ID: 508575
Sample Name: o4c8AUtX1g
Cookbook: default.jbs
Time: 11:39:45
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

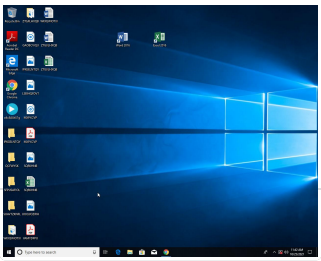
Windows Analysis Report o4c8AUtX1g

Overview

General Information

Sample Name:	o4c8AUtX1g (renamed file extension from none to exe)
Analysis ID:	508575
MD5:	c7db399951b19e..
SHA1:	b01352206ec193..
SHA256:	ceba6a7f9a2c25a..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

Score:	69
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

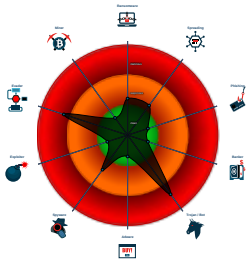
Compliance

Score:	18
Range:	0 - 100

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Detected unpacking (changes PE se…
- PE file has a writeable .text section
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Uses 32bit PE files
- Queries the volume information (nam…
- Antivirus or Machine Learning detec…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Very long cmdline option found, this…

Classification



Process Tree

- **System is w10x64**
- o4c8AUtX1g.exe (PID: 3408 cmdline: 'C:\Users\user\Desktop\o4c8AUtX1g.exe' MD5: C7DB399951B19EA446599DC3800A3111)
  - msiexec.exe (PID: 5944 cmdline: 'C:\Windows\system32\msiexec.exe' /i 'C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\adv.msi' AI_SETUPEXEPATH=C:\Users\user\Desktop\o4c8AUtX1g.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE='/exenoupdates /forcecleanup /wintime 1635154532 ' AI_EUIMSI='' MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- msiexec.exe (PID: 5776 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 768 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding D90C408BAA115D1625882500CC5A128E C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - msiexec.exe (PID: 6328 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 97E0B76AE09D0E82CE071E7BABCE98E1 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - plcd-player.exe (PID: 4744 cmdline: C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\plcd-player.exe MD5: 25DDBD309BB80942297043839 77C7268)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
"GP2bItvzCMVimwFhSq2LMu3Hl69+F5VOC4HbUzLcgCFvHPQPwYycui0JiyqQuwt1jV1IDboN9TEBxLB8CQWBGqcjZkZnRvT4fL8wjq8CCeHOLprVhSXFIxyR2QXzTHDcHr2ux9/r22BaiLqlqlqcKQ1PI6I3WFn39M0KSk1WypMPthcp
EVFSO8sVBHvcqRSV",
  "c2_domain": [
    "get.updates.avast.cn",
    "huyasos.in",
    "curves.ws",
    "huyasos.in",
    "rorobrun.in",
    "huyasos.in",
    "tfslld.ws",
    "huyasos.in"
  ],
  "botnet": "2002",
  "server": "12",
  "serpent_key": "44004499FJFHGTYB",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000003.913796145.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000003.913762032.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000002.937676135.0000000003949000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000009.00000003.913941910.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000009.00000002.937726154.0000000003E68000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Click to see the 6 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.plcd-player.exe.39494a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
9.2.plcd-player.exe.39494a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
9.2.plcd-player.exe.1270000.1.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Compliance:

- Uses 32bit PE files
- EXE planting / hijacking vulnerabilities found
- DLL planting / hijacking vulnerabilities found
- Creates license or readme file
- PE / OLE file has a valid certificate
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif

System Summary:

- PE file has a writeable .text section
- Writes or reads registry keys via WMI
- Writes registry values via WMI

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif

Stealing of Sensitive Information:

- Yara detected Ursnif

Remote Access Functionality:

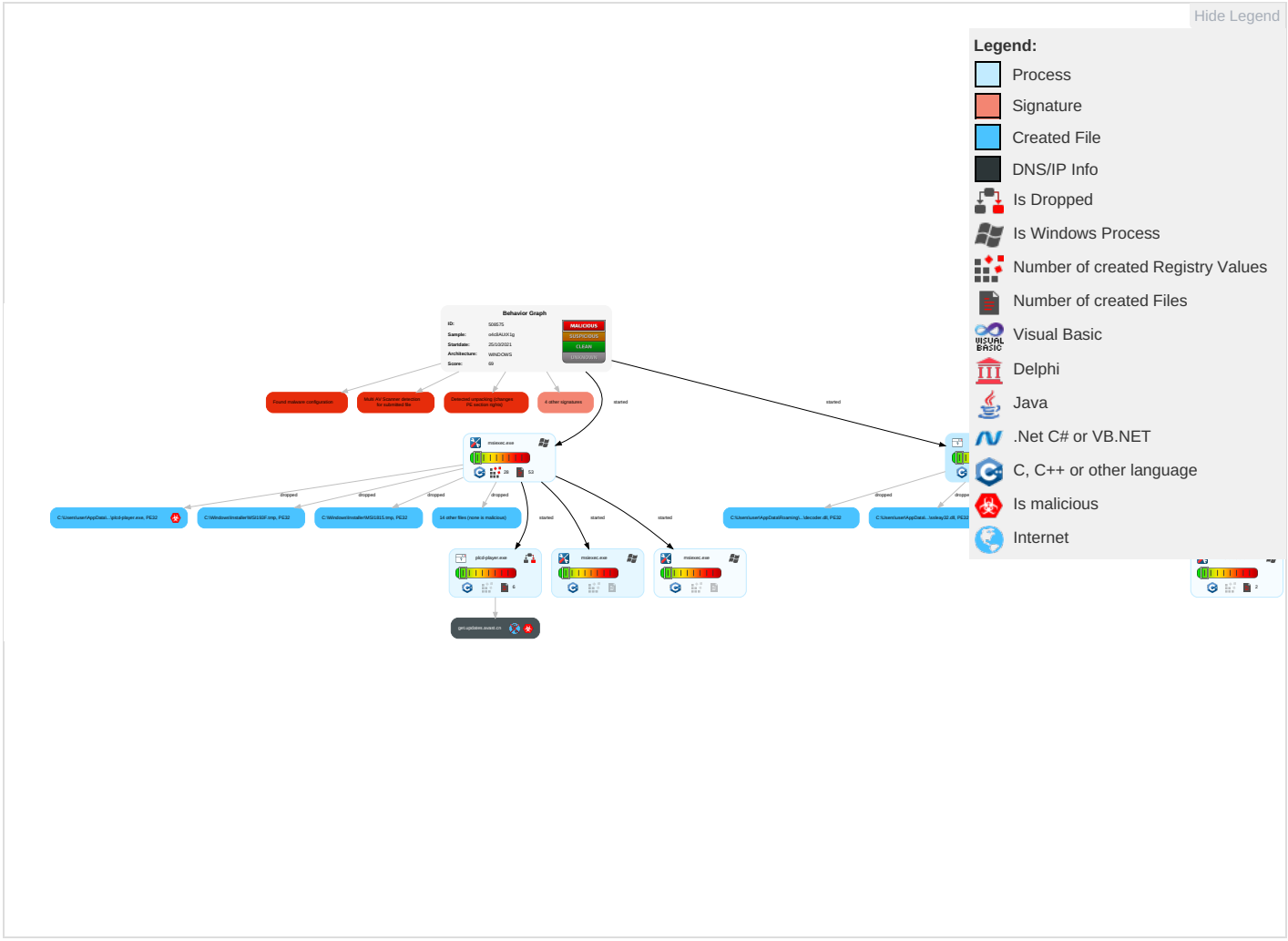
- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media 1	Windows Management Instrumentation 2	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Native API 1	DLL Search Order Hijacking 2	DLL Search Order Hijacking 2	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 3	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Search Order Hijacking 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading 3 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 2 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoc

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
o4c8AUtX1g.exe	29%	ReversingLabs	Win32.Trojan.Chapak	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSI76CC.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI76CC.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI79F9.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI79F9.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\shi7515.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\shi7515.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\AWSSDK.SimpleDB.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Delimon.Win32.IO.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Delimon.Win32.IO.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ICSharpCode.SharpZipLib.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ICSharpCode.SharpZipLib.dll	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Microsoft.Azure.KeyVault.Core.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\SslCertBinding.Net.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\System.Threading.Tasks.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\System.Threading.Tasks.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.plcd-player.exe.a70000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen8		Download File
9.2.plcd-player.exe.1270000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoPublicCodeSigningCAEVR36.crl0	0%	Avira URL Cloud	safe	
http://html4/loose.dtd	0%	Avira URL Cloud	safe	
http://ocsp.startssl.com/sub/class2/code/ca0	0%	Avira URL Cloud	safe	
http://crl.startssl.com/sfsca.crl0C	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://currencysystem.com/gfx/pub/script-icon-16x16.gif	0%	Avira URL Cloud	safe	
http://www.gesmes.org/xml/2002-08-01	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAEVR36.crt0#	0%	Avira URL Cloud	safe	
http://ocsp.startssl.com/ca00	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://.css	0%	Avira URL Cloud	safe	
http://crl.startssl.com/crtc2-crl.crl0	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0)	0%	Avira URL Cloud	safe	
http://www.ecb.int/vocabulary/2002-08-01/eurofxref	0%	Avira URL Cloud	safe	
http://www.MyBusinessCatalog.com	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://currencysystem.com/gfx/pub/script-button-88x31.gif	0%	Avira URL Cloud	safe	
http://aia.startssl.com/certs/sub.class2.code.ca.crt0#	0%	Avira URL Cloud	safe	
http://https://currencysystem.com/gfx/pub/script-icon-16x16.png	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://mybusinesscatalog.com0	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://aia.startssl.com/certs/ca.crt02	0%	URL Reputation	safe	
http://www.startssl.com/policy.pdf0	0%	Avira URL Cloud	safe	
http://www.startssl.com/0	0%	Avira URL Cloud	safe	
http://https://currencysystem.com/gfx/pub/script-button-88x31.png	0%	Avira URL Cloud	safe	
http://.jpg	0%	Avira URL Cloud	safe	
http://https://currencysystem.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
get.updates.avast.cn	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508575
Start date:	25.10.2021
Start time:	11:39:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	o4c8AUtX1g (renamed file extension from none 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:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal69.troj.evad.winEXE@10/55@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.9% (good quality ratio 1.9%) • Quality average: 91.5% • Quality standard deviation: 14.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:40:45	API Interceptor	1x Sleep call for process: o4c8AUtX1g.exe modified
11:41:10	API Interceptor	2x Sleep call for process: plcd-player.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\MSI76CC.tmp	farcry6_repack.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\MSI79F9.tmp	farcry6_repack.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\shi7515.tmp	e6d90883fd0e3c7576c140d6f12e04e1e54c3789ec4b2.exe	Get hash	malicious	Browse	
	tconnect_HCP_Software_v301_Installer.msi	Get hash	malicious	Browse	
	mWvxXYwvqU.exe	Get hash	malicious	Browse	
	farcry6_repack.exe	Get hash	malicious	Browse	
	yvY2AMOxwb.exe	Get hash	malicious	Browse	
	EpAIWOPmnA.exe	Get hash	malicious	Browse	
	EpAIWOPmnA.exe	Get hash	malicious	Browse	
	YSy9zYFtB2.exe	Get hash	malicious	Browse	
	WFrmiIfWt5.exe	Get hash	malicious	Browse	
	eAlTRSN46u.exe	Get hash	malicious	Browse	
	uhwBmJGGqo.exe	Get hash	malicious	Browse	
	fPPE8cHbql.exe	Get hash	malicious	Browse	
	qB6P2WfUjb.exe	Get hash	malicious	Browse	
	qB6P2WfUjb.exe	Get hash	malicious	Browse	
	xuXoY85NmR.exe	Get hash	malicious	Browse	
	DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF0F9CF.exe	Get hash	malicious	Browse	
	DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF0F9CF.exe	Get hash	malicious	Browse	
	9c9cdb438163a2e64adcb398a6f1f1abcdc81c1cf35ab.exe	Get hash	malicious	Browse	
	zEQyeKgNgG.exe	Get hash	malicious	Browse	
	WP6TzYzWmG.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Config.Msi\440bbf.rbs	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	5083
Entropy (8bit):	5.641804540600664
Encrypted:	false
SSDEEP:	96:JUblaV4pDyj0onGIlKjeRhmgKpdGUO7PVRGlmO1fRRDPCW9mJ+x9DZdR0qR0hwN1:JUvp2j0on2jeRhmgSGUO7NRG315RDPCU
MD5:	F1D4BF5FDB8005BECDBAA13E74F461A6
SHA1:	40D5531268D2ACE0D91E25F4F54A604FF3959FB2
SHA-256:	6BC13A98E8CBC3551B352D6B5005F5677E13773923FA0402B4F8653DF7FBF5ED
SHA-512:	AA3AF871AEDFCE520208FE815C72A983EDFAB1D9BAFAD6F299B4DE7619617F9A6D94895EFD4CBB97FA02453054DB52BEE9A7B7BBE418CD60BE8E5F60B8CB3DD2
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@"]YS.@.....@.....@.....@.....@.....@.....&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}..JDesktop Tools..adv.msi.@.....@.....@.....@.....@.....&.{D9FF1A35-78F9-49F0-A6A0-DB3A11387835}.....@.....@.....@.....@.....@.....@.....@.....@.....@.....JDesktop Tools.....Rollback..Rolling back action:....RollbackCleanup..Removing backup files..File: [1]....ProcessComponents..Updating component registration..&.{F5BA1B6B-756B-4B40-A5CB-A8A21E79DAE6}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{FC3D5B52-2561-4633-85CB-6F8B8A86F2F9}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{8C82D735-0397-4468-B16C-3DB17F7A7006}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{0B568A04-369C-43FB-98E4-C437A15709E0}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{D0054317-E107-45C9-BD82-07B794597760}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{4CE558F3-30D7-4710-8A30-53FF7CA0A97F}&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}.@.....&.{A396B091-4840-44D8-ADD7-69BE85386878}&.{4A523951-0A2F-4D65-A3

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|\.....U2U.....,9..+.\R..(.[.'M.....0.o..,t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y.}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ.,.q..".t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.096153500626319
Encrypted:	false
SSDEEP:	6:kKJw/2dFN+SkQlPlEGYRMY9z+4KlDA3RUeOlEfcTt:So2kPlE99SNxAhUefit
MD5:	B9FB343D52D6EA10E38A1F41F0622A0E
SHA1:	DA2C853B0EA5F7DC80C47F4FFEB331765737E019
SHA-256:	4CB0FFB319DBB81BEC8D15854336AE9033D886254C66A70A2865CB37FB6BFE06
SHA-512:	D4185C6946ACC58EDDBC42747F88D7A8EBBC648CEDECFB9FCA776FDD0EB4FA4830FA85325D9F2C48E7945217D548E6E709070FC7D500BB166E0641867523204
Malicious:	false
Reputation:	low
Preview:	p..... ....K].b....(..... .....^.....$.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.a.a.8.a.1.5.e.a.6.d.7.1.:.0."...

C:\Users\user\AppData\Local\Temp\MSI76CC.tmp	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F627BA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: farcry6_repack.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J...!...T..!...T..!...T...!..J..!..J..!..J..!..!... ...T...!...T..!...T..!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6\|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:.....H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B.....@..B.....

C:\Users\user\AppData\Local\Temp\MSI79F9.tmp	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\MSI79F9.tmp	
Size (bytes):	887264
Entropy (8bit):	6.436854443892135
Encrypted:	false
SSDEEP:	24576:gJgZXlAIjfQhETbF+RWQNgXAo1sVz1v0Mny+PkfsJJ10FRzVTv:F/fQhksQQNgXAo1sVzhly+PkfsJJ10FT
MD5:	0BE6E02D01013E6140E38571A4DA2545
SHA1:	9149608D60CA5941010E33E01D4FDC7B6C791BEA
SHA-256:	3C5DB91EF77B947A0924675FC1EC647D6512287AA891040B6ADE3663AA1FD3A3
SHA-512:	F419A5A95F7440623EDB6400F9ADBFB9BA987A65F3B47996A8BB374D89FF53E8638357285485142F76758BFFCB9520771E38E193D89C82C3A9733ED98AE24FCB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: farcry6_repack.exe, Detection: malicious, Browse
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....4.....3.....3.....3.?..... W....3.....Rich.....PE..L.....Ia.....'!.....KC....@.....t...d.....p.....T.....p.....@... ....h...@.....text..... ..`.rdata.....@..@.data...4.....@....rsrc.....|.....@..@.reloc..T..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\shi7515.tmp	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3440640
Entropy (8bit):	6.332754172601424
Encrypted:	false
SSDEEP:	49152:iGfM3glOz6pNbH2qLG1cWJ2asQceg4LApnrkLgQ63lOT0q4Fn6rmLn:Lc3wFeyCulhqUn
MD5:	59A74284EACB95118CEDD7505F55E38F
SHA1:	ACDC28D6A1EF5C197DE614C46BA07AEAEB25B50B
SHA-256:	7C8EA70CA8EFB47632665833A6900E8F2836945AA80828B30DA73FBF4FCAF4F5
SHA-512:	E69A82ADC2D13B413C0689E9BF281704A5EF3350694690BA6F3FE20DA0F66396245B9756D52C37166013F971C79C124436600C373544321A44D71F75A16A2B6A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: e6d90883fd0e3c7576c140d6f12e04e1e54c3789ec4b2.exe, Detection: malicious, Browse • Filename: tconnect_HCP_Software_v301_Installer.msi, Detection: malicious, Browse • Filename: mWvxXYwvqU.exe, Detection: malicious, Browse • Filename: farcry6_repack.exe, Detection: malicious, Browse • Filename: yvY2AMOxwb.exe, Detection: malicious, Browse • Filename: EpAIWOPmnA.exe, Detection: malicious, Browse • Filename: EpAIWOPmnA.exe, Detection: malicious, Browse • Filename: YSy9zYFtB2.exe, Detection: malicious, Browse • Filename: WFrmiIfWt5.exe, Detection: malicious, Browse • Filename: eAlTRSN46u.exe, Detection: malicious, Browse • Filename: uhwBmJGGqo.exe, Detection: malicious, Browse • Filename: fPPE8cHbql.exe, Detection: malicious, Browse • Filename: qB6P2WfUjb.exe, Detection: malicious, Browse • Filename: qB6P2WfUjb.exe, Detection: malicious, Browse • Filename: xuXoY85NmR.exe, Detection: malicious, Browse • Filename: DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF0F9CF.exe, Detection: malicious, Browse • Filename: DF7049B8C4D704376BE3920232B1BA6B2C8CF2FF0F9CF.exe, Detection: malicious, Browse • Filename: 9c9cdb438163a2e64adcb398a6f1f1abcdc81c1cf35ab.exe, Detection: malicious, Browse • Filename: zEQyeKgNgG.exe, Detection: malicious, Browse • Filename: WP6TzYzWmG.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E..2..a..a..a..=aa.an..`..an..`..an..`..a..a..an..`..an..`..an..`l.an.Qa ..an..`..aRich..a.....PE..d...5..r....." .....n...H.....P.....4.....g.4...`A.....p.0.L&....0.....2.....@1.....4.....F'.T .....*..(.....q..8...Tc0.....text...o..... ..`.wpp_sf.Y..... ..`.rdata...Z.....\...r.....@..@.data....A....0.....0..... .@....pdata.....@1.....0.....@..@.didat.....2.....V2.....@....rsrc.....2.....b2.....@..@.reloc.....4.....b4.....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\AWSSDK.SimpleDB.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	62088
Entropy (8bit):	5.87884188749315
Encrypted:	false
SSDEEP:	1536:0mzFpEBNMGwcQHanzzd2UE/8YVkEyDrKe2xDBoPnp:dFpEBNMGwcsa8f/8a6Pp
MD5:	5AEB79663EA837F8A7A98DC04674B37A
SHA1:	536C24EF0572354E922A8C4A09CF5350D8A6164D
SHA-256:	E13D9F958783595ACD8ACDBFF4D587BCA7E7B6A3AAB796E2EFBD65BD37431536

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\AWSSDK.SimpleDB.dll	
SHA-512:	25E4E48EC2162EA6342CFD823E789ED0B5A995BB61FA3FA68364D1EE2468974FA4E75C17EB2CB3DDB213E633136C9AAB139BBF32FB8688FF5B1ABF444E8BB652
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....tx....." ..0..... ....@.....x.. ..@.....H...O..... ....x...8..... ....H.....text..... ....`.rsrc... .....@..@.reloc..... .....@..B.....\|.....H.....$b.....v.~....}.....(.....r...p(....*.r...p*.r...p*..{....*Br...p(.....*"..(....*&...(....*:..o.....(....*:.....(....*B .....(....*&...(....*..(....*F.(....s....(...*b.(....s....%.o!...(...*6.(.....(...*6..s....(....*R..s....%.o!...(....*&...(...*:...s....(....*V...s....%.o!...(....**....("...*>....s....(....*^....s....%..o!...(....*2..... (#...*.s$...*"..(%...*.0.....(.....(.....(...+*..

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\CrashRpt License.txt	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1569
Entropy (8bit):	5.078244393355221
Encrypted:	false
SSDEEP:	48:rlXOOrpJAzJzGl0PE9432sEs32s3IEtd132RTHy:peOrpJAzJzGlBq3b38OSTS
MD5:	734B7CB601EA82D8B4A9926373323B06
SHA1:	37490788B803335FA3AAD761B3EA0010889B2D8D
SHA-256:	90F301E30B61CDF8AC5E29F4FDD0E81C535FCAABF06B48D36B110A3F35E5A3D2
SHA-512:	273F154273DEDF9B06BBA74AEB81BF905309B6F137A414310B1E96C218095CC6B49EE663932815D6771C9BE1D033B014F57E7AE72C7B7FD396A9C254FA124706
Malicious:	false
Preview:	Copyright (c) 2003, The CrashRpt Project Authors...All rights reserved.....Redistribution and use in source and binary forms, with or without modification, ..are permitted provided that the following conditions are met:.... * Redistributions of source code must retain the above copyright notice, this .. list of conditions and the following disclaimer..... * Redistributions in binary form must reproduce the above copyright notice, .. this list of conditions and the following disclaimer in the documentation .. and/or other materials provided with the distribution..... * Neither the name of the author nor the names of its contributors .. may be used to endorse or promote prod ucts derived from this software without .. specific prior written permission.....THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUT ORS "AS IS" AND ANY ..EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES ..OF MERCHANTABILITY AND FITNESS

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Delimon.Win32.IO.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	940032
Entropy (8bit):	7.265468453378986
Encrypted:	false
SSDEEP:	12288:SjtToSCODTjAKMmNRYzUubi85LKHtToSCOD7jAK4mNRP:2Vxtqw/85LKHV1pt
MD5:	40C4EA80985E48C095D9F3AF80215C12
SHA1:	B7EAECB4CF5E45F7E3946BCD1C249A46428CA8C0
SHA-256:	2B1678502F69BCCBA816FE2901A12BD15567C4113D8EC5B0C9EBA3A1AEA7C633
SHA-512:	8C1FCFACEBA8273D4307FDC2AF0E8D137CF162838ED0C9AC198D0A29EC0E4E6B8A6B8C202BC415B2353889B4429ED9B07D784F367B2B339F65090242C78D64A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P.....!.....N.....l.. ....{g.. ..@.....l..S.....Pk..... ....H.....text....L... ...N..... ..`.rsrc.....P.....@..@.rel oc.....V.....@..B.....l.....H.....x.....j...n..P .....{.Z.L&.$.....v....lk..AC4..{E.0..X.....?3!...^..Q@..L.{._wSlwnsb].E.D...H=.{.s/.....H. f.q.kn...O.1y.\e.A./.[D.:#..T.h..6...}.....}.....s....}.....s....}.....(....*J.s....}'....(....*..0..).....{-.....(....t.....|-.....(...+...3.*....0..).....{-.....(....t.....|-.....(...+...3.*....0..).....{.....(....t. .....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ICSharpCode.SharpZipLib.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	200704
Entropy (8bit):	5.683688089372797
Encrypted:	false
SSDEEP:	3072:hjMibqfQqFyGCDXiW9Pp/+Tl4abpuu201PB1BBXIDwtqSPVINrAfvp1:GibqI59PpOPf201/z7p
MD5:	C8164876B6F66616D68387443621510C
SHA1:	7A9DF9C25D49690B6A3C451607D311A866B131F4
SHA-256:	40B3D590F95191F3E33E5D00E534FA40F823D9B1BB2A9AFE05F139C4E0A3AF8D
SHA-512:	44A6ACCC70C312A16D0E533D3287E380997C5E5D610DBEAA14B2DBB5567F2C41253B895C9817ECD96C85D286795BBE6AB35FD2352FDDD9D191669A2FB0774E4

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ICSharpCode.SharpZipLib.dll

Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<.K.....!..... .....^.... .....@.. .....@..... ..@.....K..... ....H.....text...d.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\License.txt

Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	Non-ISO extended-ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4532
Entropy (8bit):	4.840297093762095
Encrypted:	false
SSDEEP:	96:D9moghaxhFkV9RGGQwGok+iOJ54d7JdEgUVVN7XzUKyeraku:knhIhmz8pJdLk/7XAKy7x
MD5:	54A36434CA791404E0EE1894A7FB257A
SHA1:	E99BA6366C22F9E4693F6317352EAA5854F0F429
SHA-256:	5FCC77BA8A6D6DCA5ECD466F7706133A17571EAAA1B45D4613E2BF5C58DEC678
SHA-512:	87942ABBE3BC1C87BB77323D4E43D63A30ACE3B569FF16363D871B77A306A64569A8655B0B3A526B31F901BA5F081BFE122B7DF7F0C491637DD3050EC948D07
Malicious:	false
Preview:	MyBusinessCatalog Platinum....Copyright: (c)2002-2021 Alexander Chulpanov..Homepage: http://www.MyBusinessCatalog.com..E-mail: info@MyBusinessCatalog.com..==========.....You should carefully read the following terms and..conditions before using this software..... ..MyBusinessCatalog is try-before-buy software. This means:....1. All copyrights to MyBusinessCatalog are exclusively owned by the author . Alexander Chulpanov.....2.1 You can use the FREE version of MyBusinessCatalog with restrictions applicable to unregistered version...The DEMO (free) version allows outputs 50 items (to PDF, Printer etc)..Trial periad - 30 days...If a Mobiliger subscription is already active, the trial period for..MyBusinessCatalog Free is automatically extended.....2.2 Registered version...MyBusinessCatalog Platinum - PDF Studio License...Allows creating PDF and Printable catalogs...Small Business License includes 1 (one) year of free software updates.....MyBusin

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Microsoft.Azure.KeyVault.Core.dll

Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16968
Entropy (8bit):	6.369067823836705
Encrypted:	false
SSDEEP:	384:YdX0XY0X+DeljFWt6O9QHRN7fhKtklxHQJ:YdXuhvU8ZOJ
MD5:	FEC0A2AB4AB150DAD477E0D4885637CE
SHA1:	5A3C8920DE1B3F2F7867A20D05C94DE5B2779B81
SHA-256:	746760FE317B9721FB761209F0F9F7E1A5126390970AAC5FD93F11504FFE3D30
SHA-512:	11C7C941D31902CCC9F9E07166CF6E181E0ADF7BAEA0986B863CEFD71591431C0D630018B5514C66D6670BFAD1F8ACD363AC19BED486FB92B06DE83A4669C70
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(....." ..0.....>.... ...@..... .....+... ..`.....-..O....@.....H$...`.....,..T..... ....H.....text...D.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....H.....P .. ..p,.....BSJB.....v4.0.30319.....l...(...#~.....#Strings.....#US.....#GUID..... ..#Blob.....G.....3.....b...+.b.....O.....&.l....*....*....*....*...?.*...\.*....*....*.....[.....<..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\SslCertBinding.Net.dll

Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24200
Entropy (8bit):	6.286319408230414
Encrypted:	false
SSDEEP:	384:PecpB4zReJOVOm9FziUm0exVSiIgm19J8AG4oHHith5kCCeYghu+:3DgeO97m0exVfKwxniQghu+
MD5:	EDCEB39D12707299F6501AE9472A2FD1
SHA1:	F4BE70378AF9FEA7355307CF66E0F5A50590E974
SHA-256:	FA2C262A94F90DAD052A6A5D190F347CD1B8D8BACD7417B8B3FFF56F7D42ECB4
SHA-512:	08406BEDE6C980A1C36EC427C1D86F05F11A41EC366F3821D7B229649B10F3AF9D37AFE7A5A55C7D32D90F0B7D0A43848AF3B20DEA2D2D3669130AAA08729BE2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\SslCertBinding.Net.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8..U.....!.....:.....X... ...`..... .....x.. ..@.....X..W....`.....B.....\W..... ....H.....text....8... ...:..... ..`.rsrc.....`.....<.....@..@.rel oc.....@.....@..B.....X.....H.....$-..8*.....P .....\7..4...tTh.....A_RF...+X.P.k.....'....R|RY.r..d.(...._..h4.*...sN.:..QU.e...RY..% .....(.Y.Kf6.7.w...T..(;._|n....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..(....*..{....*"..} ....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\System.Threading.Tasks.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	35016
Entropy (8bit):	6.54246973766738
Encrypted:	false
SSDEEP:	384:WL0xHprBefGMOrRQY+hoZhOZkcvr3Eql38WqATrOhEZ0GftpBj1x+ILKHRN7c6lE:NRBefGBkoWjvr0VabKirxmcM+
MD5:	85F6F590B5C4B8C7253E9C403C9BE607
SHA1:	D5A9DB942A50C8821BACD7F6030202C57EC4708B
SHA-256:	D20552FD5C8C8C9759608A84DB1E216DA738F5E9F46DE9E8A3F39A0D6265CB8B
SHA-512:	9C78CB444E28618D44E9DEB23571FC7BBCE268882C2803E0CCC0E84B3E6EAB89C6AF2AAC0D81EF0D2C9FD1E9611CB35334EF3304FB16C5BA0481F6A7273C3(60
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.T.....!.....@....._... ...`..... ..`.....\_..O....`.....J...>.....$^..... ..... ..H.....text....?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B....._.....H.....h.../.....P .....#..ON.... "J.0..r....6RbR[..44....F.....E.X....1.XIE...:....5.M...Txn.\rycn.....o|.V}.. .|}.1En...`.T. \(e .u..=.nA...@p:.(.....}....*R..r...p.(.....(...+*N..r...p.(....(...+*R..r...p.(.....(...+*Z...r...p.(.....(...+*Z...r...p.(.....(...+*..0..$.....(...+..-.....*..o.....*.0..... (...+..-.s....z.o....*...0.....(...+..-.s....z.o....*...0.....(...+..-..*.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencysystem4.js	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18727
Entropy (8bit):	5.228912164616093
Encrypted:	false
SSDEEP:	384:vADBz8NWcg8Yt0Mp9sXYGb0JPMfBH1FBIpz4vl:vADBz8NWcg8Y2Mp9sXlb0OfBH1F+pz4t
MD5:	E001FBA3F73ADB83B5B9DCD2A32F1C7B
SHA1:	D0B3A5615F30226072BA90A961DBAD1CE0ED23E2
SHA-256:	60A987CFE5AE817D5D5ED82E1F39C3C537321EE9AB9A0B902DB2990F66B99887
SHA-512:	6DF77E4AC29B0AF120C2EE9380BACD4D1E02C08E9F6E7CD293959F7438294182B773B3C75E0DED111C3EEFD511B09FDF2F43927D68884572F745464705EE81A
Malicious:	false
Preview:	/*...Copyright (C) 1998-2009 Currency System, Inc. All rights reserved....$VER: Currency System Script Library 4.6..*/..../// Currency object constructor..//..function Cur rency(code, nameS, nameST, symbol, rateEUR, smallestUnit, regime, physical, legalTender, popularity)..{...this.code = code;...this.nameS = nameS; // singular...this.nam eST = nameST; // singular titlestyle...this.symbol = symbol;...this.rateEUR = rateEUR;...this.smallestUnit = smallestUnit;...this.regime = regime;...this.physical = physi cal;...this.legalTender = legalTender;...this.popularity = popularity;..}..../// CurrencySystem object constructor..//..function CurrencySystem()..{...this.version = "4.6";...this.i nitialized = 0;...//...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.converterCodeExists = currencySystem_converterCodeExists;...this.converterCodeIsUsed = currencySystem_converterCodeIsUsed;...this.converterUnusedCode = currenc

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencysystem5.js	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18850
Entropy (8bit):	5.252718939622608
Encrypted:	false
SSDEEP:	192:LVJMqzg8F9zp/OQMhEF7IXs1NmrgfTPzD5bL29h1FDiTYyf1CQx/TuTmkk6aez4U:LV2lg8FanXcmrgfTlwOH1ltsz4v8
MD5:	866B6E8A186BE6005A140CFE9F578CD8
SHA1:	E0B2E5344097EF4C1C0A8BE851C5DE27C7F490DB
SHA-256:	0A5731729919FEDC1A3B81C651087AB200C9470FA75A89BEBEA73AE0478F30E5
SHA-512:	BE84B6A9B893DC0D66113287942A388BAFB0629AE67E6C02A8E09E98A028D50CCFA082A2C1B5BFAFA273ACF9E6338E961FA208B62EF6BEE43D8BFD5E6D4619 A9
Malicious:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencysystem5.js	
Preview:	/*...Copyright (C) 1998-2012 Currency System, Inc. All rights reserved....$VER: Currency System Script Library 5.2..*/..../// Currency object constructor..//..function Currency(code, nameS, nameST, symbol, rateEUR, smallestUnit, regime, physical, legalTender, popularity)..{...this.code = code;...this.nameS = nameS; // singular...this.nameST = nameST; // singular titlestyle...this.symbol = symbol;...this.rateEUR = rateEUR;...this.smallestUnit = smallestUnit;...this.regime = regime;...this.physical = physical;...this.legalTender = legalTender;...this.popularity = popularity;..}..../// CurrencySystem object constructor..//..function CurrencySystem()..{...this.version = "5.1";...this.initialized = 0;.../...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.widgetCurrencyIsListed = currencySystem_widgetCurrencyIsListed;...this.widgetCurrencyIsUsed = currencySystem_widgetCurrencyIsUsed;...this.widgetSuggestUnusedCu

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencysystem5.json	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	635
Entropy (8bit):	4.968896753287593
Encrypted:	false
SSDEEP:	12:G3in27KkdcynYKFfaYKQItIl7eTaYKRHTaYKQItI9txrZOaYKB3i8T:G3i27KkdvYKtaYK3qteTaYKRHTaYK3qz
MD5:	D5BE63A1E66E4D6597F49BFD15EB3D83
SHA1:	6B0D0E3101EDB0C92C14691745765DE49CDB7C01
SHA-256:	A1CF701C876F916AACB12A3B952D1D2A38889C2AC118AF9D89493F0A86A45C5D
SHA-512:	6F8CD8F4D18D978F9B30E00322E3CC020B1C3ADD6B6307ED96EBB47B422DD15DDE4BB82698AE755CEF57F8BA3B1BDBD6F47D83CF08471E7B131B8CF8B20AC A55
Malicious:	false
Preview:	{...<currencysystem-insert-header>....."embedLicense": "This service is free to use as long as the banner and link appear on all pages using it. See the Attribution information at currencysystem.com.",..."embedSmallBannerGfx": "https://currencysystem.com/gfx/pub/script-button-88x31.png",..."embedSmallBannerText": "Powered by Currency System",..."embedSmallBannerLink": "https://currencysystem.com",....."embedSmallHomeGfx": "https://currencysystem.com/gfx/pub/script-icon-16x16.png",..."embedSmallHomeText": "Currrency System Homepage",..."embedSmallHomeLink": "https://currencysystem.com",.....<currencysystem-insert-currencies>..}

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\ecb-eurofxref-daily.xml	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.022779704233175
Encrypted:	false
SSDEEP:	6:TMVBd/5Q3JLHAc4Mj/9mc4C7drcDqhsDgLHLvvssw92PXCEZqilvs/BRi8LqfaR/:TMHduFHjFbdrcDWPu2XCMei8Lqai8L/
MD5:	376F44C2269588374F0F7E876BB3CFFA
SHA1:	1241AC750F7CA447D7A74EB516838C39516AA841
SHA-256:	3B96E197B1A47E7A391385638E13A0CF42E04E1665470A89EABECC67D1B91323
SHA-512:	744C894429453B5E40241FEA6A2EBD354BF2B06C5AD9B4439BE1CCACD15B89C487A1FE100851F23E7A2212CCAC600FC8519224855D7AC72F09E6AABD1E8AC6 C9
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<gesmes:Envelope xmlns:gesmes="http://www.gesmes.org/xml/2002-08-01" xmlns="http://www.ecb.int/vocabulary/2002-08-01/eurofxref">..<gesmes:subject>Reference rates</gesmes:subject>..<gesmes:Sender>...<gesmes:name>European Central Bank</gesmes:name>..</gesmes:Sender>..<Cube>... currencysystem-insert-->... /currencysystem-insert-->..</Cube>.</gesmes:Envelope>.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\adv.msi	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
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 Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {D9FF1A35-78F9-49F0-A6A0-DB3A11387835}, Number of Words: 8, Subject: JDesktop Tools, Author: JDesktop Integration Components (JDIC) Project, Name of Creating Application: Advanced Installer 18.7 build 0a7fdead, Template: ;1033, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	2233856
Entropy (8bit):	6.540847260876917
Encrypted:	false
SSDEEP:	49152:TDs/YrEUl8VlvfqAE/fQhksQQNgXAo1sVzhly+PkfsJJ10FRzVT8ajBK+ByqV4Tq:GYrEkXAEfs01sVNrajM+
MD5:	9AFC8137B547561655D454AFF862E567
SHA1:	2DAB8B1B9F1AE612E9CD359207751B452C76CB0D
SHA-256:	86747F0567ADBDD895E23E25760AF726A87000BD01EBEF994352EFAD7EB3987C
SHA-512:	91B99B561FBD3C6F3C2583CBF13D9FAF31AAFE6EFDB82667F646AD9F245904D3EF8F37B4CD11E141ECBEBDB7724414E21C4A8F7886CE68FFAC7B0BB8B153 3B
Malicious:	false
Preview:	.....>.....#.....I.....v.....|..... .....c.....%. ..8..... ...!..."...#...$...0.../..'...(...)...*...+...,...-.....6...1...2...3...4...5...9...7...?...C...:...;...<...=...>...B...@...A...K...S...D. ..E...F...G...H...R.....K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\help.chm	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	325845
Entropy (8bit):	7.966997729785747
Encrypted:	false
SSDEEP:	6144:upVysoxdLmULS5Nv5czGT6ozCF6DWc4kYBDrHDDoicYs0meNdts:iAsWJmUSjBczf3c4dHDDoicYs0re
MD5:	DF113262CBB4AD90D0D889620BDEFB06
SHA1:	D94D2111F9FD566941FF96DBA6237D126591E512
SHA-256:	195BAFB549728E15B392B5A2FCBD41003D2472B1AD82AED449175C37E5834657
SHA-512:	B3DDFCCEFFDE24791DFB9587D5AEBC406B9EC3408B38D50C70AC324931C37FD7F55099C7F84B8359A76ACA1BB0E350977451639CC0E61241EBE16D6F4DB909 6
Malicious:	false
Preview:	ITSF....`.....g.....|.{....."....|.{....."..`.....x.....T.....ITSP....T.....j..].!....."..T.....PMGL...../..../#IDXHDR.. .5.../#ITBITS..../#IVB...Rd./#STRINGS...U.i./#SYSTEM....;./#TOPICS...5.p./#URLSTR...Y.|./#URLTBL...%.4./#WINDOWS.....L./$FlftiMain...}..8./$OBJINST...>.?./$WWAs sociativeLinks/..../$WWAssociativeLinks/Property...:../$WWKeywordLinks/..../$WWKeywordLinks/Property...6. /about-how-create-a-catalog.html..{.z!/catalog-makers- context-menu.html..u.62/cd-catalog-creator-first-lanche-informations.html..+.[+/checkboxes-options-in-catalog-builder.html...x.../checkboxes_html_117d54ec.png...h.../chec kboxes_html_m548d6b7e.png...m.X./checkboxes_html_m59955fe6.png..._.../checkboxes_html_m678cf8a3.png...E.2 /context_menu_html_m6108afb8.png...S.n,/create- order-from-enduser-cd-catalogue.html..A..,/create_a_catalog_related_products_user.html...x.~./how-use-cd-catalog.html

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\icuio58.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54224
Entropy (8bit):	6.686697566242328
Encrypted:	false
SSDEEP:	1536:8n6iCEsBHqIXN0llUofqcOZkE5z7L/cLlvBQ+8iAYS:GuEsdXL/cLlGD1
MD5:	249D164D4361F1BBF827331A2C5B8E64
SHA1:	225AE2D2E277B817962D3A65666706BDF7AE6067
SHA-256:	492ADEB85D95834A97FC2C1BD61347202111A3773CE4DE35FC1597C52BE7AAB3
SHA-512:	16B656E17A305503A01C7429EC44DC9DED0DEC39F50844F5CAFF2484AF3F3551F11B620C63111361A5D333AA16A7DB0A2DC7FF5C895AA6C9252F21CA42223A1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....s_..s_..s_..._..s_F.p^..s_F.v^..s_F.w^..s_F.r^..s_..r^..s_.i._..s_ ..r_a.s_..w^..s_..v^..s_..s^..s_..._..s_..._..s_..q^..s_Rich..s_.....PE..L.....Z.....!.....r...6.....r.....J.....".....8.....) .....T.....@.....text....p.....r..... .`.rdata..."......$...v.....@..@.data.....@....rsrc...8..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\lcms-5.0.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4993536
Entropy (8bit):	6.871255823719978
Encrypted:	false
SSDEEP:	98304:vdG+iN2k+e/VO+0X30DQHDbOXh9A0DESaHafv4UZDCr:A+Hk+eX0BHDbOXh9A0DeHfUZDS
MD5:	B6723B31F67956E747493BC64F2C7A59
SHA1:	72389ECF849BFDA364E84258E5857A3DF07E5BFC
SHA-256:	3361AC8727ABA86AC7F3AAC3A214C3CB76F1AF9FF7EE5E94C52C30FDCB7D5064
SHA-512:	E17FEA164BB00E65BE0E58771A728FC9CED5BD65AE2FEC9E55C5697E69A498404B6D52B529DF774012C9F1268D29D97AD3CAFD404BAD58B3C36535A52AB6E0 9B
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$..... ...A...A...A...9N..A...*...A...*...A..4...A..4...A..4...A..4...A..h(.. .A..4...A...A..C..4...A..G4...A..G4"..A...AJ..A..G4...A..Rich.A..Rich.....PE..L...2.oa.....!.....87.....Py!.....P7.....L.....DJ...@.....P. E.D.....E.....G.H2.....I.,.....@.B.....B.@.....P7.....text....77.....87..... .`.rdata.....P7.....<7.....@..@.data..... F..b....E.....@....rsrc...H2....G..4...DG.....@..@.reloc.,.....I.....xI.....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\libeay32.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1379352
Entropy (8bit):	6.864605291373112
Encrypted:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\libeay32.dll	
SSDEEP:	24576:Rcbj++KpP3xREx5Fvvr3WH9IYf0mF8wBpoJqzTi1QA96:Rrpi3r3WH9IYf+wBpoJqzTi1QA96
MD5:	7CC7637AB23A01396206E82EF45CDA0E
SHA1:	209CC6CE91E24383213F1C2456D43E48BD09B8C4
SHA-256:	E6C6568A2CD61E401DB4E4F317F139852502EEBB9FE1FBB9C92D7ECFA6524F7F
SHA-512:	E13C48D6CB7B2983221F00C3FDC5DA4221D6B0383F68D74BCAC2AAF95CC7AE702E65DA517AAD51AD7DAD0B672F8436532F4612E7F0853AE0CA924635F3983FD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a..J%..%..%..,.....,...>..%.....!....%..0..,.....,...$..,...$..,...$..Rich%.....PE..L...<K.V.....!.....L.....u.....`.....@.....0...r..l...x.....0.....:.....pb.....0...@.....`..(.....text....J.....L..... ..`.rdata...V...`...X...P.....@..@.data.....t.....@....rsrc...0.....@..@.reloc..P.....".....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ml	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PDF document, version 1.5
Category:	dropped
Size (bytes):	418532
Entropy (8bit):	**7.992704655006582**
Encrypted:	**true**
SSDEEP:	12288:gC3QjgVE/DGk/1gsQR4jflsCEqmnUT9ca7cgTe9b:F3m7zqieCU4NlTO
MD5:	EF946663D3A336BDACB512BF32C8F8F2
SHA1:	1A02B2DEE5CD8815BA977A09505F0B38FEA27665
SHA-256:	0B77203265ADCB18A878383978BCE5C8D6A1D253FE1EFC16B8B161B42F03B79F
SHA-512:	B5E45C3F22F31FD1538C982C83F75DA1015FF56235B26EA1707DCA6B1BC1E41FB11557593CED91D5BF927B985511DBA4047C898A1FE9EB7903932FDBF6C8582
Malicious:	false
Preview:	%PDF-1.5.%.....2 0 obj.<</Type /ObjStm./N 100./First 806./Length 1140 ./Filter /FlateDecode.>>.stream.x.V]o.8.|....h..H.E...m.P\q.....d.r..fe.n....%.....*.y.....KB.. .4....d.....$..$i....P...I9.Z.R....I..%.c.#.eZ.)|.%.g...0i.Q.....E...&.^c..8..g.N.Y!..W.r... .A...!,.`.....0.....O`B.$.t8X",x=.)..BHi....<.$.x.Lb..2.....L.`.l)r..M....^.R.k....%.n.....^..' `..,...3.@e....P...5.Z..8&....9..j.g....|.H..P.....".Y..D.z1)...$.c..2.&,.....B..du.....&.....T.7j%..P-..#P/.9(*&5g....W..=..f.x.fc...{".8.,.w)....0.\..(.%..1..&.`v...(g.....r.K....;.y.....n.....S...+z.> {.....l+...r.{...#x.8....n....._.....1^...u..X.....n.7.9.1..c...Kz.....2t.rQ7..L.q.I.2{....'z.....=....]9....p.0.....n.vU?n...P....n"<...9).cu>.}_.I.be>4]7.....$i*N._t...1.....t..2....nG..o).. E..6.....r...se..=...;].vz...4.....y...S...E=. aH..zp.tP.*.. .Hu;u.f..?...)L.....U.P.y..1|..\.MH..=...C.....[]s?.....h....g.B9../..l....k..1:wE.S.v.:

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\plcd-player.exe	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3768184
Entropy (8bit):	6.323324235457555
Encrypted:	false
SSDEEP:	49152:mdziNWio/OWFGZ/7pqfwbAFj1IKdn9kvOIBzuJTHPfw8xZcca9KJi4EIdG:sBaNsKKdn9AzBqw8xZcca9KJi4s
MD5:	25DDBD309BB80942297043839777C7268
SHA1:	1574D860469EE784034093199DC9533543E5C096
SHA-256:	8C7E6A620F4BBC343C2695C2E034CC628062B5C2A6B05461FC41B05436F45147
SHA-512:	16CF4205B16F83A3EFEC96660190EFE254919EA18FBC6EB23F45D5C77B0A4A7EFD5DFA36EC1FC43BD79D1D4959A2FA9E172AB842CE7DE754CDC6291275289 2BA
Malicious:	false
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....N..,.....O....X..~....X..~....X..~....X..~.....~.....e...\..~....\. .~....\.#.....K.....\..~....Rich.....`.SH..R.`[RK..RJ.3RK..R.`.SK..RRichJ..R.....PE..L....,oa.....u.....@.....9.....q.9...@..... .....,S1.d.....4..5.....l9.x.....7.....@.....H...@.....x.....text..... ....rdata..B.....@..@.data....;...p1..(... T1.....@....rsrc....5....4..6...|4.....@..@.reloc.....7.....7.....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ssleay32.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	349720
Entropy (8bit):	6.600820777591867
Encrypted:	false
SSDEEP:	6144:Nv4Nuw10tGJjPZTbGT/yMzU/RSzBnEywGrfG/ySTJ7a7hNl/K5bv3jgNZuDwsLB+:N4Nuw10tGJjPZTbkyMzU/RSzBnHHrf+0
MD5:	F0AED1A32121A577594ECD66980C3ED3
SHA1:	288954A8D6F48639B7605488D2796B14291507E5
SHA-256:	D02CC01A7D9ADC1E6F980D1A56D6A641DF9E2A63FDC5F007264D1BF59ECC1446
SHA-512:	056670F3074AF5A03326C2BE5FFA0FEC23010DDC25BBED07B295EA3F6C7F8DFBC73E40E11E20103EFEB3B230096F630FB0A3CFA61C4E0A74C15A1CB6319D85D9
Malicious:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\ssleay32.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...r...r.....r.....r.....r.....r...s.4.r....\.r.....r.....r.....r.Rich..r.. .....PE..L...<K.V.....!.....I.....).....p.....p...9).....<.... ..0.....:...0...,..0.....x{..@..... .....text..... ..`.rdata.....@..@.data....[.....@.....@....rsrc...0... .....@..@.reloc..b3...0...4.....@..B..... ....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\decoder.dll	
Process:	C:\Users\user\Desktop\o4c8AUtX1g.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	6.451841062476738
Encrypted:	false
SSDEEP:	3072:Xnc8s5yYYVegTR5eO29YoYhNsli0rCckZ9uNDOQH5TmIKO+mAwzvX5Q+M9/:fV79tRUi7ckZSFxPtM9
MD5:	454418EBD68A4E905DC2B9B2E5E1B28C
SHA1:	A54CB6A80D9B95451E2224B6D95DE809C12C9957
SHA-256:	73D5F96A6A30BBD42752BFFC7F20DB61C8422579BF8A53741488BE34B73E1409
SHA-512:	171F85D6F6C44ACC90D80BA4E6220D747E1F4FF4C49A6E8121738E8260F4FCEB01FF2C97172F8A3B20E40E6F6ED29A0397D0C6E5870A9EBFF7B7FB6FAF20C647
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....z.....r.@.....@.....@.x.....@.....Rich..... .....PE..L.....Ia.....!.....X.....p.....@.....p.....<....p.. .....p..... ..@.....p..t..... .....text...\V.....X..... ..`.rdata..\....p.....\.....@..@.data...dV.....@....rsrc... ....p.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\AWSSDK.SimpleDB.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	62088
Entropy (8bit):	5.87884188749315
Encrypted:	false
SSDEEP:	1536:0mzFpEBNMGwcQHanzzd2UE/8YVkEyDrKe2xDBoPnp:dFpEBNMGwcsa8f/8a6Pp
MD5:	5AEB79663EA837F8A7A98DC04674B37A
SHA1:	536C24EF0572354E922A8C4A09CF5350D8A6164D
SHA-256:	E13D9F958783595ACD8ACDBFF4D587BCA7E7B6A3AAB796E2EFBD65BD37431536
SHA-512:	25E4E48EC2162EA6342CFD823E789ED0B5A995BB61FA3FA68364D1EE2468974FA4E75C17EB2CB3DDB213E633136C9AAB139BBF32FB8688FF5B1ABF444E8BB652
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....tx....." ..0..... ....@.....x.. ..@.....H...O..... ....x...8..... ....H.....text..... ....`.rsrc... .....@..@.reloc..... .....@..B.....\|.....H.....$b.....v.~....}.....(.....r...p(....*.r...p*.r...p*..{....*Br...p(.....*"..(....*&...(....*:..o.....(....*:.....(....*B .....(....*&...(....*..(....*F.(....s....(...*b.(....s....%.o!...(...*6.(.....(...*6..s....(....*R..s....%.o!...(....*&...(...*:...s....(....*V...s....%.o!...(....**....("...*>....s....(....*^....s....%..o!...(....*2..... (#...*.s$...*"..(%...*.0.....(.....(.....(...+*..

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\CrashRpt License.txt	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1569
Entropy (8bit):	5.078244393355221
Encrypted:	false
SSDEEP:	48:rIXOOrpJAzJzGl0PE9432sEs32s3IEtd132RTHy:peOrpJAzJzGlBq3b38OSTS
MD5:	734B7CB601EA82D8B4A9926373323B06
SHA1:	37490788B803335FA3AAD761B3EA0010889B2D8D
SHA-256:	90F301E30B61CDF8AC5E29F4FDD0E81C535FCAABF06B48D36B110A3F35E5A3D2
SHA-512:	273F154273DEDF9B06BBA74AEB81BF905309B6F137A414310B1E96C218095CC6B49EE663932815D6771C9BE1D033B014F57E7AE72C7B7FD396A9C254FA124706
Malicious:	false
Preview:	Copyright (c) 2003, The CrashRpt Project Authors...All rights reserved.....Redistribution and use in source and binary forms, with or without modification, ..are permitted provided that the following conditions are met:.... * Redistributions of source code must retain the above copyright notice, this .. list of conditions and the following disclaimer..... * Redistributions in binary form must reproduce the above copyright notice, .. this list of conditions and the following disclaimer in the documentation .. and/or other materials provided with the distribution..... * Neither the name of the author nor the names of its contributors .. may be used to endorse or promote prod ucts derived from this software without .. specific prior written permission.....THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUT ORS "AS IS" AND ANY ..EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES ..OF MERCHANTABILITY AND FITNESS

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Delimon.Win32.IO.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	940032
Entropy (8bit):	7.265468453378986
Encrypted:	false
SSDEEP:	12288:SjtToSCODTjAKMmNRYzUubi85LKHtToSCOD7jAK4mNRP:2Vxtqw/85LKHV1pt
MD5:	40C4EA80985E48C095D9F3AF80215C12
SHA1:	B7EAECB4CF5E45F7E3946BCD1C249A46428CA8C0
SHA-256:	2B1678502F69BCCBA816FE2901A12BD15567C4113D8EC5B0C9EBA3A1AEA7C633
SHA-512:	8C1FCFACEBA8273D4307FDC2AF0E8D137CF162838ED0C9AC198D0A29EC0E4E6B8A6B8C202BC415B2353889B4429ED9B07D784F367B2B339F65090242C78D64A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P.....!.....N.....l.. ....{g.. ..@.....l..S.....Pk..... ....H.....text....L... ...N..... ..`.rsrc.....P.....@..@.rel oc.....V.....@..B.....l.....H.....x.....j...n..P .....{.Z.L&.$.....v....lk..AC4..{E.0..X.....?3!...^..Q@..L.{._wSlwnsb].E.D...H=.{.s/.....H. f.q.kn...O.1y.\e.A./.[D.:#..T.h..6...}.....}.....s....}.....s....}.....(....*J.s....}'....(....*..0..).....{-.....(....t.....|-.....(...+...3.*....0..).....{-.....(....t.....|-.....(...+...3.*....0..).....{.....(....t. .....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\ICSharpCode.SharpZipLib.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	200704
Entropy (8bit):	5.683688089372797
Encrypted:	false
SSDEEP:	3072:hjMibqfQqFyGCDXiW9Pp/+Tl4abpuu201PB1BBXIDwtqSPVINrAfvp1:GibqI59PpOPf201/z7p
MD5:	C8164876B6F66616D68387443621510C
SHA1:	7A9DF9C25D49690B6A3C451607D311A866B131F4
SHA-256:	40B3D590F95191F3E33E5D00E534FA40F823D9B1BB2A9AFE05F139C4E0A3AF8D
SHA-512:	44A6ACCC70C312A16D0E533D3287E380997C5E5D610DBEAA14B2DBB5567F2C41253B895C9817ECD96C85D286795BBE6AB35FD2352FDDD9D191669A2FB0774E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<.K.....!..... .....^.... .....@.. .....@..... ..@.....K..... ....H.....text...d.... ....`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\License.txt	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Non-ISO extended-ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	4532
Entropy (8bit):	4.840297093762095
Encrypted:	false
SSDEEP:	96:D9moghaxhFkV9RGGQwGok+iOJ54d7JdEgUVVN7XzUKyeraku:knhIhmz8pJdLk/7XAKy7x
MD5:	54A36434CA791404E0EE1894A7FB257A
SHA1:	E99BA6366C22F9E4693F6317352EAA5854F0F429
SHA-256:	5FCC77BA8A6D6DCA5ECD466F7706133A17571EAAA1B45D4613E2BF5C58DEC678
SHA-512:	87942ABBE3BC1C87BB77323D4E43D63A30ACE3B569FF16363D871B77A306A64569A8655B0B3A526B31F901BA5F081BFE122B7DF7F0C491637DD3050EC948D07
Malicious:	false
Preview:	MyBusinessCatalog Platinum....Copyright: (c)2002-2021 Alexander Chulpanov..Homepage: http://www.MyBusinessCatalog.com..E-mail: info@MyBusinessCatalog.com..==========.....You should carefully read the following terms and..conditions before using this software..... ..MyBusinessCatalog is try-before-buy software. This means:....1. All copyrights to MyBusinessCatalog are exclusively owned by the author . Alexander Chulpanov.....2.1 You can use the FREE version of MyBusinessCatalog with restrictions applicable to unregistered version...The DEMO (free) version allows outputs 50 items (to PDF, Printer etc)..Trial periad - 30 days...If a Mobiliger subscription is already active, the trial period for..MyBusinessCatalog Free is automatically extended.....2.2 Registered version...MyBusinessCatalog Platinum - PDF Studio License...Allows creating PDF and Printable catalogs...Small Business License includes 1 (one) year of free software updates.....MyBusin

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Microsoft.Azure.KeyVault.Core.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16968
Entropy (8bit):	6.369067823836705
Encrypted:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Microsoft.Azure.KeyVault.Core.dll	
SSDEEP:	384:YdX0XY0X+DeljFWt6O9QHRN7fhKtklxHQJ:YdXuhvU8ZOJ
MD5:	FEC0A2AB4AB150DAD477E0D4885637CE
SHA1:	5A3C8920DE1B3F2F7867A20D05C94DE5B2779B81
SHA-256:	746760FE317B9721FB761209F0F9F7E1A5126390970AAC5FD93F11504FFE3D30
SHA-512:	11C7C941D31902CCC9F9E07166CF6E181E0ADF7BAEA0986B863CEFD71591431C0D630018B5514C66D6670BFAD1F8ACD363AC19BED486FB92B06DE83A4669C70
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(....." ..0.....>.... ...@..... .....+... ..`.....-..O....@.....H$...`.....,..T..... ....H.....text...D.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....H.....P .. ..p,.....BSJB.....v4.0.30319.....l...(...#~.....#Strings.....#US.....#GUID..... ..#Blob.....G.....3.....b...+.b.....O.....&.l....*....*....*....*...?.*...\.*....*....*.....[.....<..... .....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\SslCertBinding.Net.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24200
Entropy (8bit):	6.286319408230414
Encrypted:	false
SSDEEP:	384:PecpB4zReJOVOm9FziUm0exVSiIgm19J8AG4oHHith5kCCeYghu+:3DgeO97m0exVfKwxniQghu+
MD5:	EDCEB39D12707299F6501AE9472A2FD1
SHA1:	F4BE70378AF9FEA7355307CF66E0F5A50590E974
SHA-256:	FA2C262A94F90DAD052A6A5D190F347CD1B8D8BACD7417B8B3FFF56F7D42ECB4
SHA-512:	08406BEDE6C980A1C36EC427C1D86F05F11A41EC366F3821D7B229649B10F3AF9D37AFE7A5A55C7D32D90F0B7D0A43848AF3B20DEA2D2D3669130AAA08729BE2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8..U.....!.....:.....X... ...`..... .....x.. ..@.....X..W....`.....B.....\W..... ....H.....text....8... ...:..... ..`.rsrc.....`.....<.....@..@.rel oc.....@.....@..B.....X.....H.....$-..8*.....P .....\7..4...tTh.....A_RF...+X.P.k.....'....R|RY.r..d.(...._..h4.*...sN.:..QU.e...RY..% .....(.Y.Kf6.7.w...T..(;._|n....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\System.Threading.Tasks.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	35016
Entropy (8bit):	6.54246973766738
Encrypted:	false
SSDEEP:	384:WL0xHprBefGMOrRQY+hoZhOZkcvr3Eql38WqATrOhEZ0GftpBj1x+ILKHRN7c6lE:NRBefGBkoWjvr0VabKirxmcM+
MD5:	85F6F590B5C4B8C7253E9C403C9BE607
SHA1:	D5A9DB942A50C8821BACD7F6030202C57EC4708B
SHA-256:	D20552FD5C8C8C9759608A84DB1E216DA738F5E9F46DE9E8A3F39A0D6265CB8B
SHA-512:	9C78CB444E28618D44E9DEB23571FC7BBCE268882C2803E0CCC0E84B3E6EAB89C6AF2AAC0D81EF0D2C9FD1E9611CB35334EF3304FB16C5BA0481F6A7273C360
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....6.T.....!.....@.....\_... ...`..... ..`.....\_..O....`.....J...>.....$^..... ..... ..H.....text....?... ...@..... ..`.rsrc.....`.....B.....@..@.rel oc.....H.....@..B....._.....H.....h..../.....P .....#..ON.... "J.0..r....6RbR[..44....F.....E.X....1.XIE...:....5.M...Txn.\rycn.....o|.V}.. .|}.1En...`.T. \(e .u..=.nA...@p:.(.....}....*R..r...p.(.....(...+*N..r...p.(....(...+*R..r...p.(.....(...+*Z...r...p.(.....(...+*Z...r...p.(.....(...+*..0..$.....(...+..-.....*..o.....*.0..... (...+..-.s....z.o....*...0.....(...+..-.s....z.o....*...0.....(...+..-..*.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\currencysystem4.js	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18727
Entropy (8bit):	5.228912164616093
Encrypted:	false
SSDEEP:	384:vADBz8NWcg8Yt0Mp9sXYGb0JPMfBH1FBIpz4vl:vADBz8NWcg8Y2Mp9sXlb0OfBH1F+pz4t
MD5:	E001FBA3F73ADB83B5B9DCD2A32F1C7B
SHA1:	D0B3A5615F30226072BA90A961DBAD1CE0ED23E2
SHA-256:	60A987CFE5AE817D5D5ED82E1F39C3C537321EE9AB9A0B902DB2990F66B99887
SHA-512:	6DF77E4AC29B0AF120C2EE9380BACD4D1E02C08E9F6E7CD293959F7438294182B773B3C75E0DED111C3EEFD511B09FDF2F43927D68884572F745464705EE81A
Malicious:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\currencysystem4.js	
Preview:	/*...Copyright (C) 1998-2009 Currency System, Inc. All rights reserved....$VER: Currency System Script Library 4.6..*/..../// Currency object constructor..//..function Currency(code, nameS, nameST, symbol, rateEUR, smallestUnit, regime, physical, legalTender, popularity)..{...this.code = code;...this.nameS = nameS; // singular...this.nameST = nameST; // singular titlestyle...this.symbol = symbol;...this.rateEUR = rateEUR;...this.smallestUnit = smallestUnit;...this.regime = regime;...this.physical = physical;...this.legalTender = legalTender;...this.popularity = popularity;..}..../// CurrencySystem object constructor..//..function CurrencySystem()..{...this.version = "4.6";...this.initialized = 0;.../...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.converterCodeExists = currencySystem_converterCodeExists;...this.converterCodeIsUsed = currencySystem_converterCodeIsUsed;...this.converterUnusedCode = currenc

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\currencysystem5.js	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18850
Entropy (8bit):	5.252718939622608
Encrypted:	false
SSDEEP:	192:LVJMqzg8F9zp/OQMhEF7IXs1NmrgfTPzD5bL29h1FDiTYyf1CQx/TuTmkk6aez4U:LV2lg8FanXcmrgfTlwOH1ltsz4v8
MD5:	866B6E8A186BE6005A140CFE9F578CD8
SHA1:	E0B2E5344097EF4C1C0A8BE851C5DE27C7F490DB
SHA-256:	0A5731729919FEDC1A3B81C651087AB200C9470FA75A89BEBEA73AE0478F30E5
SHA-512:	BE84B6A9B893DC0D66113287942A388BAFB0629AE67E6C02A8E09E98A028D50CCFA082A2C1B5BFAFA273ACF9E6338E961FA208B62EF6BEE43D8BFD5E6D4619A9
Malicious:	false
Preview:	/*...Copyright (C) 1998-2012 Currency System, Inc. All rights reserved....$VER: Currency System Script Library 5.2..*/..../// Currency object constructor..//..function Currency(code, nameS, nameST, symbol, rateEUR, smallestUnit, regime, physical, legalTender, popularity)..{...this.code = code;...this.nameS = nameS; // singular...this.nameST = nameST; // singular titlestyle...this.symbol = symbol;...this.rateEUR = rateEUR;...this.smallestUnit = smallestUnit;...this.regime = regime;...this.physical = physical;...this.legalTender = legalTender;...this.popularity = popularity;..}..../// CurrencySystem object constructor..//..function CurrencySystem()..{...this.version = "5.1";...this.initialized = 0;.../...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.widgetCurrencyIsListed = currencySystem_widgetCurrencyIsListed;...this.widgetCurrencyIsUsed = currencySystem_widgetCurrencyIsUsed;...this.widgetSuggestUnusedCu

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\currencysystem5.json	
Process:	C:\Windows\System32\msiexec.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	635
Entropy (8bit):	4.968896753287593
Encrypted:	false
SSDEEP:	12:G3in27KkdcynYKFfaYKQItIl7eTaYKRHTaYKQItI9txrZOaYKB3i8T:G3i27KkdvYKtaYK3qteTaYKRHTaYK3qz
MD5:	D5BE63A1E66E4D6597F49BFD15EB3D83
SHA1:	6B0D0E3101EDB0C92C14691745765DE49CDB7C01
SHA-256:	A1CF701C876F916AACB12A3B952D1D2A38889C2AC118AF9D89493F0A86A45C5D
SHA-512:	6F8CD8F4D18D978F9B30E00322E3CC020B1C3ADD6B6307ED96EBB47B422DD15DDE4BB82698AE755CEF57F8BA3B1BDBD6F47D83CF08471E7B131B8CF8B20AA55
Malicious:	false
Preview:	{...<currencysystem-insert-header>....."embedLicense": "This service is free to use as long as the banner and link appear on all pages using it. See the Attribution information at currencysystem.com.",..."embedSmallBannerGfx": "https://currencysystem.com/gfx/pub/script-button-88x31.png",..."embedSmallBannerText": "Powered by Currency System",..."embedSmallBannerLink": "https://currencysystem.com",....."embedSmallHomeGfx": "https://currencysystem.com/gfx/pub/script-icon-16x16.png",..."embedSmallHomeText": "Currrency System Homepage",..."embedSmallHomeLink": "https://currencysystem.com",.....<currencysystem-insert-currencies>..}

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\ecb-eurofxref-daily.xml	
Process:	C:\Windows\System32\msiexec.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.022779704233175
Encrypted:	false
SSDEEP:	6:TMVBd/5Q3JLHAc4Mj/9mc4C7drcDqhsDgLHLvvssw92PXCEZqilvs/BRi8LqfaR/:TMHduFHjFbdrcDWPu2XCMei8Lqai8L/
MD5:	376F44C2269588374F0F7E876BB3CFFA
SHA1:	1241AC750F7CA447D7A74EB516838C39516AA841
SHA-256:	3B96E197B1A47E7A391385638E13A0CF42E04E1665470A89EABECC67D1B91323
SHA-512:	744C894429453B5E40241FEA6A2EBD354BF2B06C5AD9B4439BE1CCACD15B89C487A1FE100851F23E7A2212CCAC600FC8519224855D7AC72F09E6AABD1E8AC6C9
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8"?>.<gesmes:Envelope xmlns:gesmes="http://www.gesmes.org/xml/2002-08-01" xmlns="http://www.ecb.int/vocabulary/2002-08-01/eurofxref">..<gesmes:subject>Reference rates</gesmes:subject>..<gesmes:Sender>...<gesmes:name>European Central Bank</gesmes:name>..</gesmes:Sender>..<Cube>... currencysystem-insert-->... /currencysystem-insert-->..</Cube>.</gesmes:Envelope>.

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\help.chm	
Process:	C:\Windows\System32\msiexec.exe

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\help.chm	
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	325845
Entropy (8bit):	7.966997729785747
Encrypted:	false
SSDEEP:	6144:upVysoxdLmULS5Nv5czGT6ozCF6DWc4kYBDrHDDoicYs0meNdts:iAsWJmUSjBczf3c4dHDDoicYs0re
MD5:	DF113262CBB4AD90D0D889620BDEFB06
SHA1:	D94D2111F9FD566941FF96DBA6237D126591E512
SHA-256:	195BAFB549728E15B392B5A2FCBD41003D2472B1AD82AED449175C37E5834657
SHA-512:	B3DDFCCEFFDE24791DFB9587D5AEBC406B9EC3408B38D50C70AC324931C37FD7F55099C7F84B8359A76ACA1BB0E350977451639CC0E61241EBE16D6F4DB909 6
Malicious:	false
Preview:	ITSF....`.....g.....|.{....."....|.{....."..`.....x.....T.....ITSP....T.....j..].!....."..T.....PMGL...../..../#IDXHDR.. .5.../#ITBITS..../#IVB...Rd./#STRINGS...U.i./#SYSTEM....;./#TOPICS...5.p./#URLSTR...Y.|./#URLTBL...%.4./#WINDOWS.....L./$FIftiMain...}..8./$OBJINST...>.?./$WWAs sociativeLinks/..../$WWAssociativeLinks/Property...:../$WWKeywordLinks/..../$WWKeywordLinks/Property...6. /about-how-create-a-catalog.html..{.z!/catalog-makers- context-menu.html..u.62/cd-catalog-creator-first-lanche-informations.html..+.[+/checkboxes-options-in-catalog-builder.html...x.../checkboxes_html_117d54ec.png...h.../chec kboxes_html_m548d6b7e.png...m.X./checkboxes_html_m59955fe6.png..._.../checkboxes_html_m678cf8a3.png...E.2 /context_menu_html_m6108afb8.png...S.n,/create- order-from-enduser-cd-catalogue.html..A../create_a_catalog_related_products_user.html...x.~./how-use-cd-catalog.html

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\icuio58.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54224
Entropy (8bit):	6.686697566242328
Encrypted:	false
SSDEEP:	1536:8n6iCEsBHqIXN0llUofqcOZkE5z7L/cLlvBQ+8iAYS:GuEsdXL/cLlGD1
MD5:	249D164D4361F1BBF827331A2C5B8E64
SHA1:	225AE2D2E277B817962D3A65666706BDF7AE6067
SHA-256:	492ADEB85D95834A97FC2C1BD61347202111A3773CE4DE35FC1597C52BE7AAB3
SHA-512:	16B656E17A305503A01C7429EC44DC9DED0DEC39F50844F5CAFF2484AF3F3551F11B620C63111361A5D333AA16A7DB0A2DC7FF5C895AA6C9252F21CA42223A1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....s_..s_..s_..._..s_F.p^..s_F.v^..s_F.w^..s_F.r^..s_..r^..s_.i._..s_ ..r_a.s_..w^..s_..v^..s_..s^..s_..._..s_..._..s_..q^..s_Rich..s_.....PE..L.....Z.....!.....r...6.....r.....J.....".....8.....) .....T.....@.....text....p.....r..... ..`.rdata...".....$...v.....@..@.data.....@....rsrc...8..... .....@..@.reloc.....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\lcms-5.0.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4993536
Entropy (8bit):	6.871255823719978
Encrypted:	false
SSDEEP:	98304:vdG+iN2k+e/VO+0X30DQHDbOXh9A0DESaHafv4UZDCr:A+Hk+eX0BHDbOXh9A0DeHfUZDS
MD5:	B6723B31F67956E747493BC64F2C7A59
SHA1:	72389ECF849BFDA364E84258E5857A3DF07E5BFC
SHA-256:	3361AC8727ABA86AC7F3AAC3A214C3CB76F1AF9FF7EE5E94C52C30FDCB7D5064
SHA-512:	E17FEA164BB00E65BE0E58771A728FC9CED5BD65AE2FEC9E55C5697E69A498404B6D52B529DF774012C9F1268D29D97AD3CAFD404BAD58B3C36535A52AB6E0 9B
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$..... ...A...A...A...9N..A...*...A...*...A..4...A..4...A..4...A..4...A..h(.. .A..4...A...A..C..4...A..G4...A..G4"..A...AJ..A..G4...A..Rich.A..Rich.....PE..L...2.oa.....!.....87.....Py!.....P7.....L.....DJ...@.....P. E.D.....E.....G.H2.....I.....@.B.....B.@.....P7.....text....77.....87..... ..`.rdata.....P7.....<7.....@..@.data..... F..b....E.....@....rsrc...H2....G..4...DG.....@..@.reloc..,.....I.....xI.....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\libeay32.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1379352
Entropy (8bit):	6.864605291373112
Encrypted:	false
SSDEEP:	24576:Rcbj++KpP3xREx5Fvvr3WH9IYf0mF8wBpoJqzTi1QA96:Rrpi3r3WH9IYf+wBpoJqzTi1QA96

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\libeay32.dll	
MD5:	7CC7637AB23A01396206E82EF45CDA0E
SHA1:	209CC6CE91E24383213F1C2456D43E48BD09B8C4
SHA-256:	E6C6568A2CD61E401DB4E4F317F139852502EEBB9FE1FBB9C92D7ECFA6524F7F
SHA-512:	E13C48D6CB7B2983221F00C3FDC5DA4221D6B0383F68D74BCAC2AAF95CC7AE702E65DA517AAD51AD7DAD0B672F8436532F4612E7F0853AE0CA924635F3983FD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a..J%..%..%..,.....,...>..%.....!.....%..0..,.....,...$..,...$..,...$..Rich%.....PE..L...<K.V.....!.....L.....u.....`.....@.....0...r..I...x.....0.....:.....pb.....0...@.....`..(.....text....J.....L..... ..`.rdata...V...`...X...P.....@..@.data.....t.....@....rsrc...0.....@..@.reloc..P....."....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\ml	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PDF document, version 1.5
Category:	dropped
Size (bytes):	418532
Entropy (8bit):	**7.992704655006582**
Encrypted:	**true**
SSDEEP:	12288:gC3QjgVE/DGk/1gsQR4jflsCEqmnUT9ca7cgTe9b:F3m7zqieCU4NlTO
MD5:	EF946663D3A336BDACB512BF32C8F8F2
SHA1:	1A02B2DEE5CD8815BA977A09505F0B38FEA27665
SHA-256:	0B77203265ADCB18A878383978BCE5C8D6A1D253FE1EFC16B8B161B42F03B79F
SHA-512:	B5E45C3F22F31FD1538C982C83F75DA1015FF56235B26EA1707DCA6B1BC1E41FB11557593CED91D5BF927B985511DBA4047C898A1FE9EB7903932FDBF6C8582
Malicious:	false
Preview:	%PDF-1.5.%.....2 0 obj.<<./Type /ObjStm./N 100./First 806./Length 1140 ./Filter /FlateDecode.>>.stream.x.V]o.8.|....h..H.E...m.P\q.....d.r..fe.n....%.....*.y.....KB.. .4....d.....$..$i....P...I9.Z.R....I..%.c.#.eZ.)|.%.g...0i.Q.....E...&.^c..8..g.N.Y!..W.r... .A...!,.`.....0.....O`B.$.t8X",x=.)..BHi....<.$.x.Lb..2.....L.`.l)r..M....^.R.k....%.n.....^..' `..,...3.@e....P...5.Z..8&....9..j.g....|.H..P.....".Y..D.z1)...$.c..2.&,.....B..du.....&.....T.7j%..P-..#P/.9(*&5g....W..=..f.x.fc...{".8.,.w)....0.\..(.%..1..&.`v...(g.....r.K....;.y.....n.....S...+z.> {.....l+...r.{...#x.8....n....._.....1^...u..X.....n.7.9.1..c...Kz.....2t.rQ7..L.q.I.2{....'z.....=....]9....p.0.....n.vU?n...P....n"<...9).cu>.}_.I.be>4]7.....$i*N._t...1.....t..2....nG..o).. E..6.....r...se..=...;].vz...4.....y...S...E=. aH..zp.tP.*.. .Hu;u.f..?...)L.....U.P.y..1|..\.MH..=...C.....[]s?.....h....g.B9../..l....k..1:wE.S.v.:

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\plcd-player.exe	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3768184
Entropy (8bit):	6.323324235457555
Encrypted:	false
SSDEEP:	49152:mdziNWio/OWFGZ/7pqfwbAFj1IKdn9kvOIBzuJTHPfw8xZcca9KJi4EIdG:sBaNsKKdn9AzBqw8xZcca9KJi4s
MD5:	25DDBD309BB80942297043839777C7268
SHA1:	1574D860469EE784034093199DC9533543E5C096
SHA-256:	8C7E6A620F4BBC343C2695C2E034CC628062B5C2A6B05461FC41B05436F45147
SHA-512:	16CF4205B16F83A3EFEC96660190EFE254919EA18FBC6EB23F45D5C77B0A4A7EFD5DFA36EC1FC43BD79D1D4959A2FA9E172AB842CE7DE754CDC6291275289 BA
Malicious:	**true**
Preview:	MZ.....@.....8.....!..L.!This program cannot be run in DOS mode....$.....N..,.....O....X..~....X..~....X..~....X..~.....~.....e...\..~....\. .~....\.#.....K.....\..~....Rich.....`.SH..R.`[RK..RJ.3RK..R.`.SK..RRichJ..R.....PE..L....,oa.....u.....@.....9.....q.9...@..... .....,S1.d.....4..5.....l9.x.....7.....@.....H...@.....x.....text..... ....rdata..B.....@..@.data...;...p1..(... T1.....@....rsrc....5....4..6...|4.....@..@.reloc.....7.....7.....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\ssleay32.dll	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	349720
Entropy (8bit):	6.600820777591867
Encrypted:	false
SSDEEP:	6144:Nv4Nuw10tGJjPZTbGT/yMzU/RSzBnEywGrfG/ySTJ7a7hNl/K5bv3jgNZuDwsLB+:N4Nuw10tGJjPZTbkyMzU/RSzBnHHrf+0
MD5:	F0AED1A32121A577594ECD66980C3ED3
SHA1:	288954A8D6F48639B7605488D2796B14291507E5
SHA-256:	D02CC01A7D9ADC1E6F980D1A56D6A641DF9E2A63FDC5F007264D1BF59ECC1446
SHA-512:	056670F3074AF5A03326C2BE5FFA0FEC23010DDC25BBED07B295EA3F6C7F8DFBC73E40E11E20103EFEB3B230096F630FB0A3CFA61C4E0A74C15A1CB6319D85 D9
Malicious:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\ssleay32.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...r...r.....r.....r.....r.....r...s.4.r....\.r.....r.....r.....r.Rich..r.. .....PE..L...<K.V.....!.....!.....)..... .....p.....p...9).....<.... ..0.....:...0...,..0.....x{..@..... .....text..... ..`.rdata.....@..@.data....[.....@.....@....rsrc...0... .....@..@.reloc..b3...0...4.....@..B..... ....

C:\Windows\Installer\440bbd.msi	
Process:	C:\Windows\System32\msiexec.exe
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 Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {D9FF1A35-78F9-49F0-A6A0-DB3A11387835}, Number of Words: 8, Subject: JDesktop Tools, Author: JDesktop Integration Components (JDIC) Project, Name of Creating Application: Advanced Installer 18.7 build 0a7fdead, Template: ;1033, Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	2233856
Entropy (8bit):	6.540847260876917
Encrypted:	false
SSDEEP:	49152:TDs/YrEUl8VlvfqAE/fQhksQQNgXAo1sVzhly+PkfsJJ10FRzVT8ajBK+ByqV4Tq:GYrEkXAEfs01sVNrajM+
MD5:	9AFC8137B547561655D454AFF862E567
SHA1:	2DAB8B1B9F1AE612E9CD359207751B452C76CB0D
SHA-256:	86747F0567ADBDD895E23E25760AF726A87000BD01EBEF994352EFAD7EB3987C
SHA-512:	91B99B561FBD3C6F3C2583CBF13D9FAF31AAFE6EFDB82667F646AD9F245904D3EF8F37B4CD11E141ECBEBDB7724414E21C4A8F7886CE68FFAC7B0BB8B1B53 3B
Malicious:	false
Preview:	.....>.....#.....I.....v.....|..... .....c.....%. ..8..... ...!..."...#...$...0.../...'...(...)...*...+...,...-.....6...1...2...3...4...5...9...7...?...C...:...;...<...=...>...B...@...A...K...S...D. ..E...F...G...H...R.....K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\MSI11D7.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F627 BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J..!...T..!...T..!...T..!...T..!..J..!..J..!..J..!..!... ...T...!...T..!...T..!...T. .!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6\|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI1488.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F627 BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J..!...T..!...T..!...T..!...T..!..J..!..J..!..J..!..!... ...T...!...T..!...T..!...T. .!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6\|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI15F0.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F627BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J...!...T..!...T..!...T..!..J..!..J..!..J..!..!.. ...T...!...T..!...T..!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI16EB.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	887264
Entropy (8bit):	6.436854443892135
Encrypted:	false
SSDEEP:	24576:gJgZXlAIjfQhETbF+RWQNgXAo1sVz1v0Mny+PkfsJJ10FRzVTv:F/fQhksQQNgXAo1sVzhly+PkfsJJ10FT
MD5:	0BE6E02D01013E6140E38571A4DA2545
SHA1:	9149608D60CA5941010E33E01D4FDC7B6C791BEA
SHA-256:	3C5DB91EF77B947A0924675FC1EC647D6512287AA891040B6ADE3663AA1FD3A3
SHA-512:	F419A5A95F7440623EDB6400F9ADBFB9BA987A65F3B47996A8BB374D89FF53E8638357285485142F76758BFFCB9520771E38E193D89C82C3A9733ED98AE24FCB
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....4.....3.....3.....3.?..... W....3.....Rich.....PE..L.....Ia....."!.....KC....@.....t...d.....p.....T.....p.....@... ....h...@.....text..... ..`.rdata.....@..@.data...4.....@....rsrc.....|.....@..@.reloc..T..... .....@..B..... .....

C:\Windows\Installer\MSI1815.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F627BA
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@p..!..!..!..J..!..J...!...T..!...T..!...T..!..J..!..J..!..J..!..!.. ...T...!...T..!...T..!..!..!...T..!..Rich.!.....PE..L...".Ia....."!.....*.....6|.....P.....k.....@.....p.....D.....0.....A...8..p.....@:..... .H9..@.....$.....text...6..... ..`.rdata..8.....@..@.data.....@....rsrc...0.....@..@.reloc...A.....B... .....@..B..... .....

C:\Windows\Installer\MSI193F.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	587232
Entropy (8bit):	6.421744382064001
Encrypted:	false
SSDEEP:	12288:qKrajAXKBGIpTOS7OmddoqaclGOh40JEh+DiYgZmD8x32id4PlV1uJTG:dajmU120q+Byd4V4TG

C:\Windows\Installer\MSI193F.tmp	
MD5:	2A6C81882B2DB41F634B48416C8C8450
SHA1:	F36F3A30A43D4B6EE4BE4EA3760587056428CAC6
SHA-256:	245D57AFB74796E0A0B0A68D6A81BE407C7617EC6789840A50F080542DACE805
SHA-512:	E9EF1154E856D45C5C37F08CF466A4B10DEE6CF71DA47DD740F2247A7EB8216524D5B37FF06BB2372C31F6B15C38101C19A1CF7185AF12A17083207208C6CCB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PD.z>..z>..z>...=..z>...;.Xz>...:..z>...=..z>...:..z>...;..z>...8..z>. ..?..z>..z?..{>.K.7..z>.K.>..z>.K....z>..z...z>.K.<..z>.Rich.z>.....PE..L.....la....."!.....T.....I.....p..... .....)....@.....r.....s.....h..... .....X.....p.....x...@.....p.....p..@.....text....S.....T..... ..`.rdata.....p.....X.....@..@.data.....n.....@....rsrc...h... .....|.....@..@.reloc...X.....Z.....@..B..... .....

C:\Windows\Installer\MSI3F85.tmp	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	7026
Entropy (8bit):	5.541123008392793
Encrypted:	false
SSDEEP:	192:YUSgIVbUcFgRLfqnJVjE/HT+qOLsZzibbiMMkzQe4ksKJBwb:YUSgINHFgRLfqnJVjE/HT+qwsZzibbid
MD5:	9CAB97F717701D6FB15A69CC1B29810D
SHA1:	30260027C03E49562C9C90C90DAB8BF00F295A56
SHA-256:	345CAEE89596ACE857B062A71AF36767E88F3ECEFA35DD7523888529631C4F7A
SHA-512:	2322805CC581B672BB87D9D7F38D2C2C93A0093DF2F492ED7DB346A11F4235C91A479E8A148DE071C7D6873C304924E2547D701F49233544BF27DCDD59CA496
Malicious:	false
Preview:	...@IXOS.@.....@"]YS.@.....@.....@.....@.....@.....@.....&.{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}..JDesktop Tools..adv.msi.@.....@.....@.....@.....@.....&.{D9FF1A 35-78F9-49F0-A6A0-DB3A11387835}.....@.....@.....@.....@.....@.....@.....@.....@.....JDesktop Tools.....Rollback..Rolling back action:....RollbackCleanup..Removing b ackup files..File: [1]...@.....@.....ProcessComponents..Updating component registration...@.....@.....@.].....&.{F5BA1B6B-756B-4B40-A5CB-A8A21E79DAE6}].C:\U sers\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\.@.....@.....@.....@.....&.{FC3D5B52-2561-4633-85CB-6F8B8A8 6F2F9}R.01:\Software\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Version.@.....@.....@.....@.....&.{8C82D735-0397-4468-B16C-3DB17F7A7006}f. 01:\Software\Caphyon\Advanced Installer\LZMA\{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}\3.4.0.2\AI_ExePath.@.....@.....@.....@.....&.{0B568A04-369C-43FB- 98E4-C437A15709E0}I.C:\Users\user\AppData\Roam

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	
Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	79122
Entropy (8bit):	5.282105373471904
Encrypted:	false
SSDEEP:	192:jmXs969ozNSkk3peTBYeHt0tfoI9qsjl0urmwYyio:yXs9UogeWeH29qclhmwYyio
MD5:	B5E2563FF9A8BBA4AE2605C562F1566C
SHA1:	461A990EEDB948D9F539D28A7D36147AB037B5CB
SHA-256:	B083E139C5D016B77E22DA876357A7E8CA6EFF8FE119DA02A0C91448B5611F5C
SHA-512:	2BD1C7FCF4D900EA797B7B3BE1DAF2989AA9024DC3716DE66EAFFCC4733637C34E326C79A8A92C6EA2311534F86A2E14D75DC07E48A68507B0570C4E6049E0 6
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 03:22:38.143 [320]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03 F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.159 [320]: ngen returning 0x00000000..07/23/2020 03:22:38.222 [3748]: Command line: C:\Wi ndows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Word, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7 F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.237 [3748]: ngen returning 0x00000000..07/23/2020 03:22:38.284 [64]: Command line: C:\Windows \Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Common.Implementation, Version=10.0.0.00000, Culture=neutral, PublicKeyT oken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 03:22:38.300 [64]:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.710856115150992
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%

General

File name:	o4c8AUtX1g.exe
File size:	7840232
MD5:	c7db399951b19ea446599dc3800a3111
SHA1:	b01352206ec1935a1123d7d4ea8394647e6b3d00
SHA256:	ceba6a7f9a2c25a35090470c6209aefed808786c47194a18415a7898390c20cb
SHA512:	974c8824a2bd3cc7b65d3de4c8cfdb72564ab9b351528510ffd24d50c314afb9789130cf6e46e70ba41d199f37540c1628e0ef83afea2ec2f3499e8d188a6782
SSDEEP:	196608:cL6ocnTAcca9KJi4G+eiPUei/L6StB1o4lLMjgfIg/rNv+J3U:G6JnTAcca9KJi4teSq/WSb6aagfTTiU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K...K...K...J...K...JX..K...J...K...J...K...J...K...J...K...J...K...J...K...J...K...K ..KX..J...KX.oK...K...K...KX..J...

File Icon

Icon Hash:	f0c49c70f99cc4f0

Static PE Info

General

Entrypoint:	0x52c471
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6149D0A9 [Tue Sep 21 12:31:37 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	0748c08f838865e5d72743f7fd7e551e

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=Sectigo Public Code Signing CA EV R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 9/2/2021 2:00:00 AM 9/3/2022 1:59:59 AM
Subject Chain	• CN=Baltic Auto SIA, O=Baltic Auto SIA, S=RÄ«ga, C=LV, OID.2.5.4.15=Private Organization, OID.1.3.6.1.4.1.311.60.2.1.3=LV, SERIALNUMBER=40103318287
Version:	3
Thumbprint MD5:	80D1AF7742336F8CCA96BF7A44976DF2
Thumbprint SHA-1:	30576D884D8311D503D9CB030FD547DC26D1AB6B
Thumbprint SHA-256:	1F893C08CE7915D76394082DD884A6771493247B9169B6579AED99F8606AD484
Serial:	3D3FC30099D6C7AEB806D4181992AF90

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x183b2f	0x183c00	False	0.450583796744	data	6.42629991801	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x185000	0x60684	0x60800	False	0.325258561367	data	4.58910819653	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1e6000	0x6e78	0x5600	False	0.130405159884	data	2.02713431011	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1ed000	0x38ea0	0x39000	False	0.239840323465	data	5.41863510681	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x226000	0x19c0c	0x19e00	False	0.504642210145	data	6.56301368687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 11:41:38.929428101 CEST	192.168.2.4	8.8.8.8	0xcbf4	Standard query (0)	get.updates.avast.cn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 11:41:38.952285051 CEST	8.8.8.8	192.168.2.4	0xcbf4	Name error (3)	get.updates.avast.cn	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: o4c8AUtX1g.exe PID: 3408 Parent PID: 6804

General

Start time:	11:40:42
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\o4c8AUtX1g.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\o4c8AUtX1g.exe'
Imagebase:	0x1290000
File size:	7840232 bytes
MD5 hash:	C7DB399951B19EA446599DC3800A3111
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: msiexec.exe PID: 5776 Parent PID: 568

General

Start time:	11:40:46
Start date:	25/10/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff777c90000
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

Show Windows behavior

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: msiexec.exe PID: 768 Parent PID: 5776

General

Start time:	11:40:47
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding D90C408BAA115D1625882500CC5A128EC
Imagebase:	0x290000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: 5944 Parent PID: 3408

General

Start time:	11:40:48
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\system32\msiexec.exe' /i 'C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\adv.msi' AI_SETUPEXEPATH=C:\Users\user\Desktop\o4c8AUtX1g.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE='/exenoupdates /forcecleanup /wintime 1635154532 ' AI_EUIMSI=''
Imagebase:	0x290000
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

Show Windows behavior

Analysis Process: msiexec.exe PID: 6328 Parent PID: 5776

General

Start time:	11:40:51
Start date:	25/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 97E0B76AE09D0E82CE071E7BABCE98E1
Imagebase:	0x290000
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

Show Windows behavior

File Read

Analysis Process: plcd-player.exe PID: 4744 Parent PID: 5776

General

Start time:	11:41:08
Start date:	25/10/2021
Path:	C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\plcd-player.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\plcd-player.exe
Imagebase:	0xa70000
File size:	3768184 bytes
MD5 hash:	25DDBD309BB8094229704383977C7268
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913796145.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913762032.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000009.00000002.937676135.0000000003949000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913941910.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000002.937726154.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913912827.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.914001553.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913978289.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913841738.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000009.00000003.913966024.0000000003E68000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis