ID: 501775
Sample Name:
KRSEL0000056286.JPG.scr
Cookbook: default.jbs
Time: 08:48:09
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

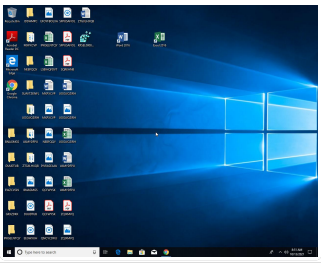
Windows Analysis Report KRSEL0000056286.JPG.scr

Overview

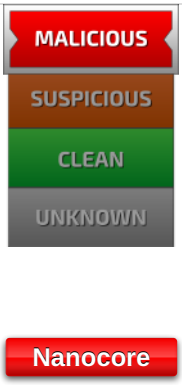
General Information

Sample Name:	KRSEL0000056286.JPG.scr (renamed file extension from scr to exe)
Analysis ID:	501775
MD5:	d6f040b4d7d217b.
SHA1:	8ed8beaceddf8e8.
SHA256:	940ad66c876976..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



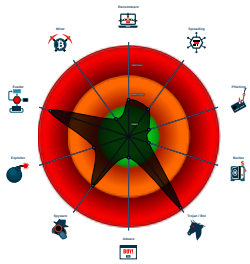
Nanocore

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

Signatures

- Sigma detected: NanoCore
- Detected Nanocore Rat
- Yara detected AntiVM autoit script
- Yara detected Nanocore RAT
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sigma detected: Bad Opsec Default…
- Connects to many ports of the same…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Uses an obfuscated file name to hid…

Classification



Process Tree

- **System is w10x64**
- KRSEL0000056286.JPG.exe (PID: 6976 cmdline: 'C:\Users\user\Desktop\KRSEL0000056286.JPG.exe' MD5: D6F040B4D7D217B8525DFF843FEBA635)
  - upstsdssm.pif (PID: 6032 cmdline: 'C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif' sqbr.wlw MD5: 8E699954F6B5D64683412CC560938507)
    - RegSvcs.exe (PID: 6404 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
      - schtasks.exe (PID: 5036 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp2BE4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 5312 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2F02.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5484 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1372 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5108 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 3280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- upstsdssm.pif (PID: 3296 cmdline: 'C:\Users\user\AppData\Local\Temp\33911166\UPSTSD~1.PIF' C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw MD5: 8E699954F6B5D64683412CC560938507)
  - RegSvcs.exe (PID: 7128 cmdline: C:\Users\user\AppData\Local\Temp\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- wscript.exe (PID: 6200 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\33911166\Update.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- dhcpmon.exe (PID: 6440 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 2600 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
0000000F.00000003.720524354.000000000465 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9dd:$x1: NanoCore.ClientPluginHost • 0xfa1a:$x2: IClientNetworkHost • 0x1354d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000003.720524354.000000000465 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000003.720524354.000000000465 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf745:$a: NanoCore • 0xf755:$a: NanoCore • 0xf989:$a: NanoCore • 0xf99d:$a: NanoCore • 0xf9dd:$a: NanoCore • 0xf7a4:$b: ClientPlugin • 0xf9a6:$b: ClientPlugin • 0xf9e6:$b: ClientPlugin • 0xf8cb:$c: ProjectData • 0x102d2:$d: DESCrypto • 0x17c9e:$e: KeepAlive • 0x15c8c:$g: LogClientMessage • 0x11e87:$i: get_Connected • 0x10608:$j: #=q • 0x10638:$j: #=q • 0x10654:$j: #=q • 0x10684:$j: #=q • 0x106a0:$j: #=q • 0x106bc:$j: #=q • 0x106ec:$j: #=q • 0x10708:$j: #=q
00000002.00000003.688014335.0000000004B6 3000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf9fd:$x1: NanoCore.ClientPluginHost • 0x44205:$x1: NanoCore.ClientPluginHost • 0xfa3a:$x2: IClientNetworkHost • 0x44242:$x2: IClientNetworkHost • 0x1356d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47d75:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000003.688014335.0000000004B6 3000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 118 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.3723f8c.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40a6:$x1: NanoCore.ClientPluginHost
5.2.RegSvcs.exe.3723f8c.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x40a6:$x2: NanoCore.ClientPluginHost • 0x4184:$s4: PipeCreated • 0x40c0:$s5: IClientLoggingHost
18.2.RegSvcs.exe.2f79650.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x42a6:$x1: NanoCore.ClientPluginHost
18.2.RegSvcs.exe.2f79650.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x42a6:$x2: NanoCore.ClientPluginHost • 0x4384:$s4: PipeCreated • 0x42c0:$s5: IClientLoggingHost
18.2.RegSvcs.exe.2f79650.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x66a6:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 112 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

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:

Yara detected Nanocore RAT

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Networking:

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

Copyright Joe Security LLC 2021

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

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)

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

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

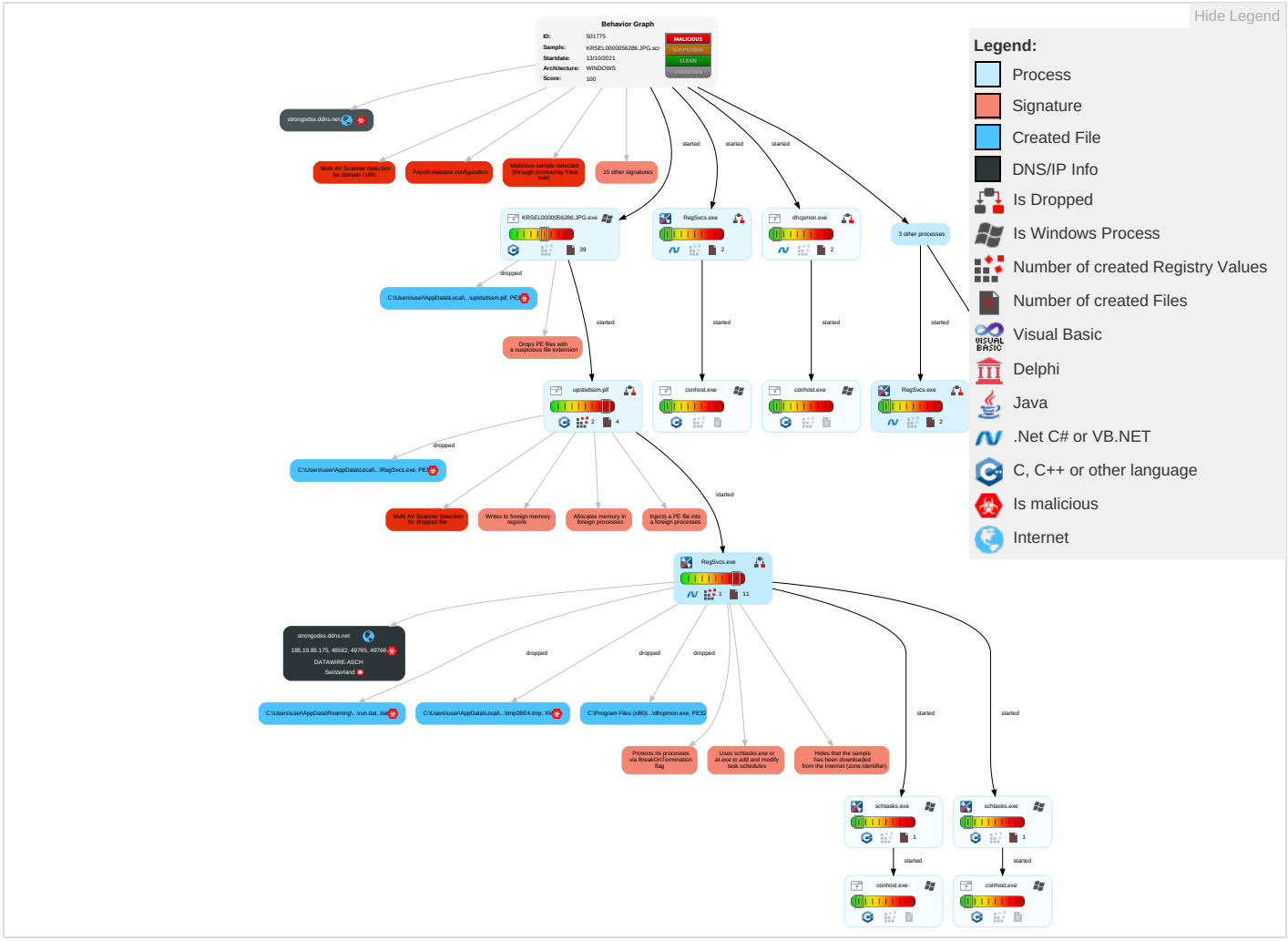
Yara detected Nanocore RAT

Copyright Joe Security LLC 2021

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com 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
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 1 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 2 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

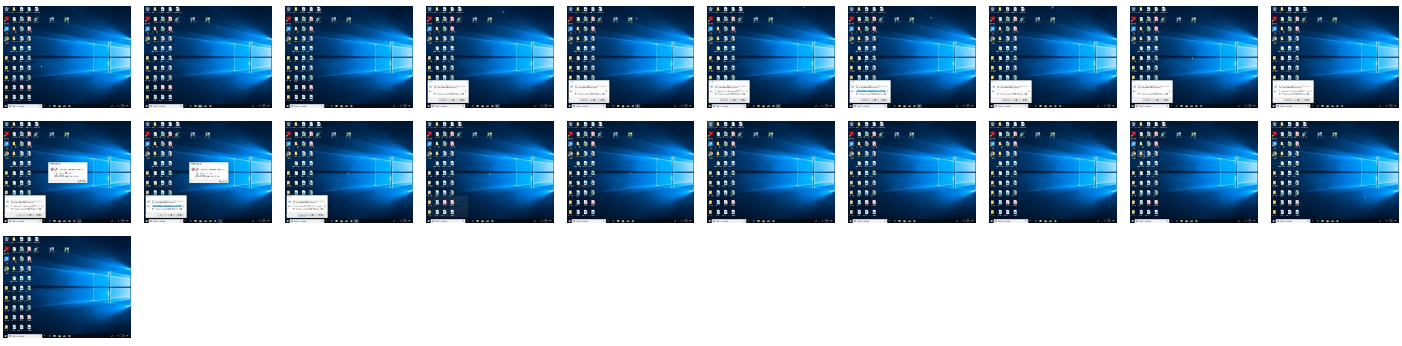
Behavior Graph



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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
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\33911166\upstsdssm.pif	32%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.1300000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.RegSvcs.exe.6fb0000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.RegSvcs.exe.9b0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
strongodss.ddns.net	13%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://secure.globalsign.net/cacert/PrimObject.crt0	0%	URL Reputation	safe	
185.19.85.175	4%	Virustotal		Browse
185.19.85.175	0%	Avira URL Cloud	safe	
http://go.microsoft.c	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://go.micU	0%	Avira URL Cloud	safe	
http://www.globalsign.net/repository/0	0%	URL Reputation	safe	
strongodss.ddns.net	0%	Avira URL Cloud	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	true	• 13%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.19.85.175	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• 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	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501775
Start date:	13.10.2021
Start time:	08:48:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KRSEL0000056286.JPG.scr (renamed file extension from scr to 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:	33
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

