ID: 679394
Sample Name:
IEmxqChwE0.exe
Cookbook: default.jbs
Time: 17:41:11
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

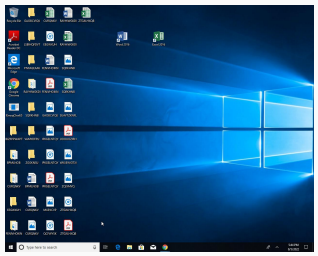
Windows Analysis Report

IEmxqChwE0.exe

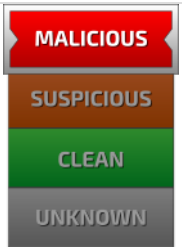
Overview

General Information

Sample Name:	IEmxqChwE0.exe
Analysis ID:	679394
MD5:	0d32ff3680a716f..
SHA1:	2aa356f14a156b..
SHA256:	21719369d4b147.
Tags:	DCRat exe
Infos:	



Detection



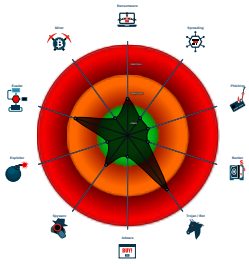
DCRat

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…
- Snort IDS alert for network traffic
- Yara detected DCRat
- Drops executable to a common third…
- Creates processes via WMI
- Machine Learning detection for sam…
- Machine Learning detection for drop…
- Uses schtasks.exe or at.exe to add…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- IEmxqChwE0.exe (PID: 6036 cmdline: "C:\Users\user\Desktop\IEmxqChwE0.exe" MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 640 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 5 /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5244 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 3564 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 14 /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- ZoFSCoTkutoORrrfFQrZkaw.exe (PID: 2988 cmdline: C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 740 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 11 /tr "'C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- ZoFSCoTkutoORrrfFQrZkaw.exe (PID: 5548 cmdline: C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 1428 cmdline: schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2320 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 9 /tr "'C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 1588 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 9 /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5560 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5912 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 9 /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- RuntimeBroker.exe (PID: 1048 cmdline: C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- RuntimeBroker.exe (PID: 4532 cmdline: C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 6060 cmdline: schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 6 /tr "'C:\Recovery\ShellExperienceHost.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5500 cmdline: schtasks.exe /create /tn "ShellExperienceHost" /sc ONLOGON /tr "'C:\Recovery\ShellExperienceHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5948 cmdline: schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 7 /tr "'C:\Recovery\ShellExperienceHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 2208 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 11 /tr "'C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- ShellExperienceHost.exe (PID: 3764 cmdline: C:\Recovery\ShellExperienceHost.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 3568 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- ShellExperienceHost.exe (PID: 336 cmdline: C:\Recovery\ShellExperienceHost.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 4924 cmdline: schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 13 /tr "'C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5804 cmdline: schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /f MD5:

838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5176 cmdline: schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- WmiPrvSE.exe (PID: 408 cmdline: C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 1752 cmdline: schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 7 /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 4736 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 12 /tr "'C:\Recovery\RuntimeBroker.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 5300 cmdline: schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\Recovery\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 1332 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 13 /tr "'C:\Recovery\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- WmiPrvSE.exe (PID: 1448 cmdline: C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe MD5: 0D32FF3680A716FD66CB9AB0E3EBC763)
- schtasks.exe (PID: 2916 cmdline: schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 13 /tr "'C:\MSOCache\All Users\RuntimeBroker.exe'" /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 3256 cmdline: schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\MSOCache\All Users\RuntimeBroker.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- **cleanup**

Malware Configuration

Threatname: DCRat


```
{
  "SCRT": "{|"W|":|"-|",|"j|":|"%|",|"i|":|"`|",|"D|":|")|",|"v|":|"!|",|"V|":|"#|",|"N|":|" |",|"a|":|",|",|"M|":|"(|",|"6|":|"_|",|"I|":|"
<|",|"p|":|"@|",|"0|":|"/|",|"H|":|"^|",|"1|":|">|",|"t|":|"*|",|"J|":|"$|",|"d|":|"&|",|"z|":|"~|",|"L|":|".|",|"O|":|";|"}",
  "PCRT": "{|"h|":|"(|",|"n|":|"@|",|"M|":|"/|",|"Y|":|"%|",|"Q|":|")|",|"l|":|"&|",|"F|":|"#|",|"O|":|"<|",|"U|":|"!|",|"W|":|"`|",|"c|":|">|",|"2|":|"^|",|"B|":|"
|",|"a|":|",|",|"K|":|".|",|"Z|":|"_|",|"m|":|"-|",|"E|":|"~|",|"o|":|";|",|"x|":|"*|",|"p|":|"$|"}",
  "TAG": "",
  "MUTEX": "DCR_MUTEX-5BbmMLF7hMWVj4tneyWz",
  "LDTM": false,
  "DBG": false,
  "SST": 5,
  "SMST": 2,
  "BCS": 0,
  "AUR": 1,
  "ASCFG": {
    "savebrowsersdatatosinglefile": true,
    "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
00000011.00000002.507606003.0000000003768000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000005.00000002.392526659.0000000002741000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000019.00000002.437075791.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000000.00000002.369748569.000000001252F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.399908705.0000000012CA5000.00000004.00000800.00020000.00000000.sdmp	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0x6e927c:$: VFZxUUFBT • 0x73128c:$: VFZxUUFBT • 0x8a19cc:$: VFZxUUFBT • 0x8ba81c:$: VFZxUUFBT • 0x8be824:$: VFZxUUFBT • 0x69eee0:$: RWcVFBQU • 0x84bd40:$: RWcVFBQU • 0x873d48:$: RWcVFBQU • 0x884470:$: RWcVFBQU • 0x7227da:$: UVnFRQUFN • 0x8a6f2a:$: UVnFRQUFN
Click to see the 10 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN DCRat Initial Checkin Server Response M4 - Source IP: 5.23.51.236 - Destination IP: 192.168.2.4

Timestamp:	5.23.51.236192.168.2.480497162850862 08/05/22-17:44:21.513896
SID:	2850862
Source Port:	80
Destination Port:	49716
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Networking

Snort IDS alert for network traffic

Persistence and Installation Behavior

Drops executable to a common third party application directory

Creates processes via WMI

Boot Survival

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

Stealing of Sensitive Information

Yara detected DCRat

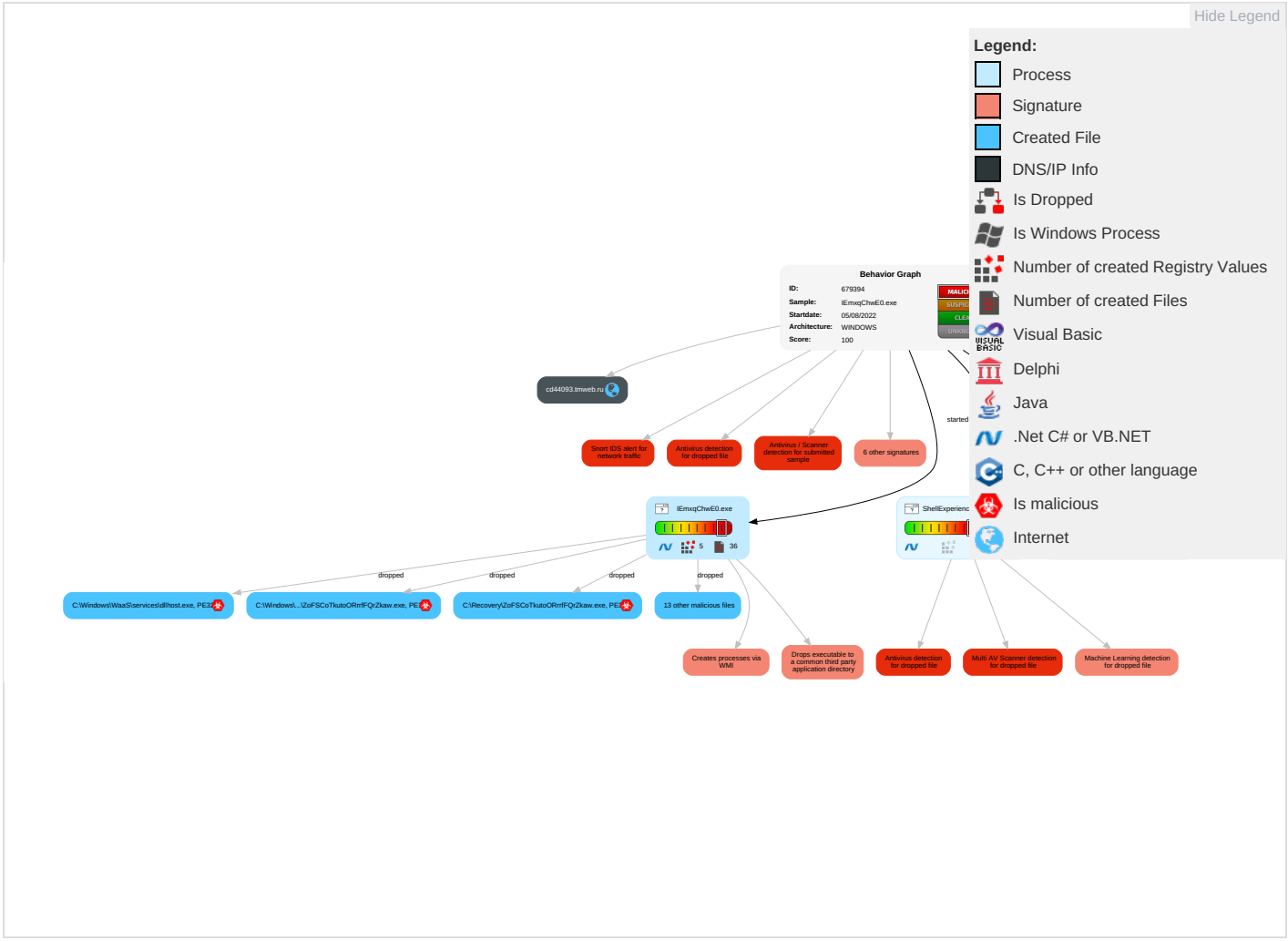
Remote Access Functionality

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 2 Process Injection	1 2 3 Masquerading	OS Credential Dumping	1 Query Registry	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
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	1 1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated 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	Steganography	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
IEmxqChwE0.exe	59%	Virustotal		Browse
IEmxqChwE0.exe	43%	Metadefender		Browse
IEmxqChwE0.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
IEmxqChwE0.exe	100%	Avira	HEUR/AGEN.1249330	
IEmxqChwE0.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Windows\WaaS\services\dllhost.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Avira	HEUR/AGEN.1249330	

Source	Detection	Scanner	Label	Link
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Avira	HEUR/AGEN.1249330	
C:\Recovery\ShellExperienceHost.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Avira	HEUR/AGEN.1249330	
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\Windows\WaaS\services\dllhost.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\RuntimeBroker.exe	100%	Joe Sandbox ML		
C:\Recovery\ShellExperienceHost.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\RuntimeBroker.exe	43%	Metadefender		Browse
C:\MSOCache\All Users\RuntimeBroker.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	43%	Metadefender		Browse
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe	43%	Metadefender		Browse
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Program Files (x86)\WindowsPowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe	43%	Metadefender		Browse
C:\Program Files (x86)\WindowsPowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe	43%	Metadefender		Browse
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\RuntimeBroker.exe	43%	Metadefender		Browse
C:\Recovery\RuntimeBroker.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\ShellExperienceHost.exe	43%	Metadefender		Browse
C:\Recovery\ShellExperienceHost.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe	43%	Metadefender		Browse
C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe	43%	Metadefender		Browse
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe	85%	ReversingLabs	ByteCode-MSIL.Backdoor.DCRat	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.IEmxqChwE0.exe.120000.0.unpack	100%	Avira	HEUR/AGEN.1249330		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://go.mic	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://cd44093.tmweb.ru8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cd44093.tmweb.ru	5.23.51.236	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_quicktime	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_wmp	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.516172430.0000000003B5E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6258784	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flash	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.516172430.0000000003B5E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cd44093.tmweb.ru	RuntimeBroker.exe, 00000011.00000002.505413951.00000000036A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_java	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://go.mic	WmiPrvSE.exe, 00000025.00000002.445673226.000000000134A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cd44093.tmweb.ru/	RuntimeBroker.exe, 00000011.00000002.505413951.00000000036A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_real	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://service.real.com/realplayer/security/02062012_player/en/	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cd44093.tmweb.ru/_Defaultwindows.php?aRMYTVOUDKp5xKJ84fbVPR0rCj=25pNzWjTJ&EI841VYtPwU=tc1VJiJ	RuntimeBroker.exe, 00000011.00000002.505413951.00000000036A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/chrome/?p=plugin_shockwave	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cd44093.tmweb.ru8	RuntimeBroker.exe, 00000011.00000002.507606003.0000000003768000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.510002464.000000000384D000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.511767123.0000000003943000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.517984489.0000000003DAA000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.509547529.000000000380D000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.509718411.000000000382E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cd44093.tmweb.ru/_Defaultwindows.php?dKi2zUqI5X9HnmLXfJLuzzS=EvZPxw2pbp0wsTa&MzkLtwK6Jlzw4K2n	RuntimeBroker.exe, 00000011.00000002.517984489.0000000003DAA000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.509547529.000000000380D000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.509718411.000000000382E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_pdf	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_divx	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fpdownload.macromedia.com/get/shockwave/default/english/win95nt/latest/Shockwave_Installer_Sl	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	lEmxqChwE0.exe, 00000000.00000002.369233850.0000000002B01000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.505413951.00000000036A1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://forms.real.com/real/realone/download.html?type=rpsp_us	RuntimeBroker.exe, 00000011.00000002.518124161.0000000003DB9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	RuntimeBroker.exe, 00000011.00000002.515301987.0000000003ADC000.00000004.00000800.00020000.00000000.sdmp, RuntimeBroker.exe, 00000011.00000002.516172430.0000000003B5E000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679394

Start date and time: 05/08/202217:41:11	2022-08-05 17:41:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IEmxqChwE0.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:	41
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.winEXE@33/36@20/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 56% • 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): Conhost.exe, SgrmBroker.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.35.236.56
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net
- Execution Graph export aborted for target IEmxqChwE0.exe, PID 6036 because it is empty
- Execution Graph export aborted for target RuntimeBroker.exe, PID 1048 because it is empty
- Execution Graph export aborted for target RuntimeBroker.exe, PID 4532 because it is empty
- Execution Graph export aborted for target ShellExperienceHost.exe, PID 336 because it is empty
- Execution Graph export aborted for target ShellExperienceHost.exe, PID 3764 because it is empty
- Execution Graph export aborted for target WmiPrvSE.exe, PID 1448 because it is empty
- Execution Graph export aborted for target WmiPrvSE.exe, PID 408 because it is empty
- Execution Graph export aborted for target ZoFSCoTkutoORrrfFQrZkaw.exe, PID 2988 because it is empty
- Execution Graph export aborted for target ZoFSCoTkutoORrrfFQrZkaw.exe, PID 5548 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 NtAllocateVirtualMemory 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
17:42:38	Task Scheduler	Run new task: ZoFSCoTkutoORrrfFQrZkaw path: "C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe"
17:42:39	Task Scheduler	Run new task: ZoFSCoTkutoORrrfFQrZkawZ path: "C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe"
17:42:41	Task Scheduler	Run new task: RuntimeBroker path: "C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe"
17:42:42	Task Scheduler	Run new task: RuntimeBrokerR path: "C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe"
17:42:44	Task Scheduler	Run new task: ShellExperienceHost path: "C:\Recovery\ShellExperienceHost.exe"
17:42:45	Task Scheduler	Run new task: ShellExperienceHostS path: "C:\Recovery\ShellExperienceHost.exe"
17:42:50	Task Scheduler	Run new task: WmiPrvSEW path: "C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe"
17:42:53	Task Scheduler	Run new task: WmiPrvSE path: "C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe"
17:42:58	Task Scheduler	Run new task: dllhost path: "C:\Windows\WaaS\services\dllhost.exe"

Time	Type	Description
17:42:58	Task Scheduler	Run new task: dllhostd path: "C:\Windows\WaaS\services\dllhost.exe"

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:\MSOCache\All Users\9e8d7a4ca61bd9

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	297
Entropy (8bit):	5.788088634875492
Encrypted:	false
SSDEEP:	6:g2ZLGJUd9LXDaiTU8X/bFK4ZzLs2EQCABCylUCq53Ug8l9YRQ54IH:zZLI8DbYG/bEOzwk1CAUb3UJHPTH
MD5:	517EB151228FB049E52A9BE4BA8926A7
SHA1:	50A0B9B6920C1D94539B01331941848FCE7894FE
SHA-256:	7716A3F86F65EECF7822FAF25C1E2201BFD70828FF87DBA01C40FF5AF6377068
SHA-512:	61CE23FB987F1E78C66C79A829364A92F054CC35BD5475F2FC17888CC44318D9B37D960FEC43C0E84DC9BD0E29F7CAA436C987552223C77CD6B47BEA2BA9A9F
Malicious:	false
Preview:	hYJScIxi66RVzz6xqRlul9ybN88wfe0iTqxt76hpw24wgfD64OR0f7JikrEdJBDbGtBJCMztt57QFB5r5C1QM9CWgOIQ1Efvycqxe33rZiHj92cjwXhHJxOGqpmxEj2oaM bnUINBJJ1o2cWowidehYlBNkGyRFnzqcJwbzOoJf795kNNS8BfFXHBlZZuBYuDgB8aTjN6UzVBblFnW2gSEHtSUILBZdmuu3d4lx4svELQCGk9TwYJ2b9YRq FKYLg0MkQhHLBi7xh96dQOiLrnEd1S4Fm5stUjiUEbzC2Iu

C:\MSOCache\All Users\RuntimeBroker.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71

SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... .....H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B..... ....

C:\MSOCache\All Users\RuntimeBroker.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\2cdddf0d5a7032

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	53
Entropy (8bit):	5.081417388403002
Encrypted:	false
SSDEEP:	3:k7nsJu+ySj/IPZGpQhWmn:WsJDBjWG2
MD5:	EE16613A20135F1728FD1434AF8CD177
SHA1:	ED7C14A906C9FC50B1D67E79B30DD09C82CDEEBC
SHA-256:	8962976E057BC55B348F135C131F90D91FDDBC4DE71BB2A7B57B2D000EC5E7DB
SHA-512:	817A9771AF507F573E92F277B64D191FE38682C0FA9AD0DB92D8F4D4F9EC302F39C5516948EFC2DEE8F14148D10BDA99B1BE48BC452FD3769ACD581844859B3
Malicious:	false
Preview:	dDwLz3JQxM7Rpu4lXxP5O2lZb3YJFkwdu1BZmjsRIo8L5DgpuZhRV

C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B..... ....

