ID: 385150
Sample Name: SWIFTS.scr.exe
Cookbook: default.jbs
Time: 05:06:16
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report SWIFTS.scr.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 11
Public 11
Private 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 14
Static File Info 23

Copyright Joe Security LLC 2021

General 23
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 24
Rich Headers 25
Data Directories 25
Sections 26
Resources 26
Imports 26
Possible Origin 27
Network Behavior 27
Snort IDS Alerts 27
Network Port Distribution 28
TCP Packets 28
UDP Packets 30
DNS Queries 30
DNS Answers 31
Code Manipulations 31
Statistics 31
Behavior 32
System Behavior 32
Analysis Process: SWIFTS.scr.exe PID: 4104 Parent PID: 6036 32
General 32
File Activities 32
File Created 32
File Deleted 34
File Written 34
File Read 45
Analysis Process: qtfarawjob.pif PID: 6132 Parent PID: 4104 45
General 45
File Activities 47
File Created 47
File Written 47
File Read 48
Registry Activities 48
Key Value Created 48
Analysis Process: RegSvcs.exe PID: 1972 Parent PID: 6132 48
General 48
File Activities 50
File Created 50
File Deleted 50
File Written 50
File Read 52
Analysis Process: schtasks.exe PID: 3120 Parent PID: 1972 52
General 53
File Activities 53
File Read 53
Analysis Process: conhost.exe PID: 2404 Parent PID: 3120 53
General 53
Analysis Process: RegSvcs.exe PID: 5864 Parent PID: 936 53
General 53
File Activities 54
File Created 54
File Written 54
File Read 54
Analysis Process: conhost.exe PID: 4908 Parent PID: 5864 55
General 55
Analysis Process: qtfarawjob.pif PID: 5900 Parent PID: 3440 55
General 55
File Activities 56
Analysis Process: RegSvcs.exe PID: 2932 Parent PID: 5900 57
General 57
File Activities 57
File Created 57
File Read 57
Disassembly 58
Code Analysis 58

Copyright Joe Security LLC 2021

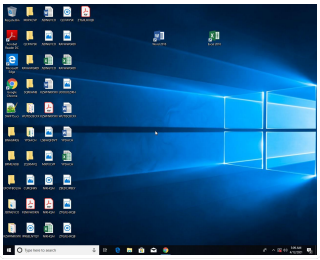
Analysis Report SWIFTS.scr.exe

Overview

General Information

Sample Name:	SWIFTS.scr.exe
Analysis ID:	385150
MD5:	0984d8481d809d..
SHA1:	be4bfdae2830859.
SHA256:	f2597b91433ba86.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

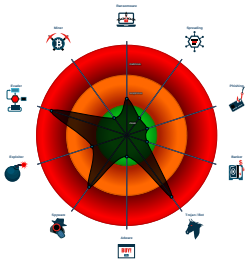
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Drops PE files with a suspicious file…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Uses schtasks.exe or at.exe to add …

Classification



Startup

- **System is w10x64**
- SWIFTS.scr.exe (PID: 4104 cmdline: 'C:\Users\user\Desktop\SWIFTS.scr.exe' MD5: 0984D8481D809D2715214D220D5F3224)
  - qtfarawjob.pif (PID: 6132 cmdline: 'C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif' odfugpcmco.org MD5: F471B7C16D5B01AF9F67F5F4A921F81F)
    - RegSvcs.exe (PID: 1972 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 3120 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA342.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 2404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5864 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- qtfarawjob.pif (PID: 5900 cmdline: 'C:\Users\user\AppData\Roaming\89378384\QTFARA~1.PIF' C:\Users\user\AppData\Roaming\89378384\ODFUGP~1.ORG MD5: F471B7C16D5B01AF9F67F5F4A921F81F)
  - RegSvcs.exe (PID: 2932 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7f972ccd-f2c1-42af-a77f-74adb4b9",
  "Group": "EGO OKU",
  "Domain1": "ekuro.hopto.org",
  "Domain2": "127.0.0.1",
  "Port": 1980,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9dd:$x1: NanoCore.ClientPluginHost • 0xfa1a:$x2: IClientNetworkHost • 0x1354d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf745:$a: NanoCore • 0xf755:$a: NanoCore • 0xf989:$a: NanoCore • 0xf99d:$a: NanoCore • 0xf9dd:$a: NanoCore • 0xf7a4:$b: ClientPlugin • 0xf9a6:$b: ClientPlugin • 0xf9e6:$b: ClientPlugin • 0xf8cb:$c: ProjectData • 0x102d2:$d: DESCrypto • 0x17c9e:$e: KeepAlive • 0x15c8c:$g: LogClientMessage • 0x11e87:$i: get_Connected • 0x10608:$j: #=q • 0x10638:$j: #=q • 0x10654:$j: #=q • 0x10684:$j: #=q • 0x106a0:$j: #=q • 0x106bc:$j: #=q • 0x106ec:$j: #=q • 0x10708:$j: #=q
00000002.00000002.593935065.0000000006F20000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
00000002.00000002.593935065.0000000006F20000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost

Click to see the 139 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegSvcs.exe.6f20000.28.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
2.2.RegSvcs.exe.6f20000.28.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost
2.2.RegSvcs.exe.34c58f4.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
2.2.RegSvcs.exe.34c58f4.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
2.2.RegSvcs.exe.6f10000.27.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
Click to see the 186 entries				

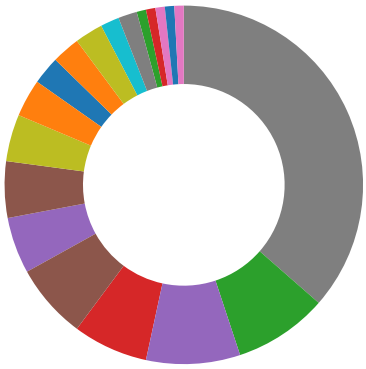
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

Yara detected Nanocore RAT

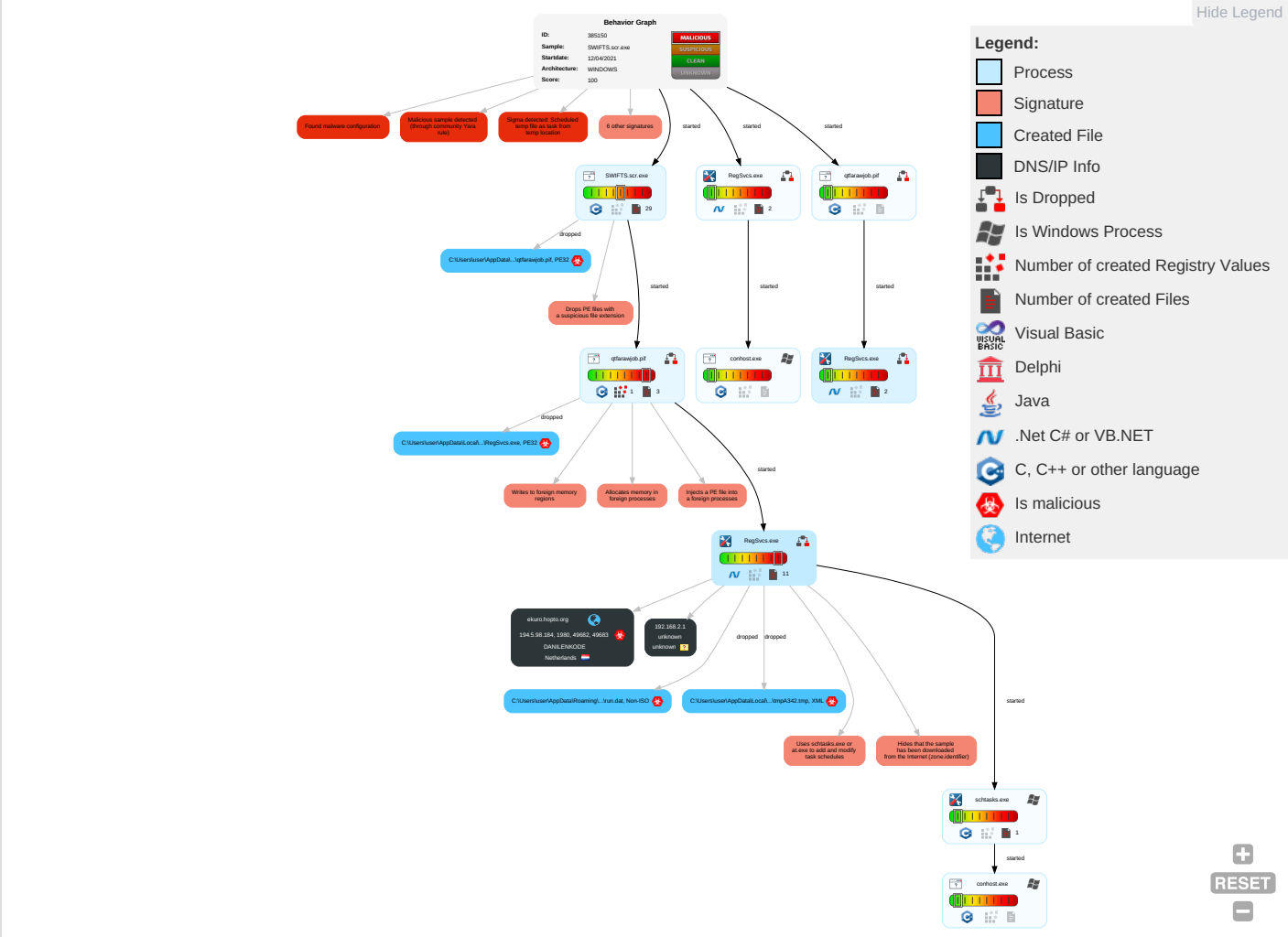
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 2	Windows Management Instrumentation 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 4 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Valid Accounts 2	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 4 1	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Valid Accounts 2	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Access Token Manipulation 2 1	Software Packing 1 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	DLL Side-Loading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Scheduled Task/Job 1	Masquerading 1 1	Cached Domain Credentials	Security Software Discovery 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 2 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

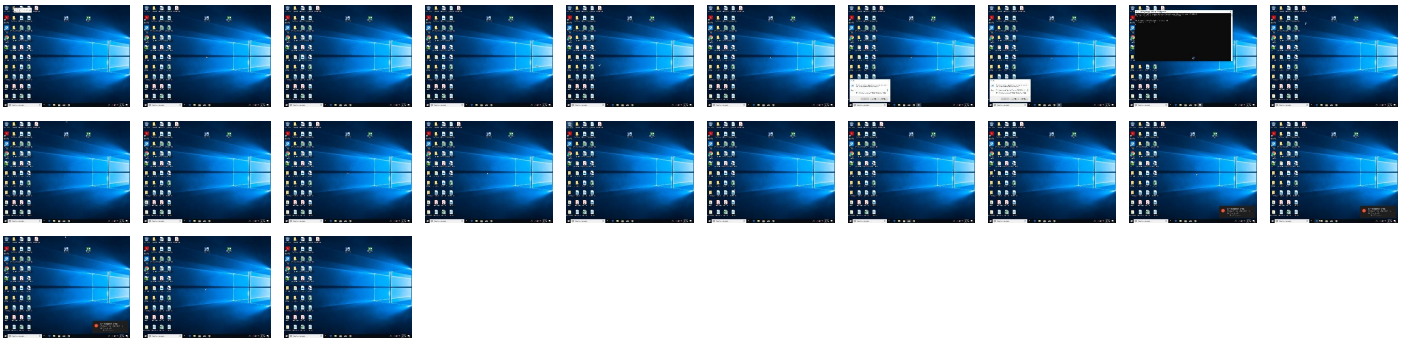
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.a00000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.RegSvcs.exe.e00000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.RegSvcs.exe.5f70000.21.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	Virustotal		Browse
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	Avira URL Cloud	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	Virustotal		Browse
http://www.globalsign.net/repository09	0%	Avira URL Cloud	safe	
ekuro.hopto.org	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ekuro.hopto.org	194.5.98.184	true	true		unknown

Contacted URLs

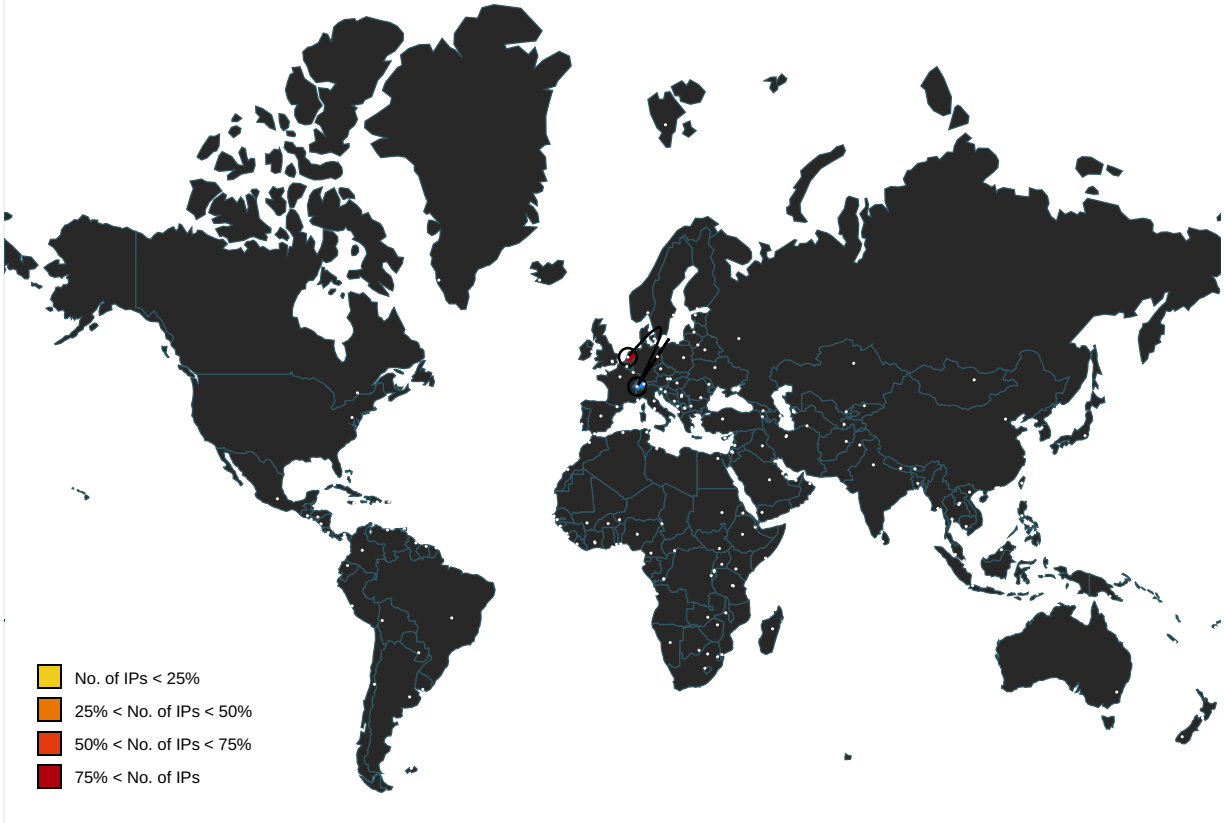
Name	Malicious	Antivirus Detection	Reputation
ekuro.hopto.org	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://secure.globalsign.net/cacert/PrimObject.crt0	qtfarawjob.pif.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://secure.globalsign.net/cacert/ObjectSign.crt09	qtfarawjob.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globalsign.net/repository09	qtfarawjob.pif.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.autoitscript.com/autoit3/0	qtfarawjob.pif.0.dr	false		high
http://www.globalsign.net/repository/0	qtfarawjob.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.globalsign.net/repository/03	qtfarawjob.pif.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.184	ekuro.hopto.org	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385150
Start date:	12.04.2021
Start time:	05:06:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFTS.scr.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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Copyright Joe Security LLC 2021

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@13/32@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8% (good quality ratio 7.6%) • Quality average: 77.9% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 2.23.155.232, 2.23.155.186, 205.185.216.10, 205.185.216.42, 23.218.208.56 • Excluded domains from analysis (whitelisted): fs.microsoft.com, 2-01-3cf7-0009.cdx.cedexis.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, a767.dspw65.akamai.net, wu-fg-shim.trafficmanager.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.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 NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
05:07:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run WindowsUpdate C:\Users\user\AppData\Roaming\89378384\QTFARA~1.PIF C:\Users\user\AppData\Roaming\89378384\ODFUGP~1.ORG
05:07:21	API Interceptor	932x Sleep call for process: RegSvcs.exe modified
05:07:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	9pZezwiVaz.exe	Get hash	malicious	Browse	• 194.5.97.116
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 194.5.98.250
	n4CeZTejKM.exe	Get hash	malicious	Browse	• 194.5.98.9
	New Order request Ref E100-#3175704534,pdf.e.exe	Get hash	malicious	Browse	• 194.5.97.14
	PO-#3175704534,PDF.exe	Get hash	malicious	Browse	• 194.5.97.14
	Evgp2DqQha.exe	Get hash	malicious	Browse	• 194.5.98.107
	Payment Copy #6578965432.exe	Get hash	malicious	Browse	• 194.5.98.52
	PO SKP 149684.jar	Get hash	malicious	Browse	• 194.5.98.48
	4EPXPkicIL.exe	Get hash	malicious	Browse	• 194.5.97.158
	xoxd454e9q.exe	Get hash	malicious	Browse	• 194.5.97.158
	1VzQLgPeAlfHSHQ.exe	Get hash	malicious	Browse	• 194.5.97.214
	XJ1lVmdiCi.exe	Get hash	malicious	Browse	• 194.5.97.237
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	• 194.5.98.182
	Revised invoice30032021.exe	Get hash	malicious	Browse	• 194.5.98.145
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	• 194.5.98.182
	Vp0VO1U2oo.exe	Get hash	malicious	Browse	• 194.5.98.107
	IpEtbpwMpM.exe	Get hash	malicious	Browse	• 194.5.98.250
	LOT 15 - Transfer Manifest.xlsx	Get hash	malicious	Browse	• 194.5.98.250
	2df27f1a3505dbd0995188d49c253f5bc53c0e994954c.exe	Get hash	malicious	Browse	• 194.5.98.107
	1AQz4ua1TU.exe	Get hash	malicious	Browse	• 194.5.98.107

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	J62DQ7fO0b.exe	Get hash	malicious	Browse	
	HSBc20210216B1.exe	Get hash	malicious	Browse	
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	
	bank transfer.exe	Get hash	malicious	Browse	
	nunu.exe	Get hash	malicious	Browse	
	quotation.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	UPDATED SOA.exe	Get hash	malicious	Browse	
	comprobante de pago bancario.exe	Get hash	malicious	Browse	
	ANS_309487487_#049844874.exe	Get hash	malicious	Browse	
	Dekont_12VK2102526 VAKIF KATILIM.exe	Get hash	malicious	Browse	
	taiwan.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	Payment Advice.exe	Get hash	malicious	Browse	
	Quotation.pdf...exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	

Copyright Joe Security LLC 2021

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D0 B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: J62DQ7fO0b.exe, Detection: malicious, Browse • Filename: HSBc20210216B1.exe, Detection: malicious, Browse • Filename: zunUbtZ2Y3.exe, Detection: malicious, Browse • Filename: bank transfer.exe, Detection: malicious, Browse • Filename: nunu.exe, Detection: malicious, Browse • Filename: quotation.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: comprobante de pago bancario.exe, Detection: malicious, Browse • Filename: ANS_309487487_#049844874.exe, Detection: malicious, Browse • Filename: Dekont_12VK2102526 VAKIF KATILIM.exe, Detection: malicious, Browse • Filename: taiwan.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: Payment Advice.exe, Detection: malicious, Browse • Filename: Quotation.pdf...exe, Detection: malicious, Browse • Filename: PURCHASE ORDER.exe, Detection: malicious, Browse • Filename: money.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,.(....~....o....9]...

C:\Users\user\AppData\Local\Temp\tmpA342.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1311
Entropy (8bit):	5.096491999374021
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Vakxtn:cbk4oL600QydbQxIYODOLedq3Bkj
MD5:	61B1AA63000F5F8ADEBA5BDF446B86BB

C:\Users\user\AppData\Local\Temp\tmpA342.tmp	
SHA1:	31771D1A80ABC92944BD4A9911BE9C1DC8A23C7E
SHA-256:	2546B14C7A9400557DE43FD855BA4A09A96FC1780BAA32AEE5BC2C22B4DD022C
SHA-512:	78DC27D462B0D41D190975D9515E50E50D39063C9DEF877652E16C9091D0C67004945F7B6D414F83EA2AFDD8B150890451E06D142A5E54F6DC17724F1D60942D
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\89378384\ajwiqng.bin	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.577187279572449
Encrypted:	false
SSDEEP:	12:jLSFYaDhiinTz2ZaDUGP35mfEUTQv/sReYpo9LbpRXr8I:QDhiwTe0zY0VBbpJz
MD5:	96690BBFA85CA3E6131B8E8CE455E2DD
SHA1:	800AE71F3FEF2A123342D980E9F40F5705477B45
SHA-256:	A297ED796C37784A40430A3B0A03A299040A8F3D98BB728A34DA8E09F5123276
SHA-512:	69C657B11AD791C4C1E23BC8F3F81446565DC5125963118D30B80BE34AECB0227AECF8FBF190F1976ED176691D809F61FC014902DBDD95EC30B9FE1E2F55CB 3
Malicious:	false
Reputation:	low
Preview:	SEr6WCVm519gXv52S5n8jMFzRI90eY2d84t4k9NVRQ79F0Bz52lv6EMRwO7f302QeR1hQO..3y96u0A54pYz96c114r3F91A8bVWxZ01xbiEC5vW0V2qIV7PMu1802TkLv6W2988otNZ22U8h1998o8rf821010221rJ716i..6GC9OzFPbSlkFYS2448b8O2ag43nZg9t73Gyf1nU69C6V33S4FGQ328rzj17y9J1R2r5020d665Dnk44z20p10Qz4Segio3g03eMbXN6a6a16i7z0a96p66Ms9K8..xh94TqQDfx35Nfr2WMhu73k174VgCokH2N1GwM225VN7832idvs9808Z51F32Qqt4V4ge50ib6b62M529H21fLpAOx94338S4648P4EIKp8Joh9rdiQ5u..o9t2EjecJ7ZfRh2499EZ196M30ze0LB13yay80g27aHWn7E0E1GIL748A7QB43CJZM2kSe319nS4fPf8FHT4P48BVnEDGFS48j052qnd4M9mc878akOm2C87F230D4j6500R86..

C:\Users\user\AppData\Roaming\89378384\ckcsljuf.txt	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	570
Entropy (8bit):	5.462095602197949
Encrypted:	false
SSDEEP:	12:bh3te9cIvgdPsV37WMqcQyOm+pX7Z+/8vA3vW0PDnovn:bh33Iv8sV3PqcQyOmJn3xun
MD5:	E83757A7EBD5201586D5CDA68BC0BEF7
SHA1:	FFA8D214260A5507C886558C9B3A2557E34D425E
SHA-256:	3D6CD22B560546BF0929D4E15F493BD420859E4F54E0F6E3B4E8973F99852687
SHA-512:	458C9E23216608B93FE9D108942AC54DB2D68B0AD2F1A7C77B48635EFF27BB8ED21760777E20741F644036104694F7F85BA632AD15C3AC1498F3E7B882ADDB8
Malicious:	false
Reputation:	low
Preview:	wrp3bm5cl9a1YWHH8ZMxT4v..423dQ512U8G147uOY2Z7f9PFK9670217ewXUgfzk8xhn27539bqlkC9ZQk53O564x26X1z36CuX3..s6A45v9a0F9309rl0K9u4maJ0F3R2Pk0566i081Tu19Hq2705Z5Sas9t..81F3057v25410143475iZ5J0242Ku5S0jf25WVM8v511l9g21mr6p031907XR08h42dVeLir3L6jB3WDJs3q42w40rBs4a2E22aM8S341IR0o19h8927781Pg9Npl857245o3nfZl047K6lUmFi17z..2HXLJ8V4004dfQ2yMMF177fyVB7Y6228KS7I1Vb153987Abe1402601704945s0YTFe74o3g691JE9c6YK9Se2E432hF40fi58YIS99GN580bktoe404n..L519453F38w5r8j9ryGV84dg138i38985R81DE79KD..A12WM5EAMa4WV6081X5l1g38wscE8w7PvHBVQF2j88Z48P80YL707DQEJ4262MX8f27VrtC27T02MT0W4e7mG7301H76..

C:\Users\user\AppData\Roaming\89378384\crfgiqf.ini	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.432323738929293
Encrypted:	false
SSDEEP:	12:M8wnoDHtPkUsEJgHkywOwSsrxOyVySPlYCZfsgsdG:aeLsZE9Ow3rxBADCZfEG
MD5:	23566124F507E82A5A885836EDB695A2
SHA1:	5D38583BAA7DBD138CE8835D50D64BAC17F8CD2A
SHA-256:	8A6B557B093C17C8A0EAF31E3649A9DC83E7DE1E77A2133718C812418981B0EC
SHA-512:	437D18CC71142321831540B9CC95063898DC2D3BFFEB019D002474C680E4B185690924605F3746CE7F67C831E7192C6AF3F65E50CEDC740510DF4D827167DAE

C:\Users\user\AppData\Roaming\89378384\crfgiqf.ini	
Malicious:	false
Preview:	es94855rt4O9mUI6137254725e7Sr6M79g26bO0qd15..Cap293h8t0Ht9p60933ghX40zO793350o7yc581525f0j29Ebvt2GV390136o7j0h90X72W5X0A6eq914b72V 4h79488JZ4i21Lg1h3H059o0898F17q59U578w52Ag1pUL590T7hu39d2Q219y..gV6ZM8v7Nfu24sqfur0W41E..hVN8V109s7tNn9J3G9Y07d280R70qu0EfDEM0pZOi ..rnuQ9G58r2k17an3EW9616S47s775Up0J1mJ4xV9e6c6869j064m44av80819727gfs64PMcnWPo2ClL8dypd155eQl5G2349Z8zng32Pd4VWfNS6v8tE7G027Bm295f 1YDJ2y0zX57x3f93..6z900Gu8b1MP30Nj87UDZ3cK88Vxc2w2A190358S41F5kHw86643Frhw844j40V26c69hu733h63MM5j4kG544imB42c5m4YL19qeOSc8P39gDA4 QZZ98V..

C:\Users\user\AppData\Roaming\89378384\cxijg.ico	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	596
Entropy (8bit):	5.513841828081032
Encrypted:	false
SSDEEP:	12:oSD1Z3dUc5yVe+VE+ZIV47v23xgFFYh+KrVIJVlY:oGXdRygJSMxg6+pJVlY
MD5:	3A2175769609498B68B21C91C1592CBF
SHA1:	150166C7F5F211F65231E784CBA68F740B2A5FAE
SHA-256:	53D5311B18DA2BB40832BAFD877A36224ED8253DF947BFF81A3ABEC75F216CEA
SHA-512:	C2BD5344EB62494CCCE463ACFD609FD4004527429EEA3073247BBC80CC901BC4846479D43D7495BD37F40FEE28D9315FC1DC4A2D8F361DE951FFE4C1FC0FD FC
Malicious:	false
Preview:	n12Tu85KO8P7g822OZuQ5qf53Fnqr39g00e59KN65897708a2nu2j4k2Z1Qx04um786h9U3UDzVShP3023Y76cwvv38NuN1z68538TabdH6859lX9B09WNEy96q86sMUB9 b81L065Vh1ULD8G4om3Ym661DY11f9uUfVtub8..vX61Df276G2GW0J11lBd1l19DX82z337o03dx3o2LC66jx1z9615Vx5Abu66A7F4SgOHN2H0d9e3l1yTcw72PPw..u 830g95iU66nJ3Y4bJyM0qA..v813xZ8vL40w57GMviw5229183dZmi32dIzf977aK584RCcz382q9909869U103..Z1K5Uw61l8988l17V2zo1GTSg3h1oN44639wOIt.. c62mvv3U21bnPG980463M718082..2WqM8bI96A3Cof4v16i00Z32hhtZhRD38fxQD8..c82F45NagU94d92jhIB12xXN4k0ic90b80EQ3y7G2wri7eWFm62Biv8a3Pnf4 ic7D5183hL5148uwd5i7392zU4J0q45e04mKEsq5G7X1m1a2O11U0z8umxX5AqV6Q1hb6793F1..

C:\Users\user\AppData\Roaming\89378384\fvltkxlub.jpg	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	529
Entropy (8bit):	5.559152430474837
Encrypted:	false
SSDEEP:	12:ucBsfeejVkIdQhYHGjGKXSSpAebQ2pyPIc7raPeo4L53dTgThOw9n:ucBsdSgQhYHcGKXSAa2p4eeFXwhOw9n
MD5:	B6556F044811B2C8F7D4CA3DBFA66126
SHA1:	62996F61B47DCFD5D95D47EFC8D5FA855EFCA0AA
SHA-256:	C93F8AEE15C3A7BE1A4FFD3865E9C2EF534EDAE06DE6C129B221417F1BE35EA8
SHA-512:	9B213424CE0C98359FD4C3C784F278AAB514E660B277EADBB8B1581114226741A633AB9827972882FF72250DA0308BA639C06B3853D638D1B805FF74AC9316CB
Malicious:	false
Preview:	T1xbKVWxk26W6Zvb33L7n60u0IMP1jI237Im383kP70ahX74oQh08803Cy0hlea6VuRON4KEH5e58R8..2C241brD954o15yku1S21xyDIXny27f92302X0o9x9u5g88Sg 0a0C4Gb36e40x0xg105604VkY04AOOU02..k6M6yer0m0098BD5148Ywsfd55p323PvwKf7..835T6g01XV4pl88LI9o22Y591hzHO09024BJuN727n4nKU7JjM9J2Lu9n 1w69NGPt53FW4R9..0H55Plg2l15..Tspp08NT98I8D2o41m38h10K0219Y35E8AU32rqkr7x8wye2w311q03O4bHS43978G7q8545lHX1o3T7WYtr4NEfG2p5p78Z8s0P 6EoD238EBb117..88qH567am4GgdFiXOJ63A24z..wE32j1563WxRz824O5llj3AnC0A58heDhRTd955w22X86zZY8F7UoG041964FD0LRF31d8bQ792814nDGIJCo17FV 3APbL6c..

C:\Users\user\AppData\Roaming\89378384\gencjb.ico	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	534
Entropy (8bit):	5.4724932938444555
Encrypted:	false
SSDEEP:	12:Xy+Mdvok6YwUZhhVXSKqZgDahE+AGSb6QgzuIa0Pv:CZAMFhDTRDahE+A5bGMa
MD5:	19D70FB9676D949E164957896690110D
SHA1:	AD0DACF83D0493D394D3B0AD13BE389E29DC1C28
SHA-256:	D1C6EEDE5958CA88872235C6C1D93C9EF5D16878E7C84AEF20C2FD8D2C2F4E9F
SHA-512:	4A3223F9CF62CD906BC2E3F360BC0CA6E8AB2C8C6B65EE48BEE91943385408DDB1D7D8795393485B47B9F3E1DFED5518B75DBFEFCD0190ADAC76904124B79 7C
Malicious:	false
Preview:	818bW6z9gcBy74p43uWf971B67367t2FqTR41..9A20N8JLtu9I90O2108B8Fx2913333r3GQ334B7b221sO3KH9uE601i30l386JNI03602F0Rd28agOGF9XM3..7723K L445j5h24j4F80x8885Y42Y9N17x52TJ2j9rE4MB4h48f84076P1Vo0y83530hSp2H0g9tKwU440M53mJw123Z2hnGtB10975Zh0Z9V69v4pu8zR4S3H8P2E63jUe7LOl9 t0SrF59657y..6RA1M9352K3C9R6YoBz3M13WFCzb38amc4p74cb445c2Qe61gmXF59xQ5ggO665265Kq7i1avfd76038b5FV3DU1t32y240T9yIiI85Q526EO491E7i0C 420h75J..122Urbq37J81pCXHX4cuv1C61zJv857h19uM6m3x9NyptND9mb45G1pvmB796R9z00U4R77Pvb910U41724YIDo2768s4McL0XWN5M9AK5d8Ku0 7PU7No1b8G6k8n5Hf4EyeU..

C:\Users\user\AppData\Roaming\89378384\hwbmxx.dll	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	504
Entropy (8bit):	5.493963089744754
Encrypted:	false
SSDEEP:	12:pFGSL4sZmygfWl09BglWhX2t1fYeWBAQUIzRz8SDpa/CU1JRgraR4DF:pFksjgI0L4tBM3zFh9a/XLRP4h
MD5:	5457DA4088B48B18E4F8EAFEA201713D
SHA1:	C239D6F9BB6414DD850BCB75CB0DBF40AC234EB9
SHA-256:	62054307C143635C361ECC57C58A7970ED39498EED84485D115765C47FAB23F3
SHA-512:	7D035A2E8C51E6F343CAB4BF380CA37DF97F62D180745774C87A03E17138804443094ED44090B90474CC2A135B65839BCD495C5AED1CF558466188BB76137821
Malicious:	false
Preview:	96o7A0DuZ2D960txm8A1T6919731272aiz0e2Ej7uEYR0VG7ZXP90FH6g5O04JXA4z0t458PZZlk1Uk0H7po210DGPh70G1..j559q6xLB9GRpD7I..xki1D63TCC1Vo66 288hw5E6s8R56L272b41bv05Egdv24Ir63..Ico0dd9ad0Fvn0863a31S202z1e93KNFA69A85K13wdY62Yshw53LJ762i7Yr6Cb1m681q9FHT0Y03246LW84V03GO5x1W 0344rnCW53RD4Z8d0P4AKJr45918Kap0k19QR4Piv5j90s86HV..8W74w50ij1107jK70U9M3M335r2k4x1F9AA708Prum2tLoUEK4uSic6I874304sgarw8t274i74i92 67L810S..1qNg0s2rr5076jE1392F95OwXiMvGS4843tR15A7qhm6MD..M86e9f5zv8g6509226dAR34o0EeZ4uq7pRY4t8767601c928m8NZlM3..

C:\Users\user\AppData\Roaming\89378384\jlotan.ini	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	574
Entropy (8bit):	5.533885609378276
Encrypted:	false
SSDEEP:	12:sDN4Bbh2ZTZdX+U/EeQuQ99dOKMkaUpianCNic:nb2dXN/U3MspianY
MD5:	CE2680210226A652203FA1EB5B67AD10
SHA1:	2C40A04295588E353F8DBCE8DBEF02DBE45C90EC
SHA-256:	835BE0A24E1CA0321101AE5D66F3873A00B82680320148D27EC163A216FEA010
SHA-512:	C8F881E9DE01FE0D8E61349CFCF4A68E1C83A92943D2036E5435403633D4B75F8BC9665AFF7DFA13670F06A20BC015FD38851C1211E3F280C5821E0618681303
Malicious:	false
Preview:	6119v07LC8L4JA5DR0ABN637zwW0dt2..HJ3W5c94o2K5kO70h2HW5D2H03LsbE2BiEk3uL0x8..6SPa66TS56o8J0k1c44Gx413364CM5JG8DT30883e1404u9n08v625 341017Ni5yd5pYkb418t111242SA1ajg012Y7Oz010ayVk23nL23h205289Wf368..0C65qkW500U0T2NsfQ517D8z7n4m..aS969s3yyXu810UEM92LZIqKvvI0s7sBt2 48Ho9yIWR7Kd0CuJO7SCPinh..h99yse6JV680OSgijk4jmV3R1BK3OR8H48u71Bb245LQq01zZ91TJ277EZ822p6..q5DFn950A8MYdg292J8JJ4zGy2MtU3Z1VR0F6G0 493kKl8t825N74T1557O87w0y3ML6e0R8B5E89hHN55y5q93tYp260GM489Ef80AsiF96L8mKq..0aX25701c3rQ0KxP1O0m33UaA7e9ghY724I7LG85074SM4597A9AM0 mU306062oL1Dm4FJ06UK7F5037V2jhwf4fn6uL97r12fMjjAwU2O..

C:\Users\user\AppData\Roaming\89378384\ksbjboc.xml	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	627
Entropy (8bit):	5.433173452980452
Encrypted:	false
SSDEEP:	12:oV5ntosObqszp24HXMSxGjjHCiRpO7PtaySpAPmbRoc8koup6TDOn:oV5ntAbtBcSUniiyd2Pbakb6TDO
MD5:	FD3665C28A5AD4CD7AFA2D37F6A2A013
SHA1:	73E8ECBB23CA1DA919528D358BC1865D42DAF60A
SHA-256:	5D33E12D3BC86FEE648E7A0F847A08C74A1CDBC1B17EBD723D9E8A0B7B2C3731
SHA-512:	04921991551F53B20811E9E71FAEC2A50F0C62F84EC302A38FC0DFA4C569DE0C1A7624DBF93B6597B1F7D9AC7EE388BF594E8E8275A0B5B9760321D72194CD2
Malicious:	false
Preview:	2Y6YB5972Q045mz3q37P2h8e4l375zO288b8489..w875u4920N6LY1Z4y8y4aHXz9Q939hezE15j4v65vr1UUz6hr3U884T5S8..h4299Nc316z1Y..3v1F..9h1Mp8o2 i78U316e2tzWvUa07gn9Z6k77l9377K1wrqc06baeqM..81Te2uWs4xvr1B854zjr2JXAKqYS3E..6577zHUe3x1T16w2l05pT24695J30dxL6289I33LR3RArz97i89N6 5g5D23ul1Cq61o33ruXA7X029B14Bv15cY226QS546wh5C0X4C7u743oB5fsY7G204H4v06YF968X3p28N8399L6MN451lq0mF2sd21do53Gf2VR25p703l2..09G841Up L1t2K96o1486c1a3rtC2o62fI893Y5680J943V140Ko116Y9F3D278716U862773qwO9Z4B266HmtD4rZ8Fyr..07i32fEJ8429I23Q431982327b23Fb7NWQTQqL9122d 8icuC994t1ANkXe8D0J2n19yy9KZlK217E9S3fNnda467qp0vR6YPAM8I2y727zr13R8g4Tzv849e56w811QV80f60se2W76P46jYrS2h..

C:\Users\user\AppData\Roaming\89378384\ksfdlrauwr.mp3	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	563
Entropy (8bit):	5.535718601608044
Encrypted:	false
SSDEEP:	12:QTHBJU3HGtRp21fMT4HvGsF4Yz57QidfnrSnelRjW7WoiY:OHImtD2lG4PGsF4IRpt677z
MD5:	ADCE3CC91704D3F8F129D799534DCB7C
SHA1:	70D31CFE92A031230BB629A8CAC8827ACD2EDA48

C:\Users\user\AppData\Roaming\89378384\ksfdlrauwr.mp3	
SHA-256:	2D18AA7B8C1CA86C08EE88F4744FD2FE19E46FC05E5262D52EECE73BE58D3D35
SHA-512:	16DA313E04B9FD5FA22EF6ECA6C9B3AECB3E4A7C04CA2B4A4578E05E2BF9216CAA9B927DC29C4817D6CB316DA06D3640ACC150E91F2DD5C53EFABF6160C6CE97
Malicious:	false
Preview:	1V69RYo7Et31RE4ET1678uBh99088Y3g44R169d69wxQk9Amo5MC11N..712c904a7oZVNGyu86LjcS3H77k6b5dje36F75AV4Y3987GZ07uZW6RZa3P0C0h Q1K2k0Q4gzK6l3..KFb3a41D6C66Ouvl1b0BwOX24v08TbX289L716Jz9HZ0S6NDRKu84rG9UT2681KgymGR3PY3nO4i6Xbdsz8018it64WE100AxCdKJZg2v2d0..08H8 dmh6E7GZ5sg8761K14b232540i2dusB65h0594otn11Un69r685k6v9yg355Ppqd0fY32A123s1bLI7vJi6083110cz0r097952s0q8a8lB3c5l5v4yerR5S3OLM565E74 7101J6W73iO04..10ER1aPQObta1352z63o29112y1S8B2YN0LM3RI60J90b2iXz4k0giDuTiJ62G7i6v5q9Bk65R444P4qj1zMC2PvFkhYU4835o..e97cz5X26g14j3M sA1R25BFyt2785UB2S06tnt276p8d4PZIa08q3er24s7Qm6V020..

C:\Users\user\AppData\Roaming\89378384\ljqg.dat	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.531138280612808
Encrypted:	false
SSDEEP:	12:r9n4zfKK9+9JihjMdzXhNUjvaHwjdSdcQDoxufi7Xwm7wzvaf9WaIzi9sw/AQerF:10K++rzdVNUsOdbQYQi7XvwDaEasGIQs
MD5:	C733796CBDC744AD5A3185CEE4B8F924
SHA1:	72E1D7082605BD623E4BA26264EB7D826890594D
SHA-256:	44522886B7DB539DD03FC01520B541484494EEAC15CBC0868AE2E9CFDEC96C64
SHA-512:	2909D444D7C028852B3BB4EEFB30BC08E4BE89D69CBB23B7701D77EF15550059A19A7F02B75C1521499D6F9D6DA8D1A6E90F90CB25E12E21009A9CBD85F7BB4 5
Malicious:	false
Preview:	bQ5OGrjz4NOg2LXZvR0nNN6Et2aR1n89i44R518n8GVM5E00b92l60pT2z1Lx4oHu0A44ZyHDHZLeY..uK6rNlxE3WhL8pU95Z3x9P1yZjdH5G020b2sr820tm8S12wwd9 26KY633C7S0jQ54i0cj650w8p..8ZR92S43P444dLie0ltFYzwdP0elFRVqx773x77AJ2j802236470gF0A4K57tK2Yq02H2zw8l2rs0613ZGnJroJ74r560Qz..4cA8n8 89fmY55882ya8pABF2SA1s5T2P964fSa3v6G606rRHbr3cP275H86Dz86fp05j6vXJ5086Sa9vL7ocJ0s3Zz6rU1jo6V5uczH98..p4K6MmQw3uHV2OX39826w8E922N8L 088d27BjPl2l8h..25vo51v2c50jz998xF5oEGV58..29TyeV42j8Z71EL7w38Bp9bVKc1DJ26t3T3f021951621285u970w215Y3eVdOaw79PUF778e6JIT723RFD0120 N7c92597237Cw5xR5MB0cK4n2qyz10pv6m8e77c43z1YU50NU54S6Z35DG3yohY8us7074X8186JSLu..

C:\Users\user\AppData\Roaming\89378384\lklphvrvl.dll	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	474485
Entropy (8bit):	4.406207301813423
Encrypted:	false
SSDEEP:	6144:7g79IKy0B266k1tvpN5KinwYBrFSKrQlTKLJEdaLj1PUbq786:0fyH6n1tRN5KiwYll0lChj1PUbU86
MD5:	42A8B623A2CE95FCEF78600C98D10194
SHA1:	7C377211B176A5648F67DCB316B105EC4002D1A4
SHA-256:	67E831370377703A709D9C19AA91DEB997AC4A48F0627E5F1656CDD773195C5A
SHA-512:	1551C857309CD0CC1E790863B2F66D13DFAF93EC52CF75BE57B75C0530B541EB7636CED9ABF0A6ED159D51B5FAE5B3273EF60C1B992E7EFB555A389C160F96 2
Malicious:	false
Preview:	9322J2lO38892691Izr5RN27cSe09t9O251j0KT59323qCTk..042HJI2k4q4Cq34bQsnRi92qba6WUq9m874ldS3X29424X0AFo2T535B98o99030GpB6..3cy8Atz247 hz8Y4wdqRM1D28lU0WJL..S22E7490neW8ojls2K6HK8853j8V1RdC868dl41m0t8C628i0D9BW8GjjoU8..sK7t409952P48496tT3QtNnJm48G37B6enNX94Y26h9Zvw K409154N13fqcv11n..wc94bF3Y746bQ7I47a5OSZx5m55Klw12271lo8Lx7w823cglPt67C8K2hs14hD4n1703lU9zJR6m556g4K15nlt1T5Z13o50E7M..668yH777Is 078a0fY818sou996994y803Ie87145CE02G15b65sv8yK5n45YpQ279X..dp7y76n71L25Am308Si77VonH480G0MgBtjp..9G0g9pm304X996gA03Fpgt6Pm9VGY9YwFh 0573YA4l136Vdo92GW9..6Y8jG5n56Cw2mapS74RJ846V790d5P92430RuL76l6US19PBZHB0ER6g77oM9fC111829f3F63124981jlAO065nL1120oh3..LgV40GR4kQ7 QGM3k5p99Xs564fTjDMAaYRiS043l47..32WCO8cb201FO48g74sK12Cl7C1L4e7kf3Zx4XKUS0imG8JxLm5BaND7q1W1en9E5p8859t8831ex5629VDl0..EGQ57Lw197 S7G5Pf148834W4hW3vdG..ZDI7F2TY84276xDb034wkm5J9zA6i597U6EUl773tc1..zi8Ez6P888M6Q5O8l96yh3c37W5618N..927k26150E63Y4308Dvs78Emi7143L 46W37A09RqB8YqD38v4289VVbai2SjnTO..6Q609A9276278805gV67zAx81eLlojXq0Sya25I68RknCY..6sOAT2l

C:\Users\user\AppData\Roaming\89378384\lpiuchwp.xls	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	534
Entropy (8bit):	5.521012864241686
Encrypted:	false
SSDEEP:	12:HzdDesWWSGdiDYRwbgj84NEnPcrNoTUbdN8k286ROp49dnmy:TkW9iMybgjT+k+23yO4bH
MD5:	4E80011AFAFFFE6CBF94D0386EEFCFA3
SHA1:	ECCCE856AB86E77C5506FF5E99543686B451ED98
SHA-256:	FD1AAA2ABF8BFE45E52271D437CB8BCE342E337A05E7EF318BE218E30D0259C7
SHA-512:	DF5DF86F42FD635F294554D58402F86D11DBF7AB72A6CB4D550491854B46EDED2FFA86419C46D7444C274F9CC1939746D9941AE046E1934486E6ADEAE7CAB5C
Malicious:	false

C:\Users\user\AppData\Roaming\89378384\lpiuchwp.xls	
Preview:	45MSA257tQeu3ahvB87975797Z6UL9ozy53L8f6cC7z2G2558JiYZ3..KA9k5wMv84igd3TDqwB4zVinPN1jkf67p803r025y779S0i2B4f1Q1j69P369N745X78HF3mS4 92gh223mt992CB01nvl047884q98..2k8937C46vH036KC896dc0OdOcCqR1l3b76YJXvp181BJ41v49..dzzJsotY38837zP58AZ7qit859q1J56mE65009161..42W9o fT5HWR7rPpvJqT9..68Z838t1T94mgQr8QF3E7YF25g1T83pnL5B2A08G913G80a1U08Gaz96qg9D4F08luj8RSYWj7d54333y8ak945qKc76t4Kv4..89F5201cPSn398 a7f6m4h2k783nGpb4368d0gn712eK3fX4Cl20p147z6oa7u3seea0hurKFzqu6jaFz9HF400I406p8DiECebq8Fc6D1W5W4syfT942H545MIM8H4Z74r5JfA9B36dtnx24 qof410N41dam..

