ID: 680351
Sample Name: Document.exe
Cookbook: default.jbs
Time: 12:54:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

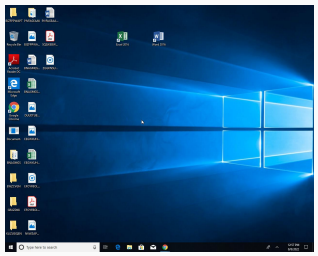
Windows Analysis Report

Document.exe

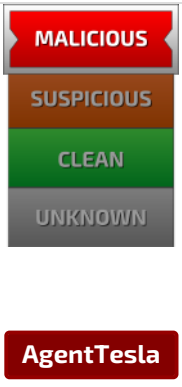
Overview

General Information

Sample Name:	Document.exe
Analysis ID:	680351
MD5:	7ed91a8a05d340.
SHA1:	370e2c4ed3a4ff0..
SHA256:	7e525faf627cca0..
Tags:	agenttesla exe
Infos:	



Detection



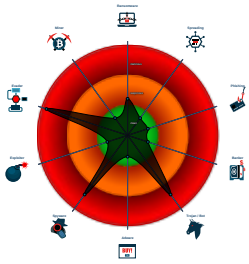
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Document.exe (PID: 5756 cmdline: "C:\Users\user\Desktop\Document.exe" MD5: 7ED91A8A05D340670440C48390AABA1C)
  - Document.exe (PID: 5156 cmdline: C:\Users\user\Desktop\Document.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
  - Document.exe (PID: 4140 cmdline: C:\Users\user\Desktop\Document.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
  - Document.exe (PID: 5076 cmdline: C:\Users\user\Desktop\Document.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
  - Document.exe (PID: 6128 cmdline: C:\Users\user\Desktop\Document.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
- InxbcD.exe (PID: 2136 cmdline: "C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe" MD5: 7ED91A8A05D340670440C48390AABA1C)
  - InxbcD.exe (PID: 4684 cmdline: C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
  - InxbcD.exe (PID: 3396 cmdline: C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
- InxbcD.exe (PID: 5532 cmdline: "C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe" MD5: 7ED91A8A05D340670440C48390AABA1C)
  - InxbcD.exe (PID: 1656 cmdline: C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe MD5: 7ED91A8A05D340670440C48390AABA1C)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "moni@seara-br.co",
  "Password": "eTLvLmQ0",
  "Host": "us2.smtp.mailhostbox.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.284409305.0000000002533000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.286387486.000000000277A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000012.00000002.356439070.0000000002E2A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 23 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Document.exe.3655e58.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Document.exe.3655e58.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Document.exe.3655e58.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30c9c:$s10: logins • 0x30703:$s11: credential • 0x2cce8:$g1: get_Clipboard • 0x2ccf6:$g2: get_Keyboard • 0x2cd03:$g3: get_Password • 0x2dfe2:$g4: get_CtrlKeyDown • 0x2dff2:$g5: get_ShiftKeyDown • 0x2e003:$g6: get_AltKeyDown
0.2.Document.exe.3655e58.6.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e3bf:$a13: get_DnsResolver • 0x2cbe1:$a20: get_LastAccessed • 0x2ed69:$a27: set_InternalServerPort • 0x2f082:$a30: set_GuidMasterKey • 0x2cce8:$a33: get_Clipboard • 0x2ccf6:$a34: get_Keyboard • 0x2dff2:$a35: get_ShiftKeyDown • 0x2e003:$a36: get_AltKeyDown • 0x2cd03:$a37: get_Password • 0x2d7a2:$a38: get_PasswordHash • 0x2e7d7:$a39: get_DefaultCredentials
0.2.Document.exe.3621838.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 22 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

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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 AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

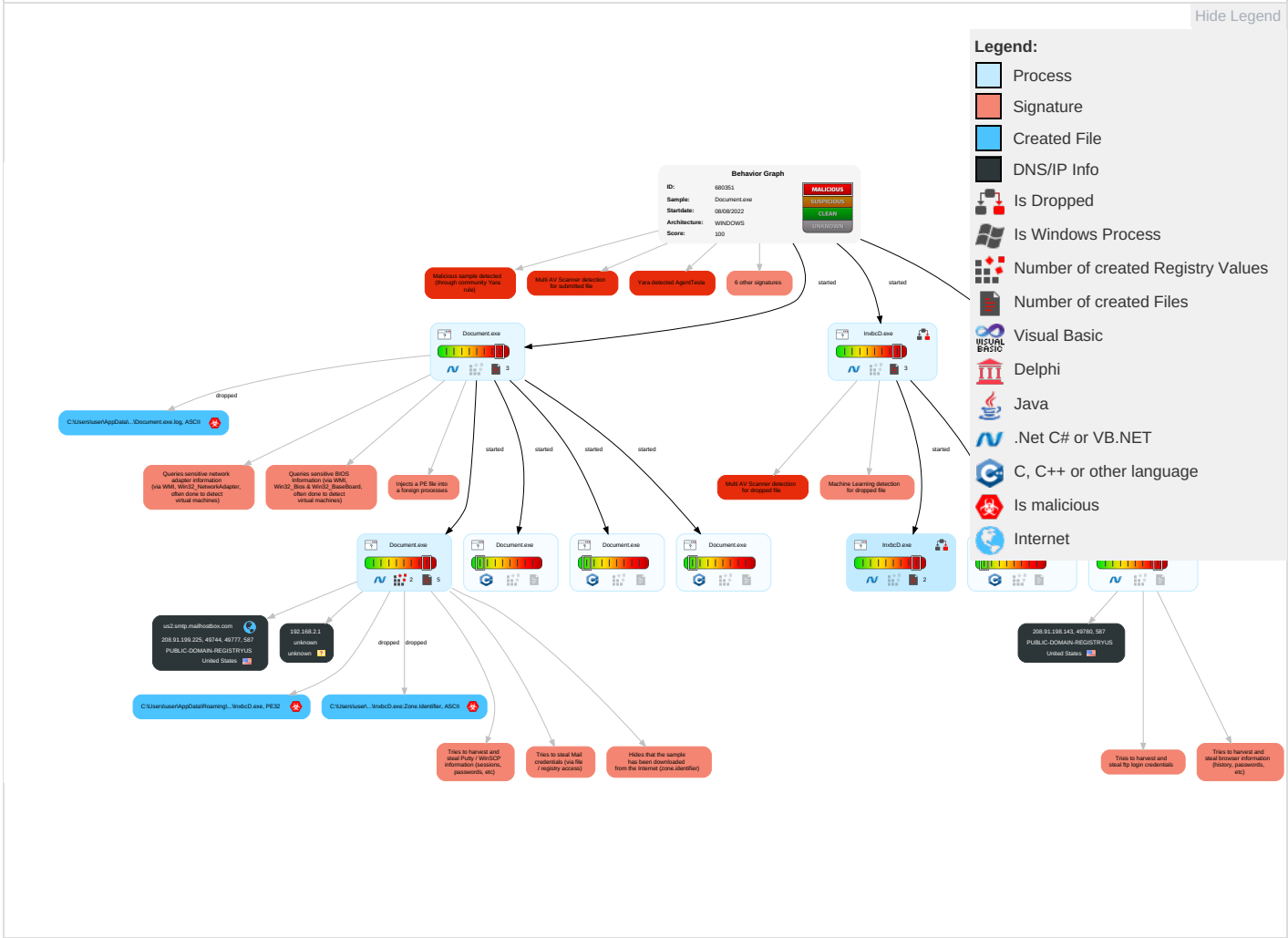
Yara detected AgentTesla

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
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	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 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 Query Registry	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masqueradi ng	LSA Secrets	1 3 1 Virtualizatio n/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic ation		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.commo n	Rc.commo n	1 3 1 Virtualizatio n/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic ation	Jamming or Denial of Service		Abuse Accessibilit y Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Manageme nt	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromis e	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	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

