ID: 831162
Sample Name:
AdobePhotoshop.exe
Cookbook: default.jbs
Time: 07:13:09
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

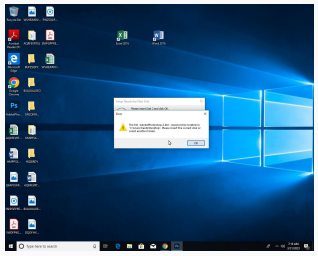
Windows Analysis Report

AdobePhotoshop.exe

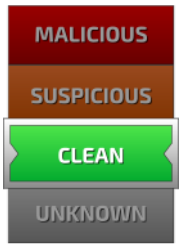
Overview

General Information

Sample Name:	AdobePhotoshop.exe
Analysis ID:	831162
MD5:	bedbec22f0ae7..
SHA1:	753a2ca15710…
SHA256:	797bd80d43c4…
Tags:	exe fakeloader stealer
Infos:	



Detection

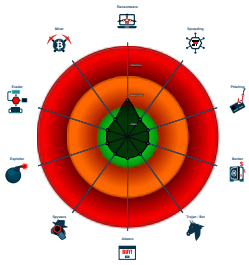


Score:	12
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Obfuscated command line found
- Uses 32bit PE files
- Antivirus or Machine Learning detec…
- Sample file is different than original …
- Drops PE files
- PE file contains sections with non-s…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Found dropped PE file which has no…
- Uses Microsoft's Enhanced Cryptog…
- PE file contains executable resourc…

Classification



Analysis Advice

Sample drops PE files which have not been started, submit dropped PE samples for a secondary analysis to Joe Sandbox

Sample may offer command line options, please run it with the 'Execute binary with arguments' cookbook (it's possible that the command line switches require additional characters like: "-", "/", "--")

Process Tree

- **System is w10x64**
- AdobePhotoshop.exe (PID: 6108 cmdline: C:\Users\user\Desktop\AdobePhotoshop.exe MD5: BEDBEC22F0AE7C2548CE8FD07BFB04EF)
  - AdobePhotoshop.tmp (PID: 6088 cmdline: "C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp" /SL5="$40258,909824,0,C:\Users\user\Desktop\AdobePhotoshop.exe" MD5: C35E48F7A65E98E6DDC5C270B899FF35)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

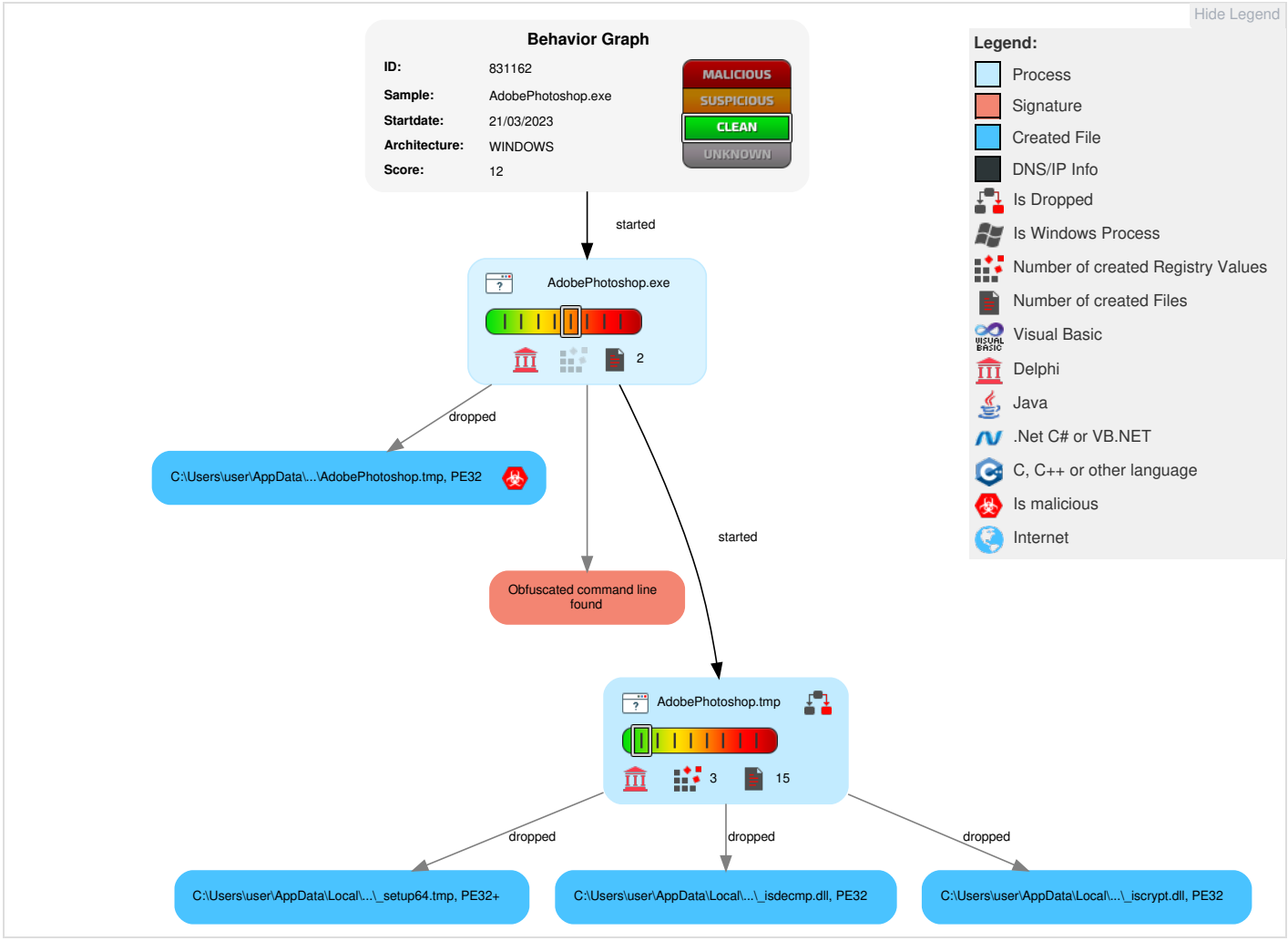
Obfuscated command line found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	2 System Owner/User Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Software Packing	LSASS Memory	2 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Behavior Graph

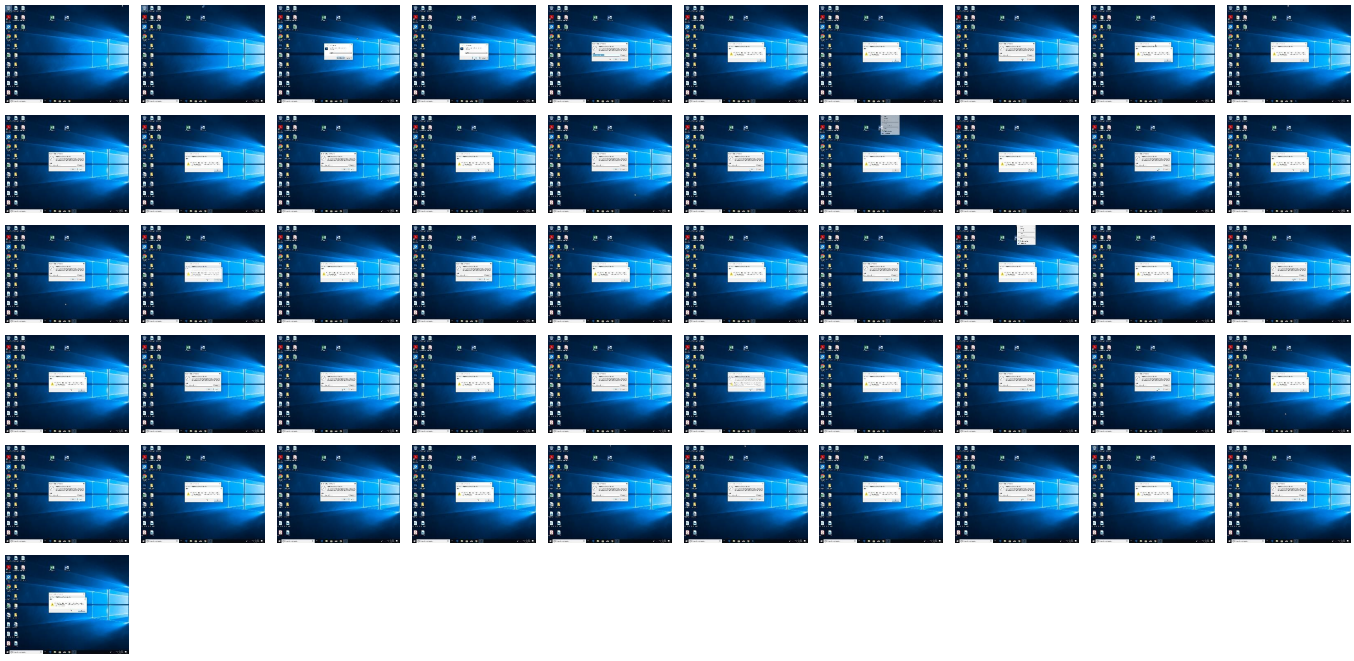
Copyright Joe Security LLC 2023



Screenshots

Thumbnails

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



Copyright Joe Security LLC 2023

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
AdobePhotoshop.exe	3%	ReversingLabs	Win32.PUA.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_iscrypt.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_isdecmp.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_setup64.tmp	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.AdobePhotoshop.tmp.36f9ed0.1.unpack	100%	Avira	TR/Patched.Ren.Gen3		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.haysoft.org%1-k	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://www.remobjects.com/ps	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	0%	URL Reputation	safe	
http://https://www.innosetup.com/	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://cscasha2.ocsp-certum.com04	0%	URL Reputation	safe	
http://https://sectigo.com/CPS05	0%	Avira URL Cloud	safe	
http://https://jrsoftware.org0	0%	Avira URL Cloud	safe	
http://ocsp.usertru	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.haysoft.org%1-k	AdobePhotoshop.exe, 00000000.00000002.513844223.0000000002378000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.exe, 00000000.00000003.247193947.0000000002680000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000003.251571715.0000000003470000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.514556832.00000000024A0000.00000004.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	AdobePhotoshop.exe, _isdecmp.dll.1.dr, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown
http://https://jrsoftware.org/ishelp/index.php?topic=setupcmdlineSetupU	AdobePhotoshop.exe	false		high
http://https://sectigo.com/CPS0	AdobePhotoshop.exe, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown
http://repository.certum.pl/ctnca.cer09	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://repository.certum.pl/cscasha2.cer0	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://ocsp.sectigo.com0	AdobePhotoshop.exe, _isdecmp.dll.1.dr, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown
http://crl.certum.pl/ctnca.crl0k	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://https://www.remobjects.com/ps	AdobePhotoshop.exe, 00000000.00000003.248003228.000000007FB90000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.exe, 00000000.00000003.247627651.00000000027C0000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000000.249756458.0000000000401000.00000020.00000001.01000000.00000004.sdmp, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	AdobePhotoshop.exe, _isdecmp.dll.1.dr, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false	• URL Reputation: safe	unknown
http://https://www.innosetup.com/	AdobePhotoshop.exe, 00000000.00000003.248003228.000000007FB90000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.exe, 00000000.00000003.247627651.00000000027C0000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000000.249756458.0000000000401000.00000020.00000001.01000000.00000004.sdmp, AdobePhotoshop.tmp.0.dr	false	• URL Reputation: safe	unknown
http://ocsp.usertru	AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0D	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false	• URL Reputation: safe	unknown
http://https://jrsoftware.org0	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false	• Avira URL Cloud: safe	unknown
http://https://jrsoftware.org/	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://https://www.certum.pl/CPS0	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://crl.certum.pl/cscasha2.crl0q	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://www.certum.pl/CPS0	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false		high
http://https://sectigo.com/CPS05	AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.certum.pl/cscasha	AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp	false		high
http://cscasha2.ocsp-certum.com04	AdobePhotoshop.tmp, 00000001.00000003.251571715.000000000353B000.00000004.00001000.00020000.00000000.sdmp, AdobePhotoshop.tmp, 00000001.00000002.517058225.00000000036EF000.00000004.00001000.00020000.00000000.sdmp, _isdecmp.dll.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl

Analysis ID:	831162
Start date and time:	2023-03-21 07:13:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
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
Sample file name:	AdobePhotoshop.exe
Detection:	CLEAN
Classification:	clean12.winEXE@3/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 90% (good quality ratio 90%) • Quality average: 91.5% • Quality standard deviation: 16.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target AdobePhotoshop.tmp, PID 6088 because there are n o executed function
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: AdobePhotoshop.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp

Process:	C:\Users\user\Desktop\AdobePhotoshop.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3248832
Entropy (8bit):	6.374526695886884
Encrypted:	false
SSDEEP:	49152:Zdx4HDQNJL0VR6SgMt+k4RiP+RmXMjiINiMq95FoHVHNTQTEjc333vw:qHDYsqiPRhINnq95FoHVBc333o
MD5:	C35E48F7A65E98E6DDC5C270B899FF35
SHA1:	614A308DB5B47D12AB9E3E457C342767BCCEE14B
SHA-256:	0C36B4BB44A2F95A6B1B43549891E40C54E29A89EF0570A7EF9E60A5CD4B48DF
SHA-512:	2A1686B3B26D997B777B21E8F50BE109492616FFB47AEBFC96ED20095F3BF7970D1D8D403FF4301BDFC63E239F034A9107F91577C7406C1641397E550F3752AA
Malicious:	**true**
Reputation:	low
Preview:	MZP.....@.....InUn.....!..L.!..This program must be run under Win32..$7..... .....PE..L...oGXb.....B,..6.....`V,.....`,...@.....`2.....2...@.....@.....-.....-..9.....Y.....|1.....-..... ....-.....-.....text.....,.....,..... ..`.itext...(...0,..*...,..... ..`.data.....`,.....F,.....@....bss.....y....-.....idata...9....-..:...,.....@....didat a.....-.....-.....@....edata.....-.....-.....@..@.tls....L.....-.....rdata..]....-..... -.....@..@.rsrc....Y.....Z..."-.....@..@.....1.....0..... @..@.....

C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_iscrypt.dll

Process:	C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2560
Entropy (8bit):	2.8818118453929262
Encrypted:	false
SSDEEP:	24:e1GSgDIX566lIB6SXvVmMPUjvhBrDsqZ:SgDKRlVImgUNBsG
MD5:	A69559718AB506675E907FE49DEB71E9
SHA1:	BC8F404FFDB1960B50C12FF9413C893B56F2E36F
SHA-256:	2F6294F9AA09F59A574B5DCD33BE54E16B39377984F3D5658CDA44950FA0F8FC
SHA-512:	E52E0AA7FE3F79E36330C455D944653D449BA05B2F9ABEE0914A0910C3452CFA679A40441F9AC696B3CCF9445CBB85095747E86153402FC362BB30AC08249A63
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.c.W.c.W.c...>.T.c.W.b.V.c.R.<.V.c.R.?.V.c.R.9.V.c.RichW. c.....PE..L....b.@.....!..... ....@.....p ..}.... ..(.....0..... ....text..... ..`.rdata..... .....@..@.reloc.....0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_isdecmp.dll

Process:	C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29472
Entropy (8bit):	7.042110181107409
Encrypted:	false
SSDEEP:	768:BD7FEAbd+EDsIOmF+OiR9rikW/F+M9OAriXiRQU:M07sIOYRiPWkWNl9WXil

MD5:	077CB4461A2767383B317EB0C50F5F13
SHA1:	584E64F1D162398B7F377CE55A6B5740379C4282
SHA-256:	8287D0E287A66EE78537C8D1D98E426562B95C50F569B92CEA9CE36A9FA57E64
SHA-512:	B1FCB0265697561EF497E6A60FCEE99DC5EA0CF02B4010DA9F5ED93BCE88BDFEA6BFE823A017487B8059158464EA29636AAD8E5F9DD1E8B8A1B6EAAAB670E547
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I...(...(...(..n ..(...(...(...$..(...$..(...$..(..Rich.(.....PE..L. .....B.....!..... .....p.....0....P.....P.....;.....;..(.....4.. ?...@.....0.....0.....text... ....`.rdata.....0.....$.....@..@.reloc.....@.....2.....@..B..... ....

C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	high, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....R.....#.....@.....`.....<!.....P..H....@..0..... ..... .....text..... ..`.rdata..|.... .....@..@.data.....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.470929133092286
TrID:	• Win32 Executable (generic) a (10002005/4) 98.45% • Inno Setup installer (109748/4) 1.08% • Win32 EXE PECompact compressed (generic) (41571/9) 0.41% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	AdobePhotoshop.exe
File size:	1894312
MD5:	bedbec22f0ae7c2548ce8fd07bfb04ef
SHA1:	753a2ca15710cf7ec16b59abc768a459f451e8e3
SHA256:	797bd80d43c4ef7ab8fde178ca551ad2f9141ca3552ce42c8e96ccc95dc6d3bb
SHA512:	d5498ddbd92e9a80b077119424d51ff4d830a60f5aee868c0d339618eaa104e448281b9ba484a8bd1f18d89ec31ba1862bd89e1e93a4508f4a797475d7e5d3b6
SSDEEP:	24576:Z7FUDowAyrTVE3U5FTd8w8cfRenhAb9hRZaOyKMG0NDU+ExFYG6i5NwImxgYxhvc:ZBuZrEU+/cz9nZ5wDPEzY3ONdmxRbLI
TLSH:	A1959E3BB268653FC46A463F2572933099F7AA51E41E8C1A87E014CCCFE5460DE3B69D
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	c498d8eccce49a44

Static PE Info

General

Entrypoint:	0x4b5eec
Entrypoint Section:	.itext
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6258476F [Thu Apr 14 16:10:23 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	e569e6f445d32ba23766ad67d1e3787f

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=Hamill.net
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 3/20/2023 7:42:06 PM 3/20/2024 8:02:06 PM
Subject Chain	• CN=Hamill.net
Version:	3
Thumbprint MD5:	D33C0CAD0E7BE3F644996784264BD732
Thumbprint SHA-1:	4BDBA3CCF708FE9787D56A496E725A699CCC587A
Thumbprint SHA-256:	BA71AEB053FBE5C0AFDC7D4381E32648A4C7D8F6A1C94296DBD8E6091EF5764F
Serial:	1167B047543881B048A6BA84E2A7B95C

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFA4h
push ebx
push esi
push edi
xor eax, eax
mov dword ptr [ebp-3Ch], eax
mov dword ptr [ebp-40h], eax
mov dword ptr [ebp-5Ch], eax
mov dword ptr [ebp-30h], eax
mov dword ptr [ebp-38h], eax
mov dword ptr [ebp-34h], eax
mov dword ptr [ebp-2Ch], eax
mov dword ptr [ebp-28h], eax
mov dword ptr [ebp-14h], eax
mov eax, 004B14B8h
call 00007F2E0CC92635h
xor eax, eax
push ebp
push 004B65E2h
push dword ptr fs:[eax]
mov dword ptr fs:[eax], esp

Copyright Joe Security LLC 2023

Instruction
xor edx, edx
push ebp
push 004B659Eh
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
mov eax, dword ptr [004BE634h]
call 00007F2E0CD35127h
call 00007F2E0CD34C7Ah
lea edx, dword ptr [ebp-14h]
xor eax, eax
call 00007F2E0CCA80D4h
mov edx, dword ptr [ebp-14h]
mov eax, 004C1D84h
call 00007F2E0CC8D227h
push 00000002h
push 00000000h
push 00000001h
mov ecx, dword ptr [004C1D84h]
mov dl, 01h
mov eax, dword ptr [004238ECh]
call 00007F2E0CCA9257h
mov dword ptr [004C1D88h], eax
xor edx, edx
push ebp
push 004B654Ah
push dword ptr fs:[edx]
mov dword ptr fs:[edx], esp
call 00007F2E0CD351AFh
mov dword ptr [004C1D90h], eax
mov eax, dword ptr [004C1D90h]
cmp dword ptr [eax+0Ch], 01h
jne 00007F2E0CD3B3CAh
mov eax, dword ptr [004C1D90h]
mov edx, 00000028h
call 00007F2E0CCA9B4Ch
mov edx, dword ptr [004C1D90h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc4000	0x9a	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc2000	0xfdc	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc7000	0x23ddc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1cd0e8	0x16c0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xc6000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xc22f4	0x254	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0xc3000	0x1a4	.didata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb39e4	0xb3a00	False	0.34525867693110646	data	6.357635049994181	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0xb5000	0x1688	0x1800	False	0.54443359375	data	5.971425428435973	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xb7000	0x37a4	0x3800	False	0.36097935267857145	data	5.048648594372454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0xbb000	0x6de8	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0xc2000	0xfdc	0x1000	False	0.3798828125	data	5.029087481102678	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.didata	0xc3000	0x1a4	0x200	False	0.345703125	data	2.7509822285969876	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.edata	0xc4000	0x9a	0x200	False	0.2578125	data	1.877162954504408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0xc5000	0x18	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xc6000	0x5d	0x200	False	0.189453125	data	1.3838943752217987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x23ddc	0x23e00	False	0.3133302482578397	data	5.150053503198692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc75b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_ICON	0xc7a20	0x9b8	Device independent bitmap graphic, 24 x 48 x 32, image size 2448	English	United States
RT_ICON	0xc83d8	0x1128	Device independent bitmap graphic, 32 x 64 x 32, image size 4352	English	United States
RT_ICON	0xc9500	0x2668	Device independent bitmap graphic, 48 x 96 x 32, image size 9792	English	United States
RT_ICON	0xcbb68	0x4428	Device independent bitmap graphic, 64 x 128 x 32, image size 17408	English	United States
RT_ICON	0xcff90	0x5638	Device independent bitmap graphic, 72 x 144 x 32, image size 22032	English	United States
RT_ICON	0xd55c8	0x9928	Device independent bitmap graphic, 96 x 192 x 32, image size 39168	English	United States
RT_ICON	0xdeef0	0x17b5	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0xe06a8	0x775a	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced	English	United States
RT_STRING	0xe7e04	0x360	data		
RT_STRING	0xe8164	0x260	data		
RT_STRING	0xe83c4	0x45c	data		
RT_STRING	0xe8820	0x40c	data		
RT_STRING	0xe8c2c	0x2d4	data		
RT_STRING	0xe8f00	0xb8	data		
RT_STRING	0xe8fb8	0x9c	data		
RT_STRING	0xe9054	0x374	data		
RT_STRING	0xe93c8	0x398	data		
RT_STRING	0xe9760	0x368	data		
RT_STRING	0xe9ac8	0x2a4	data		
RT_RCDATA	0xe9d6c	0x10	data		
RT_RCDATA	0xe9d7c	0x2c4	data		
RT_RCDATA	0xea040	0x2c	data		
RT_GROUP_ICON	0xea06c	0x84	data	English	United States
RT_VERSION	0xea0f0	0x584	data	English	United States

Copyright Joe Security LLC 2023

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xea674	0x765	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
kernel32.dll	GetACP, GetExitCodeProcess, LocalFree, CloseHandle, SizeofResource, VirtualProtect, VirtualFree, GetFullPathNameW, ExitProcess, HeapAlloc, GetCPInfoExW, RtlUnwind, GetCPInfo, GetStdHandle, GetModuleHandleW, FreeLibrary, HeapDestroy, ReadFile, CreateProcessW, GetLastError, GetModuleFileNameW, SetLastError, FindResourceW, CreateThread, CompareStringW, LoadLibraryA, ResetEvent, GetVersion, RaiseException, FormatMessageW, SwitchToThread, GetExitCodeThread, GetCurrentThread, LoadLibraryExW, LockResource, GetCurrentThreadId, UnhandledExceptionFilter, VirtualQuery, VirtualQueryEx, Sleep, EnterCriticalSection, SetFilePointer, LoadResource, SuspendThread, GetTickCount, GetFileSize, GetStartupInfoW, GetFileAttributesW, InitializeCriticalSection, GetSystemWindowsDirectoryW, GetThreadPriority, SetThreadPriority, GetCurrentProcess, VirtualAlloc, GetSystemInfo, GetCommandLineW, LeaveCriticalSection, GetProcAddress, ResumeThread, GetVersionExW, VerifyVersionInfoW, HeapCreate, GetWindowsDirectoryW, VerSetConditionMask, GetDiskFreeSpaceW, FindFirstFileW, GetUserDefaultUILanguage, lstrlenW, QueryPerformanceCounter, SetEndOfFile, HeapFree, WideCharToMultiByte, FindClose, MultiByteToWideChar, LoadLibraryW, SetEvent, CreateFileW, GetLocaleInfoW, GetSystemDirectoryW, DeleteFileW, GetLocalTime, GetEnvironmentVariableW, WaitForSingleObject, WriteFile, ExitThread, DeleteCriticalSection, TlsGetValue, GetDateFormatW, SetErrorMode, IsValidLocale, TlsSetValue, CreateDirectoryW, GetSystemDefaultUILanguage, EnumCalendarInfoW, LocalAlloc, GetUserDefaultLangID, RemoveDirectoryW, CreateEventW, SetThreadLocale, GetThreadLocale
comctl32.dll	InitCommonControls
version.dll	GetFileVersionInfoSizeW, VerQueryValueW, GetFileVersionInfoW
user32.dll	CreateWindowExW, TranslateMessage, CharLowerBuffW, CallWindowProcW, CharUpperW, PeekMessageW, GetSystemMetrics, SetWindowLongW, MessageBoxW, DestroyWindow, CharUpperBuffW, CharNextW, MsgWaitForMultipleObjects, LoadStringW, ExitWindowsEx, DispatchMessageW
oleaut32.dll	SysAllocStringLen, SafeArrayPtrOfIndex, VariantCopy, SafeArrayGetLBound, SafeArrayGetUBound, VariantInit, VariantClear, SysFreeString, SysReAllocStringLen, VariantChangeType, SafeArrayCreate
netapi32.dll	NetWkstaGetInfo, NetApiBufferFree
advapi32.dll	ConvertStringSecurityDescriptorToSecurityDescriptorW, RegQueryValueExW, AdjustTokenPrivileges, GetTokenInformation, ConvertSidToStringSidW, LookupPrivilegeValueW, RegCloseKey, OpenProcessToken, RegOpenKeyExW

Exports

Name	Ordinal	Address
TMethodImplementationIntercept	3	0x4541a8
__dbk_fcall_wrapper	2	0x40d0a0
dbkFCallWrapperAddr	1	0x4be63c

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

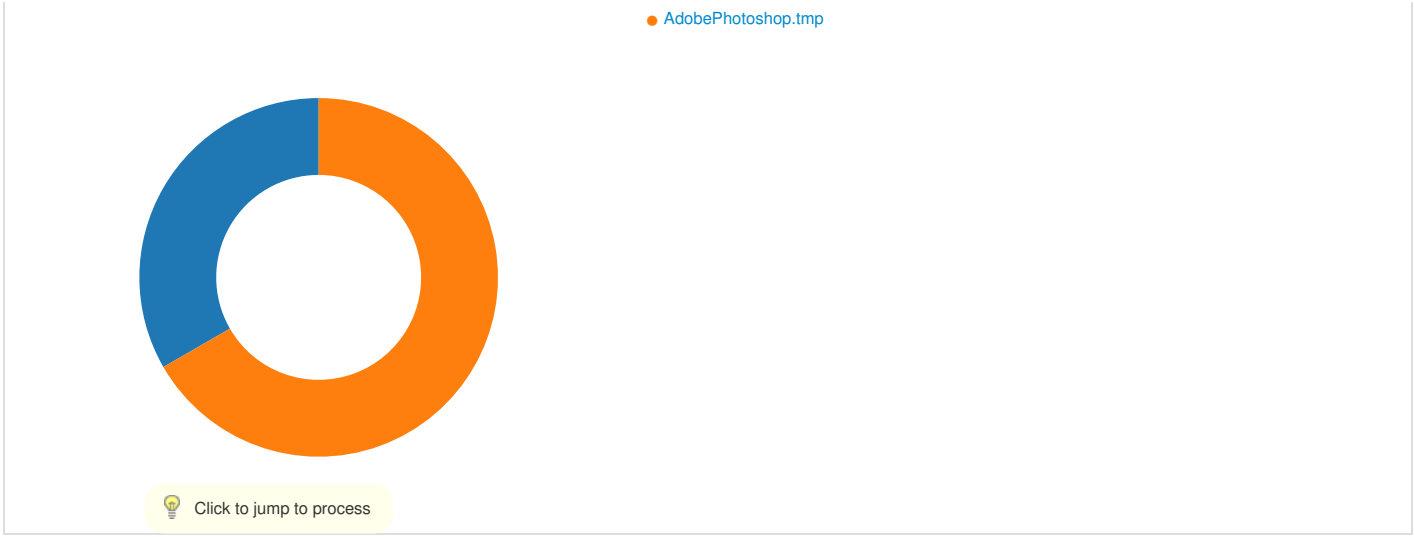
Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior

● AdobePhotoshop.exe



System Behavior

Analysis Process: AdobePhotoshop.exe PID: **6108**, Parent PID: **3452**

General

Target ID:	0
Start time:	07:14:03
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\AdobePhotoshop.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\AdobePhotoshop.exe
Imagebase:	0x400000
File size:	1894312 bytes
MD5 hash:	BEDBEC22F0AE7C2548CE8FD07BFB04EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4AF02B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	423F32	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp	0	3248832	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 49 6e 55 6e 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@InUn!L!This program must be run under Win32$7	success or wait	1	424058	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	64	success or wait	1	423FBC	ReadFile
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	4	success or wait	2	423FBC	ReadFile
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	4	success or wait	2	423FBC	ReadFile

Analysis Process: AdobePhotoshop.tmp

PID: **6088**, Parent PID: **6108**

General

Target ID:	1
Start time:	07:14:04
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-7NLVQ.tmp\AdobePhotoshop.tmp" /SL5="$40258,909824,0,C:\Users\user\Desktop\AdobePhotoshop.exe"
Imagebase:	0x400000
File size:	3248832 bytes
MD5 hash:	C35E48F7A65E98E6DDC5C270B899FF35
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	60D5EB	CreateDirectoryW

Copyright Joe Security LLC 2023

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6ACF78	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_setup64.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	423762	CreateFileW
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_isdecmp.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	423762	CreateFileW
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_iscrypt.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	423762	CreateFileW
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp\innocallback.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	5CC3DE	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_setup64.tmp	0	6144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5e fd fd fd 1a fd fd fd 1a fd fd fd 1a fd fd fd 6c 07 fd fd 17 fd fd fd 1a fd fd fd 02 fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 3d 5c fd fd 1b fd fd fd 52 69 63 68 1a fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 05 00 60 1c 52 00 00 00 00 00 00 00 00 fd 00 23 00 0b 02 08 00 00 06 00 00 00 0e 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$^I=\=\=\RichPE dR#	success or wait	1	4237AD	WriteFile

Copyright Joe Security LLC 2023

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_isdecmp.dll	0	29472	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 49 fd fd fd 28 fd fd fd 28 fd fd fd 28 fd fd 6e 20 98 fd 28 fd fd fd 28 fd fd fd 28 fd fd fd 24 18 fd 28 fd fd fd 24 d8 fd 28 fd fd fd 24 58 fd 28 fd fd 52 69 63 68 fd 28 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 42 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 07 0a 00 20 00 00 00 10 00 00 00 00 00 00 70 2e 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$I(((n ((($($($ (Rich(PELB! p.	success or wait	1	4237AD	WriteFile
C:\Users\user\AppData\Local\Temp\is-BP29Q.tmp_isetup_iscrypt.dll	0	2560	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 13 fd 0d fd 57 fd 63 fd 57 fd 63 fd 57 fd 63 fd fd fd 3e fd 54 fd 63 fd 57 fd 62 fd 56 fd 63 fd 52 fd 3c fd 56 fd 63 fd 52 fd 3f fd 56 fd 63 fd 52 fd 39 fd 56 fd 63 fd 52 69 63 68 57 fd 63 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 62 fd 40 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 07 0a 00 02 00 00 00 04 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$WcWcWc>TcWb VcR<VcR? VcR9VcRichWcPELb@!	success or wait	1	4237AD	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	64	success or wait	1	5CC468	ReadFile
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	4	success or wait	2	5CC468	ReadFile
C:\Users\user\Desktop\AdobePhotoshop.exe	unknown	4	success or wait	2	5CC468	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly