

ID: 452457
Sample Name: kS2dqbsDwD
Cookbook: default.jbs
Time: 11:42:10
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report kS2dqbsDwD 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Yara Overview 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 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 9
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 11
General Information 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 13
JA3 Fingerprints 14
Dropped Files 15
Created / dropped Files 15
Static File Info 24
General 24
File Icon 24
Static PE Info 24
General 24
Authenticode Signature 25
Entrypoint Preview 25
Data Directories 25
Sections 25
Resources 25
Imports 25
Version Infos 25
Possible Origin 25
Network Behavior 26
Network Port Distribution 26
TCP Packets 26
UDP Packets 26
DNS Queries 26
DNS Answers 26
HTTP Request Dependency Graph 27
HTTP Packets 27
HTTPS Packets 28
Code Manipulations 29
Statistics 29
Behavior 29

Copyright Joe Security LLC 2021

System Behavior 29
Analysis Process: kS2dqbsDwD.exe PID: 5492 Parent PID: 5684 30
General 30
File Activities 30
File Created 30
File Written 30
Analysis Process: 325.exe PID: 4796 Parent PID: 5492 30
General 30
File Activities 30
File Created 30
File Written 30
File Read 30
Analysis Process: 325.exe PID: 1784 Parent PID: 4796 30
General 31
File Activities 31
File Created 31
File Deleted 31
File Read 31
Registry Activities 31
Disassembly 31
Code Analysis 31

Copyright Joe Security LLC 2021

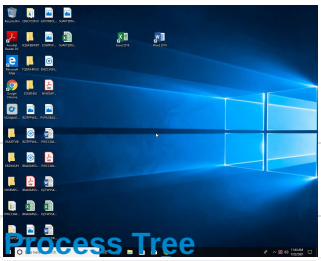
Windows Analysis Report kS2dqbsDwD

Overview

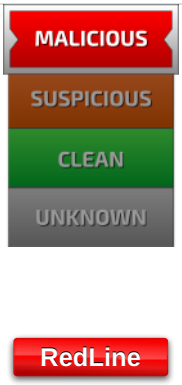
General Information

Sample Name:	kS2dqbsDwD (renamed file extension from none to exe)
Analysis ID:	452457
MD5:	888ab99280a081..
SHA1:	3a071aeadd42c1..
SHA256:	e726f2014db779e.
Tags:	exe trojan
Infos:	

Most interesting Screenshot:



Detection

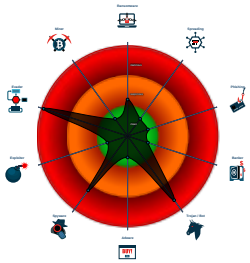


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected RedLine Stealer
- Yara detected RedLine Stealer
- .NET source code contains potentia…
- .NET source code contains very larg…
- May check the online IP address of …
- Performs DNS queries to domains w…
- Queries sensitive disk information (v…

Classification



- **System is w10x64**
- kS2dqbsDwD.exe (PID: 5492 cmdline: 'C:\Users\user\Desktop\kS2dqbsDwD.exe' MD5: 888AB99280A081717EC5C5749266D1BD)
  - 325.exe (PID: 4796 cmdline: C:\Users\user\AppData\Roaming\325.exe 325 MD5: 523AC177BFB4FB64A20B60FC0CE3E0E3)
    - 325.exe (PID: 1784 cmdline: {path} MD5: 523AC177BFB4FB64A20B60FC0CE3E0E3)
- **cleanup**

Malware Configuration

Threatname: RedLine

```
{
  "C2 url": [
    "yspasenana.xyz:80"
  ],
  "Bot Id": "world"
}
```

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.304492926.000000000295C000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.306874811.0000000003A20000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
0000000E.00000002.362046970.0000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: 325.exe PID: 4796	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: 325.exe PID: 1784	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.325.exe.3b45a60.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
14.2.325.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
2.2.325.exe.3b45a60.3.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:



May check the online IP address of the machine

Performs DNS queries to domains with low reputation

System Summary:



.NET source code contains very large strings

Sample or dropped binary is a compiled AutoHotkey binary

Data Obfuscation:



Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Malware Analysis System Evasion:



Yara detected AntiVM3

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Copyright Joe Security LLC 2021

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

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Yara detected RedLine Stealer

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

Remote Access Functionality:



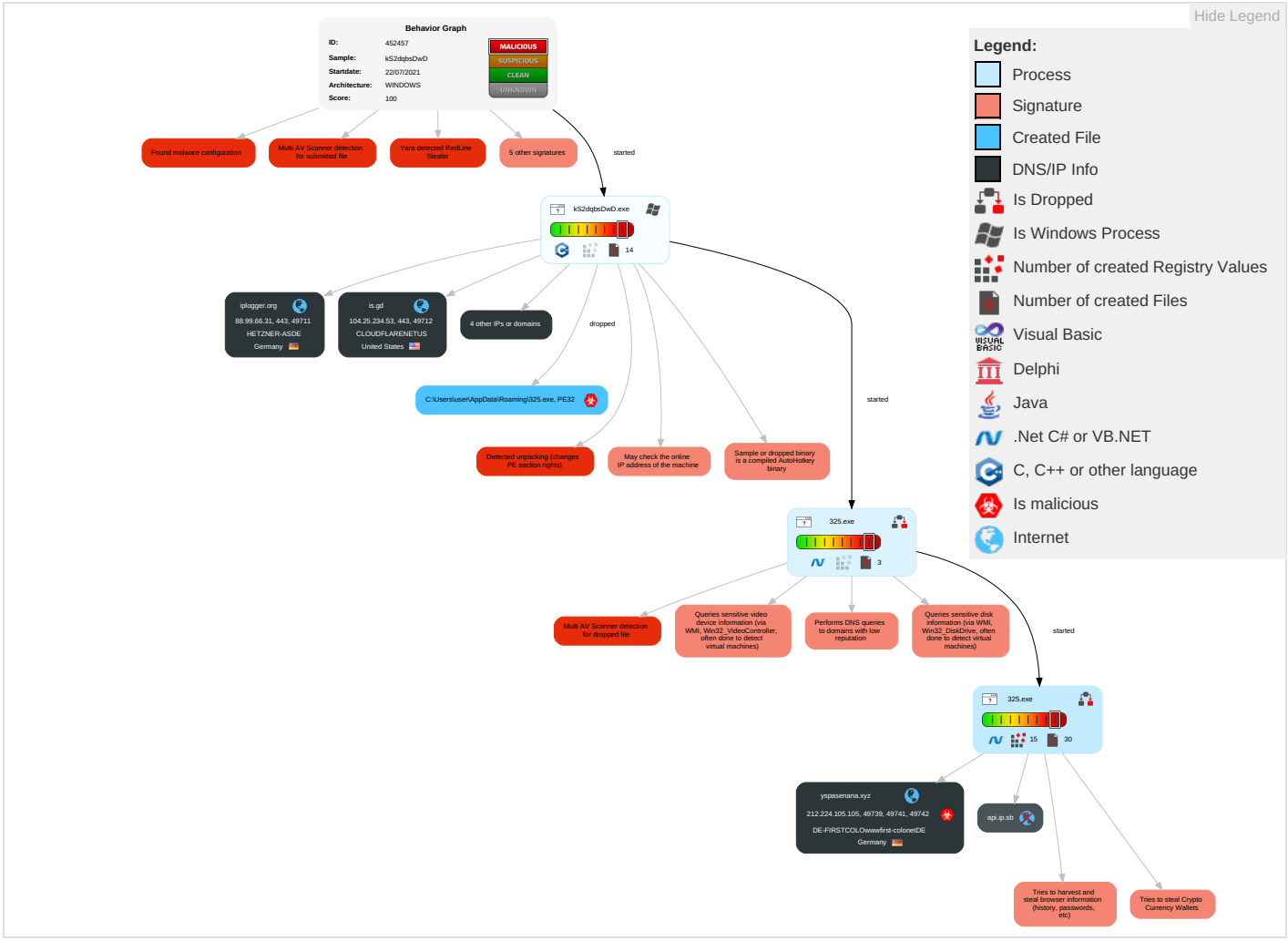
Yara detected RedLine Stealer

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Spearphishing Link 1	Windows Management Instrumentation 2 2 1	Path Interception	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Input Capture 3 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 2	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	System Information Discovery 1 3 6	Distributed Component Object Model	Input Capture 3 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 4 5 1	SSH	Clipboard Data 2	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 3 1	Cached Domain Credentials	Process Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

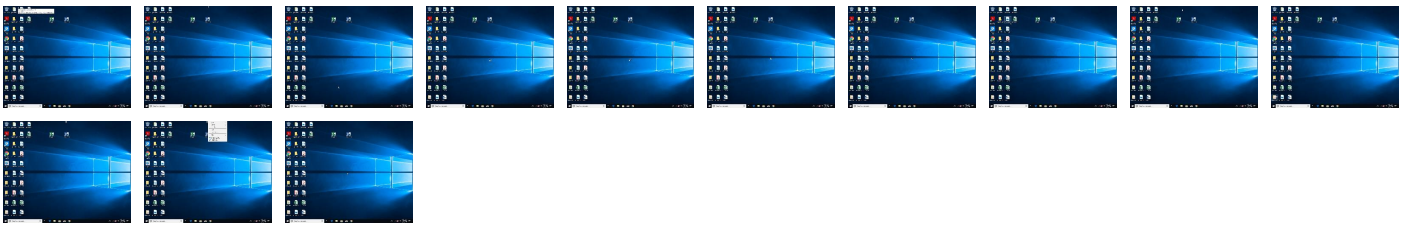
Behavior Graph



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
kS2dqbsDwD.exe	20%	Virustotal		Browse
kS2dqbsDwD.exe	13%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\325.exe	33%	ReversingLabs	ByteCode-MSIL.Infostealer.Reline	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.1.kS2dqbsDwD.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1142275		Download File
14.2.325.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140572		Download File

Domains

Source	Detection	Scanner	Label	Link
yspasenana.xyz	1%	Virustotal		Browse
api.ip.sb	2%	Virustotal		Browse

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://service.r	0%	URL Reputation	safe	
http://ahkscript.org	1%	Virustotal		Browse
http://ahkscript.org	0%	Avira URL Cloud	safe	
http://yspasenana.xyz/	1%	Virustotal		Browse
http://yspasenana.xyz/	0%	Avira URL Cloud	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip	0%	URL Reputation	safe	
http://yspasenana.xyz4	0%	Avira URL Cloud	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://yspasenana.xyz:80/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://yspasenana.xyz	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnviron	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	Avira URL Cloud	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://go.micros	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://https://d301sr5gafysq2.cloudfront.net;	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
s3-w.us-east-1.amazonaws.com	52.217.201.169	true	false		high
yspasenana.xyz	212.224.105.105	true	true	• 1%, Virustotal, Browse	unknown
bitbucket.org	104.192.141.1	true	false		high
iplogger.org	88.99.66.31	true	false		high
is.gd	104.25.234.53	true	false		high
bbuseruploads.s3.amazonaws.com	unknown	unknown	false		high
api.ip.sb	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://yspasenana.xyz/	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.224.105.105	yspasenana.xyz	Germany		44066	DE-FIRSTCOLOwwwfirst-colonetDE	true
104.192.141.1	bitbucket.org	United States		16509	AMAZON-02US	false
104.25.234.53	is.gd	United States		13335	CLOUDFLARENETUS	false
88.99.66.31	iplogger.org	Germany		24940	HETZNER-ASDE	false
52.217.201.169	s3-w.us-east-1.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452457
Start date:	22.07.2021
Start time:	11:42:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	kS2dqbsDwD (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/29@9/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2% (good quality ratio 0.9%) • Quality average: 31.8% • Quality standard deviation: 39.8%
HCA Information:	• Successful, ratio: 83% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:42:57	API Interceptor	1x Sleep call for process: kS2dqbsDwD.exe modified
11:44:07	API Interceptor	46x Sleep call for process: 325.exe modified

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
212.224.105.105	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• yspasenana.xyz/
104.192.141.1	Nb2HQZZDIf.exe	Get hash	malicious	Browse	
	r3xwkKS58W.exe	Get hash	malicious	Browse	
	P58w6OezJY.exe	Get hash	malicious	Browse	
	lpaBPnb1OB.exe	Get hash	malicious	Browse	
	2aJ9QdIdFE.exe	Get hash	malicious	Browse	
	EA4LughYnY.exe	Get hash	malicious	Browse	
	etSPaoVcAD.exe	Get hash	malicious	Browse	
	kxQkjkU9DO.exe	Get hash	malicious	Browse	
	9CMjcYFBxo.exe	Get hash	malicious	Browse	
	JvlwIeO09R.exe	Get hash	malicious	Browse	
	pEIro35JRJ.exe	Get hash	malicious	Browse	
	AEdU8eJHgN.exe	Get hash	malicious	Browse	
	YIrI3VuV0W.exe	Get hash	malicious	Browse	
	8zsiEeSTzI.exe	Get hash	malicious	Browse	
	k6sy0WOByI.exe	Get hash	malicious	Browse	
	kvAgGyJqYT.exe	Get hash	malicious	Browse	
	A7DmPhc0bs.exe	Get hash	malicious	Browse	
	Coupon-Codes-2021.doc	Get hash	malicious	Browse	
	k53f1UmAkl.exe	Get hash	malicious	Browse	
	q7jxy6gZMb.exe	Get hash	malicious	Browse	
104.25.234.53	Pdf Document.exe	Get hash	malicious	Browse	• is.gd/TGKGYYYYZ

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bitbucket.org	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 104.192.141.1
	HryPYPQtcg.exe	Get hash	malicious	Browse	• 104.192.141.1
	oOoVvuAQS9.exe	Get hash	malicious	Browse	• 104.192.141.1
	6FORhr7lC1.exe	Get hash	malicious	Browse	• 104.192.141.1
	2aJ9QdIdFE.exe	Get hash	malicious	Browse	• 104.192.141.1
	EA4LughYnY.exe	Get hash	malicious	Browse	• 104.192.141.1
	etSPaoVcAD.exe	Get hash	malicious	Browse	• 104.192.141.1
	kxQkjkU9DO.exe	Get hash	malicious	Browse	• 104.192.141.1
	9CMjcYFBxo.exe	Get hash	malicious	Browse	• 104.192.141.1
	JvlwIeO09R.exe	Get hash	malicious	Browse	• 104.192.141.1
	pEIro35JRJ.exe	Get hash	malicious	Browse	• 104.192.141.1
	AEdU8eJHgN.exe	Get hash	malicious	Browse	• 104.192.141.1
	YIrI3VuV0W.exe	Get hash	malicious	Browse	• 104.192.141.1
	8zsiEeSTzI.exe	Get hash	malicious	Browse	• 104.192.141.1
	k6sy0WOByI.exe	Get hash	malicious	Browse	• 104.192.141.1
	kvAgGyJqYT.exe	Get hash	malicious	Browse	• 104.192.141.1
	I2VQzf34i3.exe	Get hash	malicious	Browse	• 104.192.141.1
	A7DmPhc0bs.exe	Get hash	malicious	Browse	• 104.192.141.1
	Coupon-Codes-2021.doc	Get hash	malicious	Browse	• 104.192.141.1
	k53f1UmAkl.exe	Get hash	malicious	Browse	• 104.192.141.1
yspasenana.xyz	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 212.224.105.105
s3-w.us-east-1.amazonaws.com	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 52.216.94.27
	Machine Service.xlsx	Get hash	malicious	Browse	• 52.216.249.124
	Machine Service.xlsx	Get hash	malicious	Browse	• 52.217.102.108
	#Ud83d#Udd0ajs_msg_ 3pm.html	Get hash	malicious	Browse	• 52.217.11.68
	HryPYPQtcg.exe	Get hash	malicious	Browse	• 52.217.129.57
	6FORhr7lC1.exe	Get hash	malicious	Browse	• 52.217.202.41
	2aJ9QdIdFE.exe	Get hash	malicious	Browse	• 52.217.162.201
	EA4LughYnY.exe	Get hash	malicious	Browse	• 52.217.161.9
	etSPaoVcAD.exe	Get hash	malicious	Browse	• 52.217.80.164
	kxQkjkU9DO.exe	Get hash	malicious	Browse	• 52.216.128.43

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9CMjcYFBxo.exe	Get hash	malicious	Browse	• 52.216.137.244
	JvlwIeO09R.exe	Get hash	malicious	Browse	• 52.217.130.249
	pElro35JRJ.exe	Get hash	malicious	Browse	• 52.217.104.164
	AEdU8eJHgN.exe	Get hash	malicious	Browse	• 52.217.90.84
	YIrI3VuV0W.exe	Get hash	malicious	Browse	• 52.216.171.179
	8zsiEeSTzI.exe	Get hash	malicious	Browse	• 52.217.140.209
	k6sy0WOByI.exe	Get hash	malicious	Browse	• 52.217.101.132
	I2VQzf34i3.exe	Get hash	malicious	Browse	• 52.217.83.220
	k53f1UmAkl.exe	Get hash	malicious	Browse	• 52.217.10.252
	D1E3656B4E1C609B2540CFF74F59319A52D7FABF4CC51.exe	Get hash	malicious	Browse	• 52.217.164.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 104.25.233.53
	SgjcpodWpB.exe	Get hash	malicious	Browse	• 104.21.14.85
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	10303640_APMC-TRN-C0001-Stability_Calculation_Rev1.exe	Get hash	malicious	Browse	• 104.18.7.156
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 104.21.51.99
	Westernunionreceipt711 ___vaw.html	Get hash	malicious	Browse	• 104.21.40.98
	MPU702734-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	XuQRPW44hi	Get hash	malicious	Browse	• 104.21.58.112
	Remittance.html	Get hash	malicious	Browse	• 104.16.18.94
	jRPSjUSf.exe	Get hash	malicious	Browse	• 104.23.98.190
	989E2813477A4245E0357E0F8E49AFAE384AF828C95EE.exe	Get hash	malicious	Browse	• 104.21.71.170
	P58w6OezJY.exe	Get hash	malicious	Browse	• 104.25.234.53
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 172.67.130.27
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 162.159.134.233
	rxfttQnoO5	Get hash	malicious	Browse	• 1.13.147.24
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.21.72.95
	Cotizaci#U00f3n.pdf.exe	Get hash	malicious	Browse	• 104.21.36.131
	aviso de pago.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 172.67.130.27
	kRGc0HgN5b.exe	Get hash	malicious	Browse	• 172.67.188.154
DE-FIRSTCOLOwwwfirst-colonetDE	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 212.224.105.105
	SgjcpodWpB.exe	Get hash	malicious	Browse	• 212.224.105.79
	Px9H2c5Uo4.exe	Get hash	malicious	Browse	• 212.224.105.80
	eBjKjtQjDN.exe	Get hash	malicious	Browse	• 212.224.105.115
	ruoMVmVwPu.exe	Get hash	malicious	Browse	• 212.224.105.79
	GHK2s5apNB.exe	Get hash	malicious	Browse	• 212.224.105.79
	m8TJbe5yP6.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Trojan.Win32.Save.a.312.exe	Get hash	malicious	Browse	• 212.224.105.79
	SecuriteInfo.com.Variant.Cerbu.108262.10538.exe	Get hash	malicious	Browse	• 212.224.105.79
	d9MvOgFpyI.exe	Get hash	malicious	Browse	• 212.224.105.115
	0832946463ff710ff7f783ce24756f455a843852b0b96.exe	Get hash	malicious	Browse	• 212.224.105.115
	Order 161488.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 161488.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 46975986.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	PO 97179275.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	Order 46975986.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	PO 97179275.xlsb	Get hash	malicious	Browse	• 212.224.124.82
	what_is_a_xydhias_agreement.js	Get hash	malicious	Browse	• 37.17.224.94
	what_is_a_xydhias_agreement.js	Get hash	malicious	Browse	• 37.17.224.94
	no_response_will_be_considered_as_agreement_email.js	Get hash	malicious	Browse	• 37.17.224.94
AMAZON-02US	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 52.216.94.27
	ovLjmo5UoE	Get hash	malicious	Browse	• 63.34.62.30
	o3ZUDIEL1v	Get hash	malicious	Browse	• 18.151.13.78
	D1dU3jQ1Il	Get hash	malicious	Browse	• 34.208.242.240
	mal.exe	Get hash	malicious	Browse	• 52.58.78.16

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	vjsBNwolo9.js	Get hash	malicious	Browse	• 76.223.26.96
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 52.217.135.113
	A7X93JRxhp	Get hash	malicious	Browse	• 54.151.74.14
	1Ds9g7CEsp	Get hash	malicious	Browse	• 13.208.189.104
	XuQRPW44hi	Get hash	malicious	Browse	• 54.228.23.118
	Taf5zLti30	Get hash	malicious	Browse	• 44.231.84.110
	5qpsqg7U0G	Get hash	malicious	Browse	• 34.219.219.82
	LyxN1ckWTW	Get hash	malicious	Browse	• 18.139.244.68
	ZlvFNj.dll	Get hash	malicious	Browse	• 3.16.22.120
	U4r9W64doy	Get hash	malicious	Browse	• 13.245.89.196
	C4PozjQdGE	Get hash	malicious	Browse	• 18.135.214.121
	kb5IbEJU8c	Get hash	malicious	Browse	• 18.227.43.189
	MD5OxTSc6i	Get hash	malicious	Browse	• 18.149.163.217
	P58w6OezJY.exe	Get hash	malicious	Browse	• 52.217.198.209
	c51w5YSYdO	Get hash	malicious	Browse	• 108.146.15 5.164

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	#U00e2_#U00e2_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	41609787.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	B5xK9XEvzO.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	RsEvjl1iTt.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	ORD.ppt	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	39pfFwU3Ns.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	47a8af.exe.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	Comprobante1.vbs	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	ZlvFNj.dll	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	QT2kxM315B.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	4QKHQR82Xt.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	Convert HEX uit phishing mail.htm	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	192-3216-Us.gt.com.html	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	N41101255652.vbs	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	FILE_2932NH_9923.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	RDlkHCLRxE.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	#U2706_#U260e_Play _to _Listen.htm	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31
	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.217.201.169 • 104.25.234.53 • 88.99.66.31

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\325.exe	Nb2HQZZDIf.exe	Get hash	malicious	Browse	
	P58w6OezJY.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\325.exe.log	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp2299.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3

C:\Users\user\AppData\Local\Temp\tmp2299.tmp	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Temp\tmp229A.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8.....

C:\Users\user\AppData\Local\Temp\tmp5525.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\tmp5526.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C.....

C:\Users\user\AppData\Local\Temp\tmp5555.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5556.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5557.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5558.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109

C:\Users\user\AppData\Local\Temp\tmp5558.tmp	
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp5588.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8757.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8758.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp8758.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8759.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBA03.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBC57.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBC58.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960

C:\Users\user\AppData\Local\Temp\tmpBC58.tmp	
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBE63.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6969712158039245
Encrypted:	false
SSDEEP:	24:zDLHcjl8IQ6sNUYzo1jfRRMF6zzC3ZzNTWx7M00:zDL4ImUYzebRR66C3Z0JMR
MD5:	31CD00400A977C512B9F1AF51F2A5F90
SHA1:	3A6B9ED88BD73091D5685A51CB4C8870315C4A81
SHA-256:	E01ADE9C56AF2361A5ADC05ADE2F5727DF1B80311A0FDC6F15B2E0FFFACC9067
SHA-512:	0521ED245FA8F46DE9502CD53F5A50B01B4E83983CC6D9DE0CF02E54D2825C1C26A748CC27E24633DA1171CE0309323235ECF7EB536D4058214D7618794CF2F
Malicious:	false
Preview:	PWCCAWLGRESZQJYMKOMIHTZVFVPFCSAZVTKGMPWIGSDMTLFZQLHJERDPYZCJGFCRLISWNBAMIMDXCWDVGVLWLRBEVYOOPHYWACKPZXSURGSIFW TFUJKLSAQNAJEWDLUIKFHXLUAMUDGRAVFMICAHEZBIIEGWGAVVJHMHSIBGNLEHYVSOKQMYABDYCPEBOGBMYUCIGVRGYYQRAYNYHAIBMHOTRIZL LYBECMXTCFUOVXXHSEMIUWSBDHOZIZZUXFTLKXXNEMXBKLCQDPKVZNOMDYUYJRWCVILZVJDNNBMPTNOFSKRQTILJRXTKDNUIYSQCAOPCQKTXYX PPGZDZOQYLGYFPFIWNBSQZXYABPTNBJQNBZEETJSFXZNHXBRWUHOMCZAGZQJLNPMZFALBBPHBIXZHLBTBJLTUHPUYVUDWDFJANSIIDJVMUYLPZ PYGAJWMTOHGILQWHKJDQUWMTSWIBVVZGAHCNWIFZNGNERRKMSIVXWXEXRZZEWYASCIYJYCOOBWRTNZELPWKFVZKZIBGQBLGCTSTNAJSWPHYJCQ SYZVFRYFSRAVVXJIOHQCNVEOIMWPEAVCJLBHRUKDHJWPFMXAKTZVQCOUKYCBZFWBREKKHOHZVNMMJZGWIZEYRAIKTHMJRCWVWKNMJNSZHSDRUZ SQOJKCTOSNGKOKEAWUIQNIYHWKIIDHKQIJWCSGRRLEVUTENXSNNVDVYDJTIWYNCAZIEBXMIROLIBTLMGEUOCECFFWLENTJSVHFKQHKAPBXQAJJ SUOUSFCBQTHCFYZGSVVAUPLQELRWLXRCZSUSFUBCORCWMJPUNHTEEYODSFGJFTDZLLXMQYMIHIZXOYGABIAWYSBWLAJSCKBWGJBVMMJKBKLUHU LJIUHQXIXESAUTNVVZNKMIVIOHPPQAWTQSEHTQMIWNPRZRETXZHRGWOTGIEHCCSGIUCKCIFCQPTAJOFCIMYSMCOPGASEEYCNQLXCNRAPQUSQXT WPKPYCQXPE

C:\Users\user\AppData\Local\Temp\tmpBE64.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702247102869977
Encrypted:	false
SSDEEP:	24:GwASqxXUeo2spEcwb4NnVEBb2Ag1EY9TDqVEQXZvnIx+:nAD1U6+Lwb4dV42x1EIeVlXZ/5
MD5:	B734D7226D90E4FD8228EE89C7DD26DA
SHA1:	EDA7F371036A56A0DE687FF97B01F355C5060846
SHA-256:	ED3AE18072D12A2B031864F502B3DA672B4D4FA8743BEC8ADE114460F53C24D6
SHA-512:	D11ED908D0473A6BEA78D56D0E46FC05DAE642C6ED2F6D60F7859BB25C596CDAA79CC7883FEA5C175A2C04BD176943FF45670B19D6A55B3D5F29FAF40A19A 20
Malicious:	false
Preview:	QCFWYSKMHARLAFTMDAYCDPDNVLLXYAHYJQVDDKWMWZXTODMVQHOWYAKZGPKJEHLDEADLWAOYFHCRBONQYOLNJKXLXXPSVNNBUMGS SHSRYIKKLNWBJSSZQFZBFWIPYYALBWYXPUCHCBPPPRVICZHAAXDBSBDAFSJSLRPZCKMILDLKTZJTTJWTRDUXPIOSWYRPJKVLJAGHSGEPPERRAQ LAJLIRGZPORRNBHIKYMYWHJJKNXIQOPDJPXFLFPWXDCSZYFDTACTIFVHTTSPLEYMJQGMJBZKBTPKCSRPHSAJZDKKKDYFDICXMYAQSFGBCKRXTF XXUYCXPOOHXIGGOZQXUOJXGUHUEOJLEOQQRFQRNQSWAOWAWOUVFMKBPTZVBCGRCYEHPXUWCDBHICKJYVGTNPPMEWNTSWYZNREIVB OXSICNBJXTOOMRYUPEHBVWMTIZHWLGFFTIUYFBQKZOWLOZMSGJFBUHXKMGISFGKCABOUUUQJAUODQPPYPQJGLZVADLCCGHPBEUWSDDXYCCQVTR QWCEJDTNAGHKGJTRWVAQBQJBUQWMJRXXASIQFFIUCPKMEXTJTVBDCBEYZDLKHCHQXMUBNRVRITBTYGULZYWAXVJAXNQEPONBFIAUWZCXQYHHPH ZWKKUTNXAQELCSUFKXKKQLLKNVNOREOWTEVCFHSUGPNRMAPAFPTHPGPAJPOCFBZXTIYQYUSEJFOUEZDUJSRXDHTOZAMMNCCIXWLXFQZALVARMP TDBNFJAJUMFQAHUJVWMEIDRIMZQXYHMCNBVLONHTHCXFAKSQBBXFBBFYSTIWNRKGOIHMIHZKIQSYCSFIRGLYFATERWSKAZLTFNMKHFVBLMXNER MNYZHBEYHNFPIPCGHZZMBNNYITUETKSXMZHNSGROLAGIITATFDCBZCBLYQHHYFPBDWGCTQNYPHDHFBNVEJJDIVMSPKDXKQBUNSMLJDVGOKQUEV KEVEUUSGEQJDKGYLPIDXNBIPBAJRUU

C:\Users\user\AppData\Local\Temp\tmpBE65.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6980379859154695

C:\Users\user\AppData\Local\Temp\tmpBE65.tmp	
Encrypted:	false
SSDEEP:	24:A1cICRRGh4wXAyCbnhdKjiaeD+ICv1Ka42P:0clYRGh4wXyny+VEV42P
MD5:	4E3F4BE1B97FA984F75F11D95B1C2602
SHA1:	C34EB2BF97AB4B0032A4BB92B9579B00514DC211
SHA-256:	59176791FFEBB86CD28FF283F163F0A44BEC33273968AADFF3852F383F07D1E1
SHA-512:	DD9C44C85AF10ED76900A2FE9289D28D99FB56CBE5385A46E485BE0F97A3EA7B119FE3235F334D84FA15902EA78F43C334424240B834D272849356421A33B207
Malicious:	false
Preview:	QNCYCDFIJJXXFOBBXUZWOFUQSSNNMFYIDILWLHTAZLHLJONMCDCVNCVXWBMUFJZAFKEEPNXZDYZJCSPOAMORBEETMACWAZGGTOXJCHTDTMVBHR PTLBCYZORACSZOXJZRVMZHVEOODGKJRRYLCKUFAYOXVKWJMPRNRNPZEPQZONIUXPPIZMRKSMXAPWYEFYYMMEVAXOVEZSPBEJXENHLIHXQMWJRN UJFILZBVCHZGSXSCZDLUJYAIEMFAKMGZRGVOACZDULPMTHUOBPJBMVYTDCJXFDPUECDSDSUEAFWGDFBMYZQEFBBNQHNIAZWLZMSUFKUWZABFJA THSHQHDIAVRZTRYPZQQLMBOTPFBQKJDTMNKBJAFYFAYVOMBSWHOBUQSYEBLHEDVKQNGPPYYDHQTDNFMKYJBWQRTHICJRWSTTREOOBMYGBUCHFD YMGHVLBDKHYWLYGTEDTHOSIOSXLWGESBKVKNDNLHUVLLUBIQJIAQTVGZHJBFRBPSLHGPZGCZVLETNOSXQRRSQJBXTKDASBHEZXYVHEIZXGANNJ HMIMQYHDFNNALGZYXGCPYFPYZSCSPKUMVVWIRDXSMSGEKGZNWWWVXGTXWDKSTXVLHRXFELLCWRSIFVJLOUVSMBXWSHSPQZUHHYPA NCFLOAYKMMBXMIXYFORAFUEVNVTQFWGSCJZEOHRNDHLLFYLQFOZXARKDDGYWBOFNOCUJWZALYSUEUOMQHCYTBHPYEDSSAKKDECQAZIWWHOJPIM NYUNNZPDBNECENBWFCTSDYUMRCXDFCNYFVTFUUWRGBGWUGZTYCTBQVNAVSKZCNNOJNXDSQUTVJLYJMHLQJJBPEDZOTOVFCJLUVQVIEYTFNEEDH KMXTEKAIHTQBGOPUGKWWNQTAGBHAUZVKMHWVZTYKYOWJYFEGCIPREWFGAHFXDMSFOAYRDJCTSGYNSDSELZDMIXRNFGOTYBEUKLAOAVMHJKZEBG SCQHGCDZCAAGIVBGWEQA

C:\Users\user\AppData\Local\Temp\tmpBE66.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6969712158039245
Encrypted:	false
SSDEEP:	24:zDLHcjI8IQ6sNUYzo1jfRRMF6zzC3ZzNTWx7M00:zDL4ImUYzebRR66C3Z0JMR
MD5:	31CD00400A977C512B9F1AF51F2A5F90
SHA1:	3A6B9ED88BD73091D5685A51CB4C8870315C4A81
SHA-256:	E01ADE9C56AF2361A5ADC05ADE2F5727DF1B80311A0FDC6F15B2E0FFFACC9067
SHA-512:	0521ED245FA8F46DE9502CD53F5A50B01B4E83983CC6D9DE0CF02E54D2825C1C26A748CC27E24633DA1171CE0309323235ECF7EB536D4058214D7618794CF2F
Malicious:	false
Preview:	PWCCAWLGRESZQJYMKOMIHTZVFVPFCSAZVTKGMPWIGSDMTLFZQLHJERDPYZCJGFCRLISWNBAMIMDXCWDVGVLWLRBEVYOOPHYWACKPZXSURGSIFW TFUJKLSAQNAJEWDLUIKFHXLUAMUDGRAVFMICAHEZBIIEGWGAVVJHMHSIBGNLEHYVSOKQMYABDYCPEBOGBMYUCIGVRGYYQRAYNYHAIBMHOTRIZL LYBECMXTCFUOVXXHSEMIUWSBDHOZIZZUXFTLKXXNEMXBKLCQDPKVZNOMDYUYJRWCVILZVJDNNBMPTNOFSKRQTILJRXTKDNUIYSQCAOPCQKTXYX PPGZDZOQYLGYFPFIWNBSQZXYABPTNBJQNBZEETJSFXZNHXBRWUHOMCZAGZQJLNPMZFALBBPHBIXZHLBTBJLTUHPUYVUDWDFJANSIIDJVMUYLPZ PYGAJWMTOHGILQWHKJDQUWMTSWIBVVZGAHCNWIFZNGNERRKMSIVXWXEXRZZEWYASCIYJYCOOBWRTNZELPWKFVZKZIBGQBLGCTSTNAJSWPHYJCQ SYZVFRYFSRAVVXJIOHQCNVEOIMWPEAVCJLBHRUKDHJWPFMXAKTZVQCOUKYCBZFWBREKKHOHZVNMMJZGWIZEYRAIKTHMJRCWVWKNMJNSZHSDRUZ SQOJKCTOSNGKOKEAWUIQNIYHWKIIDHKQIJWCSGRRLEVUTENXSNNVDVYDJTIWYNCAZIEBXMIROLIBTLMGEUOCECFFWLENTJSVHFKQHKAPBXQAJJ SUOUSFCBQTHCFYZGSVVAUPLQELRWLXRCZSUSFUBCORCWMJPUNHTEEYODSFGJFTDZLLXMQYMIHIZXOYGABIAWYSBWLAJSCKBWGJBVMMJKBKLUHU LJIUHQXIXESAUTNVVZNKMIVIOHPPQAWTQSEHTQMIWNPRZRETXZHRGWOTGIEHCCSGIUCKCIFCQPTAJOFCIMYSMCOPGASEEYCNQLXCNRAPQUSQXT WPKPYCQXPE

C:\Users\user\AppData\Local\Temp\tmpBE67.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702247102869977
Encrypted:	false
SSDEEP:	24:GwASqxXUeo2spEcwb4NnVEBb2Ag1EY9TDqVEQXZvnIx+:nAD1U6+Lwb4dV42x1EIeVlXZ/5
MD5:	B734D7226D90E4FD8228EE89C7DD26DA
SHA1:	EDA7F371036A56A0DE687FF97B01F355C5060846
SHA-256:	ED3AE18072D12A2B031864F502B3DA672B4D4FA8743BEC8ADE114460F53C24D6
SHA-512:	D11ED908D0473A6BEA78D56D0E46FC05DAE642C6ED2F6D60F7859BB25C596CDAA79CC7883FEA5C175A2C04BD176943FF45670B19D6A55B3D5F29FAF40A19A 20
Malicious:	false
Preview:	QCFWYSKMHARLAFTMDAYCDPDNVLLXYAHYJQVDDKWMWZXTODMVQHOWYAKZGPKJEHLDEADLWAOYFHCRBONQYOLNJKXLXXPSVNNBUMGS SHSRYIKKLNWBJSSZQFZBFWIPYYALBWYXPUCHCBPPPRVICZHAAXDBSBDAFSJSLRPZCKMILDLKTZJTTJWTRDUXPIOSWYRPJKVLJAGHSGEPPERRAQ LAJLIRGZPORRNBHIKYMYWHJJKNXIQOPDJPXFLFPWXDCSZYFDTACTIFVHTTSPLEYMJQGMJBZKBTPKCSRPHSAJZDKKKDYFDICXMYAQSFGBCKRXTF XXUYCXPOOHXIGGOZQXUOJXGUHUEOJLEOQQRFQRNQSWAOWAWOUVFMKBPTZVBCGRCYEHPXUWCDBHICKJYVGTNPPMEWNTSWYZNREIVB OXSICNBJXTOOMRYUPEHBVWMTIZHWLGFFTIUYFBQKZOWLOZMSGJFBUHXKMGISFGKCABOUUUQJAUODQPPYPQJGLZVADLCCGHPBEUWSDDXYCCQVTR QWCEJDTNAGHKGJTRWVAQBQJBUQWMJRXXASIQFFIUCPKMEXTJTVBDCBEYZDLKHCHQXMUBNRVRITBTYGULZYWAXVJAXNQEPONBFIAUWZCXQYHHPH ZWKKUTNXAQELCSUFKXKKQLLKNVNOREOWTEVCFHSUGPNRMAPAFPTHPGPAJPOCFBZXTIYQYUSEJFOUEZDUJSRXDHTOZAMMNCCIXWLXFQZALVARMP TDBNFJAJUMFQAHUJVWMEIDRIMZQXYHMCNBVLONHTHCXFAKSQBBXFBBFYSTIWNRKGOIHMIHZKIQSYCSFIRGLYFATERWSKAZLTFNMKHFVBLMXNER MNYZHBEYHNFPIPCGHZZMBNNYITUETKSXMZHNSGROLAGIITATFDCBZCBLYQHHYFPBDWGCTQNYPHDHFBNVEJJDIVMSPKDXKQBUNSMLJDVGOKQUEV KEVEUUSGEQJDKGYLPIDXNBIPBAJRUU

C:\Users\user\AppData\Local\Temp\tmpBE68.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmpBE68.tmp	
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6980379859154695
Encrypted:	false
SSDEEP:	24:A1cICRRGh4wXAyCbnhdKjiaeD+ICv1Ka42P:0cIYRGh4wXyny+VEV42P
MD5:	4E3F4BE1B97FA984F75F11D95B1C2602
SHA1:	C34EB2BF97AB4B0032A4BB92B9579B00514DC211
SHA-256:	59176791FFEBB86CD28FF283F163F0A44BEC33273968AADFF3852F383F07D1E1
SHA-512:	DD9C44C85AF10ED76900A2FE9289D28D99FB56CBE5385A46E485BE0F97A3EA7B119FE3235F334D84FA15902EA78F43C334424240B834D272849356421A33B207
Malicious:	false
Preview:	QNCYCDFIJJXXFOBBXUZWOFUQSSNNMFYIDILWLHTAZLHLJONMCDCVNCVXWBMUFJZAFKEEPNXZDYZJCSPOAMORBEETMACWAZGGTOXJCHTDTMVBHR PTLBCYZORACSZOXJZRVMZHVEOODGKJRRYLCKUFAYOXVKWJMPRNRNPZEPQZONIUXPPIZMRKSMXAPWYEFYYMMEVAXOVEZSPBEJXENHLIHXQMWJRN UJFILZBVCHZGSXSCZDLUJYAIEMFAKMGZRGVOACZDULPMTHUOBPJBMVYTDCJXFDPUECDSDSUEAFWGDFBMYZQEFBBNQHNIAZWLZMSUFKUWZABFJA THSHQHDIAVRZTRYPZQQLMBOTPFBQKJDTMNKBJAFYFAYVOMBSWHOBUQSYEBLHEDVKQNGPPYYDHQTDNFMKYJBWQRTHICJRWSTTREOOBMYGBUCHFD YMGHVLBDKHYWLYGTEDTHOSIOSXLWGESBKVKNDNLHUVLLUBIQJIAQTVGZHJBFRBPSLHGPZGCZVLETNOSXQRRSQJBXTKDASBHEZXYVHEIZXGANNJ HMIMQYHDFNNALGZYXGCPYFPYZSCSPKUMVVWIRDXSMSGEKGZNWWWVXGTXWDKSTXVLHRXFELLCWRSIFVJLOUVSMBXWSHSPQZUHHYPA NCFLOAYKMMBXMIXYFORAFUEVNVTQFWGSCJZEOHRNDHLLFYLQFOZXARKDDGYWBOFNOCUJWZALYSUEUOMQHCYTBHPYEDSSAKKDECQAZIWWHOJPIM NYUNNZPDBNECENBWFCTSDYUMRCXDFCNYFVTFUUWRGBGWUGZTYCTBQVNAVSKZCNNOJNXDSQUTVJLYJMHLQJJBPEDZOTOVFCJLUVQVIEYTFNEEDH KMXTEKAIHTQBGOPUGKWWNQTAGBHAUZVKMHWVZTYKYOWJYFEGCIPREWFGAHFXDMSFOAYRDJCTSGYNSDSELZDMIXRNFGOTYBEUKLAOAVMHJKZEBG SCQHGCDZCAAGIVBGWEQA

C:\Users\user\AppData\Local\Temp\tmpEAF7.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEFBD.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEFBE.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F

C:\Users\user\AppData\Local\Temp\tmpEFBE.tmp	
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEFBF.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpEFC0.tmp	
Process:	C:\Users\user\AppData\Roaming\325.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\325.exe	
Process:	C:\Users\user\Desktop\kS2dqbsDwD.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	979968
Entropy (8bit):	7.361382512565047
Encrypted:	false
SSDEEP:	12288:cGRXJBEsyGeV5qLHKK1QK1MuSUqMidk++KANTbCPpUlmLXIRE:T9JB8rWHKK131MuadkJK4qrXIW
MD5:	523AC177BFB4FB64A20B60FC0CE3E0E3
SHA1:	BB965F2D97B19ED01702B8182BBD870670A1E75B
SHA-256:	20E702B077D7CF9780192671268C321BB0A76BAEC0A731413A1F04F735EEDCE3
SHA-512:	BD6C23385D7B914AD9A423D71DF9FA33BA917BA696270DF1435D90DE24B7B1286A7263FD10A027C17C41A899E5667F4481C83B385931ECCD244AEA7971D519F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Joe Sandbox View:	• Filename: Nb2HQZZDIf.exe, Detection: malicious, Browse • Filename: P58w6OezJY.exe, Detection: malicious, Browse

C:\Users\user\AppData\Roaming\325.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....".....@... ...`....@.. ....@.....P@..K.....0.....`..... ..... ..H.....text.... ... ...".....  ..`.sdata.. ....`.....&.....@....rsr c...0.....(.....@..@.reloc.....`.....@..B..... ....

C:\Users\user\AppData\Roaming\field	
Process:	C:\Users\user\Desktop\kS2dqbsDwD.exe
File Type:	PNG image data, 1 x 1, 1-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.529003957966892
Encrypted:	false
SSDEEP:	3:yionv//thPlE+kSI+Dtmy/Y+sR3Qhl/09h/rywOhSllln+wbp:6v/lhPfkCDtmywFghK9hm9Wlln+Yp
MD5:	EC6AAE2BB7D8781226EA61ADCA8F0586
SHA1:	D82B3BAD240F263C1B887C7C0CC4C2FF0E86DFE3
SHA-256:	B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599
SHA-512:	AA62A8CD02A03E4F462F76AE6FF2E43849052CE77CCA3A2CCF593F6669425830D0910AFAC3CF2C46DD385454A6FB3B4BD604AE13B9586087D6F22DE644F9DF(7
Malicious:	false
Preview:	.PNG.....IHDR.....%.V.....PLTE....z=.....tRNS.@..f....pHYs.....+.....IDAT..c`.....qd.....IEND.B`.

Static File Info

General

File type:	MS-DOS executable, MZ for MS-DOS
Entropy (8bit):	7.218310131625728
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	kS2dqbsDwD.exe
File size:	598944
MD5:	888ab99280a081717ec5c5749266d1bd
SHA1:	3a071aeadd42c1232ff2878d2adf7f1e4a629180
SHA256:	e726f2014db779e3605f60499f84676ceb45160c6d092be dfa115f7e09d693e8
SHA512:	85b78c1489ed6a8fd375380595f3597968d026de0bd0cfe 58e26cd4d6590f1d171626c0a8f677cc71d7405e5e647ed e4692e615fd63a63597db724da15dc2299
SSDEEP:	12288:67iuUvUF2JURoyPa5UA5/zfqb3HtwQG99:67iuU v8Paz/2ZwJ99
File Content Preview:	MZ@.....!..L.!Win64 .EXE...$@...PE ..d....4.V.....#.....R.....@..... ....@.....X.....p..4 _.....'.....

File Icon



Icon Hash:	d2ae86929a86a2c2

Static PE Info

General

Entrypoint:	0x14013c352
Entrypoint Section:	.MPRESS2
Digitally signed:	true
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, RELOCS_STRIPPED

General

DLL Characteristics:	HIGH_ENTROPY_VA
Time Stamp:	0x56F734A2 [Sun Mar 27 01:17:22 2016 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	caa5e6a2892587c2324418efee31c648

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 5/22/2019 5:00:00 PM 5/23/2023 4:59:59 PM
Subject Chain	• CN=Sublime HQ Pty Ltd, O=Sublime HQ Pty Ltd, STREET=Suite 102, STREET=377 New South Head Rd, L=Doubte Bay, S=NSW, PostalCode=2028, C=AU
Version:	3
Thumbprint MD5:	A32549731E28A0F6BA85C9B2C50FE589
Thumbprint SHA-1:	834F29A60152CE36EB54AF37CA5F8EC029ECCF01
Thumbprint SHA-256:	E025B15847B86808B69C605D7FC63A186CBF1D9A4ED5A1971B2FF5F9C6F50DF0
Serial:	00972FADA2BC13FA55C5D47FEF56AEE0F4

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.MPRESS1	0x1000	0x13b000	0x63400	False	1.00031240161	data	7.99951858505	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.MPRESS2	0x13c000	0xe80	0x1000	False	0.50732421875	data	5.63658087631	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x13d000	0x2b508	0x2b600	False	0.124651026657	data	3.38878491057	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, 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
Jul 22, 2021 11:42:58.675287962 CEST	192.168.2.3	8.8.8.8	0x574a	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.322242022 CEST	192.168.2.3	8.8.8.8	0x554	Standard query (0)	is.gd	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.694236040 CEST	192.168.2.3	8.8.8.8	0x65e1	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:00.422305107 CEST	192.168.2.3	8.8.8.8	0xd23c	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:04.846780062 CEST	192.168.2.3	8.8.8.8	0xda5e	Standard query (0)	yspasenana.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:06.823750973 CEST	192.168.2.3	8.8.8.8	0xd22d	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:06.892400026 CEST	192.168.2.3	8.8.8.8	0x9e5c	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:11.579966068 CEST	192.168.2.3	8.8.8.8	0x4d94	Standard query (0)	yspasenana.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:12.352585077 CEST	192.168.2.3	8.8.8.8	0xa170	Standard query (0)	yspasenana.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:42:58.733603001 CEST	8.8.8.8	192.168.2.3	0x574a	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.391592026 CEST	8.8.8.8	192.168.2.3	0x554	No error (0)	is.gd		104.25.234.53	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.391592026 CEST	8.8.8.8	192.168.2.3	0x554	No error (0)	is.gd		172.67.83.132	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.391592026 CEST	8.8.8.8	192.168.2.3	0x554	No error (0)	is.gd		104.25.233.53	A (IP address)	IN (0x0001)
Jul 22, 2021 11:42:59.755548954 CEST	8.8.8.8	192.168.2.3	0x65e1	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:00.481355906 CEST	8.8.8.8	192.168.2.3	0xd23c	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:43:00.481355906 CEST	8.8.8.8	192.168.2.3	0xd23c	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:43:00.481355906 CEST	8.8.8.8	192.168.2.3	0xd23c	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.201.169	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:04.907150984 CEST	8.8.8.8	192.168.2.3	0xda5e	No error (0)	yspasenana.xyz		212.224.105.105	A (IP address)	IN (0x0001)
Jul 22, 2021 11:44:06.884871960 CEST	8.8.8.8	192.168.2.3	0xd22d	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:44:06.953299999 CEST	8.8.8.8	192.168.2.3	0x9e5c	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:44:11.641484976 CEST	8.8.8.8	192.168.2.3	0x4d94	No error (0)	yspasenana.xyz		212.224.105.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:44:12.412575006 CEST	8.8.8.8	192.168.2.3	0xa170	No error (0)	yspasenana.xyz		212.224.105.105	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- yspasenana.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49739	212.224.105.105	80	C:\Users\user\AppData\Roaming\325.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:44:05.202037096 CEST	6920	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings" Host: yspasenana.xyz Content-Length: 144 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:44:05.249474049 CEST	6920	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:44:05.354886055 CEST	6922	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:44:05 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 33 65 34 0d 0a 1f 8b 08 00 00 00 00 00 02 03 bd 58 6d 8f e2 36 10 fe 2b 11 d2 4a 2d ba 25 5c b7 dd 9e 10 87 c4 4b d8 a2 2e bb 94 70 7b ad 94 2f c6 19 88 8b e3 89 6c 67 03 ab fb f1 75 42 c2 42 ef b6 2a 31 ad 84 48 3c e3 79 32 1e 8f c7 8f dd 55 1d 4f 3c 03 c7 04 9c 6d cc 85 ea a8 8f 8d 48 eb a4 e3 ba 8a 46 10 13 d5 32 72 85 24 69 a1 5c bb f9 8b 0b a5 85 db e8 75 55 67 80 e1 ae d7 35 28 4c a2 88 41 68 1f b4 66 62 ad e6 a0 12 14 aa 04 3e c0 6a 88 93 54 b2 02 ae f1 96 61 ca 75 e9 0f f9 d8 18 48 cc 14 48 6f ab 41 28 86 a2 51 aa d8 01 33 cb b2 56 76 53 40 fe d0 6e bf 77 7f 9f de fb 85 f7 d7 4c 28 4d 04 05 f3 25 d2 19 70 a4 1b 08 87 98 0a 2d 77 25 ca f2 ab 01 c7 8c 4a 54 b8 d2 2d 8a 71 0e 78 e3 be 6f bb 3e 48 46 38 7b 21 da b8 e0 f6 a5 24 3b d5 70 8f 60 27 b3 8b 21 3e 2e ff 04 aa 7f ec 69 99 42 d7 7d 6d 1f 54 b7 bd 15 e1 ea 48 77 9b eb 7c 4a 44 19 2c 75 b0 3d 11 96 9d 86 91 c4 18 2a e9 8c e8 48 5d c2 f7 5e 77 d9 51 5a 9a 39 ec 5d 7d f2 bd f9 6c fe 38 9e dc 7b 57 41 3f 49 46 44 93 e0 1e 29 e1 c1 80 68 cd a1 25 40 77 dd 83 c1 bf 33 2d 1c 67 69 1c 7c 32 8e 3b b9 e2 6c 88 3b c4 35 87 3d 12 58 e3 7c b7 fd 70 fb bd 0d d8 1c 49 6c b4 c1 63 02 92 38 be 89 73 46 24 04 67 bb 33 25 09 07 5f a7 21 c3 d2 9d 19 4f 95 c5 f8 26 92 85 76 91 fe d9 d7 44 96 ff f5 51 86 a6 32 94 99 6a 83 12 41 88 da 02 e0 89 3d 13 1e 32 0b 84 5f cd 9c 98 46 7d 00 8f 43 5e 26 95 63 1f 0e 2f 61 d4 99 49 33 26 ba bb 00 5c 3a c4 97 29 84 cc 8c 4e 12 61 01 34 06 21 99 74 26 82 06 3e 07 96 08 26 7f 0a d4 7e 5f 08 62 0c 53 0e ea 50 04 9e 18 64 20 cf 4f 05 f3 ca 99 20 77 12 d3 24 18 32 63 81 36 99 85 98 a1 a8 1e f5 71 38 83 25 b1 71 e4 37 b3 01 f9 a9 5c 59 40 3c ca 25 d3 56 6b 7e 88 66 96 30 18 49 b2 b6 8a 46 3f 66 eb 7d 30 2c 40 16 28 69 64 61 ff 07 11 21 6c cb c7 05 6a d0 3e 36 f5 01 6e 6e db 95 17 f6 de 4c c9 56 47 28 6e 6c 2a da f5 d4 10 41 9b 69 f6 93 54 0b b6 39 3c eb 23 3d 30 6a bb a3 0f 91 9a df 05 42 6b 59 04 8b fa 66 97 29 53 c2 78 6b 9e 06 7d 8d 36 ab 79 20 c9 33 1c 38 49 d1 ba be 40 e6 55 8c 32 f0 c2 b5 cd 84 3d 3c 4d 46 93 be 33 44 99 a0 2c 98 68 25 ba 83 b1 59 fb e0 78 5b 43 ab 18 98 03 c0 f9 a9 a9 81 c4 e7 cf 9d dc 25 1a 17 64 f9 cf bb aa fb 26 0f af 28 fa 88 29 8a 32 7c e5 f9 c7 c2 b2 cf 78 31 3b a1 f9 79 bb 52 31 b3 53 9e 2a 0b c9 b1 fa 3f e1 fd a9 19 49 22 71 65 3e 70 15 8c 40 6d 34 26 5f 9a 2d bd d5 ef 9a ad 10 69 f3 5d 73 03 3b f3 9f 11 ce 41 9b 17 05 10 36 bf b4 bf 1d ea 53 38 a4 69 c1 80 ce 06 74 ff 3e ec 2a 10 77 40 37 f8 ff 1f 84 2a d6 3f c5 17 c6 39 09 c6 4c c2 0a b7 35 ce 0d 9f 89 06 59 cf b4 28 df 80 a2 86 e9 22 4a cd 9e 68 d8 82 0c 6b 58 97 1b e1 84 c2 9e 27 d4 80 f8 90 00 dd aa e2 b8 63 08 e1 6e 59 37 06 0f de e2 ae bf f0 9c 05 d0 48 20 c7 35 33 04 73 c0 09 dd fc 42 b2 1a 78 53 44 41 23 c6 43 c3 ae 0d 5d a5 79 56 a8 60 46 38 38 b9 ea 1b 39 f9 75 06 56 b9 e9 53 09 20 4e 16 71 29 aa 3a e4 25 ea b4 42 ec 45 a5 7e 61 a6 77 2d 4d fb 18 e2 20 2c 3b 3d cd 1e 4e 21 72 41 a9 fb 5c 2c a9 d3 3a 52 c9 ba ee 9b 57 37 6f ea 8a fb 20 a3 ad 6e 8d dc d7 eb a7 de 5f e7 f1 c2 3e 8b 12 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 3e4Xm6+J-%\K.p{/lguBB*1H<y2UO<mHF2r$i\uUg5(LAhfb>jTauHHoA(Q3VvS@nwL(M%p-w%JT-qxo>HF8{!$;p`!>.iB}mTHw|JD,u=*H]^wQZ9]}l8{WA?IFD)h%@w3-gi|2;I;5=X|pIlc8sF$g3%_!O&vDQ2jA=2_F}C^&c/aI3&\:)Na4!t&>&~_bSPd O w$2c6q8%q7\Y@<%Vk~f0IF?f}0,@(ida!lj>6nnLVG(nl*AiT9<#=0jBkYf)Sxk}6y 38l@U2=<MF3D,h%Yx[C%d&()2|x1;yR1S*?I"qe>p@m4&_-i]s;A6S8it>*w@7*?9L5Y("JhkX'cnY7H 53sBxSDA#C]yV`F889uVS Nq):%BE~aw-M ,;=N!r A\,:RW7o n_>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	212.224.105.105	80	C:\Users\user\AppData\Roaming\325.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:44:11.703536034 CEST	6928	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/SetEnvironment" Host: yspasenana.xyz Content-Length: 1125491 Expect: 100-continue Accept-Encoding: gzip, deflate
Jul 22, 2021 11:44:11.753475904 CEST	6928	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:44:12.285859108 CEST	8049	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:44:12 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 37 65 0d 0a 1f 8b 08 00 00 00 00 00 02 03 45 ce 51 0a 83 40 0c 04 d0 ab c8 1e c0 fc 2f eb 7e 08 bd 80 9e 40 da 50 05 37 09 3b 69 69 6f af 2d b6 fe 0d 03 f3 98 84 78 91 27 af 6a dc bc ca 2a 88 e8 c2 ec 6e 91 08 d7 99 cb 84 76 ef a1 93 b5 5a ef f4 09 c4 c7 82 42 4e 88 bd de de 39 8d ec 3b b4 54 95 c2 e2 03 c3 54 70 98 7f d1 b9 d8 a3 2e 5f 29 50 4e f4 5b d3 79 23 6f 17 76 26 42 93 00 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 7eEQ@/~@P7;iio-x'j*nvZBN9;TTp._)PN[y#ov&B0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49742	212.224.105.105	80	C:\Users\user\AppData\Roaming\325.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:44:12.465971947 CEST	8050	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetUpdates" Host: yspasenana.xyz Content-Length: 1125483 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:44:12.515531063 CEST	8050	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:44:13.002619982 CEST	9171	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 09:44:12 GMT Content-Type: text/xml; charset=utf-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=3 Vary: Accept-Encoding Content-Encoding: gzip Data Raw: 62 33 0d 0a 1f 8b 08 00 00 00 00 00 02 03 65 8f c1 0a c2 30 0c 86 5f 45 7a 77 99 7a 2b 5d 0f 03 f1 a2 17 45 f0 5a b6 e0 0a 5b 5b 96 cc ce b7 77 8e 3a 41 6f e1 4f f2 e5 8b 22 b9 77 0f 6c 7d c0 d5 d8 b5 8e 24 15 a2 61 0e 12 80 aa 06 3b 43 d9 94 93 37 21 f3 fd 1d de 05 60 da 00 a1 15 c9 d2 d7 4f ad 0e c8 d7 50 1b 46 3a 23 05 ef 28 f1 16 1a 63 17 86 de ce 14 f1 33 3f b4 9c ae 9b 42 94 bd 8f 84 fd 7e 64 74 64 bd 13 a9 65 17 54 8c 31 8b bb 99 b4 cd f3 0d dc 4e c7 cb ec ba b6 8e d8 b8 0a 05 68 05 ff 4a 53 f8 f1 85 ef e3 fa 05 18 8f 8c 84 05 01 00 00 0d 0a 30 0d 0a 0d 0a Data Ascii: b3e0_Ezwz+]EZ[[w:AoO"wl}$a;C7!`OPF:#(c3?B~dtdeT1NhJS0

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jul 22, 2021 11:42:58.915039062 CEST	88.99.66.31	443	192.168.2.3	49711	CN=*.iplogger.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Fri Nov 20 01:00:00 CET 2020 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019	Sun Nov 21 00:59:59 CET 2021 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
Jul 22, 2021 11:42:59.480372906 CEST	104.25.234.53	443	192.168.2.3	49712	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=California, C=US CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Fri Jun 11 02:00:00 CEST 2021 Mon Jan 27 13:48:08 CET 2020	Sat Jun 11 01:59:59 CEST 2022 Wed Jan 01 00:59:59 CET 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Cloudflare Inc ECC CA-3, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:48:08 CET 2020	Wed Jan 01 00:59:59 CET 2025		
Jul 22, 2021 11:43:00.024015903 CEST	104.192.141.1	443	192.168.2.3	49713	CN=bitbucket.org, OU=Bitbucket, O="Atlassian, Inc.", L=San Francisco, ST=California, C=US, SERIALNUMBER=3928449, OID.1.3.6.1.4.1.311.60.2.1.2=Delaware, OID.1.3.6.1.4.1.311.60.2.1.3=US, OID.2.5.4.15=Private Organization CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Mar 27 01:00:00 CET 2020 Tue Oct 22 14:00:00 CEST 2013	Mon May 23 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert SHA2 Extended Validation Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Jul 22, 2021 11:43:00.820909977 CEST	52.217.201.169	443	192.168.2.3	49715	CN=*.s3.amazonaws.com, O="Amazon.com, Inc.", L=Seattle, ST=Washington, C=US CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 11 01:00:00 CET 2021 Tue Dec 08 13:05:07 CET 2015	Sat Feb 12 00:59:59 CET 2022 Sat May 10 14:00:00 CEST 2025	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=DigiCert Baltimore CA-2 G2, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Dec 08 13:05:07 CET 2015	Sat May 10 14:00:00 CEST 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: kS2dqbsDwD.exe PID: 5492 Parent PID: 5684

General

Start time:	11:42:57
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\kS2dqbsDwD.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\kS2dqbsDwD.exe'
Imagebase:	0x140000000
File size:	598944 bytes
MD5 hash:	888AB99280A081717EC5C5749266D1BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: 325.exe PID: 4796 Parent PID: 5492

General

Start time:	11:43:03
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\325.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\325.exe 325
Imagebase:	0x3b0000
File size:	979968 bytes
MD5 hash:	523AC177BFB4FB64A20B60FC0CE3E0E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.304492926.000000000295C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000002.00000002.306874811.0000000003A20000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 33%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 325.exe PID: 1784 Parent PID: 4796

General

Start time:	11:43:44
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\325.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6b0000
File size:	979968 bytes
MD5 hash:	523AC177BFB4FB64A20B60FC0CE3E0E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000E.00000002.362046970.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021