ID: 502665
Sample Name: niPie.exe
Cookbook: default.jbs
Time: 08:40:23
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

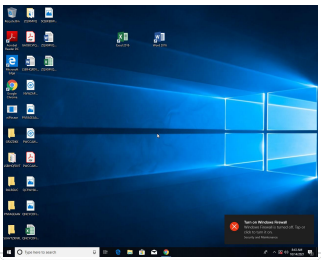
Windows Analysis Report niPie.exe

Overview

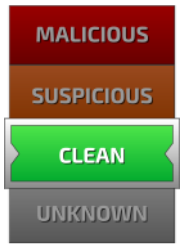
General Information

Sample Name:	niPie.exe
Analysis ID:	502665
MD5:	601fda01efb1a22..
SHA1:	925f30c4a425c13..
SHA256:	5020bbc58ef082a.
Infos:	

Most interesting Screenshot:



Detection

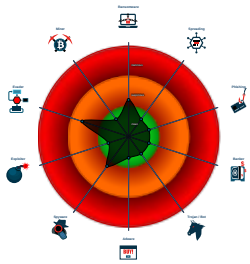


Score:	5
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- AV process strings found (often use…
- Sample file is different than original …
- One or more processes crash
- Uses code obfuscation techniques (…
- Checks if the current process is bein…
- Detected potential crypto function
- Found evasive API chain (may stop…
- Contains functionality to dynamically…
- Found large amount of non-executed…

Classification



Analysis Advice

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: "-", "/", "--")

Sample crashes during execution, try analyze it on another analysis machine

Process Tree

- **System is w10x64**
- niPie.exe (PID: 4528 cmdline: 'C:\Users\user\Desktop\niPie.exe' -install MD5: 601FDA01EFB1A22E18A19793158B51FE)
- niPie.exe (PID: 5808 cmdline: 'C:\Users\user\Desktop\niPie.exe' /install MD5: 601FDA01EFB1A22E18A19793158B51FE)
  - WerFault.exe (PID: 5344 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5808 -s 528 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- niPie.exe (PID: 5332 cmdline: 'C:\Users\user\Desktop\niPie.exe' /load MD5: 601FDA01EFB1A22E18A19793158B51FE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

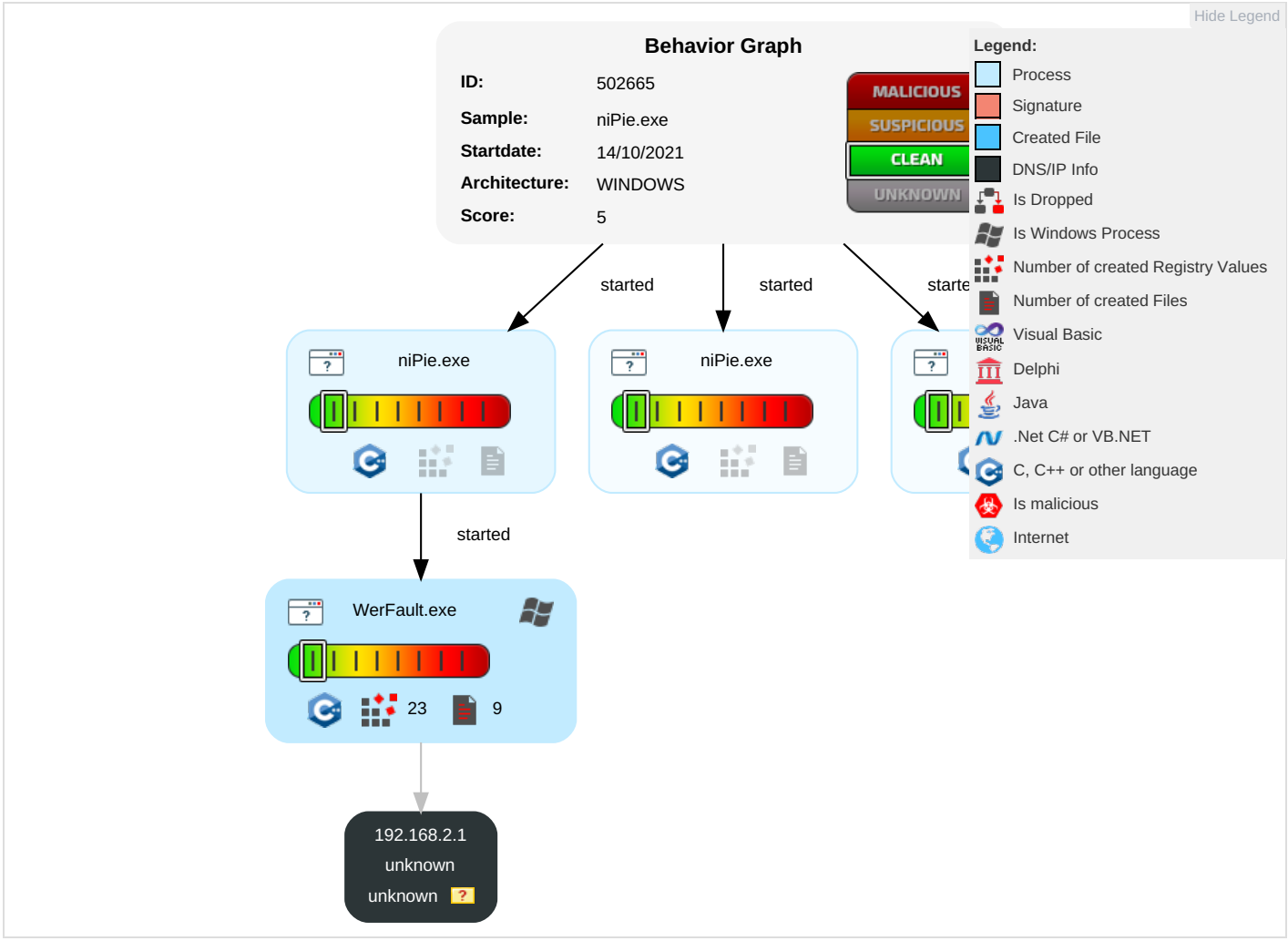
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 2	Virtualization/Sandbox Evasion 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T V A
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	C D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

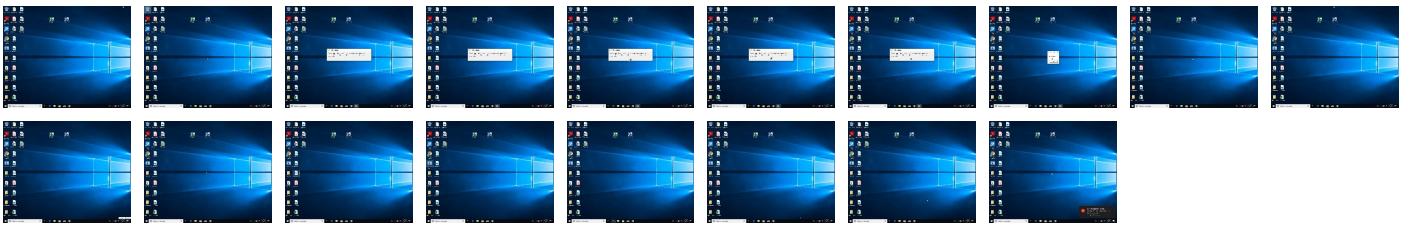
Behavior Graph



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
niPie.exe	0%	Metadefender		Browse
niPie.exe	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.thawte.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502665
Start date:	14.10.2021
Start time:	08:40:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	niPie.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
Run name:	Cmdline fuzzy
Number of analysed new started processes analysed:	28
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
Detection:	CLEAN
Classification:	clean5.winEXE@4/6@0/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 100% (good quality ratio 97.2%) • Quality average: 87.1% • Quality standard deviation: 22.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:41:26	API Interceptor	1x Sleep call for process: WerFault.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_niPie.exe_e6cde1c574634daa1e46756134802be990d9bced_e1e15161_140105c6\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8703585320712506
Encrypted:	false
SSDEEP:	192:wIBNLyipHkgdbcDhRjgIh/u7sYS274ItU:wcNeiZk0c7jj/u7sYX4ItU
MD5:	C0D7310843F8F4325C1610FDDA4668E4
SHA1:	D4DFA0568167234554D7F1BADF51561DD2D2BA72
SHA-256:	6C26895BCFD43A4A1D61A701F664F5B6264B96335A8A71670F83D33B38405E6A
SHA-512:	D7E4F3F7EE44964FDB97D4B087FAA2401277EAD1529E4873D9F7F4498DEC637A6FC5B1D14C34B54C22532316AC767405110377D0D16BA4FE4CE23CD81868C95
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.7.8.6.9.9.6.8.1.5.1.9.2.6.6.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.7.8.6.9.9.6.8.5.4.0.9.9.1.4.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.2.b.7.d.d.8.8.-.d.6.b.8.-.4.b.8.b.-.a.e.d.d.-.b.e.c.e.d.d.4.7.e.3.2.4.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.b.3.0.0.b.5.b.-.c.b.f.7.-.4.7.c.4.-.b.e.8.5.-.0.9.5.3.4.d.0.5.e.b.0.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.n.i.P.i.e...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.6.b.0.-.0.0.0.1.-.0.0.1.c.-.d.e.7.b.-.5.6.e.d.1.1.c.1.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.3.d.5.0.2.0.4.0.b.e.0.4.5.9.b.0.a.9.a.6.5.f.2.d.2.f.5.0.6.c.5.f.0.0.0.0.f.f.f.f.!.0.0.0.0.9.2.5.f.3.0.c.4.a.4.2.5.c.1.3.3.9.1.5.e.e.9.2.d.d.4.c.0.9.0.0.f.3.1.5.3.6.c.0.4.!.n.i.P.i.e...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.0.3././.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1B1.tmp.dmp

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Oct 14 15:41:22 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	54596
Entropy (8bit):	2.059817025510805
Encrypted:	false
SSDEEP:	192:1+4fNhNi0OC4OV6e6bzyN3SzEkMg96CQIhu2YlXalyCBKb:Bl+CfBX1bIhLyC8

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1B1.tmp.dmp	
MD5:	B9D0C19927DC3FC2628C9ACBCD0EA583
SHA1:	B056DEEF8A7A09F2BAB02DCD212D78466AE6579F
SHA-256:	D9BCDBA6ACD224A38C1DAF72FDA6590EFE7E013313452D72538E3FF3C0572653
SHA-512:	97F22935AC3882A0E500B0DB213BB7E4D6264D7D87446BE551E3194002EA323C6E62E5B0948AE48313D1A546CC8DDF0CE00C9BB4CCA441CD2EE816B936BDFD 01
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....Oha.....d....0.....T.....8.....T.....D.....U.....B.....d.....GenuineIn telW.....T.....Oha.....0..2.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e..... .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF656.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8284
Entropy (8bit):	3.6902502451531936
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNif66rY6YFPSUyogmfRSqXh7CprRc89b2vsfINjym:RrlsNiy606YtSUyogmfRSXJ2UfINH
MD5:	C197E246B6EBB950F52D55C6D5B459F4
SHA1:	BBBFDC67A29B9F7967EB16DF1BC7F4B984FDA502
SHA-256:	E9670D33B9E2A1F9B58E786B18C8932CF7541A02DD4F150C8803315151AA37EF
SHA-512:	ADC44F6500E8C3E4BEDD947688DDEA258B139652749F7F9D4B4507BB722F969E329E81DB8EFF4EEFF965FD81C538222A433467870216B1F3AFFDD41D3459115F
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.8.0.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERFA10.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4544
Entropy (8bit):	4.440570598188364
Encrypted:	false
SSDEEP:	48:cvIwSD8zsvJgtWI9iMWSC8BWM8fm8M4J46qE+L/bFbX+q8qsS7R/nhws60Xi8d:uITfR5lSNUxJ6Fws60Xi8d
MD5:	665AACD7328A47617D15C599E633FA94
SHA1:	1D6A3AE0B676DFB321924FF0E5CA24789ABB7336
SHA-256:	FA858B206ECE5CE3843078D4C1E489E086549140118E61652D1C9BBDA1C6A6AB
SHA-512:	89EE7E52E7157FB87E885A80DD40DD93DBE3BDA0DF9A12EA3125ED5E0D13BF3F8F40CAB187DC553285F4A95E637378C925E54246F5F31DE8DC5433B405E50A 4
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1209652" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0- 11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.275087550666143
Encrypted:	false
SSDEEP:	12288:FipMLJvchtjAw8z7nZ38GMARuhauEhP16N6xcqUEbGt4pVs1E9dZZd:UpMLJvchtjAw8zXN
MD5:	2C419893782E19E68C6EA20E61ADE4FD
SHA1:	684AF6925498E41E88494D73E2D447DB019EEA73
SHA-256:	4CEC7CBC5FF3A479E46BC0004A2DE16AD1CC45B998E527DE792CC85C0C57D7B0

C:\Windows\appcompat\Programs\Amcache.hve	
SHA-512:	84A1721FBFD55B3E8147F0126A5E0577D12C8DA31C0356E144F7B48BEA86951BBC58E7EC121591C5DE46156AA4A037C9CC636A324B857E4A292AB718B3C12D8
Malicious:	false
Reputation:	low
Preview:	regfZ...Z...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.rmtmR.K..... .....O..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.183354901830507
Encrypted:	false
SSDEEP:	768:nnUdC0MwqhBrOFftx1xJ4X7fFK7bBqXIeq5QMVyi6a74LXHuzEsFqb+v:VfB2xA/CReOhqC
MD5:	23FFAE33C71AB2637BA27D8CF7225580
SHA1:	1A345D8BBE40B02FB15DFBD9CF3EF167A3D695F1
SHA-256:	DB922318220427C790ED4E8F88672BD213D8AD2FF1D2C67C79A1B3F58F19D68E
SHA-512:	AA414C8B6D0646FB4A58D45108EEC1F1CD08F37275C534987B6B135424D0B249F48E7F54DC51E209B0205DFE3D329C97BEE2136DB3CCC8D57C56BA54D108F7F
Malicious:	false
Reputation:	low
Preview:	regfY...Y...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.rmtmR.K..... .....O.HvLE.~.....Y.....`....)..... ....0..... ..hbin.....p.\..,.....nk,..2N..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..2N..... ....Z.....Root.....lf.....Root....nk ..2N.....}..... .....*.....DeviceCensus.....vk.....WritePer

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.892836892157124
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	niPie.exe
File size:	73664
MD5:	601fda01efb1a22e18a19793158b51fe
SHA1:	925f30c4a425c133915ee92dd4c0900f31536c04
SHA256:	5020bbc58ef082a5ac8e42e394c4235e88b9c5bd1ed3cdc126a24a649997ebf3
SHA512:	0db9ac45dfa3e4530fa4a945e3cac301e1ee8b26fc2690739741d72e1b7712e205f4bf83463e51c70df141af663ffa54c4e281d93f3bc386487a42eb1778a03c
SSDEEP:	768:gjan8GnhwDHcnrkqAAO8IEwm8iNWTGzvtKsDsoxm3whvI:gjanoDGrkbAO80mhN/ZKsDnmghw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../..)k..zk..zk..z...zh..z...zx..z...zW..z...zc..z2..zl..zk..z,..zm..zo..z...zj..z...zj..zRichk..z.....PE..L...j.I>...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x402d93
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x3E49816A [Tue Feb 11 23:04:10 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	8fcbb82d712dc622f705d3815ebb3266

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=VeriSign Class 3 Code Signing 2010 CA, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 4/11/2016 5:00:00 PM 7/12/2019 4:59:59 PM
Subject Chain	• CN=National Instruments Corporation, O=National Instruments Corporation, L=Austin, S=Texas, C=US
Version:	3
Thumbprint MD5:	1C8D1A5469552A41DE716974A986D673
Thumbprint SHA-1:	70B8BA3A50BCDBAD1DC2C86C6DEB1D78215EA111
Thumbprint SHA-256:	4750C8643DF6099EA03EB3ADA1157EEFC149A3BAC6DBB31760A4DC0AFC41C007
Serial:	61C3329855F6476CFCB4FCF359E55909

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x7722	0x8000	False	0.566650390625	COM executable for DOS	6.39486324672	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0xc32	0x1000	False	0.376708984375	data	4.52160108025	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x410c	0x3000	False	0.0714518229167	data	0.996089583315	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0xa20	0x1000	False	0.26318359375	data	4.15843705735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	
German	Germany	
French	France	
Japanese	Japan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: niPie.exe PID: 4528 Parent PID: 3604

General

Start time:	08:41:14
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\niPie.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\niPie.exe' -install
Imagebase:	0x400000
File size:	73664 bytes
MD5 hash:	601FDA01EFB1A22E18A19793158B51FE

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: niPie.exe PID: 5808 Parent PID: 3604

General

Start time:	08:41:17
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\niPie.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\niPie.exe' /install
Imagebase:	0x400000
File size:	73664 bytes
MD5 hash:	601FDA01EFB1A22E18A19793158B51FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: WerFault.exe PID: 5344 Parent PID: 5808

General

Start time:	08:41:19
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5808 -s 528
Imagebase:	0xd00000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: niPie.exe PID: 5332 Parent PID: 3604

General

Start time:	08:41:19
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\niPie.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\niPie.exe' /load
Imagebase:	0x400000
File size:	73664 bytes
MD5 hash:	601FDA01EFB1A22E18A19793158B51FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis