ID: 452311
Sample Name:
mzyDSLb1u9.exe
Cookbook: default.jbs
Time: 05:16:07
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report mzyDSLb1u9.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
System Summary: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
Operating System Destruction: 7
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Entrypoint Preview 25
Rich Headers 25
Data Directories 25
Sections 25
Resources 25
Imports 25
Possible Origin 25
Network Behavior 25
Network Port Distribution 25
TCP Packets 25

UDP Packets 25
DNS Queries 25
DNS Answers 26
Code Manipulations 26
Statistics 26
Behavior 26
System Behavior 26
Analysis Process: mzyDSLb1u9.exe PID: 6848 Parent PID: 5976 26
General 26
File Activities 27
File Created 27
File Deleted 27
File Written 27
File Read 27
Analysis Process: mssvgt.pif PID: 7104 Parent PID: 6848 27
General 27
File Activities 29
File Created 29
File Written 29
File Read 29
Registry Activities 29
Key Value Created 29
Analysis Process: RegSvcs.exe PID: 4476 Parent PID: 7104 29
General 29
File Activities 30
File Created 30
File Deleted 30
File Written 30
File Read 30
Registry Activities 30
Key Value Created 30
Analysis Process: schtasks.exe PID: 5768 Parent PID: 4476 30
General 30
File Activities 31
File Read 31
Analysis Process: conhost.exe PID: 5748 Parent PID: 5768 31
General 31
Analysis Process: schtasks.exe PID: 6760 Parent PID: 4476 31
General 31
File Activities 31
File Read 31
Analysis Process: mssvgt.pif PID: 984 Parent PID: 3424 31
General 31
File Activities 33
File Deleted 33
File Written 33
File Read 33
Analysis Process: conhost.exe PID: 6452 Parent PID: 6760 34
General 34
Analysis Process: RegSvcs.exe PID: 768 Parent PID: 968 34
General 34
File Activities 34
File Created 34
File Written 34
File Read 34
Analysis Process: conhost.exe PID: 4864 Parent PID: 768 34
General 34
Analysis Process: dhcpmon.exe PID: 6576 Parent PID: 968 35
General 35
File Activities 35
File Created 35
File Written 35
File Read 35
Analysis Process: conhost.exe PID: 6500 Parent PID: 6576 35
General 35
Analysis Process: RegSvcs.exe PID: 6744 Parent PID: 984 35
General 35
File Activities 36
File Created 36
File Read 36
Analysis Process: wscript.exe PID: 6996 Parent PID: 3424 36
General 36
File Activities 36
Analysis Process: dhcpmon.exe PID: 7048 Parent PID: 3424 36
General 36
Analysis Process: conhost.exe PID: 6160 Parent PID: 7048 37
General 37
Disassembly 37
Code Analysis 37

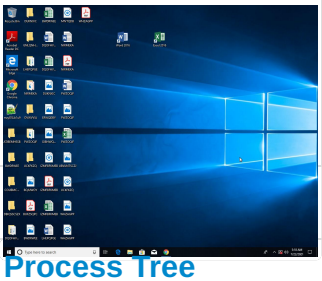
Windows Analysis Report mzyDSLb1u9.exe

Overview

General Information

Sample Name:	mzyDSLb1u9.exe
Analysis ID:	452311
MD5:	922bbf421cd0c9b..
SHA1:	993cd3bc36c7d9…
SHA256:	1bf63394fcf232d…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

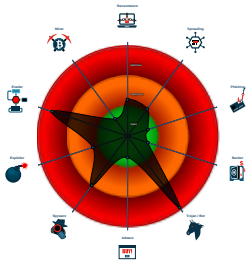
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- mzyDSLb1u9.exe (PID: 6848 cmdline: 'C:\Users\user\Desktop\mzyDSLb1u9.exe' MD5: 922BBF421CD0C9B155F45388DB7C8718)
  - mssvgt.pif (PID: 7104 cmdline: 'C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif' nlcno.gge MD5: 7C81E999E91D1D0F772010DFA4C34923)
    - RegSvcs.exe (PID: 4476 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 5768 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD629.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6760 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpDA12.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6452 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- mssvgt.pif (PID: 984 cmdline: 'C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif' C:\Users\user\AppData\Local\Temp\42926996\nlcno.gge MD5: 7C81E999E91D1D0F772010DFA4C34923)
  - RegSvcs.exe (PID: 6744 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- RegSvcs.exe (PID: 768 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 4864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6576 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- wscript.exe (PID: 6996 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\42926996\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- dhcpmon.exe (PID: 7048 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ba2baad0-dd3f-4844-a1e3-4d042f9a",
  "Group": "HOBBIT",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "185.19.85.175",
  "Port": 48562,
  "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": 30000,
  "MutexTimeout": 5000,
  "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 Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf99d:$x1: NanoCore.ClientPluginHost • 0xf9da:$x2: IClientNetworkHost • 0x1350d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf705:$a: NanoCore • 0xf715:$a: NanoCore • 0xf949:$a: NanoCore • 0xf95d:$a: NanoCore • 0xf99d:$a: NanoCore • 0xf764:$b: ClientPlugin • 0xf966:$b: ClientPlugin • 0xf9a6:$b: ClientPlugin • 0xf88b:$c: ProjectData • 0x10292:$d: DESCrypto • 0x17c5e:$e: KeepAlive • 0x15c4c:$g: LogClientMessage • 0x11e47:$i: get_Connected • 0x105c8:$j: #=q • 0x105f8:$j: #=q • 0x10614:$j: #=q • 0x10644:$j: #=q • 0x10660:$j: #=q • 0x1067c:$j: #=q • 0x106ac:$j: #=q • 0x106c8:$j: #=q
0000000A.00000003.692566467.0000000003D51000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf1d5:$x1: NanoCore.ClientPluginHost • 0xf212:$x2: IClientNetworkHost • 0x12d45:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000003.692566467.0000000003D51000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 136 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.5740000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
6.2.RegSvcs.exe.5740000.9.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
6.2.RegSvcs.exe.5750000.10.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
6.2.RegSvcs.exe.5750000.10.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost
6.2.RegSvcs.exe.3cbb041.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 158 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

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)

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with a suspicious file extension

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM autoit script

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

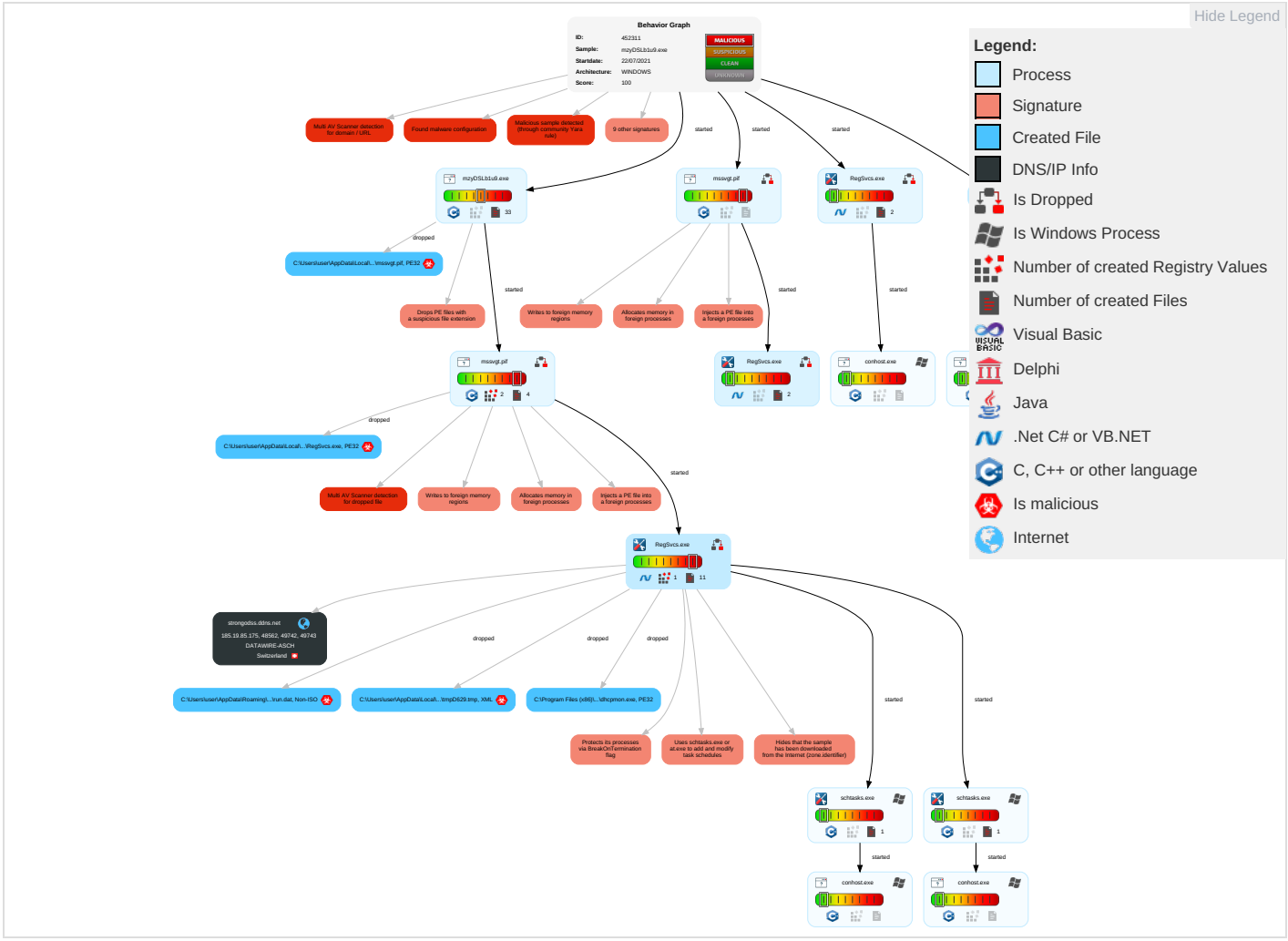
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Valid Accounts 2	Scripting 1 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	Input Capture 3 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingr Trar

