



ID: 626045
Sample Name: b2.exe
Cookbook: default.jbs
Time: 14:32:12
Date: 13/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report b2.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Telegram RAT 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\b2.exe.log 12
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll 12
Static File Info 13
General 13
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 15
Sections 15
Resources 16
Imports 16
Version Infos 16
Network Behavior 16
Statistics 16
Behavior 16
System Behavior 17
Analysis Process: b2.exePID: 4852, Parent PID: 2868 17
General 17
File Activities 17
File Created 17
File Written 17
File Read 18
Analysis Process: b2.exePID: 7148, Parent PID: 4852 19
General 19
File Activities 19

Copyright Joe Security LLC 2022

File Created 19
File Read 20
Disassembly 20

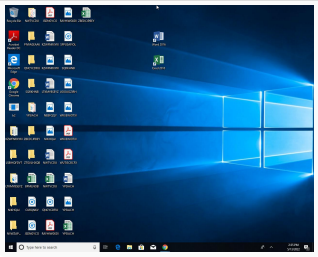
Windows Analysis Report

b2.exe

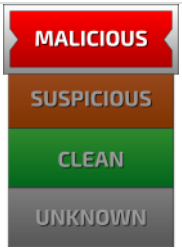
Overview

General Information

Sample Name:	b2.exe
Analysis ID:	626045
MD5:	b23f3235c02c47…
SHA1:	8dbaf4ec74cc27…
SHA256:	46b7d84280339d.
Tags:	AgentTesla exe
Infos:	



Detection



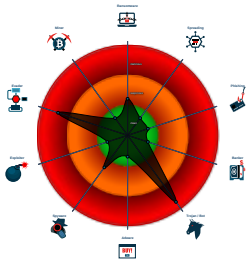
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- .NET source code contains very larg…
- Tries to detect virtualization through…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- b2.exe (PID: 4852 cmdline: "C:\Users\user\Desktop\b2.exe" MD5: B23F3235C02C47B25EA90D9830AA37C7)
  - b2.exe (PID: 7148 cmdline: C:\Users\user\Desktop\b2.exe MD5: B23F3235C02C47B25EA90D9830AA37C7)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1324911145:AAEQBcai78GJtNdHHMwAX0xQhP0p7EcyOuo/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1329186530",
  "Chat URL": "https://api.telegram.org/bot1324911145:AAEQBcai78GJtNdHHMwAX0xQhP0p7EcyOuo/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000000.522653847.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
0000000C.00000000.522653847.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000C.00000002.613014718.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.613014718.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000C.00000000.523738264.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.0.b2.exe.400000.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.0.b2.exe.400000.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
12.0.b2.exe.400000.8.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
12.0.b2.exe.400000.8.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d39:$s1: get_kbok • 0x3166d:$s2: get_CHoo • 0x322c8:$s3: set_passwordIsSet • 0x30b3d:$s4: get_enableLog • 0x35272:$s8: torbrowser • 0x33c4e:$s10: logins • 0x33527:$s11: credential • 0x2ff23:$g1: get_Clipboard • 0x2ff31:$g2: get_Keyboard • 0x2ff3e:$g3: get_Password • 0x3151b:$g4: get_CtrlKeyDown • 0x3152b:$g5: get_ShiftKeyDown • 0x3153c:$g6: get_AltKeyDown
12.0.b2.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking



Yara detected Generic Downloader

Copyright Joe Security LLC 2022

System Summary



Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion



Tries to detect virtualization through RDTSC time measurements

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality



Yara detected Telegram RAT

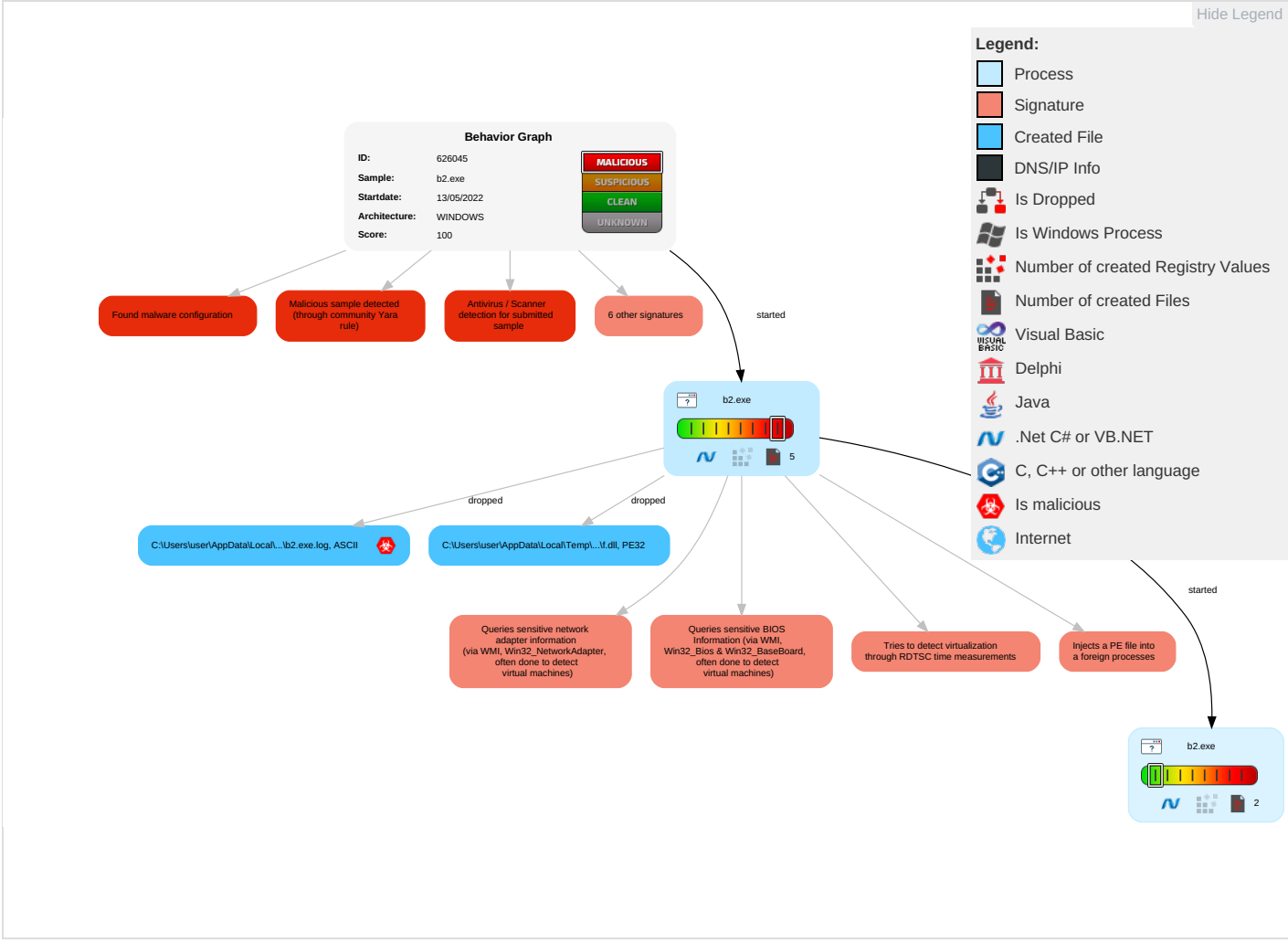
Yara detected AgentTesla

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
1 Valid Accounts	2 1 1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 Masquerading	1 Input Capture	2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 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	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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)	1 1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	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 Disable or Modify Tools	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 3 1 Virtualization/Sandbox Evasion	LSA Secrets	2 1 3 System Information 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	1 1 1 Process Injection	Cached Domain Credentials	System Owner/User 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	1 1 Deobfuscate/Decode Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 Software Packing	/etc/passwd and /etc/shadow	System Network Connections 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.



Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
b2.exe	64%	Virustotal		Browse
b2.exe	75%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
b2.exe	100%	Avira	HEUR/AGEN.1234902	
b2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll	2%	ReversingLabs		

Copyright Joe Security LLC 2022

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.0.b2.exe.e00000.9.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.2.b2.exe.e00000.1.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.5.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.0.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.3.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.13.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
0.0.b2.exe.4c0000.0.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.1.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.b2.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.b2.exe.e00000.7.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.b2.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
12.0.b2.exe.e00000.11.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.2.b2.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.b2.exe.4c0000.0.unpack	100%	Avira	HEUR/AGEN.1234902		Download File
12.0.b2.exe.e00000.2.unpack	100%	Avira	HEUR/AGEN.1234902		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://xqtbof.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://xqtbof.com	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot1324911145:AAEQBcai78GJtNdHHMwAX0xQhP0p7EcyOuo/sendDocumentdocument-----	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot1324911145:AAEQBcai78GJtNdHHMwAX0xQhP0p7EcyOuo/	b2.exe, 00000000.00000003.516030971.00000006637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.515670250.0000000006376000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.516280598.000000000637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.514691789.000000000636D000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.520969631.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.516074359.0000000006A14000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.519825219.0000000006A1A000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.515451731.0000000006376000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.518667846.000000000637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.519966505.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 0000000C.00000000.522653847.000000000402000.00000040.00000400.00020000.00000000.sdmp, b2.exe, 0000000C.00000000.522219203.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	f.dll.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.symauth.com/cps0(	f.dll.0.dr	false		high
http://www.symauth.com/rpa00	f.dll.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	b2.exe, 00000000.00000003.516030971.00000006637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.515670250.0000000006376000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.516280598.000000000637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.514691789.000000000636D000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.520969631.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.516074359.0000000006A14000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.519825219.0000000006A1A000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.515451731.0000000006376000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.518667846.000000000637B000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 00000000.00000003.519966505.0000000006A1C000.00000004.00000800.00020000.00000000.sdmp, b2.exe, 0000000C.00000000.522653847.000000000402000.00000040.00000400.00020000.00000000.sdmp, b2.exe, 0000000C.00000000.522219203.000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	f.dll.0.dr	false	• URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	b2.exe, 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626045
Start date and time: 13/05/202214:32:12	2022-05-13 14:32:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	b2.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:	20
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:	mal100.troj.evad.winEXE@3/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.2%) • Quality average: 13.9% • Quality standard deviation: 12.9%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fp-afd.azureedge.us, client.wns.windows.com, store-images.s-microsoft.com, login.live.com, fp-vp.azureedge.net, sls.update.microsoft.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, b-ring.msedge.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:33:26	API Interceptor	434x Sleep call for process: b2.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\b2.exe.log

Process:	C:\Users\user\Desktop\b2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1976
Entropy (8bit):	5.3569395659576475
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvGHKogHG1qHj:iqXeqm00YqhQnouRqjntIxHeqz+qogmm
MD5:	D1F580650522B7EBD7F438FD6B22F339
SHA1:	768BA6465A6C6107AC504EC2E254F090021EB643
SHA-256:	8280C0A16B5638C762196E6C892BF0940FF9C94435407C66992DA9D592999910
SHA-512:	BE90D7CD9009EF4BB5DE65E64CE522CBEFE3070386D937CCEACFB85E949CA39F954DD5808593D1A4FB806E990E61D465E83B87B80CD2540CF1CE80A0B18470C
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll

Process:	C:\Users\user\Desktop\b2.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	96664
Entropy (8bit):	5.567444078679915
Encrypted:	false
SSDEEP:	1536:JKQ7ZLTFq31bfnHSukoY1IPtan1sBrGxEm5g:JKc/FM1bfnyNNdkrGxJg
MD5:	14FF402962AD21B78AE0B4C43CD1F194
SHA1:	F8A510EB26666E875A5BDD1CADAD40602763AD72
SHA-256:	FB9646CB956945BDC503E69645F6B5316D3826B780D3C36738D6B944E884D15B
SHA-512:	DAA7A08BF3709119A944BCE28F6EBDD24E54A22B18CD9F86A87873E958DF121A3881DCDD5E162F6B4E543238C7AEF20F657C9830DF01D4C79290F7C9A4FCC5B
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Reputation:	moderate, very likely benign file

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....jr..jr..jr..8...ir.....kr.....cr..jr..9r..8...kr.....sr.....kr....x.kr..jr..kr..... kr..Richjr.....PE..L...5 .\.....!.....F.....0.....Z.....@.....C.....0b..d.....b.....4...`A..8.....x7..@..... .....`..0....p..`.....text...h..... ..`.rdata.....0.....".....@..@.data.....P.....:.....@....idata.....`.....<.....@..@.didat..a...p.....J..... ..@....00cfg.....N.....@..@.rsrc.....P.....@..@.reloc.....X.....@..B.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.404995176366941
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	b2.exe
File size:	410624
MD5:	b23f3235c02c47b25ea90d9830aa37c7
SHA1:	8dbaf4ec74cc2710582157100afe98ff9158d994
SHA256:	46b7d84280339d0b887a8e225d0649e1fcf86302bd553c33716b9c42d3894cc7
SHA512:	c60f1880fd35d086055c285f4c9002c0a75088a2cff0927985b8c2ae59f708bf93f100c17bf9c2baeeb7d265ca2e23c7fda1bd6981495ae82cbc0ad080667558
SSDEEP:	12288:k9D4fqRBdy4r3XyMb6U0t3TtUcIlXlWC:+fdNXPmPCJlXl
TLSH:	D2945A70F883445DC97B87F2616744F0F5B915C6FB400E0D61EA73388E1BA6BA39E16A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X`.^.....8.....W... ...`....@.. .....`.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4657ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5EAB6058 [Thu Apr 30 23:33:44 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x65778	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0x622	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Copyright Joe Security LLC 2022

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x637d4	0x63800	False	0.669809005967	data	7.42416946268	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x622	0x800	False	0.36181640625	data	3.65899044286	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x660a0	0x398	data		
RT_MANIFEST	0x66438	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

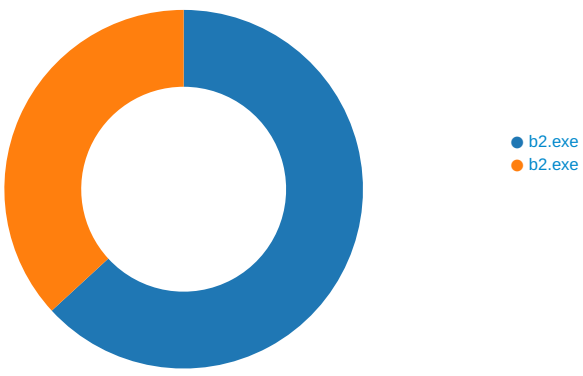
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014 - 2020
Assembly Version	0.0.0.0
InternalName	009273620200110_pdf.exe
FileVersion	9.13.18.22
CompanyName	u{5/3x9e*:6vi$01m?a_
Comments	3h:=2s8g%;0mv[69j!i/7&
ProductName	2e=y)4+3u7z~*
ProductVersion	9.13.18.22
FileDescription	2e=y)4+3u7z~*
OriginalFilename	009273620200110_pdf.exe

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: b2.exe PID: **4852**, Parent PID: **2868**

General

Target ID:	0
Start time:	14:33:23
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\b2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\b2.exe"
Imagebase:	0x4c0000
File size:	410624 bytes
MD5 hash:	B23F3235C02C47B25EA90D9830AA37C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6DC3CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC3CF06	unknown
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1ABEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C1A1E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\b2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF4C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\19f93e2a-4d97-4e0c-ade5-972e41ee6cf8\f.dll	0	96664	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 2e 13 fd fd 6a 72 fd fd 6a 72 fd fd 6a 72 fd fd 38 1a fd fd 69 72 fd fd 05 16 fd fd 6b 72 fd fd 05 16 fd fd 63 72 fd fd 6a 72 fd fd 39 72 fd fd 38 1a fd fd 6b 72 fd fd fd 1b fd fd 73 72 fd fd fd 1b fd fd 6b 72 fd fd fd 1b 78 fd 6b 72 fd fd 6a 72 10 fd 6b 72 fd fd fd 1b fd fd 6b 72 fd fd 52 69 63 68 6a 72 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08	MZ@!L!This program cannot be run in DOS mode.$.jrjrjr8irkrcr jr9r8krsrkrxkrjrkrkrRichjrPEL	success or wait	1	6C1A1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\b2.exe.log	0	1976	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa 3cd3e0ba98b5ebddbbc72e6\System .ni.dll",03,"PresentationCore, Version=	success or wait	1	6DF4C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB703DE	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	unknown	523400	success or wait	1	72B8B80F	ReadFile

Analysis Process: b2.exe PID: **7148**, Parent PID: **4852**

General

Target ID:	12
Start time:	14:34:41
Start date:	13/05/2022
Path:	C:\Users\user\Desktop\b2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\b2.exe
Imagebase:	0xe00000
File size:	410624 bytes
MD5 hash:	B23F3235C02C47B25EA90D9830AA37C7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.522653847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.522653847.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.613014718.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.613014718.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.523738264.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.523738264.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.523078417.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.523078417.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000000.522219203.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000000.522219203.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 0000000C.00000002.615030457.00000000034D1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6DC3CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC3CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC15705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC1CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC15705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1A1B4F	ReadFile

Disassembly

No disassembly