C:\Users\user\AppData\Roaming\89378384\mheqq.log	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	549
Entropy (8bit):	5.480205164580472
Encrypted:	false
SSDEEP:	12:UQTG4kUTBMrhybYZbhv0J7nB5oQiV1D4W/XZr2S2VOoIrcRryGG+z+97qSzS5s:tGqOwbQMJ7nBiNVN4MF2SGZrygQqcSe
MD5:	37C227E14C6946E4ED3A0B76F94CE0B4
SHA1:	0FFA76F2E34CEDED902E4709EAA229A00CC96755
SHA-256:	7762A1FD9088AE1DC65510BE15F2542E993329B0A8F65901BB9E45ECAFD199BE
SHA-512:	4C6E035E5DDBE04BC03D95C8FEF9AA4ECF946762BA91E9D84A4265BDF8E6F976F1C7C8E9D68B9F024A2152011301A894C3F7B51E6B1C6E7AA526FA0C884C0A 0B
Malicious:	false
Preview:	V60ZE2115599B12I25HzOBIM91qvNOmWkgEnr98Qa5dT7p..wh416mZtKycGm85x3J91W0I05wDAO36OS046Ur4NiX580dm31wP3Wc8HyE006Fx5..X0z10I862CYq2746 6SRl95y0ol1ud79r51oa1k3Z69rE77W4es6QX409Vn777Y2hb3sT794452Qt99T25J6bt67P1u06EXHM62Fw466Z..7855E32945848uq126aW70Cm5EZ4FgN1P28Ag..7 5RSQi288g7tBU..Je764f56R450W4459..V4N77W0Td79ue80477zIVpgl3VD3x9Zd2QbT8f6o9342RqJ9Or..4btv0623m1F63SvV8wc6k5Wub1fKRTR8QF0CFDeOi1g8 49v205k9w4Os6j97w562uM29HfDAr194JO0612auFd018NZdN74977po5fTi8q045s1P39I86v5l3sJ09PE743cy3ygB..7A5350287002na25V7O3330WCgC998B11386 1g8jR9Xrb99x8fF475G1B136982..

C:\Users\user\AppData\Roaming\89378384\mvadg.xl	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.59344746108483
Encrypted:	false
SSDEEP:	12:7BZ7fownIHabPIURAEFr5RDxMJYc1HZcRpUYGtU9:/fownIHaLIG5RDxMJd15cRpqi9
MD5:	B3A1A09E867E85C01BD6118F173EC6E5
SHA1:	255AA2149CF96BE8B336C4CFFFBAE461DA3E4894
SHA-256:	CF4692B4983E4CCEE77DCC64C6CC775B8A453168DD329864A4331789C7294673
SHA-512:	4B7392540244646C1C3E4F9C1F7CB0869A7BCA0422A5E488EF7E99534EE4CAC693D0C41021BC0E8D59EFEC92D58491E71A9DBB75B254F591CFFDD3DC8A042A 7
Malicious:	false
Preview:	Z811OaygtX7nlstb5Jad84KT43C03ZsdR7n2uY51dqA3VSy7..Xu0z8m79exFwW2RLC07oAhZ2Hy8Q42P9J51O0g463RR5bk200aILzpRV56W0319eC8371jy177Sm5465 BV3gCh004973n9oR5G9Z5Uno84kA884..k05W31K32h9H81q3orvi2Mhdq2608co97f24fT7t2a23yG8jV7XI68X09N4emjMWyMp6JbAUo4isk011zI25lmA40Ml121kOG 64266jR8FfofM71Bqr..1tHhKL9z59ckLtnq8bg7p1Bw65r2Rc44vXVY41253OUAh2k77G8doqBOjM2cUA..45sC55OVtH1zK3np125U27fh17EL5dX65Q0dv464Z5260s T25w96..QE5Z76FtI9X65S3I9s339uz70V6181k00j2h27w79rMMjCW96PBRCbBrv1..yS59396073K2871m4V6UW4FM21H7Rv492NT7Rmpt7724Sv3D6w9C82aY9q1JE5 4825586tO6724O7SzT7p84U9SVHagU7WF5Hxv20Q0YEa82rA4o3z8yx4uD7a4zJ646E..

C:\Users\user\AppData\Roaming\89378384\neirnbgp.txt	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	591
Entropy (8bit):	5.439152650222553
Encrypted:	false
SSDEEP:	12:Zn3ILv9K1kCLEdTyK4A4bHqgJW02bIwMQ1peKsjduj02oLPShw3:Zn0lQZ0TyQqKD8wzkK3w2orSha
MD5:	DF4BB8A2B65B0745977157B4BA904B0F
SHA1:	F58B8E0EBF696A83C84A32E0BBCBBFD4CD4CFF0C
SHA-256:	0320A702B3684D4E8765AC0046DE266B79B050ACF9280E3D788BF5E84FB0B68B
SHA-512:	C91E29F6FF4CE040AB43C07213FE0EDD125DD70A800754E16C5023B6374680B175D1591A127D82FC1EC94223BEF5D08AC437D56D458B6075B1357130F8C4D6B
Malicious:	false
Preview:	6u8fl7F0WR68YaT89tx1P4g2BCEC5..5J6qiavde3uwT413795F5rX32I19L49Jrc61L572p..O32B995..5245z12wIXUJN93U8iGe859FL7F934n1744HYtw6JO12862 5Vw5D5V8o4iaw76x5419zPC8912876MfMVRGO5U8az10N2kx2r9hctOpml01279m..145205wMj999oV02w4JQ6Gn9r23uHbatr56h86l4X43B9VxJ0LS2z83n6P15Zhy9 V62lC9657m7i8927X486fun512S54W6..015q5Ww21OtHBz7X432A92F4d14GFKQ93uhQ4xFEY16Lf94291465N9nC05f3sHR4w7e405C91P83v50231K8ua00Y3IJ4ZWv NAYy31P107491oQ9aA0IU8M8er359iqOj7R4..h5j7o3v0por5w73S1t1lVr802Fq1Wi..eWSG7155bS0IC1OnG2wE82P2I59z3382N79p577I79unM331e72HIt141J3p PaUog0u7L4aA70N083133488fz672990x24G6QhG53y866424uN0dUG7G1q2V067kju47..

C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe

C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	
File Type:	data
Category:	dropped
Size (bytes):	124716950
Entropy (8bit):	7.015438985316352
Encrypted:	false
SSDEEP:	196608:BCW+5DVqqFiaQllbRtmbHQsJVkYba/yVYSmexrxyGy72T5skD8lYPsBQ0jPWLX52:D
MD5:	39FA527A3B0A8650434BE4083D7FEB0A
SHA1:	DD0E9B5DC0A018B12E9A9EC419F07CC573832DBF
SHA-256:	2B338EC693FA6CA76C046D0E1F62ED5B3A20F6D7B21910486C580327C894F4B7
SHA-512:	9FE9BD5445FDE2DFA3A7F4D105567FA4034E7F4984493D1070CA8FF4E2492DDE394DF0EC817D2538FF4268C90B7001BD56E72E4A28E9A863805C4649DF98F8B
Malicious:	false
Preview:	..;..O]]......C..sh.....#.c.s.....|....!^Sex....Ri@..*.a.^.....K.....).a....3..{....9.x.....T..c..&7.h....*...~P..4.....h .<E.....a..?.W5.g. .`E_.M@..LM..z.FR|...v.1"eJ.3[.....o.....TW ...T...J.....s.....A.pj$...."...&Q./_3.....l.ly.K7.....F.~.a...Hd...7...8..2.....'..!<Gx#.....Gc$.H.{.q,~.u....._.$.%....Z.o.3.Y.8.4.t.9.5.H.C.7.8.3.G.S.E.z.0.1.0.l.5.b.U.4.C.5... ..4.1.4.7.j.9.4.L.6.9.e.6.1.6.i.3.A.....(.....9 .....}....c.....#....o.$f>.....2...j..G.....70.d.{b...' Z4.Sb."}...mL.....>.C+|...t.....F.Y...v.^t.O.M|s.S.it..{.&B..VW...+A....C0L.....} ...R..x...-,.M.kx..j....W.?..'...aW..l.$07.3....H.D..sB..?.o.z..O.f3...9.^...7..7B....i..#.E.....%i.Mx.H.U...S.7.:.F.....^uo.'ELZ.<}...)..f./.%..F_..E.[....`)A.J..z...3.h...&..a..=ud^.'..u.l... z..f.....5C."A.....;.h~ ...C.{j1.P.H.....M.%...y./....Fs..|o<.....Ze.0....bI>..."Zu.. ...yo.Fa.s..F|c.i^]s^.l.....1..Bo.....H...]}..x>..x..

C:\Users\user\AppData\Roaming\89378384\olvljot.icm	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	553
Entropy (8bit):	5.432434398168419
Encrypted:	false
SSDEEP:	
MD5:	384165B9E6C84F131D4A63EE529EEB05
SHA1:	B6FC12C6EDC5803F786AC9266F59FBA7F24514C7
SHA-256:	99E8D6B9065EBE32F36FA12CD09BC1C3F9BCEDEFA3966118C1F2FF53AFEDD4F2
SHA-512:	257D2EE7DEB346D1C89C84679A7C2B0CB60A87D15837C019DE57B45AC35F869B489AAAFBDC44F6DA49D561B022E444F5A208F46BC592F6794CBA4BCD48C2B 34
Malicious:	false
Preview:	85Va5DGRx4292b957Tb40n5U7H14FU09fa67186d3cD..3377t8m781iyR31NN3gpo4S0b69C2fa7hH41ws745iFH28377NL842901E299E86J7W7648M850p6934KQz6G 7w21255fF60..27UXhX024RQuul42jy89T7m5p6j776158g17819..c8m411qtuo184p762M3537e416AOyqQcsvvwaPG4431j4MGW7026blw6P4k5HS..cd6ui457zSkM Sg69K905M1RAJ32cGN80Wso2l7f39XSB1572D9D4Inv9R2JVyrua07WFstHRT50Rh43392Q14M03P8Y4E8H93FU1icV33zBNK0H51S9sCHoIox87g04X3fN9S4U9..o75f 9V576x416jpiWYtrr55p325rQ5..5My1VF7jY8UDX236f9E3Ts7438OA45h967U1117CxqtHE70Tu52Nu2D14J307EqD0To344uxi63f9..u2ps1F7E0411Dm4m20138m3 9Z32J09MM298s590I2UUYi8u543624Z..

C:\Users\user\AppData\Roaming\89378384\pravpih.msc	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	573
Entropy (8bit):	5.462559461768957
Encrypted:	false
SSDEEP:	
MD5:	B155B473CC9DEF0D4B2B38F5C9BBF7F2
SHA1:	430CF6A0262CC7A67ABA6D1DB0573291B4EAABB2
SHA-256:	9B7B77279DD6A3FF5526FC18142459BC3475D8EA92DB90E5DEACD0CC2E8261DE
SHA-512:	886A123DD9AD700F08115F7BEBD480C459329446C2E6B12F2811A193B83FA39442FA438570B3DA5330084C73042341B6D643F8F1F696AB66A24BFAC06AE459BA
Malicious:	false
Preview:	3l4e97342mqJ1b218Gaq34s1978nE01932tEc3EMAulL8..4wi047M436Y91Vloy3DEY60fJ31qg7275569vGxfaJOJ7d3EBUh15S22zYCP8g12780g5yTRqiB4W6wW6J6 59xjiD9IP8Vx0D10332conxv322pfPQXq23611K38Yt7C5Z3O699Q73qh0E3t59mEY177C73..Vq9675t53E661F2g7q26DA850fyy2Uzy3D59fK5TkBb0601Je6vWys48 074..1cL7645knXZx690S8VrneKO9wWybw972hkEo78532p37vKk5BH47B22613210Y20Q937ws3a9753575gqzVKV781w2O1757H1Tf7W14tp6UA8I455pDH1E8U542MV 2URn3bI1kq4RB06Al9LU7372p24qjvrM2041Z3og9VLX29OvY..83460811Ca1H1j3982n..64yp7c17VKvx5namos2264m0q641eWB0MDZ5vr90l6Es428MQfM26q89Z2 N8o2Vv413oj58oA6M89ep34Fc8hfWZOR75L6465s57YLq99L5e9..

C:\Users\user\AppData\Roaming\89378384\pssktmsip.ppt	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	679
Entropy (8bit):	5.524374021299318
Encrypted:	false
SSDEEP:	
MD5:	4824754E653B24D4BD4223120722413D
SHA1:	6A5177A850F7A2C48B16ADFC890310098497BDCF

C:\Users\user\AppData\Roaming\89378384\pssktmsip.ppt	
SHA-256:	1AD8F76ABE067A25D5623FEFD4A540D61E6F49690A7BF0BC1E9D4229F11E1678
SHA-512:	70D0F7C09A1560533F96D33B9A2B363D4226A41EE94A4AB1F37DE8A4282E9490229CE5CB7D4FF0FC34C42834C39E373ECF374F7C7DCA564ADDAFA14D9776D28
Malicious:	false
Preview:	023B5r1368E24NT679JZ92WeG0HB1YAAuo10m267Ln9yNptJ5377Cu005i2clN7E554aDJ89kH..Prh6P85kjl5NN081G9dxo4nwtynAan23l6w61j3EoiRj3C1210qj934qwi258sW315rgO4M6o5W851BX6EeWrHH0LF30pxj3xX5n7FmXh4A47HnS6m1241h23OaaSR951g2043814062Q13uL88bwW7w..47SegE27314A5giDqKSf2ja3289oG4sW7327WmP7M5VqzBW69w453Ip..k74093Y483b5095S82691wr28z99kUJ7T48a0mUBAAu653Bu1fUAP33z4P7fde9e48523RFy5HL0unZOO14G1OJez8iW5K13nz6Hv163Ta0X5..5KA8001Ijb98olriT5YY5..6hv907K3496ck6N3i627KDF18zG7A95K9j1n5M4729o5316j581p8wf743z5F8L486U7s..6YZ3y33o30aUw50yIFD4EA96YMZ9EsCcf323KC12k9L37aF486WKBdll55Qp4Hu4jUwPv9hm0nP26f8iLpUgJg5nL7bINP89H5Q8T06W0843sua60A739852897Zcwpp762h5JsO570nM6he3Lh5002vr44O5611zgvw1f36T1p459451N0zx896L..

C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	662768
Entropy (8bit):	6.567604064397569
Encrypted:	false
SSDEEP:	
MD5:	F471B7C16D5B01AF9F67F5F4A921F81F
SHA1:	D84A2ABAAC3E7FA6E5D4918DDBCDEC47AAF91D5B
SHA-256:	BE75E476ECA46172219A1EBD97D0F37B464D4DC079F25728D99A0F85F6060220
SHA-512:	0F1C6315F5E510C943DBE3A68C47E9C531F39CC08E3C155AC3D886F8861CD4978D6179EA23FA2D34E3499338D5CEBD0FDDE8F7F0D54B1662E582D6D7DC8779 6
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich..... .....PE..L....%O....."....d..... ....@.....p.....6....@...@.....@.....T.....04.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc...04.....6...R.....@..@.reloc...u.....v.....@..B..... .....

C:\Users\user\AppData\Roaming\89378384\rvhkj.pdf	
Process:	C:\Users\user\Desktop\SWIFTS.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	665
Entropy (8bit):	5.490381038410321
Encrypted:	false
SSDEEP:	
MD5:	23C2CDF4FF1C342864FEDD5E2EE521C1
SHA1:	68F2B63E08D26183411F4DA12EE0B6A22E597147
SHA-256:	5A358AC70C2DC504CE79751FC8F94FB93BF9D9EA8DB1914172E1D17D9CD6A4B3
SHA-512:	20B2F8162879E3B664AFFF91FA467DF6AB5784FD8C69B73823A7F272E9910137CC1522B3DF59EBDB1E9AB11D86E8316105EFB31CFD4112AD70EFF8046CA4690
Malicious:	false
Preview:	Re84z516x0VxX229zn63pa4qF862nCI1378Gu217..60v1q10F28f72624958t2L78wK4HI5V9Z5i5069kp7xM1V74I8f2g929113sD79E5a9R9V21xuHcZ1o43I771pe9s35KTt958kFdZ791t..EepJ625i6V32R635jvXsms95XJ5Sa14N..OT4Nrm5K4d5Y14jjm39YgtJC9h19191n1sO60C26ef9..164ZH5qb7o50s607X..39l5R6REe10tG9LJI3466l4AqS83LB9149Uly70r9d9oeT33P..ca34s89Nw0S9708kHKbt3HK1NGJ3180..s1tU5HjN15222028uWjuq8g1Q06379pk14S56..u6ME703OKD2Z274N175ni8KK43u54sKIlmo14t31ICfK6l6b08bm283C34sPefh3538067D147..03WH015IXaW45D9h2y1U77uNa1T6768IAjGA2..60n437PHyeC6V..c9ckX3s3q8UlP86Xqi50mC365i7497P04EB2Ff7p8POJn3jwJ06x399qOg69se8Oo46o29bef9wrpU581h96668791k42odAHCZ47Xacs95xCHuoh5n88ep0r6bk36254b9vc5Okt0U7MM3y5T563R4J1i687u4wMlm..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BE A4A
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	184D6E973996EE47090F6CDAD2A1AEF9
SHA1:	5B5DA257DBE8C2320C7F7BF006055AC700414F47
SHA-256:	7333A4089B969A2398FC56B13F1F8A2DF56EF1F3F9453FF6FEC6ACA9722E5A94
SHA-512:	B0524F62FB8BED6318D00EF9E71D5E375C8EE775A0A5D8D2406A40CDB9B30EE0C4CFA255E6653F48839E41758B814E44A0985F26F6451B5705217A58CB84C5D
Malicious:	**true**
Preview:	jP.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	48
Entropy (8bit):	4.297995052579129
Encrypted:	false
SSDEEP:	

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
MD5:	CE0CB1FF5FD6AF478BC9B018A60C6268
SHA1:	375BAD43F493898F0F7836FF08C4C9E98381717B
SHA-256:	6B93E1A15031E86950FFEDA4F5066EF4683D8ED62223AE3053E1098374E50B67
SHA-512:	7CEF4E7006C3B53454777CC356EC7F76D0BCD082CEE1B7FDAD1968260251660D133C477AB4548AE96E164D6DB280E49DD14C3FFA721A581769D0C5FDD34789F
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\lklphvrvl.dll	
Process:	C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	89
Entropy (8bit):	4.991316195702863
Encrypted:	false
SSDEEP:	
MD5:	5800002E9E3FC9321110CB9AAAEBCD4A
SHA1:	1004452BFF4A12EC0D8DF35C47F7DEB6C80CFCD3
SHA-256:	BF9250550F0A5FB651D48C09A25C2FA85D718558B071EE3E67B922D4621EB5E1
SHA-512:	086C5AD55EF93FBA1662BBA5D3A8BA38A5A8380058F20ADC7EFD9586D355C7BE5BD33A4E3DC888E8E5425D00D3D647AB3358F49A65BBFCB4F31F867E8A114EF6
Malicious:	false
Preview:	[S3tt!ng]..stpth=%appdata%..Key=WindowsUpdate..Dir3ctory=89378384..ExE_c=qtfarawjob.pif..

\Device\ConDrv	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	215
Entropy (8bit):	4.911407397013505
Encrypted:	false
SSDEEP:	
MD5:	623152A30E4F18810EB8E046163DB399
SHA1:	5D640A976A0544E2DDA22E9DF362F455A05CFF2A
SHA-256:	4CA51BAF6F994B93FE9E1FDA754A4AE74277360C750C04B630DA3DEC33E65FEA
SHA-512:	1AD53476A05769502FF0BCA9E042273237804B63873B0D5E0613936B91766A444FCA600FD68AFB1EF2EA2973242CF1A0FF617522D719F2FA63DF074E118F370B
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....The following installation error occurred:..1: Assembly not found: '0'...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.815157465823464
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:	SWIFTS.scr.exe
File size:	1020808
MD5:	0984d8481d809d2715214d220d5f3224
SHA1:	be4bfdae28308590b04709935794109a77d5ecee
SHA256:	f2597b91433ba86188dd0e53cf04d2c43d97f5231bc3077df18e75447f15c77c
SHA512:	6d3bc4b24ea6b426890310a9ddaa27047ae4dbe983790c367889a1c5452d964e11c7a3d0ead8ff96cc7f27067ffa5c9f5925e75e1d7d994c8504b01b662ff2f9
SSDEEP:	24576:BAOcZpJdk843dd0aChdB45NNgo0UBXUUHhh:bIr4tWapHP0Uy2h

General

File Content Preview:	MZ.....@.....!..L.!This is program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y..,.../y..#...&...,...._....._..'...._f.'..._..'..

File Icon

Icon Hash:	1ab8e6e663d6c77a

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Instruction
call 00007F39F8B186BFh
jmp 00007F39F8B180B3h
cmp ecx, dword ptr [0043D668h]
jne 00007F39F8B18225h
ret
jmp 00007F39F8B18835h
ret
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00433068h
mov dword ptr [ecx], 00434284h
ret
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F39F8B0B631h
mov dword ptr [esi], 00434290h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00434298h
mov dword ptr [ecx], 00434290h

Instruction
ret
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 00434278h
push eax
call 00007F39F8B1B3CDh
pop ecx
ret
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 00434278h
push eax
call 00007F39F8B1B3B6h
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F39F8B1822Ch
push 0000000Ch
push esi
call 00007F39F8B177EFh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F39F8B1818Eh
push 0043A410h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F39F8B1AAB5h
int3
push ebp
mov ebp, esp
sub esp, 0Ch

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3b540	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3b574	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x57e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0x210c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x397d0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x34218	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x32000	0x260	.rdata

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3aaec	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x30581	0x30600	False	0.589268410853	data	6.70021125825	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x32000	0xa332	0xa400	False	0.455030487805	data	5.23888424127	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3d000	0x238b0	0x1200	False	0.368272569444	data	3.83993526939	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x61000	0xe8	0x200	False	0.333984375	data	2.12166381533	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x57e8	0x5800	False	0.618430397727	data	6.34217881671	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0x210c	0x2200	False	0.786534926471	data	6.61038519378	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x62524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6306c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x64618	0xea8	data		
RT_DIALOG	0x654c0	0x286	data	English	United States
RT_DIALOG	0x65748	0x13a	data	English	United States
RT_DIALOG	0x65884	0xec	data	English	United States
RT_DIALOG	0x65970	0x12e	data	English	United States
RT_DIALOG	0x65aa0	0x338	data	English	United States
RT_DIALOG	0x65dd8	0x252	data	English	United States
RT_STRING	0x6602c	0x1e2	data	English	United States
RT_STRING	0x66210	0x1cc	data	English	United States
RT_STRING	0x663dc	0x1b8	data	English	United States
RT_STRING	0x66594	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x666dc	0x446	data	English	United States
RT_STRING	0x66b24	0x166	data	English	United States
RT_STRING	0x66c8c	0x152	data	English	United States
RT_STRING	0x66de0	0x10a	data	English	United States
RT_STRING	0x66eec	0xbc	data	English	United States
RT_STRING	0x66fa8	0xd6	data	English	United States
RT_GROUP_ICON	0x67080	0x14	data		
RT_MANIFEST	0x67094	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import

Copyright Joe Security LLC 2021

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

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-05:07:09.165021	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.202370	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/12/21-05:07:09.206372	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.245462	ICMP	449	ICMP Time-To-Live Exceeded in Transit			149.11.89.129	192.168.2.6
04/12/21-05:07:09.245877	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.281909	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.50.25	192.168.2.6
04/12/21-05:07:09.285417	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.326911	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.0.62	192.168.2.6
04/12/21-05:07:09.328747	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.375725	ICMP	449	ICMP Time-To-Live Exceeded in Transit			154.54.36.253	192.168.2.6
04/12/21-05:07:09.376183	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.424608	ICMP	449	ICMP Time-To-Live Exceeded in Transit			130.117.14.78	192.168.2.6
04/12/21-05:07:09.425435	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.488302	ICMP	449	ICMP Time-To-Live Exceeded in Transit			195.22.208.117	192.168.2.6
04/12/21-05:07:09.488998	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232

Copyright Joe Security LLC 2021

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-05:07:09.541933	ICMP	449	ICMP Time-To-Live Exceeded in Transit			93.186.128.39	192.168.2.6
04/12/21-05:07:09.542454	ICMP	384	ICMP PING			192.168.2.6	2.23.155.232
04/12/21-05:07:09.596007	ICMP	408	ICMP Echo Reply			2.23.155.232	192.168.2.6

Network Port Distribution

Total Packets: 58

- 53 (DNS)
- 1980 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 05:07:24.300146103 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:24.553714037 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:24.553814888 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:24.594976902 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:24.899915934 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:24.907613993 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:24.963887930 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.011607885 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.175003052 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.175143957 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.416940928 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.455415010 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.731025934 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.731199026 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.807913065 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.808948040 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.809035063 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.809077024 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.809874058 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.809917927 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.810072899 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.810098886 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.818993092 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.819137096 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.819881916 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.820030928 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.820038080 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.820077896 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.820125103 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.820127964 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.820137024 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.820167065 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:25.820280075 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:25.820377111 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.021815062 CEST	1980	49682	194.5.98.184	192.168.2.6

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 05:07:26.049962997 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.050889969 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.052901983 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.063838959 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.073951960 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.073997974 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.074018955 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.076772928 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.076828003 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.076905966 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.077017069 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.077320099 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.078788996 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.079766989 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.079808950 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.079879999 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.079926968 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.080810070 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.080892086 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.081938028 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.082828999 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.082921982 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.084777117 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.084990025 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.085860014 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.086765051 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.086896896 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.088843107 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.089823961 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.089993000 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.290015936 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.291001081 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.291099072 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.291941881 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.292927027 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.293257952 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.306014061 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.307832003 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.308118105 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.308803082 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.309818983 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.310132980 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.315963030 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.327943087 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.327994108 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.328058004 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.328855991 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.329191923 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.329983950 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.330846071 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.330985069 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.331796885 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.333993912 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.334151030 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.334886074 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.335721970 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.335932016 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.337846994 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.340035915 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.340250969 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.340881109 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.341854095 CEST	1980	49682	194.5.98.184	192.168.2.6
Apr 12, 2021 05:07:26.341958046 CEST	49682	1980	192.168.2.6	194.5.98.184
Apr 12, 2021 05:07:26.343851089 CEST	1980	49682	194.5.98.184	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 05:07:26.344822884 CEST	1980	49682	194.5.98.184	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 05:07:09.095623970 CEST	49366	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:09.163144112 CEST	53	49366	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:24.227725029 CEST	49288	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:24.287436962 CEST	53	49288	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:30.764930964 CEST	60892	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:30.824862003 CEST	53	60892	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:37.741466999 CEST	52157	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:37.800221920 CEST	53	52157	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:44.768863916 CEST	61182	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:44.825712919 CEST	53	61182	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:51.925920963 CEST	55673	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:51.984498978 CEST	53	55673	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:54.926422119 CEST	57773	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:54.976605892 CEST	53	57773	8.8.8.8	192.168.2.6
Apr 12, 2021 05:07:58.989599943 CEST	59986	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:07:59.047719955 CEST	53	59986	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:05.927719116 CEST	52478	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:05.984985113 CEST	53	52478	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:12.949404955 CEST	58931	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:13.006405115 CEST	53	58931	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:20.316972017 CEST	57725	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:20.374080896 CEST	53	57725	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:26.702847958 CEST	49283	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:26.762236118 CEST	53	49283	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:33.967689991 CEST	58377	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:34.026248932 CEST	53	58377	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:40.731115103 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:40.781503916 CEST	53	55074	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:41.169373989 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:41.229949951 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:47.781793118 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:47.841530085 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 12, 2021 05:08:56.024343014 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:08:56.081618071 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 12, 2021 05:09:03.148418903 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:09:03.205610037 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 12, 2021 05:09:10.201092005 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 12, 2021 05:09:10.259608030 CEST	53	49448	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 05:07:24.227725029 CEST	192.168.2.6	8.8.8.8	0x4f37	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:30.764930964 CEST	192.168.2.6	8.8.8.8	0xbb27	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:37.741466999 CEST	192.168.2.6	8.8.8.8	0x5273	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:44.768863916 CEST	192.168.2.6	8.8.8.8	0x386	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:51.925920963 CEST	192.168.2.6	8.8.8.8	0x61d2	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:58.989599943 CEST	192.168.2.6	8.8.8.8	0x3d6b	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:05.927719116 CEST	192.168.2.6	8.8.8.8	0x6d7f	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:12.949404955 CEST	192.168.2.6	8.8.8.8	0x448e	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:20.316972017 CEST	192.168.2.6	8.8.8.8	0x8276	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:26.702847958 CEST	192.168.2.6	8.8.8.8	0x957d	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 05:08:33.967689991 CEST	192.168.2.6	8.8.8.8	0xaac5	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:40.731115103 CEST	192.168.2.6	8.8.8.8	0xc55	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:47.781793118 CEST	192.168.2.6	8.8.8.8	0x2e24	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:56.024343014 CEST	192.168.2.6	8.8.8.8	0xc69b	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:09:03.148418903 CEST	192.168.2.6	8.8.8.8	0xf8d4	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)
Apr 12, 2021 05:09:10.201092005 CEST	192.168.2.6	8.8.8.8	0xeee6	Standard query (0)	ekuro.hopto.org	A (IP address)	IN (0x0001)

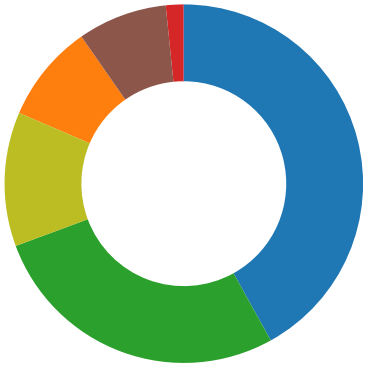
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 05:07:24.287436962 CEST	8.8.8.8	192.168.2.6	0x4f37	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:30.824862003 CEST	8.8.8.8	192.168.2.6	0xbb27	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:37.800221920 CEST	8.8.8.8	192.168.2.6	0x5273	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:44.825712919 CEST	8.8.8.8	192.168.2.6	0x386	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:51.984498978 CEST	8.8.8.8	192.168.2.6	0x61d2	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:07:59.047719955 CEST	8.8.8.8	192.168.2.6	0x3d6b	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:05.984985113 CEST	8.8.8.8	192.168.2.6	0x6d7f	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:13.006405115 CEST	8.8.8.8	192.168.2.6	0x448e	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:20.374080896 CEST	8.8.8.8	192.168.2.6	0x8276	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:26.762236118 CEST	8.8.8.8	192.168.2.6	0x957d	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:34.026248932 CEST	8.8.8.8	192.168.2.6	0xaac5	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:40.781503916 CEST	8.8.8.8	192.168.2.6	0xc55	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:47.841530085 CEST	8.8.8.8	192.168.2.6	0x2e24	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:08:56.081618071 CEST	8.8.8.8	192.168.2.6	0xc69b	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:09:03.205610037 CEST	8.8.8.8	192.168.2.6	0xf8d4	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)
Apr 12, 2021 05:09:10.259608030 CEST	8.8.8.8	192.168.2.6	0xeee6	No error (0)	ekuro.hopto.org		194.5.98.184	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- SWIFTS.scr.exe
- qtfarawjob.pif
- RegSvcs.exe
- schtasks.exe
- conhost.exe
- RegSvcs.exe
- conhost.exe
- qtfarawjob.pif
- RegSvcs.exe

Click to jump to process

System Behavior

Analysis Process: SWIFTS.scr.exe PID: 4104 Parent PID: 6036

General

Start time:	05:07:05
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\SWIFTS.scr.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SWIFTS.scr.exe'
Imagebase:	0xee0000
File size:	1020808 bytes
MD5 hash:	0984D8481D809D2715214D220D5F3224
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EE9F1F	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EE9F1F	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EE9F1F	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	EE9F1F	CreateDirectoryW
C:\Users\user\AppData\Roaming\89378384	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	EE9F1F	CreateDirectoryW
C:\Users\user\AppData\Roaming\89378384__tmp_rar_sfx_access_check_6319375	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\lklphvrvl.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\ljqg.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\hwbmxx.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\pssktmsip.ppt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\ksbjboc.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\fvltkxlub.jpg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\mvadg.xl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\olvljot.icm	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\neirnbgp.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\gencjb.ico	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\lpiuchwp.xls	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\ajwiqng.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\pravpih.msc	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\crfgiqf.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\mheqq.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\ksfdlrauwr.mp3	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\rvhkj.pdf	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\ckcsljuf.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW
C:\Users\user\AppData\Roaming\89378384\jlotan.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\cxijg.ico	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	EE95B6	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384__tmp_rar_sfx_access_check_6319375	success or wait	1	EE9E2F	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\lklphvrvl.dll	unknown	474485	39 33 32 32 4a 32 6c 4f 33 38 38 39 32 36 39 31 6c 7a 72 35 52 4e 32 37 63 53 65 30 39 74 39 4f 32 35 31 6a 30 4b 54 35 39 33 32 33 71 43 54 6b 0d 0a 30 34 32 48 4a 49 32 6b 34 71 34 43 71 33 34 62 51 73 6e 52 69 39 32 71 62 61 36 57 55 71 39 6d 38 37 34 49 64 53 33 58 32 39 34 32 34 58 30 41 46 6f 32 54 35 33 35 42 39 38 6f 39 39 30 33 30 47 70 42 36 0d 0a 33 63 79 38 41 74 7a 32 34 37 68 7a 38 59 34 77 64 71 52 4d 31 44 32 38 6c 55 30 57 4a 4c 0d 0a 53 32 32 45 37 34 39 30 6e 65 57 38 6f 6a 6c 73 32 4b 36 48 4b 38 38 35 33 6a 38 56 31 52 64 43 38 36 38 64 6c 34 31 6d 30 74 38 43 36 32 38 69 30 44 39 42 57 38 47 6a 6a 6f 55 38 0d 0a 73 4b 37 74 34 30 39 39 35 32 50 34 38 34 39 36 74 54 33 51 74 4e 6e 4a 6d 34 38 47 33 37 42 36 65 6e 4e 58 39 34 59 32 36	9322J2lO38892691lzr5RN 27cSe09t 9O251j0KT59323qCTk..04 2HJI2k4q 4Cq34bQsnRi92qba6WUq 9m874IdS3X 29424X0AFo2T535B98o99 030GpB6.. 3cy8Atz247hz8Y4wdqRM1 D28lU0WJL ..S22E7490neW8ojls2K6H K8853j8V 1RdC868dl41m0t8C628i0D 9BW8Gjjo U8..sK7t409952P48496tT3 QtNnJm4 8G37B6enNX94Y26	success or wait	1	EE9CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	unknown	4191761	ff fe 3b 00 8d 4f 5d 5d 18 f1 f2 e6 ea d6 43 15 b4 73 68 98 9f bc ac f3 0d 00 0a 00 23 00 63 00 73 00 f1 a6 0b 15 c1 10 01 d7 c5 7c 06 04 17 9c 21 5e 53 65 78 95 0b 8a dd 91 52 69 40 a5 a4 2a a7 61 df 5e 90 c0 1e 19 f6 e6 4b f3 f6 9b cd 8c 8c ee 29 94 61 14 c9 ec ce a7 33 0f c2 7b c2 8a c2 17 fb 39 e4 78 bb a1 ab b9 97 54 bb cc 63 b0 90 26 37 e4 68 c0 1a e6 e7 2a 8a 07 99 7e 50 a3 ed 34 cc f8 ff 02 9d 1a fe 68 20 d0 3c 45 ef c0 09 82 cb ba d1 a7 a3 61 98 d4 be 3f 7f 57 35 b7 67 d7 20 cd 60 45 5f 17 4d 40 ca 96 cc 99 4c 4d f2 d7 7a b7 46 52 7c 08 e5 a6 e3 76 e1 31 22 65 4a e5 33 5b be c4 92 88 ea 10 e1 6f 13 04 07 04 e7 07 54 57 8e 16 ff 54 a5 98 e4 4a 93 bf 87 94 9b 73 0d 00 0a 00 d3 41 cb 70 6a 24 dc b1 03 b0 f3 22 ac 07 ab 26 51 c1 2f 5f 33 8b b8 f3 17	..;..O]].....C..sh.....#. c.s.....|....!^Sex.....Ri @..*.a.^.....K.....).a.....3.. {.....9.x.....T..c..&7.h... .*...~P..4.....h .<E..... .a...?.W5.g. .`E_.M@....LM..z. FR|....v.1"eJ.3[.....o..... TW...T...J.....s.....A.pj$.... ."...&Q./_3....	success or wait	33	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif	unknown	65536	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 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 c2 1e 94 bf 86 7f fa ec 86 7f fa ec 86 7f fa ec 15 31 62 ec 84 7f fa ec 9d e2 50 ec 29 7f fa ec 9d e2 51 ec b3 7f fa ec 8f 07 79 ec 8f 7f fa ec 8f 07 69 ec a7 7f fa ec 86 7f fb ec 96 7d fa ec 9d e2 4e ec ce 7f fa ec 9d e2 64 ec 9a 7f fa ec 9d e2 60 ec 87 7f fa ec 86 7f 6d ec 87 7f fa ec 9d e2 67 ec 87 7f fa ec 52 69 63 68 86 7f fa ec 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....1b... ....P.).....Q.....y.....i. .....}....N.....d..... `.....m.....g.....Rich.... .....PE..L..	success or wait	21	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\ljqg.dat	unknown	601	62 51 35 4f 47 72 6a 7a 34 4e 4f 67 32 4c 58 5a 76 52 30 6e 4e 4e 36 45 74 32 61 52 31 6e 38 39 69 34 34 52 35 31 38 6e 38 47 56 4d 35 45 30 30 62 39 32 6c 36 30 70 54 32 7a 31 4c 78 34 6f 48 75 30 41 34 34 5a 79 48 44 48 5a 4c 65 59 0d 0a 75 4b 36 72 4e 6c 78 45 33 57 68 4c 38 70 55 39 35 5a 33 78 39 50 31 79 5a 6a 64 48 35 47 30 32 30 62 32 73 72 38 32 30 74 6d 38 53 31 32 77 77 64 39 32 36 4b 59 36 33 33 43 37 53 30 6a 51 35 34 69 30 63 6a 36 35 30 77 38 70 0d 0a 38 5a 52 39 32 53 34 33 50 34 34 34 64 4c 69 65 30 6c 74 46 59 7a 77 64 50 30 65 6c 46 52 56 71 78 37 37 33 78 37 37 41 4a 32 6a 38 30 32 32 33 36 34 37 30 67 46 30 41 34 4b 35 37 74 4b 32 59 71 30 32 48 32 7a 77 38 6c 32 72 73 30 36 31 33 5a 47 6e 4a 72 6f 4a 37 34 72 35 36 30 51 7a 0d 0a 34	bQ5OGrjz4NOg2LXZvR0n NN6Et2aR1n 89i44R518n8GVM5E00b92 l60pT2z1L x4oHu0A44ZyHDHZLeY..u K6rNlxE3W hL8pU95Z3x9P1yZjdH5G0 20b2sr820 tm8S12wwd926KY633C7S 0jQ54i0cj6 50w8p..8ZR92S43P444dLi e0ltFYzw dP0elFRVqx773x77AJ2j80 2236470g F0A4K57tK2Yq02H2zw8l2 rs0613ZGn JroJ74r560Qz..4	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\hwbmxx.dll	unknown	504	39 36 6f 37 41 30 44 75 5a 32 44 39 36 30 74 78 6d 38 41 31 54 36 39 31 39 37 33 31 32 37 32 61 69 7a 30 65 32 45 6a 37 75 45 59 52 30 56 47 37 5a 58 50 39 30 46 48 36 67 35 4f 30 34 4a 58 41 34 7a 30 74 34 35 38 50 5a 5a 6c 6b 31 55 6b 30 48 37 70 6f 32 31 30 44 47 50 68 37 30 47 31 0d 0a 6a 35 35 39 71 36 78 4c 42 39 47 52 70 44 37 49 0d 0a 78 6b 69 31 44 36 33 54 43 43 31 56 6f 36 36 32 38 38 68 77 35 45 36 73 38 52 35 36 4c 32 37 32 62 34 31 62 76 30 35 45 67 64 76 32 34 49 72 36 33 0d 0a 49 63 6f 30 64 64 39 61 64 30 46 76 6e 30 38 36 33 61 33 31 53 32 30 32 7a 31 65 39 33 4b 4e 46 41 36 39 41 38 35 4b 31 33 77 64 59 36 32 59 73 68 77 35 33 4c 4a 37 36 32 69 37 59 72 36 43 62 31 6d 36 38 31 71 39 46 48 54 30 59 30 33 32 34 36 4c 57 38 34 56 30 33 47	96o7A0DuZ2D960txm8A1 T691973127 2aiz0e2Ej7uEYR0VG7ZX P90FH6g5O0 4JXA4z0t458PZZlk1Uk0H 7po210DGP h70G1..j559q6xLB9GRpD7 I..xki1D 63TCC1Vo66288hw5E6s8 R56L272b41 bv05Egdv24Ir63..Ico0dd9a d0Fvn0 863a31S202z1e93KNFA69 A85K13wdY 62Yshw53LJ762i7Yr6Cb1 m681q9FHT 0Y03246LW84V03G	success or wait	1	EE9CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\pssktmsip.ppt	unknown	679	30 32 33 42 35 72 31 33 36 38 45 32 34 4e 54 36 37 39 4a 5a 39 32 57 65 47 30 48 42 31 59 41 41 75 6f 31 30 6d 32 36 37 4c 6e 39 79 4e 70 74 4a 35 33 37 37 43 75 30 30 35 69 32 63 6c 4e 37 45 35 35 34 61 44 4a 38 39 6b 48 0d 0a 50 72 68 36 50 38 35 6b 6a 6c 35 4e 4e 30 38 31 47 39 64 78 6f 34 6e 77 74 79 6e 41 61 6e 32 33 6c 36 77 36 31 6a 33 45 6f 69 52 6a 33 43 31 32 31 30 71 6a 39 33 34 71 77 69 32 35 38 73 57 33 31 35 72 67 4f 34 4d 36 6f 35 57 38 35 31 42 58 36 45 65 57 72 48 48 30 4c 46 33 30 70 78 6a 33 78 58 35 6e 37 46 6d 58 68 34 41 34 37 48 6e 53 36 6d 31 32 34 31 68 32 33 4f 61 61 53 52 39 35 31 67 32 30 34 33 38 31 34 30 36 32 51 31 33 75 4c 38 38 62 77 57 37 77 0d 0a 34 37 53 65 67 45 32 37 33 31 34 41 35 67 69 44 71 4b 53 66 32 6a 61 33 32	023B5r1368E24NT679JZ9 2WeG0HB1Y AAuo10m267Ln9yNptJ537 7Cu005i2c lN7E554aDJ89kH..Prh6P8 5kjl5NN0 81G9dxo4nwtynAan23l6w6 1j3EoiRj 3C1210qj934qwi258sW315 rgO4M6o5 W851BX6EeWrHH0LF30p xj3xX5n7FmX h4A47HnS6m1241h23Oaa SR951g2043 814062Q13uL88bwW7w..4 7SegE2731 4A5giDqKSf2ja32	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\ksbjboc.xml	unknown	627	32 59 36 59 42 35 39 37 32 51 30 34 35 6d 7a 33 71 33 37 50 32 68 38 65 34 6c 33 37 35 7a 4f 32 38 38 62 38 34 38 39 0d 0a 77 38 37 35 75 34 39 32 30 4e 36 4c 59 31 5a 34 79 38 79 34 61 48 58 7a 39 51 39 33 39 68 65 7a 45 31 35 6a 34 76 36 35 76 72 31 55 55 7a 36 68 72 33 55 38 38 34 54 35 53 38 0d 0a 68 34 32 39 39 4e 63 33 31 36 7a 31 59 0d 0a 33 76 31 46 0d 0a 39 68 31 4d 70 38 6f 32 69 37 38 55 33 31 36 65 32 74 7a 57 76 55 61 30 37 67 6e 39 5a 36 6b 37 37 6c 39 33 37 37 4b 31 77 72 71 63 30 36 62 61 65 71 4d 0d 0a 38 31 54 65 32 75 57 73 34 78 76 72 31 42 38 35 34 7a 6a 72 32 4a 58 41 4b 71 59 53 33 45 0d 0a 36 35 37 37 7a 48 55 65 33 78 31 54 31 36 77 32 49 30 35 70 54 32 34 36 39 35 4a 33 30 64 78 4c 36 32 38 39 49 33 33 4c 52 33 52 41 72 7a 39 37	2Y6YB5972Q045mz3q37P 2h8e4l375z O288b8489..w875u4920N6 LY1Z4y8y 4aHXz9Q939hezE15j4v65 vr1UUz6hr 3U884T5S8..h4299Nc316z 1Y..3v1F ..9h1Mp8o2i78U316e2tzW vUa07gn9 Z6k77l9377K1wrqc06baeq M..81Te2 uWs4xvr1B854zjr2JXAKq YS3E..657 7zHUe3x1T16w2I05pT246 95J30dxL6 289I33LR3RArz97	success or wait	1	EE9CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\fvltkxlub.jpg	unknown	529	54 31 78 62 4b 56 57 78 6b 32 36 57 36 5a 76 62 33 33 4c 37 6e 36 30 75 30 49 4d 50 31 6a 49 32 33 37 49 6d 33 38 33 6b 50 37 30 61 68 58 37 34 6f 51 68 30 38 38 30 33 43 79 30 68 6c 65 61 36 56 75 52 4f 4e 34 4b 45 48 35 65 35 38 52 38 0d 0a 32 43 32 34 31 62 72 44 39 35 34 6f 31 35 79 6b 75 31 53 32 31 78 79 44 49 58 6e 79 32 37 66 39 32 33 30 32 58 30 6f 39 78 39 75 35 67 38 38 53 67 30 61 30 43 34 47 62 33 36 65 34 30 78 30 78 67 31 30 35 36 30 34 56 6b 59 30 34 41 4f 4f 55 30 32 0d 0a 6b 36 4d 36 79 65 72 30 6d 30 30 39 38 42 44 35 31 34 38 59 77 73 66 64 35 35 70 33 32 33 50 76 77 4b 66 37 0d 0a 38 33 35 54 36 67 30 31 58 56 34 70 6c 38 38 4c 49 39 6f 32 32 59 35 39 31 68 7a 48 4f 30 39 30 32 34 42 4a 75 4e 37 32 37 6e 34 6e 4b 55 37 4a 6a 4d 39 4a	T1xbKVWxk26W6Zvb33L7 n60u0IMP1j I237Im383kP70ahX74oQh 08803Cy0h lea6VuRON4KEH5e58R8.. 2C241brD9 54o15yku1S21xyDIXny27f 92302X0o 9x9u5g88Sg0a0C4Gb36e4 0x0xg1056 04VkY04AOOU02..k6M6y er0m0098BD 5148Ywsfd55p323PvwKf7. .835T6g0 1XV4pl88LI9o22Y591hzH O09024BJu N727n4nKU7JjM9J	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\mvadg.xl	unknown	589	5a 38 31 31 4f 61 79 67 74 58 37 6e 6c 73 74 62 35 4a 61 64 38 34 4b 54 34 33 43 30 33 5a 73 64 52 37 6e 32 75 59 35 31 64 71 41 33 56 53 79 37 0d 0a 58 75 30 7a 38 6d 37 39 65 78 46 77 57 32 52 4c 43 30 37 6f 41 68 5a 32 48 79 38 51 34 32 50 39 4a 35 31 4f 30 67 34 36 33 52 52 35 62 6b 32 30 30 61 49 4c 7a 70 52 56 35 36 57 30 33 31 39 65 43 38 33 37 31 6a 79 31 37 37 53 6d 35 34 36 35 42 56 33 67 43 68 30 30 34 39 37 33 6e 39 6f 52 35 47 39 5a 35 55 6e 6f 38 34 6b 41 38 38 34 0d 0a 6b 30 35 57 33 31 4b 33 32 68 39 48 38 31 71 33 6f 72 76 69 32 4d 68 64 71 32 36 30 38 63 6f 39 37 66 32 34 66 54 37 74 32 61 32 33 79 47 38 6a 56 37 58 49 36 38 58 30 39 4e 34 65 6d 6a 4d 57 79 4d 70 36 4a 62 41 55 6f 34 69 73 6b 30 31 31 7a 49 32 35 6c 6d 41 34 30 4d 6c 31	Z811OaygtX7nlstb5Jad84 KT43C03Z sdR7n2uY51dqA3VSy7..X u0z8m79ex FwW2RLC07oAhZ2Hy8Q4 2P9J51O0g46 3RR5bk200aILzpRV56W0 319eC8371j y177Sm5465BV3gCh0049 73n9oR5G9Z 5Uno84kA884..k05W31K3 2h9H81q3o rvi2Mhdq2608co97f24fT7t 2a23yG8 jV7XI68X09N4emjMWyMp 6JbAUo4isk 011zI25lmA40Ml1	success or wait	1	EE9CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\olvljot.icm	unknown	553	38 35 56 61 35 44 47 52 78 34 32 39 32 62 39 35 37 54 62 34 30 6e 35 55 37 48 31 34 46 55 30 39 66 61 36 37 31 38 36 64 33 63 44 0d 0a 33 33 37 37 74 38 6d 37 38 31 69 79 52 33 31 4e 4e 33 67 70 6f 34 53 30 62 36 39 43 32 66 61 37 68 48 34 31 77 73 37 34 35 69 46 48 32 38 33 37 37 4e 4c 38 34 32 39 30 31 45 32 39 39 45 38 36 4a 37 57 37 36 34 38 4d 38 35 30 70 36 39 33 34 4b 51 7a 36 47 37 77 32 31 32 35 35 66 46 36 30 0d 0a 32 37 55 58 68 58 30 32 34 52 51 75 75 6c 34 32 6a 79 38 39 54 37 6d 35 70 36 6a 37 37 36 31 35 38 67 31 37 38 31 39 0d 0a 63 38 6d 34 31 31 71 74 75 6f 31 38 34 70 37 36 32 4d 33 35 33 37 65 34 31 36 41 4f 79 71 51 63 73 76 76 77 61 50 47 34 34 33 31 6a 34 4d 47 57 37 30 32 36 62 49 77 36 50 34 6b 35 48 53 0d 0a 63 64 36 75 69 34 35	85Va5DGRx4292b957Tb4 0n5U7H14FU 09fa67186d3cD..3377t8m7 81iyR31 NN3gpo4S0b69C2fa7hH41 ws745iFH2 8377NL842901E299E86J7 W7648M850 p6934KQz6G7w21255fF60 ..27UXhX0 24RQuul42jy89T7m5p6j77 6158g178 19..c8m411qtuo184p762M 3537e416 AOyqQcsvvwaPG4431j4M GW7026bIw6 P4k5HS..cd6ui45	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\neirnbgp.txt	unknown	591	36 75 38 66 6c 37 46 30 57 52 36 38 59 61 54 38 39 74 78 31 50 34 67 32 42 43 45 43 35 0d 0a 35 4a 36 71 69 61 76 64 65 33 75 77 54 34 31 33 37 39 35 46 35 72 58 33 32 49 31 39 4c 34 39 4a 72 63 36 31 4c 35 37 32 70 0d 0a 4f 33 32 42 39 39 35 0d 0a 35 32 34 35 7a 31 32 77 49 58 55 4a 4e 39 33 55 38 69 47 65 38 35 39 46 4c 37 46 39 33 34 6e 31 37 34 34 48 59 74 77 36 4a 4f 31 32 38 36 32 35 56 77 35 44 35 56 38 6f 34 69 61 77 37 36 78 35 34 31 39 7a 50 43 38 39 31 32 38 37 36 4d 66 4d 56 52 47 4f 35 55 38 61 7a 31 30 4e 32 6b 78 32 72 39 68 63 74 4f 70 6d 6c 30 31 32 37 39 6d 0d 0a 31 34 35 32 30 35 77 4d 6a 39 39 39 6f 56 30 32 77 34 4a 51 36 47 6e 39 72 32 33 75 48 62 61 74 72 35 36 68 38 36 6c 34 58 34 33 42 39 56 78 4a 30 4c 53 32 7a 38 33 6e 36 50 31	6u8fl7F0WR68YaT89tx1P 4g2BCEC5. .5J6qiavde3uwT413795F5r X32I19L 49Jrc61L572p..O32B995.. 5245z12 wIXUJN93U8iGe859FL7F9 34n1744HY tw6JO128625Vw5D5V8o4i aw76x5419 zPC8912876MfMVRGO5U 8az10N2kx2r 9hctOpml01279m..145205 wMj999oV 02w4JQ6Gn9r23uHbatr56h 86l4X43B 9VxJ0LS2z83n6P1	success or wait	1	EE9CC2	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\gencjb.ico	unknown	534	38 31 38 62 57 36 7a 39 67 63 42 79 37 34 70 34 33 75 57 66 39 37 31 42 36 37 33 36 37 74 32 46 71 54 52 34 31 0d 0a 39 41 32 30 4e 38 4a 4c 74 75 39 49 39 30 4f 32 31 30 38 42 38 46 78 32 39 31 33 33 33 33 72 33 47 51 33 33 34 42 37 62 32 32 31 73 4f 33 4b 48 39 75 45 36 30 31 69 33 30 6c 33 38 36 4a 4e 49 30 33 36 30 32 46 30 52 64 32 38 61 67 4f 47 46 39 58 4d 33 0d 0a 37 37 32 33 4b 4c 34 34 35 6a 35 68 32 34 6a 34 46 38 30 78 38 38 38 35 59 34 32 59 39 4e 31 37 78 35 32 54 4a 32 6a 39 72 45 34 4d 42 34 68 34 38 66 38 34 30 37 36 50 31 56 6f 30 79 38 33 35 33 30 68 53 70 32 48 30 67 39 74 4b 77 55 34 34 30 4d 35 33 6d 4a 77 31 32 33 5a 32 68 6e 47 74 42 31 30 39 37 35 5a 68 30 5a 39 56 36 39 76 34 70 75 38 7a 52 34 53 33 48 38 50 32 45 36 33 6a 55 65	818bW6z9gcBy74p43uWf9 71B67367t 2FqTR41..9A20N8JLtu9I9 0O2108B8 Fx2913333r3GQ334B7b22 1sO3KH9uE 601i30l386JNI03602F0Rd2 8agOGF9 XM3..7723KL445j5h24j4F8 0x8885Y 42Y9N17x52TJ2j9rE4MB4 h48f84076 P1Vo0y83530hSp2H0g9tK wU440M53m Jw123Z2hnGtB10975Zh0Z 9V69v4pu8 zR4S3H8P2E63jUe	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\lpiuchwp.xls	unknown	534	34 35 4d 53 41 32 35 37 74 51 65 75 33 61 68 76 42 38 37 39 37 35 37 39 37 5a 36 55 4c 39 6f 7a 79 35 33 4c 38 66 36 63 43 37 7a 32 47 32 35 35 38 4a 69 59 5a 33 0d 0a 4b 41 39 6b 35 77 4d 76 38 34 69 67 64 33 54 44 71 77 42 34 7a 56 69 6e 50 4e 31 6a 6b 66 36 37 70 38 30 33 72 30 32 35 79 37 37 39 53 30 69 32 42 34 66 31 51 31 6a 36 39 50 33 36 39 4e 37 34 35 58 37 38 48 46 33 6d 53 34 39 32 67 68 32 32 33 6d 74 39 39 32 43 42 30 31 6e 76 6c 30 34 37 38 38 34 71 39 38 0d 0a 32 6b 38 39 33 37 43 34 36 76 48 30 33 36 4b 43 38 39 36 64 63 30 4f 64 4f 63 43 71 52 31 6c 33 62 37 36 59 4a 58 76 70 31 38 31 42 4a 34 31 76 34 39 0d 0a 64 7a 7a 4a 73 6f 74 59 33 38 38 33 37 7a 50 35 38 41 5a 37 71 69 74 38 35 39 71 31 4a 35 36 6d 45 36 35 30 30 39 31 36 31 0d 0a	45MSA257tQeu3ahvB879 75797Z6UL9 ozy53L8f6cC7z2G2558JiY Z3..KA9k 5wMv84igd3TDqwB4zVinP N1jkf67p8 03r025y779S0i2B4f1Q1j69 P369N74 5X78HF3mS492gh223mt9 92CB01nvl0 47884q98..2k8937C46vH0 36KC896d c0OdOcCqR1l3b76YJXvp 181BJ41v49 ..dzzJsotY38837zP58AZ7 qit859q1J56mE65009161..	success or wait	1	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\ajwiqng.bin	unknown	551	53 45 72 36 57 43 56 6d 35 31 39 67 58 76 35 32 53 35 6e 38 6a 4d 46 7a 52 49 39 30 65 59 32 64 38 34 74 34 6b 39 4e 56 52 51 37 39 46 30 42 7a 35 32 6c 76 36 45 4d 52 77 4f 37 66 33 30 32 51 65 52 31 68 51 4f 0d 0a 33 79 39 36 75 30 41 35 34 70 59 7a 39 36 63 31 31 34 72 33 46 39 31 41 38 62 56 57 78 5a 30 31 78 62 69 45 43 35 76 57 30 56 32 71 49 56 37 50 4d 75 31 38 30 32 54 6b 4c 76 36 57 32 39 38 38 6f 74 4e 5a 32 32 55 38 68 31 39 39 38 6f 38 72 66 38 32 31 30 31 30 32 32 31 72 4a 37 31 36 69 0d 0a 36 47 43 39 4f 7a 46 50 62 53 6c 6b 46 59 53 32 34 34 38 62 38 4f 32 61 67 34 33 6e 5a 67 39 74 37 33 47 79 66 31 6e 55 36 39 43 36 56 33 33 53 34 46 47 51 33 32 38 72 7a 6a 31 37 79 39 4a 31 52 32 72 35 30 32 30 64 36 36 35 44 6e 6b 34 34 7a 32 30 70 31	SEr6WCVm519gXv52S5n 8jMFzRI90eY 2d84t4k9NVRQ79F0Bz52l v6EMRwO7f 302QeR1hQO..3y96u0A54 pYz96c114 r3F91A8bVWxZ01xbiEC5v W0V2qIV7P Mu1802TkLv6W2988otNZ 22U8h1998o 8rf821010221rJ716i..6GC9 OzFPbS lkFYS2448b8O2ag43nZg9t 73Gyf1nU 69C6V33S4FGQ328rzj17y 9J1R2r502 0d665Dnk44z20p1	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\pravpih.msc	unknown	573	33 6c 34 65 39 37 33 34 32 6d 71 4a 31 62 32 31 38 47 61 71 33 34 73 31 39 37 38 6e 45 30 31 39 33 32 74 45 63 33 45 4d 41 75 6c 4c 38 0d 0a 34 77 69 30 34 37 4d 34 33 36 59 39 31 56 6c 6f 79 33 44 45 59 36 30 66 4a 33 31 71 67 37 32 37 35 35 36 39 76 47 78 66 61 4a 4f 4a 37 64 33 45 42 55 68 31 35 53 32 32 7a 59 43 50 38 67 31 32 37 38 30 67 35 79 54 52 71 69 42 34 57 36 77 57 36 4a 36 35 39 78 6a 69 44 39 49 50 38 56 78 30 44 31 30 33 33 32 63 6f 6e 78 76 33 32 32 70 66 50 51 58 71 32 33 36 31 31 4b 33 38 59 74 37 43 35 5a 33 4f 36 39 39 51 37 33 71 68 30 45 33 74 35 39 6d 45 59 31 37 37 43 37 33 0d 0a 56 71 39 36 37 35 74 35 33 45 36 36 31 46 32 67 37 71 32 36 44 41 38 35 30 66 79 79 32 55 7a 79 33 44 35 39 66 4b 35 54 6b 42 62 30 36 30 31 4a 65 36 76	3l4e97342mqJ1b218Gaq3 4s1978nE0 1932tEc3EMAulL8..4wi047 M436Y91 Vloy3DEY60fJ31qg727556 9vGxfaJO J7d3EBUh15S22zYCP8g1 2780g5yTRq iB4W6wW6J659xjiD9IP8V x0D10332c onxv322pfPQXq23611K38 Yt7C5Z3O6 99Q73qh0E3t59mEY177C 73..Vq9675 t53E661F2g7q26DA850fyy 2Uzy3D59 fK5TkBb0601Je6v	success or wait	1	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\crfgiqf.ini	unknown	528	65 73 39 34 38 35 35 72 74 34 4f 39 6d 55 49 36 31 33 37 32 35 34 37 32 35 65 37 53 72 36 4d 37 39 67 32 36 62 4f 30 71 64 31 35 0d 0a 43 61 70 32 39 33 68 38 74 30 48 74 39 70 36 30 39 33 33 67 68 58 34 30 7a 4f 37 39 33 33 35 30 6f 37 79 63 35 38 31 35 32 35 66 30 6a 32 39 45 62 76 74 32 47 56 33 39 30 31 33 36 6f 37 6a 30 68 39 30 58 37 32 57 35 58 30 41 36 65 71 39 31 34 62 37 32 56 34 68 37 39 34 38 38 4a 5a 34 69 32 31 4c 67 31 68 33 48 30 35 39 6f 30 38 39 38 46 31 37 71 35 39 55 35 37 38 77 35 32 41 67 31 70 55 4c 35 39 30 54 37 68 75 33 39 64 32 51 32 31 39 79 0d 0a 67 56 36 5a 4d 38 76 37 4e 66 75 32 34 73 71 66 75 72 30 57 34 31 45 0d 0a 68 56 4e 38 56 31 30 39 73 37 74 4e 6e 39 4a 33 47 39 59 30 37 64 32 38 30 52 37 30 71 75 30 45 66 44 45 4d	es94855rt4O9mUI6137254 725e7Sr6 M79g26bO0qd15..Cap293 h8t0Ht9p6 0933ghX40zO793350o7yc 581525f0j 29Ebvt2GV390136o7j0h90 X72W5X0A 6eq914b72V4h79488JZ4i2 1Lg1h3H0 59o0898F17q59U578w52A g1pUL590T 7hu39d2Q219y..gV6ZM8v 7Nfu24sqf ur0W41E..hVN8V109s7tN n9J3G9Y07 d280R70qu0EfDEM	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\mheqq.log	unknown	549	56 36 30 5a 45 32 31 31 35 35 39 39 42 31 32 49 32 35 48 7a 4f 42 49 4d 39 31 71 76 4e 4f 6d 57 6b 67 45 6e 72 39 38 51 61 35 64 54 37 70 0d 0a 77 68 34 31 36 6d 5a 74 4b 79 63 47 6d 38 35 78 33 4a 39 31 57 30 49 30 35 77 44 41 4f 33 36 4f 53 30 34 36 55 72 34 4e 69 58 35 38 30 64 6d 33 31 77 50 33 57 63 38 48 79 45 30 30 36 46 78 35 0d 0a 58 30 7a 31 30 49 38 36 32 43 59 71 32 37 34 36 36 53 52 6c 39 35 79 30 6f 6c 31 75 64 37 39 72 35 31 6f 61 31 6b 33 5a 36 39 72 45 37 37 57 34 65 73 36 51 58 34 30 39 56 6e 37 37 37 59 32 68 62 33 73 54 37 39 34 34 35 32 51 74 39 39 54 32 35 4a 36 62 74 36 37 50 31 75 30 36 45 58 48 4d 36 32 46 77 34 36 36 5a 0d 0a 37 38 35 35 45 33 32 39 34 35 38 34 38 75 71 31 32 36 61 57 37 30 43 6d 35 45 5a 34 46 67 4e 31 50 32 38	V60ZE2115599B12I25HzO BIM91qvNO mWkgEnr98Qa5dT7p..wh4 16mZtKycG m85x3J91W0I05wDAO36 OS046Ur4NiX 580dm31wP3Wc8HyE006 Fx5..X0z10I 862CYq27466SRl95y0ol1u d79r51oa 1k3Z69rE77W4es6QX409 Vn777Y2hb3 sT794452Qt99T25J6bt67P 1u06EXHM 62Fw466Z..7855E3294584 8uq126aW 70Cm5EZ4FgN1P28	success or wait	1	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\ksfdlrauwr.mp3	unknown	563	31 56 36 39 52 59 6f 37 45 74 33 31 52 45 34 45 54 31 36 37 38 75 42 68 39 39 30 38 38 59 33 67 34 34 52 31 36 39 64 36 39 77 78 51 6b 39 41 6d 6f 35 4d 43 31 31 4e 0d 0a 37 31 32 63 39 30 34 61 37 6f 5a 56 4e 47 79 75 38 36 4c 6a 63 53 33 48 37 37 6b 36 62 35 64 6a 65 33 36 46 37 35 41 56 34 59 33 39 38 37 47 5a 30 37 75 5a 57 36 52 5a 61 33 50 30 43 30 68 51 31 4b 32 6b 30 51 34 67 7a 4b 36 6c 33 0d 0a 4b 46 62 33 61 34 31 44 36 43 36 36 4f 75 76 6c 31 62 30 42 77 4f 58 32 34 76 30 38 54 62 58 32 38 39 4c 37 31 36 4a 7a 39 48 5a 30 53 36 4e 44 52 4b 75 38 34 72 47 39 55 54 32 36 38 31 4b 67 79 6d 47 52 33 50 59 33 6e 4f 34 69 36 58 62 64 73 7a 38 30 31 38 69 74 36 34 57 45 31 30 30 41 78 43 64 4b 4a 5a 67 32 76 32 64 30 0d 0a 30 38 48 38 64 6d 68 36 45	1V69RYo7Et31RE4ET167 8uBh99088Y 3g44R169d69wxQk9Amo5 MC11N..712 c904a7oZVNGyu86LjcS3H 77k6b5dje 36F75AV4Y3987GZ07uZ W6RZa3P0C0h Q1K2k0Q4gzK6l3..KFb3a 41D6C66Ou vl1b0BwOX24v08TbX289L 716Jz9HZ0 S6NDRKu84rG9UT2681Kg ymGR3PY3nO 4i6Xbdsz8018it64WE100A xCdKJZg2 v2d0..08H8dmh6E	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\rvhkj.pdf	unknown	665	52 65 38 34 7a 35 31 36 78 30 56 78 58 32 32 39 7a 6e 36 33 70 61 34 71 46 38 36 32 6e 43 49 31 33 37 38 47 75 32 31 37 0d 0a 36 30 76 31 71 31 30 46 32 38 66 37 32 36 32 34 39 35 38 74 32 4c 37 38 77 4b 34 48 49 35 56 39 5a 35 69 35 30 36 39 6b 70 37 78 4d 31 56 37 34 49 38 66 32 67 39 32 39 31 31 33 73 44 37 39 45 35 61 39 52 39 56 32 31 78 75 48 63 5a 31 6f 34 33 49 37 37 31 70 65 39 73 33 35 4b 54 74 39 35 38 6b 46 64 5a 37 39 31 74 0d 0a 45 65 70 4a 36 32 35 69 36 56 33 32 52 36 33 35 6a 76 58 73 6d 73 39 35 58 4a 35 53 61 31 34 4e 0d 0a 4f 54 34 4e 72 6d 35 4b 34 64 35 59 31 34 6a 6a 6d 33 39 59 67 74 4a 43 39 68 31 39 31 39 31 6e 31 73 4f 36 30 43 32 36 65 66 39 0d 0a 31 36 34 5a 48 35 71 62 37 6f 35 30 73 36 30 37 58 0d 0a 33 39 6c 35 52 36 52 45	Re84z516x0VxX229zn63p a4qF862nC I1378Gu217..60v1q10F28f 7262495 8t2L78wK4HI5V9Z5i5069k p7xM1V74 I8f2g929113sD79E5a9R9V 21xuHcZ1 o43I771pe9s35KTt958kFd Z791t..E epJ625i6V32R635jvXsms9 5XJ5Sa14 N..OT4Nrm5K4d5Y14jjm3 9YgtJC9h1 9191n1sO60C26ef9..164Z H5qb7o50 s607X..39l5R6RE	success or wait	1	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\ckcsljuf.txt	unknown	570	77 72 70 33 62 6d 35 63 6c 39 61 31 59 57 48 48 38 5a 4d 78 54 34 76 0d 0a 34 32 33 64 51 35 31 32 55 38 47 31 34 37 75 4f 59 32 5a 37 66 39 50 46 4b 39 36 37 30 32 31 37 65 77 58 55 67 66 7a 6b 38 78 68 6e 32 37 35 33 39 62 71 6c 6b 43 39 5a 51 6b 35 33 4f 35 36 34 78 32 36 58 31 7a 33 36 43 75 58 33 0d 0a 73 36 41 34 35 76 39 61 30 46 39 33 30 39 72 6c 30 4b 39 75 34 6d 61 4a 30 46 33 52 32 50 6b 30 35 36 36 69 30 38 31 54 75 31 39 48 71 32 37 30 35 5a 35 53 61 73 39 74 0d 0a 38 31 46 33 30 35 37 76 32 35 34 31 30 31 34 33 34 37 35 69 5a 35 4a 30 32 34 32 4b 75 35 53 30 6a 66 32 35 57 56 4d 38 76 35 31 31 6c 39 67 32 31 6d 72 36 70 30 33 31 39 30 37 58 52 30 38 68 34 32 64 56 65 4c 69 72 33 4c 36 6a 42 33 57 44 4a 73 33 71 34 32 77 34 30 72 42 73 34 61	wrp3bm5cl9a1YWHH8ZMx T4v..423dQ 512U8G147uOY2Z7f9PFK 9670217ewX Ugfzk8xhn27539bqlkC9ZQ k53O564x 26X1z36CuX3..s6A45v9a0 F9309rl0 K9u4maJ0F3R2Pk0566i08 1Tu19Hq27 05Z5Sas9t..81F3057v2541 0143475 iZ5J0242Ku5S0jf25WVM8 v511l9g21 mr6p031907XR08h42dVeL ir3L6jB3W DJs3q42w40rBs4a	success or wait	1	EE9CC2	WriteFile
C:\Users\user\AppData\Roaming\89378384\jlotan.ini	unknown	574	36 31 31 39 76 30 37 4c 43 38 4c 34 4a 41 35 44 52 30 41 42 4e 36 33 37 7a 77 57 30 64 74 32 0d 0a 48 4a 33 57 35 63 39 34 6f 32 4b 35 6b 4f 37 30 68 32 48 57 35 44 32 48 30 33 4c 73 62 45 32 42 69 45 6b 33 75 4c 30 78 38 0d 0a 36 53 50 61 36 36 54 53 35 36 6f 38 4a 30 6b 31 63 34 34 47 78 34 31 33 33 36 34 43 4d 35 4a 47 38 44 54 33 30 38 38 33 65 31 34 30 34 75 39 6e 30 38 76 36 32 35 33 34 31 30 31 37 4e 69 35 79 64 35 70 59 6b 62 34 31 38 74 31 31 31 32 34 32 53 41 31 61 6a 67 30 31 32 59 37 4f 7a 30 31 30 61 79 56 6b 32 33 6e 4c 32 33 68 32 30 35 32 38 39 57 66 33 36 38 0d 0a 30 43 36 35 71 6b 57 35 30 30 55 30 54 32 4e 73 66 51 35 31 37 44 38 7a 37 6e 34 6d 0d 0a 61 53 39 36 39 73 33 79 79 58 75 38 31 30 55 45 4d 39 32 4c 5a 49 71 4b 76 76 49 30 73	6119v07LC8L4JA5DR0AB N637zwW0dt 2..HJ3W5c94o2K5kO70h2 HW5D2H03L sbE2BiEk3uL0x8..6SPa66 TS56o8J0 k1c44Gx413364CM5JG8D T30883e140 4u9n08v625341017Ni5yd5 pYkb418t 111242SA1ajg012Y7Oz01 0ayVk23nL 23h205289Wf368..0C65qk W500U0T2 NsfQ517D8z7n4m..aS969 s3yyXu810 UEM92LZIqKvvI0s	success or wait	1	EE9CC2	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\89378384\cxijg.ico	unknown	596	6e 31 32 54 75 38 35 4b 4f 38 50 37 67 38 32 32 4f 5a 75 51 35 71 66 35 33 46 6e 71 72 33 39 67 30 30 65 35 39 4b 4e 36 35 38 39 37 37 30 38 61 32 6e 75 32 6a 34 6b 32 5a 31 51 78 30 34 75 6d 37 38 36 68 39 55 33 55 44 7a 56 53 68 50 33 30 32 33 59 37 36 63 77 76 76 33 38 4e 75 4e 31 7a 36 38 35 33 38 54 61 62 64 48 36 38 35 39 6c 58 39 42 30 39 57 4e 45 79 39 36 71 38 36 73 4d 55 42 39 62 38 31 4c 30 36 35 56 68 31 55 4c 44 38 47 34 6f 6d 33 59 6d 36 36 31 44 59 31 31 66 39 75 55 66 56 74 75 62 38 0d 0a 76 58 36 31 44 66 32 37 36 47 32 47 57 30 4a 31 31 6c 42 64 31 6c 31 39 44 58 38 32 7a 33 33 37 6f 30 33 64 78 33 6f 32 4c 43 36 36 6a 78 31 7a 39 36 31 35 56 78 35 41 62 75 36 36 41 37 46 34 53 67 4f 48 4e 32 48 30 64 39 65 33 49 31 79 54 63 77 37 32 50	n12Tu85KO8P7g822OZuQ 5qf53Fnqr3 9g00e59KN65897708a2nu 2j4k2Z1Qx 04um786h9U3UDzVShP30 23Y76cwvv3 8NuN1z68538TabdH6859l X9B09WNEy 96q86sMUB9b81L065Vh1 ULD8G4om3Y m661DY11f9uUfVtub8..vX 61Df276G 2GW0J11lBd1l19DX82z33 7o03dx3o2 LC66jx1z9615Vx5Abu66A 7F4SgOHN2 H0d9e3I1yTcw72P	success or wait	1	EE9CC2	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SWIFTS.scr.exe	unknown	8192	success or wait	132	EE9678	ReadFile

Analysis Process: qtfarawjob.pif PID: 6132 Parent PID: 4104

General

Start time:	05:07:12
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif' odfugpcmco.org
Imagebase:	0xf0000
File size:	662768 bytes
MD5 hash:	F471B7C16D5B01AF9F67F5F4A921F81F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343262575.00000000049D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343194863.0000000004A51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343194863.0000000004A51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343194863.0000000004A51000.00000004.00000001.sdmp, Author:

Kevin Breen <kevin@techanarchy.net>

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343095716.0000000004A84000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343095716.0000000004A84000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343095716.0000000004A84000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.345055331.00000000049D1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.345055331.00000000049D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.345055331.00000000049D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.345307078.0000000004A83000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.345307078.0000000004A83000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.345307078.0000000004A83000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343476102.0000000004AB6000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343476102.0000000004AB6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343476102.0000000004AB6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343140164.0000000004A04000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343140164.0000000004A04000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343140164.0000000004A04000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343507843.0000000004AE9000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343507843.0000000004AE9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343507843.0000000004AE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343433163.0000000004AB6000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343433163.0000000004AB6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343433163.0000000004AB6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.344666735.0000000004A03000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.344666735.0000000004A03000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.344666735.0000000004A03000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.345446557.0000000004A51000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.345446557.0000000004A51000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.345446557.0000000004A51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343592182.0000000004B1B000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343592182.0000000004B1B000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343592182.0000000004B1B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.345193902.0000000004AB6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.345193902.0000000004AB6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.345193902.0000000004AB6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.343388307.0000000004A03000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.343388307.0000000004A03000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.343388307.0000000004A03000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	12362A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	13BEBA	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0	45152	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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L...zX.Z..... ....0..d.....V.... .....@.. ...."....`.....	success or wait	1	13BEBA	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
unknown	unknown	65536	success or wait	1905	10DB2F	ReadFile
unknown	unknown	24576	end of file	2	10DB2F	ReadFile
C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	unknown	65536	success or wait	1	F3B98	ReadFile
C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	unknown	65536	success or wait	1849	F3B98	ReadFile
C:\Users\user\AppData\Roaming\89378384\odfugpcmco.org	unknown	65536	end of file	1	F3B98	ReadFile
C:\Users\user\AppData\Roaming\89378384\lklphvrvl.dll	unknown	65536	success or wait	1	F3B98	ReadFile
C:\Users\user\AppData\Roaming\89378384\lklphvrvl.dll	unknown	65536	success or wait	8	F3B98	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	WindowsUpdate	unicode	C:\Users\user\AppData\Roaming\89378384\QTFARA~1.PIF C:\Users\user\AppData\Roaming\89378384\ODFUGP~1.ORG	success or wait	1	15ADDA	RegSetValueExW

Analysis Process: RegSvcs.exe PID: 1972 Parent PID: 6132

General

Start time:	05:07:17
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xa00000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593935065.0000000006F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593935065.0000000006F20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.590990913.0000000004495000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593967539.0000000006F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593967539.0000000006F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.594092572.0000000006F80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.594092572.0000000006F80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.536569006.00000000051C8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593813593.0000000006EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593813593.0000000006EC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.592048655.00000000051A7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.592048655.00000000051A7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.594107341.0000000006F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.594107341.0000000006F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.591934672.00000000050BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.591488895.0000000004E76000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.594522145.0000000007490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.594522145.0000000007490000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593310031.0000000005F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593310031.0000000005F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.593310031.0000000005F70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593746192.0000000006EB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593746192.0000000006EB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.594053531.0000000006F60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.594053531.0000000006F60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593208278.0000000005D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593208278.0000000005D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593916225.0000000006F10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593916225.0000000006F10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593893788.0000000006F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593893788.0000000006F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.591902295.00000000050A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.587691040.00000000034AC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.586093866.0000000000E02000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.586093866.0000000000E02000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.586093866.0000000000E02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.594026273.0000000006F50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.594026273.0000000006F50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.593985539.0000000006F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.593985539.0000000006F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.587531110.0000000003441000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Reputation:	high

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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA342.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA342.tmp	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	6a 50 9b 85 ab fd d8 48	jP.....H	success or wait	1	6CF41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA342.tmp	unknown	1311	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	48	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Users\user\AppData\Local\Temp\RegSvcs.exe	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	9	6CF41B4F	WriteFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CF41B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	512	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E0BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E0BD72F	unknown

Analysis Process: schtasks.exe PID: 3120 Parent PID: 1972

General

Start time:	05:07:20
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA342.tmp'
Imagebase:	0xcf0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA342.tmp	unknown	2	success or wait	1	CFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA342.tmp	unknown	1312	success or wait	1	CFABD9	ReadFile

Analysis Process: conhost.exe PID: 2404 Parent PID: 3120

General

Start time:	05:07:20
Start date:	12/04/2021
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: RegSvcs.exe PID: 5864 Parent PID: 936

General

Start time:	05:07:23
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0x7e0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CF41B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CF41B4F	WriteFile
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	6CF41B4F	WriteFile
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6E40C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile

Analysis Process: conhost.exe PID: 4908 Parent PID: 5864

General

Start time:	05:07:23
Start date:	12/04/2021
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: qtfarawjob.pif PID: 5900 Parent PID: 3440

General

Start time:	05:07:24
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\89378384\qtfarawjob.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\89378384\QTFARA~1.PIF' C:\Users\user\AppData\Roaming\89378384\ODFUGP~1.ORG
Imagebase:	0xf0000
File size:	662768 bytes
MD5 hash:	F471B7C16D5B01AF9F67F5F4A921F81F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.369835210.0000000003EF4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.369835210.0000000003EF4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.369835210.0000000003EF4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.371760898.0000000003EC1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.371760898.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.371760898.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.370790447.0000000003E17000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.370790447.0000000003E17000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.370790447.0000000003E17000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.371839238.0000000003FA6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.371839238.0000000003FA6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.371839238.0000000003FA6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.371972017.0000000003F73000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.371972017.0000000003F73000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.371972017.0000000003F73000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.372073303.0000000003F41000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.372073303.0000000003F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.372073303.0000000003F41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.369800232.0000000003F74000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.369800232.0000000003F74000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.369800232.0000000003F74000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.369871220.0000000003F41000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.369871220.0000000003F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.369871220.0000000003F41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.370824550.0000000003DF5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.370824550.0000000003DF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.370824550.0000000003DF5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.371528290.0000000003EF3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.371528290.0000000003EF3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.371528290.0000000003EF3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.369946595.0000000003EC1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.369946595.0000000003EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.369946595.0000000003EC1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.370138817.0000000003FD9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.370138817.0000000003FD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.370138817.0000000003FD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000003.370011747.0000000003F73000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000003.370011747.0000000003F73000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000003.370011747.0000000003F73000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000003.370011747.0000000003F73000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegSvcs.exe PID: 2932 Parent PID: 5900

General

Start time:	05:07:29
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x620000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.388090942.0000000000A02000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.388090942.0000000000A02000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.388090942.0000000000A02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.389362789.0000000003001000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.389362789.0000000003001000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.389636385.0000000004009000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.389636385.0000000004009000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0FCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Disassembly

Code Analysis