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Con and
Default Accounts	Native API 1	Valid Accounts 2	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 3 1	Exfiltration Over Bluetooth	Enc Cha
Domain Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Valid Accounts 2	Scripting 1 1	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Non Port
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Access Token Manipulation 2 1	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Rem Acc Soft
Cloud Accounts	Cron	Network Logon Script	Process Injection 3 1 2	Software Packing 1 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Non App Laye Prot
Replication Through Removable Media	Launchd	Rc.common	Scheduled Task/Job 1	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 1 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	App Laye Prot
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Valid Accounts 2	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 2 1	/etc/passwd and /etc/shadow	Application Window Discovery 1 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 2 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

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
mzyDSLb1u9.exe	54%	Virustotal		Browse
mzyDSLb1u9.exe	34%	Metadefender		Browse
mzyDSLb1u9.exe	68%	ReversingLabs	Win32.Backdoor.NanoCore	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif	23%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif	29%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegSvcs.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.RegSvcs.exe.a00000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.RegSvcs.exe.790000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.RegSvcs.exe.6460000.12.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
185.19.85.175	1%	Virustotal		Browse
185.19.85.175	0%	Avira URL Cloud	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://secure.globalsign.net/cacert/ObjectSign.crt09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://www.globalsign.net/repository09	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
strongodss.ddns.net	11%	Virustotal		Browse
strongodss.ddns.net	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	
http://www.globalsign.net/repository/03	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	185.19.85.175	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.19.85.175	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	strongodss.ddns.net	Switzerland		48971	DATAWIRE-ASCH	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452311
Start date:	22.07.2021
Start time:	05:16:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mzyDSLb1u9.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@21/39@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.2% (good quality ratio 54.4%) • Quality average: 78.6% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 59% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
05:17:00	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif C:\Users\user\AppData\Local\Temp\42926996\nlcno.gge
05:17:08	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Local\Temp\42926996\Update.vbs
05:17:09	API Interceptor	872x Sleep call for process: RegSvcs.exe modified
05:17:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
05:17:10	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
05:17:17	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • 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\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
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\42926996\Update.vbs	
Process:	C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	4.928015689340774
Encrypted:	false
SSDEEP:	3:FER/n0eFH5Ot+kiE2J5xAImccC1CRL0c1t+kiE2J5xAImccBzi:FER/lFHIwkn23fELlwkn23fsm
MD5:	57F868ECBD091E4FDB78520CB92C7CE9
SHA1:	B136BF81EF0CDE1ACB81805F0F720B1B27EA9AAE
SHA-256:	46A47F9E99337DC115456C5D920870A2F2319F96DE3E4FFD77D3EC27C6410E16
SHA-512:	CB788015AE9F6801BC944E5B35501E89AFB3521CE91C4A7D7CF7012AB485682B2EEB277F403468482431D3C798F0A876427DD32885B4A40D7397295B440D821D
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif C:\Users\user\AppData\Local\Temp\42926996\nlcno.gge"

C:\Users\user\AppData\Local\Temp\42926996\ckmir.docx	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	617
Entropy (8bit):	5.449426819433693
Encrypted:	false
SSDEEP:	12:YNMZFGHeCG9n5Fl8rrLeJx5GsFh7qJhThCBQ2Yg:YNkUPG9nCrrLeRGWhebh2d
MD5:	69C5527A6AEAD551FC9EC27F9B6B7498
SHA1:	EDF1652A6CACDC3491E2B6B8D0031504A70708E1
SHA-256:	FFBABE99CFBD630F4FEA2D4976BE390DBD0BA1D91FD73419BBAD456DFDF642B9
SHA-512:	B995245FB6A5F73143F1B5C075A59F8670D2CA974EA932672396A67B5CDBF22C8917CF33882A9E6CF6B7763E4776C20877B1033202CF4939A728267D569A8DD4
Malicious:	false
Reputation:	unknown
Preview:	K2627..1GA8402dH83YGM26s725062NV6794kd466S36Hj02Nm8100Rhtnpt4F6w62414rhe899..M6MZ4Q7m4UQ7T8V0431C59N..84POy..Jk538ka75F5XH4l8661XM 2703d96278zZ5H34Nf525X8p1xPp4w3fS4Z3F5D77C9qDg58kP5p93SK930GVS1yq0..bm3N24M1kk51mQ1Nv3Q7H354t7QGl7pv8K17DD01lf21412ry53WhMGZ4Y0Q7n e773w4cwKKx79y06dmK0x857A2NhN287PM1X8D01W..209386kDem6K..75y004a5W24761AaU62bnVd9N0zs47z060tUE13h89O7g5yf12MNS1Q32jD1J1vlba45p2m02 lf5E08e32dW97m43683a2V0s4N98aOj58N3Pd1CdX0zD1sx2l278Ud6tzm7HqAD2qhUa3W..oy135iFp39vI01J83JD0Zq0BzU4Fi865..vVu0O321x7agSf24gX6fXSqz SP6Q117kDN680q1bl66Na5278U9150M8g8i7C6h88FXP8v0eb56C23G907473XZfm2fX015NLYzCYai003rX883P52WKflL..

C:\Users\user\AppData\Local\Temp\42926996\cwgoehjl.pdf	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	541
Entropy (8bit):	5.479324009317679
Encrypted:	false
SSDEEP:	12:8+sYbXmRDS6+ShLLGvUF/WqSyOXCZMEcUOAlf+cth1iy:8NuaDHRNmki+JcF2rB
MD5:	2826C4C433D5C75761FF6776F84E93A2
SHA1:	372B90A33936691FB879FF904916B18D1D3427BC
SHA-256:	9FB13FC02A504733A6E277DE71D2CAAD43B08400233DEA00A17A13ED452D53A6
SHA-512:	C288814440CEA339E774CF40995E53CFD069B7B2A2CE76E99AD249E9BD816776C4749D5926D9D6EB0018347602C6A55520D79DC9CEBFD24AAA522EE19043009
Malicious:	false
Reputation:	unknown
Preview:	256c0EoLkX71748g10606T6824oGIjb319843Rps20g9RVMV40xu00U0434NHVj1wJZhY9BH1H6u053L..IY426C46pzu5sdCxH0FJCca4nMTS121xT090C57Ob1I1wKeW 2v6YbS9F7dh593B9274AG49214tB21H..v0sd60s9DQJKJ6s709g0D562ROzH7T7m9I2aA6N71cb4y2S593YPW5B541n28Yk9103A6d7605m06ov8L2282pfnbj7311AIY 5l9qZk57T9..9u6W8..l4187Rd866J825qGe9vVN6ww4t87J2882A76mtU0R78kVLq16NsWG3g3VE9514x0U380D6h..N2ol35rAU2sD3PDFgU77Oq17l3314..73375lX 594S525eVrcv797EKg270Ng7dwrQ04LA047Fd707dh1PI75o2C744O9dB6z4k2r18iv9g7RT5279h5f2o7Q68b0n9171A032Om8t2notsw44Av4JO00q1O83l67V3061A9 943pxfF80Zd54WNS1iZ..

C:\Users\user\AppData\Local\Temp\42926996\fiqhwi.cpl	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	579
Entropy (8bit):	5.514395455746834
Encrypted:	false
SSDEEP:	12:WX15avfwhfrYd33LdeYN0keB5cawzALrWWb80qsQ/FUrUBJEA:6YGfA33LUYykeB5lWsrWWblLi6QBJ1
MD5:	8018EE0EB16AFAE8BA0E390FD5F57614
SHA1:	8104C1E01EC5EDFEC260776A8DEAA713031DE8D1
SHA-256:	B3D59FCD803D678046A6CC622E29450096C58B9CC043FE239FB67EEFA5156162
SHA-512:	D929D64EBD9D2CD62F92FD27C4DA9A1DD452C5D4C82E3345CCEACEAEC0C9D0FDC5033C85EC4CAFD17F579BFAFFFFE9725DF05D066B7A2B6F1D2014243E2F4D6
Malicious:	false
Reputation:	unknown
Preview:	dcm590D385015kDPT64fF5v65125W72LU1Yp0Q3Ykp8e95r8d2Q7Q69L900b92U94Gizdw7fQet6415Chy9u073p59D45JuCs..U876K..9034U0X129e3RQ004775..9Q6Jnydx9XR9tDxuS11nYkuW07VJn7zP65j6y70U2q4l4K7bL8NRb947gOA0mQiMpsj277rdNN..65clLQ8Ck3GFu393W0858kJo29uhUA7N741v8J02fu55D476ka88RJZ0LA7ZT28HY57HU7060j7D46zI1s10x3L7R..48525nh8sLPxb2..w8rl5YArf7816qv1gY56S834X3mZK4IIre3e41fC1k6J45S99529LPw9yv1087k51068282t78E3Hgsq3A9jt3bll..x55t20BA7xpK20AAT98051D3oO42pIUQ8116Ug2M0K0h99d1h9E0QF7Glw017p36ndchVbv4..9DVhZn4w21pswjk8K9Y2v1..W23p0f8eXl8V08U20jO0s00x18799c930V04xBVS13Kj9x8Rl8Z7U7TG3yb61m3A9Es0825wRl024..

