ID: 395218
Sample Name: notifica2104.msi
Cookbook: default.jbs
Time: 10:17:10
Date: 22/04/2021
Version: 31.0.0 Emerald

Table of Contents

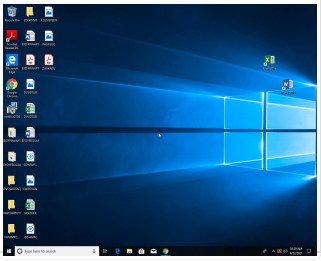
Analysis Report notifica2104.msi

Overview

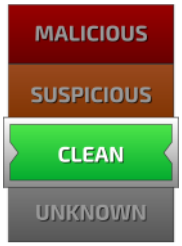
General Information

Sample Name:	notifica2104.msi
Analysis ID:	395218
MD5:	37261a4c059499..
SHA1:	1c06fb8a5bf94db..
SHA256:	f3316d7cef4978e..
Infos:	

Most interesting Screenshot:



Detection

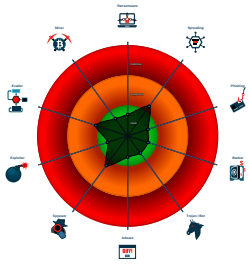


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Checks for available system drives …
- Monitors certain registry keys / valu…
- Queries the volume information (nam…
- Sample file is different than original …
- Tries to load missing DLLs

Classification



Analysis Advice

Sample is looking for USB drives. Launch the sample with the USB Fake Disk cookbook

Sample tries to load a library which is not present or installed on the analysis machine, adding the library might reveal more behavior

Startup

- **System is w10x64**
- msiexec.exe (PID: 6560 cmdline: 'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\notifica2104.msi' MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 6616 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 62996ADAF98AEA6C3E76201DA1491D0F MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- **cleanup**

Malware Configuration

No configs have been found

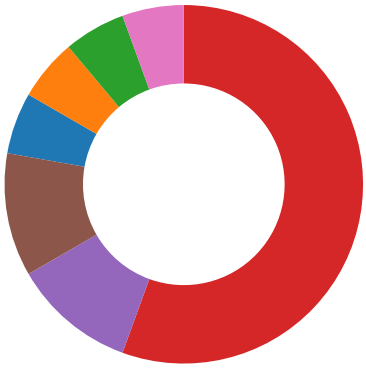
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Spreading
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Language, Device and Operating System Detection

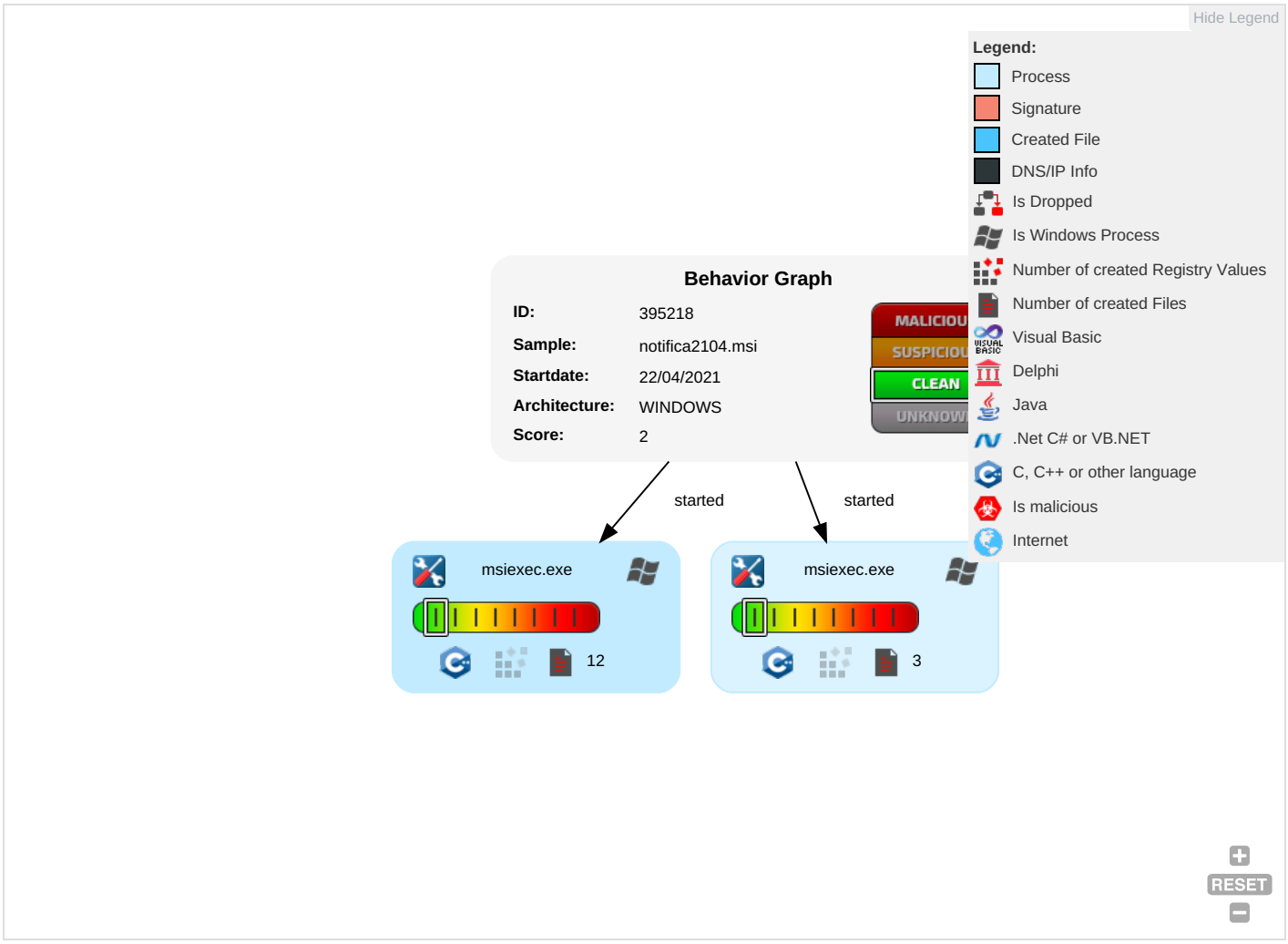
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Replication Through Removable Media 1	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Process Injection 1	OS Credential Dumping	Query Registry 1	Replication Through Removable Media 1	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mc Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	DLL Side-Loading 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Peripheral Device Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bil Fra
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Ma Ap Ra or

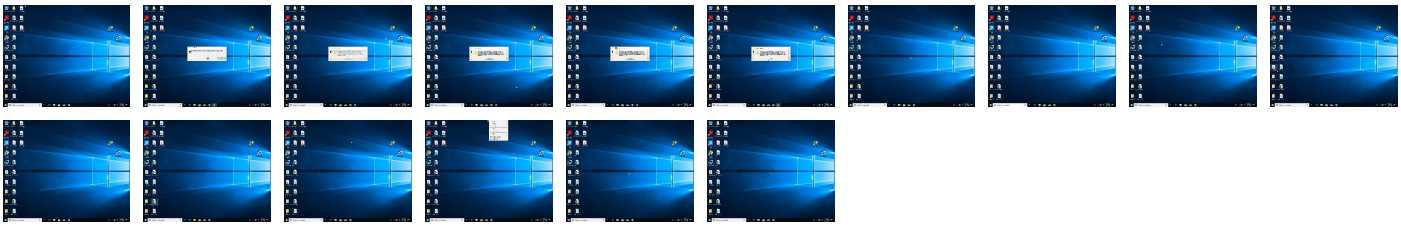
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
notifica2104.msi	5%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.advancedinstaller.com	notifica2104.msi	false		high
http://www.winimage.com/zLibDll	notifica2104.msi	false		high
http://https://www.thawte.com/cps0/	notifica2104.msi	false		high
http://www.winimage.com/zLibDll1.2.7rbr	notifica2104.msi	false		high
http://https://www.thawte.com/repository0W	notifica2104.msi	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	395218
Start date:	22.04.2021
Start time:	10:17:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	notifica2104.msi
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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean2.winMSI@2/1@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .msi

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 93.184.220.29, 52.255.188.83, 20.82.210.154, 104.43.193.48, 92.122.145.220, 40.71.254.118, 23.57.80.111, 52.147.198.201, 92.122.213.247, 92.122.213.194, 104.43.139.144, 2.20.142.209, 2.20.142.210, 20.54.26.129, 20.82.209.183 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, conlazionzzytz.eastus.cloudapp.azure.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Execution Graph export aborted for target msiexec.exe, PID 6616 because there are no executed function • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\MSIe9f32.LOG	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	72030
Entropy (8bit):	3.750914117199054
Encrypted:	false
SSDEEP:	768:Wc2+wE8XjcRxMLzsU6Ij0ZMPyu56MQWKfuMwpp4:lw3XjcRxMLzsUHMmA9
MD5:	ECD9E34B90D5ECF8B46646B87214B796
SHA1:	843A47629F2DB8A37E81AF8EEB22514054D7DB86
SHA-256:	665B770AAAA93066B77C590BFF56C4DA8133B6ADE318F737C911F2705007696A
SHA-512:	BEDFA650971EE53D7821573E2A95B1A1AD70AC4E943F0ABCA649BF6C879C9BD0939A306E70843870F090DD47A27FE88D47279F2FD8DD83CF76311292B10CEB8
Malicious:	false
Reputation:	low
Preview:	..=.=.=. .V.e.r.b.o.s.e. .l.o.g.g.i.n.g. .s.t.a.r.t.e.d.:. .4./.2.2./.2.0.2.1. . .1.0.:.1.8.:.0.3. . .B.u.i.l.d. .t.y.p.e.:. .S.H.I.P. .U.N.I.C.O.D.E. .5...0.0...1.0.0.1.1...0.0. . .C.a.l.l.i.n.g. .p.r.o.c.e.s.s.:. .C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.m.s.i.e.x.e.c...e.x.e. .=.=.=.....M.S.I. .(.c.). .(.A.0.:.A.4.). .[.1.0.:.1.8.:.0.3.:.3.8.2.].:. .F.o.n.t. .c.r.e.a.t.e.d... . .C.h.a.r.s.e.t.:. .R.e.q.=.0.,. .R.e.t.=.0.,. .F.o.n.t.:. .R.e.q.=.M.S. .S.h.e.l.l. .D.l.g.,. .R.e.t.=.M.S. .S.h.e.l.l. .D.l.g.....M.S.I. .(.c.). .(.A.0.:.A.4.). .[.1.0.:.1.8.:.0.3.:.3.8.2.].:. .F.o.n.t. .c.r.e.a.t.e.d... . .C.h.a.r.s.e.t.:. .R.e.q.=.0.,. .R.e.t.=.0.,. .F.o.n.t.:. .R.e.q.=.M.S. .S.h.e.l.l. .D.l.g.,. .R.e.t.=.M.S. .S.h.e.l.l. .D.l.g.....M.S.I. .(.c.). .(.A.0.:.B.C.). .[.1.0.:.1.8.:.0.3.:.4.2.9.].:. .R.e.s.e.t.t.i.n.g. .c.a.c.h.e.d. .p.o.l.i.c.y. .v.a.l.u.e.s.....M.S.I. .(.c.). .(.A.0.:.B.C.). .[.1.0.:.1.8.:.0.3.:.4.2.9.].:. .M.a.c.h.i.n.e. .p.o.l.i.c.y. .v.a.l.u.e. .'.D.e.b.u.g.'. .i.s. .0.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Dec 11 11:47:44 2009, Security: 0, Code page: 1252, Revision Number: {3191CFA1-AA45-460E-9697-93F9CFDE492F}, Number of Words: 10, Subject: Windows update, Author: Windows update, Name of Creating Application: Advanced Installer 16.2 build 436ecd62, Template: ;1040, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Entropy (8bit):	6.5591101160185925
TrID:	• Microsoft Windows Installer (77509/1) 52.18% • Windows SDK Setup Transform Script (63028/2) 42.43% • Generic OLE2 / Multistream Compound File (8008/1) 5.39%
File name:	notifica2104.msi
File size:	1040384
MD5:	37261a4c059499f3d379f539834b8990
SHA1:	1c06fb8a5bf94db2782bf49e080eacc25e740d7c
SHA256:	f3316d7cef4978eb334264f709301d6616089abd6272c675228614a6407ed629
SHA512:	79a543a730e9e4f6e2393210d548b54ef20af0b2fbcc79ef0fc95a893531407f701b9f2862fd5975f65747caaa057543d2f4633603c047ab35f257386c486b98
SSDEEP:	24576:ZGnFId/5IqVXCWJr6Awb2DRMIHBPHofTl6VQU1YHYlo:ZG85IqVXCWJr6AwbuLBPHKTl6VQU1YHD

General

File Content Preview:	.....>.....|..... .....x...y...z...{...|...}...~..... .....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "notifica2104.msi"

Indicators

Has Summary Info:	True
Application Name:	Advanced Installer 16.2 build 436ecd62
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary

Code Page:	1252
Title:	Installation Database
Subject:	Windows update
Author:	Windows update
Keywords:	Installer, MSI, Database
Comments:	
Template:	;1040
Last Saved By:	
Revion Number:	{3191CFA1-AA45-460E-9697-93F9CFDE492F}
Last Printed:	2009-12-11 11:47:44.850000
Create Time:	2009-12-11 11:47:44.850000
Last Saved Time:	2009-12-11 11:47:44.850000
Number of Pages:	200
Number of Words:	10
Creating Application:	Advanced Installer 16.2 build 436ecd62
Security:	0

Streams

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 504

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	504
Entropy:	4.26726860141
Base64 Encoded:	True
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . $ . . . . . 0 . . . . . ` . . . . . p . . . . . | . . . . . @ . . . # . . W z . . @ . . . # . . W z . . @ . . . # . . W z . . . . . ' . . . { 3 1 9 1 C F A 1 - A A
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 c8 01 00 00 10 00 00 00 0b 00 00 00 88 00 00 00 0c 00 00 00 94 00 00 00 0d 00 00 00 a0 00 00 00 13 00 00 00 ac 00 00 00 01 00 00 00 b4 00 00 00 09 00 00 00 bc 00 00 00 0f 00 00 00 ec 00 00 00 03 00 00 00 f4 00 00 00 04 00 00 00 0c 01 00 00

Stream Path: \x17163\x16689\x18229\x15358\x17388\x15912\x16947\x16693\x17207\x17522\x18358\x17383\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 474784

General	
Stream Path:	\x17163\x16689\x18229\x15358\x17388\x15912\x16947\x16693\x17207\x17522\x18358\x17383\x18479
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	474784
Entropy:	6.57645171277
Base64 Encoded:	True
Data ASCII:	M Z . . . . . @ . . . . . (. . . . . ! . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . . (. . } { . . } { . . } { . . ~ z . . } { . . x z | . } { . . y z . . } { F . y z . . } { F . ~ z . . } { F . x z . . } { . . y z . . } { . . ~ z . . } { . . | z . . } { . . | { . . } { . . t z . . } { . . } z . . } { . . . { . . } { . . . { . . } {
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x15870\x18088, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x15870\x18088
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.03444158006
Base64 Encoded:	False
Data ASCII:	. . . . . (. . . . . (. . . . .
Data Raw:	00 00 01 00 01 00 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x16318\x18483, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x16318\x18483
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.03693614652
Base64 Encoded:	False
Data ASCII:	. . . . . (. . . . . (. . . . .
Data Raw:	00 00 01 00 01 00 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x16702\x16812\x17848\x16695\x17894\x16894\x17391, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 381088

General	
Stream Path:	\x17163\x16689\x18229\x16702\x16812\x17848\x16695\x17894\x16894\x17391
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	381088
Entropy:	6.41664010965
Base64 Encoded:	True
Data ASCII:	M Z . . . . . @ . . . . . ! . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . . m . . +) k . x) k . x) k . x L . . y ' k . x L . . y . k . x . . . y 9 k . x . . . y ? k . x . . . y n k . x L . . y 0 k . x L . . y (k . x L . . y 6 k . x) k . x k j . x (. . y f k . x (. . y (k . x (. S x (k . x) k ; x (k . x (. . y (k . x

General	
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18485, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x59, frames 3, Stream Size: 2818

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18485
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x59, frames 3
Stream Size:	2818
Entropy:	7.55703063679
Base64 Encoded:	True
Data ASCII:	. . . . . . J F I F . . . . C . . . . $. ' " , # . . (7) , 0 1 4 4 4 . ' 9 = 8 2 < . 3 4 2 . . . C . . . . 2 ! . ! 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 . . . . . . ; . . . . " . . . . } . . . . ! 1 A . . Q a . " q . 2 . . . . #
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 08 06 06 07 06 05 08 07 07 07 09 09 08 0a 0c 14 0d 0c 0b 0b 0c 19 12 13 0f 14 1d 1a 1f 1e 1d 1a 1c 1c 20 24 2e 27 20 22 2c 23 1c 1c 28 37 29 2c 30 31 34 34 34 1f 27 39 3d 38 32 3c 2e 33 34 32 ff db 00 43 01 09 09 09 0c 0b 0c 18 0d 0d 18 32 21 1c 21 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32

Stream Path: \x17163\x16689\x18229\x16830\x16880\x17199\x17329\x17764\x17589\x18490, File Type: MS Windows icon resource - 3 icons, 16x16, 16 colors, 4 bits/pixel, 16x16, 8 bits/pixel, Stream Size: 2862

General	
Stream Path:	\x17163\x16689\x18229\x16830\x16880\x17199\x17329\x17764\x17589\x18490
File Type:	MS Windows icon resource - 3 icons, 16x16, 16 colors, 4 bits/pixel, 16x16, 8 bits/pixel
Stream Size:	2862
Entropy:	3.16043065194
Base64 Encoded:	False
Data ASCII:	. . . . (. . . 6 . . . . h . . . ^ . . . . h . . . . (. . . . w v . . . . . " " " " o . . " " " " " o . . w w w " " . . . . . . " / . . . .
Data Raw:	00 00 01 00 03 00 10 10 10 00 00 00 04 00 28 01 00 00 36 00 00 00 10 10 00 00 00 00 08 00 68 05 00 00 5e 01 00 00 10 10 00 00 00 00 20 00 68 04 00 00 c6 06 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0

Stream Path: \x17163\x16689\x18229\x16830\x17458\x17395\x17896\x18476, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x16830\x17458\x17395\x17896\x18476
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.35906224297
Base64 Encoded:	True
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . w . . . . { . . . . p . . . . x . { . w p . . . . { . w . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x16830\x17848\x17207\x17574\x18481, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x16830\x17848\x17207\x17574\x18481
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.29856879699
Base64 Encoded:	True

General	
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . w . . . . { . . . . p . . . . x . { . w p . . . . { . w . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18474, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 500x316, frames 3, Stream Size: 11791

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18474
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 500x316, frames 3
Stream Size:	11791
Entropy:	7.71486251579
Base64 Encoded:	True
Data ASCII:	. . . . . . J F I F . . . . C . . . . C . . . . < . . . . s .
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff db 00 43 00 04 02 03 03 02 04 03 03 03 04 04 04 04 05 09 06 05 05 05 05 0b 08 08 06 09 0d 0b 0d 0d 0d 0b 0c 0c 0e 10 14 11 0e 0f 13 0f 0c 0c 12 18 12 13 15 16 17 17 17 0e 11 19 1b 19 16 1a 14 16 17 16 ff db 00 43 01 04 04 04 05 05 05 0a 06 06 0a 16 0f 0c 0f 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16 16

Stream Path: \x17163\x16689\x18229\x16958\x16827\x16687\x17200\x18470, File Type: MS Windows icon resource - 1 icon, 32x32, 16 colors, Stream Size: 766

General	
Stream Path:	\x17163\x16689\x18229\x16958\x16827\x16687\x17200\x18470
File Type:	MS Windows icon resource - 1 icon, 32x32, 16 colors
Stream Size:	766
Entropy:	3.3484862649
Base64 Encoded:	True
Data ASCII:	. . . . (. . . . . . @ . . . . 3 3 1 . . . . 3 3 2 3 3 3 3 3 3 3 3 3 3 3 . 3 3 $ D D D D D D D D D D D D @ 1 . 2 D D D D D D D D D D D D D D . . 2 D D D D D D @ D D D D D D C . 2 D D D D D D 3 4 D D D D D C . 2 D D D D D @ 3 0 D D D D D . . 3 $ D D D D D 3 4 D D D D D 1 . 3 $
Data Raw:	00 00 01 00 01 00 20 20 10 00 00 00 00 00 e8 02 00 00 16 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 c0 c0 00 80 80 80 00 00 80 80 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 33

Stream Path: \x17163\x16689\x18229\x17214\x17009\x18482, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors, Stream Size: 1078

General	
Stream Path:	\x17163\x16689\x18229\x17214\x17009\x18482
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors
Stream Size:	1078
Entropy:	2.86422695486
Base64 Encoded:	False
Data ASCII:	. . . . & . . . . (. . . . . . . (. . . . . . @ . . . . p . . . . w p . . . . p . . . . p . . . . p . . . . p . . . . w w . . . w w . . . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 10 10 10 00 00 00 00 00 28 01 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0 c0 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17214\x17841\x17207\x17574\x18481, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x17214\x17841\x17207\x17574\x18481
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32

General	
Stream Size:	2998
Entropy:	4.40653521205
Base64 Encoded:	True
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . { . . . . w . . . . p . . x . . . . w . . . . x . . . w . . w . . . . . . p . . x x . . w ~ . . . . x . . . . . ~ . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17790\x17448\x18034\x16812\x18482, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x17790\x17448\x18034\x16812\x18482
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.92283562852
Base64 Encoded:	False
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . p . . . . w . . . . . . w w . . . . w . f . w . . . . w . . . . . v v f . w . . . . n f f l . w . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17790\x17640\x17188\x17205\x18470, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x17790\x17640\x17188\x17205\x18470
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.6676615263
Base64 Encoded:	True
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . w . . . . { . . . . p . . . . x . { . w p . . . . . . (. . . { . w . . . . (x x x . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17918\x16740\x16677\x17318, File Type: PC bitmap, Windows 3.x format, 1 x 200 x 24, Stream Size: 854

General	
Stream Path:	\x17163\x16689\x18229\x17918\x16740\x16677\x17318
File Type:	PC bitmap, Windows 3.x format, 1 x 200 x 24
Stream Size:	854
Entropy:	3.80253159876
Base64 Encoded:	False
Data ASCII:	B M V . . . . 6 . . . (. . . .
Data Raw:	42 4d 56 03 00 00 00 00 00 00 36 00 00 00 28 00 00 00 01 00 00 00 c8 00 00 00 01 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 e f3 f4 00 ef f3 f4 00 ef f3 f4 00 ef f4 f4 00 ef f4 f4 00 ef f4 f5 00 ef f4 f5 00 ef f4 f5 00 ef f4

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 1408

General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data

General	
Stream Size:	1408
Entropy:	4.92326571992
Base64 Encoded:	False
Data ASCII:	. . . . $. $. + . + . + . + . + . + . + . + . + . + . 5 . 5 . 5 . 5 . : . : . = . = . = . = . = . = . B . B . B . B . B . B . B . B . B . B . B . B . D . D . D . D . D . D . D . D . D . D . P . P . P . P . P . P .] .] . _ . _ . a . a . a . a . a . a . d . d . d . d . d . g . g . g . g . g . g . g . k . k . k . k . k . k . k . k . k . r . r . r . r . r . r . w . w . w . z . z . z . z . z . . . .
Data Raw:	05 00 05 00 05 00 07 00 07 00 07 00 11 00 11 00 11 00 1b 00 1b 00 1e 00 1e 00 1e 00 1e 00 1e 00 1e 00 24 00 24 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 35 00 35 00 35 00 35 00 3a 00 3a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 50 00

Stream Path: \x18496\x15498\x15359\x17388\x15208\x18098\x17393\x16690\x18471, File Type: basic-16 executable (TV), Stream Size: 12

General	
Stream Path:	\x18496\x15498\x15359\x17388\x15208\x18098\x17393\x16690\x18471
File Type:	basic-16 executable (TV)
Stream Size:	12
Entropy:	2.61749246118
Base64 Encoded:	False
Data ASCII:	C . D . E . F . G . . .
Data Raw:	43 01 44 01 45 01 46 01 47 01 19 80

Stream Path: \x18496\x15518\x16925\x17915, File Type: data, Stream Size: 444

General	
Stream Path:	\x18496\x15518\x16925\x17915
File Type:	data
Stream Size:	444
Entropy:	5.38678705165
Base64 Encoded:	False
Data ASCII:	: . . . . ! . # . % .) . + . - . / . 1 . 4 . 6 . 8 . : . < . > . @ . B . D . F . H . J . L . N . P . R . T . V . X . Z . \\ . ^ . ` . b . d . f . g . i . k . 3 . . . .
Data Raw:	3a 01 9b 06 9d 06 9e 06 a0 06 a2 06 a4 06 a5 06 a7 06 a8 06 aa 06 ac 06 ad 06 af 06 b1 06 b2 06 b4 06 b6 06 b8 06 ba 06 bc 06 be 06 bf 06 c1 06 c3 06 c5 06 c7 06 c9 06 cb 06 cd 06 cf 06 d1 06 d3 06 d4 06 d6 06 d8 06 da 06 dc 06 de 06 e0 06 e2 06 e4 06 e6 06 e8 06 ea 06 ec 06 ee 06 f0 06 f2 06 f4 06 f6 06 f8 06 fa 06 fc 06 fe 06 00 07 02 07 04 07 06 07 08 07 0a 07 0c 07 0e 07 0f 07

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: ISO-8859 text, with very long lines, with CRLF, LF line terminators, Stream Size: 97989

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	ISO-8859 text, with very long lines, with CRLF, LF line terminators
Stream Size:	97989
Entropy:	4.92680479263
Base64 Encoded:	True
Data ASCII:	T y p e T a b l e N a m e A d m i n E x e c u t e S e q u e n c e A c t i o n C o n d i t i o n S e q u e n c e C o s t F i n a l i z e C o s t I n i t i a l i z e F i l e C o s t I n s t a l l A d m i n P a c k a g e I n s t a l l F i l e s I n s t a l l F i n a l i z e I n s t a l l I n i t i a l i z e I n s t a l l V a l i d a t e A d v t E x e c u t e S e q u e n c e C r e a t e S h o r t c u t s M s i P u b l i s h A s s e m b l i e s P u b l i s h C o m p o n e n t s P u b l i s h F e a t u r e s P u
Data Raw:	54 79 70 65 54 61 62 6c 65 4e 61 6d 65 41 64 6d 69 6e 45 78 65 63 75 74 65 53 65 71 75 65 6e 63 65 41 63 74 69 6f 6e 43 6f 6e 64 69 74 69 6f 6e 53 65 71 75 65 6e 63 65 43 6f 73 74 46 69 6e 61 6c 69 7a 65 43 6f 73 74 49 6e 69 74 69 61 6c 69 7a 65 46 69 6c 65 43 6f 73 74 49 6e 73 74 61 6c 6c 41 64 6d 69 6e 50 61 63 6b 61 67 65 49 6e 73 74 61 6c 6c 46 69 6c 65 73 49 6e 73 74 61 6c 6c

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 7612

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	7612
Entropy:	3.48632478961
Base64 Encoded:	False

General	
Data ASCII:	. . . . . + ... 3 . . . . . k . . . . . n . . . . . : . s . . . . . M .
Data Raw:	e4 04 00 00 04 00 04 00 00 00 00 00 05 00 02 00 04 00 04 00 14 00 07 00 06 00 12 00 09 00 2b 00 08 00 10 00 0c 00 06 00 0e 00 06 00 08 00 05 00 13 00 02 00 0c 00 03 00 0f 00 03 00 11 00 03 00 0f 00 04 00 13 00 07 00 0f 00 03 00 14 00 03 00 11 00 03 00 0f 00 03 00 0e 00 03 00 11 00 03 00 15 00 03 00 10 00 03 00 12 00 03 00 0c 00 05 00 07 00 02 00 06 00 02 00 05 00 0d 00 05 00 02 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 76

General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	76
Entropy:	3.71174626965
Base64 Encoded:	False
Data ASCII:	. . . . . $. + . 5 . : . = . B . D . P .] . _ . a . d . g . k . r . w . z . . . . .
Data Raw:	05 00 07 00 11 00 1b 00 1e 00 24 00 2b 00 35 00 3a 00 3d 00 42 00 44 00 50 00 5d 00 5f 00 61 00 64 00 67 00 6b 00 72 00 77 00 7a 00 7f 00 83 00 86 00 8d 00 8e 00 8f 00 90 00 92 00 95 00 99 00 9a 00 a0 00 a7 00 c3 00 f2 00 14 01

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 4224

General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	4224
Entropy:	2.57766375838
Base64 Encoded:	False
Data ASCII:	. . . . . $. $. + . + . + . + . + . + . + . + . 5 . 5 . 5 . : . : . = . = . = . = . = . B . B . B . B . B . B . B . B . B . B . D . D . D . D . D . D . D . D . P . P . P . P . P .] .] . _ . _ . a . a . a . a . a . a . d . d . d . d . g . g . g . g . g . g . k . k . k . k . k . k . k . r . r . r . r . r . w . w . w . z . z . z . z . . . . .
Data Raw:	05 00 05 00 05 00 07 00 07 00 07 00 11 00 11 00 11 00 1b 00 1b 00 1e 00 1e 00 1e 00 1e 00 1e 00 1e 00 24 00 24 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 35 00 35 00 35 00 35 00 3a 00 3a 00 3d 00 3d 00 3d 00 3d 00 3d 00 3d 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 42 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 44 00 50 00

Stream Path: \x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481, File Type: data, Stream Size: 24

General	
Stream Path:	\x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481
File Type:	data
Stream Size:	24
Entropy:	2.79248125036
Base64 Encoded:	False
Data ASCII:	v . . . . .
Data Raw:	76 06 88 06 8a 06 8c 06 8e 06 90 06 92 06 89 06 8b 06 8d 06 8f 06 91 06

Stream Path: \x18496\x16667\x17191\x15090\x17912\x17591\x18481, File Type: data, Stream Size: 36

General	
Stream Path:	\x18496\x16667\x17191\x15090\x17912\x17591\x18481
File Type:	data
Stream Size:	36
Entropy:	3.62798680688
Base64 Encoded:	False
Data ASCII:	S . S . . . . . T . . . . . @ . @ . . . . .
Data Raw:	53 01 53 01 01 80 02 80 54 01 94 06 05 80 05 80 05 80 19 80 40 81 40 81 14 80 0f 80 93 06 95 06 00 00 00 00

Stream Path: \x18496\x16778\x17207\x17522\x16925\x17915, File Type: data, Stream Size: 450

General	
Stream Path:	\x18496\x16778\x17207\x17522\x16925\x17915
File Type:	data
Stream Size:	450

General	
Entropy:	4.86962854226
Base64 Encoded:	False
Data ASCII:	. . . . 7 . 9 . . . . $. (. + . - . . 2 . 6 . 9 . < . A . D . H . J . L . P . U . X . [.] . d . g . j . l . o . q . t . v . x . z . } . . . . * . * . 5 . . . ; . ? . . . & . F . N . R . S . " . ` . b . . . @ . . . . % .) . , . . . 0 . 3 . 7 . : . = . B . E . I . K . M . Q . V . Y . \\ . ^ . e .
Data Raw:	09 00 0a 00 0b 00 0c 00 0d 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 37 01 39 01 f3 01 f5 01 f8 01 fc 01 01 02 03 02 06 02 09 02 0e 02 10 02 11 02 14 02 17 02 19 02 1c 02 1f 02 24 02 28 02 2b 02 2d 02 2f 02 32 02 36 02 39 02 3c 02 41 02 44 02 48 02 4a 02 4c 02 50 02 55 02 58 02 5b 02 5d 02 64 02 67 02 6a 02 6c 02 6f 02 71 02 74 02 76 02 78 02 7a 02 7d 02 7f 02

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.11008776073
Base64 Encoded:	False
Data ASCII:	. . . . < . . . . x .
Data Raw:	09 00 0a 00 0b 00 0c 00 0d 00 0e 00 0f 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 84 83 3c 8f a0 8f c8 99 dc 85 78 85

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 66

General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	66
Entropy:	3.74819904327
Base64 Encoded:	False
Data ASCII:	. . . . V . . . .
Data Raw:	09 00 0a 00 0b 00 97 02 98 02 99 02 9a 02 9b 02 9c 02 9d 02 9e 02 00 00 00 00 00 00 00 00 00 00 56 01 00 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 84 83 00 85 ce 84 01 80 14 85 ff 7f fd 7f 8c 80 fe 7f

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 84

General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	84
Entropy:	3.43893323285
Base64 Encoded:	False
Data ASCII:	. . . . x . . . j . 8 . . . . . . \\ . $ . . .
Data Raw:	09 00 0a 00 0e 00 0f 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 c8 99 dc 85 78 85 94 91 6a 98 38 98 9c 98 00 99 f8 91 5c 92 24 93 c0 92

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 12

General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	data
Stream Size:	12
Entropy:	1.89624062518
Base64 Encoded:	False
Data ASCII:	' . ' . ' . (.) . * .
Data Raw:	27 00 27 00 27 00 28 00 29 00 2a 00

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: data, Stream Size: 16

General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	data

General	
Stream Size:	16
Entropy:	2.48345859334
Base64 Encoded:	False
Data ASCII:	' . . . ' . 4 . . . .
Data Raw:	27 00 00 00 27 00 34 00 01 80 01 80 a4 02 00 80

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: data, Stream Size: 12

General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	data
Stream Size:	12
Entropy:	2.35538854221
Base64 Encoded:	False
Data ASCII:	) . . . 5 . 6 . . .) .
Data Raw:	29 00 01 80 35 01 36 01 00 00 29 00

Stream Path: \x18496\x16925\x17915\x17884\x17404\x18472, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x16925\x17915\x17884\x17404\x18472
File Type:	data
Stream Size:	48
Entropy:	3.09028891162
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	c8 01 96 06 99 06 9a 06 98 06 97 06 98 06 98 06 08 80 0d 80 08 80 08 80 00 00 00 80 00 00 00 80 00 00 00 80 ff ff ff 80 00 80 01 80 01 80 00 80

Stream Path: \x18496\x17100\x16808\x15086\x18162, File Type: data, Stream Size: 12

General	
Stream Path:	\x18496\x17100\x16808\x15086\x18162
File Type:	data
Stream Size:	12
Entropy:	2.221251836
Base64 Encoded:	False
Data ASCII:	q . . . . . V . V . V .
Data Raw:	71 01 dd 01 a2 02 56 01 56 01 56 01

Stream Path: \x18496\x17163\x16689\x18229, File Type: data, Stream Size: 60

General	
Stream Path:	\x18496\x17163\x16689\x18229
File Type:	data
Stream Size:	60
Entropy:	2.7112204457
Base64 Encoded:	False
Data ASCII:	M . . . . .
Data Raw:	4d 01 c4 01 c6 01 cc 01 ce 01 d0 01 d2 01 d4 01 d6 01 d8 01 da 01 e1 01 9f 02 a0 02 a1 02 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 30

General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	30
Entropy:	3.37302351458
Base64 Encoded:	False
Data ASCII:	(. E . . . . .
Data Raw:	28 00 45 01 a4 02 f7 02 e3 03 f7 02 e3 03 f7 02 00 00 f7 02 e6 03 e4 03 e2 03 e1 03 e5 03

Stream Path: \x18496\x17165\x17380\x17074, File Type: data, Stream Size: 616

General	
Stream Path:	\x18496\x17165\x17380\x17074

General	
File Type:	data
Stream Size:	616
Entropy:	4.22908405498
Base64 Encoded:	False
Data ASCII:	. . . . % . A . K . O . S . V . \\ . ` . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . . . r . r . r . r . r . r . r . . . r . r . r . r . r . r . r . (. r . r . r . r . r . r . r . r . r . r . . . i . . . . U . . . .
Data Raw:	8e 01 97 02 98 02 9b 02 9c 02 9d 02 9e 02 a7 02 ac 02 bc 02 d0 02 d1 02 d3 02 d5 02 d9 02 f1 02 f4 02 05 03 0a 03 10 03 25 03 41 03 4b 03 4f 03 53 03 56 03 5c 03 60 03 32 80

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 468

General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	468
Entropy:	5.64089512208
Base64 Encoded:	False
Data ASCII:	. . . . 7 . 9 . . . . $. / . 2 . 6 . A . D . H . J P . U . X . [.] . d . g . j . l . o . q . t . v . x . z . } . . . . w . y . . . . | . . . . u . . . v . s . v . u . t . r . { . . . x . . . . t . . . . t . . . . x . } . . . . . ~ .
Data Raw:	09 00 0a 00 0b 00 0d 00 0e 00 0f 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 37 01 39 01 f3 01 f5 01 f8 01 03 02 09 02 0e 02 10 02 11 02 14 02 17 02 24 02 2f 02 32 02 36 02 41 02 44 02 48 02 4a 02 50 02 55 02 58 02 5b 02 5d 02 64 02 67 02 6a 02 6c 02 6f 02 71 02 74 02 76 02 78 02 7a 02 7d 02 7f 02 81 02 83 02 85 02 87 02 89 02 8b 02 8e 02 90 02 92 02 94 02 96 02

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 192

General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	192
Entropy:	5.01958964518
Base64 Encoded:	False
Data ASCII:	. . . . . . 7 . 9 . 6 . A . . . . V . \\ . . . . z . { . . . . o . . . . . o . . . . u . . . { . . . . d . . . . . L . . . . K . . . . c . 4 . 3 . . . . . e . 5 . . . .
Data Raw:	09 00 0a 00 0b 00 37 01 39 01 36 02 41 02 97 02 9a 02 9b 02 9c 02 9d 02 9e 02 d5 02 f1 02 56 03 5c 03 b2 03 b8 03 ba 03 bc 03 c4 03 c6 03 c9 03 cd 03 cf 03 d3 03 d8 03 d9 03 da 03 db 03 dc 03 00 00 00 00 00 00 00 00 75 06 00 00 00 00 00 00 00 00 85 06 00 00 00 00 86 06 7a 03 7b 03 7f 03 80 03 00 00 00 00 00 00 87 06 6f 06 b3 03 00 00 6f 06 80 06 80 03 84 06 75 06 83 06 7b 06 7f 06

Stream Path: \x18496\x17547\x17906\x17910\x16693\x17651\x17768\x15518\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48

General	
Stream Path:	\x18496\x17547\x17906\x17910\x16693\x17651\x17768\x15518\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.73590234443
Base64 Encoded:	False
Data ASCII:	7 . 9 . : . < . = . ? . @ . A . 8 . 8 . ; . ; . > . > . ; . B . . . . E . ^ . w . . .
Data Raw:	37 01 39 01 3a 01 3c 01 3d 01 3f 01 40 01 41 01 38 01 38 01 3b 01 3b 01 3e 01 3e 01 3b 01 42 01 98 80 9b 80 af 80 c8 80 45 81 5e 81 77 81 db 81

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: data, Stream Size: 36

General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	data
Stream Size:	36
Entropy:	2.77432067357

General	
Base64 Encoded:	False
Data ASCII:	(.) . * . . . . . (. . . E . . . .) . . .
Data Raw:	28 00 29 00 2a 00 a5 02 a3 02 a6 02 28 00 a4 02 45 01 00 80 04 80 00 80 00 00 00 00 00 00 00 00 29 00 00 00

Stream Path: \x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522, File Type: data, Stream Size: 72

General	
Stream Path:	\x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522
File Type:	data
Stream Size:	72
Entropy:	3.373933168
Base64 Encoded:	False
Data ASCII:	. . . . . = . > . . . . . s . s . s . s . w . w . s . s . s . v . v . u . u . x . x . t . . t .
Data Raw:	9b 02 9b 02 9b 02 9b 02 9c 02 9c 02 10 03 10 03 10 03 b5 02 b7 02 b9 02 bb 02 3d 03 3e 03 c2 02 18 03 1a 03 73 03 73 03 73 03 73 03 77 03 77 03 73 03 73 03 73 03 76 03 76 03 75 03 75 03 78 03 78 03 74 03 74 03 74 03

Stream Path: \x18496\x17548\x17905\x17589\x15279\x16953\x17905, File Type: data, Stream Size: 1536

General	
Stream Path:	\x18496\x17548\x17905\x17589\x15279\x16953\x17905
File Type:	data
Stream Size:	1536
Entropy:	4.92706864825
Base64 Encoded:	False
Data ASCII:	. . . . . % . A . A . A . K . K . K O . S . S . S . V . V . V . V . \\ . \\ . \\ . \\ . \\ . \\ . ` .
Data Raw:	8e 01 8e 01 8e 01 8e 01 8e 01 8e 01 8e 01 97 02 98 02 98 02 98 02 9b 02 9b 02 9b 02 9c 02 9c 02 9c 02 9d 02 9e 02 9e 02 a7 02 a7 02 a7 02 a7 02 a7 02 a7 02 ac 02 ac 02 bc 02 bc 02 bc 02 bc 02 bc 02 bc 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d0 02 d1 02 d1 02 d1 02 d1 02 d1 02 d1 02 d1 02 d3 02 d3 02 d3 02 d3 02 d3 02 d3 02 d3 02 d3 02 d5 02 d5 02

Stream Path: \x18496\x17548\x17905\x17589\x18479, File Type: data, Stream Size: 7280

General	
Stream Path:	\x18496\x17548\x17905\x17589\x18479
File Type:	data
Stream Size:	7280
Entropy:	4.53629155714
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	8e 01 8e 01 8e 01 8e 01 8e 01 8e 01 8e 01 8e 01 97 02 97 02 97 02 97 02 97 02 97 02 97 02 97 02 97 02 97 02 97 02 98 02 98 02 98 02 98 02 98 02 98 02 9b 02 9b 02 9b 02 9b 02 9b 02 9b 02 9b 02 9b 02 9b 02 9c 02 9c 02 9c 02 9c 02 9c 02 9c 02 9c 02 9c 02 9c 02 9c 02 9d 02 9d 02 9d 02 9d 02 9d 02 9d 02 9d 02 9d 02 9d 02 9e 02 9e 02 9e 02 9e 02 9e 02

Stream Path: \x18496\x17630\x17770\x16868\x18472, File Type: data, Stream Size: 32

General	
Stream Path:	\x18496\x17630\x17770\x16868\x18472
File Type:	data
Stream Size:	32
Entropy:	2.76201589562
Base64 Encoded:	False
Data ASCII:	. . . . f . m . . . f . . . . n .
Data Raw:	e6 01 e6 01 66 01 6d 07 00 00 66 01 00 00 00 00 02 00 00 80 01 01 00 80 00 00 00 00 87 06 6e 07

Stream Path: \x18496\x17740\x16680\x16951\x17551\x16879\x17768, File Type: data, Stream Size: 8

General	
Stream Path:	\x18496\x17740\x16680\x16951\x17551\x16879\x17768
File Type:	data

General	
Stream Size:	8
Entropy:	2.15563906223
Base64 Encoded:	False
Data ASCII:	(. E . (. * .
Data Raw:	28 00 45 01 28 00 2a 00

Stream Path: \x18496\x17742\x17589\x18485, File Type: data, Stream Size: 2564

General	
Stream Path:	\x18496\x17742\x17589\x18485
File Type:	data
Stream Size:	2564
Entropy:	6.53931732391
Base64 Encoded:	False
Data ASCII:	. . . . ! . . . M . . . . ! . " . # . $. % . & . ' . (.) . * . + . , . - . . . / . 0 . 1 . 2 . 3 . 4 . 5 . 6 . 7 . 8 . y . z . { .	. } . ~ . . . . . A . B . C . D . E . F . G . H . I . . . . . m . n . o . p .
Data Raw:	00 80 01 80 02 80 03 80 04 80 05 80 06 80 07 80 08 80 09 80 0a 80 0b 80 0c 80 0d 80 0e 80 0f 80 10 80 11 80 12 80 13 80 14 80 15 80 16 80 17 80 20 80 21 80 e9 83 4d 84 15 85 16 85 17 85 18 85 19 85 1a 85 1b 85 1c 85 1d 85 1e 85 1f 85 20 85 21 85 22 85 23 85 24 85 25 85 26 85 27 85 28 85 29 85 2a 85 2b 85 2c 85 2d 85 2e 85 2f 85 30 85 31 85 32 85 33 85 34 85 35 85 36 85 37 85 38 85

Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: data, Stream Size: 384

General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	data
Stream Size:	384
Entropy:	4.70925269452
Base64 Encoded:	False
Data ASCII:	) . i . . . H . J . L . N . P . Q . S . U . X . Y . [.] . _ . a . c . e . g . i . k . m . o . q . r . t . u . w . y . { . } . ~ . . . . . W . I . K . M . O . K . R . T . V . O . Z . \\ . ^ . ` . b . d . f . h . j . l . n . p . V . s . h . v . x . z .	.	.
Data Raw:	29 00 69 00 08 01 48 01 4a 01 4c 01 4e 01 50 01 51 01 53 01 55 01 58 01 59 01 5b 01 5d 01 5f 01 61 01 63 01 65 01 67 01 69 01 6b 01 6d 01 6f 01 71 01 72 01 74 01 75 01 77 01 79 01 7b 01 7d 01 7e 01 80 01 82 01 84 01 85 01 87 01 88 01 89 01 8b 01 8d 01 8f 01 90 01 92 01 94 01 96 01 98 01 9a 01 9c 01 9e 01 a0 01 a2 01 a4 01 a6 01 a8 01 aa 01 ac 01 ae 01 af 01 b1 01 b3 01 b4 01 b6 01

Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 324

General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data
Stream Size:	324
Entropy:	3.97479493951
Base64 Encoded:	False
Data ASCII:	. . . . . 3 . . . A . 3 . . . . . A . A . 3 . . . 3 . 3 . 3 . 3 . e . 3 . 3 . 3 . 3 . . . . . z . . . . . z . { . . . . . V . . . . . V . V . V . V . . . . .
Data Raw:	f8 01 06 02 10 02 19 02 1c 02 99 02 97 03 a3 03 b2 03 b8 03 ba 03 bc 03 c2 03 c4 03 c6 03 c9 03 ca 03 cd 03 cf 03 d2 03 d3 03 d6 03 d8 03 d9 03 da 03 db 03 dc 03 01 80 01 ac 01 80 01 ad 01 ac 33 80 01 80 41 80 33 80 01 80 41 81 13 80 41 80 41 80 33 80 01 80 33 80 33 81 33 81 33 80 33 80 65 86 33 80 33 80 33 80 33 80 01 80 9f 02 9f 02 9f 02 9f 02 9f 02 d5 03 a0 02 a0 02 b3 03 a0 02

Stream Path: \x18496\x17998\x17512\x15799\x17636\x17203\x17073, File Type: PGP\011Secret Sub-key -, Stream Size: 128

General	
Stream Path:	\x18496\x17998\x17512\x15799\x17636\x17203\x17073
File Type:	PGP\011Secret Sub-key -
Stream Size:	128
Entropy:	4.21020611944
Base64 Encoded:	False
Data ASCII:	. . . . . Z . . . . . ! . . . d . . . Z . f . . d . f . g . g . g . l . k . l . j . i . N . e . N . N . f . N . e . f . h . h . h . m . N . m . N . N .

General	
Data Raw:	97 02 97 02 9d 02 9d 02 a7 02 f4 02 f4 02 0a 03 10 03 10 03 10 03 10 03 10 03 10 03 10 03 10 03 86 00 f5 02 86 00 5a 03 fa 02 86 00 f5 02 fa 02 cc 02 14 03 16 03 18 03 1a 03 1a 03 1f 03 21 03 86 00 64 06 86 00 5a 03 66 06 86 00 64 06 66 06 67 06 67 06 6c 06 6b 06 6c 06 6a 06 69 06 4e 00 65 06 4e 00 4e 00 66 06 4e 00 65 06 66 06 68 06 68 06 68 06 6d 06 4e 00 6d 06 4e 00 4e 00

Network Behavior

UDP Packets

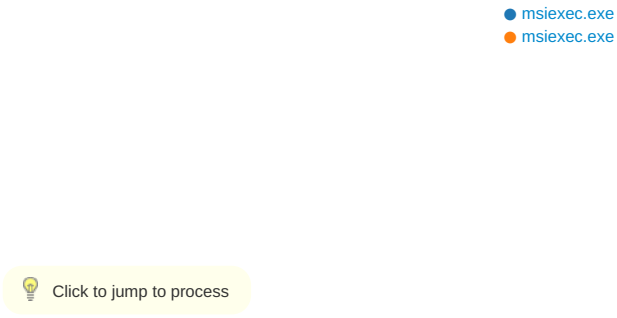
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 10:17:56.135256052 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:56.187124968 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 22, 2021 10:17:56.323693037 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:56.372802019 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 22, 2021 10:17:56.954571009 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:57.004539013 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 22, 2021 10:17:57.161745071 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:57.227842093 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 22, 2021 10:17:57.368511915 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:57.417515993 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 22, 2021 10:17:59.896270990 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:17:59.950319052 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:00.867660046 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:00.916368008 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:01.213684082 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:01.271773100 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:02.113773108 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:02.165416956 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:05.546844006 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:05.669281960 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:21.718178034 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:21.789001942 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:33.175560951 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:33.227010965 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:34.651837111 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:34.700604916 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:39.810395002 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:39.861974001 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:43.712039948 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:43.775580883 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:45.120851040 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:45.169464111 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:45.960325003 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:46.020528078 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:46.909456968 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:46.958533049 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:47.809371948 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:47.861540079 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 22, 2021 10:18:52.396596909 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:18:52.455595016 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:09.756323099 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:09.809004068 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:12.368953943 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:12.427176952 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:20.103347063 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:20.152254105 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:32.397269964 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:32.465845108 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:50.014134884 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:50.071806908 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 22, 2021 10:19:52.266226053 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 22, 2021 10:19:52.334182024 CEST	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: 6560 Parent PID: 5640

General

Start time:	10:18:02
Start date:	22/04/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\msiexec.exe' /i 'C:\Users\user\Desktop\notifica2104.msi'
Imagebase:	0x7ff664ee0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: 6616 Parent PID: 992

General

Start time:	10:18:04
Start date:	22/04/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 62996ADAF98AEA6C3E76201DA1491D0F
Imagebase:	0xfb0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis