Prezi Next

Date: September 9th, 2018.

Description

This software is used to create presentations. However, it brings also vulnerabilities such as: (i) the ability to invocate tools capable to modify the registry and (ii) mechanisms of persistence through an extensive use of functions in the kernel32.dll. Additional red flags were also identified as associated with those vulnerabilities.

Antivirus tools did not detect suspicious contents in the software and in one instance a suspicious file was detected. The software has a compressed file inside another compressed file, in which it shows data after the end of the payload data that prevented to unpack the software.

The software has an extensive internet traffic through subdomains of prezi.com and the Amazon CloudFront.net which could increase the security risks related to remote access and process injection.

Table of Contents

File Identification.. 2

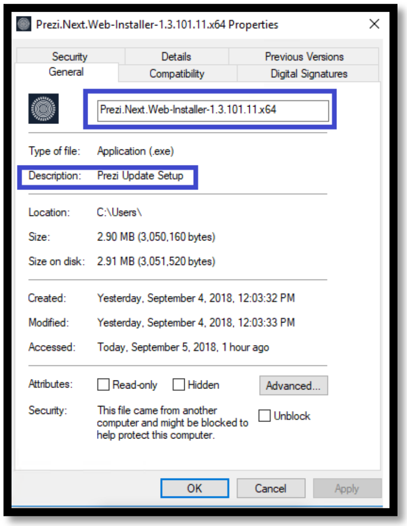
Red Flags.. 3

Detection.. 8

Attacks.. 12

File Identification

This is the software



Prezi.Next.Web-Installer-1.3.101.11.x64

Type of file: Application (.exe)

Description: Prezi Update Setup

Location: C:\Users\

Size: 2.90 MB (3,050,160 bytes)

Size on disk: 2.91 MB (3,051,520 bytes)

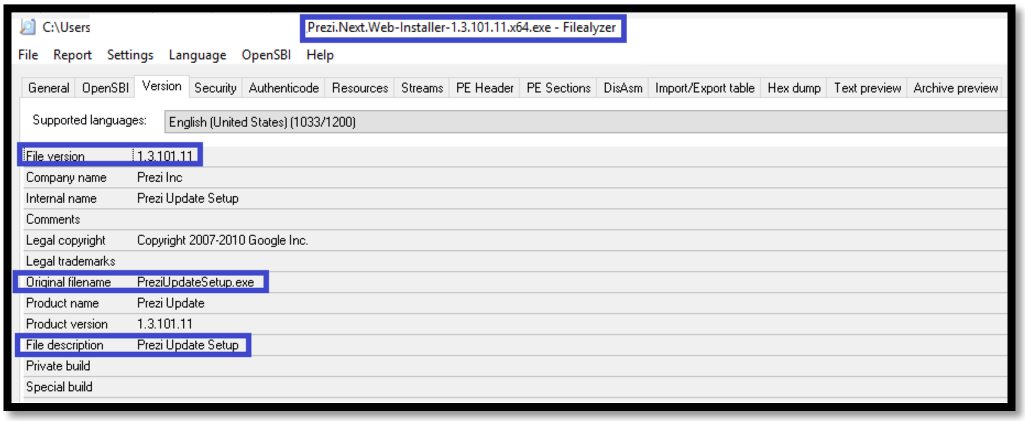
Created: Yesterday, September 4, 2018, 12:03:32 PM

Modified: Yesterday, September 4, 2018, 12:03:33 PM

Accessed: Today, September 5, 2018, 1 hour ago

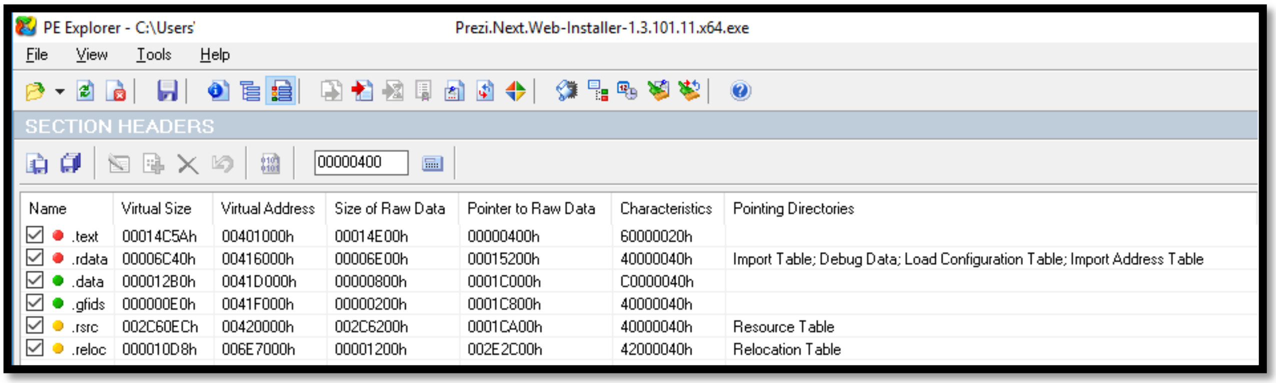
Attributes: □ Read-only □ Hidden

Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock



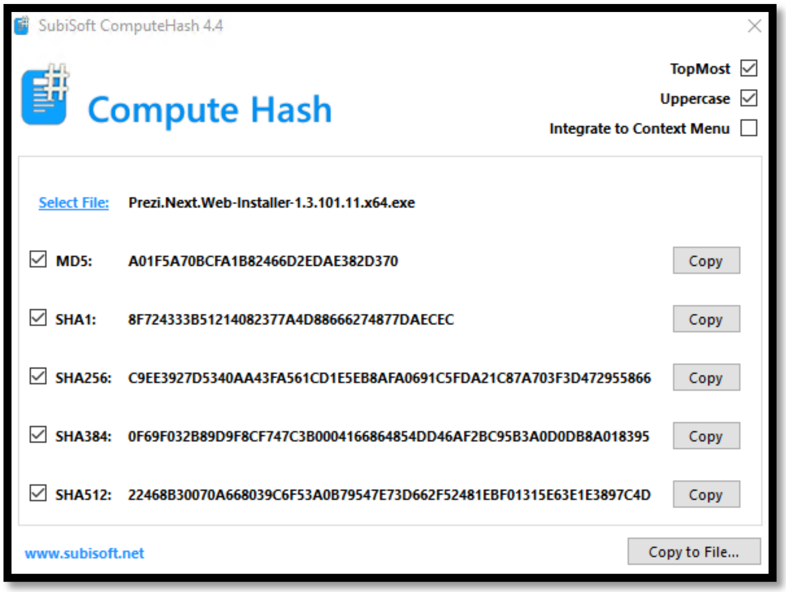
Supported languages: English (United States) (1033/1200)

File version	1.3.101.11
Company name	Prezi Inc
Internal name	Prezi Update Setup
Comments	
Legal copyright	Copyright 2007-2010 Google Inc.
Legal trademarks	
Original filename	PreziUpdateSetup.exe
Product name	Prezi Update
Product version	1.3.101.11
File description	Prezi Update Setup
Private build	
Special build	



Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
☑ 🔴 .text	00014C5Ah	00401000h	00014E00h	00000400h	60000020h	
☑ 🔴 .rdata	00006C40h	00416000h	00006E00h	00015200h	40000040h	Import Table; Debug Data; Load Configuration Table; Import Address Table
☑ 🟢 .data	000012B0h	0041D000h	00000800h	0001C000h	C0000040h	
☑ 🟢 .gfids	000000E0h	0041F000h	00000200h	0001C800h	40000040h	
☑ 🟡 .rsrc	002C60ECh	00420000h	002C6200h	0001CA00h	40000040h	Resource Table
☑ 🟡 .reloc	000010D8h	006E7000h	00001200h	002E2C00h	42000040h	Relocation Table

Calculate the hash:



Select File: Prezi.Next.Web-Installer-1.3.101.11.x64.exe

☑ MD5: A01F5A70BCFA1B82466D2EDAE382D370

☑ SHA1: 8F724333B51214082377A4D88666274877DAECEC

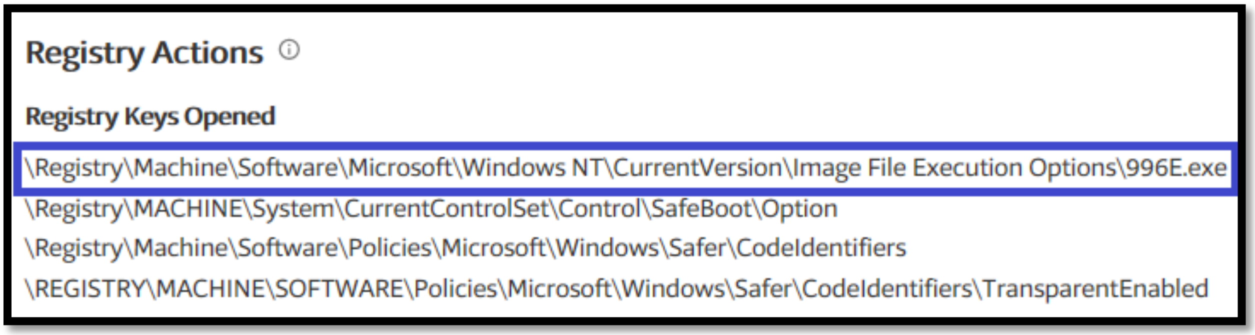
☑ SHA256: C9EE3927D5340AA43FA561CD1E5EB8AFA0691C5FDA21C87A703F3D472955866

☑ SHA384: 0F69F032B89D9F8CF747C3B0004166864854DD46AF2BC95B3A0D0DB8A018395

☑ SHA512: 22468B30070A668039C6F53A0B79547E73D662F52481EBF01315E63E1E3897C4D

Red Flags

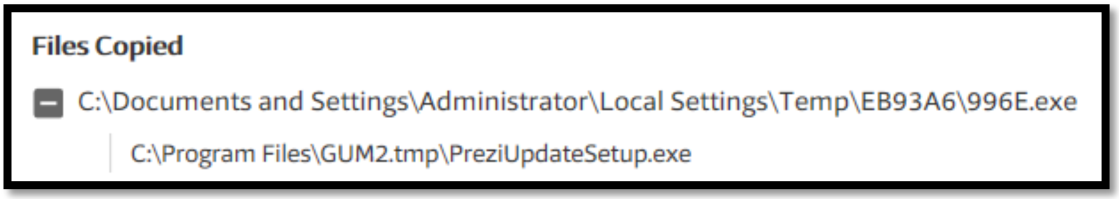
1. The software has a possible suspicious[1] file located in the registry:



Registry Actions

Registry Keys Opened

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe
\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers
\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled

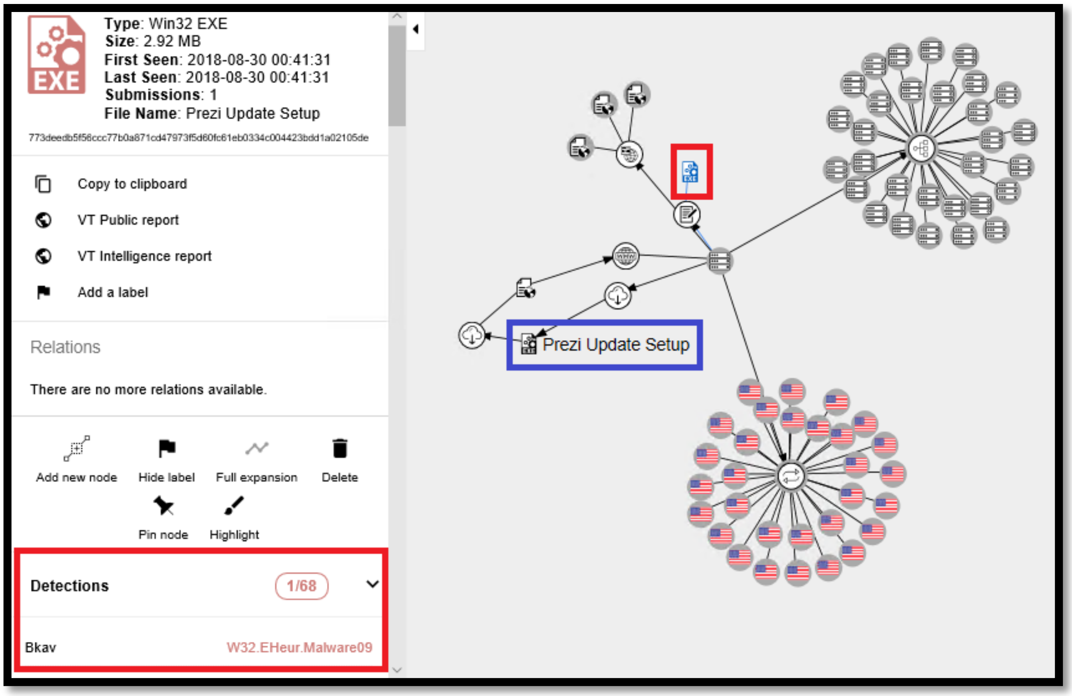


Files Copied

C:\Documents and Settings\Administrator\Local Settings\Temp\EB93A6\996E.exe
C:\Program Files\GUM2.tmp\PreziUpdateSetup.exe

[1] http://www.exefilesupport.com/easy-guide-to-remove-996e-exe-from-pc

2. A malicious malware could open other connections:



Type: Win32 EXE
Size: 2.92 MB
First Seen: 2018-08-30 00:41:31
Last Seen: 2018-08-30 00:41:31
Submissions: 1
File Name: Prezi Update Setup

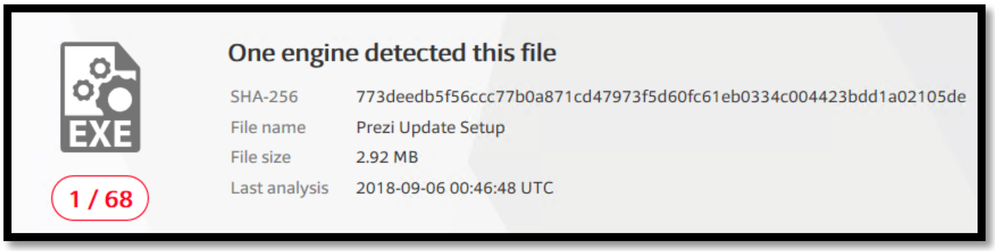
773deedb5f56ccc77b0a871cd47973f5d60fc61eb0334c004423bdd1a02105de

Relations

There are no more relations available.

Detections	1/68
Bkav	W32.EHeur.Malware09

The multiple connections are related to subdomains from prezi.com and connections with the Amazon CloudFront (content delivery network). The hash of the executable file is:

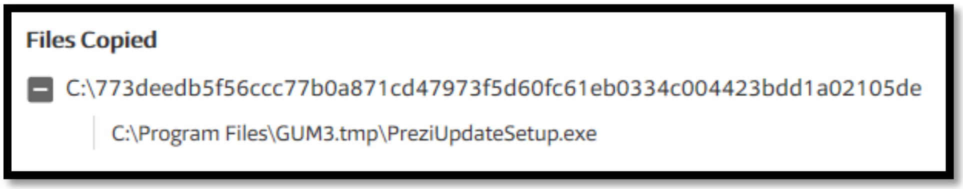


One engine detected this file

SHA-256	773deedb5f56ccc77b0a871cd47973f5d60fc61eb0334c004423bdd1a02105de
File name	Prezi Update Setup
File size	2.92 MB
Last analysis	2018-09-06 00:46:48 UTC

1 / 68

And it can be introduced by itself into the software folder:



Files Copied

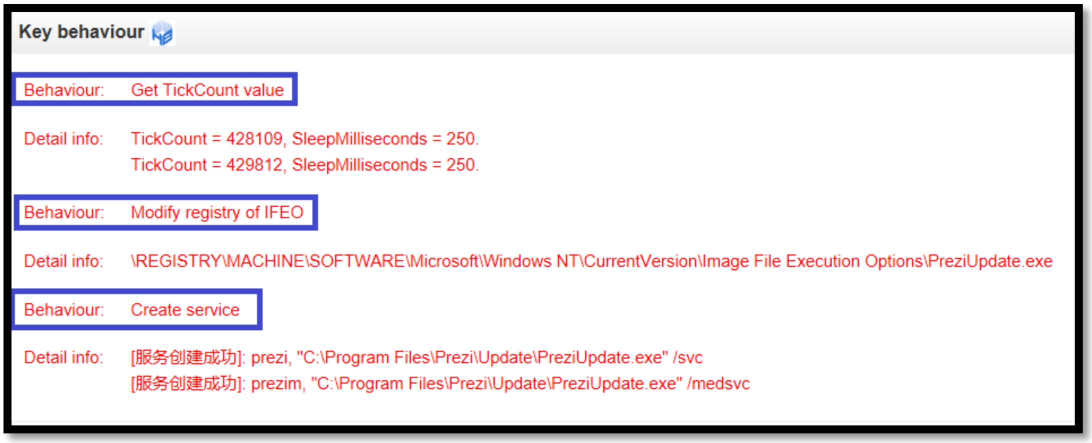
C:\773deedb5f56ccc77b0a871cd47973f5d60fc61eb0334c004423bdd1a02105de

C:\Program Files\GUM3.tmp\PreziUpdateSetup.exe

By using the hash, the software could makes the access to the functions less time consuming, is some way similar to a hash injection attack[2].

[2] https://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283

3. The software could modify the Image File Execution Options (IFEO). Which could represent one of the means to create persistence and/or an entry door to inject a malicious code[3].



Key behaviour

Behaviour: Get TickCount value

Detail info: TickCount = 428109, SleepMilliseconds = 250.
TickCount = 429812, SleepMilliseconds = 250.

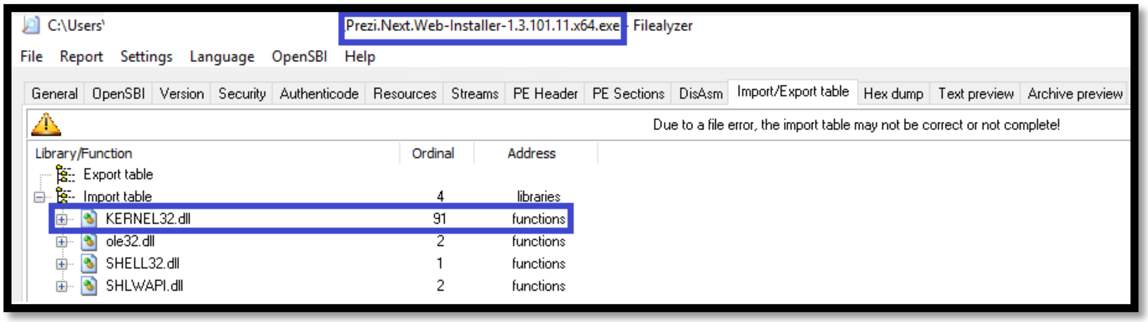
Behaviour: Modify registry of IFEO

Detail info: \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PreziUpdate.exe

Behaviour: Create service

Detail info: [服务创建成功]: prezi, "C:\Program Files\Prezi\Update\PreziUpdate.exe" /svc
[服务创建成功]: prezim, "C:\Program Files\Prezi\Update\PreziUpdate.exe" /medsvc

4. The software has a long list of functions mainly in the Kernel32 that could create a broad access to the user systems:

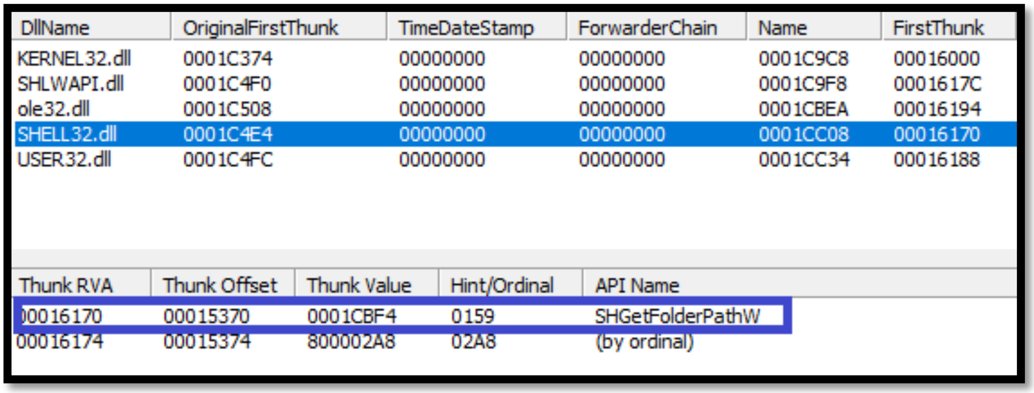


C:\Users\ Prezi.Next.Web-Installer-1.3.101.11.x64.exe - Filealyzer

Due to a file error, the import table may not be correct or not complete!

Library/Function	Ordinal	Address
Export table		
Import table	4	libraries
KERNEL32.dll	91	functions
ole32.dll	2	functions
SHELL32.dll	1	functions
SHLWAPI.dll	2	functions

The SHELL32.dll shows a deprecated function such as SHGetFolderPathW[4]:



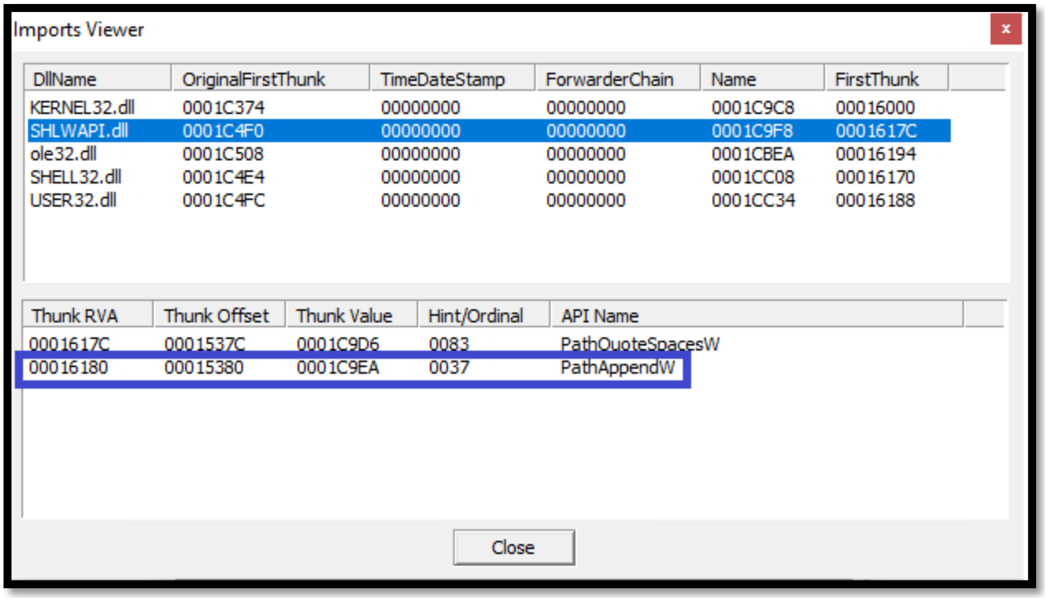
DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0001C374	00000000	00000000	0001C9C8	00016000
SHLWAPI.dll	0001C4F0	00000000	00000000	0001C9F8	0001617C
ole32.dll	0001C508	00000000	00000000	0001CBEA	00016194
SHELL32.dll	0001C4E4	00000000	00000000	0001CC08	00016170
USER32.dll	0001C4FC	00000000	00000000	0001CC34	00016188

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00016170	00015370	0001CBF4	0159	SHGetFolderPathW
00016174	00015374	800002A8	02A8	(by ordinal)

[3] https://attack.mitre.org/wiki/Technique/T1183

[4] https://docs.microsoft.com/en-us/windows/desktop/api/shlobj_core/nf-shlobj_core-shgetfolderpathw

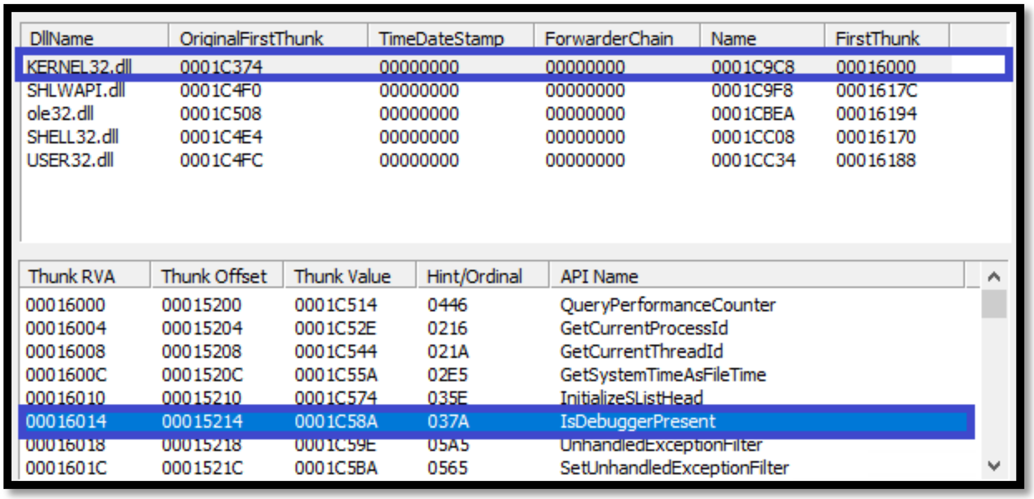
On the SHLWAPI.dll, the PathAppendW[5] could lead to a buffer overrun:



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0001C374	00000000	00000000	0001C9C8	00016000
SHLWAPI.dll	0001C4F0	00000000	00000000	0001C9F8	0001617C
ole32.dll	0001C508	00000000	00000000	0001CBEA	00016194
SHELL32.dll	0001C4E4	00000000	00000000	0001CC08	00016170
USER32.dll	0001C4FC	00000000	00000000	0001CC34	00016188

Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
0001617C	0001537C	0001C9D6	0083	PathQuoteSpacesW
00016180	00015380	0001C9EA	0037	PathAppendW

A function (IsDebuggerPresent[6]) that could modify the application behavior if debugged is located on kernel32 and could create security risks[7]:



DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
KERNEL32.dll	0001C374	00000000	00000000	0001C9C8	00016000
SHLWAPI.dll	0001C4F0	00000000	00000000	0001C9F8	0001617C
ole32.dll	0001C508	00000000	00000000	0001CBEA	00016194
SHELL32.dll	0001C4E4	00000000	00000000	0001CC08	00016170
USER32.dll	0001C4FC	00000000	00000000	0001CC34	00016188

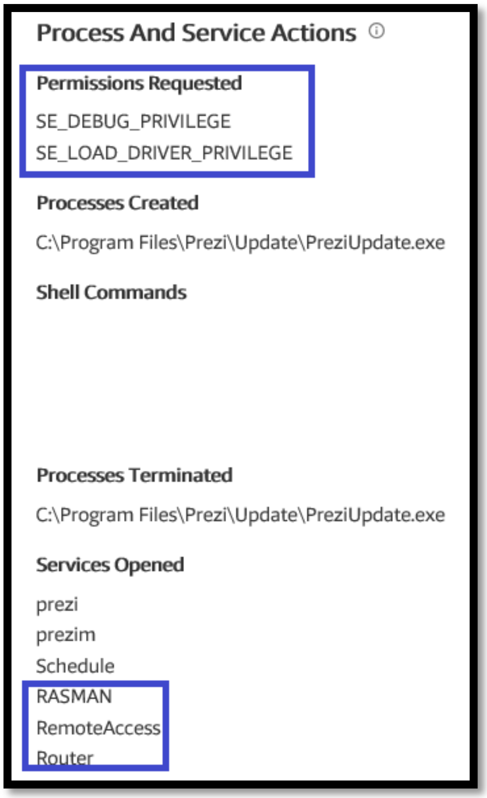
Thunk RVA	Thunk Offset	Thunk Value	Hint/Ordinal	API Name
00016000	00015200	0001C514	0446	QueryPerformanceCounter
00016004	00015204	0001C52E	0216	GetCurrentProcessId
00016008	00015208	0001C544	021A	GetCurrentThreadId
0001600C	0001520C	0001C55A	02E5	GetSystemTimeAsFileTime
00016010	00015210	0001C574	035E	InitializeSListHead
00016014	00015214	0001C58A	037A	IsDebuggerPresent
00016018	00015218	0001C59E	05A5	UnhandledExceptionFilter
0001601C	0001521C	0001C5BA	0565	SetUnhandledExceptionFilter

[5] https://docs.microsoft.com/en-us/windows/desktop/api/shlwapi/nf-shlwapi-pathappendw

[6] https://msdn.microsoft.com/en-us/library/windows/desktop/ms680345(v=vs.85).aspx

[7] https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/security-during-kernel-mode-debugging

5. The software require permissions that increase security risk such as the debug privilege[8], which provides complete access to sensitive and critical operating system components:



Process And Service Actions

Permissions Requested

SE_DEBUG_PRIVILEGE
SE_LOAD_DRIVER_PRIVILEGE

Processes Created

C:\Program Files\Prezi\Update\PreziUpdate.exe

Shell Commands

Processes Terminated

C:\Program Files\Prezi\Update\PreziUpdate.exe

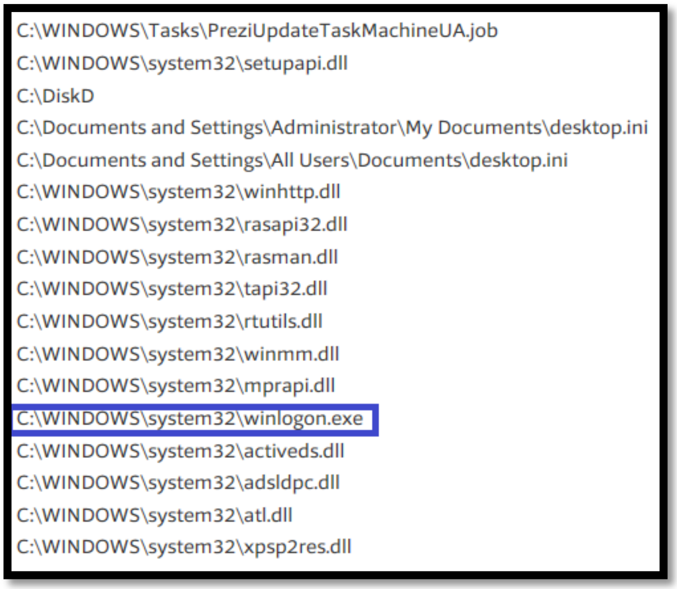
Services Opened

prezi
prezim
Schedule
RASMAN
RemoteAccess
Router

And others services like rasman[9], and remoteaccess[10], router that could be used as backdoors in the software.

[8] https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/debug-privilege
[9] https://www.processlibrary.com/en/directory/files/rasman/20943/
[10] https://docs.microsoft.com/en-us/windows/desktop/rras/remote-access-start-page

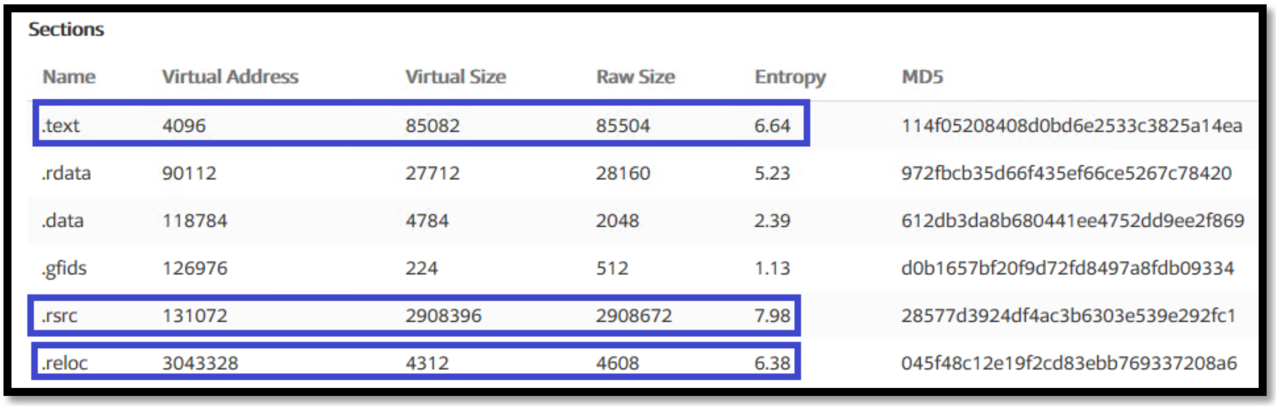
6. Under these circumstances, users should consider the risk of having winlogon.exe[11] as part of the software, since it could record keyboard and mouse inputs, manipulate other programs and monitor applications.



```
C:\WINDOWS\Tasks\PreziUpdateTaskMachineUA.job
C:\WINDOWS\system32\setupapi.dll
C:\DiskD
C:\Documents and Settings\Administrator\My Documents\desktop.ini
C:\Documents and Settings\All Users\Documents\desktop.ini
C:\WINDOWS\system32\winhttp.dll
C:\WINDOWS\system32\rasapi32.dll
C:\WINDOWS\system32\rasman.dll
C:\WINDOWS\system32\tapi32.dll
C:\WINDOWS\system32\rtutils.dll
C:\WINDOWS\system32\winmm.dll
C:\WINDOWS\system32\mprapi.dll
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\activeds.dll
C:\WINDOWS\system32\adsldpc.dll
C:\WINDOWS\system32\atl.dll
C:\WINDOWS\system32\xpsp2res.dll
```

Detection

The file shows some compressed sections that could create barriers for antivirus detection:

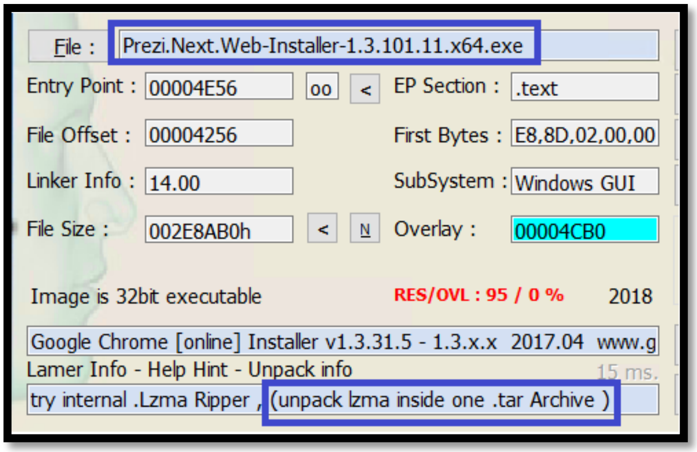


Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	85082	85504	6.64	114f05208408d0bd6e2533c3825a14ea
.rdata	90112	27712	28160	5.23	972fbcb35d66f435ef66ce5267c78420
.data	118784	4784	2048	2.39	612db3da8b680441ee4752dd9ee2f869
.gfids	126976	224	512	1.13	d0b1657bf20f9d72fd8497a8fdb09334
.rsrc	131072	2908396	2908672	7.98	28577d3924df4ac3b6303e539e292fc1
.reloc	3043328	4312	4608	6.38	045f48c12e19f2cd83ebb769337208a6

[11] https://www.file.net/process/winlogon.exe.html

Then, it is necessary to unpack the file:



File : Prezi.Next.Web-Installer-1.3.101.11.x64.exe

Entry Point : 00004E56 oo < EP Section : .text

File Offset : 00004256 First Bytes : E8,8D,02,00,00

Linker Info : 14.00 SubSystem : Windows GUI

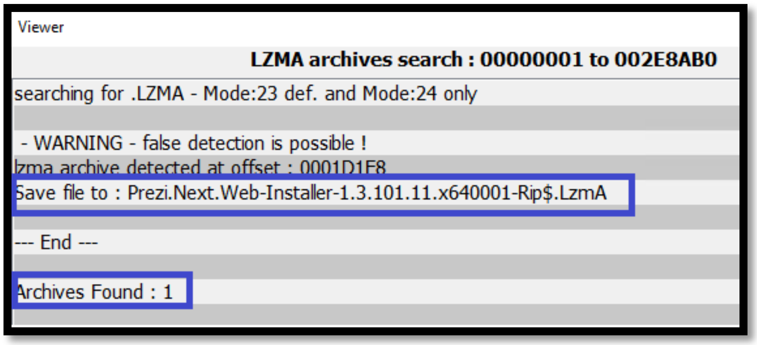
File Size : 002E8AB0h < N Overlay : 00004CB0

Image is 32bit executable RES/OVL : 95 / 0 % 2018

Google Chrome [online] Installer v1.3.31.5 - 1.3.x.x 2017.04 www.g

Lamer Info - Help Hint - Unpack info 15 ms.

try internal .Lzma Ripper , (unpack lzma inside one .tar Archive)



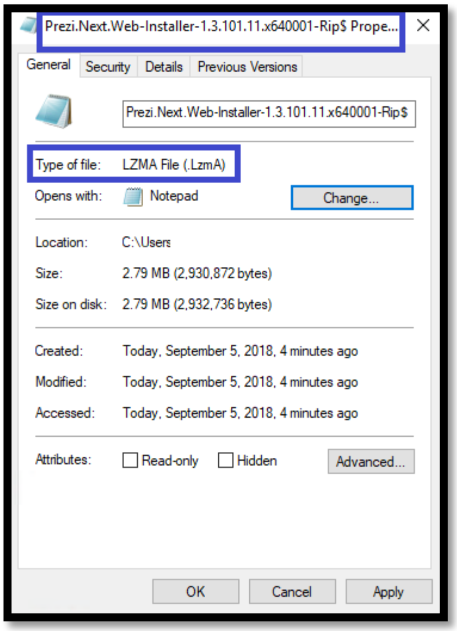
```
Viewer
                    LZMA archives search : 00000001 to 002E8AB0
searching for .LZMA - Mode:23 def. and Mode:24 only

 - WARNING - false detection is possible !
lzma archive detected at offset : 0001D1F8
Save file to : Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$.LzmA

--- End ---

Archives Found : 1
```

And identify the file (first compression):



Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$ Prope...

Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$

Type of file: LZMA File (.LzmA)

Opens with: Notepad

Location: C:\Users

Size: 2.79 MB (2,930,872 bytes)

Size on disk: 2.79 MB (2,932,736 bytes)

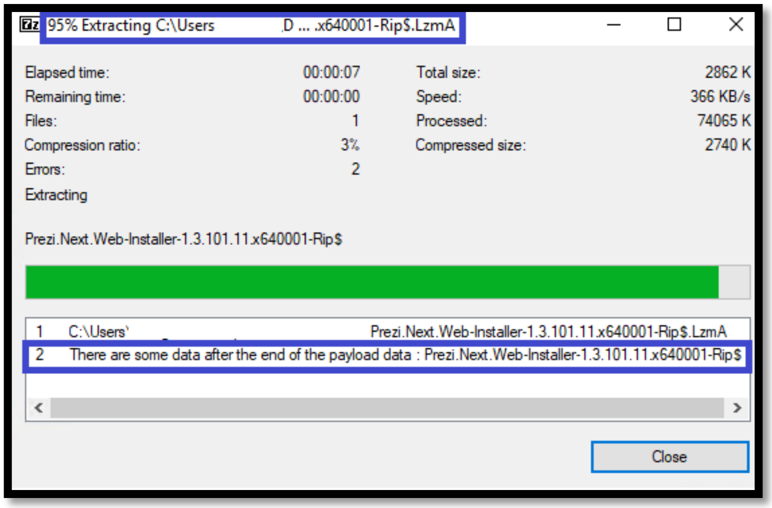
Created: Today, September 5, 2018, 4 minutes ago

Modified: Today, September 5, 2018, 4 minutes ago

Accessed: Today, September 5, 2018, 4 minutes ago

Attributes: □ Read-only □ Hidden

However the extraction (second compression) is not possible because there are data after the end of the payload data:



95% Extracting C:\Users D ... x640001-Rip$.LzmA

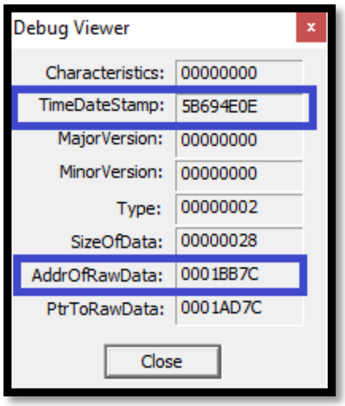
Elapsed time:	00:00:07	Total size:	2862 K
Remaining time:	00:00:00	Speed:	366 KB/s
Files:	1	Processed:	74065 K
Compression ratio:	3%	Compressed size:	2740 K
Errors:	2		

Extracting

Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$

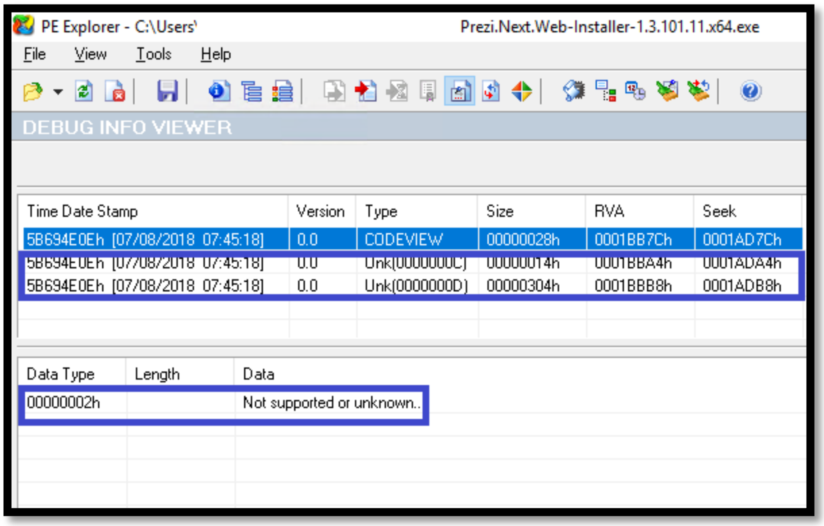
```
1   C:\Users\                    Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$.LzmA
2   There are some data after the end of the payload data : Prezi.Next.Web-Installer-1.3.101.11.x640001-Rip$
```

Additional data was identified using the debug info:



Debug Viewer

Characteristics:	00000000
TimeDateStamp:	5B694E0E
MajorVersion:	00000000
MinorVersion:	00000000
Type:	00000002
SizeOfData:	00000028
AddrOfRawData:	0001BB7C
PtrToRawData:	0001AD7C

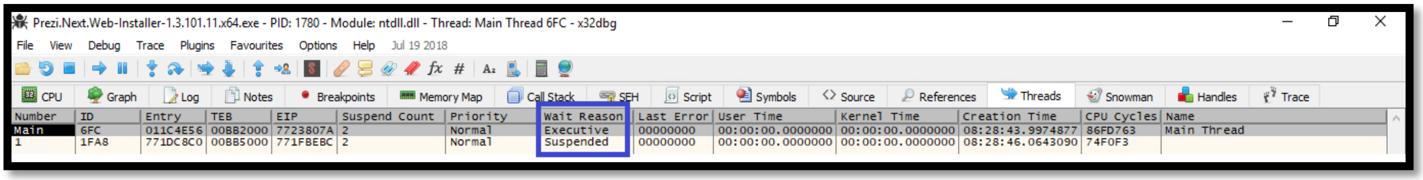


PE Explorer - C:\Users\ Prezi.Next.Web-Installer-1.3.101.11.x64.exe

Time Date Stamp	Version	Type	Size	RVA	Seek
5B694E0Eh [07/08/2018 07:45:18]	0.0	CODEVIEW	00000028h	0001BB7Ch	0001AD7Ch
5B694E0Eh [07/08/2018 07:45:18]	0.0	Unk(0000000C)	00000014h	0001BBA4h	0001ADA4h
5B694E0Eh [07/08/2018 07:45:18]	0.0	Unk(0000000D)	00000304h	0001BBB8h	0001ADB8h

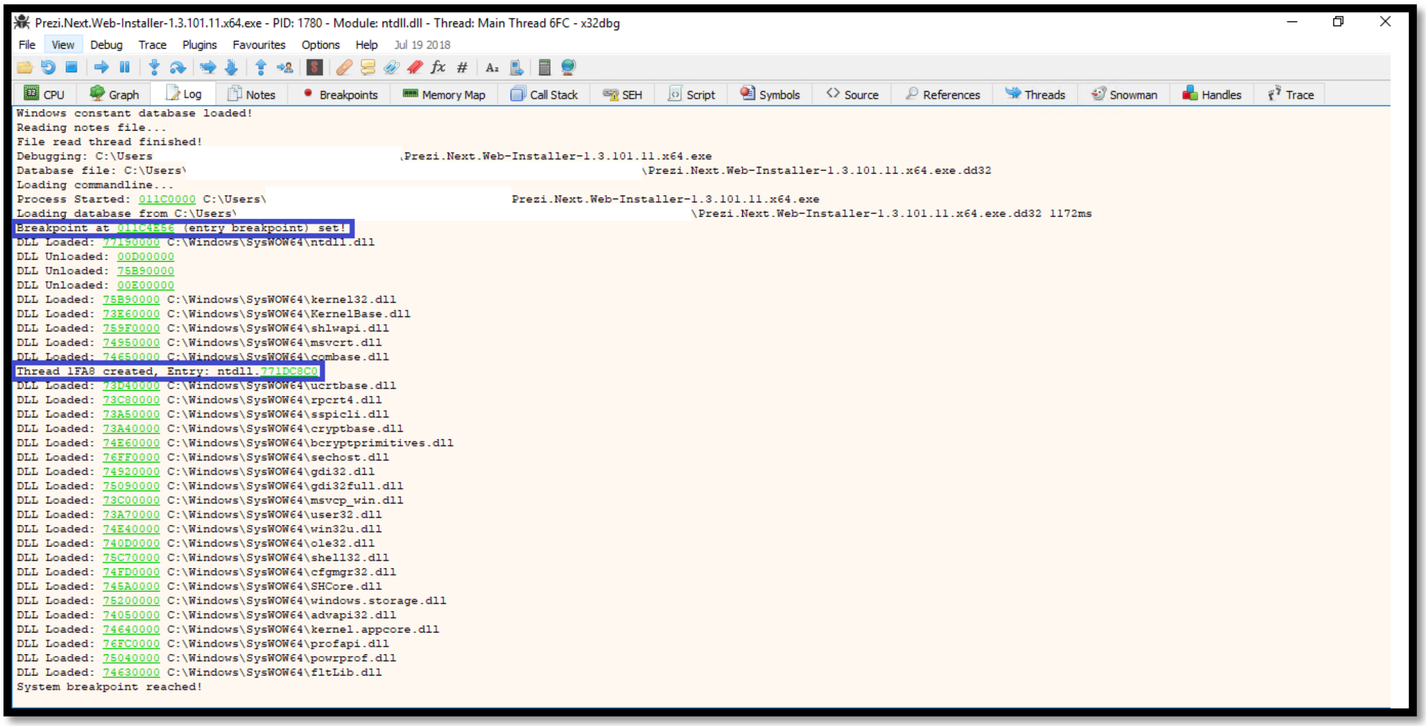
Data Type	Length	Data
00000002h		Not supported or unknown..

A possible explanation is that these data could be waiting a specific process:


Prezi.Next.Web-Installer-1.3.101.11.x64.exe - PID: 1780 - Module: ntdll.dll - Thread: Main Thread 6FC - x32dbg
File View Debug Trace Plugins Favourites Options Help Jul 19 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

Number	ID	Entry	TEB	EIP	Suspend Count	Priority	Wait Reason	Last Error	User Time	Kernel Time	Creation Time	CPU Cycles	Name
Main	6FC	011C4E56	00BB2000	7723807A	2	Normal	Executive	00000000	00:00:00.0000000	00:00:00.0000000	08:28:43.9974877	86FD763	Main Thread
1	1FA8	771DC8C0	00BB5000	771FBEBC	2	Normal	Suspended	00000000	00:00:00.0000000	00:00:00.0000000	08:28:46.0643090	74F0F3	

Which is confirmed, by examining the logs:


Prezi.Next.Web-Installer-1.3.101.11.x64.exe - PID: 1780 - Module: ntdll.dll - Thread: Main Thread 6FC - x32dbg
File View Debug Trace Plugins Favourites Options Help Jul 19 2018
CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Snowman Handles Trace

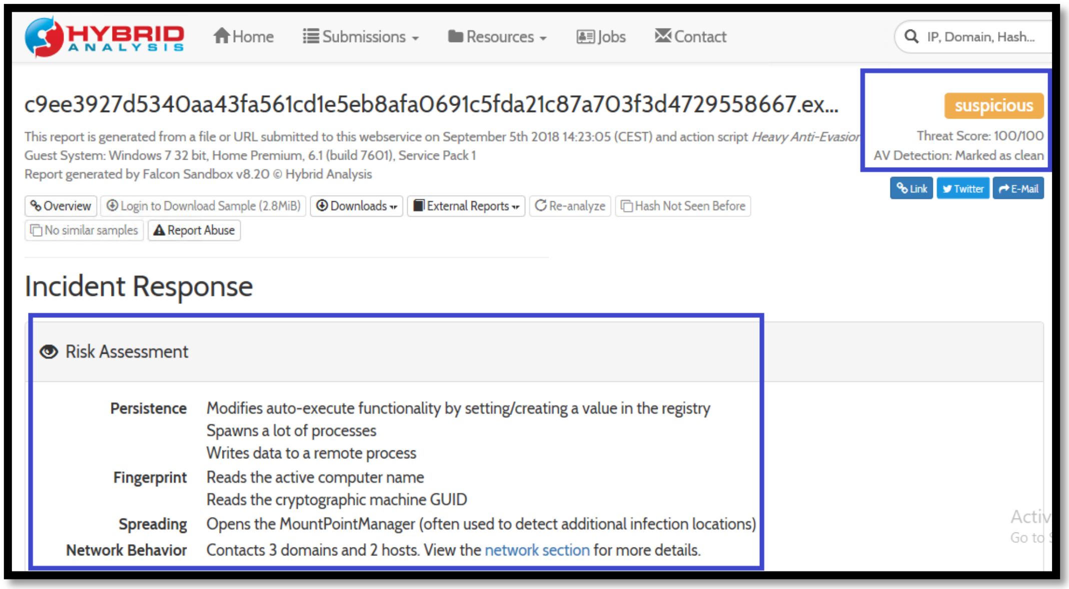
```
Windows constant database loaded!
Reading notes file...
File read thread finished!
Debugging: C:\Users [redacted] .Prezi.Next.Web-Installer-1.3.101.11.x64.exe
Database file: C:\Users\ [redacted] \Prezi.Next.Web-Installer-1.3.101.11.x64.exe.dd32
Loading commandline...
Process Started: 011C0000 C:\Users\ [redacted] Prezi.Next.Web-Installer-1.3.101.11.x64.exe
Loading database from C:\Users\ [redacted] \Prezi.Next.Web-Installer-1.3.101.11.x64.exe.dd32 1172ms
Breakpoint at 011C4E56 (entry breakpoint) set!
DLL Loaded: 77190000 C:\Windows\SysWOW64\ntdll.dll
DLL Unloaded: 00D00000
DLL Unloaded: 75B90000
DLL Unloaded: 00E00000
DLL Loaded: 75B90000 C:\Windows\SysWOW64\kernel32.dll
DLL Loaded: 73E60000 C:\Windows\SysWOW64\KernelBase.dll
DLL Loaded: 759F0000 C:\Windows\SysWOW64\shlwapi.dll
DLL Loaded: 74950000 C:\Windows\SysWOW64\msvcrt.dll
DLL Loaded: 74650000 C:\Windows\SysWOW64\combase.dll
Thread 1FA8 created, Entry: ntdll.771DC8C0
DLL Loaded: 73D40000 C:\Windows\SysWOW64\ucrtbase.dll
DLL Loaded: 73C80000 C:\Windows\SysWOW64\rpcrt4.dll
DLL Loaded: 73A50000 C:\Windows\SysWOW64\sspicli.dll
DLL Loaded: 73A40000 C:\Windows\SysWOW64\cryptbase.dll
DLL Loaded: 74E60000 C:\Windows\SysWOW64\bcryptprimitives.dll
DLL Loaded: 76FF0000 C:\Windows\SysWOW64\sechost.dll
DLL Loaded: 74920000 C:\Windows\SysWOW64\gdi32.dll
DLL Loaded: 75090000 C:\Windows\SysWOW64\gdi32full.dll
DLL Loaded: 73C00000 C:\Windows\SysWOW64\msvcp_win.dll
DLL Loaded: 73A70000 C:\Windows\SysWOW64\user32.dll
DLL Loaded: 74E40000 C:\Windows\SysWOW64\win32u.dll
DLL Loaded: 740D0000 C:\Windows\SysWOW64\ole32.dll
DLL Loaded: 75C70000 C:\Windows\SysWOW64\shell32.dll
DLL Loaded: 74FD0000 C:\Windows\SysWOW64\cfgmgr32.dll
DLL Loaded: 745A0000 C:\Windows\SysWOW64\SHCore.dll
DLL Loaded: 75200000 C:\Windows\SysWOW64\windows.storage.dll
DLL Loaded: 74050000 C:\Windows\SysWOW64\advapi32.dll
DLL Loaded: 74640000 C:\Windows\SysWOW64\kernel.appcore.dll
DLL Loaded: 76FC0000 C:\Windows\SysWOW64\profapi.dll
DLL Loaded: 75040000 C:\Windows\SysWOW64\powrprof.dll
DLL Loaded: 74630000 C:\Windows\SysWOW64\fltLib.dll
System breakpoint reached!
```

Note that all kernel32 functions were loaded before the second entry, where additional dynamic-link libraries (*dll) files were then loaded into the software. An additional review of those dynamic-link libraries files is recommended.

Attacks

Risk Identification

The software introduces several vulnerabilities through persistence, collection of user information, and network behavior:



c9ee3927d5340aa43fa561cd1e5eb8afa0691c5fda21c87a703f3d4729558667.ex...

suspicious

Threat Score: 100/100
AV Detection: Marked as clean

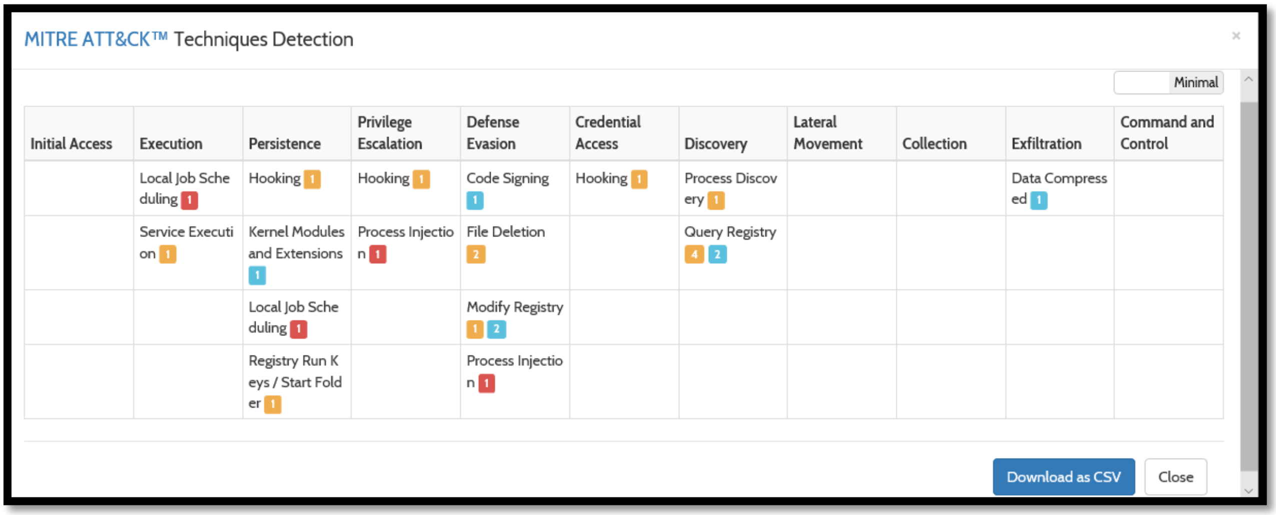
This report is generated from a file or URL submitted to this webservice on September 5th 2018 14:23:05 (CEST) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1
Report generated by Falcon Sandbox v8.20 © Hybrid Analysis

Incident Response

Risk Assessment

Persistence	Modifies auto-execute functionality by setting/creating a value in the registry Spawns a lot of processes Writes data to a remote process
Fingerprint	Reads the active computer name Reads the cryptographic machine GUID
Spreading	Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior	Contacts 3 domains and 2 hosts. View the network section for more details.

Which makes the software vulnerable to several documented attack strategies:



MITRE ATT&CK™ Techniques Detection

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Local Job Scheduling 1	Hooking 1	Hooking 1	Code Signing 1	Hooking 1	Process Discovery 1			Data Compressed 1	
	Service Execution 1	Kernel Modules and Extensions 1	Process Injection 1	File Deletion 2		Query Registry 4 2				
		Local Job Scheduling 1		Modify Registry 1 2						
		Registry Run Keys / Start Folder 1		Process Injection 1						