Copyright Joe Security LLC 2021

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@21/45@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.6% (good quality ratio 23.4%) • Quality average: 75.1% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:49:17	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run Chrome C:\Users\user\AppData\Local\Temp\33911166\UPSTSD~1.PIF C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw
08:49:22	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\RegSvcs.exe" s>$(Arg0)
08:49:23	API Interceptor	902x Sleep call for process: RegSvcs.exe modified
08:49:25	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:49:26	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run AutoUpdate C:\Users\user\AppData\Local\Temp\33911166\Update.vbs
08:49:34	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.19.85.175	dAkJsQr7A9.exe	Get hash	malicious	Browse	
	dUzAkYsvl8.exe	Get hash	malicious	Browse	
	voo7b2BBq6.exe	Get hash	malicious	Browse	
	xmsGPH324z.exe	Get hash	malicious	Browse	
	dVWsghK4Aj.exe	Get hash	malicious	Browse	
	2E9xpfvD2O.exe	Get hash	malicious	Browse	
	uF74GlbXPc.exe	Get hash	malicious	Browse	
	jFjTeUfek3.exe	Get hash	malicious	Browse	
	Q7DYDgQhKp.exe	Get hash	malicious	Browse	
	dlDGpRFSEo.exe	Get hash	malicious	Browse	
	s8uDlcv0XT.exe	Get hash	malicious	Browse	
	LRlhF3NgEM.exe	Get hash	malicious	Browse	
	iCtAiCA2Eg.exe	Get hash	malicious	Browse	
	STC8924578611.JPG.exe	Get hash	malicious	Browse	
	BK7489583093410.JPG.exe	Get hash	malicious	Browse	
	FFXML21050419.exe	Get hash	malicious	Browse	
	mzyDSLb1u9.exe	Get hash	malicious	Browse	
	Doc.202107028.exe	Get hash	malicious	Browse	
	Shipping#docs.exe	Get hash	malicious	Browse	
	DOEN100000597.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	dAkJsQr7A9.exe	Get hash	malicious	Browse	• 185.19.85.175

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dUzAkYsvl8.exe	Get hash	malicious	Browse	• 197.210.84.227
	voo7b2BBq6.exe	Get hash	malicious	Browse	• 105.112.32.231
	xmsGPH324z.exe	Get hash	malicious	Browse	• 105.112.32.231
	dVWsghK4Aj.exe	Get hash	malicious	Browse	• 105.112.32.231
	s8uDIcv0XT.exe	Get hash	malicious	Browse	• 185.19.85.175
	LRlhF3NgEM.exe	Get hash	malicious	Browse	• 105.112.228.76
	iCtAiCA2Eg.exe	Get hash	malicious	Browse	• 105.112.228.76
	STC8924578611.JPG.exe	Get hash	malicious	Browse	• 105.112.98.218
	BK7489583093410.JPG.exe	Get hash	malicious	Browse	• 185.19.85.175
	FFXML21050419.exe	Get hash	malicious	Browse	• 185.19.85.175
	mzyDSLb1u9.exe	Get hash	malicious	Browse	• 185.19.85.175
	Doc.202107028.exe	Get hash	malicious	Browse	• 185.19.85.175
	Shipping#docs.exe	Get hash	malicious	Browse	• 185.19.85.175
	DOEN100000597.exe	Get hash	malicious	Browse	• 185.19.85.175

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATAWIRE-ASCH	Quotation Request.pdf.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 185.19.85.137
	MT103 10.11.pdf.exe	Get hash	malicious	Browse	• 185.19.85.136
	dAkJsQr7A9.exe	Get hash	malicious	Browse	• 185.19.85.175
	GIV PO 00254.xls.exe	Get hash	malicious	Browse	• 185.19.85.136
	dUzAkYsvl8.exe	Get hash	malicious	Browse	• 185.19.85.175
	BL & INVOICE.exe	Get hash	malicious	Browse	• 185.19.85.171
	Routing Details.vbs	Get hash	malicious	Browse	• 185.19.85.170
	Nueva orden #7624.xls.exe	Get hash	malicious	Browse	• 185.19.85.136
	voo7b2BBq6.exe	Get hash	malicious	Browse	• 185.19.85.175
	xmsGPH324z.exe	Get hash	malicious	Browse	• 185.19.85.175
	dVWsghK4Aj.exe	Get hash	malicious	Browse	• 185.19.85.175
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	ShippingDocs.exe	Get hash	malicious	Browse	• 185.19.85.171
	2E9xpfvD2O.exe	Get hash	malicious	Browse	• 185.19.85.175
	Proof of payment.jpg.scr.exe	Get hash	malicious	Browse	• 185.19.85.137
	uF74GlbXPc.exe	Get hash	malicious	Browse	• 185.19.85.175
	jFjTeUfek3.exe	Get hash	malicious	Browse	• 185.19.85.175
	Q7DYDgQhKp.exe	Get hash	malicious	Browse	• 185.19.85.175

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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Malicious:	false
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\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
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\33911166\Update.vbs	
Process:	C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif
File Type:	ASCII text, with no line terminators
Category:	modified
Size (bytes):	143
Entropy (8bit):	5.044581587746334
Encrypted:	false
SSDEEP:	3:FER/n0eFH5Ot+kiE2J5xAIdcET6WGbUouZDt+kiE2J5xAIdcETpHu0:FER/lFHIwkn23fdcE+wouNwkn23fdcEX
MD5:	BED3F060611547B9D81952389AC2B088
SHA1:	E616E3AA0EA8E297A2602242E13A3477681287A2
SHA-256:	B7A9F2DD4089C938788C6051D903B01E0C2AED713513E4DFB134FE5C91949255
SHA-512:	2846E849DFB88B360CAD6B8278AC6817F9930CD45F0D64EF67EBD1F187A1DA87B9FC2FA4CD9BD8728FBE2D822F15481649F3576F58DDA061AE1A22428A038A0
Malicious:	false
Reputation:	unknown
Preview:	CreateObject("WScript.Shell").Run "C:\Users\user\AppData\Local\Temp\33911166\UPSTSD~1.PIF C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw"

C:\Users\user\AppData\Local\Temp\33911166\acdtfoidpw.exe	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	530

C:\Users\user\AppData\Local\Temp\33911166\acdtfoidpw.exe	
Entropy (8bit):	5.482370918685384
Encrypted:	false
SSDEEP:	12:c+uhAYRz7mGknY23TSWKm9VjOSK74jh51Nd7DQAycx3/:buhRz7GY21Km9tKcjh5eAF
MD5:	EFAC1E031262E2FD22D77BE15E450C43
SHA1:	BBF4B853791A783536E3BC4CDFB81493210A50FF
SHA-256:	883906DBD80E79B4B55A2F49D42E19B816A8C37822918923875C57A9D2BB3F34
SHA-512:	D8680BABFC3ACD23ABEE5B4928C79C2BFCD00ABC6DF736D96BDC0E9644D530747981311F8280E585E351BDAA0BDAE2ED62D8FE8E33DA748626A5AB7CB813116A
Malicious:	false
Reputation:	unknown
Preview:	8K7X17O1885c..j1KAMNUl252X1sHZ51..u7it910lQO9dAt9456Ev719K37eZ7720306ZXpvVZ991pQ3Ev0c7KM26k8P6uE4spLS30tk01yl15..i889Dogm41v1ZfL04ri56R3L4sT27C377C571SH6xR0F057y6OE30Ng9xkC7eE57VHVy80f5eL7295pd9..J995x8CHo0wCK145p7J22V69dor0Hb38o0T53ZX01D5KB7E9X4F30tu4lS0M..I1aR0d2997oWYEn5BL23n487H98508LP0J1DchsD06jqM945NM931e3Z26ZG0mx62PINc91kj773tYl5849l818a728d19P2s2rvj1do3vk16Yl815633m135GrdN7F04r..71tjt8392h49FHXM3Ra31E9b43UrK78NRZ9pb8ts14473M66t8PyP5189gbia01YUH0UG9SO21517qs8vFuGA3o2c8246i768x7n8h8i83107LSz950m572o4yAy8r85BZxgDGY38p..

C:\Users\user\AppData\Local\Temp\33911166\bbslmxx.mp3	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	508
Entropy (8bit):	5.503691278659062
Encrypted:	false
SSDEEP:	12:zRsYoVZfEJIX/USsdRdy5pX29Ib5vimc1Q62U8dz8wYIPpyTVRyuZQh:9snVSJqcc5pX2eb5viw7dz83IRyTdZQh
MD5:	B9BE27AD54D7859E5865D3F2A9511ED4
SHA1:	3DCEB86073B93C870191B8272A158F1E45E68246
SHA-256:	F53C1F020873EC6243B519A39A8AD0B8FB46AD23536847BB3A82F3B68BC3EF14
SHA-512:	830EDF52B04C1894D00C4CB39C879BD6559031C1B3B2B01187BAA1A34D23CE369336A09AAE3A19D69C41BC36256CFE00B7B246AC682A52351A363B9FE023296
Malicious:	false
Reputation:	unknown
Preview:	m92sa69qA70jT794Y9U8gl2U5QJrk87y2c34q95QZKCWfi60X736A4FB603S9E20dzNLa..9R0Y55m2ui46Tlo6g9F000924mJt6ED1HMFlW2p0171n29b3iWwlS7i84NV8ac031Pb4Eyf55g4Bj77kxTw2L519R1cT7054r87Z9g41292w59v563C5T9N03a0N0692926827G1Qa846T8750v2x9N1M5BlDGci..6Z3T719h14YM48sa8261iJ3nBi48s606P2NJuPC990B55UU0331HEk2kH44Lar253Mt7BY2st2O55NPVtOx7I89..il9jcg1Zu2Wz3358j09b441CRdfHL2aH8tyOO3E8ab29V361yL94O8nw9XBa54253U6SMs1263jhJj530oDPxYWClgP699ZB3Q1W6Q79WC0JmT4424L0u41Y7WDrYxa42e6T975l273Q8D6vA5f3XBz3F61..71W8SmKH41i6TLfMhc71LwUrMr7..

C:\Users\user\AppData\Local\Temp\33911166\blmcuvi.bin	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	658
Entropy (8bit):	5.467503965290551
Encrypted:	false
SSDEEP:	12:+cfeRsKimVAe1UNHkAEaBHuLycVA/2hMfX+SS/cF+pHXAG:jfeRsKLBrK0yczhMvjSUF+JXB
MD5:	07B5B11DD6CFDF00045139785AB35285
SHA1:	EAEF5689C59036D435A492A918060F4219C3DA97
SHA-256:	81D5A96885A8D2CEC546D2E35259A79F77B3EFCC094DD69A17E7C838B50D431D
SHA-512:	87DC099983D80B18FA2598AC5B0995E17D699669C042DD8F8C13F0C9250DDC955ECBE2AF68A83FFA3E53EC5A89CE2F532B733C11E7A2AC5723E0C43BA742981
Malicious:	false
Reputation:	unknown
Preview:	HJR5W1vkK1FO27gUC3Ex90xV6PO85..6E044l1246U7740FAdPbd34679GDz72a9N32636a13h4Jqoo342F0..li2lY041680r7567tl56s7Ft3VzmZ347JE40QQ1r9gd7Rn0R0B4qd19OLyyS377d90r61w58bw..9LF7q8c251VO1s2YvzSX33169m350Q7w14fZ05Ibnm6a84EUC8M71n0CEaq9U3926c45w9C0I56x3b3P5PWK6qOA..3XL5eGsn0cw6n3H7f5585oM82d3002V3560740L543nPVdFK77090g8A15y27N9WnBY1Ot8J2X7M9w8951x7M3Y28D9Dm8WH1dgh9gZF124PVkCf558C7T7768yA7l6..5490qz70DQ6J..VjEN33117T10784F84y342DFd3m473P374bfHe7561b09P09o2J0275aq5DN0ee792x7ab1884Su71D68A93uhYTRN3786eSb23Ed..98V3408q1VCNDo6l58Jqrv80YO9R7nF92vsA5899yb6881ecYJT3x80yyl2p12o5269G8Rp8W42O2L19338GV34H4m2Ti5Ol846kKi3A1Ig5115RTsJ2p9S7043b6GPCKD31UK86l6L2v968341rHeEh5ph1lf..

C:\Users\user\AppData\Local\Temp\33911166\efupmjbj.log	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	601
Entropy (8bit):	5.452469277963245
Encrypted:	false
SSDEEP:	12:H25YoBjHv8bI4Cs9bSURlMj88Zd8jAGRWutiQ/XGc3yThf:aYwjPqRRSwe88TuA0WXkR3yThf
MD5:	B7344FC88743A3363933C407A6CFB8A3

C:\Users\user\AppData\Local\Temp\33911166\efupmjbj.log	
SHA1:	8B6A0AF17F9D47F2808D18E0BB16070F70546BA1
SHA-256:	D9B344EFA5CC19DF933DE017C2310C1D4F4B76FBCC75CB47C00AB1F269C8CD35
SHA-512:	CACCAA4968B6FB795F697722481234016E8BB214B24186A75989E4F4E01E5EA75A6477A4CEF0C156BE611BF1728134C6E50AE3A736F4C2B6D0E1EAA974FD424
Malicious:	false
Reputation:	unknown
Preview:	3Ak222AS325P254YMKr2u8FTKpISJb43G2H7Uyh82U4359eCaR5l43395p7K6G7Q90nl99gj9x12q821G88q27W111W4uz96eib9eTy834E09E24..GK76e30iv97m7586 u2deq8GJK85NJ67sw6525U70580lPCB03WZ0s4OC1n539RpwMY0Y7p99R654Bjdxs81s454xj1K2765J9b37t3Zs..e0avgh4G4jB1d27E3eyewv7M0Q64qKYG277g130u 02mrEZZbZf57297ic9N8kWs15T74497Gn..p41t3gE84y9G07J1173CDC7uSzu0185l3DLf6k1l83gi8I238myo3A500l7179P6578T27L..90V03i1N0Q3JQ0355x72j2 w6L7jy1r7n742nvB74Sd9d5NY9IoaW2aP6C4491W9D0t0676Qv8q6x811Rj0s8MX1w88m126sJW208QLOJ22Q6RDiDwNAw50..Q269PO39L878R2989Z0V3n 4Ks95H2Y4v1fQ4J8Cx8G17X5l950V3i8rg485eTh0W531uCax353Zh98PpNYYjh1j61KfOY420g775qb45t316656..

C:\Users\user\AppData\Local\Temp\33911166\egccradum.rpq	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	430098
Entropy (8bit):	4.00001165117451
Encrypted:	false
SSDEEP:	6144:2pppWZDs2KIfh1c5iCuUtz1zdH6tL7GdFfwT2dtk5:2pCffhwJzhtaUs2dw
MD5:	8A7C869AD69DD7EC00AA3FBD4AFA5DA0
SHA1:	4760A47040FC0F93BE6CCC80261DB6BC31700E55
SHA-256:	22B4837BB2B0E795AEFD607EFE9175CA7EA6DA100300CB9277EA84D9CD19D3D3
SHA-512:	54FBB02F7537692784FC461ACDA2DA8AA831294838FEF5602FF5E401F09B8084D369B06045F3EF187391AFCE8BF346C9896B3565EE8337CE21C0AE6B7B72118F
Malicious:	false
Reputation:	unknown
Preview:	5EBE37A26E72B0F566EC598D610DCFE028EE1EB18ABB8C63C81F551428447E1532D3A2FCD533D167A4DDEFA36CFB533FFD5CED53DFB89B32AA88E8A0 1BC457CD4F61C6E244BD5D51C7BF57AE7A315233E964B13BA190EF80921BEE462AE7869D2B8D8CAA1EE5AF2F39D3A784C9C563FF584079871EFEFC0A E1C55D838BD374336CE900F9CD97CC0DDFB67275243AD6AED9BA0689F5133CA5A1287FF023CD28D8B1C2DD8B3E182BF99919ACBB110E139A623295E3 FCE01B4F7EDA0E677AB0CA947C55F532247ADC2EB92F59BF13479D296E350A239F98063B833D0D1F5CC4D913AFD81D127D4F31ACA64B4B3861946012 4ABAB4E311F847EEBBB4E4D3FBC07C241B1E668208AB6D9B2C18C259A025BAB1923D4B242AA293245E0BEEF1188418534E05B6D33012617C2C28BD0C 54CDD2E0213F47AFE512DEF40421419C825C1409D276453ACFB60BEC24835BA0BD70B03A0DE4BB7F0086054EEB4B2C2B4A6CA30217645DDFBCB8BC1C D5E572340B80F24B1A9D98CCA5EBF7EA6B68029DA41392209F9C187965521ABF77EC71F3757AD01F292EE49D664C06C6D15701F5A31E010CB13E0C4A 7A637F5A6A680A43600404E8BC796B59A7B80C1FF843923E56E40DD80F311648F625B3997BF69FA582F2B42BAADD3CE8BB70CF102243BF093B4C2A0B DDE2748820FB20045E67A5244022D4B37D74AF7E

C:\Users\user\AppData\Local\Temp\33911166\eiad.jpg	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	633
Entropy (8bit):	5.431173825499616
Encrypted:	false
SSDEEP:	12:xCdMhs1pRVwhU12wSxdRS6Toei5iaUc22s2dHVT4GvoH+EVl:QGaDVP12wQdRS6TAQ2s2Ee8l
MD5:	E8D22557BB5F6603C532C98865CCD5A9
SHA1:	636DC732C27BBDB8B629F8BCBB57274F7BDB63B0
SHA-256:	5F494B2BA3C5700F128E56495D533105A8D371F443C7CB45BCEFB90AA927C3C2
SHA-512:	0329FDCD8373367637370A36A3A6A50E1B2409CD48F1FBB2CECCB9A217FAD0B3AD92B0863B857E53956ABBB295D9B33B353F123228E91501EF89E7DE34A0D2A 3
Malicious:	false
Reputation:	unknown
Preview:	832b8X228176..7U04w6oX6O4FI9g8a3S8q27Y69r645i7vz9Z1466HNZYyg11B76F5IpXEL86R6V655n9993dVM6d2TY2pO9Qg94sRF0857Z2355QB6IV726l91638q54 698gz8SJpXX14n3A533P4..Exkd1dV37Lz3s8lYnk2p8P99415NG19Ac85Q99JW260Kctm476VQ664s7eG456WhHAU96901713896rs7Uq25p50mE47K5Zu4aYo395Llo4 ..q4ae26R35s8wT1bqa5600l33zL2fQK2K9MJeB495G71y1MCV76qc064y3w7ByO8m3jz7q86Yu90RKB324X7T61..5X5a3Q9R9jk44n812AC50ETe8ZqWg4Z96IzT1T5m l86n5A6BJRlbThjYh5V49Opp2e8Ewi65865F5Z5ZDFW..6m25986k81127009u8S6iB5IO7cuF9y6SL977578c..dPo9U66342O44G38A9Uv07iXgX02l067P2B1x13E2N g624671r97heI6rO3725a01v9ir77p21Y9UzW371gJ04zjn4nS1zp3D73B28lw2k30136Gf7lz97935556651d4b9OO048xp5IiX0b75pTSZGzp..

C:\Users\user\AppData\Local\Temp\33911166\fagbcbo.ico	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	533
Entropy (8bit):	5.432805479294794
Encrypted:	false
SSDEEP:	12:ubljeOfOYdnKCZLVoIzlbV6wwVFT0jC7MqVY3zdZAff82jVMXUDn:ubEcTgwwVV0mMqVSsE2jIUD
MD5:	55CD69436FA392FC74563FEA94C0D9CC
SHA1:	A393C02EA3EE453274CF25F96404236A3255EA1C
SHA-256:	D9535DE1EA8CA1E086C374620D483E5B1253C2589B62D80480FAC4A2129BAD38

C:\Users\user\AppData\Local\Temp\33911166\fagbcbo.ico	
SHA-512:	A79E93E2681062A18B64903EF2DF82FE7B4C3B213851B5EEBB21F328DA59A96327EF41AD1C5EEC61B77FC11765895E11A35810C4EB9DC765FB16E71050A7D0D
Malicious:	false
Reputation:	unknown
Preview:	tZA8aNPQfB91vxsm3Y89E2wN9779f9e86j1tC7594YH9d9ZUVn1Yc2SzK429Nl9n552TpVo9385Wa90BC6b76R777RiNBgE8Pe4b96n23943c12B1E0271mxB3pykET8d4 691563433DhI9oxb0aH2HrnFH8vz..81652031E1o3h8Ww675x9HH476B7w73791242ix9252r2501d070vjM49h141t0ls8uAa8x589bpLg1662wg9KY95Q..U829BoP4 y3KfNkCT3f8500570646Y..8aT188E1Jkpefq0x552o336gA1793icj25LXg730Ue2Qk3UMzkMNp2vfS23..i2bv2Kj3FMib610C36sqy3100r17x9eX7L32fm0q60..6Kt15zm0xz1f 83v..Q9o20667e8Ug0226..0934L8f9MG8878w95Ax3mgU0mqlv806508Z52136S5c6K91Z2Oe9196Y48M24kbEXCwdmoii7W945970n1HDEx3RQv9YU621kekbX052A4Y 3..

C:\Users\user\AppData\Local\Temp\33911166\ftsqid.ppt	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	604
Entropy (8bit):	5.465100475991333
Encrypted:	false
SSDEEP:	12:WnTt5dLVroBrW6drqhDr/yim81cmmzIpr4UCQ5mVqcepIm1XYr:WnpBd6hSDzytDm5r4UCZVqcepImFYr
MD5:	EF740CD570DD4766D6AE0A4C462E4C86
SHA1:	6EBEA042B020CA9E4A76ED1B7D528BA426A62A27
SHA-256:	23AB3D6E1C7366171C810C8C303836BD953705E37766DC3673C8D1ADA9C60BF0
SHA-512:	193E507762A514EC4F73F294B700554FB5907A59189A87B65192E91CD7B83FFB0AB8360D7A38AA48CD011C6499D69F5BCCD0D60DF88F68A919A869F4085A5A58
Malicious:	false
Reputation:	unknown
Preview:	RG02V1mzXb750616Y34H10n31fK3jl48q96fQ3vF3k77O6912vK2IG708B11ZK1j1Ga170JJ3J8o8d1T1SeL97Io8V98IfXUzbw..2xEY3Y6r9Aw4X4U5wZPUJL7g5844f 0fR9T634821j4hr30qQ89Q9qd9f9o5nec52u24f3u84f9231CEnaf216iJ5i0C8h4j..JKot24ptaj53Nt1aevWB82dv6J1t01lPu302K80c888Y91pY0y1yX667W33003a20Y3358o4 B9Q604F406x7ALP379x03ynQ999s299453h77..6m915ESJ8XI1itAop81I9FsX7fN4S5nU1J1488Mtn95e749Uh6bBK4E9442JAy0k6e1C5x6Q375A4n0lWtUodTm0S6c 1420h..399W9JZTj8R7ls8F0176pn0vWP51A46k91v..Up85a1V99g6rh14p0Q607Q3s493YCGTl8e353292e8s1Y9288Emu42255w5QkVDw8J32913zt3TAW49xyT6Za3 88k6bWm06Ixd4gXJ8D2dx987B13u29O6j2p50n0m43818r5Ri0M75D07NSG40Jswo0bOU421..

C:\Users\user\AppData\Local\Temp\33911166\ftwkmrtqp.docx	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	548
Entropy (8bit):	5.465064929486492
Encrypted:	false
SSDEEP:	12:ozjMCyFovbegtECerBNk0iKpKdnyHLqfFC1zllBoGoxn:qvAovbeCE/sHKcdnyHLqfKtoGQ
MD5:	51C93DF30373E2B4808CCD94060AF817
SHA1:	CCD9097DE3DC6CF69DF311CD7BC266DC9232A702
SHA-256:	6BD27A359F02E248CDB45E6E150119ADD745AA028BE3009DB71578859BD7E149
SHA-512:	7F22F1C8494E0760837D0B110E75589020C0EE2E71C437D96EE736DF8A3C9B7FE9F809C199C63AB5E39BB66A1B129BABCB4C75C73645D3DFA9690FD13F6CF2E 8
Malicious:	false
Reputation:	unknown
Preview:	nZy8E5N0030atBonTW762vOpE4p07kq2o1863r5v75h47l1iDR35lj43jU83Zb9770d..m8713o8GWP4Od7fn6tf140388h6Fkvm5s5nglkH8Pt9Z90Ro18sY5LNY20ttX lr94vX9158Fhg85jvFy0c9075hxrWij6Ur8h8ibu2..09ZU35977zlT99iTsA03W8Y03IHFUbWz52J945O2s5j1n7a8l47y1417..39e754h6Xp7v13U6al6z362R9pmI173w2b23W2y Ab33pI93h641G3b9do..n6fU7x96i731y3353N7TY49X7506NQ5uzN4Sf5Y263RxCM0iGF4PI8FL30J8WK15x0Smbc86..oR056n4l6pe6Z3m597965e8724rRH3XHuiBr 82c5D679j82G08fab4i8AMl6si79af7rm1a48RtG0sr6P..ki229D6V85IQV3C754RB5Xw97P48pq5p9b0tp6385K0378O7G36n8L9I537F49Hl6L4GG1027k2980r93RE 26u2Nc379y99io73..

C:\Users\user\AppData\Local\Temp\33911166\gbjrbcio.ppt	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	505
Entropy (8bit):	5.473101669206148
Encrypted:	false
SSDEEP:	12:1sYFONrX7jOPqZgmQhhzc6ORhfdTj5E0PKrqqBGN0y:1LMNrngT3MR5d6SwfBGGy
MD5:	FD088B0DD1DA3EC4F335AE136030DB08
SHA1:	A068795B4A6315E8EC6FBEDF6506BBB2AB007541
SHA-256:	BCA36CB79511273DFA8BBBF029D6E94DAEAEEBE46F6571881AAA1352CC8F6FA5
SHA-512:	4E097D2FCF97DFFD6A1316BA52E908C804E7AC7A20D3923765A685EDE3DF570C53ABD74716606027816A055D9C1DC86039A90C04B8217DDB72FEDCBFE79B8D 3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\33911166\gbjrbcio.ppt	
Preview:	6Bsa2cWvatCb003J18tmyKa51dz956MARg54iy6cH0O75W31i6b5R7Mj2p7F91klcgIpVb538z43..4u2K025LV2S9I0g682orjcF3q490p849762IZHAm4U20OoPvv3k0 4B0fcbq02LbvJxK..k3E3Z5j2BAi823z8qyyL0Y7WJI1H65B98TPny45w17q7P1oCU1DZ0F31k3Z0RC1K18ddK53M61LG4l5T78Tl611y..34h78qE6..r41X587iJ73s9 8292b1m032x2Y17b3VqeS8148hRxx4GaeG35R80972h91y1R3845i62A0D086i6uZ445063485521o1F3f733764t9O5..n063058SlxPoT76n83659245c6g0XCsAN75U 03lq3e9VOk3Uky56880Y03MxX1s31lA9K1MUI610T7qD1Fy472m2GFFP70mS53mzG1wU449758n5Y2m98s03l195kuYM03f7thNA4155GJv25W0HV..

C:\Users\user\AppData\Local\Temp\33911166\gdljljtq.cpl	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	48980
Entropy (8bit):	5.5709636707326045
Encrypted:	false
SSDEEP:	768:mPmqXrVN5vK2fOoiIGRVHrzTBmqFTv+lIJT7FiyU/4AM0tRQWMJGggQCDavT+VIJ:zgr75v9OoihRVHBzFT+6lha410tRQWMj
MD5:	A7A133BCD7D03BBF6ADDC1658BF20DAC
SHA1:	0A3A664884BA14B7738368307AF1E498069D5348
SHA-256:	AB5E48986B6BA499E11720D12E42BCAA8C6D712E59CCD29369F7425BD1D4A678
SHA-512:	C205518FB94D1BC33E729E3790355FBAEDDD8073966EA44F906C1321FAD325B73108AE1575A09EFC4E1FFDE4DC4485DD53373C8219AA2C820E30B28C5602574
Malicious:	false
Reputation:	unknown
Preview:	Tv27Gs7spk08qJf6b7S5A85819gU4XRjX9636D4d1UP0Y4..y07Fz8fW73Ro263j65KPyxu1T4D6xl2qD4Ej7j0A256975ZLr9R49RHAp4OHknl7E4E97Y..b0h5244kqk AyX3I35c0828H2T4n1650eN0uiR55Vf10054l72wa46nzV..49122C082ha0j153NApk76tRCj316bm6Sr6Q5r30n6a51779303N940727809e6o13g032..6SN9Os624t 9Z0K0Y29962H746p1j0lmR7e3IQhHSQ200d899o2xq9C8Tf6co58hbVL60U..o3K9p744580l5XPq4qsYd5838Vmn533F8Xt1353A42567B97..066247607DOM7M35U09 E9b73P8..89bFNiZzCJX1z024mVpFaqx55pt0212e5ArQ..7Eg3P9hL18x0c821771f5wyl26n89V4217a22j2ie9409PO74530..3gmcljb460HarNC98Z81pkY0h53mk 50rKwA..8948mn846gbN569h01NcFP49390fH0Es0S3Y..Mo8e96z0jd7W8j4L9sL9Vi42r2i8bQnaK39Rr4gL0264mn..ywdrxEmE62C0qDy9emAz5b3Ce66wT71bvu8f cj9Fy..521g7ofCmqn1K4Q8395VssQk9GbTX626T0l72..KA825v89U1y68082o12674kK0P96750D1QG6872QBo563619151q7CPj1ZoomNlj772Y..P7s93148a69aD1 Y2K5584208lJ35154Kl3eb193c6P9ffMRD0l88ETyp5i988JoW4406496724M236..g5151C2BiR3eZ37s24H67Y15p0512R50K4CFqh9g2u1EBw17nD3..w579791159f ERlVd927t9p36cx47gl075Dd7F5NR4aPDL2H..YjQ3T4y5Lg12t2m6zF5g0OZC701F1mE1X7..349QKz78YW1201pz

C:\Users\user\AppData\Local\Temp\33911166\grwmscle.bmp	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	551
Entropy (8bit):	5.464613608461425
Encrypted:	false
SSDEEP:	12:j3lvpXmJgFeoon+sroHuQ6xc8Y4YXHXja4R/b+t/w3ENsVQHQ:m58gFejnFAf6Nq3DRQw3Aw
MD5:	FAEC8B3E9041BBBAE67F552C91764776
SHA1:	0EF8E9676EEAB9716AD08EE6BF75BB727B8A6E43
SHA-256:	0D36C32258EDB46B3B9325B207126B530D3D4073060CB32B08E5FB9FBE924591
SHA-512:	E46F365FD17FB91CBB0FD3D105D521C9F4BF33FA825FF85F5E2CC52EBA7C88B607B2DD673C1C4571B893FD97848491646C0D137390AE31EF5214BCADEB5E68A
Malicious:	false
Reputation:	unknown
Preview:	4z2a09BY47L29726tMLce330wZBFweJdEogFT885Ow8r2Uh565414J5J8c708H2H1NwW6PO1Frf9UUvYHi3728R2JAz4LO7Iv208Sx5N1..O6Kz68244K9L98H88FkmWN3 39tK0O63U200324GZmlD0d79Yn19XQ6C0n8GrV6zV967ZRi4..1hPzt8R5nW6vAV50jS546z1R8573345sC9dXqjylgz0V2WnJ6J2C2K505YGEn9L54XRR475Chz3..9ua 5970p1KG702q19433V75tpI909937v12UA8857S9YlfCX3803k89W72060dn91438SS06c8fDlRD2Z0hG3H0Q899G8NzQf381K14hx7F352l8234..JD7054F51qtsJE6n f813hI4g98NKf77Ak346G25612wKqGf7TshsJp2Y0437197R54Cy85AjJovAY84u799gU5EI49N88K047..J6SozV3EMo10D414GUK482HnnzbA0k5F59L60nFo9uA096V Qd05vu43GiNKf27D94054v4S960X6..

C:\Users\user\AppData\Local\Temp\33911166\ihkq.pdf	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	572
Entropy (8bit):	5.553967984733832
Encrypted:	false
SSDEEP:	12:XcwyUNHr6XC2sobJkpf8UvqyT1cr5E4VkDQyIgTdHQI2v5F1hZHtmsT8BBhiK:6c6XisOQa/DQpgTh0pT8B/iK
MD5:	14632FC015393D244C193C33C1C3DBCA
SHA1:	C084DF5AF865D0548C73CFE942208EA09A541521
SHA-256:	F73ECBCAC7B42C2A2CDEF1F102026D210708C24964401C286C876F13BA43F17B
SHA-512:	42855F0573F76358FEC1341CCA2A35B02AFB2A00E770FCD85A791B344730278003A4D749B89D9596000D9820CD78D1EED9026ACF75202AEA51576492DBE62309
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\33911166\ihkq.pdf	
Preview:	ayx9365n0t50aQrGTunz155N5X7g5tyV8390I41W3MiQS6h3M5P1ZG3315C7821Gz6nu4899m2ltW4z2U7J810V1qDo6C5SaG..1F9LS525n66r809nw3KyTt0257cew11 AJFkjV3L39M5RR0iBhxnFI70z75d2f05p4eem0J7W3742a83hR8d72GJ9VIdh9l1243dG4160x335tLiuHj728JL5X0270j181bK2ZB21gq3W175Q..O04wDJ3871v539c j5O762qusnRf2pn9f45i9aa7N63342jsh6CZ307K205I7XSy9087Y1E17RVYGll926C2rc22009N..rIgL6WOUC06wd0DVj9Poqm5gZ8r085G1P50065sUi4chBMx89j64 vfB15B4LE8Xyf3a0xoav12ujF1HFB8lqNR1dHa94m1n7Px15B9..u9L4v2cUO77930Ikt612W7LFU6qkk4J5S90Ca701803uD3u42H3aO01EMK398Jbn6BYlV3qpzz882Y 60f54893jpb1t9fL39id9c7S4Y2h2ZeQ18otELaGl2LW5ag932..

C:\Users\user\AppData\Local\Temp\33911166\ivexkhsw.bin	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	539
Entropy (8bit):	5.492587055677928
Encrypted:	false
SSDEEP:	12:wBPVejJwZVUX1V69pJ/LA1w15dcubSTQiu4nsorWETTJMBcUAUzrD:TGUXyn/U1w15BSMi7WtxzrD
MD5:	FE7B76FE43B0D48EC09E649D3791669C
SHA1:	9F16FE9CC7FB6D11409083D6D84586951DB9F44F
SHA-256:	5BBCB104598FD0CF02D426D6385613E8CCE500A253DA17C0FB06425306960C03
SHA-512:	F5B32D62FD836A0BFA71FE5594EF77064B354BEA2DD97AFEBD7D014A98DE495776521A55BBCF094358173FE498DB42DC166FDCC0D9DDC432A95EA33C2F7C7 4A
Malicious:	false
Reputation:	unknown
Preview:	rHwJe4es52vvbII8Ox6PTt4690JBsdvr22r69c6845n19UX274O3t8085C6hn2qN7q40c555qx69kx1gn8Zy6WWV0eO1545sVFip580U2phqjXAG4845ag778biTL..127 CQWv46..75U2B1G6093mw9zO3r0GZ04m8uU02USb356w16XJZdg1sFX3l512H302VWI801cJ38236Uns529097AE09176wOV0l55vuo67093G7z3Bwu317WE 0Q6t9r2G35r7q75y0WE7Gm304dx4R8d944vb2Om0mW..79ke47J7t2geN2tN0U289k9yA3qE74F184J8FG67667mL9714Fb1wL21UZfQ503Z33b762q2F03DJpKSPGK8Gd mwRks2jf2J4u0n0076Ek4H0..h5Z0lti829m218hdE916i75J6yJmY1..D7k3tD7J93V471ufaD5TfRCoE8z6395890o585yFU9091L5VX4i08J0mCj75iJckM2D83Z30R 50zD4e1cB0t3451A7o124r2h3QC..

C:\Users\user\AppData\Local\Temp\33911166\jowmpf.dat	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	596
Entropy (8bit):	5.497302797959579
Encrypted:	false
SSDEEP:	12:ClrnQwJ1Rt8oVHUOSReHJVALg+UOGRRROVt65kXSv:C1Q8b/rJVALYRW65kXSv
MD5:	07F615871C99E860DF4A51C2608589AD
SHA1:	E7D9977357F4B148E0C9F9DDDC25A11C3A2A3B0C
SHA-256:	9A6657FD3B23DBF7AAC5FCF306E0E9B18EA81496C1C8127EB31EFB6956F3B879
SHA-512:	567239D4584DF19688EF88D950A250D385D96A0BA9C90A9C2696DE5CE7AC5E081C74F7CB5F935D6A988921E8CC4EF88B90ECA5FEFF827293497FE8E8CB0DE5 7
Malicious:	false
Reputation:	unknown
Preview:	3ogO2OkJeC71EF32653e2p8U7NkVL75G3z5q1637941w1hDKh538w4rIk3w9DF2N1807Om5yYG7sjI687hAm6l1..73N0082xA6T31630722te0219502f1HT14RHs4N58 d6F393e8B1lENChi9DGr38C79822p89hhnkGl8Rt1O45W6A..2290704s63sSShbS2krbXeyeNCD69aL090R9Zu726pv6E06t402Y092XP8t830CGJN91ufI70Z24W028B 47sfZro05OLD35620c5m3b8E3mwV8c8y18ZiUKhX6gy445LppJe8w10853O63Ezh41De01ut61lIuh0p76GgS6288116r15GJ9Wj9O3b23H7vc1XR..ALl0435bb7O1krZ 7Fl53gx8k9n..302EM8xnTlwOX1mZkPU1r18V61pBZ782yUYSMF8R1G1Rk07579Dvvr6Wo90La2Jy0977P447K223..T4K9714M3Q0wEJQ5f2900u7pA9Xor6028A229HQ i90DBh1nT8B0d4BBd4s12700ZPVA2wpJ6662Yt39ZHSu6A3Y890Y0Q7h47l964R3450K53WHJ1..

C:\Users\user\AppData\Local\Temp\33911166\liqucucmm.xl	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	528
Entropy (8bit):	5.445249383001988
Encrypted:	false
SSDEEP:	12:6XEvkollIAArNGiGizpRKSXX0otCzEG+IZTcZQStN7bfLbLyJD:30cGi/Ke/tnGnZQZHbf/Lyx
MD5:	DDDC12E603249AE7413C0F1152E415BE
SHA1:	20D6ED41E340B890CA845A1800E0FEA6310B5371
SHA-256:	B4AF5EB959E3823BA63CFF92CA7A3A480FA8EFF6FEC25611F9D2448C8EB975D1
SHA-512:	35DE0D18909A298D8BAF56EB3F2E4236223B2FA723C476042F264CB97A97775E5EF4CA61D23BE3AC5A4335F14733E54F58E89C58EAB86E2A2477CF430DF2343E
Malicious:	false
Reputation:	unknown
Preview:	jr7RN26AtoFG2L..2Xv7061C8jX5l7674Q29ss466l324Vq2DeN8k4zcuH13A0Web25P..9z0bH0AO96220SH..421192pb74yN9Edbe7DnY05V061CY68lj9jcX0XGJws 0l2Bz3895597j863P042e1XZs2E10b509d267N7BiT7R7cMz9eP1k6XFz973s6002yg37xzUANQ5091Jn3lK4pQa82573punMwh1dTJ8B07ax9Ch4..uOp9zL7npd744PW 8g480919051BL4tM6l654RP463M2i26oL5WlV9Vfb..A299449512883Ufcm3w928r6U65823Dn6FIt69s93O47800r2d17CPf5d064F6..1763G2HzG68G5CJoc88i68L 9g0498301ZP46zY4V27jX26bi5jGj87c039zk7yscQ2f5i3u6Ym4p9p984VQ2988469y8eF91O03S94j18E41ViFKlYLl974hj61U9R4C4g7P8a1dbygBemQ598zcB9id9E58n72..

C:\Users\user\AppData\Local\Temp\33911166\lpekjev.dat	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	632
Entropy (8bit):	5.505372170374117
Encrypted:	false
SSDEEP:	12:eOvlHskQ7KZEYf0pjlFhWzg+YNAJAXVr/ToZlzcCVu5UvvVFVDUj0:FUKZEYf0ezR5JErbWlXVEU5K0
MD5:	90F85E9DAA7BB4A1A1D029FD3D8F2CCF
SHA1:	A30E08BDC0506CFEC1CDAC32B9534A7F9920EA23
SHA-256:	5E56F31FBC40A67E7AFBA14117BD6DDF69D3656360D980DE7033997A8D0265B8
SHA-512:	2F801C5F8EF9EB7641123AA11644A0654C8DEC8ADDFBB560341624E3D5749E40BBB67F4EFFD44EB9CE1C460EDAA8BBC4CA1E77996EE1FA627067B7710E608897
Malicious:	false
Reputation:	unknown
Preview:	33442C7S7ADR8fS..oH5739s158CG23wtTL2909M323VF81Gr2mK1oE6XE6VpB68Ly95vr1xIDt8f8VBbY7F7b5wQepDCA548T62ovs19z2Cl041X60iuo5r9NOTXD69TC66Bz00jc3ciZ022ki19p083736fm991U81ckzI296181..bc00C0ppox5NnO963xd7Ee2Y05e80O67Khf5PDCgIS24Fp7932wg48i054Z0A5Jh19h0tfv6i28K3ZH12707Hi61p38g4Av36R..6D8KRy1F19I47X7Ou09ZeRqbXIMeXrRSA16Ra9684P3B..20Co8s992v2O1ItqR..5324h1i6k654nDGSJ26v9u251q1624Z170990S15m0XB3j15wnv6z86UTx595I0z577AS4iFE15U09788HS2ALim6mU8Fp02A76CaQeR4M9kS5kl89X22114a1gC3GHjr74KSq8V18ESH0D45..9k93LQEu4Ru9SxDJ06cPpn984863356F2LmlOUj6F7Xli9l63009C718Y7857nL4iR081IueGOlW4Sb83q9up078qN88ki5R7h16T2j9q11R48F498H331q8S4VlWO669rU7Dw1s74Ax3a..

C:\Users\user\AppData\Local\Temp\33911166\lsgredal.xml	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	540
Entropy (8bit):	5.532441952803367
Encrypted:	false
SSDEEP:	12:8P1N0fS4L87XKay9/O8/GKi7c/ozQrCqBj61hwcS3ydrDJcSBn:8z/e6aay92NKCcAMGGj6zSiPc0n
MD5:	D471202643E357DA5B108B128DC7B903
SHA1:	694485C499C670F4ACBAE82D2B5776EFA1C4E6B3
SHA-256:	C38FC9C91DA774E70034CD82E83BA1A5A732019EBF20CA43B587C91EF343D131
SHA-512:	508D3725A9E71ADDFB2528181FD3AF02267FA1092FDB0B61C3F0FAA401BCDD29BDCB3180016D30F2089A9C4338F22899AC2479443FC46DEDF97A9A5724EDF26
Malicious:	false
Reputation:	unknown
Preview:	s9344l2XB53256cYxS459V6qyAeT72xCC1JdQF1444S7H77445yb5IJ3Gs256K2GmVw410VF2TTsL73Dt6kmVKAR08U0..738D2m617sRU7kv8FO1CMZ843iA0mtW00EAPS9YQtn29ccO0Jl584H006p5GOs071DYN1WwuD0..083RUDU2Mmc7B0733UIlHW1Kj55To6NSa1Fi622ri4nL3ThdQmsuN5789sD06f05et0g5..448u6221M7anl4675T7q7s2BBMY9a7r22M73fE6GwoRMu9q4b28467gCTWpH39Mb6o086nk1Eiv0D5c17398FW00ls38WP79O7w04i753XY8V40gUGr41vDCu82134g8..3r16410AYIvwkB25qJ2EP29Cf8y52071048z85M41lq2ey92Z1JCv5SBT1S7EIV2PBG9J0s9CU702Yo0oZU696297RlHM211u6InG03561izH5j117676NLAM9rlnC1508183380xDFbn6L88CQiOJ4I7e888953Gr5y2oK..

C:\Users\user\AppData\Local\Temp\33911166\mfnquskjg.xls	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	519
Entropy (8bit):	5.573296492791862
Encrypted:	false
SSDEEP:	12:0SpP2kZZfmh0PeipDdZ3a4QER9Y4KGdeBJC:0S52kvmym89KGIrC
MD5:	A9983318B76F9C053B2F9EC83D35E9C7
SHA1:	63CC776DD26B2DDE4352B729FB1B5E8F5F851E6E
SHA-256:	2249D2D3DC78D28FFF96998C83AA1EC9E9E8D30163984DC4924AAB8179FB4AB4
SHA-512:	30CE1F0AF2B1E825CBE440665F26E4D9A9A0FDA227F3D41F6AC79403F5FB400B95491C3A8A0E0DEB4D64B22C7139D86DC1ADEFEBAE0C5E53815C645E50B2BBBC
Malicious:	false
Reputation:	unknown
Preview:	08wHb274y73Si12t574700fn75e4nW..XvY79U19Qcw906BQ4SaU7DgtjD07yP54w99P091j4J1Ea5RxHA0e1590885y9FZ5N18VvPqe30Q60fycD4g6GtTpcH0A71iC8eNA9w25q95Yuff3I10Q14QeQZfDv26u7p03Og5M9Rj17dyvjK15hN1rPh94p8..ETXI4M0C5dd61e05QZz7uC0FU42257jJ6I369EVR19ZdW9MJ0U8koi7Tv57Qlbj465JA219a9E6Wt1..T0B01S0twl9B921558NrqTIzWLi57X70T7UZC38ifY9mak98q7u3H59fJXKf5cm56RuVXmY76Zx6262q6bnX..zebXm71N88l3x79zm3764zp263u8c97lzXc2v2s8Wx3kd..9w9378n0m61J0hVV3p8tJJ4336da8301fri16bI02u2G7260O3CTCfer0j949q1q38jhe58aJ0p5612f8szuWU7G1eY4O92Wb359Rcj644zL71ry..

C:\Users\user\AppData\Local\Temp\33911166\mvbphn.mp3	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	523
Entropy (8bit):	5.4783974308238825

C:\Users\user\AppData\Local\Temp\33911166\mvbphn.mp3	
Encrypted:	false
SSDEEP:	12:GrFt507gzMYcwErFBB3xZfSL7Ic/788ZBozOH2oM8Lc:Gx07gzM3xrXZrfSLccj8yalf
MD5:	8C9C4D223F47A96416446C0A49F595FF
SHA1:	558BE3F0C1FE5F8FD1FD2DEF9D56BEE3358A65F4
SHA-256:	8DA7F767634CE2F72AB495047B2BAE14FBB33389EEC28E41CE9B1434D0E29DC6
SHA-512:	C03BEEDE1E688FCCA260BCD13972D595344C86A1389C3AF0E621C3518A7AD2721B7DE366BE96B89FDE37727FD63018196EFE9233D266FBEBD59861E432C4FBD
Malicious:	false
Reputation:	unknown
Preview:	418J046ZUYreU03PhN6q7k12580Of34347xfvL8y633K8n4K962da96L9Z4E78AZ4rwfRX3s2IpR6i1LzPW24A2Hfot71344aaRW1m3r08eiVLf1V4..m0HH4l726i3m3T 0and082B8C480i21wXKs45k8q8K0HwW2Oy07a9UNa1D006727eO49J993qN38o1C30fOsa80flk766Y1o8P6GhQb9R07si02n9J8a1De5296975A8589U21VAPAZH..qZK 9GA9H53b9pPJ8..3h21zrQ55TJw1X6469a5qqC4Jjf5L4Kk7..65179t5p2757..f0QK52TUpmvLZuiU2i6uW53v7Stkg68dR2TZ3FL79l096Dp07O3rCc7Lbz3et89q82 0N1QW558b955D24fo09887..wV6tKG7o7355224N329URh6e7II953KaVHm5FR7em2Po53276p92Sb86LcF06n19U738i7J11H19M1Zai6bW4EKT9LmRET7N4m1K143r0DH..

C:\Users\user\AppData\Local\Temp\33911166\oexk.ini	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	569
Entropy (8bit):	5.4773736308617655
Encrypted:	false
SSDEEP:	12:mnnWdM3QMAou+SykUqgUH8uHYqW0bIVn9VBuAdc/7s2XumakoT1:mW23XAd5c56O8IVn9V8Adc/Iwux
MD5:	35C3A3E406066C083E25DEFE8E4A921E
SHA1:	9C2526B9706866CE1B75924F3AA967C1C8E20500
SHA-256:	C069BAE783EC8AD4D582B2C160D28ECDEFBDD3654488A8C2129EBCD3FC2B9B34
SHA-512:	7A6C3C9075C7AC4FA4FEF98C537907779FF5DB0A3CACF0F0AC6129A7CAE25E76D0F45E82CED5C4626CCFB7FACCFCD63E7986314657986097A45BAAD21267A23
Malicious:	false
Reputation:	unknown
Preview:	Cz1Jj404UpG2w6NbQZ9r8FaTd1CyW5B2973e49782gDe20u7vIa81o060..SUBV46isaByWyVvL8..738QOtKC7Ky6l590KUA4WQ01gyX7GMZp6J56CDae52y6c0D7Lulo 105v67M2qd0844c64H996388jaR056Bl231530hxHb8..J832H58Tle1QT819R05yE5JP1n350K3545a5U0957v423j0Z63365nQ8746764E5241Z8G3u6M9ykdTT68xT8 1i67d396Ik29q57o9Q7XL50J1O8t2VjIf2pU1Sv23KV..05n1rFsm396p13675iWF7V7MM5cPA7pSGZ0J31bz921O235M0TcfYb1z5C4Ld61Pq94163M8z009DB8dm8LYp 519mX6ST..8cIr209s469v8bJ77G70D66yx0745xmFCQR7f631O3L45Gh36K0k550z9341f9s425..85dW04394Q60R0J5EM8g4X774yf56u413122abSGe4Kf3Dq5td2x 7zUvlY7480L0pG24o56Jn9fiA5R62V6U2n7GYX05k8vvh7x..

C:\Users\user\AppData\Local\Temp\33911166\qtthsrfrd.ppt	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	589
Entropy (8bit):	5.494103483866326
Encrypted:	false
SSDEEP:	12:E1h2WziB70vlEW2+ADg4Jo1FATJtdlJmN4Jbgw6XB7oiy:E13zW09Ex+io1YWnXpoiy
MD5:	ADF668485BE537AE0D6D5C0BD66705FF
SHA1:	5BE524D0D0E1B7FC42280224CAC2EE68EE0B49C8
SHA-256:	E1429751B756E17CFF90303EABD84985A6DE8264821901E78734BBCDE1D7ADB1
SHA-512:	631714903D57F3869D34F05C023685CEE8B4D0B505674A71CD268DBFBAD2F2FEC66D6137675AFB287A83E04636A738012359BCC9C96B98EE3224FEDD72F570B3
Malicious:	false
Reputation:	unknown
Preview:	18Sj5m3R0239xlyPuv691Q0n94lky7s4H80CgCf59WSU3pAv82Dh4PG03yx4e17r195h8464Tll7F828Xrx6648d975SEM197rW8E8M1mjt71A28811yJm95RF714X71p5 3T..nRge88545JHK72E1UxGVl61Ju8je2kD3gj7F..zsQ7h7J249743011Nv1LZdm89XhTSX9U97L20l..706j4Cy83fkKG81d8zL9q3ew8x319J3nkN5VKm5e53Zf6336 2eoho7717L034Lq0db0cKjt392..11Hk269oBVCoTqK1q9TJ4jmh78OBsY9187pDXKWW34M7409640W85Ek2A9e0l11U4P6146A89ErKo605i897K93nprmW1F6365ZHq6 f27jN6e19922pJMu66f5F6nD07m4a270hz1O18579m9V9326wjjjuW317x3bN..4S8OC1F6z3S73Lsa7h3U90Mu540t0Q425nkfLzzJF718jM68du65T4540t6xk41U9e4 1n147JVIPj9l62Zcaqq9T9SG7n3D6iaJ9pUl951R2258B1V0TuTJn215fe6OUGuIp87..

C:\Users\user\AppData\Local\Temp\33911166\qxhdhpfdj.log	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.380432007459812
Encrypted:	false
SSDEEP:	12:gTD1TxGNYlJ7w/yszYThtywin1OTDDmaPv9ztd6SUzWU1O:gv1VoZJYUThMH1OTv5ztd5UzTI
MD5:	A91B92473AF61DC091981BFFF41A3A88
SHA1:	410EF9F87CAF3801C87D69637BB469FEF3C6A369

C:\Users\user\AppData\Local\Temp\33911166\qxhdhpfdj.log	
SHA-256:	38425C4F1F21ABEF2915051403B35003ED7274DC14B547FE84453F227510E1D2
SHA-512:	E0D08974FEE7065EF6DA299D6CE5BDE8119C625B79F1B92978D3A512221C5EBD76DDD5C3C36650EA3D49036ADBA08C6B2636F65750373C87747F1B94FD01284
Malicious:	false
Reputation:	unknown
Preview:	vxn7601M6s58rxU12527Kz472a4Cs6teWsbFTn25G41oJN02ey7wJ0L925fGFbZ96NPU1106oXBo86dS2k9175i788C9U2k254c672616nH2057o8j0..36P6291t7wla4 5Qg1pkOM9N6f76LwDa73h04unx620lWpbn7862179tT95SO95PS78q7Nf060628v8768k..GZ59S38w37V2v2BNmwI6P67176T3z90p1UONe0p8p8CPy7994fg561V7rO0 851TnBYXf6033K1Vsv6Bm56GK..E66g9954vv5ac5fcM..158m41l38904961bA9OBZD8Um5GVnN0QM4Wy4932..Z731kA9D1Z08aqFk33t4x78t758X6S4j9wKU7ut5Rc 9Ck17KqvX4K5Jp4v31KE90k281T1g1J4U944N2..54823l4waM1641K98y75K9595BD2xN393UL235LrfKG5m9UrI948U5qX334029D400bzGs314S82271v073c154k96 3z6..

C:\Users\user\AppData\Local\Temp\33911166\rwnbbebwm.ini	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	550
Entropy (8bit):	5.450135505815625
Encrypted:	false
SSDEEP:	12:UWsdYUrk6GI6UzY9piQh9ncQz1LpeLULCLPhpZeYk/cgsQTHucy:bsdPkc6UzYesncQ1perPhpZe9sQTNy
MD5:	F8DC6E3E70B4432C180B7FA0B27B8E50
SHA1:	5075849AB1FAEBEBD28D3660034C5C45E65EFA8F
SHA-256:	E94A2F8E556B0195E242AB5D6E0ADE9872BD67857D150E7E4640CF2AD21669B8
SHA-512:	63A14DAF5728FB278E8A3AC05AE1F8DB2B11899B8347CF14D399D028E8BA1B4EBBC3901584925BF421F6E515E042DD6647384FE10D7E1EE823DBC3DBB68F690 B
Malicious:	false
Reputation:	unknown
Preview:	922jUv2o489k8Y013231DY977D..0771r20wj26TL1c8g7J2e5yYoE79024cAh4366Vjc4T94huJw391m3Yo621107hZ1V09Ey2j3tJi568e5h317TJ6wG9Ht5cS3ff42W 7q704KK6E5899F1j8471460z73pg44ticdOM3tne1hIz7..598w84e693L5G78SIlm3606178l35hfCb9A3h93rrd9qH7i4O93omE8F7S50V74Z9U2jV3uSJn9l8Sur24i7r1rV8L9A0 8Kd..Xt1S48e7x03s540o1NSW8f1dreU..y831zzFMH5RVvWGX36nm90594J8cQk6305CcA31Y3oi949dxl49l4h7l3G47f924Aq7..83111VG9fu5t49mI10H2c478qHy 3dN9T6iwBBEr2g129L67i58gS5H063XzZZAXwRP70rUeMC0f273400J..78367R422G8O562a2p5526Z11Wf9lM1T5Ud34KSnl90I5rgiv4t674240v268p7692ryYcVn5 1n2SsM6JIYJtboZ527..

C:\Users\user\AppData\Local\Temp\33911166\sbipvhb.docx	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	591
Entropy (8bit):	5.576834965418453
Encrypted:	false
SSDEEP:	12:SJxsCAM6SL26TpOuCEG20RHTtXGKsbNsdXD3ndFWE4gMc7G8WUqBhmX0l0:SJxdlLroEGjRXGEVZFH5k/BhK
MD5:	CCC74C070D273ABA95D7F8754706A255
SHA1:	171E25C7C895A8B583A8BEF713D077DE2419001A
SHA-256:	27DF235367CCC09F310E790A89511AB986A972722CD5F1BFC39D10019C7EBC74
SHA-512:	631C4DFF189499B858D927897869BD5C76DACD323A0E6C0F37C1E65038504972F3447DD6A52B3B0E3BB0A59EAEF05A7B2EDDBBBD9D0A098E9CC5854A9974C4 B
Malicious:	false
Reputation:	unknown
Preview:	2748E82k63ayl53YX38l4545OT9s059X6h8bX7hv2Bm397q35m36bs7J390cQI65n3U7jC17c4HB4OIOc5wj0b..TV8LwMkW1K2D7IU69K9g573AKT4m99nGL9013r7740 r4gRRGK24n0o9w4dCdl5H7fl7q4EY7cq058h3KpDX7ycp0a5z1Vp00zJ0S8u1e588jod37H3tb1689PY2tB6D2R833C77P84D402..03w9gmDY785159547ZXd67ptqNL4 l56Z7x842ePU3EnmFgaa6Zc1ejT0py57Ma17ViTeC6lQ67ska01atbi65r5p3z1W69a569wku00h777g0lOht50b2WjWOh6HK73l01fc4e67oWh1KJw14P4UP8I5jo5ioF fEAD19..641SMD18M2S0i12V2EoR9W9..z186Ov121Cok9XhU3jFRZP4x8v221xhtZkJi7..Ue342i188p353998017612H504Bt9YlsQa57aj3A992Fvrv3O78p3R7rtE 8YWs427dxn0q0Kl614gp6D4E4Vt2KsC97C7u283K24PNnFdMY1p00Y81AhVH2zp59pkc6..

C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	170560850
Entropy (8bit):	7.04008382283949
Encrypted:	false
SSDEEP:	196608:gdZxa4ul1+Nl/u+wy25wEPjq+L3gl8teH9pxCgiNZNgZlazblTenMzSvb4cJAka3:P
MD5:	A78521017EA74E5BE68BEAF3D0ADC368
SHA1:	1694584C416256DE6BFB0AB72C57675910F479B3
SHA-256:	17DCEB208F35A9966672EC161B2BA8D5A893DD51C204F2E62E291BE06F7595EC
SHA-512:	DA4C35668E82DF4E3BB4A8BEE982A809E495DBB375ECE7A330B08436F4B8ACC5E1508F31BD00C2434ADBDB4127D4B198111934CFBFD2423F1F9E796DDC06AE 91
Malicious:	false

C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw	
Reputation:	unknown
Preview:	..;.E.#...._.9@..E.O$e'.;4..N.pc....#.c.s..X...?#.Kk'.!.-.O3]...&.].M./Q..`E..b.hI. ..zh.w.....F}....1%.>.....c.W....d.U)-.L.N.S.....r...~rQt..o.....L..8..1.....#.....!.r.G..+...#2.= .`..Mh./...<.S..G.-..f....".v.X....F.g...P.q.=.`A.&k...3x7.Ek.A....`...V.v~.....6.6.H.5.8.8.4.9.8.n.4.u.6.1.3.4.N.1.C.y.8.9.f.o.I.5.0.6.3.U.1.6.a.Y.2.5.5.n.D.4.z.z.Y.4.M.3.....7.5 .X.a.9.D.8.I.8.0.....J.M.8.J.i.H.K.M.C.4.n.v.E.0.y.4.I.0.a.8.5.4.D.q.i.5.8.x.L.1.X.F.9.3.....O.b.g.1.o.o.v.7.9.9.1.7.q.....1..X,5I ....Y.TL.....M.w^.{.7K.=.....`i_.:...pd.....w..._..D.D ....6.e./K7...t....L..X..uV_...>s...M8u\.v.t58../d..o.c.~.A}o6..[...4.=bq...l.:%..X.>].....`k.qy..p=.n..R...+\.8X..{&.-ai.#4./f.....).....c.5.8.X.w.H.4.3.C.0.9.g.2.4.5.7.0.n.4.7.Q.6. M.9.t.5.2.Z.2.7.0.r.7.6.6.y.1.Z.U.1.0.....D\.....Sz....5@..r.~.....>>..\..O....{.RF..\6.S`.\.84.JM..S*.~.....p\..^Q...}.Q.C KzF.*.b...;.0....[.(.x...7JY9q....F..E 9.....l:...O...g.. NO0?..a.'.u..y...K..t..k..*.xt1R

C:\Users\user\AppData\Local\Temp\33911166\tvdjw.ppt	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	582
Entropy (8bit):	5.516494390661715
Encrypted:	false
SSDEEP:	
MD5:	4D4F70BE0D08FD75119FE18C6F570095
SHA1:	654F9A02148D393B885A5803C2F3BB0146F2767F
SHA-256:	EB0B3CCE80BA0ACBA03CFBFE229AD3590F7F913CEB3F8378D5DCB93A427114DE
SHA-512:	6459017B3CB56B80CC43B82AAFF88292C05F9BE64B7376F4415CE98195F7C9F865BD8B9281963BE029AA524892E0D82082681C07B64FF3D64A9E25BDC352C7DD
Malicious:	false
Reputation:	unknown
Preview:	5j49fLc19681366ouR45..8RY68801988Bz7e1ZrHp3Ex23aIVZ0R595wqSIhg3t71SrM4vn2miABgU35Q96c962N705z7a89b4g06Afom6wv15d21v188HE5q0L2knf4K 35oUA4T69rS05om513IMN3Ex732S0rVFWUL2Y1189xU41..J284Z9E91..818Kd25e4zy98Rz0O47fa1P4rM5n0E31M4y28vo17ED7OcX12Q9resPDP7476M8705AfaD7k Lo48zP6eo1Flw16m3nR1R49..n7t0Qyg75X9690jy3Jt..hr7646vZQTx..33y09l4nlA3r3SCKa4V048zNJ03Aoj7j86X37uw432spt422W2R214h49T88X6r25seOA49 t036012m9431y..aT10t77B17F6v49vf5Z6396aCs5yXI67L..82Y17500C2Q9h4ZPGYnlgJ494Vj8i9ycwdx..n838TDIeI2PEA97NECz8ff5yO6z31CT0VAMpp6z4126 499O1W90Sof9lcyC1M00i73iAP829p523u8Q3949f2DBeFa45j1T95uO882p..

C:\Users\user\AppData\Local\Temp\33911166\uetndqd.dat	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	543
Entropy (8bit):	5.575912124605288
Encrypted:	false
SSDEEP:	
MD5:	6E7FF95EA98F7C0131B3CF7359F58AA4
SHA1:	78FF124AB67972F7ECC64B4BEF0B8F77B8E182FB
SHA-256:	6E5191C99610CA5611A7F7A68F45239BB4E22B904D96E2F2DB8D24112A540FBA
SHA-512:	B2312BD0C8F8C84FE21D4C6981856573CA5DB7C07989943D75020AE1211BFCEE6A1B5D7F1D74966D068BD442BB96BBED9B379747EAFAA8FEBC6E8CD28FE45214
Malicious:	false
Reputation:	unknown
Preview:	veLkqnBL4Pj200kuJ4O2pV4228j54ju5UgkZ4N514JyW0RS54y53j81AkCf3OFV547TJ2771As82Ioi2rePm5t4LJhr02Aje9LcGAkV5C26McT351DwSYF8m9ZXFVi6D02 1zbkg8jAD6JDVM9iOw55Ug667P37a3G71XLpP9i270Rw81u8..08zl4k50Gwh0rWK6370m1MDJ8ljue301f287B40d982E730YVcGv82Q362ah5C919Z12PZMHEQS166fM 9d94U5V70D439q2KgHcBU980..9801wV706S3m63cu4X16Er6qYn651GO6n48W3977NWf2hs28mGcu703d30wIe6Eb8818knP6RgnlidDZ3903J442Ps715605lMG8d0EU Vv39760Sz2XiP2KKGkJ7A9g8..TRNG1o14b1886iq447d03m8427V8ED6QlhmEe057uT68vbQB30HV6o4Mt942R495nBu5SH5d..j6g0gahF8Bc40Fl96C09Yyr1835lZ2 VH292X4jqEeYt4Zk40U1V..

C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	777456
Entropy (8bit):	6.353934532007735
Encrypted:	false
SSDEEP:	
MD5:	8E699954F6B5D64683412CC560938507
SHA1:	8CA6708B0F158EACCE3AC28B23C23ED42C168C29
SHA-256:	C9A2399CC1CE6F71DB9DA2F16E6C025BF6CB0F4345B427F21449CF927D627A40
SHA-512:	13035106149C8D336189B4A6BDAF25E10AC0B027BAEA963B3EC66A815A572426B2E9485258447CF1362802A0F03A2AA257B276057590663161D9D55D5B737B02
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.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..... ....@.....0.....@...@.....@.....T.....c..... ..D..... .....text..... ..`.rdata..... .....@..@.data...X.....h.....@....rsrc.....R.....@..@.reloc...u.....v...H.....@..B..... ....

C:\Users\user\AppData\Local\Temp\33911166\viah.xls	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	626
Entropy (8bit):	5.540591955140838
Encrypted:	false
SSDEEP:	
MD5:	39583EFD61806B202DC523FE9CDA7EE8
SHA1:	0B9870CBAFCFD8017719B7EFB0FF192C04F73946
SHA-256:	8D13B7155EAB011986B11319C58A49145BB3290E6CA6C1F41758365739C07496
SHA-512:	A66CA5978DBC2EEFD608CF08BB87CEB8DEFAF570353B8417417C6C39E72119298D31D74BFFAE495F2532B9B5FE54FDDDCCC1259DD350209ECD5338C222505(DE
Malicious:	false
Reputation:	unknown
Preview:	7s8b4LG3Y20r0515Zv5G82g30196JD5XX16965Vi80gN9FiV3655838CdG06x2N82Q250a4g5y34Z4X2SXb8e5rd5J47xu0xQBKJ1h6bjOtLt16PeU7lQ0Xsam35NQ6mwY m5K1242Kp6..kQgr8yYw6N13ncn4D9GW0So986UTudHnI4o..h3h4eZ3970E367d738348zs11J6wdyc62Mv5..g4vFGv..NN1iX10Fsc5eor908udBY75Hv8..0kb46VB n7FUQ8591k21g13pL3tMW99b0sM5u45CsMkPDj02l3RzF7C421YmdV0h9f0h33P213u9i0QWklf5RFkE1ebTl808jU39490066I056bVN44l..MHo4CI0jq93U1768re35 em7VD08F37321LElf87663MD1ar8418790klw4520Q59ut4E7t99vk88QBl8N3C..496u120J73F836Xm13oIs3N59d764wm65619pn8ZEJTIH2cr563g4ClS7x3t95Z0i pi50eRn355He47Rr8239MY27OPwySex53yTPgbf53P44y2bh7NPIyi3z0Y121Z7sSeO9772759zur0GVd13GfP7h8967f83Y7C378YlJ..

C:\Users\user\AppData\Local\Temp\33911166\vvspktn.docx	
Process:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	566
Entropy (8bit):	5.503301815812772
Encrypted:	false
SSDEEP:	
MD5:	F50497247FF0B9655419829B94AAB136
SHA1:	87BFA58A7442428899D2CFEFB207DF673FB37919
SHA-256:	754CD760794897FCF41FC99EADAD2E31F125653E8A2A7398288E746BAC1C9881
SHA-512:	CA57A5C1254520EA59E6D31CD8751F2508EA61618606226CCD9E41CF57C23257D974D6B23C665B983B5B78047950687359592 4F87160A816A3F3F511AE27750D
Malicious:	false
Reputation:	unknown
Preview:	4RGr4a447sj6C1C384..55o8lt0n4ycuW2iQ4A94l74PU469qf7msQ8Mi072B2x5td0N5Px119rK13zYX7l67m..xK11m895U47vh902Bg187oqL678yk120pg444..qW8 T30A3S2sMtql8td738jkl0y3Gn7jEf1yH0jT8r554Y28N1Ua90lwt1639614ce34396jF61e29kBFC2..i2YFXAXC130tR57..kU016pE80FG0x361817FVI47P770EeU7 Z33B83v775TOdL3R53Q3vB0Z9I9d368708A9AT0V17jh9P1E1tGX5eC0yp7sw3n3lBO6B4236276531EadB01153g20Z02yUf362r9iO47..40yB02M841HH8..1Y9Qwmd iK71d4PGI30886993XHV22m7rV7OGr2sqLhgzzxHT687e5pKnDOm4c2u3Q5y2B7LR74Kn1b05130238r9001sCXi778WC46E20L91wCA85Xx1c0624v3290SKrPLxdeA68 13a7U5kMfcnwBwwTeB6r149EG1dwE2bs1Qr0Mqa29SYJ..

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
Process:	C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.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**
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\RegSvcs.exe	
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\tmp2BE4.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\tmp2F02.tmp	
Process:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	
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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	
MD5:	09F439F8276044197F56C9B93E11E0A8
SHA1:	8EE20441D07988E58B2594DDD07B87D13FFD08B8
SHA-256:	EA4302CC1AE911347FEF20023AEDCBBBD32FAFB4FA5126B1A76E556B4B00C0CE
SHA-512:	14B40E1B79510346B54239BECDE54890F6C44D0410B78FD8D7856352691C7D7D34419A601B3C76472462A1E7982AB4E37BE0809360B9F1C9019FAE915AE38A28
Malicious:	**true**
Reputation:	unknown
Preview:	).....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\gdljljtq.cpl	
Process:	C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	78
Entropy (8bit):	4.830274579293434
Encrypted:	false
SSDEEP:	
MD5:	516DFE5000E662A83C141F92FD1F5BCE
SHA1:	A96118D40F41AE06A8E3CAEAD9052F45D28692FC
SHA-256:	3A2E9484A8ED6BB903A1C03DA059D22F463608CD2BBDBBA833EE4F81C628BBA8
SHA-512:	22A8E5264B6BA380FC313087BF1515988D453111BDF0BCB8EB1F07460333FA5E066819F4BC20BDB75CA48A5F70E1F7EFECA526EEB75E8D1E3743D6642A068B9
Malicious:	false
Reputation:	unknown
Preview:	[S3tt!ng]..stpth=%temp%..Key=Chrome..Dir3ctory=33911166..ExE_c=upstsdssm.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):	7.8363360657594985

General

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:	KRSEL0000056286.JPG.exe
File size:	1096674
MD5:	d6f040b4d7d217b8525dff843feba635
SHA1:	8ed8beaceddf8e8e9ba4b601d1e985e5c7c2d7d9
SHA256:	940ad66c876976f4a05f12710687f5abb76443f693dd3986d1ff7a4c73fc866f
SHA512:	fcbd072ba0b64e41931cf9e5bb8b2b73fd18ee9788907f1791cb13a52450e5bc81732f7fcd0d8d4af737cca4e9b59658a5292129848dbb9a7197aa86e405a4b7
SSDEEP:	24576:rAOcZEhIj7BkIMcXzBQuX+a6TPY5I7nT1RMwaz7:t8GI3XXN6c5IzTXM7P
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:	b491b4ecd336fb5b

Static PE Info

General

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

Entrypoint Preview

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x62000	0x4c28	0x4e00	False	0.602263621795	data	6.36874241417	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x67000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-08:49:24.622129	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65298	8.8.8.8	192.168.2.4
10/13/21-08:49:30.043800	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59123	8.8.8.8	192.168.2.4
10/13/21-08:50:01.852937	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56534	8.8.8.8	192.168.2.4
10/13/21-08:50:27.576419	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64801	8.8.8.8	192.168.2.4
10/13/21-08:50:59.183707	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55046	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 08:49:24.601938963 CEST	192.168.2.4	8.8.8.8	0x3741	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:30.023174047 CEST	192.168.2.4	8.8.8.8	0x9c44	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:35.296396971 CEST	192.168.2.4	8.8.8.8	0x73f7	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:56.480530024 CEST	192.168.2.4	8.8.8.8	0xddf6	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:01.832587004 CEST	192.168.2.4	8.8.8.8	0x3ccd	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:06.958302975 CEST	192.168.2.4	8.8.8.8	0x105c	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:27.557086945 CEST	192.168.2.4	8.8.8.8	0xc403	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:33.346246004 CEST	192.168.2.4	8.8.8.8	0x3f56	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:38.527420998 CEST	192.168.2.4	8.8.8.8	0xaa96	Standard query (0)	strongodss.ddns.net	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 08:50:59.161433935 CEST	192.168.2.4	8.8.8.8	0xc626	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:51:04.375217915 CEST	192.168.2.4	8.8.8.8	0x468	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Oct 13, 2021 08:51:09.531922102 CEST	192.168.2.4	8.8.8.8	0xabe8	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
Oct 13, 2021 08:49:24.622128963 CEST	8.8.8.8	192.168.2.4	0x3741	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:30.043800116 CEST	8.8.8.8	192.168.2.4	0x9c44	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:35.314847946 CEST	8.8.8.8	192.168.2.4	0x73f7	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:49:56.498676062 CEST	8.8.8.8	192.168.2.4	0xddf6	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:01.852936983 CEST	8.8.8.8	192.168.2.4	0x3ccd	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:06.976814985 CEST	8.8.8.8	192.168.2.4	0x105c	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:27.576419115 CEST	8.8.8.8	192.168.2.4	0xc403	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:33.364629030 CEST	8.8.8.8	192.168.2.4	0x3f56	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:38.546122074 CEST	8.8.8.8	192.168.2.4	0xaa96	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:50:59.183706999 CEST	8.8.8.8	192.168.2.4	0xc626	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:51:04.393402100 CEST	8.8.8.8	192.168.2.4	0x468	No error (0)	strongodss .ddns.net		185.19.85.175	A (IP address)	IN (0x0001)
Oct 13, 2021 08:51:09.551088095 CEST	8.8.8.8	192.168.2.4	0xabe8	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: KRSEL0000056286.JPG.exe PID: 6976 Parent PID: 2432

General

Start time:	08:49:02
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\KRSEL0000056286.JPG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KRSEL0000056286.JPG.exe'
Imagebase:	0xa30000
File size:	1096674 bytes
MD5 hash:	D6F040B4D7D217B8525DFF843FEBA635
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: upstsdssm.pif PID: 6032 Parent PID: 6976

General

Start time:	08:49:11
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif' sqbr.wlw
Imagebase:	0x950000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.688014335.0000000004B63000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.688014335.0000000004B63000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.688014335.0000000004B63000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.689229706.0000000004AFA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.689229706.0000000004AFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.689229706.0000000004AFA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.689830421.0000000004B2E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.689830421.0000000004B2E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.689830421.0000000004B2E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.691685371.0000000003D67000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.691685371.0000000003D67000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000002.00000003.691685371.0000000003D67000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.687930988.0000000004A91000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.687930988.0000000004A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.687930988.0000000004A91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.689465374.0000000004AC6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.689465374.0000000004AC6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.689465374.0000000004AC6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.687770374.0000000004A91000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.687770374.0000000004A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.687770374.0000000004A91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.687890008.0000000004AC6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.687890008.0000000004AC6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.687890008.0000000004AC6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.689659391.0000000004B2E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.689659391.0000000004B2E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.689659391.0000000004B2E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.687860827.0000000003D67000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.687860827.0000000003D67000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.687860827.0000000003D67000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.690506336.0000000004A91000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.690506336.0000000004A91000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.690506336.0000000004A91000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.687835172.0000000004AFA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.687835172.0000000004AFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.687835172.0000000004AFA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.688888724.0000000004B63000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.688888724.0000000004B63000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.688888724.0000000004B63000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 32%, 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: 6404 Parent PID: 6032

General

Start time:	08:49:16
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0xef0000
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: 00000005.00000002.926541928.00000000036F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.928515040.00000000063A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.928515040.00000000063A0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.927287391.0000000004739000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.927287391.0000000004739000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.928459238.0000000006380000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.928459238.0000000006380000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.925657154.0000000001302000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.925657154.0000000001302000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.925657154.0000000001302000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.928835225.0000000006FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.928835225.0000000006FB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.928835225.0000000006FB0000.00000004.00020000.sdmp, Author: Joe Security
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: 5036 Parent PID: 6404

General

Start time:	08:49:21
Start date:	13/10/2021
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\tmp2BE4.tmp'
Imagebase:	0xc40000
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: 5560 Parent PID: 5036

General

Start time:	08:49:21
Start date:	13/10/2021
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: 5312 Parent PID: 6404

General

Start time:	08:49:22
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp2F02.tmp'
Imagebase:	0xc40000
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: 5492 Parent PID: 5312

General

Start time:	08:49:22
Start date:	13/10/2021
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: 5484 Parent PID: 968

General

Start time:	08:49:22
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe 0
Imagebase:	0x490000
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: 1372 Parent PID: 5484

General

Start time:	08:49:23
Start date:	13/10/2021
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: 5108 Parent PID: 968

General

Start time:	08:49:25
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xd60000
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%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 3280 Parent PID: 5108

General

Start time:	08:49:25
Start date:	13/10/2021
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

Copyright Joe Security LLC 2021

Analysis Process: upstsdssm.pif PID: 3296 Parent PID: 3424

General

Start time:	08:49:26
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\33911166\upstsdssm.pif
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\33911166\UPSTSD~1.PIF' C:\Users\user\AppData\Local\Temp\33911166\sqbr.wlw
Imagebase:	0x950000
File size:	777456 bytes
MD5 hash:	8E699954F6B5D64683412CC560938507
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: 0000000F.00000003.720524354.0000000004651000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720524354.0000000004651000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720524354.0000000004651000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720574571.00000000046BA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720574571.00000000046BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720574571.00000000046BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720414849.0000000003967000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720414849.0000000003967000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720414849.0000000003967000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720446261.0000000004686000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720446261.0000000004686000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720446261.0000000004686000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.722243638.0000000004723000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.722243638.0000000004723000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.722243638.0000000004723000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.723424340.00000000046EE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.723424340.00000000046EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.723424340.00000000046EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.723331373.00000000046EE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.723331373.00000000046EE000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.723331373.00000000046EE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.723579153.0000000003967000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.723579153.0000000003967000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.723579153.0000000003967000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.723493908.0000000004651000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.723493908.0000000004651000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.723493908.0000000004651000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720373529.00000000046BA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720373529.00000000046BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720373529.00000000046BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720687094.00000000046EF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720687094.00000000046EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720687094.00000000046EF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720808959.0000000004757000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720808959.0000000004757000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720808959.0000000004757000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720643972.00000000046EF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720643972.00000000046EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720643972.00000000046EF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720715564.0000000004723000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720715564.0000000004723000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720715564.0000000004723000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.722731102.00000000046BA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.722731102.00000000046BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.722731102.00000000046BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.723107754.0000000004686000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.723107754.0000000004686000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.723107754.0000000004686000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000003.720259774.0000000004651000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000003.720259774.0000000004651000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000003.720259774.0000000004651000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities | Show Windows behavior

Analysis Process: RegSvcs.exe PID: 7128 Parent PID: 3296

General

Start time:	08:49:32
Start date:	13/10/2021
Path:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegSvcs.exe
Imagebase:	0x5e0000
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: 00000012.00000002.742141197.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.742141197.0000000002F11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.741599350.00000000009B2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.741599350.00000000009B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.741599350.00000000009B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.742225136.0000000003F19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.742225136.0000000003F19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities | Show Windows behavior

File Created

File Read

Analysis Process: wscript.exe PID: 6200 Parent PID: 3424

General

Start time:	08:49:34
Start date:	13/10/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\33911166\Update.vbs'
Imagebase:	0x7ff65ee40000
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

Copyright Joe Security LLC 2021

Analysis Process: dhcpmon.exe PID: 6440 Parent PID: 3424

General

Start time:	08:49:42
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xf50000
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: 2600 Parent PID: 6440

General

Start time:	08:49:42
Start date:	13/10/2021
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021