ID: 796783
Sample Name:
026910003102350.pdf.scr.exe
Cookbook: default.jbs
Time: 08:08:12
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2023

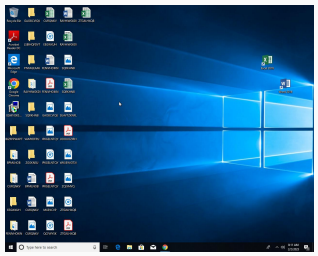
Windows Analysis Report

026910003102350.pdf.scr.exe

Overview

General Information

Sample Name:	026910003102350.pdf.scr.exe
Analysis ID:	796783
MD5:	c2a80ccf6362b..
SHA1:	c7a0ca8b35e2...
SHA256:	592217d2590a...
Tags:	exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

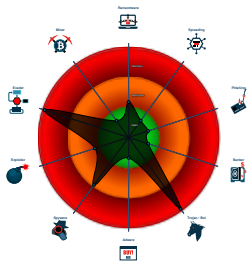
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: Scheduled temp fil...
- Multi AV Scanner detection for dom...
- Multi AV Scanner detection for drop...
- Starts an encoded Visual Basic Scr...

Classification



Process Tree

- **System is w10x64**
- 026910003102350.pdf.scr.exe (PID: 4980 cmdline: C:\Users\user\Desktop\026910003102350.pdf.scr.exe MD5: C2A80CCF6362BBA805072DE9CE963EA5)
  - wscript.exe (PID: 2312 cmdline: "C:\Windows\System32\wscript.exe" daitsfsh-waune.icm.vbe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - itugx.exe (PID: 5920 cmdline: "C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe" rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
      - RegSvcs.exe (PID: 5960 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
        - schtasks.exe (PID: 4544 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp897A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 5648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 2216 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp8D34.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 1648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- itugx.exe (PID: 3300 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
  - RegSvcs.exe (PID: 4736 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- RegSvcs.exe (PID: 5072 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 2960 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 2896 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - itugx.exe (PID: 4036 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
    - RegSvcs.exe (PID: 3624 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 576 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- itugx.exe (PID: 5928 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
  - RegSvcs.exe (PID: 5508 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 4776 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - itugx.exe (PID: 5420 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
    - RegSvcs.exe (PID: 5736 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- itugx.exe (PID: 5552 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
  - RegSvcs.exe (PID: 3928 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 5776 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs" MD5:

Copyright Joe Security LLC 2023

9A68ADD12EB50DDE7586782C3EB9FF9C)
- itugx.exe (PID: 1712 cmdline: "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls MD5: 8A57722EC9067FAAA9FF2980C5F02838)
  - RegSvcs.exe (PID: 4764 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)

- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "d95e5ad5-6193-4689-a919-7befded6",
  "Group": "ITEego",
  "Domain1": "december2n.duckdns.org",
  "Domain2": "december2nd.ddns.net",
  "Port": 60705,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 29996,
  "MutexTimeout": 4996,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1104d:$x1: NanoCore.ClientPluginHost • 0x1108a:$x2: IClientNetworkHost • 0x14bbd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10db5:$a: NanoCore • 0x10dc5:$a: NanoCore • 0x10ff9:$a: NanoCore • 0x1100d:$a: NanoCore • 0x1104d:$a: NanoCore • 0x10e14:$b: ClientPlugin • 0x11016:$b: ClientPlugin • 0x11056:$b: ClientPlugin • 0x10f3b:$c: ProjectData • 0x11942:$d: DESCrypto • 0x1930e:$e: KeepAlive • 0x172fc:$g: LogClientMessage • 0x134f7:$i: get_Connected • 0x11c78:$j: #=q • 0x11ca8:$j: #=q • 0x11cc4:$j: #=q • 0x11cf4:$j: #=q • 0x11d10:$j: #=q • 0x11d2c:$j: #=q • 0x11d5c:$j: #=q • 0x11d78:$j: #=q
00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x1104d:$a1: NanoCore.ClientPluginHost • 0x1100d:$a2: NanoCore.ClientPlugin • 0x12f66:$b1: get_BuilderSettings • 0x10e69:$b2: ClientLoaderForm.resources • 0x12686:$b3: PluginCommand • 0x1103e:$b4: IClientAppHost • 0x1b4be:$b5: GetBlockHash • 0x135be:$b6: AddHostEntry • 0x172b1:$b7: LogClientException • 0x1352b:$b8: PipeExists • 0x11077:$b9: IClientLoggingHost
00000010.00000003.455956530.000000000151D000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x103bd:$x1: NanoCore.ClientPluginHost • 0x103fa:$x2: IClientNetworkHost • 0x13f2d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 247 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
28.3.itugx.exe.146edb8.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
28.3.itugx.exe.146edb8.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
28.3.itugx.exe.146edb8.0.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
28.3.itugx.exe.146edb8.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Copyright Joe Security LLC 2023

Source	Rule	Description	Author	Strings
28.3.itugx.exe.146edb8.0.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 362 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Antivirus detection for dropped file

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Networking

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

Creates multiple autostart registry keys

Creates autostart registry keys with suspicious values (likely registry only malware)

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)

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion

Yara detected AntiVM autoit script

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Found API chain indicative of sandbox detection

HIPS / PFW / Operating System Protection Evasion

Starts an encoded Visual Basic Script (VBE)

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

Detected Nanocore Rat

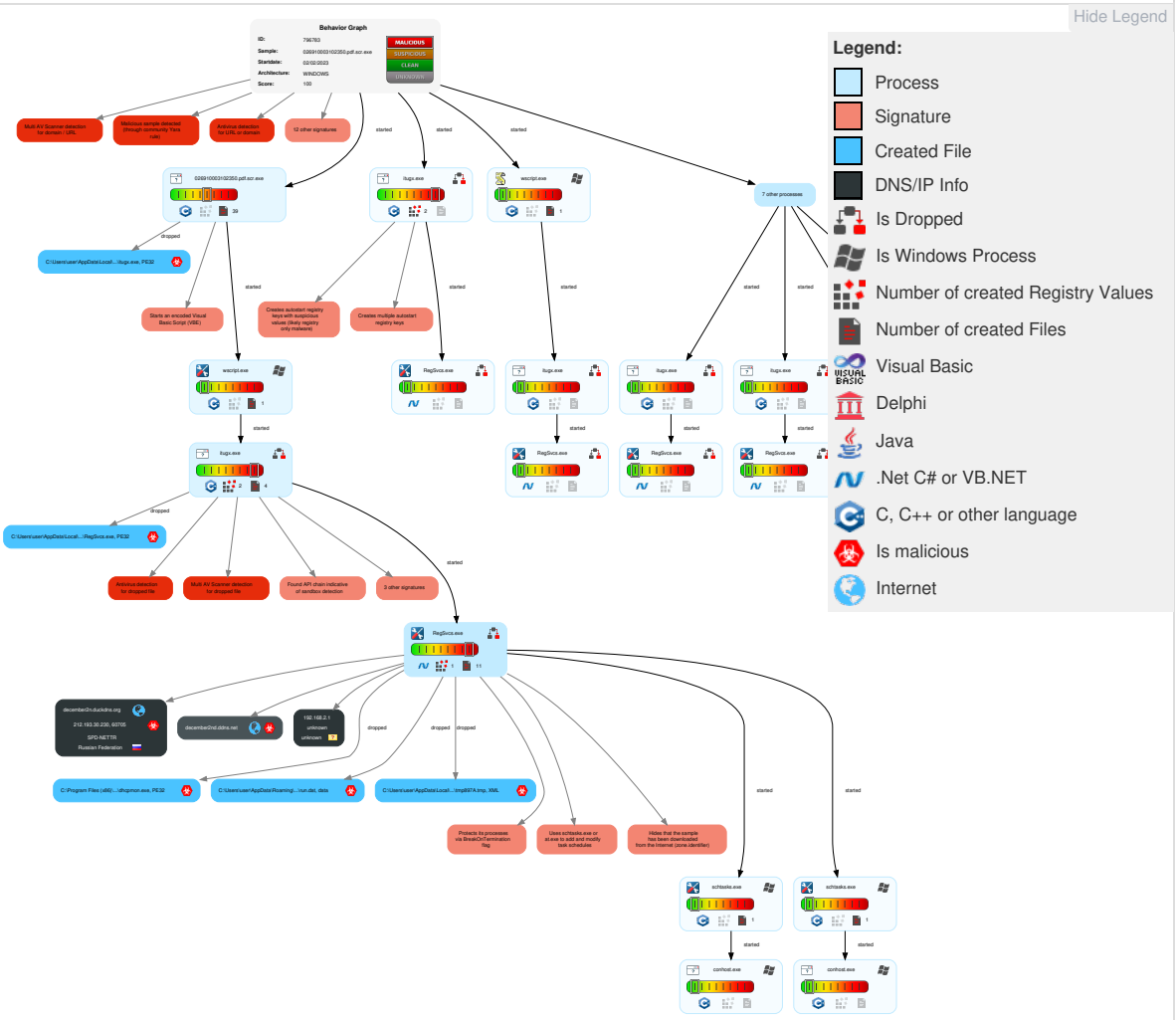
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
2 Valid Accounts	1 1 1 Scripting	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 1 Disable or Modify Tools	3 1 Input Capture	2 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	2 Valid Accounts	1 DLL Side-Loading	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	3 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	2 Valid Accounts	1 1 1 Scripting	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	2 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Scheduled Task/Job	2 1 Registry Run Keys / Startup Folder	2 1 Access Token Manipulation	1 2 Obfuscated Files or Information	NTDS	3 6 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Data Encoding	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	3 1 2 Process Injection	1 2 Software Packing	LSA Secrets	3 4 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Remote Access Software	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Scheduled Task/Job	1 DLL Side-Loading	Cached Domain Credentials	1 2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 Non-Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	2 1 Registry Run Keys / Startup Folder	1 2 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	2 1 Application Layer Protocol	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Valid Accounts	Proc Filesystem	1 1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 2 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	2 1 Access Token Manipulation	Network Sniffing	1 Remote System Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	3 1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Hidden Files and Directories	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

Copyright Joe Security LLC 2023

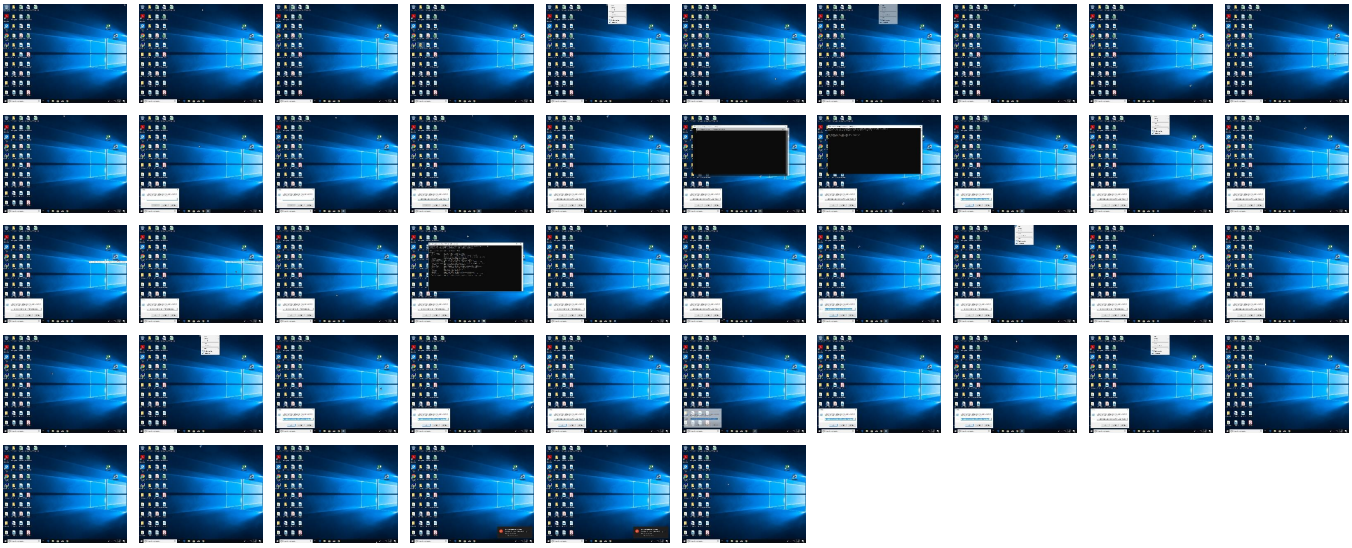
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
026910003102350.pdf.scr.exe	46%	ReversingLabs	Win32.Trojan.Lisk	
026910003102350.pdf.scr.exe	46%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe	100%	Avira	DR/AutoIt.Gen	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe	46%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegSvcs.exe.60b0000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
19.2.RegSvcs.exe.d00000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	12%	Virustotal		Browse
december2n.duckdns.org	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	12%	Virustotal		Browse
december2n.duckdns.org	6%	Virustotal		Browse
december2n.duckdns.org	100%	Avira URL Cloud	malware	
december2nd.ddns.net	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	212.193.30.230	true	true	• 12%, Virustotal, Browse	unknown
december2n.duckdns.org	212.193.30.230	true	true	• 6%, Virustotal, Browse	unknown

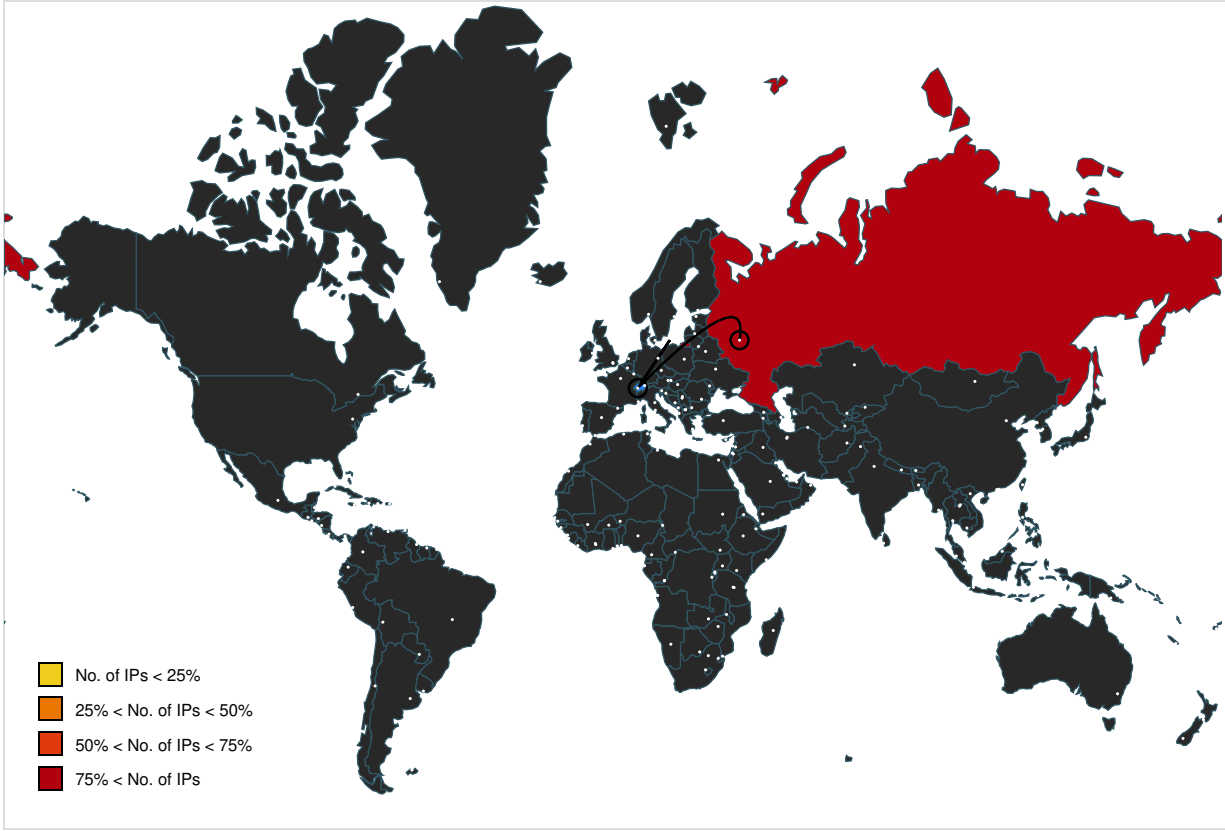
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
december2n.duckdns.org	true	• 6%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.autoitscript.com/autoit3/	026910003102350.pdf.scr.exe, 00000000.00000003.334455690.000000000739F000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RegSvcs.exe, 00000003.00000002.580107208.0000000003781000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.230	december2nd.ddns.net	Russian Federation		57844	SPD-NETTR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796783
Start date and time:	2023-02-02 08:08:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	026910003102350.pdf.scr.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@43/44@4/2

Copyright Joe Security LLC 2023

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99.7% (good quality ratio 92.3%) • Quality average: 78.7% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- 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 NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:10:03	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
08:10:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs
08:10:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
08:10:14	API Interceptor	602x Sleep call for process: RegSvcs.exe modified
08:10:15	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:10:21	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:10:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
08:10:41	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs
08:10:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
08:11:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
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+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\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:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	unknown
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\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.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:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0
Malicious:	false
Reputation:	unknown
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\Folder8_410\Update.vbs	
Process:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	143
Entropy (8bit):	4.963345814111803
Encrypted:	false
SSDEEP:	3:FER/n0eFH5OUkh4E2J5xAIzbgFCdSfNUkh4E2J5xAIzbgbi1A:FER/lFHI923fzbgFeSfN923fzbgb7
MD5:	C3DAE34C95AFBA3A4E22F956B6761EF7
SHA1:	8DD9C50F51E1D8FA7492922AE3E05C8526824D88
SHA-256:	60DFA2FD6C51979E9A3E669F487471408474A5ABB43FFFF5536160401FB0712F
SHA-512:	987681FF2FC61676FE4FDFCBB748740BED5FC64AE9C7087D4D2EB0F492891ABDCBCD34CE2ADBBD50CCB390E098D867C0CE8B1CB4A10C7DD26AB6F1CFF58821E
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls"

C:\Users\user\AppData\Local\Temp\Folder8_410\accdciolx.icm	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	597
Entropy (8bit):	6.186253247413455
Encrypted:	false
SSDEEP:	12:oXEXUz6MlWRGKb57dGZ47amIGP115oCnWRi8UVEpmyvLSoK/:OEXU+71dGG7apGRoYWRizVimyJg
MD5:	9D23B8A8A8DC43EC163438D3E58CDB4E
SHA1:	083823FFA163D66242EC8E04AD9C9A02A3F5F32E
SHA-256:	D249EC95400898681404C2D824E77651C8D8ACFFEBE92F51BC6D337DF11DB895
SHA-512:	ABA25C811AC517981F7F68F803B205E326B89F390E4E4208FE0CA51312EA15F403468C88EBC3C64EDCF8447E377012FCBA100D0BCB04A3BC861FCE041B7EE6D6
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\adietmenbj.mp3	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	503
Entropy (8bit):	6.217480782110286
Encrypted:	false
SSDEEP:	12:BRE/nyLFn4WfUw7LT6aZXxGOAl54d3JcfZCMJL+VUftgAeryz/:n0YdRlFZwvlUJcfZL+VVqr
MD5:	2732EEA4B454A9C18455717D791AA346
SHA1:	6E3F73A1A0ADEA9FDBAE17F9E0208D6AD08B05EC
SHA-256:	64E99289977F284CE1C930F9E27A813C60C4F379E3E38F845E4EF11703ADE375
SHA-512:	69ADE759606DAF638525F6DACBAD04CD8CCCF724F2D1768CA5B3F16545F937D62B28DA738510BA78FBA83A7190DFAF80A1E19914A027DAFDBFDDEAD655F67FCC
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\cgkjjhlj.icm	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	6.181783102675102
Encrypted:	false

SSDEEP:	12:AjJFkEaE4BuYCDwUEY7Yn6eb0yVIHmMY7EC0LuHvZ2ltWDNEpKnFg0T:AjJDZ4BSDwURYn6eb0yVIIvMqEFv
MD5:	B999711E1C647771E59A27D40F75E908
SHA1:	E1DBE34813EF6241B4B227042649805372321794
SHA-256:	6A9A2E454761426D0B07209E1958C520D008D8EFAABB12CFAFE777C15B0FA562
SHA-512:	7A5783199BB73E284E56A3D4D26268DABC6D1973562D91D4253D3EDA9EBD483F89F9D2545146CDE4935FAFF70F981B5B617CDA7B3A25E769C0C9E44BFCE6B876
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\chcekckp.gfh

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	407473
Entropy (8bit):	4.048588207938584
Encrypted:	false
SSDEEP:	3072:/JGA8gDqUGMl95jTDOWmA72KRvgr00mvIIRHqsEZipg7O65J48al5plklct4wyNu:h5VGMBJRvgr09nZiq7OIy8az0a4DuP
MD5:	48F9952AAAFE4CA15D39581E78889AC0
SHA1:	569F6FB010FEFB412192A968784DB355B8311853
SHA-256:	7F322D3E2096AA1F60CBF945595F155314D434A4FDD5A35640DF9363570FE666
SHA-512:	BAE18549694F7D75F24D057F21380C30CA6F9C7579EE3D4EAD2F4CAFF92E541797ABFA970688170501DE1EA378B5F0CAF071B46BD7C28030D6C15EFBA5296B87
Malicious:	false
Reputation:	unknown
Preview:	0x4D5*9--3---04---FFFF--_8-------4----------08----E/F_*0E-_409CD2/_80/4CCD2/546869732070726F67726/6D20636/6E6E6F742062652072756E20696E20444F53206D6F64652E0D0D0*24-------5045--4C0/03-*/27E954--------E--E0/0_0/06--C80/--7E0/-----92E70/--2-----2---4--02----2--04--------04--------*-3--02------02-----/--0/----0/0/------0/----------038E70/-57----2-2-787*0/----------02-0C----------2---8----------082--048----------2E74657874---98C70/--2---0C80/--02-------2--0602E72656C6F63--0C-----02--02---C*0/----------4--0422E72737263---787*0/--2-2--7C0/--CC0/----------4--04----------074E70/-----48---02-05-E4D6--54/-/-03---CE0/-06CCC4--/8/2----------/33-3-5/---0/--//026F35--0*/82E02/62*026F36--0*/E2D0*2606/69//F0*2E332_030*2_F406/69/20*C---330E06/79//F0F3/0706/79//F2032/606/69/20C---0330*06/79/20*8---2E02/62*/72*---033-9-45-------7337--0*/92D28267338--0*/72D26267339--0*/62C242673

C:\Users\user\AppData\Local\Temp\Folder8_410\daitsfsh-waune.icm.vbe

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	62820
Entropy (8bit):	6.7478449446190245
Encrypted:	false
SSDEEP:	768:EaauGtmxdbAYaauGtmxdbAXaauGtmxdbAbaauGtmxdbAXaauGtmxdbA9aauGtmxt:NqJ5qJOqJ6qJOqJYqJ7qJrqJ/qJ5
MD5:	F96269E1056B12E82772B66B0884F8A6
SHA1:	C4D4F2D680A1A95B3FE3462A0F2CF80DC5DD8B05
SHA-256:	2A8C2D73D15B644CFCB109F61099B5501C706CD539D885C3929E35F636A886B8
SHA-512:	4A38D9B82454101EC0BAFE7EA472BCDC457724377F6B4277B7BBBEAE362B402C9012B17F0613B46817F5BF80355E005A01A57A6FE85E6EDF7AB90BF654572596
Malicious:	false
Reputation:	unknown
Preview:	..'..XU}.}...M.....h..)..J...<.]W....C.!..X8:.....'.I.9.0.j.t.6.t.t.6.0.5.1.M.K.7.C.8.7.R.Z.b.z.1.9.5.w.K.8.2.6.2.p.Q.6.9.Z.C.8.5.R.t.8.5.f.....'...!?<.k{.N.3.&g.Q}.S..MS..z.....{.(.5F.9E..vsW...M.....'..b.WqRj..8a..PCd...~c..)o.>.?3...._[Rx..Pb.<I...g..F!.x.O..p.rC..S.I~.9M...*^rD=..8x..h..h..8..9..P....'.w.c.b.o.6.t.e.u.K.2.6.5.Z.X.1.w.O.W.3.8.B.t.d.4.E.a.w.1.8.3.V.1.4.3.8.Y.t.0.7.a.6.1.....'.9.Z.0.4.2.8.6.6.s.3.y.T.1.8.R.Z.0.A.e.t.0.X.R.v.4.i.l.1.j.Z.3.v.r.l.L.0.l.5.Q.8.d.....'.X.9.y.T.5.J.k.0.0.5.l.1.7.R.V.x.7.1.6.c.6.6.8.3.Q.y.m.E.u.6.K.2.a.2.h.7.4.6.1.7.6.E.5.x.O.7.....'.J.V.n.3.9.1.Q.l.4.....'.i.4.4.6.2.W.s.6.7.5.r.0.3.9.4.l.9.f.M.7.M.e.9.7.b.A.5.....'.?.z...!]D...Z.l@.^<..z.so...S...w.:...Jc.wP.....Mm.}.VT.~.....'...3.....c...)Q.zK...D.X.C..3-....w..H0M.hL..(P...~.....\c.5>.B.a.,.&.n.....&..l$3K.....Xz...lq.+U.....E.|.z...i..F#.[M..../\.r}.ZR^.)....c= ..x....'.9.E.7.5.7.p.N.V.0.1.J.6.2.4.a.r.5.....'.....)...C.b./..d....Z..c.....'.e^,...

C:\Users\user\AppData\Local\Temp\Folder8_410\dbhplsxd.msc

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	6.237962640598812
Encrypted:	false
SSDEEP:	12:6Dap/0JWG75MfHN4BgfCct6W/9TM3GoUDAPt4RV:6aEWD7dkl96GNDAPt4RV
MD5:	E96279C4B834A0D1348BA98595380443

SHA1:	B6857B68DE2711C498632D7FAE63702F800B29A0
SHA-256:	E9BC070312838661A856486A6D4433C46AB42AD7C18FA0D0D56943838B44F125
SHA-512:	F267F094F2F39B2225238FB02EB1CB99EB176D6F9DC380F75CF59439D0DF6229DD5F3987377BB23D3424C92288DE86D835605CA0EA0162B4EEB2441259119A71
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\dldgexp.dll

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	6.218187584585582
Encrypted:	false
SSDEEP:	12:B/ZQ2hmQ7kCAxtYCU2QXbx0VgIrrkUC7GDAIh7mJbHz+t:B58DbLexFIV4GD3tmpSt
MD5:	06FEEDE36DB05B3D230E3081419A19A2
SHA1:	2D69F4B7F32BB925AA0CE16208F36BF5FE052F19
SHA-256:	76C4B7C04D21D13CA2B8344485033B11A3631C04F9F3F0EF55C466A443EBBEAD
SHA-512:	770031C2511B3A3E41CC0C0906927D5878B797A8FC5CDE7E33D725AC46934DA573F5D19C13C53C11BB1C626FED611ED2F87A377890863DD06F25ABDCA540B56
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\fedenpfm.xml

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	744
Entropy (8bit):	6.252068466825267
Encrypted:	false
SSDEEP:	12:pMzbyFRPpIHRufJX36MPoeyUTPg1vOlZvapSJYzD7xsgvj3IOeEwvnbkSkAQFQov:mzbyFHieJH6rtlmzapSJ47xX7DA/mJ9v
MD5:	5068F342795DD0ABC182D3E210DEA3DC
SHA1:	D19EF854A23175FB29C2E4477DD9FEBAACD7F113
SHA-256:	1938E80FD584E5F0AEA8FB71CEC826411B8E69F8541EAE8C820315462A9053B3
SHA-512:	BECF5BF96FBEF2F4809E62DF6DC7B3640ACBE2AE76CADA9E912BE9ABFE02F394C694D864318699B6AFF1CAE3A7B597A1929F7AB5C4D630127DEB7A0F7F070600
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\gfgrxolm.dat

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	698
Entropy (8bit):	6.258683715544326
Encrypted:	false
SSDEEP:	12:VD+CEZtzDSITZIvJD7zmPAa0U5O6sr2mXd6GhVYNTx9+LiKyjfftWBdd:ArfSclvJ3SPP5O6s8GhsT3+LyLtsd
MD5:	DBC9AC22BDEEB8CD96BBAECD453652C1
SHA1:	089BD73581553744ADBA703B7254B0238C8C3E30
SHA-256:	1F9293BE18FEB28F2FB505E0C14660FD0CE8930A5FB8644EB908F187643C9C07
SHA-512:	BFD581BDE6C31E4F67EC5A1302F4B80756979A468B2C13DF24B67041D31B8D4DB9006598DACEF5B299D0A6DC1E809EF6AE7A99176E313E756DF89C0013EEE574
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\gvcjf.ppt

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	624
Entropy (8bit):	6.242263123832009
Encrypted:	false
SSDEEP:	12:ZgDtdbmShRjjA6D1IDDjUzIDZMo1S5Rn21D5akY/B15v:eDtdiSvjbGUUDZH1S5BUlcjx
MD5:	C516FA4A75BF057057BE211416395C0F
SHA1:	04E8F9798E788912ED41BEC8BBB0DF98662D5271
SHA-256:	D897EE20C42EE8D2DC2E1950F12FB254C62931DBC840D971FF26E45967045771
SHA-512:	69D91E298BC4619AEBADDEBFACAFA49BE66C1182F28CC91D83E98702B4E3213458A0A83B9DA15AB5B521EAFEA3CE07983A0185BB7A3B867BDB310E4713D78594
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\gvguxlvv.xls

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	6.198216479466076
Encrypted:	false
SSDEEP:	12:15QbzLiR3mkusiHTHvYHC5qMXzyOWPz/wZdOyGhKPw/PcherOa:LQW3mQkAi5qOGyCEmchED
MD5:	DCC586BBC725E3FFB47CADEE31309C8E
SHA1:	D3630384B5A6D579453AB671607F8E51AE9C8CDA
SHA-256:	6B9C0567140D3565DD3B1D56C6B18E424DD6C1E0AE2F3DB521F234B9F108EE16
SHA-512:	05A5CA6133D7558B3F95278C01084540CEDE28BE9B34DB1AF0D4DA14EC8615EBA57D4A46CA272D94A95052CC471077421D6B3ED01DC879FA6E2FB34726DE92A2
Malicious:	false
Reputation:	unknown
Preview:	.....T.....

C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	936754
Entropy (8bit):	6.601305917045285
Encrypted:	false
SSDEEP:	24576:cYgAon+KfqNbXD2XJ2PH1ddATgs/u2karPK:c37+KSbq5e1diEnHam
MD5:	8A57722EC9067FAAA9FF2980C5F02838
SHA1:	F528308591C99004567DD76123E6D241ECDB5817
SHA-256:	3097D4413844FA305E10FB19DA3086848F2F3715B5B877E2F8691997BC25CD25
SHA-512:	27DFCA42250C1A0959023E9EB586CFE69BDA8166E5DE7C775370C30620D0E5E3515EBB85CC75AD57E7DBD65AE1612DD29CFD520B12BE64CD5C6EAE677A06A5AC
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 46%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..h..h..hX;1h..hX;3hq..hX;2h..hr..h..h...i...h...i...h...i...h..Ch..h..Sh..h..h..hI..i...hI..i..hI.?h..h.Wh..hI..i..hRich..h.....PE..L...).(c.....".....~.....@.....p.....P....@...@.....@.....|....P.....X&.....Pv.....C.....@.....text...|..... ..`.rdata.....@..@.data...lp.....H.....@....rsrc.....P.....@..@.reloc..Pv.....x.....@..B.....

C:\Users\user\AppData\Local\Temp\Folder8_410\kulqol.dat

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	537

Entropy (8bit):	6.2210381148806615
Encrypted:	false
SSDEEP:	12:cMSRrTZ3kkt6JJy9Lidiius2n4Hoboa5hPb1K9rL3XMd+Y1:cMSRrV3T/xiT64uoOjgtL3XM84
MD5:	DECFF247A10D1AB7F53AA5D798ECA2F7
SHA1:	E5DB2B53CB14488EC5EDD81D7CDE5FA53A11E837
SHA-256:	AC3428221792D658F6690BAB568201DB966D220EBB29E3426877941810DA4A96
SHA-512:	34272C48FFDA25F4C05CF0DF5FFA56D7B99EF09E4A2C2468739BA03C93D4EF171A1CE56E33C0E3CAD791E67E5079F6B5BCAD5E683B74FD615E60CF34CC02BCD
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\laaa.ini

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	506
Entropy (8bit):	6.2100184686076965
Encrypted:	false
SSDEEP:	12:04/uIl8/4p0YqXRhMeXVfbpc6HumsDS1cAuzj:5GD8/4p0YARaexp7umoSI
MD5:	0F4EF68A2745715CF4B89D383968D0EB
SHA1:	50D039BF131F5F11EC21E7EEBF7E22B81937C0A5
SHA-256:	173AA7C8B7671410C3F73767A1DFE2711403B3F045DBF9825BDB115BF13B2D8F
SHA-512:	2DC45A2B0BA4E58486B6BF128D7C91B00B732A1A2BBBB4CC90369E70DF7A654350FC2854E99B0DEA9B53ADDF2EE68BB97AB4F278247A4F3C486F43710950A226
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\ldgreqiiqi.msc

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	6.220072157041624
Encrypted:	false
SSDEEP:	12:lB7l5Fye8aehibvAui24ti7a/7skAywESg:lxcFb8obh3skA/Et
MD5:	DDAA651BD0ED9660CE485161F3DA0A31
SHA1:	F209147B7A434D9FF63997C57634694DD51E70C5
SHA-256:	6688EA36289339B7E8ABC74401F8338F14C7B824BEA4C56ACDEAE1082228B693
SHA-512:	966681795DF387F155F8D27D61AA4917E30F4A49E28B375700FBBBCA2F02AB45E5970891327795A0892B7466B412CEC537177D125251D983AA53A460176BBE05
Malicious:	false
Reputation:	unknown
Preview:	.....W.....

C:\Users\user\AppData\Local\Temp\Folder8_410\lhtfibp.docx

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	515
Entropy (8bit):	6.204575666587385
Encrypted:	false
SSDEEP:	12:4r0qRbHsWBKiUtlBQ9+6t5pAaFJukpJ5Hx+pWpZe30ANx:4rRHsWUilobppz3pR+pWve30A3
MD5:	C43B0D8E855F60BC8988C239AE91430E
SHA1:	38A9CC908239A6174A8C6CDD07DF2E65ED03C557
SHA-256:	F63FD422159E07439272BB6B603C3EB696C785AED53DBB0C693F9A9343869B89
SHA-512:	A7889E83FDA300933D47A34FA927EC0059BDFB518707DF227C157A82320A6E28189B8F88803DF45CE1C0FE6080E89FE034D84F8F1F7E0D044C4FCDE181AB59DE
Malicious:	false

Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\lulajc.bmp

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	6.212535146320597
Encrypted:	false
SSDEEP:	12:uuIc8nn8GGMe+xg0IKcrRR6Th9dZ73G/jaPCOtQwPGtMRZAV1uav:uuIc8V0+xgFvzm9dF3G/GVpY1t
MD5:	165255E5120FD4986C2B288F9FCAB09F
SHA1:	8CB0C248BB9A4BA714EA6739C74C1DE960BC7343
SHA-256:	CD7EC8254B748B3FE738147E27DF2FD3F7643D02835A46B15E93ECD060D06581
SHA-512:	AF748CC3EE4BA6747ABA50BE8AE6D568B7E913BBB33678C2E1116B4AA9AB14F7AB5860922223E62B3E6D9D3F72D81AE773D73EF3FE0CC0BA4069261E45280C26
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\lvgkma.msc

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	36396
Entropy (8bit):	5.572411470115854
Encrypted:	false
SSDEEP:	768:JF/d5vD40//MnSKd5+GcpEl51vx6q91kB6S9nxIBAIU9Fd9jVvAyAg3thc:HPLQdYpEIIqHkB6SsBDylaLg9hc
MD5:	3016649ED3E9A031DA118886A15144F7
SHA1:	58913D264B171A708F3AB825B14C096E47112677
SHA-256:	429880966442E56D685B62933A30BB780092C5B664C7E546AEA2B3CAB49945CE
SHA-512:	6C8EFD796609CDE371A5FA01B579742CF877CC1C604B933C09F52FB01D501C16E84AB1ADAD121B43C65D1EB88FBA6F1528E832D51E8AF7360EC120EDB9E0D5EB
Malicious:	false
Reputation:	unknown
Preview:	vSI328SN6k..b22U8437q8J47L5U907l3x7B5Y173A7N8Puz85zIL8T36k234Fzf99ob92l45b..95547jX65212mG58m4f6199235nR31CZ7621256s00beA28JC7Pv3h3ea..cRPTaZwN1KFY3P076jKj31A6JKuoeIkLZ6N1i8r..b7306180tbqJ63og7n5Uh1467IY717g5XgFrh05679A..09f912e5Y36u6t52g3439jKgW5b8k42E4j7g7Cbl741..D1f8596n4941f27UB1t32l2cM263vurrb82Z2h3100j5f13a4t..rntp69qYNq3H6521nc714p98TX9mMvSg0674q43O2u0IA..5B3H154vL47q8nePs766m2e42cZ15Xmr40L7HaUE..v524j8Gx185Z181p4v24..236U8cOS4HGZh7B40XN5924T6k2zT1564p4v89k0F6Lk9kJ034S8q114091yksqW02r27A..K6Sp61sV712736fTwF9H65U6u6V0357jX9610p2mQp553HE0K5S4Qgs86894DeX9n9Ec11y1ka9950F860HQbu7S6b..7OE857clz14431ERN8MeP4k9g8Q29j251BY9b0175jy06Kr3Sy95Vv8328VD..ZsK306xkJ23BQiMc9cU90zZ80q536T281mA7402q6EU6j1w9S6w13LF51tlYduPt5Zo7aL461..2238gW13r2y9i5C1kn9VtiHb8ZUX7066HHV417u9L491Z..6h0E54hz8njAB25hKg9438hZ30p46453jZTD9y8g6Q1Fu5P4r6y0bz80QE..11ms0765691T2104Dl7vO4r2v8063n4DDS582d1K6ru303X4517..518aV5l5v525y6dwf875F8Il8cxO9097658fhw3103cv26w548HMM57yTYfv5T1L83V69Wj75LO081s7MBlQQM..o6i966447vH00X60wi7fu0

C:\Users\user\AppData\Local\Temp\Folder8_410\mlvmtln.bin

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	739
Entropy (8bit):	6.2201318566424275
Encrypted:	false
SSDEEP:	12:jg/w0bWJnCzp5tnSA/hVmT6beGfLZKUTyD+wh5z6Wcg7ycQuzV7TWu2xD:juwbnap5siiT6vZD6jz6WMcQAi
MD5:	5B2FFEFEDF016705B02E548D343BD273
SHA1:	71C0005C0BB5259D7A8DF04607DB55E1DC48CFDF
SHA-256:	AE355FD9415586E5D427089E8E8E279A6F1BAAAC4CE24A9FA2039F0B9598BAD8
SHA-512:	BF6146C8C199501B43B2ADBED4A87E812B2E1A00C7E6D24FC2DFA81B47C5B1A85A3E7B189209EE571B33F57DDAA52159C77D91B621AB25EF87DC6E4F2670DB50
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\mujswngck.docx	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	625
Entropy (8bit):	6.227007206665302
Encrypted:	false
SSDEEP:	12:/bBc8DsAO60OpRKP5WQBpnOjhF0BCynUZEz6i5eQbGcb5x6MniiIAa:D9zpRMbEjhOBT0EjeQtX6Miea
MD5:	EA84F04FF07EFE4DD573DF81C8D73112
SHA1:	56C7C452FDF7EC05DF7EEED80019520B4636636E
SHA-256:	51948EA1E1786F3639B5688CF099946AFEEC48A6DB2B4151E2340CDA19113607
SHA-512:	58EC762815FBB2D3A15FA06610B19017BC7B30D8868E968B93F5478908BEBA2B72551D784A8630835E7F9D50C047FA64452F4B212F4B6430D554A710FC8B9C22
Malicious:	false
Reputation:	unknown
Preview:	.....i.....M.....

C:\Users\user\AppData\Local\Temp\Folder8_410\nbmc.pdf	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	6.2469950217286945
Encrypted:	false
SSDEEP:	12:MREuUZDYGXGpGzsyc8eo4jCEicYevV344JQ8LbHpQFPKs:E5G2Jyc8UCNsI4JQuJQFCs
MD5:	2E80CBC3177C60A2048EFD086D26DB0C
SHA1:	60011CEE58CDCE00026D09516C147445A399265C
SHA-256:	ADB88228E475C736251FD3A11BC7FB41F536FC8F0B80EA7C977153C054AB48FB
SHA-512:	A8DD351B67BEC96AA68512833DD76FF7B02757ACFF82758C93CA4F3D22F98436399FAB1D9E50D9E25C66993A35DE7649207278C49E80B4D0F3683AA3914F32E
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\quxisn.ini	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	6.191048141141158
Encrypted:	false
SSDEEP:	12:7OguD7Nc+8a2rZvnUqyLbSWfhCSl7EF07V4OEnz9T6eJpsjchWZPODQm9y:7Zui+8a2rVVyLbRISl95DEnz9+en9gqy
MD5:	BD2C67C8D59FE4FA46C2BD40B65F2014
SHA1:	303E8754D55A90565DC43581367644F3CF7F3A7A
SHA-256:	3AC63CC62CAEB2B9CA24141616FA10AEF0C64EA6721AB16B8B3E33878B09098D
SHA-512:	40A0D3D8C56F68908B273B532825E9F79BE73DFBBC02CBF0CDC72E4572CADF7837D36F5C75CB1BFDF2D87B39FC0EDE366D45AEEB0B37A80FD8A0968F2425917
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\rbtj.dat	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	620
Entropy (8bit):	6.216440012089495
Encrypted:	false
SSDEEP:	12:KmsJX62KCMdStvQy6ws9M7odswOngZll7tSghIbCFDbfCEvM4cW1PYDAePA4o:K1562KKIXws9ywOBlsghbf9M4cwZ
MD5:	B4D931185A25EC221C09C2E0C7DE0409

SHA1:	3580DF306627E9BE85243FDDE91165A24279273A
SHA-256:	508D3E6C83EF0A34BEBB22F6EE99B11A7214CED3E0748D1D4C751ACA8CCA7C71
SHA-512:	48E022E2ABCF790F95E1198523262EBBAE541C428A090E0D715F502CDBEDFD880B1EAC69AB5528A9055D845D9B722F30D08F0D0FEC2F1616F28403BDFDB623F
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	109765414
Entropy (8bit):	7.149822507862373
Encrypted:	false
SSDEEP:	786432:jeiFTzFm2V+Ws11rx9irns45XQ0bWPu1EOi6h7ReyeLCD5oAD4Fk/YhswDvybX7+:E
MD5:	1A4F87FE68FAF07769D93372246F7315
SHA1:	756DBF9A1C5C60FA13B3285DF696C370C117A9AD
SHA-256:	AE5869183348BB70CDF4745B2629425B3DC5B9A96A9DCDE7862AC9F0BC97E346
SHA-512:	6C67055DB74FEEEFB9C03B2EA25DEB0680ACE4A9421AC0C458EA7AE4EC17CE24D093F47F7C43AA6553071994AADDCCA0BFF348B751AE7EBCCA6400009C097B2F
Malicious:	false
Reputation:	unknown
Preview:	..;....+L.,.I...4m.U7~.'...ka6k.,H'.I..(cr..?.e...A.{\.D.~.(S{..V.-..&X{...Cq.P..(Jj.saac.....#.c.s....,7..3..U..?..6.4>\...av.8...&...R.D.....L.u.-ej.%.B....E..6.R..39.Ei..`.....@.T...nB. ...w.D.....(Z..HZln....7.....o=...qi.."....w.tw..m....p.Q.C.8.3.1.....Q.k.9.2.0.e.h.4.Y.o.6.n.G.2.x.Z.G.U.t.j.T.2.2.d.X.2.7.....4.3.U.4.7.7.....P.. ...|.b....xrMl.g...$....1..]]f..}..^C.I.. sir`)Kcwj..H.....V.DH.&.1n.N....C)..9.d....z:t...ed.....":.....H..s.zTc!A..p.[...;..D.A..A:.....c.C.E.7.7.1.5.s.P.J.6.F.1.7.4.4.M.W.O.c.3.1.0.y.6.1.0.8.0.6.0.e.1.1.e.D.0.z.3.Z .....B...u...#`...$.k.....|...n....}:.....?.c..!..c..m...lm ...u.....w...g.{C.2*.....s....o..{.....".(.RLD..G$.....xi*.h..@a.#.c...y...Hr.,.s..J(.....$..{...O.H.7VQ...p,....sA..X.....<d.)ql.1E..{..... .....Y.9.l.....t.=.P.....2.B.5.3.1.e.X.7.z.4.4.l.z.P.z.7.....0^i.....7..~..@..V..W.n...%....H...?..Z.i..[.(d3.....7.3.5.5.0.5.8.8.4.9.w.9.2.U.8.8.7.6.D.p.r.1.0.0.3.w.D.a.4.I.P.3.

C:\Users\user\AppData\Local\Temp\Folder8_410\tpfplabhr.ppt

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	515
Entropy (8bit):	6.204797250067207
Encrypted:	false
SSDEEP:	12:kXIjadX52agNuuF0Qc4fR1a7EUOAH4MKITBawUQTHI:ktX5xgNuNxURobwMKIIZF
MD5:	62058854A3A0211391D23AFE642D51C5
SHA1:	4333B74DCE3F8564D4156F2D11B66069EE3372F2
SHA-256:	D8E824CBC1D0F179F3733A2B5508200335A6EC646226F0B023E9FB4F94EA6CDE
SHA-512:	FC32610AFF79A33A8BF60624F36AFB4F705C22CFF0FD04C764DA1785EBCE3C69B2DEC865D43D73EC8A9A8F1296836AF73D94681CA1E589EB6423D453D921ABD2
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\vgbluarp.xl

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	550
Entropy (8bit):	6.251960168682925
Encrypted:	false
SSDEEP:	12:/yLLQ8dGYT/PD4jifw5AFTdBvnOh8LEUvXbkM/:KLLPdp/PDeUw5ArBvOh+7kc
MD5:	9F994AFD9BB142AB8A36D4C58F102F93
SHA1:	8DCB457E7F5EC4BB6B7E32305DD26A4F8D2A681E
SHA-256:	BD5CD1567D60D85D393A1DDCA22A737C89C1B3A3E5A7F8A772BFDE48B8CEA3B6
SHA-512:	BFA1BF3B846EFFFA96A48E91AE6A73E014F74D3459870979EB1117723D88928F8A183723AE5A5A2DA80301F3AFC6B50870E447252D1944664887C375E735ED13
Malicious:	false
Reputation:	unknown
Preview:	.....K.....[.....

C:\Users\user\AppData\Local\Temp\Folder8_410\vgpgtuex.bmp	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	568
Entropy (8bit):	6.181793571320447
Encrypted:	false
SSDEEP:	12:4SJXAaJc93zJwGBv1ofBoOzwyc6it/ShtmACzggy+DjyJ:JQaJm39wi8DzRddMAC7PyJ
MD5:	7D0D7010210F47BBC571277006C8C174
SHA1:	73ED48688E61A32FC3A92E1099C411825FF5E59A
SHA-256:	814C2970E6246BF86415067D9780E8E2F1DD9EAF947C6BC425A815E749A08042
SHA-512:	CC91B14EC49EB15FD9F140C30D5321A42417C1F4C6C81222746A7A616AF83B9FEE4FCF4F8CAEE203688A08C6D1C6D3B74E4D9F6AEB4B1B50F3813F57387A04 4
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\vjdtaskm.txt	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	659
Entropy (8bit):	6.246268360923076
Encrypted:	false
SSDEEP:	12:RUGtgFsr3B1AMOed5A3CEm5s6K6l5/FuMOkJ7vzu5hgrr/YoBVw1G+uD:CGtVr3B83C7s6NPuPVhg3zw1Gf
MD5:	166AD43D9C2CA35E2F55412A6ED8B515
SHA1:	5A5E8831BABF7E9FC4233417AA04046D45FFFC57
SHA-256:	4CB41D553941E698BD92DD077AE3CCE0E4ECA9DCCA9EAF2C3EA76C48C3A9A26E
SHA-512:	135E04042383237D766F1FB3CEC42C9E9400C71C34A8F0D7B46CBBD594189DD186507DA05E5DB8E71121FA57E7A74E6B38FACB424038CC65D993BE1EAF8D91 B
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\Folder8_410\vtmv.xls	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	603
Entropy (8bit):	6.243174528289961
Encrypted:	false
SSDEEP:	12:brw87rpvWqPZNtLlQN1MxCRQqw5ShuQYL2ptJ7BTmhFKAPN6bjEr2JM02Wb6rRn:brw87VeuzfQN1sCRQqCOUMtXUk1jhxGt
MD5:	02C0FBC15743BE076F645E223C92ACCB
SHA1:	76DB0F874C4462B5DED61D9104FCEC0E3C95D273
SHA-256:	C74821B50B9A993F24F4BB8788FF69A77A96C4A19DE69711564C26103D6D3F68
SHA-512:	E6CE845F43A37429DA29690951780958EFD7F95CA1AAE1D2D9F8146B93419C8DDFF0750A8F29127E3B89482890075964843C3D17C5FDC08704CD6E6079CE4DA
Malicious:	false
Reputation:	unknown
Preview:	.....T...'.....

C:\Users\user\AppData\Local\Temp\Folder8_410\xnhbpesj.pdf	
Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	555
Entropy (8bit):	6.222922480311702
Encrypted:	false

SSDEEP:	12:BRudpgMXWpbVanAogLyE9387xsqwp7kxG8f5bUxjl:BkDWpbVanAo9EB8V/wpgA8f5bUJl
MD5:	CE86D4806786B5285DC23D378067A353
SHA1:	0D61DE00AC334DCBDA6B3E320E880DFADB2482C3
SHA-256:	24FD150DC97AC04C8D9AA8F482A994788D5B77578B16B6028B9980249FC724A8
SHA-512:	6ADE617608EB8453DEB3E43FBA45A1F3B39D6D7C78809CE9504676ECAD7CDE8F1B59BFC79C561E9687AE13FF5F359EBFE3C4DD198207298BEA25E530D412DEC3
Malicious:	false
Reputation:	unknown
Preview:	.....F.....>.....

C:\Users\user\AppData\Local\Temp\Folder8_410\xopcgkw.xl

Process:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
File Type:	Unicode text, UTF-8 text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	6.20969596633477
Encrypted:	false
SSDEEP:	12:ZRlLCc8+8GvDRpsxyyNPPHO8VJG1tK3vtueUUtCn2l1sa0Jxun:Z6cftWyypPuB8wiCtF0Jxun
MD5:	55F53F4F242C0DB1E519E3E72DEED805
SHA1:	E9B4CC8F1401B641B5ACA044BF0379C1C2D653F4
SHA-256:	8E858683D645E559E93B7F3C2AD65E847A2EAAADF434190AC8278DDE580BA874
SHA-512:	A4EEF16E2C05DAA7100DCBA1C6044D3333BB947DC79EE66817EF5394E8355686A2A51A0C0F2BE1DE917EDC7E9AD663F34E49380709F356499C95683651951A7
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Temp\RegSvcs.exe

Process:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
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+SdIBf0k2dsYyV6lq87PiU9FViaLmf:EoOlBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D6B42
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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\tmp897A.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):	1309
Entropy (8bit):	5.0990514427386
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK04kxtn:cbk4oL600QydbQxIYODOLedq35kj
MD5:	77AF6D1744407EBD7E0CEC16F3C7168D
SHA1:	FF4E58917D1AB719E40C68542F663121299DAE67
SHA-256:	A519EB5414D05AC7565B5399D9F1EF717D6846695221B21B51820AA69120EDDC
SHA-512:	529FD47B0605315DDD60D10A99A4830C234C5046C9EE575524C3FC85105C701DCD8EEA4F2A1D8AE444D2E42A2CEF37CE23FB9A2BAF4CB0BAA91B590FB555E91

Malicious:	**true**
Reputation:	unknown
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8D34.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):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4
Malicious:	false
Reputation:	unknown
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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

Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ZSp:Q
MD5:	6C844091DCB061AD2B62761D1939F235
SHA1:	813C89B6606B3A5510FD924A02BAFCC6FE2B8574
SHA-256:	FBC2997715CCA9BD5F3F08FB0FABD33DD3D13489C40E47952208ED854127AA2C
SHA-512:	62CE0F17F06E366D2CBE8C1C73569D39D50BA3EB2403C8AAD48314B213166A3DC5538375992D3FD99827565B720B029244379A854EAA189EE3B0E0F33D50D66
Malicious:	**true**
Reputation:	unknown
Preview:	Fb..7..H

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):	46
Entropy (8bit):	4.3523814564716385
Encrypted:	false
SSDEEP:	3:oNUkh4E2J5xAIwGMNn:oN923fA
MD5:	E01C7B4BFFC4D8966DFDD6831E4904F7
SHA1:	FE638E970FB82742E2C4D7EA3AE7E043589304FB
SHA-256:	ECFA3D73848685C232F4B352A5E24F4995B7D55FF4130A26B7BAEB3839280300
SHA-512:	FD9C41391E076E66F9A65DF18CA790EF06518B8033A5D24BF631E6E7F5EACECF34AD2AA7197FEB8B8FC7ED571A3BEFA0C8C940631F6EE5C0F5996D703B6AC 50A
Malicious:	false

Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\lvgkma.msc	
Process:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	90
Entropy (8bit):	4.969700668999775
Encrypted:	false
SSDEEP:	3:YRRvutvEOVBJcRAoovKXRGdY2JRMow7:AvCEOVHcoXzpi
MD5:	B48D7F5C0CC7E6A4C737BE0D827B9867
SHA1:	906E2605871B8F319FA2A455C06F2E53940ED777
SHA-256:	B2BACD88BAFE8C668A45AB03A2D5647A9BDDA6CF1361FC821D5A70480B8CCB69
SHA-512:	9E3F4634AF71BCD600576BBD09EBC569E8D5D286ACD07D8E516AD61A80D3447156AEACB59194F24D9C39A1BBE666E038375A94E4AA5A7821D971FD166A7DD6 94
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%localappdata%\temp..Key=Chrome..Dir3ctory=Folder8_410..ExE_c=itugx.exe..

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141 5
Malicious:	false
Reputation:	unknown
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.826498922764083
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:	026910003102350.pdf.scr.exe
File size:	1064658
MD5:	c2a80ccf6362bba805072de9ce963ea5
SHA1:	c7a0ca8b35e2c08e69f48d754dbdbf20f2d1d53f
SHA256:	592217d2590ae9ca688346688b2d7d13a78190f9562889597ebb79060136034c
SHA512:	377fbc8008b63f9380ebe0a90db28a191fd3f0eea97dd10e6f16607eb42c51f713cbfb744f2ce73b74093f4866a05e3b00ec7f8b57e2bff2c6a9c8f2118ce707
SSDEEP:	24576:9TbBv5rUeTA/TYaxVKPijItG0bKL1xRMa2LSmnbrDrF:XBvIHBMG02L1N29rDx
TLSH:	95351202BEC196B2D0A3093256767721B97DB9601F68CEDFA3D1466CAD325C0E7317B2

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x_c.<>..<>..<>.....1>.....>.....$>...I..>>...I../>...I..+>...I...>..5F..7>..5F..;>..<>..)?...I...>...I..=>...I..=>...I..=>.

File Icon

Icon Hash:	938c8c90b2ea6ab2

Static PE Info

General

Entrypoint:	0x41f530
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, GUARD_CF, TERMINAL_SERVER_AWARE
Time Stamp:	0x6220BF8D [Thu Mar 3 13:15:57 2022 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:	12e12319f1029ec4f8fcbed7e82df162

Entrypoint Preview

Instruction
call 00007FF9B4BF9B7Bh
jmp 00007FF9B4BF948Dh
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007FF9B4BEC2D7h
mov dword ptr [esi], 004356D0h
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], 004356D8h
mov dword ptr [ecx], 004356D0h
ret
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 004356B8h
push eax
call 00007FF9B4BFC91Fh
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007FF9B4BF961Ch
push 0000000Ch
push esi
call 00007FF9B4BF8BD9h
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 00007FF9B4BEC252h
push 0043BEF0h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FF9B4BFC3D9h
int3
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007FF9B4BF9598h
push 0043C0F4h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007FF9B4BFC3BCh
int3
jmp 00007FF9B4BFDE57h
int3
int3
int3
int3
push 00422900h
push dword ptr fs:[00000000h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3d070	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3d0a4	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x4a8c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x69000	0x233c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3b11c	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	0x355f8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x278	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3c5ec	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	0x31bdc	0x31c00	False	0.5909380888819096	data	6.712962136932442	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xaec0	0xb000	False	0.4579190340909091	data	5.261605615899847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x24720	0x1000	False	0.451416015625	data	4.387459135575936	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didat	0x63000	0x190	0x200	False	0.4453125	data	3.3327310103022305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x64000	0x4a8c	0x4c00	False	0.6105571546052632	data	6.391160230365552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x69000	0x233c	0x2400	False	0.7749565972222222	data	6.623012966548067	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x64524	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x6506c	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x66618	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192		
RT_DIALOG	0x66740	0x286	data	English	United States
RT_DIALOG	0x669c8	0x13a	data	English	United States
RT_DIALOG	0x66b04	0xec	data	English	United States
RT_DIALOG	0x66bf0	0x12e	data	English	United States
RT_DIALOG	0x66d20	0x338	data	English	United States
RT_DIALOG	0x67058	0x252	data	English	United States
RT_STRING	0x672ac	0x1e2	data	English	United States
RT_STRING	0x67490	0x1cc	data	English	United States
RT_STRING	0x6765c	0x1b8	data	English	United States
RT_STRING	0x67814	0x146	data	English	United States
RT_STRING	0x6795c	0x46c	data	English	United States
RT_STRING	0x67dc8	0x166	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x67f30	0x152	data	English	United States
RT_STRING	0x68084	0x10a	data	English	United States
RT_STRING	0x68190	0xbc	data	English	United States
RT_STRING	0x6824c	0xd6	data	English	United States
RT_GROUP_ICON	0x68324	0x14	data		
RT_MANIFEST	0x68338	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, InterlockedDecrement, 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, DecodePointer, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineA, GetOEMCP, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, LocalFree, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage
OLEAUT32.dll	SysAllocString, SysFreeString, VariantClear
gdiplus.dll	GdipAlloc, GdipDisposeImage, GdipCloneImage, GdipCreateBitmapFromStream, GdipCreateBitmapFromStreamICM, GdipCreateHBITMAPFromBitmap, GdiplusStartup, GdiplusShutdown, GdipFree

Possible Origin

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

Network Behavior

Network Port Distribution

Total Packets: 16

- 53 (DNS)
- 60705 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:58.131228924 CET	49700	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:01.243844986 CET	49700	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:07.244303942 CET	49700	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:24.303241014 CET	49705	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:27.408564091 CET	49705	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:33.418741941 CET	49705	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:49.414972067 CET	49707	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:52.435837984 CET	49707	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:10:58.508714914 CET	49707	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:11:07.956806898 CET	49709	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:11:11.050592899 CET	49709	60705	192.168.2.5	212.193.30.230
Feb 2, 2023 08:11:17.053057909 CET	49709	60705	192.168.2.5	212.193.30.230

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:09:57.770723104 CET	60841	53	192.168.2.5	8.8.8.8
Feb 2, 2023 08:09:57.877348900 CET	53	60841	8.8.8.8	192.168.2.5
Feb 2, 2023 08:10:24.189878941 CET	49724	53	192.168.2.5	8.8.8.8
Feb 2, 2023 08:10:24.299720049 CET	53	49724	8.8.8.8	192.168.2.5
Feb 2, 2023 08:10:49.296843052 CET	65323	53	192.168.2.5	8.8.8.8
Feb 2, 2023 08:10:49.405663013 CET	53	65323	8.8.8.8	192.168.2.5
Feb 2, 2023 08:11:07.934437990 CET	63446	53	192.168.2.5	8.8.8.8
Feb 2, 2023 08:11:07.953950882 CET	53	63446	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 08:09:57.770723104 CET	192.168.2.5	8.8.8.8	0x830a	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:10:24.189878941 CET	192.168.2.5	8.8.8.8	0x17be	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:10:49.296843052 CET	192.168.2.5	8.8.8.8	0x8dd7	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:11:07.934437990 CET	192.168.2.5	8.8.8.8	0x1c9a	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false

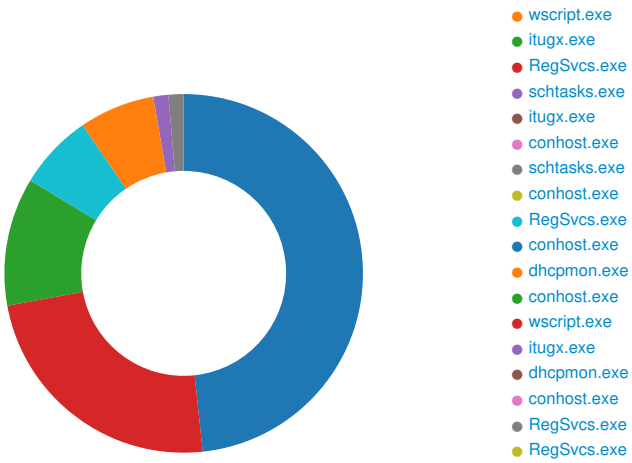
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 08:09:57.877348900 CET	8.8.8.8	192.168.2.5	0x830a	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:10:24.299720049 CET	8.8.8.8	192.168.2.5	0x17be	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:10:49.405663013 CET	8.8.8.8	192.168.2.5	0x8dd7	No error (0)	december2n.duckdns.org		212.193.30.230	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:11:07.953950882 CET	8.8.8.8	192.168.2.5	0x1c9a	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false

Statistics

Behavior

- 026910003102350.pdf.scr.exe



Click to jump to process

System Behavior

Analysis Process: 026910003102350.pdf.scr.exe PID: **4980**, Parent PID: **3324**

General

Target ID:	0
Start time:	08:09:32
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\026910003102350.pdf.scr.exe
Imagebase:	0xcc0000
File size:	1064658 bytes
MD5 hash:	C2A80CCF6362BBA805072DE9CE963EA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: wscript.exe PID: **2312**, Parent PID: **4980**

General

Target ID:	1
Start time:	08:09:46
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\wscript.exe" daitsfsh-waune.icm.vbe
Imagebase:	0x50000
File size:	147456 bytes

Copyright Joe Security LLC 2023

MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000001.00000003.359286205.00000000036B5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: itugx.exe PID: **5920**, Parent PID: **2312**

General

Target ID:	2
Start time:	08:09:54
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe" rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
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: 00000002.00000003.379717765.0000000000F09000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.379717765.0000000000F09000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.379717765.0000000000F09000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.379717765.0000000000F09000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.381511725.0000000000F08000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.381511725.0000000000F08000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.381511725.0000000000F08000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.381511725.0000000000F08000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.381281377.0000000003813000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.381281377.0000000003813000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.381281377.0000000003813000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.381281377.0000000003813000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.379880100.0000000000F71000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.379880100.0000000000F71000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.379880100.0000000000F71000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.379880100.0000000000F71000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.379756044.0000000000F3D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.379756044.0000000000F3D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.379756044.0000000000F3D000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.379756044.0000000000F3D000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.380269423.0000000000F40000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.380269423.0000000000F40000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.380269423.0000000000F40000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.380269423.0000000000F40000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.380361986.0000000000F5C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.380361986.0000000000F5C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.380361986.0000000000F5C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.380361986.0000000000F5C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.380642798.0000000000ED4000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.380642798.0000000000ED4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.380642798.0000000000ED4000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.380642798.0000000000ED4000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 46%, ReversingLabs
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	37DADF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Folder8_410\Update.vbs	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	3559A8	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	37DA78	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Folder8_410\Update.vbs	0	143	43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 2e 52 75 6e 20 22 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 46 4f 4c 44 45 52 7e 31 5c 69 74 75 67 78 2e 65 78 65 20 43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 46 4f 4c 44 45 52 7e 31 5c 72 6e 6e 73 68 2e 78 6c 73 22	CreateObject("Wscript.Shell").Run "C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls"	success or wait	1	37D4EC	WriteFile
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 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 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	37DA78	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	65536	success or wait	1677	3493D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	36864	end of file	2	3493D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	65536	success or wait	1677	3493D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	36864	end of file	2	3493D3	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	65536	success or wait	1	31B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	65536	success or wait	1630	31B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\rnnsh.xls	unknown	65536	end of file	1	31B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\Update.vbs	unknown	65536	end of file	1	31B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\chcekckp.gfh	unknown	65536	success or wait	2	31B0B2	ReadFile
C:\Users\user\AppData\Local\Temp\Folder8_410\chcekckp.gfh	unknown	65536	success or wait	14	31B0B2	ReadFile

Registry Activities

Key Value Created

Copyright Joe Security LLC 2023

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	Chrome	unicode	C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls	success or wait	1	39D017	RegSetValueExW
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	AutoUpdate	unicode	C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs	success or wait	1	39D017	RegSetValueExW

Analysis Process: RegSvcs.exe PID: **5960**, Parent PID: **5920**

General

Target ID:	3
Start time:	08:10:05
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xe80000
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: 00000003.00000002.585880095.00000000060B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.585880095.00000000060B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.585880095.00000000060B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.585880095.00000000060B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.585880095.00000000060B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.580107208.0000000003781000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.580107208.0000000003781000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.585759853.0000000006040000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.585759853.0000000006040000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.585759853.0000000006040000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.585759853.0000000006040000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.585651630.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.585651630.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.585651630.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.585651630.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Antivirus matches:	• 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	7222CF06	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	7222CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	7107BEFF	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	71071E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7107BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	7107DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp897A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	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	71071E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8D34.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71077038	GetTempFileNameW
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	7107BEFF	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	7107BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp897A.tmp	success or wait	1	71076A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8D34.tmp	success or wait	1	71076A95	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	0	8	46 62 fd fd 37 05 fd 48	Fb7H	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 7a 58 fd 5a 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 fd 00 00 00 20 00 00 00 fd 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 fd 00 00 00 02 00 00 fd 22 01 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELzXZ0dV @ "`	success or wait	1	7107DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp897A.tmp	0	1309	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	71071B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	46	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 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	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8D34.tmp	0	1310	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	71071B4F	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	721603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71071B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	721ED72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	721ED72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	4096	success or wait	1	721ED72F	unknown
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	unknown	512	success or wait	1	721ED72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	7107646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **4544**, Parent PID: **5960**

General	
Target ID:	4
Start time:	08:10:12
Start date:	02/02/2023
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\tmp897A.tmp
Imagebase:	0x2c0000
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\tmp897A.tmp	unknown	2	success or wait	1	2CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp897A.tmp	unknown	1310	success or wait	1	2CABD9	ReadFile

Analysis Process: itugx.exe PID: **3300**, Parent PID: **3324**

General	
Target ID:	5
Start time:	08:10:12
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2023

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.445033484.0000000003E2F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.445033484.0000000003E2F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.445033484.0000000003E2F000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.445033484.0000000003E2F000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.444608093.0000000001593000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.444608093.0000000001593000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.444608093.0000000001593000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.444608093.0000000001593000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.445168798.00000000015C6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.445168798.00000000015C6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.445168798.00000000015C6000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.445168798.00000000015C6000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_LNK_SuspiciousCommands, Description: Detects LNK file with suspicious content, Source: 00000005.00000003.451151702.00000000014BE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.442020848.00000000015C7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.442020848.00000000015C7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.442020848.00000000015C7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.442020848.00000000015C7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.443014017.00000000015FF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.443014017.00000000015FF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.443014017.00000000015FF000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.443014017.00000000015FF000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.442280554.00000000015FC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.442280554.00000000015FC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.442280554.00000000015FC000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.442280554.00000000015FC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.443097060.000000000161A000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.443097060.000000000161A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.443097060.000000000161A000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.443097060.000000000161A000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000003.442615320.000000000162F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000003.442615320.000000000162F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.442615320.000000000162F000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000003.442615320.000000000162F000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

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

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5648**, Parent PID: **4544**

General	
Target ID:	6
Start time:	08:10:13
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: schtasks.exe PID: **2216**, Parent PID: **5960**

General	
Target ID:	7
Start time:	08:10:13
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp8D34.tmp
Imagebase:	0x2c0000
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\tmp8D34.tmp	unknown	2	success or wait	1	2CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8D34.tmp	unknown	1311	success or wait	1	2CABD9	ReadFile

Analysis Process: conhost.exe PID: **1648**, Parent PID: **2216**

General	
Target ID:	8
Start time:	08:10:13
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: 5072, Parent PID: 1084

General

Target ID:	9
Start time:	08:10:14
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xc60000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71071B4F	WriteFile
\Device\ConDrv	141	141	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 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	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	71071B4F	WriteFile
\Device\ConDrv	186	45	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	71071B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71071B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	0	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",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile

Copyright Joe Security LLC 2023

Analysis Process: conhost.exe PID: **4124**, Parent PID: **5072**

General

Target ID:	10
Start time:	08:10:15
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **2960**, Parent PID: **1084**

General

Target ID:	11
Start time:	08:10:15
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x400000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, ReversingLabs

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\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7253C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71071B4F	WriteFile
\Device\ConDrv	141	141	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 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	The following installation error occurred:1: Assembly not found: '0'.	success or wait	1	71071B4F	WriteFile
\Device\ConDrv	186	45	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	71071B4F	WriteFile
\Device\ConDrv	215	29	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	71071B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	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",01,"WinRT","NotApp",12,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0	success or wait	1	7253C907	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	72205705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72205705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	721603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7220CA54	ReadFile

Analysis Process: conhost.exe PID: **5092**, Parent PID: **2960**

General

Target ID:	12
Start time:	08:10:15
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **2896**, Parent PID: **3324**

General

Target ID:	13
Start time:	08:10:21
Start date:	02/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff60c2e0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: itugx.exe PID: **4036**, Parent PID: **2896**

General

Target ID:	16
Start time:	08:10:24
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2023

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.455419127.0000000001530000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.455956530.000000000151D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.455956530.000000000151D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.455956530.000000000151D000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.455956530.000000000151D000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.456804036.00000000014C7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.456804036.00000000014C7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.456804036.00000000014C7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.456804036.00000000014C7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.455090351.00000000014FD000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.455090351.00000000014FD000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.455090351.00000000014FD000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.455090351.00000000014FD000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.454885906.00000000014C8000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.454885906.00000000014C8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.454885906.00000000014C8000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.454885906.00000000014C8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.456419289.0000000003AA0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.456419289.0000000003AA0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.456419289.0000000003AA0000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.456419289.0000000003AA0000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.456270575.0000000001494000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.456270575.0000000001494000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.456270575.0000000001494000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.456270575.0000000001494000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000003.455869267.0000000001501000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000003.455869267.0000000001501000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000003.455869267.0000000001501000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000003.455869267.0000000001501000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **576**, Parent PID: **3324**

General

Target ID:	17
Start time:	08:10:33
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x840000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **1880**, Parent PID: **576**

General	
Target ID:	18
Start time:	08:10:33
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **4736**, Parent PID: **3300**

General	
Target ID:	19
Start time:	08:10:34
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x910000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.468974735.0000000004169000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.468974735.0000000004169000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.468974735.0000000004169000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.462925300.0000000000D02000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.462925300.0000000000D02000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.462925300.0000000000D02000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.462925300.0000000000D02000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.467749940.0000000003161000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.467749940.0000000003161000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.467749940.0000000003161000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **3624**, Parent PID: **4036**

General	
Target ID:	20
Start time:	08:10:40
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x9c0000

File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: itugx.exe PID: **5928**, Parent PID: **3324**

General

Target ID:	21
Start time:	08:10:41
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.499747206.0000000001382000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.499747206.0000000001382000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.499747206.0000000001382000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.499747206.0000000001382000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.498827487.00000000013EB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.498827487.00000000013EB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.498827487.00000000013EB000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.498827487.00000000013EB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.499159077.00000000013EE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.499159077.00000000013EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.499159077.00000000013EE000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.499159077.00000000013EE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.500004480.0000000003C6C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.500004480.0000000003C6C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.500004480.0000000003C6C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.500004480.0000000003C6C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000003.500237895.00000000013B5000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000003.500237895.00000000013B5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000003.500237895.00000000013B5000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000003.500237895.00000000013B5000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: wscript.exe PID: **4776**, Parent PID: **3324**

General

Target ID:	22
Start time:	08:10:50
Start date:	02/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false

Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff60c2e0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: itugx.exe PID: **5420**, Parent PID: **4776**

General

Target ID:	23
Start time:	08:10:55
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.519976244.0000000000D86000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.519976244.0000000000D86000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.519976244.0000000000D86000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.519976244.0000000000D86000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.522419154.0000000000DBF000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.522419154.0000000000DBF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.522419154.0000000000DBF000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.522419154.0000000000DBF000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.522729745.0000000000D52000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.522729745.0000000000D52000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.522729745.0000000000D52000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.522729745.0000000000D52000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.520896058.0000000000DBB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.520896058.0000000000DBB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.520896058.0000000000DBB000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.520896058.0000000000DBB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.521795477.0000000000DEE000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.521795477.0000000000DEE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.521795477.0000000000DEE000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.521795477.0000000000DEE000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.523166921.0000000003588000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.523166921.0000000003588000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.523166921.0000000003588000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.523166921.0000000003588000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.523729347.0000000000D85000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.523729347.0000000000D85000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.523729347.0000000000D85000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.523729347.0000000000D85000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000017.00000003.522501129.0000000000DDB000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000003.522501129.0000000000DDB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000003.522501129.0000000000DDB000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000017.00000003.522501129.0000000000DDB000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **5508**, Parent PID: **5928**

General

Target ID:	24
Start time:	08:11:00
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x6f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	.Net C# or VB.NET

Analysis Process: itugx.exe PID: **5552**, Parent PID: **3324**

General

Target ID:	25
Start time:	08:11:04
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000003.544675872.0000000004778000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000003.544675872.0000000004778000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000003.544675872.0000000004778000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000019.00000003.544675872.0000000004778000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000003.543882986.00000000019ED000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000003.543882986.00000000019ED000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000003.543882986.00000000019ED000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000019.00000003.543882986.00000000019ED000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000003.544569868.0000000001984000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000003.544569868.0000000001984000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000003.544569868.0000000001984000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000019.00000003.544569868.0000000001984000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000003.544269018.00000000019F0000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000003.544269018.00000000019F0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000003.544269018.00000000019F0000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000019.00000003.544269018.00000000019F0000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000003.544903428.00000000019B7000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000003.544903428.00000000019B7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000003.544903428.00000000019B7000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000019.00000003.544903428.00000000019B7000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **5736**, Parent PID: **5420**

General

Target ID:	26
Start time:	08:11:11
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x6c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: wscript.exe PID: **5776**, Parent PID: **3324**

General	
Target ID:	27
Start time:	08:11:13
Start date:	02/02/2023
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Local\Temp\FOLDER~1\Update.vbs"
Imagebase:	0x7ff60c2e0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: itugx.exe PID: **1712**, Parent PID: **5776**

General	
Target ID:	28
Start time:	08:11:16
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\Folder8_410\itugx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\FOLDER~1\itugx.exe" C:\Users\user\AppData\Local\Temp\FOLDER~1\rnnsh.xls
Imagebase:	0x310000
File size:	936754 bytes
MD5 hash:	8A57722EC9067FAAA9FF2980C5F02838
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2023

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000003.573295191.0000000001405000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000003.573295191.0000000001405000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000003.573295191.0000000001405000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000003.573295191.0000000001405000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000003.572597608.000000000143D000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000003.572597608.000000000143D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000003.572597608.000000000143D000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000003.572597608.000000000143D000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000003.572853168.00000000013D2000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000003.572853168.00000000013D2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000003.572853168.00000000013D2000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000003.572853168.00000000013D2000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000003.572980994.0000000003F04000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000003.572980994.0000000003F04000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000003.572980994.0000000003F04000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000003.572980994.0000000003F04000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_1, Description: Yara detected AntiVM autoit script, Source: 0000001C.00000002.577313681.00000000012C7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000003.572167005.000000000143B000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000003.572167005.000000000143B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000003.572167005.000000000143B000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000001C.00000003.572167005.000000000143B000.00000004.00000020.00020000.00000000.sdmp, Author: unknown

Analysis Process: RegSvcs.exe PID: **3928**, Parent PID: **5552**

General

Target ID:	30
Start time:	08:11:21
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x950000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: RegSvcs.exe PID: **4764**, Parent PID: **1712**

General

Target ID:	31
Start time:	08:11:35
Start date:	02/02/2023
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xe70000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly

Copyright Joe Security LLC 2023