C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Program Files (x86)\Mozilla Firefox\plugins\24dbde2999530e

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	496
Entropy (8bit):	5.8655755513814345
Encrypted:	false
SSDEEP:	12:NqarCOSmoCC67SuqE54L9jviFXHSJ39gnJCg5AyMbqhA:wa2moCCqEdvF9gJCgGyMbqhA
MD5:	6C1B0AD1F77643EBE280DD0B5E57A661
SHA1:	3E3E9275E41F4E7A4BE7211FAB8B68220F4BD6A2
SHA-256:	0111DEC5CA74B80616CB05D713183244FFBB42D5F82DD947C870F3967E011BBA
SHA-512:	C6AB2C82FE0CB699845AEA2DA3A765C20C5FDD7D8B744B8B91BB2355344FCED1797BA71CF88C076E95E1DF289414DED4E91811542B8B74114F7F1F93A64F1CFC
Malicious:	false
Preview:	9yE8wj3ZeXWtYqCfHDDa7PzwwIdvwags6QZsMX4OrC2WjvldK3XdvSht8SLoFHnD1oxIQUStIyt5WdMAgAl2DC7otpu3MPIjYyf48dNzknU6ilXfFKIFfu9yrIZkjYg3pJ gi7SCCxwRarAFHSOyBHDDnyrNzDmPLGbRYFyhxIFStcjGrDSSVkfvmG2tQFM9KgGTQtqBerA3BuTKOkfwvT4llpoSMEQs6GHNWQ08WQxnjlu1wrfqjZN1lfr kEXyZaS65mFy7uhaefRB95wgfjkIg2Qm1jP38bYNRoyPq3h5B9sVUdsoR1T00JaCVd6YeobCHEuUGhzlBoHhJ5SX1lmGIiWHOw3N6IbXhqNPtXiuCryLC22aKjh3CU4jrm FUolp3Mt9dsCodC1EatLFW4cDXkiVNvniGROGaC49S2YsH5E0KPdzghtZLiRSoYwrEehLyvoYyLwdfu5cgrL7SxCjiy51umU3GqnnX2BYlEBUuQ4anzv

C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K....'.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B..... ....

C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Program Files (x86)\WindowsPowerShell\2cdddf0d5a7032

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	459
Entropy (8bit):	5.862814806898702
Encrypted:	false
SSDEEP:	12:nthMB5w1VAY/V1ct1wpxz5zdxFaiEnsNUaRbcvjpqX4:nY/wUY/83wFpDEn8Uax8q4
MD5:	DBA96A5587BE1A22B7C7D59B1E57613F
SHA1:	A347701B5FD8E3B2B9BA1FFABFC47122F609E7DF
SHA-256:	57D02EE59FA0B93B6616316F3702901CC57AE809F7509E119B810AF79119CD9B
SHA-512:	4B3D6CCFE77638673CC50C1BC7D2A5C22F3842D0DE1A27FD91B335E331529D5A83D6C98137FF08EC8C38CC825E3B451C33AFF6D9FAC6B12EF00986C96EA15 CE
Malicious:	false
Preview:	RY3ZZC1LqsiNi93Jdw2fqQhIs4eEIZBk5HQLNdvmx0RSAL1miEVqScvB0vqfhwCQr7Rass5AAPrz9PHgC1fEDURdWPUbwPEByAkC4a30lVpDu5CloKdpQ7NX qyEdYeNuKqB9oEml8p6roOsaMtxmwZu0wNWFWZboI52E4D6jh1rlBfsbFoQpqk7v5LMbrgPiNSjtWnfJwOE5rJzQf4ArJw7h7GIt0f1BllXt68FbIH2cgCEwV56xghZbUB wPfwSRWDTjwGUgyiiC3fB4CWX5jEeEt6Y5M06WyIFdsfAPkZ889XhzA1NIYXrSiPz0rZT8lMNSZiMhWlUJFgEVYj4Vmx7b3x4dpKhLG9XxJPZbppwQCiMCKe bIe8VxOwYmns2LkJDFJRLJKcp6AqZVk2SKsZqHojiX1wy6xlp2eH33SS8BTYwiWCCuardLc5bjtxSXosJZAg0d9Z2

C:\Program Files (x86)\WindowsPowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C7 75B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`...@.. .....'..... .@.....['.K....'.....'..... .....H.....text...$<'.. ...>'..... .`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Program Files (x86)\WindowsPowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Program Files\Common Files\microsoft shared\vgx\9e8d7a4ca61bd9

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.857164797311588
Encrypted:	false
SSDEEP:	12:PACb6cZ6Y2x86tC0bAXPXXcFtqhgdGjl9VjspG50jAWdi9ANr:PTblDt6LbIcFtqhgYlzL0jQANr
MD5:	90DFB91DEF995ACDEA99CB4FF87F5E1B
SHA1:	546487FF8401281FC34FA6BC922B44FDA955094B
SHA-256:	EB548F74019DA516DC31E4EE768C4C5C4EE35DEAE918DDEAB528C07512DAEE59
SHA-512:	6FBBAA94D47000CA998408DB5FD134973D09997BC413A669046C316423EEDB97207DACB5637F02A399A5FD0FA53FE8F2733C7A6D16391E6EBDD055217E3ABA A
Malicious:	false
Preview:	HuE6LwseqCw680j4U5YpkyHK2O9fmdsiv0HRz5KU3t4iuJbBm8pTck7Tm3E7wN2MTOKHsSEZuEv14jZtx72nxYFL3yo61Nhq1rOg8TTU4QjXyFYDeUKyUOZ5I9O3oIghE ANU2vdoitgzsWyalcgDtWnRTY8FZqvsC0uFKsljqJve3FZmZdDqBdysX6BewYP18xx2msP207XjkJYO8Wp5nFqiCBsOrGwR43fFRh9rNKzEGOIOhxfasTO2HOzIAAKuKFp qnS6bW8rcQlcx3dq4lWikpn8CrYqM9E4AjbkP0EDumvmfwCrgTQJxgFAAU3t8RedLrcNb2bDgTx73AdQoqK3s5Hdebk56UFdHSbxTzQn2MmdsHH90nERHluP j8sASgHMOU0kjp6zagAgTnuXTkETPxWfiLNUGQVVFaPYQgaLqP1klO66OUqrcx6a7VCXbmsKLoa2XVHxK2mA6v4UORGvjo3Rdza4dCuEgrZ6xEj2N2gjK6dLasIKf6kguI Yh5MTHIidPW7gKrNiqHUGhWOdv3kijG2LopB7AiZa

C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C7 75B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`...@.. .....'..... .@.....['.K....'.....'..... .....H.....text...$<'.. ...>'..... .`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Recovery\2cdddf0d5a7032

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	181
Entropy (8bit):	5.699431476206666
Encrypted:	false
SSDEEP:	3:W7Lrcf31m/xecCuDdUnvGkEMmXOEI9VRGMvWGy3LauSMTSBftEvuteYd9iJIrcgU:W7u36kwoGOEI97GMvm3FyftEW6Cc0nk
MD5:	D68A6FD1F81653C134C4E114E10230FB
SHA1:	52F115CC8C14C745A47BC8B9D2C7C46B0A0176B3
SHA-256:	9300C62C1051BB081293CAC523CAF62F535BE4D607AA070CF7A2DA4877B06A8A
SHA-512:	37674593AA4E1E46CE418644B2AFDF5148BC8020CAD2B43EF220FEA79A8B309E48C46B7C8A862049C2A29EF74FBD90427D91DE0576573A6D6AD7CFB881E9AA7E
Malicious:	false
Preview:	sf6XNJn8iBwloo9zRPUOkWCPDFgOOKl5EOO0WEVkrRVmqAY6SVRYtCkWcrUImYuYZ1gaaJcN3ugSAaiCrk622MLCo2YptN7Sh7Mzd8gI3Ef9fRVBIRbCc1fM pewivwdqwNvDNtjtEx9xrMhWgWgcw50pb9J9L8XGlyMSfRyZrr8o2sfd7ZBYP

C:\Recovery\9e8d7a4ca61bd9

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	792
Entropy (8bit):	5.907993793467935
Encrypted:	false
SSDEEP:	24:FZXhzoftQ1iFsWRjyySafyK6UARqy6Kan:rhzemzCdr+UiqyW
MD5:	6C01AC5B1FA633E96C29E06F1A233E78
SHA1:	ED6E6C76DEDC38A1E7D8B1B23933922333C33449
SHA-256:	0A6EAED3E68F7E2EE1F6BFC480E11E89B934CB784B1AFBBF9BD24E20020027FC
SHA-512:	A44FBC775D368C085478A4618BF937EA8C60D90F117F771A8833C732CAA1928A6C3CFB5EA73DC391494E89D977F21C5F3897087A956A014516E9B255EA57A1EF
Malicious:	false
Preview:	oM13WyHREoqwVNwsyR3eN50YqRRWMZOBhyayc13FSVuGQadLdtJWGVjsVdMFhuFoaoOhx7P7YxL1LtHQxG2cQ24MPrd9oxiiQFqlL6XgeM7SKrhlV6Rb1mYi tCRFePSkPnlFDgE1sW8E4lChK1osgHrnrH1JoSBO3XDgFbiy2atenToHAt4mkjDH57X5o4NZVuKgifcsT0zGYM9YdtJ4XYoTT5kHDmJ7NTJ3IHjfRMTut7tt89b4vSC6F0 Nm4Uoqq23EDFPWKnmLF3jVM1JELOM4RMyR36k7hmE1Eop2uEuHp11LQ1aCKkfbp8x0R7dNDpnczsQhLRUGeEOaVmABghx7HmLF1zkwlhEANYVik212QZ6ltX ep7bqf2qVNgKqWrhe6AOM7Qcboq4qrpkWdU5zK0ilhCICZMfLs4AlfKhYfACz79nh5yMBvsUGbGp5HZBbLt7xp90SxgUKytKhYlGk9dZAj4KZflRF8knOB01684NPYKRr5 HggTacrT7NvybwLPOLNF6giuJmEQKlZmcdYFuwiH65DmFHgHB9J8Dl9l8wJxXbIWyJW8YGecmGJAc6oBF7OKbai0dxG8mvtfwry6vis5frW7c8lCHHraM75Xlfel9gz1Wn OvHrQhOTptEkYeoE0fDTSyvbVPEH592elyuW4Z1KL3SLSAH965pUyCVZ9qWAcHYq1k9juSKao2lZgkIUIFL9ThqidVXND0sEflTsAhPouOq5462YhB2X6YWT 3bGY46XxKE44RaUkzhPE1unhc8pB8UHGO9yjb0tx12

C:\Recovery\RuntimeBroker.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false

SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Recovery\RuntimeBroker.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Recovery\ShellExperienceHost.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Recovery\ShellExperienceHost.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false

SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... .....H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Recovery\f8c8f1285d826b

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	171
Entropy (8bit):	5.718695427460925
Encrypted:	false
SSDEEP:	3:5OsAkQoZomx3W1Unxrt45RvLJ4pG2J5aYAbkWjRkssKc2YCcCmTu1RI5EFtN:sZkzNG5pLIhbaY5WtkyK/YfCmfEF/
MD5:	3446F1ADC6A84482B968A6E5DB94BD1E
SHA1:	339127E3CB3CFDA396716A276FC3EC07D3D22E4D
SHA-256:	98D5805887A8846F8D50D5FD58AB48CECB61BDEFBD1BCD6398F080C41CBAAEC4
SHA-512:	09B510A5C0F0C4C9EEB63545C7659656B6B5A820F23B3231F8A0C84AC4BEE1CF7602B026828BBA4B9E0FFFFD6071339BD4ABAC5AEA883E31921E1A34AD373A53
Malicious:	false

Preview:	e9kXkPWh0LjvAyCuxHMxtwdnkMCRgGRxqPXa0RO9ZcKmLSfRFtmbdfbsf7wYMFBu4vFvbl4f3MXQm1cSquMwd0UKyp52ezwUbasZNt0ezGiQIKFoferc3ORD a47vqBADZDyLICF64r7WRDCnjQXAIUbMJo8SvFyxGe1EW4fdZuh

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\IEmxqChwE0.exe.log

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1915
Entropy (8bit):	5.357013020641263
Encrypted:	false
SSDEEP:	48:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1hAHKKPzJHVHpH+RHKl:iqnwmI0qerYqGgAoPtzG1eqKPF1Jgql
MD5:	D51ACEABB86EE1011F30283D80CCC5CB
SHA1:	3AC7C663B0BBDD03E8902007AA3339AB15799AD4
SHA-256:	BD8B47AC2ABAF695C87F5C2B1DEF43D95416A0BEF5FE6BF0E7E713E662942024
SHA-512:	E0B6D2E9BB1DE33ECA36FE7884CD92AE69C2565DB6661EE299BC192C172FE30AA67EFDCD2E8372F63E8974B1A0BE95105A6A9C505D102FDAB4082B8BCE1CEA07
Malicious:	**true**
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\ShellExperienceHost.exe.log

Process:	C:\Recovery\ShellExperienceHost.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\WmiPrvSE.exe.log

Process:	C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.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\ZoFSCoTkutoORrrfFQrZkaw.exe.log

Process:	C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.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\Temp\n1eJyN2FEu

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	25
Entropy (8bit):	4.133660689688186
Encrypted:	false
SSDEEP:	3:a7LkeS2G3mHX:aPfSE
MD5:	499499A2CB4BF12AA06138B1232C9337
SHA1:	CA7C9EE80B67C84A327FC047EF59BB7102D53063
SHA-256:	A45B1E1B38A5D964C1DE9ED0AA53E88C25D29CDD38835696DB439D3A09CEF02D
SHA-512:	0D90B9EA9B8BCDB2C882D6FC65F70D6438506F5549EC61B8080990AE1A3F7F745529FD4B9F8AA0908E2865F6DF9FAA2171B4A21FF79F0950B3A6F7EC69F63C8
Malicious:	false
Preview:	K0JkK0nASgaw6bg2S1DbcRCbr

C:\Users\user\AppData\Local\Temp\vHbeHiYPsn.bat

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	DOS batch file, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	204
Entropy (8bit):	5.094678987510775
Encrypted:	false
SSDEEP:	6:hITg3Nou11r+DE/EaA5AEWDUvIKOZG1wkn23fTac8h:OTg9YDE/ELiEVCf7Sh
MD5:	B4AF0F85058566A42EB036CE38F7762B
SHA1:	E8C6E1E310D7F924EEECE7FCBC611A7E431A855E
SHA-256:	25A19F866E685FD3E507BC995D38946DEE54EA123FF668E3A1B944C4FFF26998
SHA-512:	82B82B8B2DB52C5C50DF84DB30E49423F63A5195387E237A5EF02295EE663F00D3AC5B09D0D0606C47B480C5013EE8FE7CB5BD71F71DE8B11723402B22DC3E0
Malicious:	false
Preview:	@echo off..w32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2 1>nul..start "" "C:\MSOCache\All Users\RuntimeBroker.exe"..del /a /q /f "C:\Users\user\AppData\Local\Temp\\vHbeHiYPsn.bat"

C:\Windows\Speech_OneCore\Engines\TTS\2cdddf0d5a7032

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	630
Entropy (8bit):	5.902849781764413
Encrypted:	false
SSDEEP:	12:cY/Q36NK4TYbPQ+pPLlT3/1vQGSepIL6qvXBg5GswAfuG5YBPivi8:c0c6NBYUULxP1GepYxg5JuGEyn
MD5:	E7A1192471D8C47373C72AA7D919F6F5
SHA1:	7091E3A7FED5ECFA25D08CB299A47869F7BA3D8D
SHA-256:	F4DB2B7D322311608E540D8367FFA0F59D2E3515477ED8F029552A01D9282CE0
SHA-512:	FBC8E59F1284166D748059C7267A4BF597BB7C83C3AF1BC23EA9025B01E6B2C32DABA1A4CBCE06BE85FB09C076FD6A1F70BF53D4032BB06C79DA5857A27A136B
Malicious:	false
Preview:	Md3vss8nCiGzNc7blYyYfTj2OSwY4nyf1GIGoiVt1ZzjoA7n6i0ZlbH23Aha6jsZuk8GT1wCDFhGdANOUJbVwY3Z9QNoB4wRqayEC0TFwxWg4BY2xTGxIXmWqiHDoIBISQZDMJLdzVj8CXf81U1sy9JTxbXdtPbnwNOnlVqnHm7wxoUTDIMTRSUSHGPuvrtk46MyJ1XgoNlLCWfJHEakCHWe35geF52Z2W11bfKLvqpErIPukGmqRJhwjr4NU2atVLSpeorl4PyWcSxuqw38SLItzFRul603P6tf0kP6YBwBUKTR4Khi8baJDi0ZX7A7Y5GgiS4Fg7kRZGZov9zaZR5xfjbRu0ibAynYEwsmPbCA1Ju6JLnXHjhGASB90nVpYIRlcAk8QNL8P46WzeHiNLTaQgYvvtwmGWls1JeIkoH4Yj1FWpKVfwcNz0U6mzNhbj22SNeqA98iDYBroSYGjaHT4Y3Byhgvbkdzr9xJLeUgy4KbznRTbG7Abi74Ud1ccMGd5M9peO5EFlf9ObMLQNUUmcXIB3zrm1DlxrgmnmyML340C7p2RpMO2v0cz1nlZNbOh3Mh5jhoYIJthgGDN6a6pytB0Dxw8Nw7bqTIvI6rHi0tmH4Suj

C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 85%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'.....@.....['.K.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....'.....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\WaaS\services\5940a34987c991

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	93

Entropy (8bit):	5.361213918402281
Encrypted:	false
SSDEEP:	3:YCRAOL7dJYqbaTK2nULQd9k1cfWcCrEn/n:YCm31UU+cfRCrE/
MD5:	B95568F4AF0FE053C93D13045CBE0F67
SHA1:	5DD1D2B20E3F181C1889594399319D1530F734B9
SHA-256:	A621F6B2692F8DBCD788F6CCD4613132258EE64A83AD86D73FD7F41E6DFAADAC
SHA-512:	11CEE7726B9EBD2AE335A4CCE868562F60C5009745EFD4539C38BE27D8AC1381796948E1C39DD02D22647DC6A30BC338CA17A13854E545895E9083ECBDD625D
Malicious:	false
Preview:	AtyG8AZtJeBYzTL6Hl8lbE5W2oXbzDFwRSdDpctJv7tRtRVDAVtm9qn5xcOTm74FZOHhzHQp1yzeVnmlTUbdTdxlohPNN

C:\Windows\WaaS\services\dllhost.exe

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	2586624
Entropy (8bit):	7.6461087366315
Encrypted:	false
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
MD5:	0D32FF3680A716FD66CB9AB0E3EBC763
SHA1:	2AA356F14A156BF56EFC66E39E0654BDDB4FD95A
SHA-256:	21719369D4B1474AD31C61C60EC7510AB511A21BA5659CCA266F1E6A933CDC71
SHA-512:	4B8943FA3058E48C1D27AAB2B6A8AFB0493CA7A7E0BFFCCEBE6A709A19CB467A8EA89C5673912C05BF4DAC3F0D942D097BE6C39BF658C5E9B14053FF505C775B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....rb.....>'..6.....\'.. ...`'...@.. .....'..... .@.....['.K.....'.....'..... ..... ..H.....text...$<'.. ...>'..... ..`.sdata.../...`'..0...B'.....@....rsrc.....' .....r'.....@..@.reloc.....'.....v'.....@..B.....

C:\Windows\WaaS\services\dllhost.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\IEmxqChwE0.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6461087366315
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	IEmxqChwE0.exe

File size:	2586624
MD5:	0d32ff3680a716fd66cb9ab0e3ebc763
SHA1:	2aa356f14a156bf56efc66e39e0654bddb4fd95a
SHA256:	21719369d4b1474ad31c61c60ec7510ab511a21ba5659cca266f1e6a933cdc71
SHA512:	4b8943fa3058e48c1d27aab2b6a8afb0493ca7a7e0bffccebe6a709a19cb467a8ea89c5673912c05bf4dac3f0d942d097be6c39bf658c5e9b14053ff505c775b
SSDEEP:	49152:5Ad/na1hwN3zHvJB4x365neVoe51QDr67tUKR8jJLYPYI553bpGes:5cG6N3kBoi1QDr6RwjNYP15VVs
TLSH:	8DC5D001BE04CE11F0891A33D3EF49444BB4DC516AA6E31B7DBA376E56123A73D1DACA
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....rb.................>'..6.......\'.. ...`'...@.. ....'...........@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x675c1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6272A3D7 [Wed May 4 16:03:35 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x275bd0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27a000	0x218	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x273c24	0x273e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.sdata	0x276000	0x2fdf	0x3000	False	0.3101399739583333	data	3.2417089896030418	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x27a000	0x218	0x400	False	0.2646484375	data	1.8390800949553323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27c000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x27a058	0x1c0	data	English	United States

Imports

DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
5.23.51.236192.168.2.480497162850862 08/05/22-17:44:21.513896	TCP	2850862	ETPRO TROJAN DCRat Initial Checkin Server Response M4	80	49716	5.23.51.236	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 17:44:20.843542099 CEST	54003	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:20.862442970 CEST	53	54003	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:21.180304050 CEST	62099	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:21.199279070 CEST	53	62099	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:21.284873009 CEST	53775	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:21.302407980 CEST	53	53775	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:21.387284994 CEST	54800	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:21.404872894 CEST	53	54800	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:26.476664066 CEST	64454	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:26.494714022 CEST	53	64454	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:26.561148882 CEST	60506	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:26.580562115 CEST	53	60506	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:26.650312901 CEST	64277	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:26.669388056 CEST	53	64277	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:31.742499113 CEST	56076	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:31.760230064 CEST	53	56076	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:31.827970028 CEST	60758	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:31.847630024 CEST	53	60758	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:31.884614944 CEST	60647	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:31.904481888 CEST	53	60647	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:36.982038021 CEST	64909	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:36.999560118 CEST	53	64909	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:37.068160057 CEST	60381	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:37.087369919 CEST	53	60381	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:37.154230118 CEST	56509	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:37.173491955 CEST	53	56509	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:42.258498907 CEST	54069	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:42.278067112 CEST	53	54069	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:42.343139887 CEST	57747	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:42.360688925 CEST	53	57747	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:42.383513927 CEST	58171	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:42.402864933 CEST	53	58171	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:47.476401091 CEST	57594	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:47.495313883 CEST	53	57594	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:47.564364910 CEST	60512	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:47.583703995 CEST	53	60512	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 17:44:47.649759054 CEST	61361	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:47.669043064 CEST	53	61361	8.8.8.8	192.168.2.4
Aug 5, 2022 17:44:52.772794008 CEST	50445	53	192.168.2.4	8.8.8.8
Aug 5, 2022 17:44:52.789918900 CEST	53	50445	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 17:44:20.843542099 CEST	192.168.2.4	8.8.8.8	0xc823	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.180304050 CEST	192.168.2.4	8.8.8.8	0x640	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.284873009 CEST	192.168.2.4	8.8.8.8	0xb8bb	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.387284994 CEST	192.168.2.4	8.8.8.8	0xd575	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.476664066 CEST	192.168.2.4	8.8.8.8	0x7f2f	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.561148882 CEST	192.168.2.4	8.8.8.8	0x589e	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.650312901 CEST	192.168.2.4	8.8.8.8	0xb22d	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:31.742499113 CEST	192.168.2.4	8.8.8.8	0x5a0a	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:31.827970028 CEST	192.168.2.4	8.8.8.8	0x75b7	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:31.884614944 CEST	192.168.2.4	8.8.8.8	0xac2f	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:36.982038021 CEST	192.168.2.4	8.8.8.8	0x94c1	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:37.068160057 CEST	192.168.2.4	8.8.8.8	0xd88f	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:37.154230118 CEST	192.168.2.4	8.8.8.8	0x8a97	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.258498907 CEST	192.168.2.4	8.8.8.8	0xb51a	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.343139887 CEST	192.168.2.4	8.8.8.8	0x9ab5	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.383513927 CEST	192.168.2.4	8.8.8.8	0xea05	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.476401091 CEST	192.168.2.4	8.8.8.8	0x7d50	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.564364910 CEST	192.168.2.4	8.8.8.8	0xde67	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.649759054 CEST	192.168.2.4	8.8.8.8	0x8841	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:52.772794008 CEST	192.168.2.4	8.8.8.8	0x3f08	Standard query (0)	cd44093.tmweb.ru	A (IP address)	IN (0x0001)

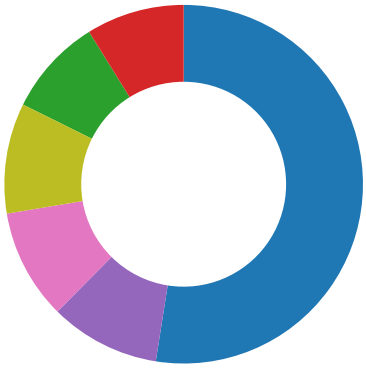
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 17:44:20.862442970 CEST	8.8.8.8	192.168.2.4	0xc823	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.199279070 CEST	8.8.8.8	192.168.2.4	0x640	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.302407980 CEST	8.8.8.8	192.168.2.4	0xb8bb	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:21.404872894 CEST	8.8.8.8	192.168.2.4	0xd575	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.494714022 CEST	8.8.8.8	192.168.2.4	0x7f2f	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.580562115 CEST	8.8.8.8	192.168.2.4	0x589e	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:26.669388056 CEST	8.8.8.8	192.168.2.4	0xb22d	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:31.760230064 CEST	8.8.8.8	192.168.2.4	0x5a0a	No error (0)	cd44093.tmweb.ru		5.23.51.236	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 17:44:31.847630024 CEST	8.8.8.8	192.168.2.4	0x75b7	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:31.904481888 CEST	8.8.8.8	192.168.2.4	0xac2f	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:36.999560118 CEST	8.8.8.8	192.168.2.4	0x94c1	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:37.087369919 CEST	8.8.8.8	192.168.2.4	0xd88f	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:37.173491955 CEST	8.8.8.8	192.168.2.4	0x8a97	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.278067112 CEST	8.8.8.8	192.168.2.4	0xb51a	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.360688925 CEST	8.8.8.8	192.168.2.4	0x9ab5	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:42.402864933 CEST	8.8.8.8	192.168.2.4	0xea05	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.495313883 CEST	8.8.8.8	192.168.2.4	0x7d50	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.583703995 CEST	8.8.8.8	192.168.2.4	0xde67	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:47.669043064 CEST	8.8.8.8	192.168.2.4	0x8841	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)
Aug 5, 2022 17:44:52.789918900 CEST	8.8.8.8	192.168.2.4	0x3f08	No error (0)	cd44093.tm web.ru		5.23.51.236	A (IP address)	IN (0x0001)

Statistics

Behavior



- IEmxqChwE0.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- ZoFSCoTkutoORrrfFQrZkaw.exe
- schtasks.exe
- ZoFSCoTkutoORrrfFQrZkaw.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- RuntimeBroker.exe
- RuntimeBroker.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- ShellExperienceHost.exe
- schtasks.exe
- ShellExperienceHost.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- WmiPrvSE.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- schtasks.exe
- WmiPrvSE.exe
- schtasks.exe
- schtasks.exe

Click to jump to process

System Behavior

Analysis Process: IEmxqChwE0.exe PID: 6036, Parent PID: 5324

General

Target ID:	0
Start time:	17:42:11
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\IEmxqChwE0.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\IEmxqChwE0.exe"
Imagebase:	0x120000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
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: 00000000.00000002.369748569.000000001252F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000002.399908705.0000000012CA5000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth
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	7FFFE1D6F1E9	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	7FFFE1D6F1E9	unknown
C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.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	7FFFE127817A	CopyFileW
C:\Recovery\ZoFSCoTkutoORrrfFQ rZkaw.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Recovery\2cdddf0d5a7032	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files\Common Files\microsoft shared\vgx\9e8d7a4ca61bd9	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Program Files (x86)\windows powershell\ZoFSCoTkutoORrrfFQrZkaw.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	7FFFE127817A	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Windows PowerShell\ZoFSCoTkutoORrrfFQr Zkaw.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files (x86)\windows powershell\2cdddf0d5a7032	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Recovery\ShellExperienceHost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFFE127817A	CopyFileW
C:\Recovery\ShellExperienceHos t.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	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	7FFFE0B96FDD	CreateFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.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	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe \:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\2cdddf0d5a7032	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files (x86)\mozilla firefox\plugins\24dbde2999530e	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Recovery\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	7FFFE127817A	CopyFileW
C:\Recovery\RuntimeBroker.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Recovery\9e8d7a4ca61bd9	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\MSOCache\All Users\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	7FFFE127817A	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\RuntimeBroker.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\9e8d7a4ca61bd9	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	7FFFE127817A	CopyFileW
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Windows\Speech_OneCore\Engines\TTS\2cdddf0d5a7032	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Windows\WaaS\services\dllhost.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	7FFFE127817A	CopyFileW
C:\Windows\WaaS\services\dllhost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFFE127817A	CopyFileW
C:\Windows\WaaS\services\5940a34987c991	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\n1eJyN2FEu	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\vHbeHiYPsn.bat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFFE0B96FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\IEmxqChwE0.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFE21D86ED	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\n1eJyN2FEu	success or wait	1	7FFFE0B9F270	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\Recovery\2cdddf0d5a7032	0	181	73 66 36 58 4e 4a 6e 38 69 42 77 6c 6f 6f 39 7a 52 50 55 4f 6b 57 43 50 44 46 67 4f 4f 4b 45 4f 4f 30 57 45 56 6b 72 52 56 6d 71 41 59 36 53 56 52 59 74 43 6b 57 63 72 55 49 6d 59 75 59 5a 31 67 61 61 4a 63 4e 33 75 67 53 41 61 69 43 72 6b 36 32 32 4d 4c 43 6f 32 59 70 74 4e 37 53 68 37 4d 7a 64 38 67 49 33 45 66 39 66 52 56 42 49 52 62 43 63 31 66 4d 70 65 77 69 76 77 64 71 77 4e 76 44 4e 74 6a 74 45 78 39 78 72 4d 68 57 67 57 67 63 77 35 30 70 62 39 4a 39 4c 38 58 47 6c 79 4d 53 66 52 79 5a 72 72 38 6f 32 73 66 64 37 5a 42 59 50	sf6XNJn8iBwloo9zRPUOkWCPDFgOOKl5EOO0WEVkrRVmqAY6SVRYtCkWcrUImYuYZ1gaaJcN3ugSAaiCrk622MLCo2YptN7Sh7Mzd8gI3Ef9fRVBIRbCc1fMpewivwdqwNvDNtjtEx9xrMhWgWgcw50pb9J9L8XGlyMSfRyZrr8o2sfd7ZBYP	success or wait	1	7FFFE0B9B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe	0	524288	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 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files\Common Files\microsoft shared\vgx\9e8d7a4ca61bd9	0	551	48 75 45 36 4c 77 73 65 71 43 77 36 38 30 6a 34 55 35 59 70 6b 79 48 4b 32 4f 39 66 6d 64 73 69 76 30 48 52 7a 35 4b 55 33 74 34 69 75 4a 62 42 6d 38 70 54 63 6b 37 54 6d 33 45 37 77 4e 32 4d 54 4f 4b 48 73 53 45 5a 75 45 76 31 34 6a 5a 74 78 37 32 6e 78 59 46 4c 33 79 6f 36 31 4e 68 71 31 72 4f 67 38 54 54 55 34 51 6a 58 79 46 59 44 65 55 4b 79 55 4f 5a 35 49 39 4f 33 6f 49 69 67 68 45 41 4e 55 32 76 64 6f 69 74 67 7a 73 57 79 61 6c 63 67 44 74 57 6e 52 54 59 38 46 5a 71 76 73 43 30 75 46 4b 73 6c 6a 71 4a 76 65 33 46 5a 6d 5a 64 44 71 42 64 79 73 58 36 42 65 77 59 50 31 38 78 78 32 6d 73 50 32 30 37 58 6a 6b 4a 59 4f 38 57 70 35 6e 46 71 69 43 42 73 4f 72 47 77 52 34 33 66 46 52 68 39 72 4e 4b 7a 45 47 4f 49 4f 68 78 66 61 73 54 4f 32 48 4f 7a 6c 41 41	HuE6LwseqCw680j4U5YpkyHK2O9fmdsiv0HRz5KU3t4iuJbBm8pTck7Tm3E7wN2MTOKHsSEZuEv14jZtx72nxYFL3yo61Nhq1rOg8TTU4QjXyFYDeUKyUOZ5I9O3oIighEANU2vdoitgzsWyalcgDtWnRTY8FZqvsC0uFKsljqJve3FZmZdDqBdysX6BewYP18xx2msP207XjkJYO8Wp5nFqiCBsOrGwR43fFRh9rNKzEGOIOhxfasTO2HOzlAA	success or wait	1	7FFFE0B9B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Windows PowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' ``'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Program Files (x86)\Windows PowerShell\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\Program Files (x86)\Windows PowerShell\2cdddf0d5a7032	0	459	52 59 33 5a 5a 43 31 4c 71 73 69 4e 69 39 33 4a 64 77 32 66 71 51 68 49 73 34 65 45 49 5a 42 6b 35 48 51 4c 4e 64 76 6d 78 30 52 53 41 4c 31 6d 69 45 56 71 53 63 76 42 30 76 71 66 68 77 43 51 72 37 52 61 73 73 35 41 41 50 72 7a 39 50 48 67 43 31 66 45 44 55 52 64 57 50 55 62 77 50 45 42 79 41 6b 43 34 61 33 30 49 56 70 44 75 35 43 6c 6f 4b 64 70 51 37 4e 58 71 79 45 64 59 65 4e 75 4b 71 42 39 6f 45 6d 6c 38 70 36 72 6f 4f 73 61 4d 74 78 6d 77 5a 75 30 77 4e 57 46 57 5a 62 6f 49 35 32 45 34 44 36 6a 68 31 72 6c 42 66 73 62 46 6f 51 70 71 6b 37 76 35 4c 4d 62 72 67 50 69 4e 53 6a 74 57 6e 66 4a 77 4f 45 35 72 4a 7a 51 66 34 41 72 4a 77 37 68 37 47 49 74 30 66 31 42 6c 49 58 74 36 38 46 62 49 48 32 63 67 43 45 77 56 35 36 78 67 68 5a 62 55 42 77 50 66 77 53	RY3ZZC1LqsiNi93Jdw2fqQhIs4eEIZ Bk5HQLNdvmx0RSAL1 miEVqScvB0vqf hwCQr7Rass5AAPrz9PH gC1fEDURdWP UbwPEByAkC4a30IVpDu 5CloKdpQ7NX qyEdYeNuKqB9oEml8p6 roOsaMtxmwZ u0wNWFWZboI52E4D6jh 1rlBfsbFoQp qk7v5LMbrgPiNSjtWnfJw OE5rJzQf4 ArJw7h7GIt0f1BlIXt68FbI H2cgCEw V56xghZbUBwPfwS	success or wait	1	7FFFE0B9B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\ShellExperienceHost.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Recovery\ShellExperienceHost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\Recovery\f8c8f1285d826b	0	171	65 39 6b 58 6b 50 57 68 30 4c 6a 76 41 79 43 75 78 48 4d 78 74 77 64 6e 6b 4d 43 52 67 47 52 78 71 50 58 61 30 52 4f 39 5a 63 4b 6d 4c 53 66 52 46 74 6d 62 64 66 62 73 66 37 77 59 4d 46 42 75 34 76 46 76 62 6c 34 66 33 4d 58 51 6d 31 63 53 71 75 4d 77 64 30 55 4b 79 70 35 32 65 7a 77 55 62 61 73 5a 4e 74 30 65 7a 47 69 51 49 4b 46 6f 66 65 72 63 33 4f 52 44 61 34 37 76 71 42 41 44 5a 44 79 4c 49 43 46 36 34 72 37 57 52 44 43 6e 6a 51 58 41 49 55 62 4d 4a 6f 38 53 76 46 79 78 47 65 31 45 57 34 66 64 5a 75 68	e9kXkPWh0LjvAyCuxHMxtwdnkMCRgGRxqPXa0RO9ZcKmLSfRFtmbdfbsf7wYMFBu4vFvbl4f3MXQm1cSquMwd0UKyp52ezwUbasZNt0ezGiQIKFoferc3ORDa47vqBADZDyLICF64r7WRDCnjQXAIUbMJo8SvFyxGe1EW4fdZuh	success or wait	1	7FFFE0B9B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\2cdddf0d5a7032	0	53	64 44 77 4c 7a 33 4a 51 78 4d 37 52 70 75 34 6c 58 78 50 35 4f 32 6c 5a 62 33 59 4a 46 6b 77 64 75 31 42 5a 6d 6a 73 52 49 6f 38 4c 35 44 67 70 75 5a 68 52 56	dDwLz3JQxM7Rpu4lXxP5O2lZb3YJFkwdu1BZmjsRIo8L5DgpuZhRV	success or wait	1	7FFFE0B9B526	WriteFile
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe	0	524288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Mozilla Firefox\plugins\24dbde2999530e	0	496	39 79 45 38 77 6a 33 5a 65 58 57 74 59 71 43 66 48 44 44 61 37 50 7a 77 77 49 64 76 77 61 67 73 36 51 5a 73 4d 58 34 4f 72 43 32 57 6a 76 6c 64 4b 33 58 64 76 53 68 74 38 53 4c 6f 46 48 6e 44 31 6f 78 49 51 55 53 74 49 79 74 35 57 64 4d 41 67 41 6c 32 44 43 37 6f 74 70 75 33 4d 50 49 6a 59 79 66 34 38 64 4e 7a 6b 6e 55 36 69 6c 58 66 46 4b 49 46 66 75 39 79 72 49 5a 6b 6a 59 67 33 70 4a 67 69 37 53 43 43 78 77 52 61 72 41 46 48 53 4f 79 42 48 44 44 6e 79 72 4e 7a 44 6d 50 4c 47 62 52 59 46 79 68 78 49 46 53 74 63 6a 47 72 44 53 53 56 6b 66 76 6d 47 32 74 51 46 4d 39 4b 67 47 54 51 74 71 42 65 72 41 33 42 75 54 4b 4f 6b 66 77 76 54 34 6c 6c 70 6f 53 4d 45 51 73 36 47 48 4e 57 51 30 38 57 51 78 6e 6a 6c 75 31 77 72 66 71 6a 5a 4e 31 6c 66 72 6b 45 58 79 5a	9yE8wj3ZeXWtYqCfHDDa7PzwwIdvwags6QZsMX4OrC2WjvldK3XdvSht8SLoFHnD1oxIQUStIyt5WdMAgAl2DC7otpu3MPIjYyf48dNzknU6ilXfFKIFfu9yrIZkjYg3pJgi7SCCxwRarAFHSOyBHDDnyrNzDmPLGbRYFyhxIFStcjGrDSSVkfvmG2tQFM9KgGTQtqBerA3BuTKOkfwvT4llpoSMEQs6GHNWQ08WQxnjlu1wrfqjZN1lfrkEXyZ	success or wait	1	7FFFE0B9B526	WriteFile
C:\Recovery\RuntimeBroker.exe	0	524288	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 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Recovery\RuntimeBroker.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Recovery\9e8d7a4ca61bd9	0	792	6f 4d 31 33 57 79 48 52 45 6f 71 77 56 4e 77 73 79 52 33 65 4e 35 30 59 71 52 52 57 4d 5a 4f 42 68 79 61 79 63 31 33 46 53 56 75 47 51 61 64 4c 64 74 4a 57 47 56 6a 73 56 64 4d 46 68 75 46 6f 61 6f 4f 68 78 37 50 37 59 78 4c 31 4c 74 48 51 78 47 32 63 51 32 34 4d 50 72 64 39 6f 78 69 69 51 46 71 6c 4c 36 58 67 65 4d 37 53 4b 72 68 6c 56 36 52 62 31 6d 59 69 74 43 52 46 65 50 53 6b 50 6e 6c 46 44 67 45 31 73 57 38 45 34 6c 43 68 4b 31 6f 73 67 48 72 6e 72 48 31 4a 6f 53 42 4f 33 58 44 67 46 62 69 79 32 61 74 65 6e 54 6f 48 41 74 34 6d 6b 6a 44 48 35 37 58 35 6f 34 4e 5a 56 75 4b 67 69 66 63 73 54 30 7a 47 59 4d 39 59 64 74 4a 34 58 59 6f 54 54 35 6b 48 44 6d 4a 37 4e 54 4a 33 49 48 6a 66 52 4d 54 75 74 37 74 74 38 39 62 34 76 53 43 36 46 30 4e 6d 34 55 6f	oM13WyHREoqwVNwsy R3eN50YqRRWMZ OBhyayc13FSVuGQadL dtJWGVjsVdMF huFoaoOhx7P7YxL1LtH QxG2cQ24MPr d9oxiiQFqlL6XgeM7SKrh lV6Rb1mYi tCRFePSkPnlFDgE1sW8 E4lChK1osgH rnrH1JoSBO3XDgFbiy2at enToHAt4m kjDH57X5o4NZVuKgifcs T0zGYM9Ydt J4XYoTT5kHDmJ7NTJ3I HjfRMTut7tt 89b4vSC6F0Nm4Uo	success or wait	1	7FFFE0B9B526	WriteFile
C:\MSOCache\All Users\RuntimeBroker.exe	0	524288	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 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\MSOCache\All Users\RuntimeBroker.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\MSOCache\All Users\9e8d7a4ca61bd9	0	297	68 59 4a 53 63 49 78 69 36 36 52 56 7a 7a 36 78 71 52 6c 75 49 39 79 62 4e 38 38 77 66 65 30 69 54 71 78 74 37 36 68 70 77 32 34 77 67 66 44 36 34 4f 52 30 66 37 4a 69 6b 72 45 64 4a 42 44 62 47 74 42 4a 43 4d 7a 74 74 35 37 51 46 42 35 72 35 43 31 51 4d 39 43 57 67 4f 49 51 31 45 66 76 79 63 71 78 65 33 33 72 5a 69 48 6a 39 32 63 6a 77 58 68 48 4a 78 4f 47 71 70 6d 78 45 6a 32 6f 61 4d 62 6e 55 49 4e 42 4a 4a 31 6f 32 63 57 6f 77 69 64 65 68 59 6c 42 4e 6b 47 79 52 46 6e 7a 71 63 4a 77 62 7a 4f 6f 4a 66 37 39 35 6b 4e 4e 53 38 42 66 46 58 48 42 6c 5a 5a 75 42 59 75 44 67 42 38 61 54 6a 4e 36 55 7a 56 42 62 6c 46 6e 57 32 67 53 45 48 74 53 55 49 4c 42 5a 64 6d 75 75 33 64 34 6c 78 34 73 76 45 4c 51 43 47 6b 39 54 77 59 4a 32 62 39 59 52 71 46 4b 59 4c 67	hYJScIxi66RVzz6xqRluI9ybN88wfe0iTqxt76hpw24wgfD64OR0f7JikrEdJBDbGtBJCMztt57QFB5r5C1QM9CWgOIQ1Efvycqxe33rZiHj92cjwXhHJxOGqpmxEj2oaMbnUINBJJ1o2cWowidehYlBNkGyRFnzqcJwbzOoJf795kNNS8BfFXHBlZZuBYuDgB8aTjN6UzVBblFnW2gSEHtSUILBZdmuu3d4lx4svELQCGk9TwYJ2b9YRqFKYLg	success or wait	1	7FFFE0B9B526	WriteFile
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe	0	524288	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 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Windows\Speech_OneCore\Engines\TTS\ZoFSCoTkutoORrrfFQrZkaw.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Speech_OneCore\Engines\TTS\2cdddf0d5a7032	0	630	4d 64 33 76 73 73 38 6e 43 69 47 7a 4e 63 37 62 6c 59 79 59 66 54 6a 32 4f 53 77 59 34 6e 79 66 31 47 49 47 6f 69 56 74 31 5a 7a 6a 6f 41 37 6e 36 69 30 5a 6c 62 48 32 33 41 68 61 36 6a 73 5a 75 6b 38 47 54 31 77 43 44 46 68 47 64 41 4e 4f 55 4a 62 56 77 59 33 5a 39 51 4e 6f 42 34 77 52 71 61 79 45 43 30 54 46 77 78 57 67 34 42 59 32 78 54 47 78 49 58 6d 57 71 69 48 44 6f 49 42 49 53 51 5a 44 4d 4a 4c 64 7a 56 6a 38 43 58 66 38 31 55 31 73 79 39 4a 54 78 62 58 64 74 50 62 6e 77 4e 4f 6e 6c 56 71 6e 48 6d 37 77 78 6f 55 54 44 49 4d 54 52 53 55 53 48 47 50 75 76 72 74 6b 34 36 4d 79 4a 31 58 67 6f 4e 6c 4c 43 57 66 4a 48 45 61 6b 43 48 57 65 33 35 67 65 46 35 32 5a 32 57 31 31 62 66 4b 4c 76 71 70 45 72 49 50 75 6b 47 6d 71 52 4a 68 77 6a 72 34 4e 55 32 61	Md3vss8nCiGzNc7blYyYfTj2OSwY4nyf1GIGoiVt1ZzjoA7n6i0ZlbH23Aha6jsZuk8GT1wCDFhGdANOUJbVwY3Z9QNoB4wRqayEC0TFwxWg4BY2xTGxIXmWqiHDoIBISQZDMJLdzVj8CXf81U1sy9JTxbXdtPbnwNOnlVqnHm7wxoUTDIMTRSUSHGPuvrtk46MyJ1XgoNlLCWfJHEakCHWe35geF52Z2W11bfKLvqpErIPukGmqRJhwjr4NU2a	success or wait	1	7FFFE0B9B526	WriteFile
C:\Windows\WaaS\services\dllhost.exe	0	524288	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 e3 72 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 3e 27 00 00 36 00 00 00 00 00 00 1e 5c 27 00 00 20 00 00 00 60 27 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 27 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.$PELrb.>'6\' `'@ '@	success or wait	5	7FFFE127817A	CopyFileW
C:\Windows\WaaS\services\dllhost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFFE127817A	CopyFileW
C:\Windows\WaaS\services\5940a34987c991	0	93	41 74 79 47 38 41 5a 74 4a 65 42 59 7a 54 4c 36 48 6c 38 6c 62 45 35 57 32 6f 58 62 7a 44 46 77 52 53 64 44 70 63 74 4a 76 37 74 52 74 52 56 44 41 56 74 6d 39 71 6e 35 78 63 4f 54 6d 37 34 46 5a 4f 48 68 7a 48 51 70 31 79 7a 65 56 6e 6d 6c 54 55 62 64 54 64 78 6c 6f 68 50 4e 4e	AtyG8AZtJeBYzTL6Hl8lbE5W2oXbzDFwRSdDpctJv7tRtRVDAVtm9qn5xcOTm74FZOHhzHQp1yzeVnmlTUbdTdxlohPNN	success or wait	1	7FFFE0B9B526	WriteFile
C:\Users\user\AppData\Local\Temp\n1eJyN2FEu	0	25	4b 30 4a 6b 4b 30 6e 41 53 67 61 77 36 62 67 32 53 31 44 62 63 52 43 62 72	K0JkK0nASgaw6bg2S1DbcRCbr	success or wait	1	7FFFE0B9B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vHbeHiYPsn.bat	0	204	40 65 63 68 6f 20 6f 66 66 0d 0a 77 33 32 74 6d 20 2f 73 74 72 69 70 63 68 61 72 74 20 2f 63 6f 6d 70 75 74 65 72 3a 6c 6f 63 61 6c 68 6f 73 74 20 2f 70 65 72 69 6f 64 3a 35 20 2f 64 61 74 61 6f 6e 6c 79 20 2f 73 61 6d 70 6c 65 73 3a 32 20 20 31 3e 6e 75 6c 0d 0a 73 74 61 72 74 20 22 22 20 22 43 3a 5c 4d 53 4f 43 61 63 68 65 5c 41 6c 6c 20 55 73 65 72 73 5c 52 75 6e 74 69 6d 65 42 72 6f 6b 65 72 2e 65 78 65 22 0d 0a 64 65 6c 20 2f 61 20 2f 71 20 2f 66 20 22 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 5c 76 48 62 65 48 69 59 50 73 6e 2e 62 61 74 22	@echo offw32tm /stripchart /computer:localhost /period:5 /dataonly /samples:2 1>nulstart "" "C:\MSOCache\All Users\RuntimeBroker.exe"del /a /q /f "C:\Users\user\AppData\Local\Temp\\vHbeHiYPsn.bat"	success or wait	1	7FFFE0B9B526	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\IEmxqChwE0.exe.log	0	1915	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	7FFFE21D8769	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C42625	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	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runteb92aa12#\5be3331dc99f83f7338fe65ac942ad9f\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	7FFFE1D112E7	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center	success or wait	1	7FFFE0B9E75B	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks	success or wait	1	7FFFE0B9E75B	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0	success or wait	1	7FFFE0B9E75B	RegCreateKeyExW
HKEY_CURRENT_USER\Software\c0c40df0fc4d1585d5de603ec4f3d9f726afeeba	success or wait	1	7FFFE0B9E75B	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Action Center\Checks\{C8E6F269-B90A-4053-A3BE-499AFCEC98C4}.check.0	CheckSetting	binary	23 00 41 00 43 00 42 00 6C 00 6F 00 62 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FFFE127A79D	RegSetValueExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\c0c40df0fc4d1585d5de603ec4f3d9f726afeeba	16211b4c33c8ccf43124ddbe6c57634ab86b6ebc	unicode	WyJDOlxcVXNlcnNcXGpvbmVzXFxEZXNrdG9wXFxJRW14cUNod0UwLmV4ZSIsIkM6XFxSZWNvdmVyeVxcWm9GU0NvVGt1dG9PUnJyZkZRclprYXcuZXhlIiwiQzpcXFByb2dyYW0gRmlsZXNcXENvbW1vbiBGaWxlc1xcbWljcm9zb2Z0IHNoYXJlZFxcdmd4XFxSdW50aW1lIQnJva2VyLmV4ZSIsIkM6XFxQcm9ncmFtIEZpbGVzIChDb21tb24gRmlsZXMpXFxNaWNyb3NvZnQgU2hhcmVkXFxDbGljayBUbyBSdW4gMDAtMDAwMC0wMDAwLTAwMDAtMDAwMDAwMDAwMDAwMEZGMUNFfS1DXFxab0ZTQ29Ua3V0b09ScnJmRlFyWmthdy5leGUiLCJDOlxcUHJvZ3JhbSBGaWxlcyAoeDg2KVxcbW96aWxsYSBmaXJlZm94XFxCcnQwQnNcXFJ1bnRpbWVCcm9rZXIuZXhlIiwiQzpcXE1TT0NhY2hlXFxBbGwgVXNlcnNcXFJ1bnRpbWVCcm9rZXIuZXhlIiwiQzpcXFdpbmRvd3NcXFNwZWVjaF9PbmVDb3JlXFxUVFNcXFpvRlNDb1RrdXRvT1JycmZGUXJaa2F3LmV4ZSIsIkM6XFxXaW5kb3dzXFxXYWFTXFxzZXJ2aWNlc1xcZGxsaG9zdC5leGUiXQ==	success or wait	1	7FFFE0BA03AD	RegSetValueExW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	LangID	binary	09 04	success or wait	1	7FFFDFD07E2A	ShellExecuteExW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Windows\System32\cmd.exe.FriendlyAppName	unicode	Windows Command Processor	success or wait	1	7FFFDFD07E2A	ShellExecuteExW
HKEY_CURRENT_USER_Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache	C:\Windows\System32\cmd.exe.ApplicationCompany	unicode	Microsoft Corporation	success or wait	1	7FFFDFD07E2A	ShellExecuteExW

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	PromptOnSecureDesktop	dword	1	0	success or wait	1	7FFFE127A911	RegSetValueExW

Analysis Process: schtasks.exe PID: **640**, Parent PID: **4892**

General

Target ID:	1
Start time:	17:42:36
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false

Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 5 /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /f
Imagebase:	0x7ff7b6070000
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: **5244**, Parent PID: **4892**

General

Target ID:	2
Start time:	17:42:37
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **3564**, Parent PID: **4892**

General

Target ID:	3
Start time:	17:42:37
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 14 /tr "'C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: ZoFSCoTkutoORrrfFQrZkaw.exe PID: **2988**, Parent PID: **960**

General

Target ID:	5
Start time:	17:42:38
Start date:	05/08/2022
Path:	C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe
Imagebase:	0x270000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
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: 00000005.00000002.392526659.0000000002741000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 43%, Metadefender, Browse • Detection: 85%, 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	7FFFE1D6F1E9	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	7FFFE1D6F1E9	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ZoFSCoTkutoORrrfFQrZkaw.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFFE21D86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ZoFSCoTkutoORrrfFQrZkaw.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	7FFFE21D8769	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C42625	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	7FFFE1D112E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile

Analysis Process: schtasks.exe PID: **740**, Parent PID: **4892**

General

Target ID:	7
Start time:	17:42:39
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 11 /tr '"C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe"' /f
Imagebase:	0x7ff7b6070000
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: ZoFSCoTkutoORrrfFQrZkaw.exe PID: **5548**, Parent PID: **960**

General

Target ID:	8
Start time:	17:42:39
Start date:	05/08/2022
Path:	C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\ZoFSCoTkutoORrrfFQrZkaw.exe
Imagebase:	0xb80000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	7FFFE1D6F1E9	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	7FFFE1D6F1E9	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	7FFFE1C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FFFE1C42625	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	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile

Analysis Process: schtasks.exe PID: **1428**, Parent PID: **4892**

General

Target ID:	9
Start time:	17:42:39
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **2320**, Parent PID: **4892**

General	
Target ID:	11
Start time:	17:42:39
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 9 /tr "'C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **1588**, Parent PID: **4892**

General	
Target ID:	13
Start time:	17:42:40
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 9 /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /f
Imagebase:	0x7ff7b6070000
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: **5560**, Parent PID: **4892**

General	
Target ID:	15
Start time:	17:42:41
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **5912**, Parent PID: **4892**

General	

Target ID:	16
Start time:	17:42:41
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 9 /tr "'C:\Program Files (x86)\windowspowershell\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: RuntimeBroker.exe PID: **1048**, Parent PID: **960**

General

Target ID:	17
Start time:	17:42:41
Start date:	05/08/2022
Path:	C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe
Imagebase:	0xf10000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
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: 00000011.00000002.507606003.0000000003768000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 43%, Metadefender, Browse • Detection: 85%, 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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFE1D6F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFE1D6F1E9	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C42625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile

Analysis Process: RuntimeBroker.exe PID: **4532**, Parent PID: **960**

General

Target ID:	19
Start time:	17:42:42
Start date:	05/08/2022
Path:	C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Common Files\microsoft shared\vgx\RuntimeBroker.exe
Imagebase:	0x320000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFE1D6F1E9	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFFE1D6F1E9	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	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	7FFFE1C42625	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	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile

Analysis Process: schtasks.exe PID: **6060**, Parent PID: **4892**

General

Target ID:	21
Start time:	17:42:42
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 6 /tr "'C:\Recovery\ShellExperienceHost.exe'" /f
Imagebase:	0x7ff7b6070000
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: **5500**, Parent PID: **4892**

General

Target ID:	22
Start time:	17:42:43
Start date:	05/08/2022
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:	0x7ff7b6070000
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: **5948**, Parent PID: **4892**

General	
Target ID:	23
Start time:	17:42:43
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ShellExperienceHostS" /sc MINUTE /mo 7 /tr '"C:\Recovery\ShellExperienceHost.exe"' /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **2208**, Parent PID: **4892**

General	
Target ID:	24
Start time:	17:42:44
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 11 /tr '"C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe"' /f
Imagebase:	0x7ff7b6070000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ShellExperienceHost.exe PID: **3764**, Parent PID: **960**

General	
Target ID:	25
Start time:	17:42:44
Start date:	05/08/2022
Path:	C:\Recovery\ShellExperienceHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\ShellExperienceHost.exe
Imagebase:	0x880000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
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: 00000019.00000002.437075791.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 85%, 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	7FFFE1D6F1E9	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	7FFFE1D6F1E9	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	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFFE1C42625	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	7FFFE1C42625	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	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFFE1D112E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFFE1C3B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFFE0B9B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFFE0B9B526	ReadFile

Analysis Process: schtasks.exe PID: **3568**, Parent PID: **4892**

General

Target ID:	26
Start time:	17:42:45
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkaw" /sc ONLOGON /tr "'C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe"' /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ShellExperienceHost.exe PID: **336**, Parent PID: **960**

General	
Target ID:	27
Start time:	17:42:46
Start date:	05/08/2022
Path:	C:\Recovery\ShellExperienceHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\ShellExperienceHost.exe
Imagebase:	0x750000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: schtasks.exe PID: **4924**, Parent PID: **4892**

General	
Target ID:	28
Start time:	17:42:46
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "ZoFSCoTkutoORrrfFQrZkawZ" /sc MINUTE /mo 13 /tr "'C:\MSOCache\All Users\{90160000-00BA-0409-0000-0000000FF1CE}-C\ZoFSCoTkutoORrrfFQrZkaw.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **5804**, Parent PID: **4892**

General	
Target ID:	29
Start time:	17:42:50
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 14 /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /f
Imagebase:	0x7ff7b6070000
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: **5176**, Parent PID: **4892**

General	
Target ID:	30
Start time:	17:42:50
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe

Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "WmiPrvSE" /sc ONLOGON /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WmiPrvSE.exe PID: **408**, Parent PID: **960**

General

Target ID:	31
Start time:	17:42:51
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe
Imagebase:	0xe00000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 85%, ReversingLabs

Analysis Process: schtasks.exe PID: **1752**, Parent PID: **4892**

General

Target ID:	32
Start time:	17:42:51
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "WmiPrvSEW" /sc MINUTE /mo 7 /tr "'C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **4736**, Parent PID: **4892**

General

Target ID:	33
Start time:	17:42:52
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 12 /tr "'C:\Recovery\RuntimeBroker.exe'" /f
Imagebase:	0x7ff7b6070000
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: **5300**, Parent PID: **4892**

General

Target ID:	34
Start time:	17:42:52
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\Recovery\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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: **1332**, Parent PID: **4892**

General

Target ID:	36
Start time:	17:42:53
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 13 /tr "'C:\Recovery\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WmiPrvSE.exe PID: **1448**, Parent PID: **960**

General

Target ID:	37
Start time:	17:42:53
Start date:	05/08/2022
Path:	C:\Program Files (x86)\Mozilla Firefox\plugins\WmiPrvSE.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\mozilla firefox\plugins\WmiPrvSE.exe
Imagebase:	0xba0000
File size:	2586624 bytes
MD5 hash:	0D32FF3680A716FD66CB9AB0E3EBC763
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: schtasks.exe PID: **2916**, Parent PID: **4892**

General

Target ID:	38
Start time:	17:42:54
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBrokerR" /sc MINUTE /mo 13 /tr "'C:\MSOCache\All Users\RuntimeBroker.exe'" /f
Imagebase:	0x7ff7b6070000
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: **3256**, Parent PID: **4892**

General	
Target ID:	39
Start time:	17:42:55
Start date:	05/08/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "RuntimeBroker" /sc ONLOGON /tr "'C:\MSOCache\All Users\RuntimeBroker.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7b6070000
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