C:\Users\user\AppData\Local\Temp\42926996\grkdutke.log	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	538
Entropy (8bit):	5.4956415265284875
Encrypted:	false
SSDEEP:	12:Vi+LEl/gjqzXRFDxElJqwEVNU1fkEVskq+TFxBDcip24AzvKov:VBLauqrtEEz1fNskq+cAFADKy
MD5:	69C2E12C93CF11B56188F941B01DA7B8
SHA1:	16F78D9EAC39095F5A739C7B2FAACB1303581A1B
SHA-256:	E492A1AF16382B8391FA9365BAD3693DC68D8A171AA19AFA90708459E6F1F136
SHA-512:	EC241B94F9721C9E38A1F9C4242B19B41781537EF2A73D1BD57F9A7D578B76A2C276F6F6C843C83EC0E5C3F876AC52949EBA212B253B03228C096CEA786F55A
Malicious:	false
Reputation:	unknown
Preview:	7oOf0O58zs677R374561OK5qC7mpkcahO2ST791dSSU7a6..6lc0qxsV9cEFGG0075Z6tJRGEp6yZ447m7Br5eU11R73Unm061K560Am7c567rw5626l5H6EH0egDv..wv30c5Ti7dp70V5e69h0cO56OtkN40IK9uZ8996E..kEQem9Gv0m832sw2E37445qUU5ydd..5ei122X40wB3522Fi4cw22Yndl36AT08E22P5Z9721Me22St175134k8o6ik9867MtN5vN4916067zLDISJf4na77s61946P57a5Q9L8281j99v1Ox3m004478852Pg5..48OO71B8DhpcK3Tjvg1S9S35g712BaO2wKuo480YhQ7cQX33djx74R9D210uMWrh7cjTz2s54hk38w144Atf9HVx2aZ29Q73..AOuN6wV555W4nN86UE78dm8f2wd430YGuNQ5Nx44890Z1CCTH227161g3zt7vhV59xf0477Eg714p0z15H1ly7C0037a6UYioJf65Mc0708..

C:\Users\user\AppData\Local\Temp\42926996\hbnbumf.ico	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	620
Entropy (8bit):	5.5422947484886045
Encrypted:	false
SSDEEP:	12:fepl9EmceL0Oq2A9DJg0SSr+dQ+YQ13lSeY0Y/DDFU9:fUpeDJTSSriQ9o1SeY0QZU9
MD5:	1919C73E61E57957681F1BD1FDF85C83
SHA1:	2D0725A62BDDACE1D0E3D383D89AA159D901E838
SHA-256:	6C6F2FE2BAA0B45090F5451E54CEABCC04B8B822C66250A7C04FE4DF9694B20F
SHA-512:	4500C06B44B7ADF1B5DC7C10115B7CD2E54157B85F090CB6C1105989113610CE90E3A03D5C9482B33E065C73B1A8905ED9A8BAA6676D0B66CA195B5A3415E7E
Malicious:	false
Reputation:	unknown
Preview:	SIkg6764sWm2l3WIJH6Q78Ezi460tu1Z57pC4C7e1qXk901t3RsT91R2Vd1BI9g4Wj3d281075m564z9Z7jv7KyMOR9MHwCv5N56c7370tz0F4Se7Q..9j1RaF4mY2239RRlo6q9BZ44oM6Hn21777vQ5g1K3apC8mBE03i96Ms259L7OwS03Nn53034n09pxZlF317wMXxA9410K1461PB51o38v2J6R9h17NJGV1E..64bi31w7jl2..I29T74l21XG0YczP10Cd80mNU27078i4V79Rx28ydQ485N9K81B26Q07plW9w3rT5W22PT..n7z55D2R70e54A1F089S1So2IH22r717qRBeFbp..Z044hOgH5x1H0XV9TKS01ObiE1e0q313p0R5518487iZW27tMEoERRil6C90S1..01VFJ96I8pf..6227b4w6..2T2p64vdE3PlND000etT4w8467j3OC2lkR9r3O8L7knlcMa1P2J22068q7c7clT8s343o9zFOUEG568Go58x07eB04Fo85wsAyOE8l6Sa754x3jib6u13a56MS2349h8Kc2346Z29z00l7JS8rCml7PjL79f04nLP5FM93Tc..

C:\Users\user\AppData\Local\Temp\42926996\hfnchgbbo.xl	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	646
Entropy (8bit):	5.443595298898935

C:\Users\user\AppData\Local\Temp\42926996\hfnchgbbo.xl	
Encrypted:	false
SSDEEP:	12:WxyC3WgVsoCK5MTeVmH4CQlJQxdiQ4dS37T3McYX41QkJEOE668wKR43GVEqL02h:YGgqyVmYCQYxUS3nGl8wH3CEa07s1h8y
MD5:	4622EA27860D80356A2C95B906759959
SHA1:	12C5DA2DA50C0C3A76C153BB0DE2213D391B09C7
SHA-256:	CFDE0EF36739DD63F651EC9944BF13AF38DAF9A8426ADF98F23D14D7945245D3
SHA-512:	54A7EB01D5FC0075281AF6D28E434F0748C57A3A946A1E016EC28AC3B1D2099599A4B4AB3CBF428998BB370A6609C35E374C1286EFF2212B0033E35260DD6F1E
Malicious:	false
Reputation:	unknown
Preview:	nli41a823R693jgAmT3wx..9jclU3qG6J088T8..miwT25vE4xztgs7pM5o21N8TcYrA8h2K4988M7D6bSC90Bf0HXg0A950l8EdzzcOK3Mm32A5u0Zo32E5U488H87CA5 h983909Tj79bc892WTA5294fe10lkV791w5..v6964L5G588dFS80NjZ2fjqog4Muf74gzLM6nK6Z7SebMO2Cw6P48mJQ83727SW024887ATj0M0r225y9R53a3279H517 vOe..79jdx55D497mlc9Uasfl9V8tVMW9e9I33810RH7Eq55z7ZFq0iVB329k0..618j571934J3o0g2QrW9N98tQx4onLRa7B65G4374O9hoO2IO31G49677kmci2u9Am F7wdk5o8w7s6C556V1Jge7C4D6P7S54883893J217H6G055J035G5W459g31mbi29..84QOB11305qzB7Fg1..3f3lo135j985tKI8..1tDVocN4z1089J7w81S7161754 84269s0407o8X3355569bV7g2hQ864duF8556sx040z4252mg099X4txJ2UlS615S4W40S675eP363WaTcIo1c1yB4G45xM07431917e17Du9Un8g88853jg6Y6Y..

C:\Users\user\AppData\Local\Temp\42926996\ifst.icm	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	521
Entropy (8bit):	5.4431785971520705
Encrypted:	false
SSDEEP:	12:r0LULkV/31WQMHnHI7uUfshdwIdY4jWW5MSdTU/APBQBXGaKLysn:FLA/3sH0ussLwIi4xOnAPBQlGzLLn
MD5:	745022BF11251404193A08B59C632B63
SHA1:	DD7CA88057967A568045511B287500BE630A1BF6
SHA-256:	84D0BE7CE0472C0B09E8511F183C803ABAEB20E3268244EAE34F3871E7E4E7FA
SHA-512:	74163C541AB9292DD4036A5E028CC7FB19A7ECF67E054D5DFB1A00F0CC9B8B34BCBB6DEE65B91C0DD3838CD523567ADFB54C406F86E9C3B86E1C216CACC1 346
Malicious:	false
Reputation:	unknown
Preview:	Jnd515ky83qSv6R0155841797Mqr937376nDS759T813eTn6e620mr5A0198m95mf6NY50D220tSq49kopQ69kgn9eD5pY9sg79XX6v1L26l4594nL4a3Vd329vu..en59 B9H5FV6t7Zvzx96560Fk997072ux55Bd29qAi8t66L92zSFQN6546kh2n5U7G12KdCq4mhy0lt..223Mhh342YS2s4Ng1C0AO65e3g3E41h08463y9g1886733cU..0wiR 6659B8ow8sc6W73Nvd36F00vL49a7SH0792dg1wr3b3z6742806608j38qmy3W8e23f7R64wa3Lxg504Wp8i3S6iSR5QCg541QO525W8uQg6v8X6tt6P7H7..aI417C1k6 L6Y551bopDECnLk99d70qM4cQCn598F0VQg..6oVMe7586lQ7k405a1p79ZN0K196e9nvVt9635yU9sBP65kVK800xESogfPTKe4ljY3797Z2n5CF133D3562z5B24sDo..

C:\Users\user\AppData\Local\Temp\42926996\kjra.log	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	524
Entropy (8bit):	5.528005365651393
Encrypted:	false
SSDEEP:	12:3smWrPADVS+qdP8fZm2w7D/rBjAOvBRDoN1QcGH1U8wud5A:cmDDVbAzBj3BFonQFT6
MD5:	1F1E59FECF5DF5D67EB5EA8F76757A82
SHA1:	A7583FACAC88C72EBE0153748DBF8F15168C8C0F
SHA-256:	A96E17A36BDDB28D181AB94B1D1A71AD8F9777C3371C622F09572FA48DE98858
SHA-512:	F03DC39ABC911CADF704314DBA7D0F117D3FF8BD8D7E57801AD32844D5827B590E1D6A7D942E60793E5142ED71DA7D4981992554994C164EAD279064617E0CA
Malicious:	false
Reputation:	unknown
Preview:	DK0gd59THXol0jz39V3969Zy56525I3Ecb959yoJf5pBef7IKl8e9W3E9231W6rgm796JIOe7hY9Jo789gbxbs08t2056W9fZ3hTktljt1jTD93288wG3d28XgCF..981g 4155p5753pLJTDDhBH9C0sY88R01HUG30z0tk4qS74xRUeYx0NwZPFy2yhvbK0V5I54603F4407l1vt13v36r9C55x7MS252xi36DP44zRUAE8j237e717uhCr45GHF9YN eR7hB4cG30r2..Z4Jv769401QbYDdN147327cIRW45l872nku9HxK36m05sQHO8605k99IG5ICJIo50r74B1I5389l08E806b4W1K1sdnuCtK75bFr9Cv5kb0n2lVI7..5 9e6Pl46B6RnFm1pL00739D45E698Dc12weSbR44..13Q33645a631159r08Y37j757PUScsbgm..4R2p82246OE1f2f4P1h166ByQ97NUS7b3v61x17WwCE503Z8yrh4dp W4..

C:\Users\user\AppData\Local\Temp\42926996\lbmvv.exe	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	574
Entropy (8bit):	5.476882831858443
Encrypted:	false
SSDEEP:	12:Ls1NqtoRYoSRmzT0CEo2SxGoH4l12bYfC6cfHVDU6RjIPpuwrKXSK:gq7oimf0CB2SsoH4f2bY66cdU6RjsPKR
MD5:	5E60119B2669886F999279009DA914AA
SHA1:	47E8ADE1FBA418C5C6D89F91A652B7D465D0982A
SHA-256:	445D2F496120BA52AB586F17CA0060B76529E090C9E6D3B388E2C44E5AAB4D0D
SHA-512:	20881FFC12CA10F7C86FB56231715765E05F60CFC61972C5570167C5C81C89B7FB896D04BD95C68CAC1D28420B0248DA48EA8F1E1FB1023DC20DF2FF00D33EE

C:\Users\user\AppData\Local\Temp\42926996\lbmvv.exe	
Malicious:	false
Reputation:	unknown
Preview:	6w027Sdr9mL4M70UIk9cv5m26300444H3VA83w7354nx4eL7k62Pkwo..Iq11M7W494896K2ArX3782Jdu74a8ZM091G9T9LHmeg01dbH09S..4N44i997N2168..7hj0L tC6mn800M0709T8461201TpC36T01Yg3D5YHt3s72t8rT12C0A50MpWrgP7ee9bSe25Y7Vz6223c6kS60FgdIZ1F5796D7..QVc5L3Y20IDip47T746RW7P2u45549Vc29 p568D91lle0180K3E641qn0F6Si883j105484PR11dW042o..2NwB14oMr853249j6759a10YB031yRhC33wcU5oysj2jna86vtE4kl8n4h79dUA53vKF7i9e6AIq7cdzz 667L..IhB6Q39BM9V0267a7qwoC813p0cB1j466THoh310JmZ5V725Q25tIk5C7k68q7e4tM4tly2kv2nDlOxQp76R9g..3t358M9ngPD5CV321HR0Fj0F0BC1B54pvEun 20376D55p7X071W9w9050SQG0e7quA9Mv94C000qILc33CfgB27z..

C:\Users\user\AppData\Local\Temp\42926996\miwpdssknh.msc	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	590
Entropy (8bit):	5.498198413930072
Encrypted:	false
SSDEEP:	12:1uO7nuPKbGfQXmBo2N1j2lxuavYBMz5SYEf94ncojOX8:1uO7k1Bo27SavsMz54fEhOX8
MD5:	7E44ED3E3F35671005625036A8C6FA5F
SHA1:	DDE31F00B9EDDA3A43A97F013930DF5580CC9D0A
SHA-256:	86E93351ED56297C38ABBEEFDEB5774C521A7A9AE0C1A0026F1111040BC47D60
SHA-512:	62B6F21650ADA4782F65C09A33A8BAE5E9C83478C3CB8254D9FBEC54E2650C691E46DA00D3D8DE6C32D45C6C1E91077BEF867C6876E27F58609919182FE32CA
Malicious:	false
Reputation:	unknown
Preview:	978l4g9T29D..1R3718Gh1QX7034hO157Lm65k7d1WG4v2XZT33XxJ06TB1dhM7J2VrPrFa7mP9C79mV0ED0jW4e2l1h85X6859515z9h2dzUN4c58MW06U3 9kpR91Wj82c..f5xE3oAunY34H3M6G61PR0j50g8e0A1159y88xl14HGs7fY8Rgc28919nA60tScp4986sdZP5F21a0767gU8..gSL0746aEy34s8s681o83959Ja73Xx2 n23cSA569v99m9w7w5198N0k888yt939d5Q6R280nl5r03w2yHm3Ws4Vp6s618nai0GY6..FCRvgc7OR3J79C6dQ54G39oo87s95Aog4n2p4hG15IQ30A26L39rE761nmT ZiJol591N369f82W821l9ydif644HaT5av1IR11Eb894a4z8447A5fBz468STol7FgmTJ6O4zT2qwx5O328b1H808w8..88aJjU5mH57Qf9RJ29Hy1Ol57i5VD7BHC138x uw3RkiEzDfxv08C13317749Hr5B35kQX1iFI6n8u4j264150aJ8X6VV7vNfhtZV9v49765B690u56P..

C:\Users\user\AppData\Local\Temp\42926996\movg.mp3	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	507
Entropy (8bit):	5.5028954520443465
Encrypted:	false
SSDEEP:	12:+ikTNSNWhkTk4BXfbIwO86SBWAGvJiZCgiRnpYF:4SPPbIwBLZGvk
MD5:	72B74DE7322DDB09C5D3A61BD25BF679
SHA1:	53BB1720B7F09DA2B88AF19B3D40CB4DDEC9272A
SHA-256:	FB155D6C46F4A9A431F8C93F072BF49A55B9A788CA922A16EE966976B5D0CAE0
SHA-512:	1937D98877EDE2D3E30FB87317451FD8DE3F96D575187F2DDE1284CEF48D665081CE938D2905B5DE39AA3549228B83396423DD0DCADA076AD3369FCD4CF551
Malicious:	false
Reputation:	unknown
Preview:	PCo2eg9U7325..zvEnNXmsAqeH..4lV7ckhs889z6P5777D8uBD7GBR24tdo0199m1D41j0gU34D1x5IkA032igV8RfXA769eWYP36d33kC305dW63v1Ru348U2D91499T 60amrA65V75wNdkzs..ow954018wH2Lkq53cbH0640s4SPB28n7UgrPZzJUp29mj6pQ2jU9d02u15kIB6s20d2i3W657u590RM5U101M5L56RcSu6u63m..22z87UFh9k5 84ZwT0SzqD4C47l3FK64URYh9q4M083746eo8Y8X455Ghj12FI8F9I17zg0OyU24pFiv0187s..5kzcQ3N9870HY0N4870N3s185t553h561G3372780Aq9Y22LYEE4C4q 303696e6Vik89j7y0i5sdG6G336oyS9ymcIk052mO0084c100JfLxUs1D7k176813g661I11p42jZm..Sd414Q5C71O2h34XPbNY2I388VwHkTKk9Y8..

C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	855280
Entropy (8bit):	6.394628658129692
Encrypted:	false
SSDEEP:	12288:8BzZm7d9AZAYJVB7ii/XAvKxRJBnwvogSJ4M4G4aBgZ7u/8u5DGDt2:ucneJVBvXAvwRJdwvZ5aGzu5DGR2
MD5:	7C81E999E91D1D0F772010DFA4C34923
SHA1:	76CAADC92346688B50A408B6C48017563A24844F
SHA-256:	73A52A4C60D253CCDB79E5D50814D1689A49FD85F9E0A40A0DC57BA7FB54E5C0
SHA-512:	EE5777AAFC4B568465B85322BA6FFCF0A38ECADDE6274A2E4FDF440CF2EA061762A4B07EEB9A5B40B61D8BF3DAB91871715BC5E64DA74768F0BE342B1F79AE27
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 23%, Browse • Antivirus: ReversingLabs, Detection: 29%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1b.....P.)....Q.....y.....i.....}...N.....d.....`.....m.....g....Rich..... .....PE..L....%O....."..... .....d..... ....@.....`.....@...@.....@.....T.....%.....D.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc....%.....&...R.....@..@.reloc...u.....v...x.....@..B..... ....

C:\Users\user\AppData\Local\Temp\42926996\nlcno.gge	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	127058776
Entropy (8bit):	7.046934448053015
Encrypted:	false
SSDEEP:	196608:dHzjoiE/XUnPtU0aQcLqutJQpBFSf+3sdH7zYagPjPKzi4hpKR8tOZA9ZKW76+wy:y
MD5:	92361A2C6EEA87C6307831A666FA7D2C
SHA1:	63AB641C55862BCFA206961541F76F880DA724E1
SHA-256:	971FC12991949A36D791C0E78F3C2AF5E8F2F12220C875D196CEEA03541F6E11
SHA-512:	4A9E383AB333DFCC1098F703F8716967AFB5938B47796CD1B3C77162AF7A6713967483FECE000211703B581DA2F5738364D2EDBB1F77269FC7D5BDE935D347AF
Malicious:	false
Reputation:	unknown
Preview:	..;....F.....H.)...b].7p.10X..i....0Ze.j...u.b..T...Z.84.....t..>.....E../..nG.%].....<....Ul..N%.....j.G-.z..T.....#.c.s...H.u>.o..... ..=<.p.....y..g....C7.bog....x..4VX....~..W..U.. ..0..\.1..1.D..p.....9.1.6.4.M.0.8.X.2.h.1.p.5.1.E.8.i.p.7.X.4.s.4.9.3.G.m.0.0.3.5.0.c.7.L.f.c.W.9.2.5.....r.@..>O...A.'.a.O.W..=3...b.i....(....SPB..DF.|^a.%.N..hL>.y.B.....'2_. 4U.2..8....J..e.....[.....y2E&.....f.....#.$&j.R..R....d..vP.D/_N..S=.....hS2..C...'..UK0....1....%3m.b...6..1l.Q. .Z..5...7.....g8.....i.W..h.H)MF.-... 6%.b$.*;....W..c..T..,.oX*[b q..y.8....#K.....z...n. .....r./b.....,vFj.H..F.Uk.jk#`.'..L.....F..D.....E.G..Y..6f6@g.c..J....@e.;...Q_.hZ.....D.v..4.%...Ru.....<.8..J..C.z...c...u.....'=5.....x...i.... N.~.**B..t.w.j.#.C.v.....".].w..)z.6.r.+.j..._.{.J..... ...+.w...4.....#,6Gj2.j'.c....'...;.JwZ....r.Y.6.Y.q.L.5.1.7.C.j.9.5.l.6.m.s.8.3.N.9.T.....~l.~.....'...d...3.U.^)....H

C:\Users\user\AppData\Local\Temp\42926996\oglqugsxk.cpl	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	571
Entropy (8bit):	5.449934915839515
Encrypted:	false
SSDEEP:	
MD5:	CF085B6E054EDDF34B1EA65EC358E493
SHA1:	0A4E8F79E20562A700BE4398A08B9731D0372AB3
SHA-256:	D7F0516C623C0CF7AA93F4A440682AFBA44C46559C47FE1BCAE53EE2B69678E2
SHA-512:	55702C9025B1B8E40F724B12A72D70F10251E4F946ABA32EFCC17762B90437A084F0610E0C1BEC2E412A94E30DE46559DF9920DFCDD36192B7792739B08249B3
Malicious:	false
Reputation:	unknown
Preview:	s1002R7ZKDEsd8Q3M9J23D2j7p29X38TJN7j3K5xto53bm4a6V34WY332G44n243KbE7iy4038r3QD2eLj10559FS3C4492M0Y9ZWQY4P6te63Kqg9HBY022 Qo4793Po24j1l9131W4T60K5NZri42KS5ZBKA6759wR..4nF37Cj0cWm72X0YS68NwcEa764v073lxhwx39m0450K2K12ky8o714Z30S2Gc676tpVtoTSi0a126P7q1336 2Dl2u46sbBD491yr1336U894RG9c1J6t7B768A78s3b8516eNFn66y3L10sVoZi5t3138U5sz7YK1501Y75Qo595AT5JZ7..g3S0HTyQmz697jo1O0K08G7517r26P9JM3 67c62bT0a417225RR531L4KF5Z2G..5J0v6Hm213MO5rB4JW458xAx8cd45M82o0yy70rkWxm55N5KH2C5l65d6P96o..9bl81C0om64s751Jks4Dry5OnVl66s1t6482A 3374pb5y33R7xn755l0zu4RaR63T2ZSC8eF9WR66l9bf8pGGVdx9Ss1Dl90..

C:\Users\user\AppData\Local\Temp\42926996\osmphj.xml	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	491927
Entropy (8bit):	4.409452520509473
Encrypted:	false
SSDEEP:	
MD5:	1FC724968D0BF0390A4AEFBF97D8DE8C
SHA1:	EA72BD83EDD43EC5D44722355A90F5DAC04C5DEA
SHA-256:	CB686EADCFC96AF6C8ABDF3C8C71F498D51045784ADAA62504EFA8146481739C
SHA-512:	2D566754A67A516DAA3081B8319A869060E78D5BCEB190F36450B7F115528CFD681A582550A5B9462360E1358D21C946836D25E6DBEC15E426B2094AF89F2D8B
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\42926996\osmphj.xml	
Preview:	800o4TBqPL2E57v4TVP0569e4H9F095v6A8Gthsj899op0MJ..94080jmj..0bykqpX17Ef5ggQ7P9HF4..ieK1081zi31IPAp06z6123s2EG8Oa7UhCw2t684C6p7O38K 4YAY6Df..67N966f5645ZQ5FTV9D16OG61GQKxn4W4tvaukw0qlDIdS5fR2iW9qC3O73702Ojdx4..8DZpHCc1Z305115A434s1kX007118pqq85l993Scb4a62iu8MkW1 X0V20d4T5r9X..I2229H6853mHz0Pj2lMK877764nW47r5Si5GVMR..6O88xk22c7V74163w7la6o1OCs0d5fd31HrMqlhf..S73522aN1907A6d2w40vmef270693yt.. 412054L8Io64598685063069cS772UD0436Jz38AO3GV7f7fSP98n5YKhx5JZ3u0406Zw5AIlK368A15..sl3bk3Q0gMX74heeo3E3u2a67Tx02ce0c87gq8yN508156I7 LY6R5mAF9g21J2LQ718567OCzp1G7Y0g2F8..m783t3Q3ac2ngukZ6x409A74U5529uGQ1dSSEl6B1Za9Jw67DS8g3be724mdB193m2AXDxYcadAQf60..31 ERYW422T134WW442o5040uh7e9078fA046v5kL4184F11je27c547r03b897QX33..5M7i6r180147z1tB3X58gq2K4ZK2v636eg609YYdM8w37Cg4UX4o30uu0D3545C6 nz3GpZvK..rl20K88sV9376v7EdL90Ho7222l7xE997..eY5i9q203Y284l31R998E3ec7f90oq2J2wld680G3z2y277p9vS4L1..L89654bm016Alj47m7S3S54f2aS0vt9..21252L 3a2544m292vQe92J6sR1j81vVa5W7999kp7jV05lmW2818W6KQR9Mq30V72389Q0QQTG5..L4451m1WU574i6B1YhF

C:\Users\user\AppData\Local\Temp\42926996\pxoxuqd.mp3	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	512
Entropy (8bit):	5.408101591607319
Encrypted:	false
SSDEEP:	
MD5:	2A8111F27A0B2DE0EA3147A7A525B60A
SHA1:	24CE7AB45455E8723260750FDA7E921828285CA4
SHA-256:	68287F784D6DB192934DDC2037BD35DBC4CE86D7932FB8A6144F176ED8A3C529
SHA-512:	B31EB7E7A2DB36452372BE51CB679E3BFFAAC17C96D90935660A4A27BC22865A55004C52A2758E37B1EAAA9BAE4FFD8E461CB5314B4FB03BC5033CB431475AF7
Malicious:	false
Reputation:	unknown
Preview:	0meN933b6T4BP9GbAOo6f..86ee68vDp477b982W8gt4i2zvR046732632PIB66Q9yDUn4sD9ayMmM..C0p1i0cD8m24uG9c4838yWG33S75b15SH6v5S98O06gY7tKbp6 5WBv3j62Oc84S5106ZHj57t7yb695w009DGr34D93..26iBd99YD4z5x3EG1DeZ9K14858sGcEe8466l3plrT5LC5Bl2N2S4R103Hh3lW5156..M2FZ1eFz6H204EmK897 41n3t51D58gd3Ta1727058W58j0092r7e44U322sp98p0p9n6aXLkqk3zt44097Pn2Vm5K4827wFb..t94BK66Fy32t8..i9a166heyi0G6e1W2D7h2D20d079M8H13i9A 01g95Plc3UjwxB560nGB78G89i5NZ9ge41699D9vR0U8KG5d629b871S428H8w80Ed1..8Q8v56MpgFP07B5911976Pu6960JT10ADT8c1dSt7D464J1NyCv..

C:\Users\user\AppData\Local\Temp\42926996\qbfcdn.ini	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.451436816252411
Encrypted:	false
SSDEEP:	
MD5:	3DB4894C43392B664A37F1A8B4C932FD
SHA1:	F5B3978E81964AA29DB40E7EE757D084B6311C97
SHA-256:	25758D73FDA9A55FB2ED6ED00FD0792EF1265958B0491F95BBBE47C4C5D4243C
SHA-512:	DBCE3DDAAF70295484DD837C13E82D7954C6DB5014038D811700E6E917238EFD3122EAFEB1D64CE51D28B72619BC2157D958AD67C2D0B2E1BF33ADCE1F7DCAC
Malicious:	false
Reputation:	unknown
Preview:	50vwc81cTX6297A32v63kp090116PaG02K3P9r2108DJWu0lA0m41K36t04FUXN8N7zf36oQ6e0W53r8vaSS23O51v33tQdW094UMO98150O680L..w0350707LfZ307AA 4ZVGv61kv07KrvEb3i3N95..o3Q809DRj4p8T36505rzWwa0506005ns79078gE0a70j3t55i5I3lXQ5V2w1n4JdbJvK92Ruj82Rs163JpVowUeX88amP3FgVLG1Y7m0P8 79t..4R8U3g26L4m4jhScJCW2mlgyfy92aR82c0CP0VtmBb6i4P95V0VM2923uw9Atq2U2HmQp90k4Zwm913c724SjUR75Se3l9Np1obb1768uc1..I9ue6Ha4H3vi8P43 1P4K8dFRU0921613lF5a9yg3N7m3GR9un0fbgFG4JkO8897IG9388lT5z48p..4n6576298Kl4039jc000ql43gF3662ob8j32K1h4LP23QW8U53723fax9825n10z8168 637146..

C:\Users\user\AppData\Local\Temp\42926996\qqnevdri.mp3	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.430749806877986
Encrypted:	false
SSDEEP:	
MD5:	27D65CC4AF528CB21FB2B413D4AB5844
SHA1:	BEADD1DEB8E398574ACB2A1502357C670648E089
SHA-256:	C33D4B875023C27F725707B6F365F9E5DAB4207490FFE81E64FDBF98960FCEED
SHA-512:	BBB050F35A374FFE15A0790D6D15708F5C638873E2EC2C9AE27AFB27922F059C11048168F77E9013BD8638CB901AE358C59EBB09D76B55670E53ACB81A13B6F2
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\42926996\qqnevdri.mp3	
Preview:	nLvFD941P4OnW2983tw8y2g56L8Yk422SE2nE94yu7j7045KR9A4493r3H1C6cl861S1x..PTrD1Z0119751ed92Z7wSAtto6R14Te29k52582L061d345a4a9uOzA5Q5e PF35326ZF..9BJ490899076 76Q5kV6737F5xs9T5gdXLL988V3gW899V84HrvL6n09BqqxR674564123l98ZVrV0ti67R1P7X2BT926A16t35ex90351W2g80735J48urB 76R54lT87MXu39ZkB2W3..U6tV3s701x7q7Xj17d2O0Ig..uJ8j08n0g9So0umQn3jzf280CKO3AMK4267RY02358J1e21f5735..Wu640p4N27H02N4gYJ35j287P3dY1 6V9wEf902w06e70976Mlz4ACK390i7g960G2JJ58Lw965V7X89Nd5DLkm5W7Baz5i4Ys7J5Y973zc75u77Ob89224M35o8l4C598O241Ee1f19hO93Jp22e8Qm002Nlfg6 fqrU2i6y25e5kE8FbCE03H76Uhzh0..

C:\Users\user\AppData\Local\Temp\42926996\shobbgka.dll	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	591
Entropy (8bit):	5.514752960740008
Encrypted:	false
SSDEEP:	
MD5:	FB8633E239A437B6DD04D393AF0A9DC0
SHA1:	8311C0A918CD5D065582451AB266F35F8601AA9C
SHA-256:	5DB471159EA29EE26D76B8798A663C56EC8D1128803C283DD5404E7172B46276
SHA-512:	EDF48BD307B69B238B916F948187ABCBA72F99FBDAF88DC142EEE0D6B43D1A22DB6D1519104EA1A88064E3B983DE8F266A41DE57D82C429218E1721450DA575 D
Malicious:	false
Reputation:	unknown
Preview:	kYK25871oN296Ce735rU8e6e6gM78006092cmk457W9QLCa8W621l6580CmC19qG203y0MY1J9..53UoWtw9R7cFjdSX1wH439p285TI69DcOi36345Q8H0Z E8B2Prm9l34y42W0A..2knJdan8D5n0w1OuPAO7sMQy6FA17..a7T2lq7v45i..oXq84147m5GcAJ0933bR..IbwR538e846pD05FpJ743J164WF6ot970NO714FaPgs52 5e144uz600RW1m11u8ni1Z3mV30004bgR2K57fg8xflp20r785PBw879vU2486ZL344I7i10..i236B25h71e39K1IHSu53WKofVPH8hHv5Z01u9O729x5d08QzL81R1OD bl2zw70e083y72V22O0t688p01B1961f44TK4600fJjc65p..h76d725f204eYBi16QdSn..3X54x..yX1l41q85l6a5U2Yh3332vua3YbaB89UWNlyuk86e46X11X3t24 n4Wm63a7D320sY4PAg36iL1O73l5225s1xb4X0zWa913ERf6RWf88989nhb46j5kG4228S3U5W2uBn9..

C:\Users\user\AppData\Local\Temp\42926996\thpdqkp.pdf	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	510
Entropy (8bit):	5.519377268156367
Encrypted:	false
SSDEEP:	
MD5:	083A56319C90AC888FA43E325AABB387
SHA1:	21FBCD1112593525F29A825863303B98C3C831E2
SHA-256:	9EA121439F1BB0B856A93760A2C99ED8568B30F193D0897F697C64D66541B6F9
SHA-512:	2393BE1E7CEDD27AD07CCF54D3D9161CCDCFD27AABF602857D8B7190C61C6C522350C38C80F6CF3E6DFAD329E20018948D1004997431E3432976D2620EA805
Malicious:	false
Reputation:	unknown
Preview:	4X3QNA8qnst394Z357cI6053ImJvWx1PfzV1bOFe184t21qB59YXu8m03v6pO..D89MY60q27646Q77C198hcEEZ479KC2O64v6m00vwi64tdTSyKJT1t0dHqU2W9p7kNJ 85..r1j19007s0xz91Cp82C95g486..546S4o65rww14M4go0c0c68sJ5D061925w3V5l452h2745LB6G939iwuAH66874lc1eZz61vVf2Oq0EM79efc55Qhg90f029..5 kCTL0klo84jY5pqi298cAL1A1B844u5922Dh821S3596P9RE9Czc42G4966h380bD245EU561J1AB7g6M731LeR5Ro8dXlTJ6lfS324565Y11VZ9Qj0cNC3w501oRSYdO2 Zz94n56629..9P5Y0bFoGUE96G9W8Ce5P78kK0Kk0sy4td2N53la5gA1oydpK4XO01BiR28u3P..59K5n25..r71916779X8p56Fh5wE16Os..2o9bUvl1..

C:\Users\user\AppData\Local\Temp\42926996\ukudgfq.xml	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.473572389146889
Encrypted:	false
SSDEEP:	
MD5:	EFC5299F3B16950EC2D874A4025ADA59
SHA1:	E10316D89FD25B136CA01FF70C955BC82DC39B2D
SHA-256:	C857B3F2573C1E58D33950FD32362921293E1CFEF7F626FA0A5D6BB0F807D17D
SHA-512:	D66128915C587797DC5C0F39982003815AAEA7A80618B3EBC986FA6CE695FAD651A803036E11B375B00AB31505CFFC74E6F8116736589A1E2D054D0A4DC82417
Malicious:	false
Reputation:	unknown
Preview:	5nB17086a7zSkGd9on4FE276cqzE22eL27kx16181C0Pl9vQ76O63iU3V88Z16zx03v59G40q25R6cD7tg5m3fK9TW44d..Co0k8Y0h1J4WwnqF4Hx42z510Fm9506Hnt1 g7HO53ZEDWDmGaPy867b92d0Z8ZP6ic4J15y0f5816d149rd4aL6MeeCO979p33930E37B2np3J1qf4adaROP0ug35dQ0F236N..4MFj3hfl945Z91dkxeD68B0g01ut31 235pMU118u2V9qI6vrh71..242513u8WmS8t7R46L0b564Rg3om7277RicwbE04490R6i972s2hKM15FRFwsIy49G3bF85S373lL855e5VK769O79jwHq007eV44H91xu3 wB6227a7p2c0L3h17lC962s99781BS96v7O64664pe7W6K91pO91c6A08205..1i2B16h12A8nZM1Xk1F048X7r57AddvO9868B175l7aruY17j240H8GM38fe6Ggg95FrQC2..

C:\Users\user\AppData\Local\Temp\42926996\uobpsvii.dat	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	567
Entropy (8bit):	5.367499746051203
Encrypted:	false
SSDEEP:	
MD5:	690BF341B7ECAE1D001856FC5197EC58
SHA1:	30BF5F660B39908575DA05C20EBE7F3D2644B1AF
SHA-256:	C2544CEF2E10F78AAF1849FB8630DDCD3F55BF314F1187BA4EBD580DC45B94E0
SHA-512:	8EA6D62596517C66400CA9BCD0A2B749ECCBDC273FCF83FAFA9ED80878DD69B335A63E8CC0AB4AF48F6BEC03E7379CE33E9CC3C6C073DC8FF57841570CC0F7C
Malicious:	false
Reputation:	unknown
Preview:	nf12iBB5483S5V8b63HY85m8Zemmu29GZkt23UW2o3L63740E14334Z62F99A..98304Tb5X64..3I829jY27d46wCp9Mt2U5j0U10x22wD69r3PK5x9f8e48MZ3i3O9m7G1T7751vcTo1n78fy15160D981240ek08620ZQlITZh27220YQ1..RCI8Gy6g128..2hSV32c1B99Y6382Sui227JA9Bh752x1aF8..7WdA0lxjy8713tEr09T50X14j8d3Ga4EFMU683820193RRb05L0T0353Y5676614gLs2Fqtef9059mm471Ewd7k864y45B86fX3T50O98208fh7999Wh3F8ox3TnSz76n0JaA16G3yA2n7X874z9037hfD55t4668S6..xiO4gfb087AfiQ69j6222L95c888ym497h11snsA4IH89O5w0Ht1rO192362u3uX6B160zTsIZ1N4mTQY..6Y736fcD2ff0u0F222m15t2v681ED3OW9I6C0J631W8nEOeXyj5o5cNe74N2S0022274W1630AI26403160F..

C:\Users\user\AppData\Local\Temp\42926996\urbtqojdqc.jpg	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.496982614180 81
Encrypted:	false
SSDEEP:	
MD5:	5766C274DE702CA72DF424B24CC29E23
SHA1:	39B4D297590E5C68D8260CCB6C842FF66AD27B81
SHA-256:	E1BD1D686B52D783C8320752FF98988948B1C4651F318BFD12AE19E9F5E3F934
SHA-512:	EA774FC1991C9CBC77140DE3F147898606A29D69FF040894CC0AB22B4DC8681D476C6E9EF55FAF2AAF13AF04DF296550AB3D5B87F55A52C6F8AC905478A643C
Malicious:	false
Reputation:	unknown
Preview:	aryaYzMV1x9U07x2t4y4nK2yk6GRZ00422gfoNT6q93E782G03Cr6BfkD67268R3Hqr7V154Oi7964CtblL1uG73r4C61ft9fZC722d7129r84anmP215k2o7xQbcMa3..8LogxVgXFy1063y39CmkByv75BJJF8zSu0DbX8i819525RVDN3o5s0K126otOB49jh90DK8CwVUNH9K48m1N281662950y637M497078Dvh09Fu6fJ..3g5uP535934G04KB2VtNq3TRmwYQ04kH90n55rneNYc65v51b1e776453L8s2B2Ed18655z2hf4ySKB100g3Y8GH2E2SI5j71jEH3VXj7uDBN4..60RC5U9Tj62n7yN819VrN4480lh4BVv1956x80iJOC38J7Auy282t662O0tY9M03199BU6y4K23m5eE75s7g92W50J96e674V24Z45n38Pfiz..FfoYVs1FV6Nby94r2893K4Az1Q90vN2i2c125b07pSz4mi170as70N44R0S..

C:\Users\user\AppData\Local\Temp\42926996\wgvn.ico	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	514
Entropy (8bit):	5.447096286891588
Encrypted:	false
SSDEEP:	
MD5:	CE265A5F7AFC99949B591F0034A9E8E8
SHA1:	D1C0810CEB4EFC47FD096B0F4961F0282100ACCD
SHA-256:	602B62FA3EF9C041EA580C6C4149EB997821EE3BDE455A6416D830E5DD1F3F2F
SHA-512:	B8DCD51303B664BBC1BEA2C9C52B49D8F2E5C42B99C822CA12AEACE5998D634D704B1F6F3FC02C0B188517641E36BE17AE8EA906EA34D681DCCF4D8FF2500C3
Malicious:	false
Reputation:	unknown
Preview:	4r0d985H687657gzTfA142d134qK33t600BqZ1G4t97G73i0bs491e37F4EP8Ga563EWh9iga64489e9n20jLma88H597ur705cj0QRB88Xw060S4C59pdV607S008e48..274fJ1VYk22NGA69xPzg233Q9bqA7M420907OB968Oy9LZQOnC61F1K10p0D92c3103VO3OyHs7m99wvE36389V51oVA0..7Cl3aGZ3V7Tz6z4z12w061316502YSe9A4E2Lr4525nja31sq9392vJ8oXtZ5G1f517i2T1sYz24V3BS4K11X60pAn3V52907490014t5Ib8xjPc76T5r143p32J..G884w34F4za2Dt615888KAY4v89huUh4ic2c904jfdrS9lPQQ8mHWPJ4pk836SeNqwlm1lau410js34n8PvI8k6S487jT2qZ92nvK46t8z793kf6a1P8BEG9EGO7t4OUOK8eqk80..n8412P6639y8POa425srD0..

C:\Users\user\AppData\Local\Temp\42926996\wmlwvee.icm	
Process:	C:\Users\user\Desktop\mzyDSLb1u9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	567
Entropy (8bit):	5.490641957756693

C:\Users\user\AppData\Local\Temp\42926996\wmlwvee.icm	
Encrypted:	false
SSDEEP:	
MD5:	C8160408AD877D37FDC8C63CF6AE7CA5
SHA1:	943E7ACBF7DFBACFA3905EE4DB8EF10775F8D487
SHA-256:	9C9F59702F59B2FE573979814C465EFDBA277F21607B6A36CBF68C936A49B924
SHA-512:	3CC4DE58ABEC68011E66769EAB6FE4088C5B84A3959EE2A536A10E8A7A463BC63E21FA9EFA7C0C00BA85B933D3520D625C3404F1DE69C0CF0DCA8D3BB090F 6E
Malicious:	false
Reputation:	unknown
Preview:	Lth83z375608nR0W2635Lp7fB86ybEs9Ipm6x0JOyiZ83L6f3z615dvO2VtU52Q0F631B89600K67d2w0uk4hF9413in81I1MO9Xp70B..bNWh13aF374J7bKYZnhBjBk4 21K4y54ub3D1982h31sPKP2jps830IEm9k3A6157LIRu3b739MH021G67o82jrYiTF0kf37M..3B066Vju0RuYS562V478p6YbT..3x8wgCk6353Ag27hALe1qzJE..j8o 86VuHbh1BpRpf64BW8fnNbMM22LzSh948F8Q8RS3ZuTb92W96ega1437T1QP6094x78A013u91Fgs98GvP0688xuD30I86GV08pV0k44277RAw1j9C21E89. .3KK77994W653EW49H067C0Sx0l71X9l784N7lKK3681u9w9r4y59n118c14Up24..kVizW7GI4G4308ob2a018Nuy8a4n4rv..9Z8PIq223ocdBP7kEl4h70ks91669w5 1F178KsV7YsFG255uE630Fh0115e381mR702Wz6pj936MgfFS279Z1l..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • 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\tmpD629.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):	1308
Entropy (8bit):	5.103583470672722
Encrypted:	false
SSDEEP:	
MD5:	990B7A403BC76992021F9FA8008904F2
SHA1:	42911051D889BC22633FB4EC99794202975260A8
SHA-256:	2C4DC85A9C8127D7F864AB718245EBC0C5B625C04837AC84E012429E956936EE
SHA-512:	C5FF697E356C84B83D18952A5EDA27E225E649B89F8E43BEE565C6DFC87B12D15D8AD0698C03D6915786120042DABFBCB11493E233B8B3B2742EE8C0C5E4A0 C
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>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpDA12.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

C:\Users\user\AppData\Local\Temp\tmpDA12.tmp	
Encrypted:	false
SSDEEP:	
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
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>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	EF7DF6C58626F07283BD6EF32DD88723
SHA1:	6242A65E99D003E1D488C91B5AB6FEBE93E6B2A1
SHA-256:	3D834F7BE4A8CFE63C334B3F61B7A4DC367EBE223A81CA31D28F85A8D305710A
SHA-512:	B005C37DF518466CC17300F731177D0A595AF5589941C85F25C042F43D87EE43519AD0F650B202094E728ED5F1C7ED5D4E2D20332189AA870284974539DF2EA1
Malicious:	**true**
Reputation:	unknown
Preview:	Y....L.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):	45
Entropy (8bit):	4.324534762707879
Encrypted:	false
SSDEEP:	
MD5:	47370DB2229FE5D11F48C7C4DCF1D3DA
SHA1:	02F189B1593B564FAF6B30C1573A6C4156EEA2B8
SHA-256:	8DA13D1ABADD97A50839C4237102C680E32B80F56B8B594ACC289D603779F743
SHA-512:	0FAE24E7BA758031C3850E96BFB9F93B71E9CDF886A83F83F8B0BB57C76403DA0563E3B9117360968AA279927EB7FB8F77BA48B446635E60D159AFFB96979550
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe

C:\Users\user\temp\osmphj.xml	
Process:	C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	75
Entropy (8bit):	4.876817484945778
Encrypted:	false
SSDEEP:	
MD5:	4D73E5FEE5042E52A2E24A33B2E2A030
SHA1:	699961AE1A3D3C0ABA1D7C5D00A00688B5C30A70
SHA-256:	A214B4565266B8E2758372703467765341D9A972D9E602DECF593A50E7827096
SHA-512:	31E6A516A9B6681626042B11BDE7A07848955189E22D0465B7D9892776BDF1563F2A5F48CD2D990642354BD375AF298B03AD87A68B483E04F0888886122AA34B
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%temp%..Key=Chrome..Dir3ctory=42926996..ExE_c=mssvgt.pif..

\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:	
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
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):	7.837252000939896
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:	mzyDSLb1u9.exe
File size:	1105214
MD5:	922bbf421cd0c9b155f45388db7c8718
SHA1:	993cd3bc36c7d903846cf9ee4fb1e8e01dec4947
SHA256:	1bf63394fcf232d3a303d17df87252e2f47c43205edadc99ed15a50c9e193ebc
SHA512:	1af0064f0524fd93ee173467b490a407e3d4f43ce97a0d0fa599964f4ad787b302155b3e0d859f8fb2dbaacc99ab399cd7b368011d29f61e6981f05396ec3bf9
SSDEEP:	24576:BAOcZpJ/cpMh+itmP6UvJmoSSvVUYG4Y7:bLRit6YoSyVUYG4I
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y../../y..#...&...,...._....._..'...._f.'...._..'..

File Icon

Icon Hash:	1ab8e6e663d6c77a

Static PE Info

General

Entrypoint:	0x41e1f9
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5E7C7DC7 [Thu Mar 26 10:02:47 2020 UTC]

General

TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Rich Headers

Data Directories

Sections

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

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 05:17:11.742209911 CEST	192.168.2.4	8.8.8.8	0xf73b	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 05:17:18.392772913 CEST	192.168.2.4	8.8.8.8	0xd127	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jul 22, 2021 05:17:25.090871096 CEST	192.168.2.4	8.8.8.8	0x8bae	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:10.076064110 CEST	192.168.2.4	8.8.8.8	0x25a	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:15.936439991 CEST	192.168.2.4	8.8.8.8	0x8f60	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:22.325500965 CEST	192.168.2.4	8.8.8.8	0x27ed	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 05:17:11.804403067 CEST	8.8.8.8	192.168.2.4	0xf73b	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Jul 22, 2021 05:17:18.451010942 CEST	8.8.8.8	192.168.2.4	0xd127	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Jul 22, 2021 05:17:25.148137093 CEST	8.8.8.8	192.168.2.4	0x8bae	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:10.132956028 CEST	8.8.8.8	192.168.2.4	0x25a	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:15.994916916 CEST	8.8.8.8	192.168.2.4	0x8f60	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Jul 22, 2021 05:18:22.385513067 CEST	8.8.8.8	192.168.2.4	0x27ed	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: mzyDSLb1u9.exe PID: 6848 Parent PID: 5976

General

Start time:	05:16:49
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\mzyDSLb1u9.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\mzyDSLb1u9.exe'
Imagebase:	0x13c0000
File size:	1105214 bytes
MD5 hash:	922BBF421CD0C9B155F45388DB7C8718
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: mssvgt.pif PID: 7104 Parent PID: 6848

General

Start time:	05:16:56
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif' nlcno.gge
Imagebase:	0xa90000
File size:	855280 bytes
MD5 hash:	7C81E999E91D1D0F772010DFA4C34923
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: 00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.662507687.00000000044F5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.659920002.00000000044F5000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.659920002.00000000044F5000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.659920002.00000000044F5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.662369446.0000000004539000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.662369446.0000000004539000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.662369446.0000000004539000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.660958539.0000000003724000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.660958539.0000000003724000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.660958539.0000000003724000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.660913492.0000000003705000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.660913492.0000000003705000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.660913492.0000000003705000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.659777206.0000000004476000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.659777206.0000000004476000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.659777206.0000000004476000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.659743510.00000000044F5000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.659743510.00000000044F5000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.659743510.00000000044F5000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.662616297.00000000044C1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.662616297.00000000044C1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.662616297.00000000044C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.659811723.00000000044C1000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.659811723.00000000044C1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.659811723.00000000044C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.661010431.0000000003727000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.661010431.0000000003727000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.661010431.0000000003727000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.662013671.0000000004441000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.662013671.0000000004441000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.662013671.0000000004441000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.661068688.0000000004538000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.661068688.0000000004538000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.661068688.0000000004538000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.662163487.00000000049D2000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.662163487.00000000049D2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.662163487.00000000049D2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.661829199.0000000004538000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.661829199.0000000004538000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.661829199.0000000004538000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.660075291.0000000004538000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.660075291.0000000004538000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000003.660075291.0000000004538000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.661660900.0000000004475000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.661660900.0000000004475000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.661660900.0000000004475000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.659878466.0000000004441000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.659878466.0000000004441000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.659878466.0000000004441000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.660813067.0000000004538000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.660813067.0000000004538000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.660813067.0000000004538000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000003.660033291.000000000456E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000003.660033291.000000000456E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000003.660033291.000000000456E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 23%, Metadefender, Browse • Detection: 29%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: RegSvcs.exe PID: 4476 Parent PID: 7104

General

Start time:	05:17:01
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x3c0000
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: 00000006.00000002.905012001.0000000005740000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.905012001.0000000005740000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.901251206.0000000000792000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.901251206.0000000000792000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.901251206.0000000000792000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.905032778.0000000005750000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.905032778.0000000005750000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.902994074.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.902994074.0000000003CA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.905317731.0000000006460000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.905317731.0000000006460000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.905317731.0000000006460000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5768 Parent PID: 4476

General

Start time:	05:17:07
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD629.tmp'
Imagebase:	0x30000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5748 Parent PID: 5768

General

Start time:	05:17:08
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6760 Parent PID: 4476

General

Start time:	05:17:08
Start date:	22/07/2021
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\tmpDA12.tmp'
Imagebase:	0x30000
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

Show Windows behavior

File Read

Analysis Process: mssvgt.pif PID: 984 Parent PID: 3424

General

Start time:	05:17:09
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\42926996\mssvgt.pif' C:\Users\user\AppData\Local\Temp\42926996\nlcno.gge
Imagebase:	0xa90000
File size:	855280 bytes
MD5 hash:	7C81E999E91D1D0F772010DFA4C34923
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: 0000000A.00000003.692566467.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.692566467.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.692566467.0000000003D51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.689820753.0000000003D86000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.689820753.0000000003D86000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.689820753.0000000003D86000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690180075.0000000003E7E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690180075.0000000003E7E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690180075.0000000003E7E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690030414.0000000003D85000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690030414.0000000003D85000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690030414.0000000003D85000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.692643816.0000000003E49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.692643816.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.692643816.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.691361381.0000000003E48000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.691361381.0000000003E48000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.691361381.0000000003E48000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690095645.0000000003E49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690095645.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690095645.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.691863501.0000000003D85000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.691863501.0000000003D85000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.691863501.0000000003D85000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.689852195.0000000003DD1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.689852195.0000000003DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.689852195.0000000003DD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.692788641.0000000003E05000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.692788641.0000000003E05000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.692788641.0000000003E05000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690118955.0000000003E49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690118955.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690118955.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.692903177.0000000003DD1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.692903177.0000000003DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.692903177.0000000003DD1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690447296.0000000003EB1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690447296.0000000003EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690447296.0000000003EB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.689909094.0000000003D51000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.689909094.0000000003D51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.689909094.0000000003D51000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690354835.0000000003E48000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690354835.0000000003E48000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690354835.0000000003E48000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.690069103.0000000003E48000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.690069103.0000000003E48000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.690069103.0000000003E48000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.689784104.0000000003E05000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.689784104.0000000003E05000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.689784104.0000000003E05000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000003.692445105.0000000003E48000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000003.692445105.0000000003E48000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.692445105.0000000003E48000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6452 Parent PID: 6760

General

Start time:	05:17:09
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 768 Parent PID: 968

General

Start time:	05:17:10
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0xbd0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4864 Parent PID: 768

General

Start time:	05:17:10
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: dhcpmon.exe PID: 6576 Parent PID: 968

General

Start time:	05:17:10
Start date:	22/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x2b0000
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%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6500 Parent PID: 6576

General

Start time:	05:17:11
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6744 Parent PID: 984

General

Start time:	05:17:15
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x630000
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: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.715341016.0000000002F91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.715341016.0000000002F91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.714424502.0000000000A02000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.714424502.0000000000A02000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.714424502.0000000000A02000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.715442161.0000000003F99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.715442161.0000000003F99000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: wscript.exe PID: 6996 Parent PID: 3424

General

Start time:	05:17:17
Start date:	22/07/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\42926996\Update.vbs'
Imagebase:	0x7ff780f70000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: dhcpmon.exe PID: 7048 Parent PID: 3424

General

Start time:	05:17:26
Start date:	22/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x1c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6160 Parent PID: 7048

General

Start time:	05:17:26
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis