ID: 738927
Sample Name: giLqLXLHs3.exe
Cookbook: default.jbs
Time: 20:03:28
Date: 05/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

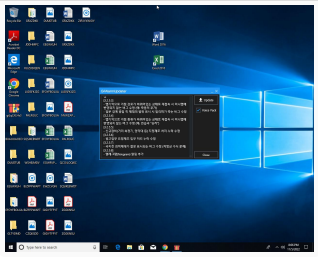
Windows Analysis Report

giLqLXLHs3.exe

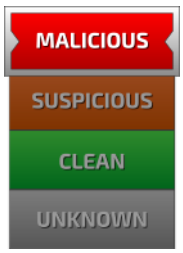
Overview

General Information

Sample Name:	giLqLXLHs3.exe
Analysis ID:	738927
MD5:	d7f34f1712688bb.
SHA1:	1245a185de1880.
SHA256:	c9944c04100d2b..
Tags:	exe
Infos:	



Detection

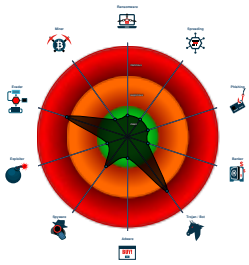


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dom…
- Yara detected Costura Assembly Lo…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Uses dynamic DNS services
- Uses 32bit PE files
- Queries the volume information (nam…
- Sample file is different than original …
- Detected TCP or UDP traffic on non…
- Internet Provider seen in connection…
- Binary contains a suspicious time s…
- Enables debug privileges

Classification



Process Tree

- **System is w10x64**
- giLqLXLHs3.exe (PID: 6084 cmdline: C:\Users\user\Desktop\giLqLXLHs3.exe MD5: D7F34F1712688BB9564296842355A8B9)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
giLqLXLHs3.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.520653994.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
00000000.00000000.241342686.00000000007F2000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: giLqLXLHs3.exe PID: 6084	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.giLqLXLHs3.exe.7f0000.0.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Networking

Uses known network protocols on non-standard ports

Uses dynamic DNS services

Data Obfuscation

Yara detected Costura Assembly Loader

Hooking and other Techniques for Hiding and Protection

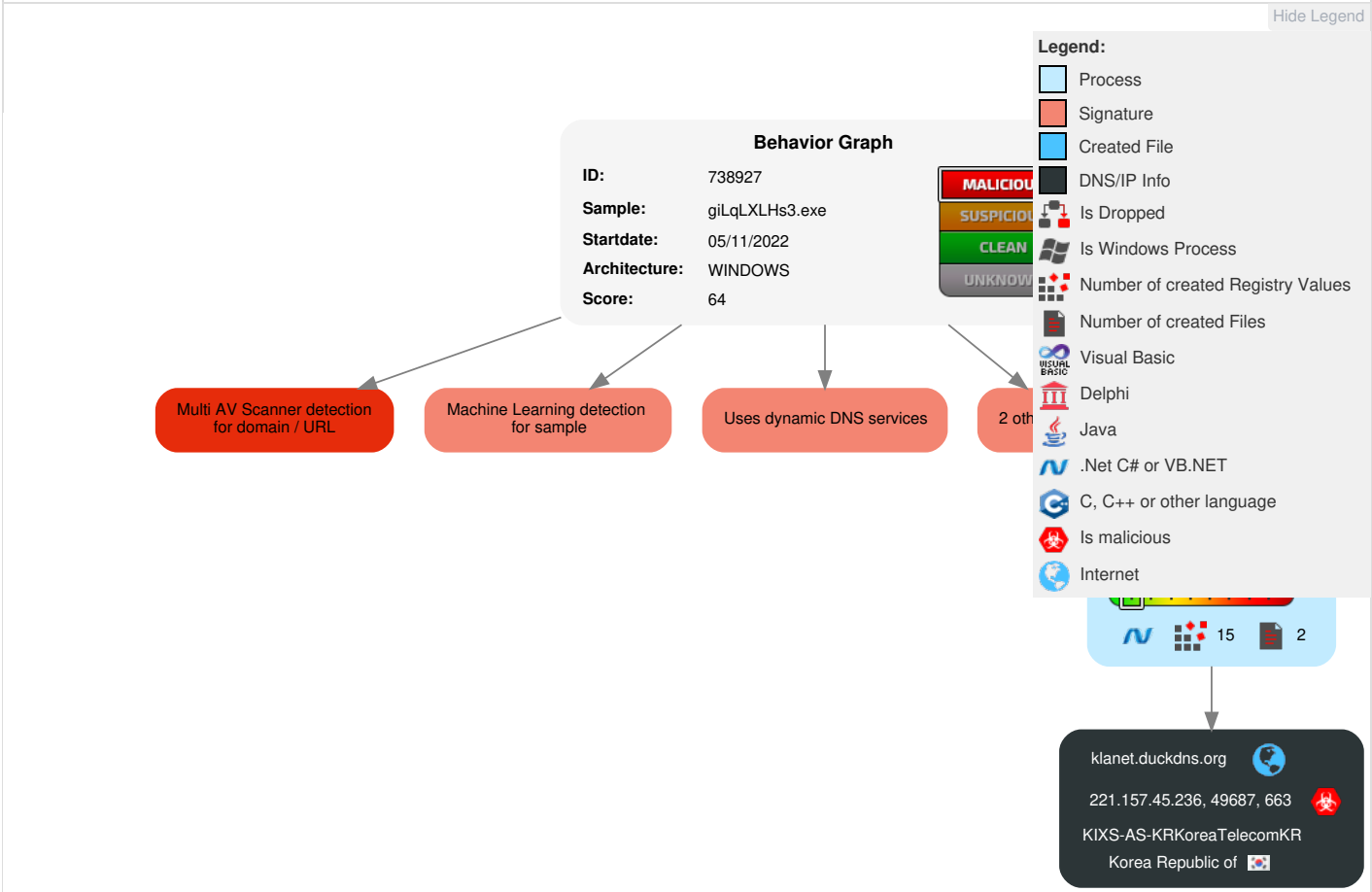
Uses known network protocols on non-standard ports

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Disable or Modify Tools	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Timestomp	LSASS Memory	1 2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Remote System Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

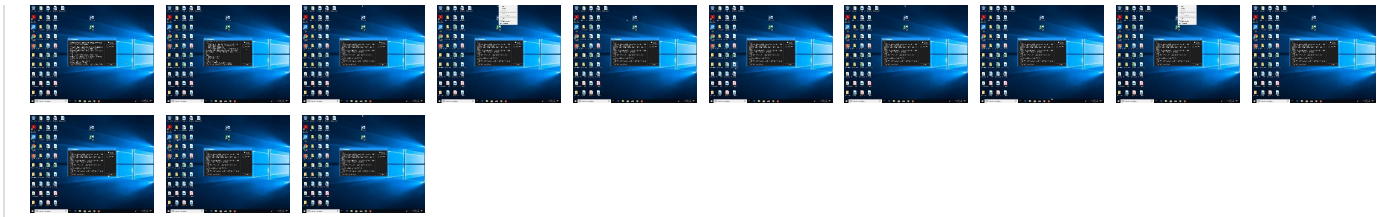
Behavior Graph



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
giLqLXLHs3.exe	0%	ReversingLabs		
giLqLXLHs3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
klanet.duckdns.org	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://klanet.duckdns.org:663/resource/version.tsv#downloadVoicePack#WindowBorderBrush	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://metro.mahapps.com/winfx/xaml/iconpacksp	0%	Avira URL Cloud	safe	
http://www.quickzip.org/BaseControlsx	0%	Avira URL Cloud	safe	
http://klanet.duckdns.org:663/resource/version.tsv#downloadVoicePack#WindowBorderBrush	3%	Virustotal		Browse
http://metro.mahapps.com/winfx/xaml/iconpackseup	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://metro.mahapps.com/winfx/xaml/iconpacks	0%	Virustotal		Browse
http://klanet.duckdns.org:663	0%	Avira URL Cloud	safe	
http://www.quickzip.org/BaseControls	0%	Avira URL Cloud	safe	
http://klanet.duckdns.org:663/version	0%	Avira URL Cloud	safe	
http://klanet.duckdns.org:663/resource/version.tsv	0%	Avira URL Cloud	safe	
http://metro.mahapps.com/winfx/xaml/iconpacks	0%	Avira URL Cloud	safe	
http://https://design.googleGoogle	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
klanet.duckdns.org	221.157.45.236	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://klanet.duckdns.org:663/resource/version.tsv	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

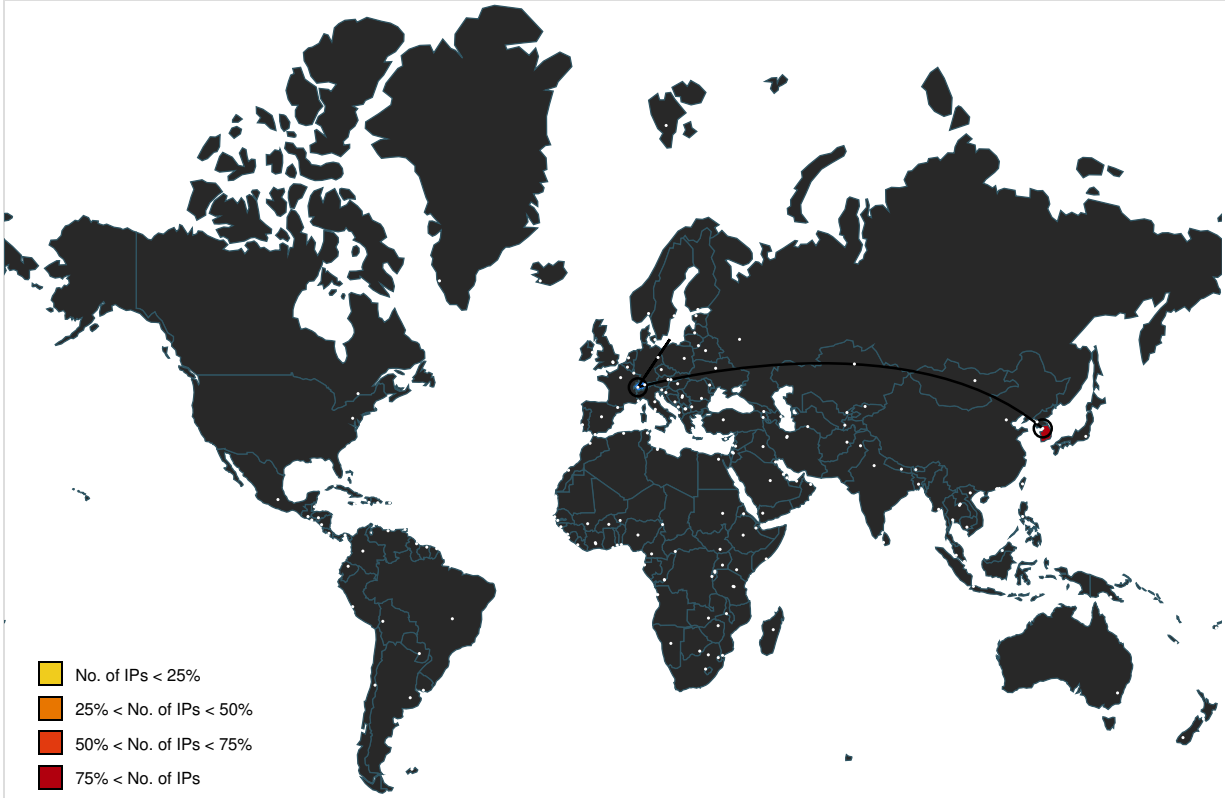
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/Templarian/MaterialDesign/blob/master/LICENSE	giLqLXLHs3.exe, 00000000.00000003.275151839.0000000004179000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.521156580.0000000002E80000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532888552.0000000005590000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.283786696.00000000047D9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://design.google	giLqLXLHs3.exe, 00000000.00000003.254202440.0000000005DEB000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.254322553.0000000005DEB000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.254180030.0000000005DEB000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.254271837.0000000005DEB000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.544737200.000000000A232000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/MahApps/MahApps.Metro.IconPacks.git&	giLqLXLHs3.exe, 00000000.00000002.537357922.0000000005A20000.00000004.08000000.00040000.00000000.sdmp	false		high
http://klanet.duckdns.org:663/resource/version.tsv#downloadVoicePack#WindowBorderBrush	giLqLXLHs3.exe	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://materialdesignicons.com/	giLqLXLHs3.exe, 00000000.00000003.283786696.00000000047D9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.quickzip.org/BaseControlsx	giLqLXLHs3.exe, 00000000.00000002.520653994.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://metro.mahapps.com/winfx/xaml/iconpacksp	giLqLXLHs3.exe, 00000000.00000002.520653994.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://nlog-project.org/	giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/json	giLqLXLHs3.exe, 00000000.00000003.245106817.0000000004059000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.244673513.0000000003E22000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532173168.00000000053A0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://github.com/MahApps/MahApps.Metro.IconPacks.git	giLqLXLHs3.exe, 00000000.00000003.275151839.0000000004179000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532888552.0000000005590000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.537357922.0000000005A20000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.283786696.00000000047D9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://metro.mahapps.com/winfx/xaml/iconpacks	giLqLXLHs3.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://metro.mahapps.com/winfx/xaml/iconpackseup	giLqLXLHs3.exe, 00000000.00000002.520653994.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	giLqLXLHs3.exe, 00000000.00000002.544818086.000000000A24E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.nuget.org/packages/NLog.Web.AspNetCore	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://design.googleGoogle	giLqLXLHs3.exe	false	• Avira URL Cloud: safe	unknown
http://james.newtonking.com/projects/json	giLqLXLHs3.exe, 00000000.00000002.532173168.00000000053A0000.00000004.08000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://klanet.duckdns.org:663	giLqLXLHs3.exe, 00000000.00000002.525163252.000000000330F000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nlog-project.org/ws/T	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nlog-project.org/ws/ILogReceiverServer/ProcessLogMessagesResponsep	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://gall.dcinside.com/micateam/1644952)	giLqLXLHs3.exe, 00000000.00000002.525163252.000000000330F000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://klanet.duckdns.org:663/version	giLqLXLHs3.exe	true	• Avira URL Cloud: safe	unknown
http://nlog-project.org/dummynamespace/	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nlog-project.org/ws/ILogReceiverOneWayServer/ProcessLogMessages	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.newtonsoft.com/jsonschema	giLqLXLHs3.exe, 00000000.00000002.532173168.00000000053A0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	giLqLXLHs3.exe, 00000000.00000003.245106817.0000000004059000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.244673513.0000000003E22000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532173168.00000000053A0000.00000004.08000000.00040000.00000000.sdmp	false		high
http://nlog-project.org/ws/	giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	giLqLXLHs3.exe, 00000000.00000002.544818086.000000000A24E000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.544737200.000000000A232000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nlog-project.org/ws/ILogReceiverServer/ProcessLogMessagesT	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.quickzip.org/BaseControls	giLqLXLHs3.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	giLqLXLHs3.exe, 00000000.00000002.525163252.000000000330F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://gall.dcinside.com/	giLqLXLHs3.exe, 00000000.00000002.525163252.000000000330F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/Templarian/MaterialDesign/blob/master/LICENSE-	giLqLXLHs3.exe, 00000000.00000003.275151839.0000000004179000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532888552.0000000005590000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.283786696.00000000047D9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nlog-project.org/ws/3	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nlog-project.org/ws/5	giLqLXLHs3.exe, 00000000.00000002.537390197.0000000005A30000.00000004.08000000.00040000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.529086758.0000000003E01000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.530861599.0000000004059000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/JamesNK/Newtonsoft.Json	giLqLXLHs3.exe, 00000000.00000003.245106817.0000000004059000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000003.244673513.0000000003E22000.00000004.00000800.00020000.00000000.sdmp, giLqLXLHs3.exe, 00000000.00000002.532173168.00000000053A0000.00000004.08000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
221.157.45.236	klanet.duckdns.org	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	738927
Start date and time:	2022-11-05 20:03:28 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	giLqLXLHs3.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
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:	mal64.troj.evad.winEXE@1/0@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Execution Graph export aborted for target giLqLXLHs3.exe, PID 6084 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.864152844370486
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	giLqLXLHs3.exe
File size:	2366976
MD5:	d7f34f1712688bb9564296842355a8b9
SHA1:	1245a185de18808ef075297fc4740d7a3b7b6381
SHA256:	c9944c04100d2b5d75b8bff00359b3bef6481bdb72d965032ac800d99cb4fe1a
SHA512:	686e1a19c760f48dc029d7fea8a523817a88e05f503780b7e0270787d7dd2e87fdc0d080ba711bc38dbfecf2d8d001cd011d80f3826156eb4fe8728f56077ae1
SSDEEP:	49152:TcGa5dzwr9jrwnkUeZw+W7SCYFllu0DcJ:LuUr9jrwn7eq2Fl/4J
TLSH:	90B50218B2DABE2DDBAB25FD46B5E2A9DD77615D1319821F3047F322E8290C00F446DE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...\|....."...0...#..~.....#.. .....@.. .....`$.....`.....

File Icon

Icon Hash:	ceb292d2d2d2d2d2

Static PE Info

General

Entrypoint:	0x63bc1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x81A88C7C [Tue Dec 7 03:54:36 2038 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23bbd0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x23c000	0x7a6c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x244000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x23bb44	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x239c24	0x239e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x23c000	0x7a6c	0x7c00	False	0.44137474798387094	data	6.562813008648801	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x244000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

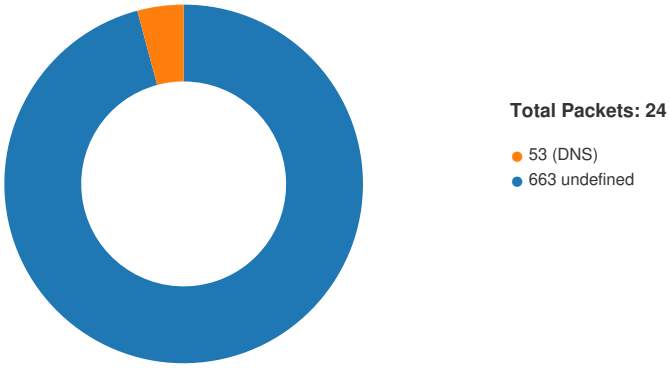
Name	RVA	Size	Type	Language	Country
RT_ICON	0x23c180	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024		
RT_ICON	0x23c5f8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304		
RT_ICON	0x23cf90	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x23e048	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x240600	0x23a8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x2429b8	0x4c	data		
RT_VERSION	0x242a14	0x34c	data		
RT_MANIFEST	0x242d70	0xcf8	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 5, 2022 20:04:33.673718929 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:33.928922892 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:33.929167032 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:33.955842972 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.210021973 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210508108 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210542917 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210567951 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210593939 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210614920 CET	49687	663	192.168.2.7	221.157.45.236

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 5, 2022 20:04:34.210617065 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210640907 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210664034 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210685968 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210690975 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.210690975 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.210707903 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210731030 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.210740089 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.210774899 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.464986086 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465080023 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465141058 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465190887 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465192080 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465245008 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465277910 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465320110 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465359926 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465395927 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465399027 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465440989 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465440989 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465482950 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465527058 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465533972 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465568066 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465606928 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465615988 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465646982 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465687037 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465691090 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465727091 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465764999 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465770006 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465804100 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465856075 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.465857029 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465898037 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.465949059 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.720782042 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720823050 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720845938 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720869064 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720911980 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720953941 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.720993996 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.721034050 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.721067905 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.721072912 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.721112967 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:04:34.721148968 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:04:34.721196890 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:05:39.212266922 CET	663	49687	221.157.45.236	192.168.2.7
Nov 5, 2022 20:05:39.212785959 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:06:14.806737900 CET	49687	663	192.168.2.7	221.157.45.236
Nov 5, 2022 20:06:15.061157942 CET	663	49687	221.157.45.236	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 5, 2022 20:04:33.538115025 CET	58346	53	192.168.2.7	8.8.8.8
Nov 5, 2022 20:04:33.651215076 CET	53	58346	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 5, 2022 20:04:33.538115025 CET	192.168.2.7	8.8.8.8	0xd662	Standard query (0)	klanet.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 5, 2022 20:04:33.651215076 CET	8.8.8.8	192.168.2.7	0xd662	No error (0)	klanet.duckdns.org		221.157.45.236	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- klanet.duckdns.org:663

Statistics

No statistics

System Behavior

Analysis Process: giLqLXLHs3.exe PID: 6084, Parent PID: 3320

General

Target ID:	0
Start time:	20:04:25
Start date:	05/11/2022
Path:	C:\Users\user\Desktop\giLqLXLHs3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\giLqLXLHs3.exe
Imagebase:	0x7f0000
File size:	2366976 bytes
MD5 hash:	D7F34F1712688BB9564296842355A8B9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.520653994.0000000002DF1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000000.241342686.00000000007F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D80CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D7E5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7ECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D7E5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C651B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C651B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatioaec034ca#\71c166f74def9b205fafc80dbd0c1015\PresentationFramework.Aero2.ni.dll.aux	unknown	1252	success or wait	1	6D7403DE	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly