Investigation and actions

Screenpressobeta.zip

Allowed 1 time for 1 user
Source details

Time of analysis

File analysis: 2021-10-28 08:57:00
Sandstorm: 2021-10-28 08:57:01

Overall verdict

SUSPICIOUS

Analysis discovered 4 suspicious activities and 0 malware detection. Details

Memory	Suspicious
Changes the permissions of a memory region used by system libraries	Reads data from the local Windows system configuration
Creates a memory region with executable permission	Performs injection by UserQueueApc into another process Thread

Analysis summary

LIKELY CLEAN	SUSPICIOUS	SUSPICIOUS	LIKELY CLEAN	SUSPICIOUS	NOT DETECTED	None
Machine learning Overall analysis	Machine learning Feature analysis	Machine learning Feature combinations	Machine learning Structure analysis	Reputation	Sandstorm	XG malware scan

Information about your file

File name	Screenpressobeta.zip
File type	application/zip
SHA1	a8a7f4868bca823cd6b759eb5be0ae6c1842146d
SHA256	648d8a9bb60f8d6593a045cd8adf9c6c4b46f2e4b64fcb989f864bcb5ace30ee
File size	17.735.680 bytes

All details

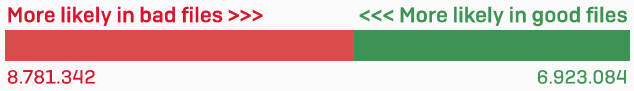
Machine learning

LIKELY CLEAN Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples.
The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own, but in combination, they provide a critical insight. This model identifies many different characteristics of your file and compares the occurence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

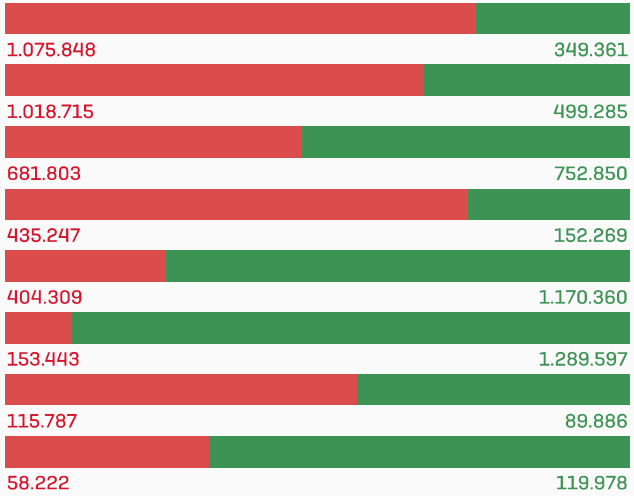
Feature analysis SUSPICIOUS

- Identifies specific features of the file
- Randomly selects ten million known bad files from our data warehouse.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The final verdict may also take into account more complex combinations of features.



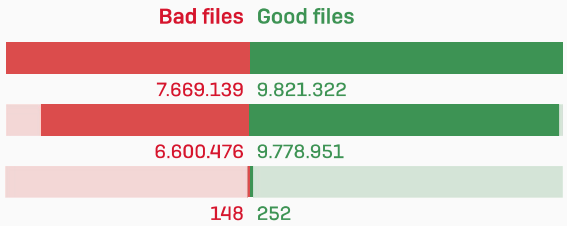
File feature

Stack Canary: "disabled"



Feature combinations SUSPICIOUS

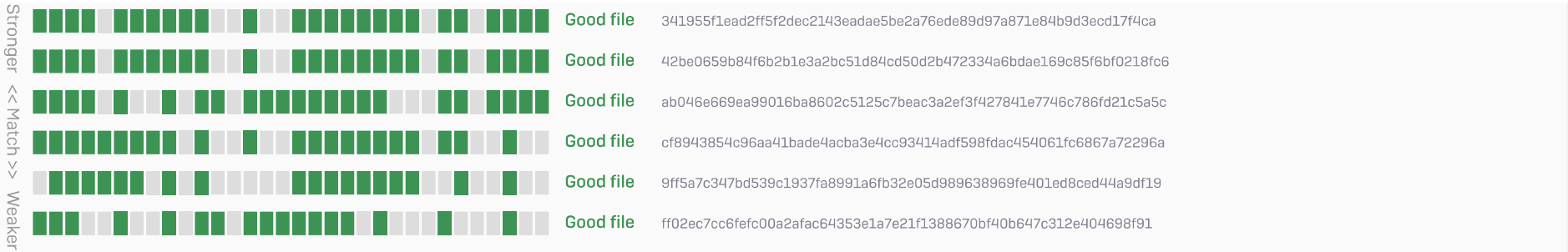
- Counts the number of good and bad sample files that have one feature in common with your file.
- Adds an additional feature and counts the sample files that have both features.
- Continue adding features and counting sample files that combine all features.
- Combinations of features can provide a more precise indication than individual features.



Malware probability	File feature
44%	Feature NOT Observed: Packer: "Unusual section name found: UPX1"
40%	**Add:** Feature NOT Observed: Packer: "Section .text is both writable and executable."
37%	**Add:** Feature Observed: Contains references to internet browsers: "iexplore.exe"

Structure analysis LIKELY CLEAN

- Identifies 32 distinctive structural genes in the file.
- Scans Sophos database for files with these genes.
- Ascertains the likelihood of the genes' presence in good versus malicious files.
- The chart below shows **6** of the files in the sample set with the strongest genetic match.



Reputation

SUSPICIOUS

We use live cloud lookups to ascertain file reputation based on how widely the file has been seen. This enables us to block emerging, fast-moving threats while preventing false positives.

Verdict comment Unknown reputation

Sandstorm detonation

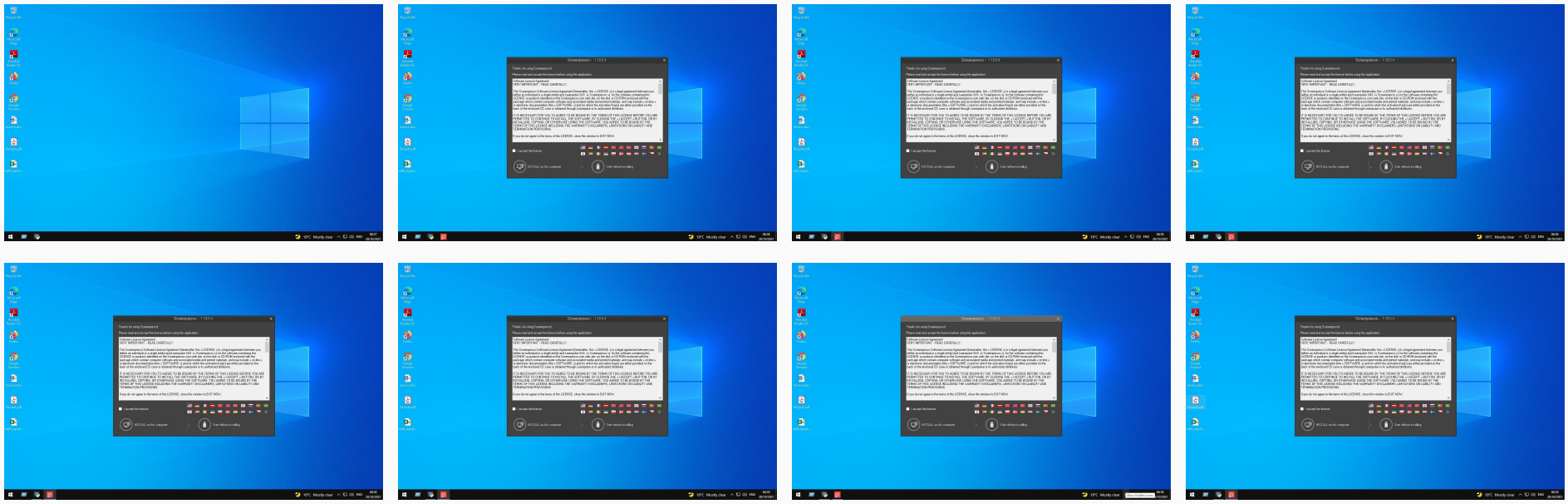
NOT DETECTED

Submitted at	2021-10-28 08:57:01
Detonated at	2021-10-28 08:57:31
Analysis duration	201 seconds
Sandbox version	4.3.3.573
File type	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
File executed as	exe
SHA1	81228f11a7824dcecb708153b350959d826ccc6d
SHA256	e9c03b4412218ccf3fec69d664331f66107bb2752608c6d8b7460cb41b9b190f

Malicious activity

Memory	Changes the permissions of a memory region used by system libraries
	Creates a memory region with executable permission
Suspicious	Reads data from the local Windows system configuration
	Performs injection by UserQueueApc into another process Thread

Screenshots: 8



File activity: 4

#	Action	File path	Process
1	Written	%temp%\screenpresso.log	%input_sample% (pid=8560)
2	Written	%appdata%\learnpulse\screenpresso\fum.bin	%input_sample% (pid=8560)
3	Written	%userprofile%\appdata\locallow\microsoft\cryptneturlcache\metadata\e0f5c59f9fa661f6f4c50b87fef3a15a	%input_sample% (pid=8560)
4	Written	%userprofile%\appdata\locallow\microsoft\cryptneturlcache\content\e0f5c59f9fa661f6f4c50b87fef3a15a	%input_sample% (pid=8560)

Network activity: 15

DNS requests: 4

#	Domain	IP address
1	apps.identrust.com	95.101.89.66
2	apps.identrust.com	95.101.89.35
3	www.google-analytics.com	142.250.185.238
4	stats.screenpresso.com	213.186.33.17

Connections: 10

#	Protocol	IP address	Port	Hostname	Process
1	tcp	104.92.93.19	80		
2	tcp	131.253.33.203	443	api.msn.com	
3	tcp	142.250.185.238	443	www.google-analytics.com	%input_sample% (pid=8560)
4	tcp	20.54.110.249	443	displaycatalog.mp.microsoft.com	
5	tcp	213.186.33.17	443	stats.screenpresso.com	%input_sample% (pid=8560)
6	tcp	40.90.65.18	443		
7	tcp	52.168.112.67	443		
8	tcp	52.222.250.30	80		
9	tcp	93.184.220.29	80		
10	tcp	95.101.89.66	80	apps.identrust.com	%input_sample% (pid=8560)

HTTP flows: 1

#	URI	Method	IP address	Origin	Response status	Response MIME type	Bytes	SHA1
1	hxxp://apps.identrust.com/roots/dstrootcax3.p7c	GET		User agent: Microsoft-CryptoAPI/10.0	200	application/pkcs7-mime	893	b06f409fa14bab33cbaf4a37811b8740b624d9e5

Registry activity: 1

Keys added: 1

#	Key	Process	When	Value	Data
1	HKLM\system\controlset001\control\securityproviders\schannel	%input_sample% (pid=8560)	2021-10-28 08:58:02		

File analysis

File name	Screenpressobeta.zip
File type	application/zip
SHA1	a8a7f4868bca823cd6b759eb5be0ae6c18421146d
SHA256	648d8a9bb60f8d6593a045cd8adf9c6c4b46f2e4b64fcb989f864bcb5ace30ee
File size	17.735.680 bytes
Image size	17.735.680 bytes
Image base	4194304
File time stamp	2021-10-28 08:48:16
Machine type	I386
Subsystem	WINDOWS_GUI
Languages	RESOURCE_LANGS.NEUTRAL
Sections	3
Debug information	N/A
PE flags	LARGE_ADDRESS_AWARE, EXECUTABLE_IMAGE
Original file name	Screenpresso.exe
Internal name	Screenpresso.exe
File description	Screenpresso
File version	1.10.5.4
Private build	
Special build	
Comments	Screen capture tool
Product name	Screenpresso
Product version	1.10.5.4
Company name	Learnpulse
Copyright	Copyright © Learnpulse 2021
Trademarks	

Signature and certificates: Not signed

Signing date Not specified

Signature trust chain: 3

#	Common name	Issuer	Validity	Usage	Algorithm	Depth	Details
1	Learnpulse SAS	DigiCert SHA2 Assured ID Code Signing CA	From: 2021-05-12 14:00:00 To: 2024-05-14 13:59:00	Code Signing	sha256RSA	0	Serial: 03 49 86 B9 7D BF 2B AC 7F 96 A1 D7 D9 92 56 A5 Thumbprint: CA0C441626446F9CF70F758E810656275E07F8A7

2	DigiCert SHA2 Assured ID Code Signing CA	DigiCert Assured ID Root CA	From: 2013-10-22 14:00:00 To: 2028-10-22 14:00:00	Code Signing	sha256RSA	1	Serial: 04 09 18 1B 5F D5 BB 66 75 53 43 B5 6F 95 50 08 Thumbprint: 92C1588E85AF2201CE7915E8538B492F605B80C6
3	DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	From: 2006-11-10 13:00:00 To: 2031-11-10 13:00:00	All	sha1RSA	2	Serial: 0C E7 E0 E5 17 D8 46 FE 8F E5 60 FC 1B F0 30 39 Thumbprint: 0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43

File sections: 3

#	Section name	Physical address	Raw data (bytes)	Virtual address	Virtual size (bytes)	Entropy	Characteristics
1	.text	512	17562112	8192	17562064	7.076158379753564	CNT_CODE, MEM_EXECUTE, MEM_READ
2	.rsrc	17562624	151.552	17571840	151.064	3.676248805659227	CNT_INITIALIZED_DATA, MEM_READ
3	.reloc	17714176	512	17727488	12	2.125814583693911	CNT_INITIALIZED_DATA, MEM_DISCARDABLE, MEM_READ

Resources: 11

#	Resource type	Bytes	Code page	Language
1	RT_ICON	7.267	0	0x0
2	RT_ICON	67.624	0	0x0
3	RT_ICON	38.056	0	0x0
4	RT_ICON	16.936	0	0x0
5	RT_ICON	9.640	0	0x0
6	RT_ICON	4.264	0	0x0
7	RT_ICON	2.440	0	0x0
8	RT_ICON	1.128	0	0x0
9	RT_GROUP_ICON	118	0	0x0
10	RT_VERSION	914	0	0x0
11	RT_MANIFEST	2.031	0	0x0

Imports: 1

#	DLL name	APIs	By ordinal?
1	mscoree.dll	_CorExeMain	No