

JoeSandbox Cloud BASIC



ID: 528552

Sample Name: jXzrIReInY

Cookbook: default.jbs

Time: 13:49:18

Date: 25/11/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report jXzrIReInY	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Ursnif	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
Jbx Signature Overview	5
AV Detection:	5
Compliance:	5
Key, Mouse, Clipboard, Microphone and Screen Capturing:	5
E-Banking Fraud:	5
System Summary:	5
Data Obfuscation:	6
Hooking and other Techniques for Hiding and Protection:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
Contacted IPs	10
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	33
General	33
File Icon	33
Static PE Info	33
General	33
Authenticode Signature	34
Entrypoint Preview	34
Data Directories	34
Sections	34
Resources	34
Imports	34
Version Infos	34
Possible Origin	34
Network Behavior	34
Network Port Distribution	34
UDP Packets	35
DNS Queries	35
DNS Answers	35
Code Manipulations	35
Statistics	35
Behavior	35
System Behavior	35
Analysis Process: jXzrIReInY.exe PID: 7000 Parent PID: 4732	35
General	35
File Activities	35
File Created	35

File Deleted	36
File Written	36
File Read	36
Analysis Process: msixec.exe PID: 4360 Parent PID: 560	36
General	36
File Activities	36
File Written	36
File Read	36
Registry Activities	36
Analysis Process: msixec.exe PID: 4344 Parent PID: 4360	36
General	36
Analysis Process: msixec.exe PID: 6512 Parent PID: 7000	36
General	36
File Activities	37
Analysis Process: msixec.exe PID: 4852 Parent PID: 4360	37
General	37
File Activities	37
Analysis Process: plcd-player.exe PID: 6620 Parent PID: 4360	37
General	37
File Activities	37
File Read	37
Disassembly	38
Code Analysis	38

Windows Analysis Report jXzrlReInY

Overview

General Information

Sample Name:

jXzrlReInY (renamed file extension from none to exe)

Analysis ID:

528552

MD5:

4ec77eb8280485..

SHA1:

85215638743eeb..

SHA256:

716ce7fe411f352..

Tags:

BABADEDA-Crypter

exe

Ursnif

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Ursnif

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Detected unpacking (overwrites its o...

Yara detected Ursnif

Antivirus / Scanner detection for sub...

Detected unpacking (changes PE se...

Antivirus detection for dropped file

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...

Classification

System is w10x64

jXzrlReInY.exe (PID: 7000 cmdline: "C:\Users\user\Desktop\jXzrlReInY.exe" MD5: 4EC77EB8280485764B6BC22F6CF7D57E)

- msiexec.exe (PID: 6512 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\jXzrlReInY.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE="/exenoupdates /f orcecleanup /wintime 1637876902 " AI_EUIMSI=" MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- msiexec.exe (PID: 4360 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 4344 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding C5EB72BDE2B80B60A07F51ECA26339C7 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- msiexec.exe (PID: 4852 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding 54779E8B78CD501470CD2E1995D98D79 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
- plcd-player.exe (PID: 6620 cmdline: C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\plcd-player.exe MD5: 25DDBD309BB8094229704383977C7268)

cleanup

Malware Configuration

Threatname: Ursnif

```
{
  "RSA Public Key":
    "GP2bItvzCMVimwFhSq2LMu3Hl69+F5VOC4HbUzLcgCFvHPQPwYycui0JiyqQuwt1jv1IDboN9TEBxLB8CQWBGqcjZkZnRvT4fL8wjQ8CCeHOLprVhSXFIXyR2QXzTHDcHr2ux9/r22BaIlqLqKQ1PI6I3WFn39M0K5k1WypMPthcp
    EVFS08sVBHvcqRSV",
  "c2_domain": [
    "get.updates.avast.cn",
    "huyasos.in",
    "curves.ws",
    "huyasos.in",
    "rorobrun.in",
    "huyasos.in",
    "tfsllld.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
00000011.00000002.530777240.00000000035F9000.00000004.00000040.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000011.00000002.530869037.0000000003BA8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: plcd-player.exe PID: 6620	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.plcd-player.exe.35f94a0.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
17.2.plcd-player.exe.35f94a0.2.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
17.2.plcd-player.exe.2ce0000.1.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

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Compliance:



Detected unpacking (overwrites its own PE header)

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 (overwrites its own PE header)

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:

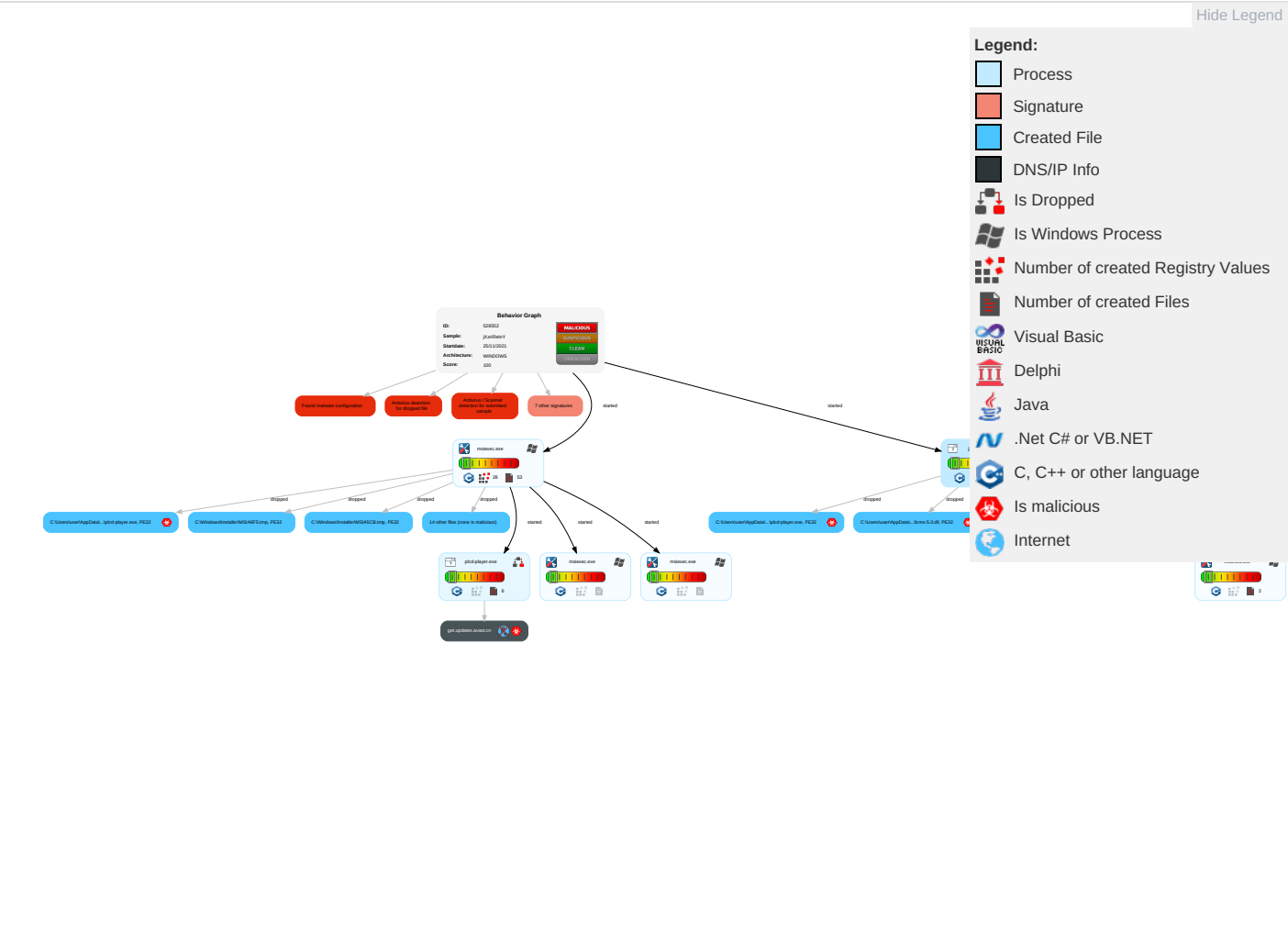


Yara detected Ursnif

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	Input Capture 1	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	Scheduled Task/Job 1	Process Injection 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	Account Discovery 1	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)	Logon Script (Mac)	Software Packing 2 3	NTDS	File and Directory Discovery 1	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	System Information Discovery 3 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicat
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Security Software Discovery 2 1	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	Masquerading 3 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)	Virtualization/Sandbox Evasion 2 1	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoco

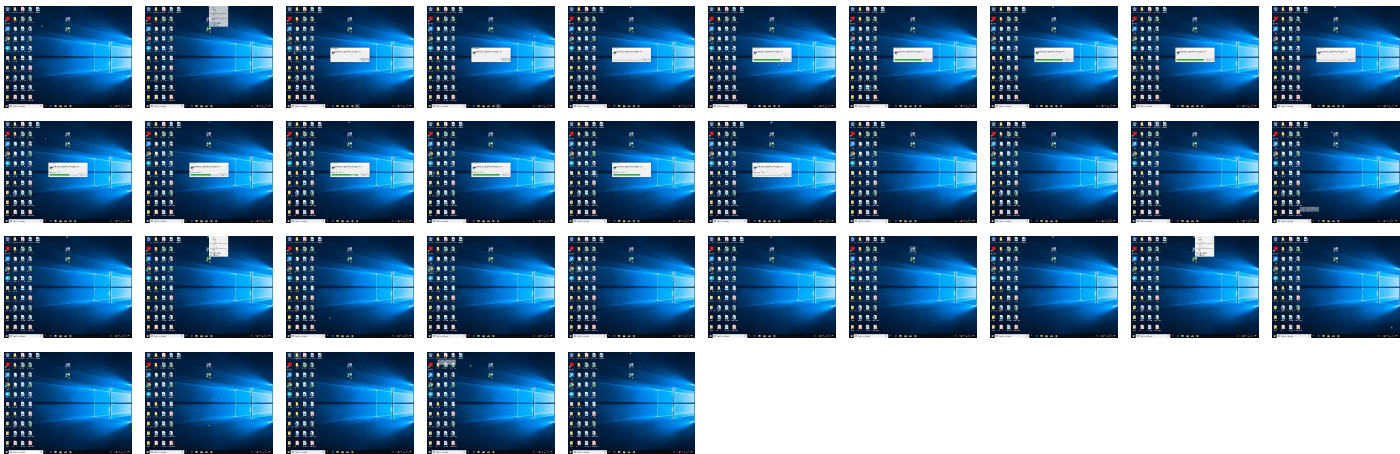
Behavior Graph



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
jXzrIReInY.exe	52%	Virustotal		Browse
jXzrIReInY.exe	23%	Metadefender		Browse
jXzrIReInY.exe	36%	ReversingLabs	Win32.Trojan.Chapak	
jXzrIReInY.exe	100%	Avira	TR/Agent.IIseq	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\lcm5-5.0.dll	100%	Avira	TR/Redcap.chbhs	
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\plcd-player.exe	100%	Avira	TR/Agent.kkknq	
C:\Users\user\AppData\Local\Temp\MSI1B4.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI1B4.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSI4D2.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSI4D2.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\shi1C.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\shi1C.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%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\AWSSDK.SimpleDB.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\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		
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%	Metadefender		Browse
C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\SslCertBinding.Net.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.plcd-player.exe.2ce0000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
17.2.plcd-player.exe.1a0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
windowsupdate.s.llnwi.net	0%	Virustotal		Browse
get.updates.avast.cn	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://get.updates.avast.cn/sreamble/g9_2FKpoNdUnXGannE6/i8VP6bKIh0KEVZxtH_2Fnm/ZbHMSZIAuG_2F/S_2FZ	0%	Avira URL Cloud	safe	
http://crl.startssl.com/sfsca.crl0C	0%	Virustotal		Browse
http://crl.startssl.com/sfsca.crl0C	0%	Avira URL Cloud	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://crt.sectigo.com/SectigoPublicCodeSigningCAEVR36.crt0#	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://www.ecb.int/vocabulary/2002-08-01/eurofxref	0%	Avira URL Cloud	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://mybusinesscatalog.com0	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://www.startssl.com/policy.pdf0	0%	Avira URL Cloud	safe	
http://https://currencysystem.com/gfx/pub/script-button-88x31.png	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAEVR36.crl0	0%	Avira URL Cloud	safe	
http://ocsp.startssl.com/sub/class2/code/ca0	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://get.updates.avast.cn/\$\$	0%	Avira URL Cloud	safe	
http://www.gesmes.org/xml/2002-08-01	0%	Avira URL Cloud	safe	
http://ocsp.startssl.com/ca00	0%	URL Reputation	safe	
http://crl.startssl.com/crtc2-crl.crl0	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	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-icon-16x16.png	0%	Avira URL Cloud	safe	
http://https://get.updates.avast.cn/SN	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://aia.startssl.com/certs/ca.crt02	0%	URL Reputation	safe	
http://www.startssl.com/0	0%	Avira URL Cloud	safe	
http://https://get.updates.avast.cn/	0%	Avira URL Cloud	safe	
http://https://get.updates.avast.cn/rentVersion	0%	Avira URL Cloud	safe	
http://https://currencysystem.com	0%	Avira URL Cloud	safe	
http://https://get.u	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.lnwi.net	178.79.225.128	true	false	• 0%, Virustotal, Browse	unknown
get.updates.avast.cn	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528552
Start date:	25.11.2021
Start time:	13:49:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	jXzrlReInY (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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/70@1/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.9% (good quality ratio 4.8%) • Quality average: 73.1% • Quality standard deviation: 26.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:50:26	API Interceptor	1x Sleep call for process: jXzrlReInY.exe modified
13:51:02	API Interceptor	2x Sleep call for process: plcd-player.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	m5AIAQ7Q8p.exe	Get hash	malicious	Browse	• 95.140.230.128
	0BPXSzHXZE.exe	Get hash	malicious	Browse	• 95.140.230.128
	hdgqcfpqji.exe	Get hash	malicious	Browse	• 178.79.225.0
	lhvzcskYLPyellowfacebrownietacohead.dll	Get hash	malicious	Browse	• 95.140.236.128
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 178.79.225.128
	nXOpgPAbKC.dll	Get hash	malicious	Browse	• 178.79.242.128
	yezVNLNobB.dll	Get hash	malicious	Browse	• 178.79.242.128
	d2EyAMvU47.dll	Get hash	malicious	Browse	• 95.140.236.128
	5Fp1yvQIGM.dll	Get hash	malicious	Browse	• 178.79.242.0
	IQKullAiRd.dll	Get hash	malicious	Browse	• 178.79.242.128
	BKHDGAM73508.vbs	Get hash	malicious	Browse	• 95.140.236.128
	DHL Shipping Document.exe	Get hash	malicious	Browse	• 178.79.242.128
	DHL Delivery Doc.exe	Get hash	malicious	Browse	• 178.79.242.0
	KgtyOfJo2W.dll	Get hash	malicious	Browse	• 95.140.236.128
	h5ZcTHDXbJ.dll	Get hash	malicious	Browse	• 95.140.236.128
	SCygJvetwW.dll	Get hash	malicious	Browse	• 178.79.242.0
	56ccc26e09e1216a0a310091d538c178ae68492ebc6bb.exe	Get hash	malicious	Browse	• 178.79.242.0
	DOC_1003394276473336675207.docm	Get hash	malicious	Browse	• 95.140.236.0
	details_2229.xlsb	Get hash	malicious	Browse	• 178.79.242.0
	items.doc	Get hash	malicious	Browse	• 178.79.242.128

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\MSI1B4.tmp	L5Q0nTmSYF.exe	Get hash	malicious	Browse	
	m5AIAQ7Q8p.exe	Get hash	malicious	Browse	
	KILljqCnUf.exe	Get hash	malicious	Browse	
	769sEMcQXR.exe	Get hash	malicious	Browse	
	3kRLUW6m5a.exe	Get hash	malicious	Browse	
	hdgqcfpqji.exe	Get hash	malicious	Browse	
	yRqHWQ91dT.exe	Get hash	malicious	Browse	
	o4c8AUtX1g.exe	Get hash	malicious	Browse	
	farcry6_repack.exe	Get hash	malicious	Browse	
	cX0XLcXbVY.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\MSI4D2.tmp	L5Q0nTmSYF.exe	Get hash	malicious	Browse	
	m5AIAQ7Q8p.exe	Get hash	malicious	Browse	
	KILljqCnUf.exe	Get hash	malicious	Browse	
	769sEMcQXR.exe	Get hash	malicious	Browse	
	3kRLUW6m5a.exe	Get hash	malicious	Browse	
	hdgqcfpqji.exe	Get hash	malicious	Browse	
	o4c8AUtX1g.exe	Get hash	malicious	Browse	
	farcry6_repack.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Config.Msi\3e96f5.rbs	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	modified
Size (bytes):	5179
Entropy (8bit):	5.646075332370666
Encrypted:	false
SSDEEP:	96:+UblaV4pDyJ0onGllKjeRhmgKpdGUO7PVRTlOAfk8Gy/W9DJzEgGMeOnTVw/r04U:+Uvp2j0on2jeRhmgSGUO7NRTSAs8Gy/c
MD5:	A44D4B86A5F1C60E3C03BD1622C56A04
SHA1:	3146AD6015538397C20ED912EFA484745DB1D756
SHA-256:	976E88DAC72E3E7AC6B2399066B7180E5F52400E5ED4CA380AD844D33B5978BD
SHA-512:	7FEB4D5AE07BF189C9B32804EAF0960DB70D466E6CDF1D1D38C67A6B22EFEDCE59B8FCBAC425FA648CEABF3F328B0429A460E74D0908815F9298CD9CEBD6A824
Malicious:	false
Reputation:	low
Preview:	...@IXOS.@.....@ZnyS.@.....@.....@.....@.....&{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\Local\Low\Microsoft\CryptnetUrlCache\Content\77EC63BDA748BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	Microsoft Cabinet archive data, 61414 bytes, 1 file
Category:	dropped
Size (bytes):	61414
Entropy (8bit):	7.995254868798237
Encrypted:	true
SSDEEP:	1536:EysgU6qmzixT64jYMZ8HbVPGfVDwm/xLZ9rP:wF6qmeo4eH1m9wmLvRP
MD5:	ACAEDA60C79C6BCAC925EEB3653F45E0
SHA1:	2AAAE490BCDACCC6172240FF1697753B37AC5578
SHA-256:	6B0CECCF0103AFD89844761417C1D23ACC41F8AEFB3B7230765209B61EEE5658
SHA-512:	FEAA6E7ED7DDA1583739B3E531AB5C562A222EE6ECD042690AE7DCFF966717C6E968469A7797265A11F6E899479AE0F3031E8CF5BEBE1492D5205E9C5969090
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....l.....;w.....RSNj.authroot.stl.>.(5.CK.8T...c_d...AK...+d.H..*i.RJJ.IQIR.\$t)Kd.-[.TV{.ne.....<w.....A.B.....c_wi.....D.....cOD.L.....f y...Rg...=.....i,3.3..Z.....~^ve<...TF.*...f.zy....m.@.0.0...m.3..l((...+v#...(2....e...L...*y.V.....~U.....<ke.....l.X:Dt..R<7.5vA7L0=.T.V...lDr..8<....r&...l-^..b.b."Af....E..._ r>`,`Hob..S.....7`..l.RS."g..+..64..@nP.....k3...B`.G..@D....L.....`^#OpW.....l.....rf:}.R.@....gR.#7....l..H.#...d.Qh..3.fCX....==#.M.l..~&...[J9\..Ww.....Tx.%....].a4E ...q+.#`a..x..O.V.t.Y1!T..U...-...<_@...[(....0.3`.LU...E0.Gu.4KN....5.?....l.p.....N<d.O.dH@c1t..[w/..T....cYK.X>0..Z....O>..9.3.#9X.%b...5.YK.E.V.....`/3._ ..nN]...=.M.o.F...z.....g.Y..lZ..?l.....vp.l:d.Z.W.....~..N...k...&.....\$.....i.F.d....Dle...Y...E..m.;1H..\$.F.O.F.o_}uG.....%>..Zx.....o....c./;....g&.....

C:\Users\user\AppData\Local\Low\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0944535883568105
Encrypted:	false
SSDEEP:	6:kKgl7k8SN+SkQlPIEGYRM9z+4KIDA3RUeYlUmlUR/t:079kPIE99SNxAhUeYlUSA/t
MD5:	B39D2A576D114D01CC782C8A3C9A4EBF
SHA1:	3A6748FCED922413C2310733C19505213B3E68F8
SHA-256:	0A38BF1EFDBE38B3ED2C5632C5B55C6237171A019D35A6E92CFC6EF19894807E
SHA-512:	B41F25324078467D81FC645716D35EFFF283C2EE5D00C0512167CB3B70D99E4EDF663CDD766E52BF44552EC3D6727FADF4ACA7A167D9303005F39070752018F
Malicious:	false
Reputation:	low
Preview:	p.....,itF..{.....q.}\.....&.....h.t.t.p://.c.t.i.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..."0.7.1.e.1.5.c.5.d.c.4.d.7.1.:0"...

C:\Users\user\AppData\Local\Temp\MSI1B4.tmp		
Process:	C:\Users\user\Desktop\ijXzrReInY.exe	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	

C:\Users\user\AppData\Local\Temp\MSI1B4.tmp	
Category:	dropped
Size (bytes):	402912
Entropy (8bit):	6.383799484265228
Encrypted:	false
SSDEEP:	6144:hsEQsy5dfBkvAUnBU76LNaiDWbw0EAOqcmCIVKVPgvf:4sw6vAUUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	- Filename: L5Q0nTmSYF.exe, Detection: malicious, Browse - Filename: m5AIAQ7Q8p.exe, Detection: malicious, Browse - Filename: KILJqCnUf.exe, Detection: malicious, Browse - Filename: 769sEMcQXR.exe, Detection: malicious, Browse - Filename: 3kRLUW6m5a.exe, Detection: malicious, Browse - Filename: hdgqcfpqji.exe, Detection: malicious, Browse - Filename: yRqHWQ91dT.exe, Detection: malicious, Browse - Filename: o4c8AUtX1g.exe, Detection: malicious, Browse - Filename: farcry6_repack.exe, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....@p.....l.....j.....j.....t.....t.....t.....j.....j.....j.....t.....t.....t..... !.....T....Rich!.....PE..L..."la....."!.....*.....6P.....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\MSI4D2.tmp	
Process:	C:\Users\user\Desktop\jXzrlReInY.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:gJgZXIAIlfQhETbF+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: cX0XLcXbVY.exe, Detection: malicious, Browse - Filename: L5Q0nTmSYF.exe, Detection: malicious, Browse - Filename: m5AIAQ7Q8p.exe, Detection: malicious, Browse - Filename: KILJqCnUf.exe, Detection: malicious, Browse - Filename: 769sEMcQXR.exe, Detection: malicious, Browse - Filename: 3kRLUW6m5a.exe, Detection: malicious, Browse - Filename: hdgqcfpqji.exe, Detection: malicious, Browse - Filename: o4c8AUtX1g.exe, Detection: malicious, Browse - Filename: farcry6_repack.exe, Detection: malicious, Browse
Preview:	<pre> MZ.....@.....!..!This program cannot be run in DOS mode...\$.4.....3....3....3.?.... W...3...Rich.....PE..L...la....."!.....KC...@.....t...d.....p.....T.....p.....@... ...h...@.....text.....`..rdata.....@...@.data...4.....@...@.rsrc.....@...@.reloc..T.....@...B..... </pre>

C:\Users\user\AppData\Local\Temp\shi1C.tmp		
Process:	C:\Users\user\Desktop\jXzrlReInY.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	

C:\Users\user\AppData\Local\Temp\shi1C.tmp		
SHA-512:	E69A82ADC2D13B413C0689E9BF281704A5EF3350694690BA6F3FE20DA0F66396245B9756D52C37166013F971C79C124436600C373544321A44D71F75A16A2B6A	
Malicious:	false	
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....E..2..a..a..=aa.an..`..an..`..a..a..an..`..an..`..an..`..l.an.Qa ..an..`..aRich.a.....PE..d...5..f....."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\jXzrlReInY.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/8YVvKEyDrKe2xDBoPnp:dFpEBNMGwcsa8f/8a6Pp	
MD5:	5AEB79663EA837F8A7A98DC04674B37A	
SHA1:	536C24EF0572354E922A8C4A09CF5350D8A6164D	
SHA-256:	E13D9F958783595ACD8ACDBFF4D587BCA7E7B6A3AAB796E2EFBD65BD37431536	
SHA-512:	25E4E48EC2162EA6342CFD823E789ED0B5A995BB61FA3FA68364D1EE2468974FA4E75C17EB2CB3DDB213E633136C9AAB139BBF32FB8688FF5B1ABF444E8BB652	
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...tx....." ..0.....@.....X.. ..@.....H...O.....X..8.....H.....text.....`..rsrc.....@..@.reloc.....@..B.....H.....\$b.....V...}.....(.....f...p(...*f...p*f..{...*Br...p(...**"..(....*&...(....*...0....(....*:.....(....*B(....*&...(....*F.(....S....(...*b.(....S....%0!...(...*6.(.....(...*6.S....(....*R.S....%0!...(....*&...(...*S....(....*V...S....%0!...(....**....(" ...*>....S....(....*^....S....%0!...(....*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\jXzrlReInY.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1569	
Entropy (8bit):	5.078244393355221	
Encrypted:	false	
SSDEEP:	48:rIXOOrpJAzJzGI0PE9432sEs32s3IEtd132RTHy:peOrpJAzJzGIBq3b38OSTS	
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\jXzrlReInY.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	


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

Preview:
MZ.....@.....!..L!This program cannot be run in DOS mode...$.PE.L...(. ...." ..0.....>.....@.....+...
..\.....-O...@.....HS.....T.....H.....text...D.....\..rsrc.....@.....@...@.rel
oc.....\.....@...B.....H...P .. .....p.....BSJB.....v4.0.30319...I...(#~.....#Strings.....#US.....#GUID.....
#Blob.....G.....3.....b...+b...O.....&I...*...*...*...?*\*...*...*...[.....<.....<.....
```

[illegible]

C:\Users\user\AppData\Roaming\JDDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\OCE0CF4\System.Threading.Tasks.dll	
Process:	C:\Users\user\Desktop\jXzrlReINy.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:WL0xHprBefGMORQY+hoZhOZkcvr3EqI38WqATrOhEZOGftpbj1x+ILKHNRNc6IE:NRBefGBkoWjvrOVabKirxmcm+
MD5:	85F6F590B5C4B8C7253E9C403C9BE607
SHA1:	D5A9DB942A50C8821BACD7F6030202C57EC4708B
SHA-256:	D20552FD5C8C8C9759608A84DB1E216DA738F5E9F46DE9E8A3F39A0D6265CB8B
SHA-512:	9C78CB444E28618D44E9DEB23571FC7BBCE268882C2803E0CCC0E84B3E6EAB89C6AF2AAC0BD1EF0D2C9FD1E9611CB35334EF3304FB16C5BA0481F6A7273C360
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.....T.....@..B....._.....H.....h../.....P#..ON... "J.O.f...6RbR[.44...F....E.X...1.XIE.....5.M...Txn.lycn....o].V).. .l}.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...*(.....(.....(+.+-.*

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\jXzrlReInY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18727
Entropy (8bit):	5.228912164616093
Encrypted:	false
SSDEEP:	384:vADBz8NWcg8Yt0Mp9sXYGb0JPMfBH1FB1pz4vl:vADBz8NWcg8Y2Mp9sXlb0OfBH1F+pz4t
MD5:	E001FBA3F73ADB83B5B9DCD2A32F1C7B
SHA1:	D0B3A5615F30226072BA90A961DBAD1CE0ED23E2
SHA-256:	60A987CFE5AE817D5D5ED82E1F39C3C537321EE9AB9A0B902DB2990F66B99887
SHA-512:	6DF77E4AC29B0AF120C2EE9380BACD4D1E02C08E9F6E7CD293959F7438294182B773B3C75E0DED11C3EEFD511B09FDF2F43927D68884572F745464705EE81A
Malicious:	false

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencyssystem4.js

Preview:	<pre>/*...Copyright (C) 1998-2009 Currency System, Inc. All rights reserved....\$VER: Currency System Script Library 4.6..*/....// Currency object constructor...//..function Cur rncy(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</pre>
----------	---

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencyssystem5.js

Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18850
Entropy (8bit):	5.252718939622608
Encrypted:	false
SSDEEP:	192:LVMJqzg8F9zp/OQMhEF7IXs1NmrgfTPzD5bL29h1FDiTyyf1CQx/TuTmkk6aez4U:LV2lg8FanXcmrgfTlwOH1ltsz4v8
MD5:	866B6E8A186BE6005A140CFE9F578CD8
SHA1:	E0B2E5344097EF4C1C0A8BE851C5DE27C7F490DB
SHA-256:	0A5731729919FEDC1A3B81C651087AB200C9470FA75A89BEBEA73AE0478F30E5
SHA-512:	BE84B6A9B893DC0D66113287942A388BAFB0629AE67E6C02A8E09E98A028D50CCFA082A2C1B5BFafa273ACF9E6338E961FA208B62EF6BEE43D8BFD5E6D4619A9
Malicious:	false
Preview:	<pre>/*...Copyright (C) 1998-2012 Currency System, Inc. All rights reserved....\$VER: Currency System Script Library 5.2..*/....// Currency object constructor...//..function Cur rncy(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 = "5.1";...this.i nitialized = 0;...//...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.widgetCurrencyIsListed = curr encySystem_widgetCurrencyIsListed;...this.widgetCurrencyIsUsed = currencySystem_widgetCurrencyIsUsed;...this.widgetSuggestUnusedCu</pre>

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\currencyssystem5.json

Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	635
Entropy (8bit):	4.968896753287593
Encrypted:	false
SSDEEP:	12:G3in27KkdcynYKFfaYKQlIl7eTaYKRHTaYKQlI9txrZOaYKB3i8T:G3i27KkdvYKtaYK3qteTaYKRHTaYK3qz
MD5:	D5BE63A1E66E4D6597F49BFD15EB3D83
SHA1:	6B0D0E3101EDB0C92C14691745765DE49CDB7C01
SHA-256:	A1CF701C876F916AACB12A3B952D1D2A38889C2AC118AF9D89493F0A86A45C5D
SHA-512:	6F8CD8F4D18D978F9B30E00322E3CC020B1C3ADD6B6307ED96EBB47B422DD15DDE4BB82698AE755CEF57F8BA3B1BDBD6F47D83CF08471E7B131B8CF8B20ACAA55
Malicious:	false
Preview:	<pre>{...<currencyssystem-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 infor mation at currencyssystem.com.",... "embedSmallBannerGfx": "https://currencyssystem.com/gfx/pub/script-button-88x31.png",... "embedSmallBannerText": "Powered by Cur rrency System",... "embedSmallBannerLink": "https://currencyssystem.com",..... "embedSmallHomeGfx": "https://currencyssystem.com/gfx/pub/script-icon-16x16.png",... " embedSmallHomeText": "Currrency System Homepage",... "embedSmallHomeLink": "https://currencyssystem.com",.....<currencyssystem-insert-currencies>..}</pre>

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\Templates\lecb-eurofxref-daily.xml

Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	403
Entropy (8bit):	5.022779704233175
Encrypted:	false
SSDEEP:	6:TMVBd/5Q3JLHAc4Mj/9mc4C7drcDqhsDgHLHlvssw92PXCEZqilvs/BRI8LqfaR/:TMHduFHjFbdrCWpU2XCMei8Lqai8L/
MD5:	376F44C2269588374F0F7E876BB3CFFA
SHA1:	1241AC750F7CA447D7A74EB516838C39516AA841
SHA-256:	3B96E197B1A47E7A391385638E13A0CF42E04E1665470A89EABECC67D1B91323
SHA-512:	744C8944294538B5E40241FEA6A2EBD354BF2B06C5AD9B4439BE1CCACD15B89C487A1FE100851F23E7A2212CCAC600FC8519224855D7AC72F09E6AABD1E8AC6C9
Malicious:	false
Preview:	<pre><?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>... currencyssystem-insert->... /currencyssystem-insert->..</Cube>.</gesmes:Envelope>.</pre>

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\jXzrlReInY.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/YrEUI8VlvfqAE/fQhksQQNgXAo1sVzhly+PkfsJJ10FRzVT8ajBK+ByqV4Tq:GYrEkXAEfs01sVNrajM+
MD5:	9AFC8137B547561655D454AFF862E567
SHA1:	2DAB8B1B9F1AE612E9CD359207751B452C76CB0D
SHA-256:	86747F0567ADBDD895E23E25760AF726A87000BD01EBEF994352EFAD7EB3987C
SHA-512:	91B99B561FBD3C6F3C2583CBF13D9FAF31AAFE6EFDB82667F646AD9F245904D3EF8F37B4CD11E141ECBEBDB7724414E21C4A8F7886CE68FFAC7B0BB8B1B5303B
Malicious:	false
Preview:	>.....#.....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\jXzrlReInY.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:	B3DDFCCEFFDE24791DFB9587D5AEB406B9EC3408B38D50C70AC324931C37FD7F55099C7F84B8359A76ACA1BB0E350977451639CC0E61241EBE16D6F4DB9056
Malicious:	false
Preview:	ITSF....g..... {....."..... {.....".....`.....x.....T.....ITSP...T.....PMGL...../.../#IDXHDR.. ..5.../#ITBITS.../#IVB...Rd./#STRINGS...U.i./#SYSTEM.....;/#TOPICS...5.p./#URLSTR...Y. /#URLTBL...%4./#WINDOWS.....L./\$FItMain...}.8./\$OBJINST...>?./\$WWAs sociativeLinks/.../\$WWAssociativeLinks/Property...../\$WWWKeywordLinks/.../\$WWWKeywordLinks/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\icuiu58.dll	
Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	54224
Entropy (8bit):	6.686697566242328
Encrypted:	false
SSDEEP:	1536:8n6iCEsBHqIXN0IIUofqcOZkE5z7L/cLlvBQ+8iAYS:GuEsdXL/cLIGD1
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_v^..s_s^..s_s...s...s...s...q^..s_Rich..s.....PE..L.....Z.....!....f...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\jXzrlReInY.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4993536
Entropy (8bit):	6.871255823719978

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\lcms-5.0.dll		 
Encrypted:	false	
SSDEEP:	98304:vdG+iN2k+e/VO+0X30DQHDbOXh9A0DESaHafv4UZDCr:A+Hk+eX0BHDboXh9A0DeHfUZDS	
MD5:	B6723B31F67956E747493BC64F2C7A59	
SHA1:	72389ECF849BFDA364E84258E5857A3DF07E5BFC	
SHA-256:	3361AC8727ABA86AC7F3AAC3A214C3CB76F1AF9FF7EE5E94C52C30FDCB7D5064	
SHA-512:	E17FEA164BB00E65BE0E58771A728FC9CED5BD65AE2FEC9E55C5697E69A498404B6D52B529DF774012C9F1268D29D97AD3CAFD404BAD58B3C36535A52AB6E09B	
Malicious:	true	
Antivirus:	Antivirus: Avira, Detection: 100%	
Preview:	MZ.....@.....(.....!..L!This program cannot be run in DOS mode...\$.....A...A...A...9N...A...*...A...*...A...A...A...A...A...A...h(..A...A...A...C...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.....l...xl.....@..B.....	

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\libey32.dll	
Process:	C:\Users\user\Desktop\jXzrlReInY.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:Rpi3r3WH9IYf+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...f...l...x.....0.....pb.....0...@.....`..(.....text...J.....L.....`..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\lml		
Process:	C:\Users\user\Desktop\jXzrlReInY.exe	
File Type:	PDF document, version 1.5	
Category:	dropped	
Size (bytes):	418532	
Entropy (8bit):	7.992704655006582	
Encrypted:	true	
SSDEEP:	12288:gC3QjgVE/DGk/1gsQR4jflsCEqmnUT9ca7cgTe9b:F3m7zqieCU4NITO	
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.Vjo.8.h..H.E...m.P!q.....d.r..fe.n....%.....*..y....KB..A...d....\$.\$.i....P...I9.Z.R...l..%..c.#.eZ..).%g...0i.Q.....E...&^c..8..g.N.Y!..W.r...A...!..`.....0.....O`B.\$t8X"x=.)..BHi...<\$.x.Lb..2....L.`.)r..M....^R.k...%..n....^..`.....3.@...P...5.Z.&....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....2trQ7..L.q.l.2{...z....=...}9...p.0....n.vU?n..P...n"<...9).cu>}_l.be>4j7.....\$i*N_t..1.....t..2...nG..o)..E..6.....r...se.=...j.vz...4....y...S...E=. aH..zp.IP.*..Hu;u.f.?...)L.....U.P.y..1].LMH..=.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\jXzrlReInY.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/OWFGZ7pqfwbAFj1IKdn9kvOIBzuJTHPfw8xZcca9KJi4EIdG:sBaNsKkDn9AzBqw8xZcca9KJi4s	
MD5:	25DDBD309BB8094229704383977C7268	
SHA1:	1574D860469EE784034093199DC9533543E5C096	
SHA-256:	8C7E6A620F4BBC343C2695C2E034CC628062B5C2A6B05461FC41B05436F45147	

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0.2\install\0CE0CF4\plcd-player.exe	
SHA-512:	16CF4205B16F83A3EFEC96660190EFE254919EA18FBC6EB23F45D5C77B0A4A7EFD5DFA36EC1FC43BD79D1D4959A2FA9E172AB842CE7DE754CDC62912752892BA
Malicious:	true
Antivirus:	Antivirus: Avira, Detection: 100%
Preview:	<pre> MZ.....@.....8.....!..L!This program cannot be run in DOS mode...\$.....N.....O...X..~..X..~..X..~..X..~..e...\.~..\. ~..\.#.....K.....\..~..Rich...`SH.R.`[RK..RJ3RK..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...j4.....@...@.reloc.....7.....@..B..... </pre>

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\jXzr\ReInY.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
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$......r...r...r...r...r...r...r...s.4.r...\.r.....r.....r.Rich...PE...<K.V.....I.....I.....).p.....p..9).....<.....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\jXzrlReInY.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....la....."l"....X.....p.....@.....p.....<...p.....p.....@.....@.....p..t.....text...lV....X.....`..rdata..l..p.....l.....@..@..data..dV.....@...rsrc...p.....@..@..reloc.....@..B.....

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools 3.4.0\install\holder0.aiph	
Process:	C:\Users\user\Desktop\jXzrlReInY.exe
File Type:	data
Category:	dropped
Size (bytes):	12613117
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	5EB8E16CA980C4FD12FB68F5BDEA2453
SHA1:	A28C1272997B3EE0AFE2C4FB9FBA8153BAE0D6B2
SHA-256:	6FAE30A56DA63F2DDB1E8BA7B636EA0167B8DDEA08F4F600E81DC6393CB624A4
SHA-512:	91245C324225023A98B3A5CCA52F07660D2AB740884BF84083E65347DC8FF9F12322A908D52D6D91D2933834A01AB851816EDDA01229710C3D0FB675F563065F
Malicious:	false
Preview:	

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\ICSharpCode.SharpZipLib.dll	
SSDEEP:	3072:hjMibqfQqFyGCDXiW9Pp/+Tl4abpuu201PB1BBXIDwtqSPVINrAfvp1:Gibqf59PpOPf201/z7p
MD5:	C8164876B6F66616D68387443621510C
SHA1:	7A9DF9C25D49690B6A3C451607D311A866B131F4
SHA-256:	40B3D590F95191F3E33E5D00E534FA40F823D9B1BB2A9AFE05F139C4E0A3AF8D
SHA-512:	44A6ACCC70C312A16D0E533D3287E380997C5E5D610DBEAA14B2DBB5567F2C41253B895C9817ECD96C85D286795BBE6AB35FD2352FDD9D191669A2FB0774E4
Malicious:	false
Preview:	<pre> MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L...<K.....!.....^.....@..@..... ..@.....K.....H.....text...d......src.....@..@.reloc.....@..B..... </pre>

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\License.txt	
Process:	C:\Windows\System32\lsimsexec.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+iQJ54d7JdEgUVVN7XzUKyeraku:knhlhlmz8pJdLk/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 period - 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\lsimsexec.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+DeljFWt6O9QHRN7fhKtkxHQJ:YdXuhvU8ZOJ
MD5:	FEC0A2AB4AB150DAD477E0D4885637CE
SHA1:	5A3C8920DE1B3F2F7867A20D05C94DE5B2779B81
SHA-256:	746760FE317B9721FB761209F0F9F7E1A5126390970AAC5FD93F11504FFE3D30
SHA-512:	11C7C941D31902CCC9F9E07166CF6E181E0ADF7BAEA0986B863CEDF71591431C0D630018B5514C66D6670BFAD1F8ACD363AC19BED486FB92B06DE83A4669C70
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.....Pp.....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\lsimsexec.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:PecpB4zReJOVom9FziUm0exVSilgm19J8AG4oHHith5kCCeYghu+:3DgeO97m0exVfKwxniQghu+
MD5:	EDCEB39D12707299F6501AE9472A2FD1
SHA1:	F4BE70378AF9FEA7355307CF66E0F5A50590E974
SHA-256:	FA2C262A94F90DAD052A6A5D190F347CD1B8D8BACD7417B8B3FFF56F7D42ECB4
SHA-512:	08406BEDE6C980A1C36EC427C1D86F05F11A41EC366F3821D7B229649B10F3AF9D37AFE7A5A55C7D32D90F0B7D0A43848AF3B20DEA2D2D3669130AAA08729B02
Malicious:	false

[illegible]

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:WL0xHprBefGMO rQY+hoZhOZkcvr3EqI38WqATrOhEZ0GftpBj1x+ILKHRN7c6IE:NRBefGBkoWjvr0VabKirxmcM+
MD5:	85F6F590B5C4B8C7253E9C403C9BE607
SHA1:	D5A9DB942A50C8821BACD7F6030202C57EC4708B
SHA-256:	D20552FD5C8C8C9759608A84DB1E216DA738F5E9F46DE9E8A3F39A0D6265CB8B
SHA-512:	9C78CB444E28618D44E9DEB23571FC7BBCE268882C2803E0CCC0E84B3E6EAB89C6AF2AAC0D81EF0D2C9FD1E9611CB35334EF3304FB16C5BA0481F6A7273C360
Malicious:	false
Preview:	<pre> 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).. .J].1En...`T. \e .u..=nA...@p:.(.....)*R..r...p.(.....(+*N..r...p.(.....(+*Z..r...p.(.....(+*Z..r...p.(.....(+*..0.\$.....(+..-.....*..o.....*0..... (+..-..S...Z.0.....*..0.....(+..-..S...Z.0.....*..0.....(+..-..S...Z.0.....*..0.....(+..-..S...Z.0.....*..0.....(+..-..S...Z.0.....*..0..... </pre>

C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\currencysystem4.js

Process:	C:\Windows\System32\lsass.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	18727
Entropy (8bit):	5.228912164616093
Encrypted:	false
SSDEEP:	384:vADBz8NWcg8Yt0Mp9sXYGb0JPMfBH1FBlpz4vl:vADBz8NWcg8Y2Mp9sXlb0OfBH1F+pz4t
MD5:	E001FBA3F73ADB83B5B9DCD2A32F1C7B
SHA1:	D0B3A5615F30226072BA90A961DBAD1CE0ED23E2
SHA-256:	60A987CFE5AE817D5D5ED82E1F39C3C537321EE9AB9A0B902DB2990F66B99887
SHA-512:	6DF77E4AC29B0AF120C2EE9380BACD4D1E02C08E9F6E7CD293959F7438294182B773B3C75E0DED111C3EEFD511B09FDF2F43927D68884572F745464705EE81A
Malicious:	false
Preview:	<pre> /*...Copyright (C) 1998-2009 Currency System, Inc. All rights reserved....\$VER: Currency System Script Library 4.6..*/...// Currency object constructor..//.function Cur rncy(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 </pre>

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:LJVmqzg8F9zp/OQMhEF7IXs1NmrgfTPzD5bL29h1FDiTYyf1CQx/TuTmkk6aez4U:LV2lg8FanXcmrgfTlwOH1Itsz4v8
MD5:	866B6E8A186BE6005A140CFE9F578CD8
SHA1:	E0B2E5344097EF4C1C0A8BE851C5DE27C7F490DB
SHA-256:	0A5731729919FEDC1A3B81C651087AB200C9470FA75A89BEBEA73AE0478F30E5
SHA-512:	BE84B6A9B893DC0D66113287942A388BAFB0629AE67E6C02A8E09E98A028D50CCFA082A2C1B5BFAFA273ACF9E6338E961FA208B62EF6BEE43D8BFD5E6D4619A9
Malicious:	false
Preview:	<pre> /*...Copyright (C) 1998-2012 Currency System, Inc. All rights reserved....\$VER: Currency System Script Library 5.2..*/...// 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.physi cal;...this.legalTender = legalTender;...this.popularity = popularity;...}...// CurrencySystem object constructor...//.function CurrencySystem(){...this.version = "5.1";...this.i nitialized = 0;...//...this.initialize = currencySystem_initialize; // object.method=function(){} syntax not supported in Netscape Navigator 3...this.widgetCurrencyIsListed = curr encySystem_widgetCurrencyIsListed;...this.widgetCurrencyIsUsed = currencySystem_widgetCurrencyIsUsed;...this.widgetSuggestUnusedCu </pre>

C:\Users\user1\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:G3in27KkdcynYKFfAYKQItll7eTaYKRHTaYKQItl9txrZOaYKB3i8T: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 infor mation at currencysystem.com." ,,..."embedSmallBannerGfx": "https://currencysystem.com/gfx/pub/script-button-88x31.png" ,,..."embedSmallBannerText": "Powered by Cur rency 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\user1\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\Templates\lecb-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/:TMHduFHjFbdrDWPu2XCMei8Lqai8L/
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\user1\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\help.chm	
Process:	C:\Windows\System32\msiexec.exe
File Type:	MS Windows HtmlHelp Data
Category:	dropped
Size (bytes):	325845
Entropy (8bit):	7.966997729785747
Encrypted:	false
SSDEEP:	6144:upVysoxdLmULS5Nv5czGT6ozCF6DWc4kYBDrHDDoicYs0meNdt:iAsWJmUSjBczf3c4dHDDoicYs0re
MD5:	DF113262CBB4AD90D0D889620BDEFB06
SHA1:	D94D2111F9FD566941FF96DBA6237D126591E512
SHA-256:	195BAFB549728E15B392B5A2FCBD41003D2472B1AD82AED449175C37E5834657
SHA-512:	B3DDFCCEFFDE24791DFB9587D5AEB406B9EC3408B38D50C70AC324931C37FD7F55099C7F84B8359A76ACA1BB0E350977451639CC0E61241EBE16D6F4DB90 6
Malicious:	false
Preview:	ITSF....`.....g..... . {....."..... . {.....".....x.....T.....ITSP....T.....j..}!.....".T.....PMGL...../.../##IDXHDR.. .5.../##TBITS..../##IVB...Rd./##STRINGS...U.i./##SYSTEM.....;./##TOPICS...5.p./##URLSTR...Y. ./##URLTBL...%.4./##WINDOWS.....L./\$FiftiMain...}.8./\$OBJINST...>?./\$WWAs sociativeLinks/.../\$WWAssociativeLinks/Property..../\$WWWKeywordLinks/.../\$WWWKeywordLinks/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\user1\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\licuio58.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:	1536:8n6iCEsBHqIXN0lIUofqcOZkE5z7L/cLlvBQ+8iAYS:GuEsdXL/cLIGD1
MD5:	249D164D4361F1BBF827331A2C5B8E64

C:\Users\user1\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\licuio58.dll	
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_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\user1\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+OX30DQHDbOXh9A0DESaHafv4UZDCr:A+Hk+eX0BHDboXh9A0DeHfUZDS
MD5:	B6723B31F67956E747493BC64F2C7A59
SHA1:	72389ECF849BFD4364E84258E5857A3DF07E5BFC
SHA-256:	3361AC8727ABA86AC7F3AAC3A214C3CB76F1AF9FF7EE5E94C52C30FDCB7D5064
SHA-512:	E17FEA164BB00E65BE0E58771A728FC9CED5BD65AE2FEC9E55C5697E69A498404B6D52B529DF774012C9F1268D29D97AD3CAFD404BAD58B3C36535A52AB6EC9B
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...h(..A...4...A...A...C...4...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.....xl.....@..B.....

C:\Users\user1\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
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\user1\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\lml	
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:F3m7zqieCU4NITO
MD5:	EF946663D3A336BDACB512BF32C8F8F2
SHA1:	1A02B2DEE5CD8815BA977A09505F0B38FEA27665
SHA-256:	0B77203265ADCB18A878383978BCE5C8D6A1D253FE1EFC16B8B161B42F03B79F
SHA-512:	B5E45C3F22F31FD1538C982C83F75DA1015FF56235B26EA1707DCA6B1BC1E41FB11557593CED91D5BF927B985511DBA4047C898A1FE9EB7903932FDBF6C8582
Malicious:	false

Preview:

```
%PDF-1.5.5.2 0 obj.<<./Type /ObjStm/N 100./First 806./Length 1140          ./Filter /FlateDecode>>.stream.x.Vj0.8.]....h..H.E.m.Plq.....d.r.f.e.n....%.....*.y.....KB..
.4...d...$. $i...P...19.Z.R...1.%c.#eZ.].%g...0i.Q.....E...&^c.8.g.N.Y!..W.r...A...l.....0.....O^B.$t8X"x=).BHi...<$.x.L.b.2...L...l...r).M...^R.k...%n...^'
`...3.@e.P...5.Z.8&...9.j.g...].H.X....."Y.D.z1)...$.c.2.&...B.du...&...T.7]%.P...#P.9(^&5g.W...f.x.fc...l("8..w)...0..(.%1.&^'v...g...r.K...;y...n...S...+z>
...+...r.f...#x.8...X.....1^...u.X.....H...7.9.1.c.Kz...2tr.Q7.L.q.l.2{...z...=...j9...p.0.n.vU?P...n...P...c...u).>_l.be>4]7}$*N_t..1...2...nG..o)...
E...6...f..se...;].vz..4...y...S...E..aH.zp.tP.*...u(u.f.?...)L...U.P.y...z...l...].MH...=...C...j[s?>...g.B9./...k...1..wE.S.v..
```


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/7pqfwbAFj1IKdn9kvOIBzuJTHPfw8xZcca9KJi4EldG:sBaNsKKdn9AzBqw8xZcca9KJi4s
MD5:	25DDBD309BB8094229704383977C7268
SHA1:	1574D860469EE784034093199DC9533543E5C096
SHA-256:	8C7E6A620F4BBC343C2695C2E034CC628062B5C2A6B05461FC41B05436F45147
SHA-512:	16CF4205B16F83A3EFEC96660190EFE254919EA18FBC6EB23F45D5C77B0A4A7EFD5DFA36EC1FC43BD79D1D4959A2FA9E172AB842CE7DE754CDC62912752892BA
Malicious:	true
Preview:	<pre> 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.....I9.x...7.....@.....H...@.....x.....text.....rdata.B.....@..@.data...p1..(.. T1.....@....fsrc....S...4.6... 4.....@..@.reloc.....7.....@..B..... </pre>

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/ySTJ7a7hNI/K5bv3jgNZuDwsLB+:N4Nuw10tGJjPZTbkyMzU/RsZBnHHrf+0
MD5:	F0AED1A32121A577594ECD66980C3ED3
SHA1:	288954A8D6F48639B7605488D2796B14291507E5
SHA-256:	D02CC01A7D9ADC1E6F980D1A56D6A641DF9E2A63FDC5F007264D1BF59ECC1446
SHA-512:	056670F3074AF5A03326C2BE5FFA0FEC23010DDC25BBED07B295EA3F6C7F8DFBC73E40E11E20103EFEB3B230096F630FB0A3CFA61C4E0A74C15A1CB6319D85D9
Malicious:	false
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......r...r.....r.....r.....r.....r.....s.4.r...\r.....r.....r.Rich..r.....PE.L...<K.V.....I.....I.....)......p.....p..9).....<....0.....:0...0.....X{..@.....text.....`rdata.....@..@.data...[.....@.....@.....@.rsrc.0.....@..@.reloc..b3..0..4.....@..B.....

C:\Windows\Installer\3e96f3.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/YrEUI8VlfqAE/fQhksQQNgXAo1sVzhly+PkfsJJ10FRzVT8ajBK+ByqV4Tq:GYrEkXAEfs01sVNrajM+
MD5:	9AFC8137B547561655D454AFF862E567
SHA1:	2DAB8B1B9F1AE612E9CD359207751B452C76CB0D
SHA-256:	86747F0567ADBDD895E23E25760AF726A87000BD01EBEF994352EFAD7EB3987C
SHA-512:	91B99B561FBD3C6F3C2583CBF13D9FAF31AAFE6EFD82667F646AD9F245904D3EF8F37B4CD11E141ECBEBDB7724414E21C4A8F7886CE68FFAC7B0BB8B1B533B
Malicious:	false
Preview:	>.....#.....l.....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\MSI9CCF.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:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
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.....J.....T.....Rich!.....PE..L..."..la....."!.....*.....6].....P.....k.....@.....p.....D.....0.....A...8..p.....@:......H9..@.....\$......text...6......`.rdata..8.....@..@.data.....@.....rsrc...0.....@..@.reloc...A.....B.....@..B.....

C:\Windows\Installer\MSIA23E.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:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
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.....J.....T.....Rich!.....PE..L..."..la....."!.....*.....6].....P.....k.....@.....p.....D.....0.....A...8..p.....@:......H9..@.....\$......text...6......`.rdata..8.....@..@.data.....@.....rsrc...0.....@..@.reloc...A.....B.....@..B.....

C:\Windows\Installer\MSIA368.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:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227BA
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.....J.....T.....Rich!.....PE..L..."..la....."!.....*.....6].....P.....k.....@.....p.....D.....0.....A...8..p.....@:......H9..@.....\$......text...6......`.rdata..8.....@..@.data.....@.....rsrc...0.....@..@.reloc...A.....B.....@..B.....

C:\Windows\Installer\MSIA463.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

C:\Windows\Installer\MSIA463.tmp

SSDEEP:	24576:gJgZXIAIjfhETbF+RWQNgXAo1sVz1v0Mny+PkfsJJ10FRzVTv:F/fQhksQQNgXAo1sVzhly+PkfsJJ10FT
MD5:	0BE6E02D01013E6140E38571A4DA2545
SHA1:	9149608D60CA5941010E33E01D4FDC7B6C791BEA
SHA-256:	3C5DB91EF77B947A0924675FC1EC647D6512287AA891040B6ADE3663AA1FD3A3
SHA-512:	F419A5A95F7440623EDB6400F9ADBF9BA987A65F3B47996A8BB374D89FF53E8638357285485142F76758BFFCB9520771E38E193D89C82C3A9733ED98AE24FCB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......4.....3.....3.....3.?..... W...3.....Rich.....PE..L....la....."!.....KC...@.....t...d.....p.....T.....p.....@... ...h...@.....text.....`..rdata.....@...@.data...4.....@...rsrc.....@...@.reloc..T.....@...B.....

C:\Windows\Installer\MSIA5CB.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:hsEQsy5dfBkvAUUnBU76LNaiDWbqw0EAOqcmCIVKVPgvf:4sw6vAUUnBU7qax0EzIVYgvf
MD5:	3D24A2AF1FB93F9960A17D6394484802
SHA1:	EE74A6CEEA0853C47E12802961A7A8869F7F0D69
SHA-256:	8D23754E6B8BB933D79861540B50DECA42E33AC4C3A6669C99FB368913B66D88
SHA-512:	F6A19D00896A63DEBB9EE7CDD71A92C0A3089B6F4C44976B9C30D97FCBAACD74A8D56150BE518314FAC74DD3EBEA2001DC3859B0F3E4E467A01721B29F6227 BA
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..."la....."!.....*.....6P.....k....@.....p.....D.....0.....A...8..p.....@:..... ..H9..@.....\$......text...6.....`..rdata..8.....@...@.data.....@...rsrc...0.....@...@.reloc...A.....B...@...B.....

C:\Windows\Installer\MSIA6F5.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:qKrajAXKBGIpTOS7OmdoqacGOh40JEh+DiYgZmD8x32id4PIV1uJTG:dajmU120q+Byd4V4TG
MD5:	2A6C81882B2DB41F634B48416C8C8450
SHA1:	F36F3A30A43D4B6EE4BE4EA3760587056428CAC6
SHA-256:	245D57AFB74796E0A0B0A68D6A81BE407C7617EC6789840A50F080542DACE805
SHA-512:	E9EF1154E856D45C537F08CF466A4B10DEE6CF71DA47DD740F2247A7EB8216524D5B37FF06BB2372C31F6B15C38101C19A1CF7185AF12A17083207208C6CCB
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>.K.<..z>.Rich.z>.....PE..L....la....."!.....T.....!.....p.....@.....@.....f.....S.....h.....X.....p.....x...@.....p.....p..@.....text...S.....T.....`..rdata.....p.....X.....@...@.data.....n.....@...rsrc...h...@...@.reloc...X.....Z.....@..B.....

C:\Windows\Installer\MSIDECF.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	7110
Entropy (8bit):	5.543883277518376
Encrypted:	false
SSDEEP:	192:GUvgIVGUpQJuKqSJVmRiKWrvO2RZzibbiMMkzQetksKkBhlb:GUvgIIKQJuKqSJVmRiKWrvFRZzibbiMM
MD5:	8B98AC6CB180A723BA52B66DE98DBB00
SHA1:	F240F752D1906C927646942C76171B4BEB2FD66B
SHA-256:	52DAE72056C096A15C030B72425A7AA2CE40B1EB5E93C6336EBDD1D288BD3654
SHA-512:	59CBF88B3096B90790E7B1EDE78B01C3BAF61EA37E85CCA40506907929FC53CF2596E8F4BC932682B16BA490BAF7E02343A6ACABE8135F316A2A5CE2011ECD D4
Malicious:	false

C:\Windows\Installer\MSIDECF.tmp

Preview:	...@IXOS.@.....@YnyS.@.....@.....@.....@.....@.....@.....&{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}a.C:\Users\user\AppData\Roaming\JDesktop Integration Components (JDIC) Project\JDesktop Tools\.@.....@.....@.....@.....&{FC3D5B52-2561-4633-85CB-6F8B8A86F2F9}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_ExecPath.@.....@.....@.....@.....&{0B568A04-369C-43FB-98E4-C437A15709E0}p.C:\Users\user\AppData
----------	--

C:\Windows\Installer\SourceHash{4A523951-0A2F-4D65-A31E-BB22D0CE0CF4}

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.847457778563187
Encrypted:	false
SSDEEP:	48:OrgT6DEIt40I79ne//nTebf8GLx63my22yE7aN9I:0Pi4279e//GUGLxAPsEON9
MD5:	EC9297E1D1B30FD062C3D13EC6FAE024
SHA1:	B76ED0A7D03642896231301DEB05E66C3EA379C2
SHA-256:	87D8368D2560FDF65964732CAC93534A714C78E131E8195671C07356E46333ED
SHA-512:	F68EC8E4498CAA022BAEE9D60E699FE065EC043FB5E2B1CCCAC4213E3778D1C24B0E02C7D100865F048110C1B9BAB75877581F31E881729A6E2F5D9E15A0FE7
Malicious:	false
Preview:	>.....

C:\Windows\Installer\inprogressinstallinfo.ipi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.7748956870858386
Encrypted:	false
SSDEEP:	48:J8PhtuRc06WXzVFT5gN/QRGN/WML4WS+N/F48AE+ICyTYFDVfMLN/CS+N/eTkfPD:Eht1sFTaq8b1rXsZICMYwLkrZT
MD5:	9A3C4924DCD6AFF398A879B0B2FEE47B
SHA1:	6B1E8A43D852E11C3644B28AC5A5DF32A07AE930
SHA-256:	2D9E26197CD8B6E1D81CBD936A35DEEB7DA0377DA1CEB273830100DB6681CE7B
SHA-512:	9C22A09275FCEB280EC4A680DBCEE5F2F322F959074C993E42D1E3F0C75EBC69867130232B932F44C50CF9E39BFD31D420FEED46EA2A1C6F8D8ED3A7877470
Malicious:	false
Preview:	>.....

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 very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	174137
Entropy (8bit):	5.355131335414791
Encrypted:	false
SSDEEP:	768:2JcfxyJbOd+nlnu0SXmV9UmtiBMwM5CSXKqQMXlqNYL/AxVDTAMOfbDj/nCwpTA:2Jcl4n9Umtip5QctdL
MD5:	4A462112D12416AC50BBC02C2B36FD38
SHA1:	B7E892E195C31991A0D018587CEB1B3DB3909B1A
SHA-256:	E2011163D0DCD32141BB6DA4881354953197BD0EBC3533B6F882B1B4084E684D
SHA-512:	FFA25783EF36C6673A82012D2310F9821195854C0A07C616FB23B2E039E3CC1B91DB9DFCC45357661B375CED5DE58A6A3C147BE174E005837D719FB9ACA85C0
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 11:01:23.494 [4132]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting.v9.0, Version=9.0.0.00000000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 11:01:23.494 [4132]: ngen returning 0x00000000..07/23/2020 11:01:23.541 [2300]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument.v10.0, Version=10.0.0.00000000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 11:01:23.557 [2300]: ngen returning 0x00000000..07/23/2020 11:01:23.603 [5144]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.Outlook.v9.0, Version=9.0.0.00000000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3

C:\Windows\Templ~DF10CCF93C50CD522A.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.4065531844948
Encrypted:	false
SSDEEP:	48:DIVuZs4aFXzET5IUaN/QRGN/WML4WS+N/F48AE+ICyTYFDVfMLN/CS+N/eTkfPD:0V5WTLtq8b1rXsZICMYwLkrZT
MD5:	B83D4AD57B22D6C840CABAF481DF7B69
SHA1:	FD3A9D0C806D2DE3E775158B3260F2757769271F
SHA-256:	E6904D40BE74A50E33EC8A884BE38A402522AB04078EC407874A6736B36001D7
SHA-512:	F235B635A20E993DFA438873FFAE21605CE842135B6EE7D06DAB40DAF460C96475788DED1374DDC4ED6E580263D4A87F49318DE401B2E38B050ECBB8924401D
Malicious:	false
Preview:	>.....

C:\Windows\Templ~DF1B68F00AAEC82988.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	

C:\Windows\Templ~DF3E7A433E0C409AFC.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.7748956870858386
Encrypted:	false
SSDEEP:	48:J8PhtuRc06WXzVFT5gN/QRGN/WML4WS+N/F48AE+ICyTYFDVfMLN/CS+N/eTkfPD:Eht1sFTaq8b1rXsZICMYwLkrZT
MD5:	9A3C4924DCD6AFF398A879B0B2FEE47B
SHA1:	6B1E8A43D852E11C3644B28AC5A5DF32A07AE930
SHA-256:	2D9E26197CDB86E1D81CBD936A35DEEB7DA0377DA1CEB273830100DB6681CE7B
SHA-512:	9C22A09275FCEB280EC4A680DBCEEE5F2F322F959074C993E42D1E3F0C75EBC69867130232B932F44C50CF9E39BFD31D420FEED46EA2A1C6F8D8ED3A7877470
Malicious:	false
Preview:	>.....

C:\Windows\Templ~DF46C604FEF4F449F2.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	1.7748956870858386
Encrypted:	false
SSDEEP:	48:J8PhtuRc06WXzVFT5gN/QRGN/WML4WS+N/F48AE+ICyTYFDVfMLN/CS+N/eTkfPD:Eht1sFTaq8b1rXsZICMYwLkrZT
MD5:	9A3C4924DCD6AFF398A879B0B2FEE47B
SHA1:	6B1E8A43D852E11C3644B28AC5A5DF32A07AE930
SHA-256:	2D9E26197CDB86E1D81CBD936A35DEEB7DA0377DA1CEB273830100DB6681CE7B

C:\Windows\Temp\~DF46C604FEF4F449F2.TMP	
SHA-512:	9C22A09275FCB280EC4A680DBCCEE5F2F322F959074C993E42D1E3F0C75EBC69867130232B932F44C50CF9E39BFD31D420FEED46EA2A1C6F8D8ED3A7877470
Malicious:	false
Preview:	>.....

C:\Windows\Temp\~DF55CEC612D7410AC0.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	0.21722949201266403
Encrypted:	false
SSDEEP:	48:1PDYETSN/CS+N//N/WML4WS+N/F48AE+ICyTYFDVfM8AAN/./JYzkrbt1rXsZICMYwjA
MD5:	47C8CE31C5FD1A6F95E8227E33DC01CA
SHA1:	C2F4C22CF36C8046573FDDFC8F6917DF58F17660
SHA-256:	2A10145F68A6B37A9DB43623B1D40F5F467A17D685FD6D7BC75D0531FBD3AAA2
SHA-512:	D6C1098782C67F723F09A44D1BA15D3EC613202F896BAE7AAD496E464E6289230896540CBD1E543604C1EB324DB9B7CE97988DD9D90F33421A5FE2692C7B44A
Malicious:	false
Preview:	

C:\Windows\Temp\~DF761133D2E041DEFE.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.5618868915910008
Encrypted:	false
SSDEEP:	48:d9lsaml6DElt40l79ne//nTebfGLx63my22yE7:d9aaPi4279e//GUGLxAPsE
MD5:	619F55E8D28CF4BC286BB7BE49918993
SHA1:	A3CCAA9D38D12C041A3E42450DA4B1AC00A4E518
SHA-256:	9F2482C4E402EAC636ED64BF09BA117483F462D67791CEA785F3F3F157CF05D5
SHA-512:	C733F3355F8741D7E629516A2380283B6E7ED8DC4038B3F25101D38BF4F65E8DF377FDA6EF4E163250C53B94F7FA4941B5B8189A3061D02685508821F80CA782
Malicious:	false
Preview:	

C:\Windows\Temp\~DF776763C8FB17AE54.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.4065531844948
Encrypted:	false
SSDEEP:	48:DIVuZs4aFXzET5IUaN/QRGN/WML4WS+N/F48AE+ICyTYFDVfMLN/CS+N/eTkfPD:0V5WTLtq8b1rXsZICMYwLkrZT
MD5:	B83D4AD57B22D6C840CABAF481DF7B69
SHA1:	FD3A9D0C806D2DE3E775158B3260F2757769271F
SHA-256:	E6904D40BE74A50E33EC8A884BE38A402522AB04078EC407874A6736B36001D7
SHA-512:	F235B635A20E993DFA438873FFAE21605CE842135B6EE7D06DAB40DAF460C96475788DED1374DDC4ED6E580263D4A87F49318DE401B2E38B050ECBB8924401C
Malicious:	false
Preview:	>.....

C:\Windows\Temp\~DF91038100F0FB06FB.TMP	
Process:	C:\Windows\System32\msiexec.exe
File Type:	data

C:\Windows\Templ~DF91038100F0FB06FB.TMP

Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED341FE
Malicious:	false
Preview:	>.....

C:\Windows\Templ~DF94144FA3D8D2F215.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	1.4065531844948
Encrypted:	false
SSDEEP:	48:DI\UzS4aFXzET5IUaN\QRGN\WML4WS+N\F48AE+ICyTYFDVfMLN\CS+N/eTkfPD:0V5WTLtq8b1rXsZICMYwLkrZT
MD5:	B83D4AD57B22D6C840CABAF481DF7B69
SHA1:	FD3A9D0C806D2DE3E775158B3260F2757769271F
SHA-256:	E6904D40BE74A50E33EC8A884BE38A402522AB04078EC407874A6736B36001D7
SHA-512:	F235B635A20E993DFA438873FFAE21605CE842135B6EE7D06DAB40DAF460C96475788DED1374DDC4ED6E580263D4A87F49318DE401B2E38B050ECBB8924401CD
Malicious:	false
Preview:	>.....

C:\Windows\Templ~DFBABDC1C846730072.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED341FE
Malicious:	false
Preview:	>.....

C:\Windows\Templ~DFCB1E467AADEF7E4C.TMP

Process:	C:\Windows\System32\msiexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED341FE
Malicious:	false

C:\Windows\Templ~DFCB1E467AADEF7E4C.TMP

Preview:	
	

C:\Windows\Templ~DFECF05E5DA56163B3.TMP

Process:	C:\Windows\System32\lsimexec.exe
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	
	

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.710859774528812
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: flic, fli, cel) (7/3) 0.00%
File name:	jXzrlReInY.exe
File size:	7840296
MD5:	4ec77eb8280485764b6bc22f6cf7d57e
SHA1:	85215638743eeb6800aaada5d057e96032db6906
SHA256:	716ce7fe411f352686b4071074aa96e1456ab7a67445b3cf1c475e18a4e5ac25
SHA512:	770b14b133ac0a7bfee3a973d43a5342cd021a731f1be4c557a332aa4945dbb9be6b25909291feeb766c3fd640ff943780d4172e2fe6f6c77a128585e7914954
SSDEEP:	196608:cL6ocnTAcca9KJi4G+eiPUei/L6StB1o4lMjgflg/rNv+J3e:G6JnTAcca9KJi4teSq/WSb6aagfTTie
File Content Preview:	MZ.....@.....!..L!Th is 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...K...KX...J...KX.oK...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

General		
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:		
Signature Issuer:		
Signature Validation Error:		
Error Number:		
Not Before, Not After		
Subject Chain		
Version:		
Thumbprint MD5:		
Thumbprint SHA-1:		
Thumbprint SHA-256:		
Serial:		

Entrypoint Preview

Data Directories

Sections								
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
Nov 25, 2021 13:51:32.522811890 CET	192.168.2.7	8.8.8.8	0x41f2	Standard query (0)	get.update s.avast.cn	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 13:51:04.875520945 CET	8.8.8.8	192.168.2.7	0x9886	No error (0)	windowsupdate.s.llnwi.net		178.79.225.128	A (IP address)	IN (0x0001)
Nov 25, 2021 13:51:04.875520945 CET	8.8.8.8	192.168.2.7	0x9886	No error (0)	windowsupdate.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)
Nov 25, 2021 13:51:04.969217062 CET	8.8.8.8	192.168.2.7	0x5864	No error (0)	windowsupdate.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)
Nov 25, 2021 13:51:04.969217062 CET	8.8.8.8	192.168.2.7	0x5864	No error (0)	windowsupdate.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)
Nov 25, 2021 13:51:32.603698969 CET	8.8.8.8	192.168.2.7	0x41f2	Name error (3)	get.update s.avast.cn	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: jXzrlReInY.exe PID: 7000 Parent PID: 4732

General

Start time:	13:50:21
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\jXzrlReInY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\jXzrlReInY.exe"
Imagebase:	0x2b0000
File size:	7840296 bytes
MD5 hash:	4EC77EB8280485764B6BC22F6CF7D57E
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: msixec.exe PID: 4360 Parent PID: 560

General

Start time:	13:50:27
Start date:	25/11/2021
Path:	C:\Windows\System32\msixec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msixec.exe /V
Imagebase:	0x7ff73a390000
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: msixec.exe PID: 4344 Parent PID: 4360

General

Start time:	13:50:28
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msixec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding C5EB72BDE2B80B60A07F51ECA26339C7C
Imagebase:	0xef0000
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: msixec.exe PID: 6512 Parent PID: 7000

General

Start time:	13:50:29
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msixec.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_SETUP EXEPATH=C:\Users\user\Desktop\jXzrlReInY.exe SETUPEXEDIR=C:\Users\user\Desktop\ EXE_CMD_LINE="/exenoupdates /forcecleanup /wintime 1637876902 " AI_EUIMSI="
Imagebase:	0xef0000
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: 4852 Parent PID: 4360

General

Start time:	13:50:33
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding 54779E8B78CD501470CD2E1995D98D79
Imagebase:	0xef0000
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: plcd-player.exe PID: 6620 Parent PID: 4360

General

Start time:	13:51:00
Start date:	25/11/2021
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:	0x1a0000
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_1, Description: Yara detected Ursnif, Source: 00000011.00000002.530777240.00000000035F9000.00000004.00000040.sdmp, Author: Joe Security - Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000011.00000002.530869037.0000000003BA8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

[File Activities](#)

Show Windows behavior

[File Read](#)

Disassembly

Code Analysis