VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: StickyPassword_rev80778.exe
File Type: PE32 executable (GUI) Intel 80386, for MS Windows
SHA1: aec828e428597071622b556fde69b65c7cc61068
MD5: b3bceb937f6a14a0f04a4e979449459e
First Seen Date: 2016-04-10 03:24:02 UTC
Number of Clients Seen: 2
Last Analysis Date: 2016-04-10 03:24:02 UTC
Human Expert Analysis Result: No human expert analysis verdict given to this sample yet.
Verdict Source: Signature Based Detection

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT	
Signature Based Detection	2016-04-10 03:24:02 UTC	Clean	
Static Analysis Overall Verdict	2016-04-10 03:24:02 UTC	No Threat Found	
Dynamic Analysis Overall Verdict	2016-04-10 03:24:02 UTC	No Threat Found	
File Certificate Validation		Not Applicable	

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT	
Optional Header LoaderFlags field is valued illegal	Clean	
Non-ascii or empty section names detected	Clean	
Illegal size of optional Header	Clean	
Packer detection on signature database	Unknown	
Based on the sections entropy check! file is possibly packed	Clean	
Timestamp value suspicious	Clean	
Header Checksum is zero!	Clean	
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Suspicious	
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean	
Anti-vm present	Clean	
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean	
TLS callback functions array detected	Suspicious	

Anti-debug calls

UnhandledExceptionFilter

Dynamic Analysis

DYNAMIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

SUSPICIOUS BEHAVIORS	
Opens a file in a system directory	
Has no visible windows	

Behavioral Information

LoadLibrary

C:\Users\win7\AppData\Local\Temp\is-J9GPS.tmp\sample.ENU
C:\Users\win7\AppData\Local\Temp\is-J9GPS.tmp\sample.EN
imm32.dll
uxtheme.dll
shell32.dll
C:\Windows\system32\ole32.dll
ADVAPI32.dll
comctl32.dll
UxTheme.dll

LowerChar

ample

ReadRegisteryKey

MS Shell Dlg 2
Disable
DataFilePath
Plane1
Plane2
Plane3
Plane4
Plane5
Plane6
Plane7
Plane8
Plane9
Plane10
Plane11
Plane12
Plane13
Plane14
Plane15
Plane16

CreateFile

C:\sample
C:\Windows\Fonts\staticcache.dat

OpenRegisteryKey

Software\CodeGear\Locales
Software\Borland\Locales
Software\Borland\Delphi\Locales
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
System\CurrentControlSet\Control\Keyboard Layouts\041F0409
System\CurrentControlSet\Control\Keyboard Layouts\04090409
SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink

SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
Tahoma

OpenMutex

Local\MSCTF.Asm.MutexDefault1

QueryFilePath

C:\Users\win7\AppData\Local\Temp\is-J9GPS.tmp\sample.tmp
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\USER32.dll

Precise Detectors Analysis Results

No Detector Result Received

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0x525A5794 [Sun Oct 13 08:19:32 2013 UTC]
Entry Point	0x4113bc (.itext)
File Size	29778600
Machine Type	Intel 386 or later - 32Bit
Legal Copyright	Copyright © 2016 Lamantine Software a.s.
File Version	8.0.7.78
Company Name	Lamantine Software
Comments	This installation was built with Inno Setup.
Product Name	
Product Version	8.0.7.78
File Description	Sticky Password Manager
Translation	0x0000 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	8
Sha256	d38f552d4e1e57ddf5dfbba1c7f798a64596deb0714812558b45a2f4bc125c36

File Paths

FILE PATH ON CLIENT	SEEN COUNT
aec828e428597071622b556fde69b65c7cc61068	1

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xf12c	0xf200	6.391483	-
.itext	0x11000	0xb44	0xc00	5.732071	-
.data	0x12000	0xc88	0xe00	2.246313	-
.bss	0x13000	0x56b4	0x0	0.000000[SUSPICIOUS]	-
.idata	0x19000	0xdd0	0xe00	4.971882	-
.tls	0x1a000	0x8	0x0	0.000000[SUSPICIOUS]	-
.rdata	0x1b000	0x18	0x200	0.204488[SUSPICIOUS]	-
.rsrc	0x1c000	0xb200	0xb200	4.132168	-