ID: 679166
Sample Name: bP5g4FsSJk.exe
Cookbook: default.jbs
Time: 11:11:07
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

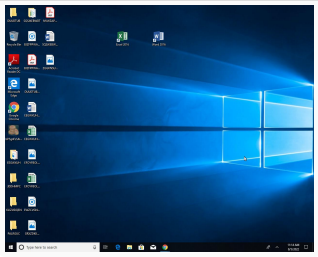
Windows Analysis Report

bP5g4FsSJk.exe

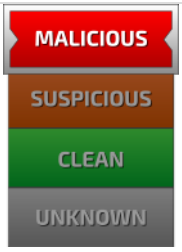
Overview

General Information

Sample Name:	bP5g4FsSJk.exe
Analysis ID:	679166
MD5:	28fb096cbce32c…
SHA1:	50ceaddc379e13..
SHA256:	1918cc07f0b41a…
Tags:	exe Stop
Infos:	



Detection



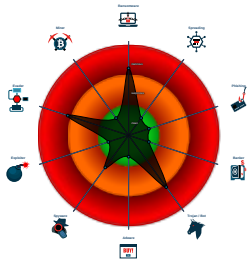
Djvu

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Djvu Ransomware
- Antivirus detection for URL or domain
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Yara signature match
- Contains functionality to check if a d…
- Contains functionality to query local…
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- bP5g4FsSJk.exe (PID: 5468 cmdline: "C:\Users\user\Desktop\bP5g4FsSJk.exe" MD5: 28FB096CBCE32CF1F87719254452014F)
  - bP5g4FsSJk.exe (PID: 5604 cmdline: "C:\Users\user\Desktop\bP5g4FsSJk.exe" MD5: 28FB096CBCE32CF1F87719254452014F)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://rgyui.top/dl/build2.exe",
    "http://acacaca.org/files/1/build3.exe"
  ],
  "C2 url": "http://acacaca.org/test2/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-QsoSRIeAK6\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@bestyourmail.ch\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0531Jhyjd",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:\\SystemID\\",
```

```
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwX6oUNb4mk19lyNBxK80||||nWDzdQgJ9XMg2LdYk3Hm0F0zP2rWDuKVpyAbosbOzGKbJOkVa||/1XbytFAm8RYfkB||/||||nnfEgGh5OGcw||/CcqqOL3R4Vpd7slLVXc56FLkTWEMSShzg1sNxgIiQm8VcaXOgUk8||||ntvWKcUIV9ujXmn5UBSy||/ICDPveI3QCaxZod7kIBwZzszO||/3CvNwAy3eejgJ6j8ie||||nmwJ9pjskzLjmq92yhDGUQygWfGw0tL1KtSiqUy2M7KNdmD4FX1aVeutZC9bggvn8||||nV4ksJChvMxI521ms58donyKjwBAbKXBfVRaXUV2k34bI0NQqhLz5OeGIRhn67oe+||||njwIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.271002067.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xd9ef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF

Source	Rule	Description	Author	Strings
00000000.00000002.278389009.0000000004235000.00000040.00000800.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x798:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_STOP	Detects STOP ransomware	ditekSHen	• 0xffe88:$x1: C:\SystemID\PersonalID.txt • 0x100334:$x2: /deny *S-1-1-0:(OI)(CI)(DE,DC) • 0xffcf0:$x3: e:\doc\my work (c++)_git\encryption\ • 0x105b28:$x3: E:\Doc\My work (C++)_Git\Encryption\ • 0x1002ec:$s1: " --AutoStart • 0x100300:$s1: " --AutoStart • 0x103f48:$s2: --ForNetRes • 0x103f10:$s3: --Admin • 0x104390:$s4: %username% • 0x1044b4:$s5: ?pid= • 0x1044c0:$s6: &first=true • 0x1044d8:$s6: &first=false • 0x1003f4:$s7: delself.bat • 0x1043f8:$mutex1: {1D6FC66E-D1F3-422C-8A53-C0BBCF3D900D} • 0x104420:$mutex2: {FBB4BCC6-05C7-4ADD-B67B-A98A697323C1} • 0x104448:$mutex3: {36A698B9-D67C-4E07-BE82-0EC5B14B4DF5}
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.bP5g4FsSJk.exe.400000.2.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
1.0.bP5g4FsSJk.exe.400000.0.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
1.0.bP5g4FsSJk.exe.400000.3.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
1.0.bP5g4FsSJk.exe.400000.1.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xcdef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
1.0.bP5g4FsSJk.exe.400000.5.raw.unpack	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0xd9ef:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
Click to see the 64 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

Spam, unwanted Advertisements and Ransom Demands

Yara detected Djvu Ransomware

System Summary

Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion

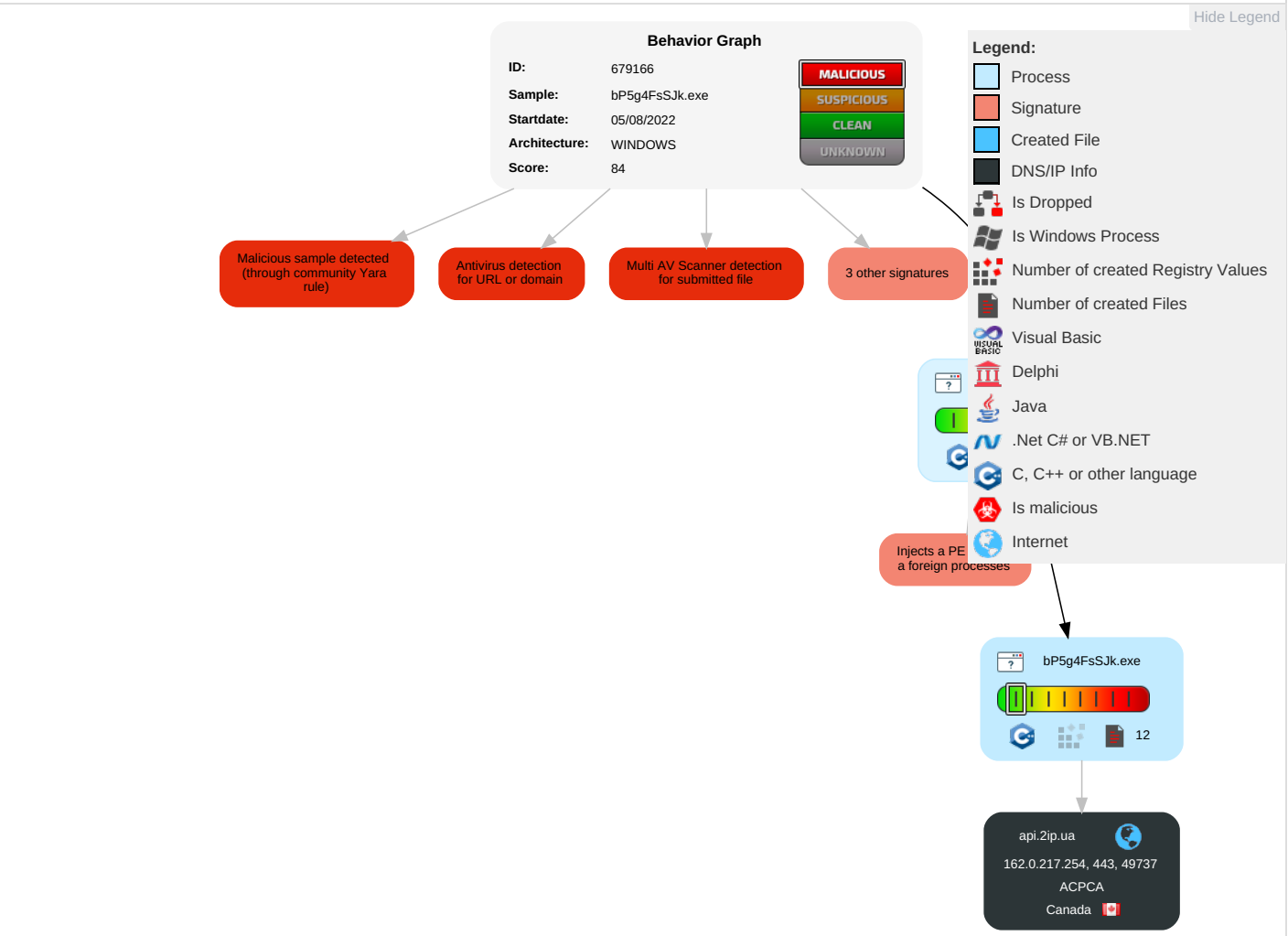
Injects a PE file into a foreign processes

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	2 Command and Scripting Interpreter	Path Interception	1 Exploitation for Privilege Escalation	1 1 1 Process Injection	OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	3 Native API	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	4 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	2 3 System Information Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

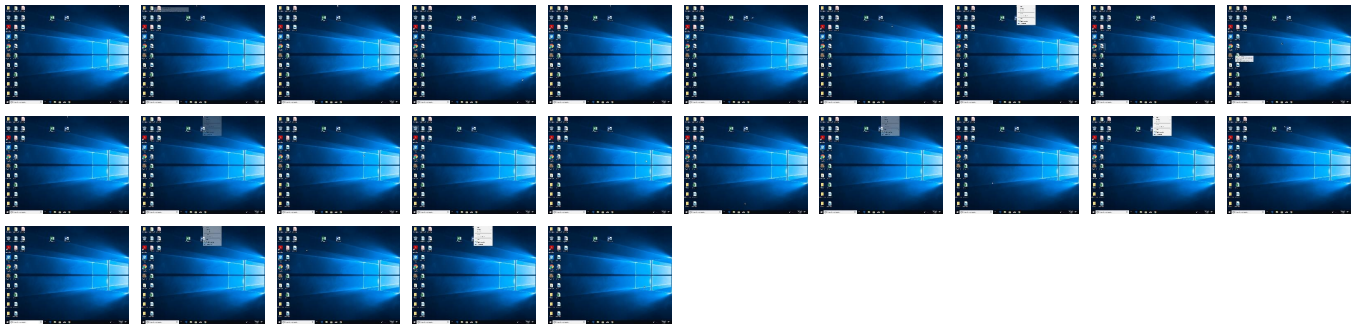
Behavior Graph



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
bP5g4FsSJk.exe	53%	ReversingLabs	Win32.Trojan.Azorult	
bP5g4FsSJk.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.bP5g4FsSJk.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.2.bP5g4FsSJk.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1229097		Download File
1.0.bP5g4FsSJk.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.0.bP5g4FsSJk.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.0.bP5g4FsSJk.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Source	Detection	Scanner	Label	Link	Download
1.0.bP5g4FsSJk.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.0.bP5g4FsSJk.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.2.bP5g4FsSJk.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
1.0.bP5g4FsSJk.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1223627		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://acacaca.org/test2/get.php	100%	Avira URL Cloud	malware	
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.2ip.ua	162.0.217.254	true	false		high

Contacted URLs

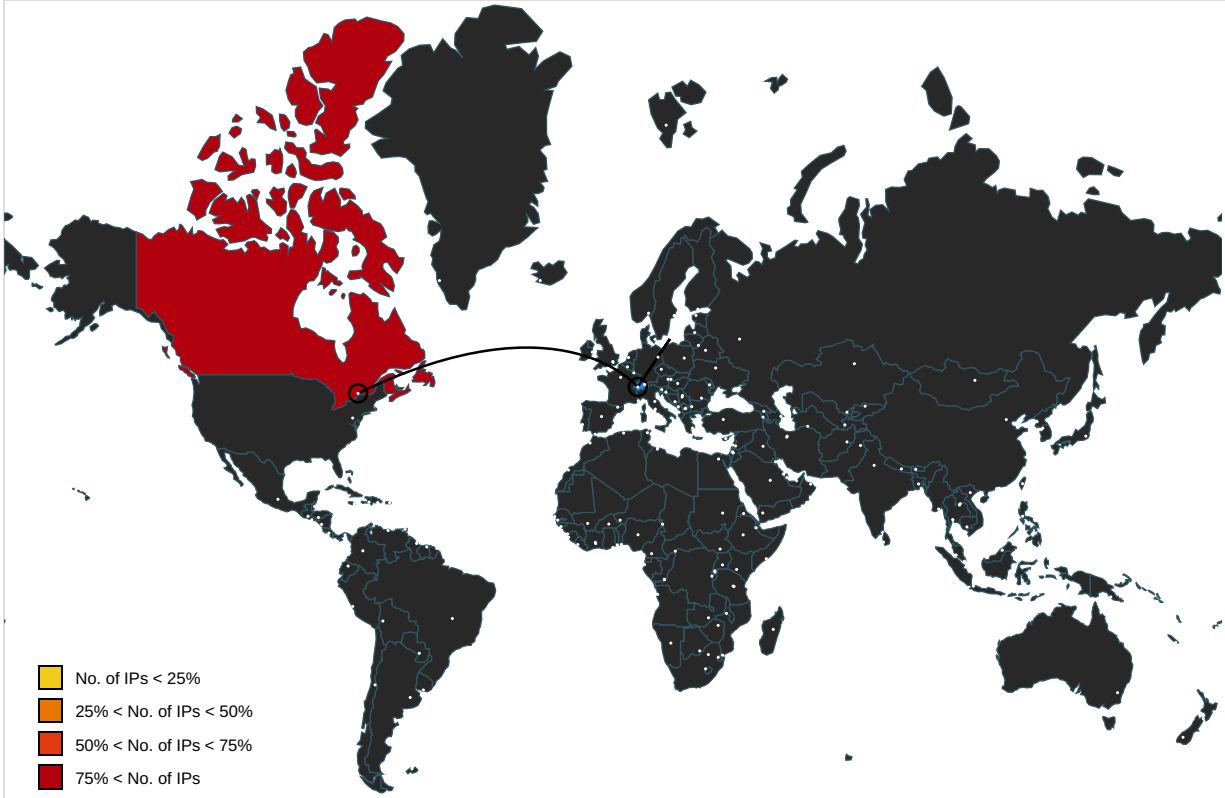
Name	Malicious	Antivirus Detection	Reputation
http://acacaca.org/test2/get.php	true	• Avira URL Cloud: malware	unknown
http://https://api.2ip.ua/geo.json	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ns1.kriston.ugns2.chalekin.ugns3.unalelath.ugns4.andromath.ug/Error	bP5g4FsSJk.exe, 00000000.00000002.278746171.00000000042D0000.00000040.00001000.00020000.00000000.sdmp, bP5g4FsSJk.exe, 00000001.00000002.281265111.0000000000400000.00000040.00000400.00020000.00000000.sdmp, bP5g4FsSJk.exe, 00000001.00000000.273505881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, bP5g4FsSJk.exe, 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.2ip.ua/geo.jsonY	bP5g4FsSJk.exe, 00000001.00000002.286593471.00000000008EF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/	bP5g4FsSJk.exe, 00000001.00000002.286817281.000000000090D000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsont	bP5g4FsSJk.exe, 00000001.00000002.286414138.00000000008C7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsong	bP5g4FsSJk.exe, 00000001.00000002.286593471.00000000008EF000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.json6	bP5g4FsSJk.exe, 00000001.00000002.286414138.00000000008C7000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.openssl.org/support/faq.html	bP5g4FsSJk.exe, 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://api.2ip.ua/geo.jsons	bP5g4FsSJk.exe, 00000001.00000002.286414138.00000000008C7000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.2ip.ua/Y%	bP5g4FsSJk.exe, 00000001.00000002.286817281.000000000090D000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679166
Start date and time: 05/08/202211:11:07	2022-08-05 11:11:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bP5g4FsSJk.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:	mal84.rans.troj.evad.winEXE@3/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 91.7% (good quality ratio 84.8%) • Quality average: 79.9% • Quality standard deviation: 30.9%
HCA Information:	• Successful, ratio: 60% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.
- VT rate limit hit for: bP5g4FsSJk.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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.841901633749817
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:	bP5g4FsSJk.exe
File size:	748032
MD5:	28fb096cbce32cf1f87719254452014f
SHA1:	50ceaddc379e1376a579e4c9d4465fd3c734c277
SHA256:	1918cc07f0b41a9e9dc18e715e5862a68ca49d61fdad7d76126953629c05be98
SHA512:	eb5468f817ca4dee892eb200e920796e175298667fc86f934912c6bd304aa54d39ad4535fa12bdd0c803ac7ee164281372dc364ad97542585209fa39447b5a9f
SSDEEP:	12288:+5v3qTuu7zbgLsSFKUilhkehB/MLfSTOIPAU+dmb:+5vo1SogidMLZHmb
TLSH:	18F4123032E1C036E1B61238447D8FA51ABEFC222BB4898767D42A1D6E677C05E7975F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ADK. *.. *.. *..V... *..V... *..X... *.. +.f *..V... *..V... *..V... *.Rich. *.....PE..L...!.K`.....

File Icon

Icon Hash:	8a9099a9ca8cd2f2

Static PE Info

General

Entrypoint:	0x498550
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x604BC821 [Fri Mar 12 19:59:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	52981a63110ae9001dc5c79717e57d47

Entrypoint Preview

Instruction
call 00007FB788BC00DBh
jmp 00007FB788BB970Eh
int3
int3
int3
int3
int3
int3
call 00007FB788BB98BCh
xchg cl, ch

Instruction
jmp 00007FB788BB98A4h
call 00007FB788BB98B3h
fxch st(0), st(1)
jmp 00007FB788BB989Bh
fabs
fld1
mov ch, cl
xor cl, cl
jmp 00007FB788BB9891h
mov byte ptr [ebp-00000090h], FFFFFFFEh
fabs
fxch st(0), st(1)
fabs
fxch st(0), st(1)
fpatan
or cl, cl
je 00007FB788BB9886h
fldpi
fsubrp st(1), st(0)
or ch, ch
je 00007FB788BB9884h
fchs
ret
fabs
fld st(0), st(0)
fld st(0), st(0)
fld1
fsubrp st(1), st(0)
fxch st(0), st(1)
fld1
faddp st(1), st(0)
fmulp st(1), st(0)
ftst
wait
fstsw word ptr [ebp-000000A0h]
wait
test byte ptr [ebp-0000009Fh], 00000001h
jne 00007FB788BB9887h
xor ch, ch
fsqrt
ret
pop eax
jmp 00007FB788BC02AFh
fstp st(0)
fld tbyte ptr [004024DAh]
ret
fstp st(0)
or cl, cl
je 00007FB788BB988Dh
fstp st(0)
fldpi
or ch, ch
je 00007FB788BB9884h
fchs
ret
fstp st(0)
fldz
or ch, ch
je 00007FB788BB9879h

Instruction
fchs
ret
fstp st(0)
jmp 00007FB788BC0285h
fstp st(0)
mov cl, ch
jmp 00007FB788BB9882h
call 00007FB788BB984Eh
jmp 00007FB788BC0290h
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
add esp, 00FFFD30h

Rich Headers

Programming Language:	• [ASM] VS2010 build 30319 • [C] VS2010 build 30319 • [IMP] VS2008 SP1 build 30729 • [C++] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa638c	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x212e000	0xd568	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1230	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x3690	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1e0	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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	0xa5eb4	0xa6000	False	0.9462317041603916	data	7.945996199237986	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xa7000	0x20861cc	0x3000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x212e000	0xd568	0xd600	False	0.6642997955607477	data	6.526730178678878	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

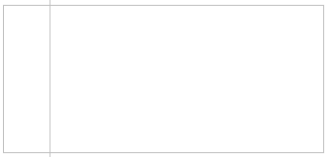
Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x212e4e0	0xea8	data	Kannada	Kanada
RT_ICON	0x212f388	0x8a8	data	Kannada	Kanada
RT_ICON	0x212fc30	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x2130198	0x25a8	data	Kannada	Kanada
RT_ICON	0x2132740	0x10a8	data	Kannada	Kanada
RT_ICON	0x21337e8	0x988	data	Kannada	Kanada
RT_ICON	0x2134170	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x2134640	0xea8	data	Kannada	Kanada
RT_ICON	0x21354e8	0x8a8	data	Kannada	Kanada
RT_ICON	0x2135d90	0x6c8	data	Kannada	Kanada
RT_ICON	0x2136458	0x568	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_ICON	0x21369c0	0x25a8	data	Kannada	Kanada
RT_ICON	0x2138f68	0x10a8	data	Kannada	Kanada
RT_ICON	0x213a010	0x468	GLS_BINARY_LSB_FIRST	Kannada	Kanada
RT_DIALOG	0x213a688	0x78	data		
RT_STRING	0x213a700	0x67a	data	French	Switzerland
RT_STRING	0x213ad80	0x464	data	French	Switzerland
RT_STRING	0x213b1e8	0x380	data	French	Switzerland
RT_GROUP_ICON	0x21345d8	0x68	data	Kannada	Kanada
RT_GROUP_ICON	0x213a478	0x68	data	Kannada	Kanada
RT_VERSION	0x213a4f0	0x194	data		
None	0x213a4e0	0xa	data		

Imports

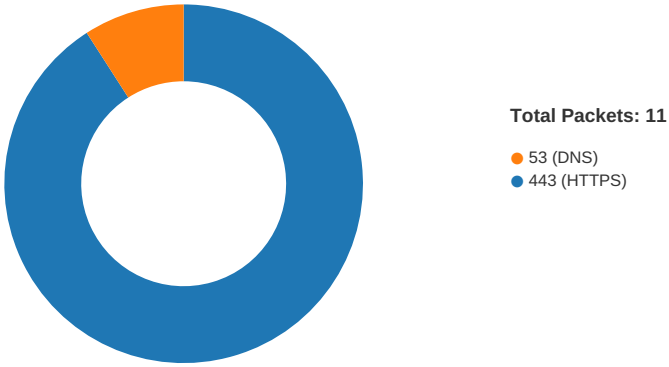
DLL	Import
KERNEL32.dll	GetModuleFileNameA, FoldStringA, GetLocalTime, InterlockedDecrement, GetLocaleInfoA, InterlockedCompareExchange, _hwrite, CancelWaitableTimer, GetSystemDirectoryW, CreateEventW, ReadConsoleA, BuildCommDCBA, GetConsoleAliasExesLengthW, SetSystemTimeAdjustment, PeekConsoleInputW, EnumDateFormatsA, CreateFileW, RegisterWaitForSingleObjectEx, LoadLibraryW, VerifyVersionInfoW, WaitNamedPipeA, GetEnvironmentStrings, FindResourceExA, VirtualProtect, GetFirmwareEnvironmentVariableW, BeginUpdateResourceW, GetConsoleAliasExesLengthA, WriteConsoleA, EnumCalendarInfoExA, WriteConsoleW, DeleteFileW, FillConsoleOutputCharacterA, GetProcAddress, GetModuleHandleW, GetUserDefaultLCID, FindFirstChangeNotificationW, GetFileAttributesExA, GetCalendarInfoA, SetConsoleTitleA, GetBinaryTypeW, GlobalAlloc, GetComputerNameExA, FindNextFileA, OpenJobObjectA, HeapSize, _lclose, GetComputerNameW, TlsGetValue, SetCalendarInfoW, SetComputerNameW, CreateDirectoryExA, InitializeCriticalSectionAndSpinCount, FindFirstChangeNotificationA, GetVolumePathNameA, LoadLibraryA, GetProcessHandleCount, GetThreadLocale, GetSystemDefaultLangID, GetCurrentProcess, ReadFile, HeapFree, GetDiskFreeSpaceW, GetProcessHeap, RaiseException, RtlUnwind, MultiByteToWideChar, GetCommandLineW, HeapSetInformation, GetStartupInfoW, EncodePointer, HeapAlloc, GetLastError, IsProcessorFeaturePresent, DecodePointer, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, SetHandleCount, GetStdHandle, GetFileType, DeleteCriticalSection, SetFilePointer, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, TerminateProcess, EnterCriticalSection, LeaveCriticalSection, ExitProcess, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CloseHandle, WriteFile, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, Sleep, SetStdHandle, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, FlushFileBuffers, CreateFileA, LCMapStringW, GetStringTypeW, HeapReAlloc, SetEndOfFile
USER32.dll	ClientToScreen

Possible Origin

Language of compilation system	Country where language is spoken	Map
Kannada	Kanada	
French	Switzerland	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:12:25.482526064 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:25.482600927 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:25.482718945 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:25.501522064 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:25.501563072 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:25.570105076 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:25.570306063 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.063847065 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.063880920 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:26.064246893 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:26.064321041 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.068742037 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.103678942 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:26.103773117 CEST	443	49737	162.0.217.254	192.168.2.3
Aug 5, 2022 11:12:26.103781939 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.103825092 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.187181950 CEST	49737	443	192.168.2.3	162.0.217.254
Aug 5, 2022 11:12:26.187218904 CEST	443	49737	162.0.217.254	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 11:12:25.400958061 CEST	64851	53	192.168.2.3	8.8.8.8
Aug 5, 2022 11:12:25.428997040 CEST	53	64851	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 11:12:25.400958061 CEST	192.168.2.3	8.8.8.8	0x62d8	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 11:12:25.428997040 CEST	8.8.8.8	192.168.2.3	0x62d8	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.2ip.ua

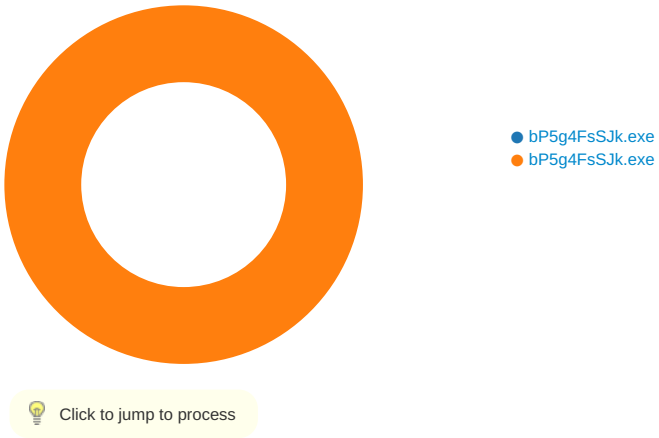
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49737	162.0.217.254	443	C:\Users\user\Desktop\bP5g4FsSJk.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-05 09:12:26 UTC	0	OUT	GET /geo.json HTTP/1.1 User-Agent: Microsoft Internet Explorer Host: api.2ip.ua
2022-08-05 09:12:26 UTC	0	IN	HTTP/1.1 429 Too Many Requests Date: Fri, 05 Aug 2022 09:12:26 GMT Server: Apache Strict-Transport-Security: max-age=63072000; preload X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block; report=... Access-Control-Allow-Origin: * Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, PATCH, DELETE Access-Control-Allow-Headers: X-Accept-Charset,X-Accept,Content-Type Upgrade: h2,h2c Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8
2022-08-05 09:12:26 UTC	0	IN	Data Raw: 32 32 61 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 63 6c 61 73 73 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 22 3e 0a 09 09 09 09 4c 69 6d 69 74 20 6f 66 20 72 65 74 75 72 6e 65 64 20 6f 62 6a 65 63 74 73 20 68 61 73 20 62 65 65 6e 20 72 65 61 63 68 65 64 2e 20 46 6f 72 20 6d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 70 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 62 79 20 65 6d 61 69 6c 20 3c 61 20 68 72 65 66 3d 22 6d 61 69 6c 74 6f 3a 68 65 6c 70 40 32 69 70 2e 6d 65 3f 73 75 62 6a 65 63 74 3d 32 69 70 2e 6d 65 22 3e 68 65 6c 70 40 32 69 70 2e 6d 65 3c 2f 61 3e 2e 20 3c 62 72 3e 3c 62 72 3e 20 d0 Data Ascii: 22a<link rel="stylesheet" href="classes/style.css" type="text/css" /> Limit of returned objects has been reached. For more information please contact by email help@2ip.me.

Statistics

Behavior



System Behavior

Analysis Process: bP5g4FsSJk.exe PID: **5468**, Parent PID: **2216**

General	
Target ID:	0
Start time:	11:12:11
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\bP5g4FsSJk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bP5g4FsSJk.exe"
Imagebase:	0x400000
File size:	748032 bytes
MD5 hash:	28FB096CBCE32CF1F87719254452014F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.278389009.0000000004235000.00000040.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000000.00000002.278746171.00000000042D0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000000.00000002.278746171.00000000042D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: bP5g4FsSJk.exe PID: **5604**, Parent PID: **5468**

General	
Target ID:	1
Start time:	11:12:18
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\bP5g4FsSJk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bP5g4FsSJk.exe"
Imagebase:	0x400000
File size:	748032 bytes
MD5 hash:	28FB096CBCE32CF1F87719254452014F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.271002067.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.272056178.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.275253694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.275253694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.275253694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.275253694.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000002.281265111.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000002.281265111.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000002.281265111.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000002.281265111.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.273505881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.273505881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.273505881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.273505881.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.272842398.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.272842398.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.272842398.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.272842398.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000001.00000000.274561888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000001.00000000.274561888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000001.00000000.274561888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000001.00000000.274561888.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly