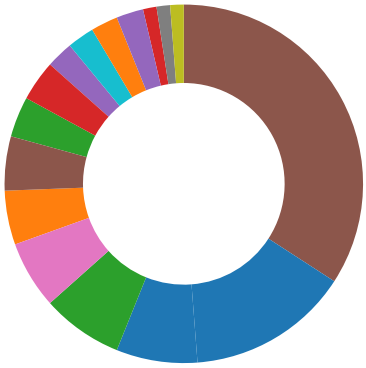
Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance



- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

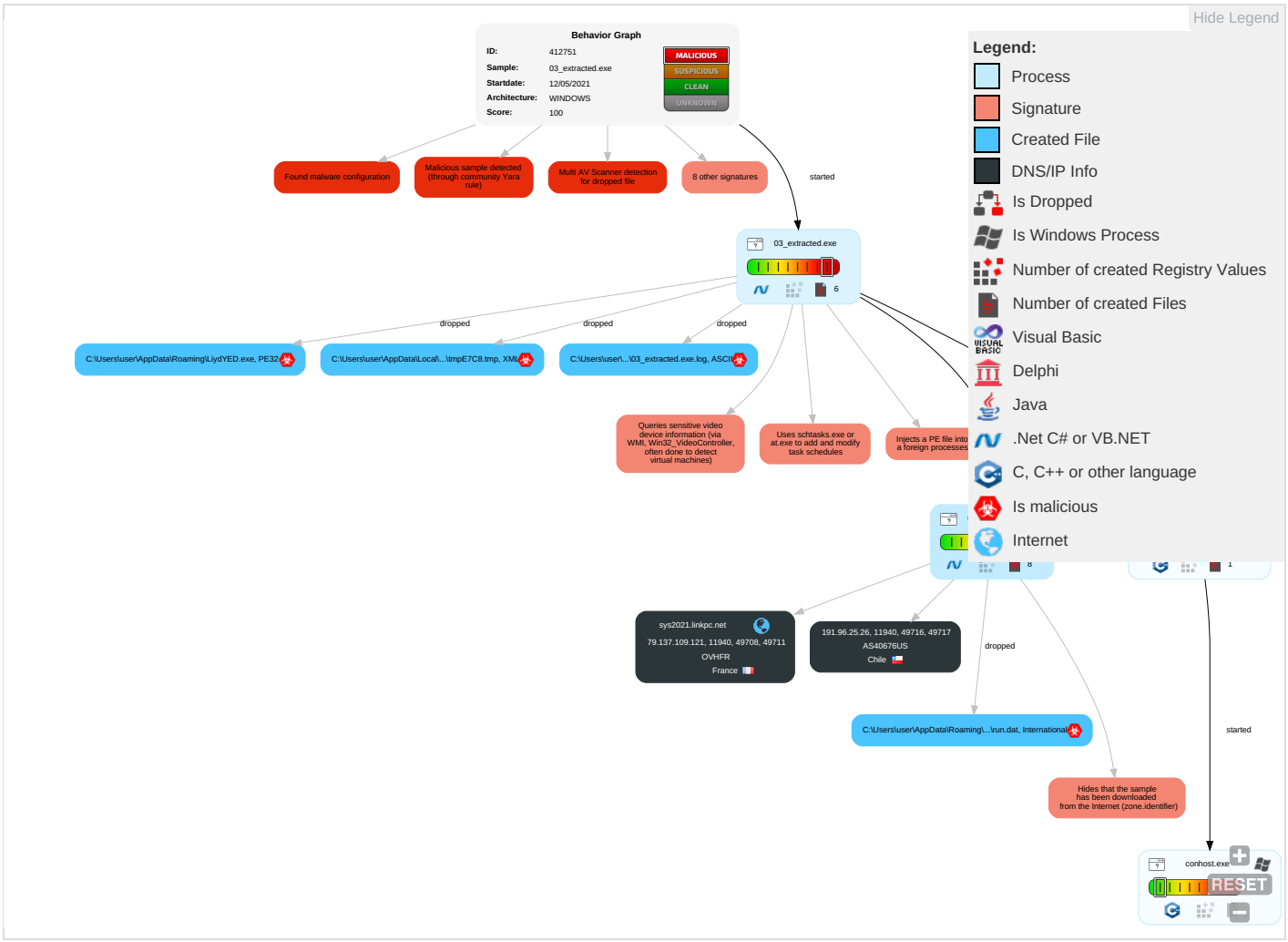
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co and
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non Por
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rer Sof
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	App Lay Pro
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

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
03_extracted.exe	41%	Virustotal		Browse
03_extracted.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LiydYED.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.03_extracted.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.03_extracted.exe.5650000.12.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krense	0%	Avira URL Cloud	safe	
http://www.tiro.com.	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e$	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sajatypeworks.comhe	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cng	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cne	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.com-d	0%	Avira URL Cloud	safe	
http://www.fonts.comlo	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ita	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/-	0%	Avira URL Cloud	safe	
http://www.fonts.com0	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnk-s	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cn#	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sys2021.linkpc.net	79.137.109.121	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
sys2021.linkpc.net	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-e	03_extracted.exe, 00000000.00003.226058625.0000000005AA4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.krense	03_extracted.exe, 00000000.00003.224075054.0000000005AA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com.	03_extracted.exe, 00000000.00003.223493292.0000000005ABB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	03_extracted.exe, 00000000.00002.254230229.0000000005B90000.00000002.00000001.sdmp, 03_extracted.exe, 00000000.00000003.223530764.0000000005ABB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp, 03_extracted.exe, 00000000.00000003.228394931.0000000005AAD000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	03_extracted.exe, 00000000.00000003.223195518.0000000005ABB000.00000004.00000001.sdmp, 03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgrita	03_extracted.exe, 00000000.00000002.254191981.0000000005AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-e$	03_extracted.exe, 00000000.00000003.226058625.0000000005AA400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comhe	03_extracted.exe, 00000000.00000003.223195518.0000000005ABB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	03_extracted.exe, 00000000.00000003.223324934.0000000005ABB000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cng	03_extracted.exe, 00000000.00000003.224439658.0000000005ADD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cne	03_extracted.exe, 00000000.00000003.224684993.0000000005AA400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnLog	03_extracted.exe, 00000000.00000003.224684993.0000000005AA400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krt	03_extracted.exe, 00000000.00000003.224075054.0000000005AA600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	03_extracted.exe, 00000000.00000003.226058625.0000000005AA400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com-d	03_extracted.exe, 00000000.00000003.223195518.0000000005ABB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comlo	03_extracted.exe, 00000000.00000003.223286632.0000000005ABB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/;	03_extracted.exe, 00000000.00000003.226058625.0000000005AA4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	03_extracted.exe, 00000000.00000003.225848525.0000000005AAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	03_extracted.exe, 00000000.00000003.226058625.0000000005AA4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comt	03_extracted.exe, 00000000.00000002.254191981.0000000005AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ita	03_extracted.exe, 00000000.00000003.226058625.0000000005AA4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	03_extracted.exe, 00000000.00000002.254191981.0000000005AA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/-	03_extracted.exe, 00000000.00000003.226058625.0000000005AA4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	03_extracted.exe, 00000000.00000002.254230229.0000000005B90000.00000002.00000001.sdmp	false		high
http://www.fonts.com0	03_extracted.exe, 00000000.00000003.223303861.0000000005ABB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnk-s	03_extracted.exe, 00000000.00000003.224439658.0000000005ADD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comc	03_extracted.exe, 00000000.00000003.223512202.0000000005ABB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn#	03_extracted.exe, 00000000.00000003.224453104.0000000005AA4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers4	03_extracted.exe, 00000000.00000003.228394931.0000000005AAD000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.96.25.26	unknown	Chile		40676	AS40676US	false
79.137.109.121	sys2021.linkpc.net	France		16276	OVHFR	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412751
Start date:	12.05.2021
Start time:	22:39:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	03_extracted.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/4@9/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.64.90.137, 20.82.209.183, 93.184.220.29, 184.30.21.144, 104.43.193.48, 23.57.80.111, 20.49.157.6, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.143.16, 20.54.26.129, 20.50.102.62 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, iris-de-ppe-azsc-uks.uksouth.cloudapp.azure.com • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:40:14	API Interceptor	945x Sleep call for process: 03_extracted.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
191.96.25.26	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Spec_PDF.vbs	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SpecPDF.vbs	Get hash	malicious	Browse	
79.137.109.121	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	
	Transcation03232016646pdf.exe	Get hash	malicious	Browse	
	NEW SC #ORDER.exe	Get hash	malicious	Browse	
	NEW SC #ORDER.exe	Get hash	malicious	Browse	
	NEW SC.exe	Get hash	malicious	Browse	
	NEW SC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sys2021.linkpc.net	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 87.98.245.48
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 79.137.109.121
	Spec_PDF.vbs	Get hash	malicious	Browse	• 105.112.11.245
	SpecPDF.vbs	Get hash	malicious	Browse	• 179.43.166.32

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	0987654332.exe	Get hash	malicious	Browse	• 107.160.232.135
	POI09876OIUY.exe	Get hash	malicious	Browse	• 107.160.232.135
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• 107.160.234.116
	f41e9f9d_by_Libranalysis.exe	Get hash	malicious	Browse	• 107.160.177.197
	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	2f50000.exe	Get hash	malicious	Browse	• 38.39.192.78
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 104.217.141.249
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 107.160.232.135
	Spec_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	8CgG2kY3Ow.dll	Get hash	malicious	Browse	• 45.61.138.153
	DHL_S390201.exe	Get hash	malicious	Browse	• 45.34.249.30
	978463537_BL FOR APPROVAL.doc	Get hash	malicious	Browse	• 45.34.114.71
	SpecPDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	7mB68AZqJs.exe	Get hash	malicious	Browse	• 104.217.143.44
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 172.107.55.6
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 172.107.55.6
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 107.160.118.15
OVHFR	hLrFhmoMMg.exe	Get hash	malicious	Browse	• 51.195.61.169
	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 51.222.80.112
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	Copy-384955799-05102021.xlsm	Get hash	malicious	Browse	• 167.114.48.59
	DHL_Shipment11052021pdf.exe	Get hash	malicious	Browse	• 51.210.201.99
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 217.182.77.10
	INV74321.exe	Get hash	malicious	Browse	• 87.98.148.38
	aa04cdcc_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.105.217.100
	correct invoice.exe	Get hash	malicious	Browse	• 213.186.33.5
	Kb0p7FYmN0yNdzP.exe	Get hash	malicious	Browse	• 66.70.204.222
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 193.70.33.51
	guluh4pYFQybxL8.exe	Get hash	malicious	Browse	• 66.70.204.222
	qA9D8QVC4LrzlPR.exe	Get hash	malicious	Browse	• 66.70.204.222
	OLy4KI85kB3HENF.exe	Get hash	malicious	Browse	• 66.70.204.222
	generated purchase order 6149057.xlsm	Get hash	malicious	Browse	• 158.69.48.225
	scan of document 5336227.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	67w7Ez6lvb.exe	Get hash	malicious	Browse	• 91.121.251.178
	generated check 8460.xlsm	Get hash	malicious	Browse	• 145.239.93.251
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 193.70.33.51

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\LiydYED.exe	Invoice No F1019855_PDF.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\03_extracted.exe.log

Process:	C:\Users\user\Desktop\03_extracted.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192E 48
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp

Process:	C:\Users\user\Desktop\03_extracted.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.168034599644377
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBhtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3d
MD5:	774DF64BD8637D20678EC5B636C078F6
SHA1:	027CD9FEB42E61AF4A6A7E4C13F7835CC9FAB454
SHA-256:	5B86A79F159C9724A9AC8BCE9E68D56FB54092931B5656B626D19AAE1D68929B
SHA-512:	87EF5A78C8A50A3D98F72B229E5B4C6FA23198E572C03723345FB7CCE7001753D073085D8A3F09E2196F610EA4606FE4378262F97A7BC8358BE04B4D78194DC7
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014- 10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

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

Process:	C:\Users\user\Desktop\03_extracted.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:gw8n:gj
MD5:	D24B6D1F3C25FABB06DAD0E517C8684F

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA1:	A8BA98E9F68D2563C94CBAE5D26B7C4DFE5AD3F2
SHA-256:	BB554C96F80D4024210AA29BABC04017C642382793EAE8992541466E7A9ECDAF
SHA-512:	E8FE15EDABC35C61D88243C39FF0C174D0BA0AC065A0908270D31672B208046C181BEC769654614D40635625CCFE7D659997E4B6651795AC4189BB46B42BEE9
Malicious:	**true**
Reputation:	low
Preview:	.e....H

C:\Users\user\AppData\Roaming\LiydYED.exe	
Process:	C:\Users\user\Desktop\03_extracted.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	784896
Entropy (8bit):	7.328703413450174
Encrypted:	false
SSDEEP:	12288:OoLLoS60/K7yh036vCww4Scd3IGj483ESuvkuDKsjLtZTMfLodiMW2G:OoLA3AScdYKSvkItxeUdinh
MD5:	43C4F163196FF02E7AA8C5040375FDA4
SHA1:	F826B410B31CB251DD85F3663735B2F410906517
SHA-256:	A585841F956F17925242996A98836B0D08767DDB179B4B41FD18A5DE719C531C
SHA-512:	264FB4514257080068CEC2915BE6F81EA759812F059B9B969B2F40EE6E502497F22F66C0EFE9B2F5736D6C61F1C7967E9F801B1DF33D100261D4A1B560DDEF7E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Joe Sandbox View:	• Filename: Invoice No F1019855_PDF.vbs, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0.....:.... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text...@.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....e..,~.....v...$....).....0.....r...p.+..*..0.....r...p.+..*".(.....*.0..C.....(L...&.....(....h}.....(...h }.....(!... .....(V...&*>...("...(.....*..0..C.....(L...&.....(....h}.....(...h}.....(!... .....(V...&*>...("...(.....*..0..2.....(#.....($.....,...(!.....(%....(&...(.....*>...("...(.....*...0..... .....b`.+..*...(!... .....(....h..(...h(....(Q...&*..0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.328703413450174
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	03_extracted.exe
File size:	784896
MD5:	43c4f163196ff02e7aa8c5040375fda4
SHA1:	f826b410b31cb251dd85f3663735b2f410906517
SHA256:	a585841f956f17925242996a98836b0d08767ddb179b4b41fd18a5de719c531c
SHA512:	264fb4514257080068cec2915be6f81ea759812f059b9b969b2f40ee6e502497f22f66c0efe9b2f5736d6c61f1c7967e9f801b1df33d100261d4a1b560ddef7e
SSDEEP:	12288:OoLLoS60/K7yh036vCww4Scd3IGj483ESuvkuDKsjLtZTMfLodiMW2G:OoLA3AScdYKSvkItxeUdinh
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....c.....0.....:.... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c0e3a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xE963C9E9 [Fri Jan 29 19:18:01 2094 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc0de8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc2000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc0dcc	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbee40	0xbf000	False	0.734753354058	data	7.33039162712	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x5b4	0x600	False	0.422526041667	data	4.1233888382	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc2090	0x324	data		
RT_MANIFEST	0xc23c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

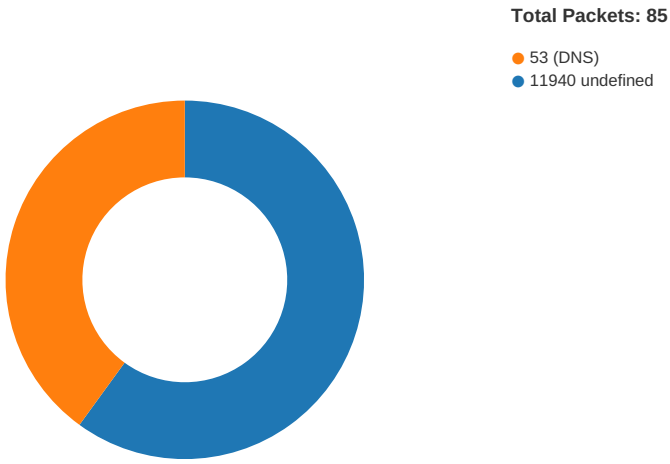
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	MXvDG34.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Handle Leaker
ProductVersion	1.0.0.0
FileDescription	Handle Leaker
OriginalFilename	MXvDG34.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:40:20.181857109 CEST	49708	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:20.394779921 CEST	11940	49708	79.137.109.121	192.168.2.5
May 12, 2021 22:40:20.950453043 CEST	49708	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:21.189028025 CEST	11940	49708	79.137.109.121	192.168.2.5
May 12, 2021 22:40:21.841078997 CEST	49708	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:22.051414013 CEST	11940	49708	79.137.109.121	192.168.2.5
May 12, 2021 22:40:26.391540051 CEST	49711	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:26.647887945 CEST	11940	49711	79.137.109.121	192.168.2.5
May 12, 2021 22:40:27.153624058 CEST	49711	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:27.435940027 CEST	11940	49711	79.137.109.121	192.168.2.5
May 12, 2021 22:40:27.950536013 CEST	49711	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:28.265122890 CEST	11940	49711	79.137.109.121	192.168.2.5
May 12, 2021 22:40:32.368869066 CEST	49713	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:32.684233904 CEST	11940	49713	79.137.109.121	192.168.2.5
May 12, 2021 22:40:33.275163889 CEST	49713	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:33.567784071 CEST	11940	49713	79.137.109.121	192.168.2.5
May 12, 2021 22:40:34.169770002 CEST	49713	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:34.445559025 CEST	11940	49713	79.137.109.121	192.168.2.5
May 12, 2021 22:40:38.557212114 CEST	49716	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:38.746800900 CEST	11940	49716	191.96.25.26	192.168.2.5
May 12, 2021 22:40:39.342087984 CEST	49716	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:39.532274008 CEST	11940	49716	191.96.25.26	192.168.2.5
May 12, 2021 22:40:40.045340061 CEST	49716	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:40.235362053 CEST	11940	49716	191.96.25.26	192.168.2.5
May 12, 2021 22:40:44.265254021 CEST	49717	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:44.454807997 CEST	11940	49717	191.96.25.26	192.168.2.5
May 12, 2021 22:40:45.155085087 CEST	49717	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:45.344358921 CEST	11940	49717	191.96.25.26	192.168.2.5
May 12, 2021 22:40:45.952081919 CEST	49717	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:46.143121004 CEST	11940	49717	191.96.25.26	192.168.2.5
May 12, 2021 22:40:50.316963911 CEST	49718	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:50.506433010 CEST	11940	49718	191.96.25.26	192.168.2.5
May 12, 2021 22:40:51.155723095 CEST	49718	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:51.345418930 CEST	11940	49718	191.96.25.26	192.168.2.5
May 12, 2021 22:40:51.952533960 CEST	49718	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:40:52.142770052 CEST	11940	49718	191.96.25.26	192.168.2.5
May 12, 2021 22:40:56.248692036 CEST	49721	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:56.577107906 CEST	11940	49721	79.137.109.121	192.168.2.5
May 12, 2021 22:40:57.172049999 CEST	49721	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:57.421186924 CEST	11940	49721	79.137.109.121	192.168.2.5
May 12, 2021 22:40:57.984330893 CEST	49721	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:40:58.203782082 CEST	11940	49721	79.137.109.121	192.168.2.5
May 12, 2021 22:41:02.311530113 CEST	49722	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:02.654825926 CEST	11940	49722	79.137.109.121	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:41:03.156591892 CEST	49722	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:03.392868042 CEST	11940	49722	79.137.109.121	192.168.2.5
May 12, 2021 22:41:03.906749010 CEST	49722	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:04.130737066 CEST	11940	49722	79.137.109.121	192.168.2.5
May 12, 2021 22:41:08.254611969 CEST	49724	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:08.598133087 CEST	11940	49724	79.137.109.121	192.168.2.5
May 12, 2021 22:41:09.110224962 CEST	49724	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:09.371365070 CEST	11940	49724	79.137.109.121	192.168.2.5
May 12, 2021 22:41:09.876256943 CEST	49724	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:10.128433943 CEST	11940	49724	79.137.109.121	192.168.2.5
May 12, 2021 22:41:14.143450975 CEST	49727	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:14.332782984 CEST	11940	49727	191.96.25.26	192.168.2.5
May 12, 2021 22:41:14.845030069 CEST	49727	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:15.034599066 CEST	11940	49727	191.96.25.26	192.168.2.5
May 12, 2021 22:41:15.548228979 CEST	49727	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:15.738030910 CEST	11940	49727	191.96.25.26	192.168.2.5
May 12, 2021 22:41:19.753288984 CEST	49733	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:19.942635059 CEST	11940	49733	191.96.25.26	192.168.2.5
May 12, 2021 22:41:20.454910994 CEST	49733	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:20.644310951 CEST	11940	49733	191.96.25.26	192.168.2.5
May 12, 2021 22:41:21.158118963 CEST	49733	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:21.348942995 CEST	11940	49733	191.96.25.26	192.168.2.5
May 12, 2021 22:41:25.364053965 CEST	49734	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:25.555480003 CEST	11940	49734	191.96.25.26	192.168.2.5
May 12, 2021 22:41:26.064924955 CEST	49734	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:26.254933119 CEST	11940	49734	191.96.25.26	192.168.2.5
May 12, 2021 22:41:26.768134117 CEST	49734	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:41:26.958157063 CEST	11940	49734	191.96.25.26	192.168.2.5
May 12, 2021 22:41:32.345263004 CEST	49735	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:32.657366991 CEST	11940	49735	79.137.109.121	192.168.2.5
May 12, 2021 22:41:33.159749031 CEST	49735	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:39.159621954 CEST	49735	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:49.543638945 CEST	49737	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:49.747009993 CEST	11940	49737	79.137.109.121	192.168.2.5
May 12, 2021 22:41:50.254332066 CEST	49737	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:50.544728994 CEST	11940	49737	79.137.109.121	192.168.2.5
May 12, 2021 22:41:51.051290989 CEST	49737	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:51.286560059 CEST	11940	49737	79.137.109.121	192.168.2.5
May 12, 2021 22:41:55.388365984 CEST	49739	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:55.648849964 CEST	11940	49739	79.137.109.121	192.168.2.5
May 12, 2021 22:41:56.162950993 CEST	49739	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:56.385699034 CEST	11940	49739	79.137.109.121	192.168.2.5
May 12, 2021 22:41:56.895621061 CEST	49739	11940	192.168.2.5	79.137.109.121
May 12, 2021 22:41:57.121793985 CEST	11940	49739	79.137.109.121	192.168.2.5
May 12, 2021 22:42:01.133452892 CEST	49740	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:01.322891951 CEST	11940	49740	191.96.25.26	192.168.2.5
May 12, 2021 22:42:01.833502054 CEST	49740	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:02.022944927 CEST	11940	49740	191.96.25.26	192.168.2.5
May 12, 2021 22:42:02.536616087 CEST	49740	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:02.726476908 CEST	11940	49740	191.96.25.26	192.168.2.5
May 12, 2021 22:42:06.742265940 CEST	49741	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:06.935261965 CEST	11940	49741	191.96.25.26	192.168.2.5
May 12, 2021 22:42:07.443434954 CEST	49741	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:07.636456013 CEST	11940	49741	191.96.25.26	192.168.2.5
May 12, 2021 22:42:08.146445036 CEST	49741	11940	192.168.2.5	191.96.25.26
May 12, 2021 22:42:08.339524031 CEST	11940	49741	191.96.25.26	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:39:59.130805016 CEST	54302	53	192.168.2.5	8.8.8.8
May 12, 2021 22:39:59.170433998 CEST	53784	53	192.168.2.5	8.8.8.8
May 12, 2021 22:39:59.195631027 CEST	65307	53	192.168.2.5	8.8.8.8
May 12, 2021 22:39:59.198559999 CEST	53	54302	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 22:39:59.219163895 CEST	53	53784	8.8.8.8	192.168.2.5
May 12, 2021 22:39:59.253983021 CEST	53	65307	8.8.8.8	192.168.2.5
May 12, 2021 22:39:59.303869009 CEST	64344	53	192.168.2.5	8.8.8.8
May 12, 2021 22:39:59.355463982 CEST	53	64344	8.8.8.8	192.168.2.5
May 12, 2021 22:39:59.490895987 CEST	62060	53	192.168.2.5	8.8.8.8
May 12, 2021 22:39:59.549663067 CEST	53	62060	8.8.8.8	192.168.2.5
May 12, 2021 22:40:00.382235050 CEST	61805	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:00.430938005 CEST	53	61805	8.8.8.8	192.168.2.5
May 12, 2021 22:40:01.343189955 CEST	54795	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:01.402440071 CEST	53	54795	8.8.8.8	192.168.2.5
May 12, 2021 22:40:01.485665083 CEST	49557	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:01.534554005 CEST	53	49557	8.8.8.8	192.168.2.5
May 12, 2021 22:40:02.369940042 CEST	61733	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:02.418869972 CEST	53	61733	8.8.8.8	192.168.2.5
May 12, 2021 22:40:03.499629974 CEST	65447	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:03.548351049 CEST	53	65447	8.8.8.8	192.168.2.5
May 12, 2021 22:40:04.678842068 CEST	52441	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:04.737075090 CEST	53	52441	8.8.8.8	192.168.2.5
May 12, 2021 22:40:05.802606106 CEST	62176	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:05.851377010 CEST	53	62176	8.8.8.8	192.168.2.5
May 12, 2021 22:40:06.729510069 CEST	59596	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:06.778430939 CEST	53	59596	8.8.8.8	192.168.2.5
May 12, 2021 22:40:07.734236956 CEST	65296	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:07.786509037 CEST	53	65296	8.8.8.8	192.168.2.5
May 12, 2021 22:40:08.685148954 CEST	63183	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:08.735106945 CEST	53	63183	8.8.8.8	192.168.2.5
May 12, 2021 22:40:09.624185085 CEST	60151	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:09.675853968 CEST	53	60151	8.8.8.8	192.168.2.5
May 12, 2021 22:40:19.997391939 CEST	56969	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:20.157730103 CEST	53	56969	8.8.8.8	192.168.2.5
May 12, 2021 22:40:26.209935904 CEST	55161	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:26.390404940 CEST	53	55161	8.8.8.8	192.168.2.5
May 12, 2021 22:40:27.417108059 CEST	54757	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:27.476603031 CEST	53	54757	8.8.8.8	192.168.2.5
May 12, 2021 22:40:32.305219889 CEST	49992	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:32.367516041 CEST	53	49992	8.8.8.8	192.168.2.5
May 12, 2021 22:40:37.018873930 CEST	60075	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:37.093877077 CEST	53	60075	8.8.8.8	192.168.2.5
May 12, 2021 22:40:51.300076962 CEST	55016	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:51.362493038 CEST	53	55016	8.8.8.8	192.168.2.5
May 12, 2021 22:40:54.686959028 CEST	64345	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:54.748883963 CEST	53	64345	8.8.8.8	192.168.2.5
May 12, 2021 22:40:56.189538002 CEST	57128	53	192.168.2.5	8.8.8.8
May 12, 2021 22:40:56.247328043 CEST	53	57128	8.8.8.8	192.168.2.5
May 12, 2021 22:41:02.251971960 CEST	54791	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:02.310091972 CEST	53	54791	8.8.8.8	192.168.2.5
May 12, 2021 22:41:03.510574102 CEST	50463	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:03.661768913 CEST	53	50463	8.8.8.8	192.168.2.5
May 12, 2021 22:41:08.195278883 CEST	50394	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:08.252734900 CEST	53	50394	8.8.8.8	192.168.2.5
May 12, 2021 22:41:12.564413071 CEST	58530	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:12.630131960 CEST	53	58530	8.8.8.8	192.168.2.5
May 12, 2021 22:41:15.441653013 CEST	53813	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:15.506529093 CEST	53	53813	8.8.8.8	192.168.2.5
May 12, 2021 22:41:32.280656099 CEST	63732	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:32.342036963 CEST	53	63732	8.8.8.8	192.168.2.5
May 12, 2021 22:41:48.390013933 CEST	57344	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:48.462822914 CEST	53	57344	8.8.8.8	192.168.2.5
May 12, 2021 22:41:49.484816074 CEST	54450	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:49.542527914 CEST	53	54450	8.8.8.8	192.168.2.5
May 12, 2021 22:41:50.027245045 CEST	59261	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:50.084286928 CEST	53	59261	8.8.8.8	192.168.2.5
May 12, 2021 22:41:55.326957941 CEST	57151	53	192.168.2.5	8.8.8.8
May 12, 2021 22:41:55.386250973 CEST	53	57151	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 22:40:19.997391939 CEST	192.168.2.5	8.8.8.8	0xe9bc	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:40:26.209935904 CEST	192.168.2.5	8.8.8.8	0x79c1	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:40:32.305219889 CEST	192.168.2.5	8.8.8.8	0x641c	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:40:56.189538002 CEST	192.168.2.5	8.8.8.8	0x6c41	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:41:02.251971960 CEST	192.168.2.5	8.8.8.8	0x3616	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:41:08.195278883 CEST	192.168.2.5	8.8.8.8	0x91c	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:41:32.280656099 CEST	192.168.2.5	8.8.8.8	0x4edd	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:41:49.484816074 CEST	192.168.2.5	8.8.8.8	0x6b4a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 12, 2021 22:41:55.326957941 CEST	192.168.2.5	8.8.8.8	0x6736	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

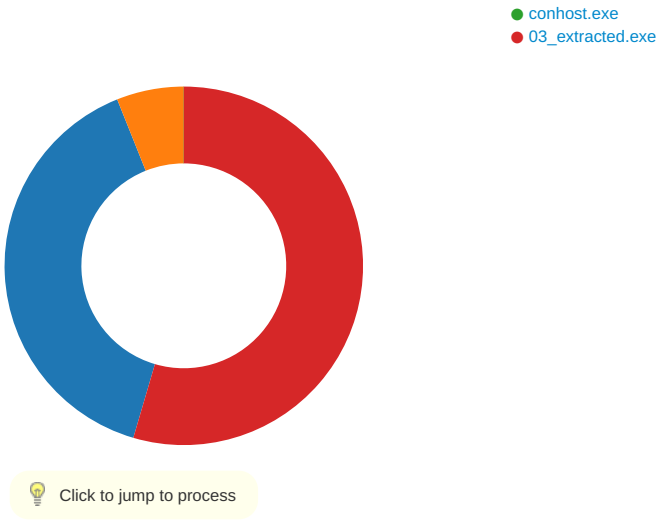
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 22:40:20.157730103 CEST	8.8.8.8	192.168.2.5	0xe9bc	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:40:26.390404940 CEST	8.8.8.8	192.168.2.5	0x79c1	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:40:32.367516041 CEST	8.8.8.8	192.168.2.5	0x641c	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:40:56.247328043 CEST	8.8.8.8	192.168.2.5	0x6c41	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:41:02.310091972 CEST	8.8.8.8	192.168.2.5	0x3616	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:41:08.252734900 CEST	8.8.8.8	192.168.2.5	0x91c	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:41:32.342036963 CEST	8.8.8.8	192.168.2.5	0x4edd	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:41:49.542527914 CEST	8.8.8.8	192.168.2.5	0x6b4a	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 12, 2021 22:41:55.386250973 CEST	8.8.8.8	192.168.2.5	0x6736	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● 03_extracted.exe
● schtasks.exe



System Behavior

Analysis Process: 03_extracted.exe PID: 5976 Parent PID: 5744

General

Start time:	22:40:06
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\03_extracted.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\03_extracted.exe'
Imagebase:	0xfb0000
File size:	784896 bytes
MD5 hash:	43C4F163196FF02E7AA8C5040375FDA4
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: 00000000.00000002.252199912.00000000048E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.252199912.00000000048E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.252199912.00000000048E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LiydYED.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	77A16AB	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	721B9869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\03_extracted.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp	success or wait	1	77A2322	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LiydYED.exe	unknown	784896	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 e9 c9 63 e9 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 f0 0b 00 00 08 00 00 00 00 00 00 3a 0e 0c 00 00 20 00 00 00 20 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 60 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L.....c........... ....0.............:.... ... .@.. ....` ....@................	success or wait	1	77A1933	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp	unknown	1644	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 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	77A1933	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\03_extracted.exe.log	unknown	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\03_extracted.exe	unknown	784896	success or wait	1	77A1933	ReadFile

Analysis Process: schtasks.exe PID: 4652 Parent PID: 5976

General

Start time:	22:40:16
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LiydYED' /XML 'C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp'
Imagebase:	0xbc0000
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\tmpE7C8.tmp	unknown	2	success or wait	1	BCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE7C8.tmp	unknown	1645	success or wait	1	BCABD9	ReadFile

Analysis Process: conhost.exe PID: 5476 Parent PID: 4652

General

Start time:	22:40:16
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 03_extracted.exe PID: 5548 Parent PID: 5976

General

Start time:	22:40:17
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\03_extracted.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x680000
File size:	784896 bytes
MD5 hash:	43C4F163196FF02E7AA8C5040375FDA4

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: 00000006.00000002.489322816.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.489322816.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.489322816.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.496381211.0000000003DE7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.496381211.0000000003DE7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.497217215.0000000005290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.497217215.0000000005290000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.497557539.0000000005650000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.497557539.0000000005650000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.497557539.0000000005650000.00000004.00000001.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	72B860AC	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	72B860AC	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	50407A1	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	504089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	50407A1	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	50407A1	CreateDirectoryW
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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72B860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\03_extracted.exe:Zone.Identifier	success or wait	1	5040B41	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	a0 65 ee 97 d1 15 d9 48	.e.....H	success or wait	1	5040A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\03_extracted.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\03_extracted.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5040A53	ReadFile

Disassembly

Code Analysis