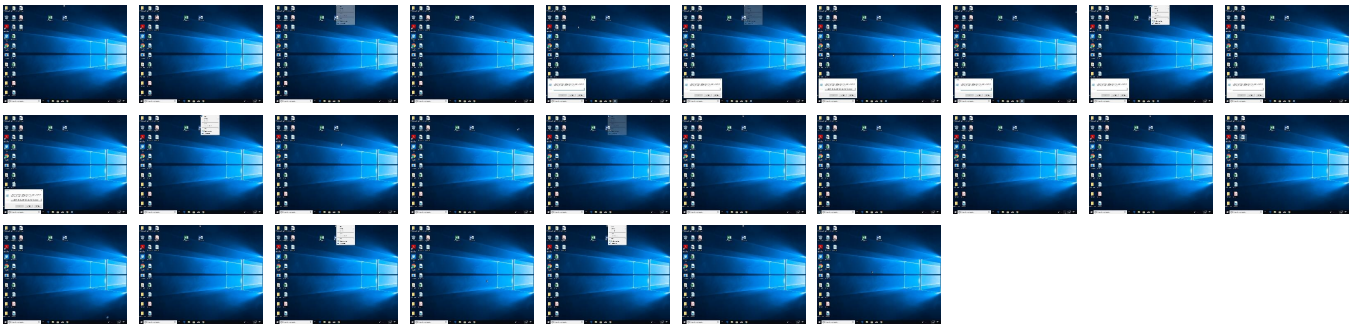
Behavior Graph



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
Document.exe	28%	Virustotal		Browse
Document.exe	17%	ReversingLabs		
Document.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	28%	Virustotal		Browse
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	17%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.Document.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://api.ipify.org%appdata	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://JaRAdc.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://0PYcqQo9t3HlEFYDO.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high

URLs from Memory and Binaries

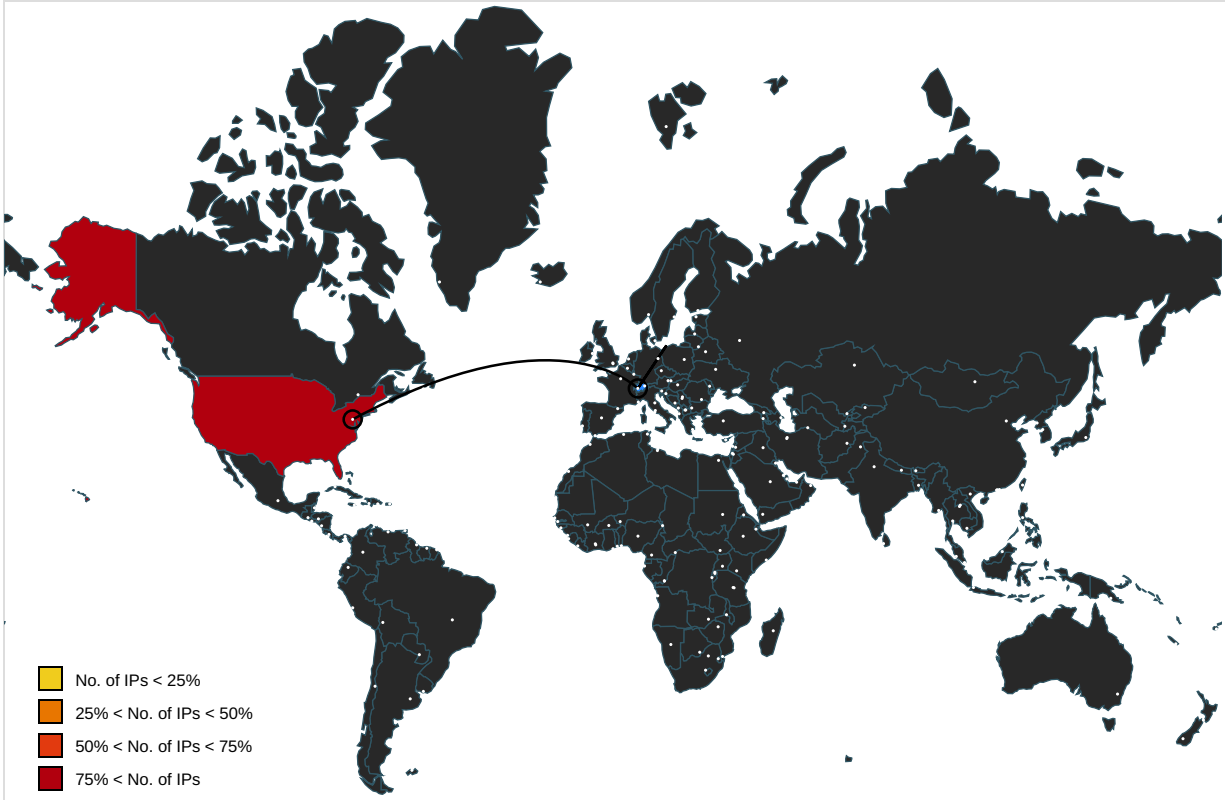
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Document.exe, 00000008.00000002.56803125 5.0000000006872000.00000004.00000800.000 20000.00000000.sdmp, Document.exe, 00000 008.00000002.551388083.000000000363F000. 00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.52074030 5.0000000000DD6000.00000004.00000020.000 20000.00000000.sdmp, InxbcD.exe, 0000001 8.00000002.550192268.0000000002F20000.00 000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.522158378. 0000000000E12000.00000004.00000020.00020 000.00000000.sdmp, InxbcD.exe, 00000019. 00000002.523803830.0000000000DD4000.0000 0004.00000020.00020000.00000000.sdmp, In xbcD.exe, 00000019.00000002.572962420.00 00000006680000.00000004.00000800.0002000 0.00000000.sdmp, InxbcD.exe, 00000019.00 000002.553154806.0000000002D11000.000000 04.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	Document.exe, 00000008.00000002.52707020 8.00000000032E1000.00000004.00000800.000 20000.00000000.sdmp, InxbcD.exe, 0000001 8.00000002.524941648.0000000002BC1000.00 000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.529474477. 00000000029BC000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	Document.exe, 00000008.00000002.56803125 5.0000000006872000.00000004.00000800.000 20000.00000000.sdmp, Document.exe, 00000 008.00000002.551388083.000000000363F000. 00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.52074030 5.0000000000DD6000.00000004.00000020.000 20000.00000000.sdmp, InxbcD.exe, 0000001 8.00000002.550192268.0000000002F20000.00 000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.522158378. 0000000000E12000.00000004.00000020.00020 000.00000000.sdmp, InxbcD.exe, 00000019. 00000002.523803830.0000000000DD4000.0000 0004.00000020.00020000.00000000.sdmp, In xbcD.exe, 00000019.00000002.572962420.00 00000006680000.00000004.00000800.0002000 0.00000000.sdmp, InxbcD.exe, 00000019.00 000002.553154806.0000000002D11000.000000 04.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	Document.exe, 00000008.00000002.55138808 3.000000000363F000.00000004.00000800.000 20000.00000000.sdmp, InxbcD.exe, 0000001 8.00000002.550192268.0000000002F20000.00 000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.553154806. 0000000002D11000.00000004.00000800.00020 000.00000000.sdmp	false		high
http://https://api.ipify.org%appdata	InxbcD.exe, 00000019.00000002.529474477. 00000000029BC000.00000004.00000800.00020 000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fontbureau.com/designers?	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	Document.exe, 00000008.00000002.527070208.00000000032E1000.00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.524941648.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	InxbcD.exe, 00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://JaRAdc.com	InxbcD.exe, 00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Document.exe, 00000000.00000002.290637100.0000000006562000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0A	Document.exe, 00000008.00000002.568031255.0000000006872000.00000004.00000800.00020000.00000000.sdmp, Document.exe, 00000008.00000002.551388083.000000000363F000.00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.520740305.0000000000DD6000.00000004.00000020.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.550192268.0000000002F20000.00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000018.00000002.522158378.0000000000E12000.00000004.00000020.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.523803830.0000000000DD4000.00000004.00000020.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.572962420.0000000006680000.00000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.553154806.0000000002D11000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Document.exe, 00000000.00000002.29063710 0.0000000006562000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	Document.exe, 00000008.00000002.52707020 8.00000000032E1000.00000004.00000800.000 20000.00000000.sdmp, InxbcD.exe, 0000001 8.00000002.524941648.0000000002BC1000.00 000004.00000800.00020000.00000000.sdmp, InxbcD.exe, 00000019.00000002.529474477. 00000000029BC000.00000004.00000800.00020 000.00000000.sdmp	false	• URL Reputation: safe	low
http://0PYcqQo9t3HlEFYDO.org	InxbcD.exe, 00000019.00000002.552920598. 0000000002D0B000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
208.91.199.225	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680351
Start date and time: 08/08/202212:54:10	2022-08-08 12:54:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Document.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:	35
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.spyw.evad.winEXE@17/4@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 23.213.164.66
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:55:23	API Interceptor	674x Sleep call for process: Document.exe modified
12:55:34	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run InxbcD C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
12:55:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run InxbcD C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
12:55:51	API Interceptor	698x Sleep call for process: InxbcD.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\Document.exe.log

Process:	C:\Users\user\Desktop\Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InxbcD.exe.log

Process:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427

SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..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..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe

Process:	C:\Users\user\Desktop\Document.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	823808
Entropy (8bit):	7.781001148520893
Encrypted:	false
SSDEEP:	24576:FFxgV10lgTyhAvtvFhdTOZPe9IbUDHDl:pgVWUyhAvtvFhdTY7U
MD5:	7ED91A8A05D340670440C48390AABA1C
SHA1:	370E2C4ED3A4FF0F6FC6BC6D634AD29D7690AE0A
SHA-256:	7E525FAF627CCA0905153E9AB2D1308006466097A041395573E2FF31C58B69A7
SHA-512:	569077E17AC42E6BE529A7A22E45A8D947A1C5DFC62BAF172C59E81C40DCA99264DFC0CB7B257068A26C560EAE24C04A4F3E6035702541384382041 8F80280E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 28%, Browse • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..."..b.....0..... .....@.. ..... .@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....S..(U.....0..k.....%.r...p.%.r[..p.%.ri..p.}.....}.....(.....(.....{.....o.....{.....o.....~....t.....{....(....&*&.. (.....*..*.0.....{....o.....o.....sL.....o.....o....o....(.....oD.....o.....9.....{....o ...o!.....{....o"....o#...r...p.o$...oU...o%....M...(&...o'.....8.....o$...oU.....o(...o)...s*.....o.....o $...oU.....o(...o+...o,...o-...&.o.....o$...oU.....o(...o+...o....o-

C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.781001148520893
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:	Document.exe
File size:	823808
MD5:	7ed91a8a05d340670440c48390aaba1c
SHA1:	370e2c4ed3a4ff0f6fc6bc6d634ad29d7690ae0a
SHA256:	7e525faf627cca0905153e9ab2d1308006466097a041395573e2ff31c58b69a7
SHA512:	569077e17ac42e6be529a7a22e45a8d947a1c5dfc62baf172c59e81c40dca99264dfc0cb7b257068a26c560eae24c04a4f3e6035702541384382041 8f80280ee
SSDEEP:	24576:FFxgV10lgTyhAvtvFhdTOZPe9IbUDHDl:pgVWUyhAvtvFhdTY7U
TLSH:	BE05BE5BBF147708C5A36AB4EE0BB96267F61C5D3135E0B83E547C4A4AFF301E52242A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".b.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ca9f2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0BB22 [Mon Aug 8 07:28:34 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xca9a0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x3d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	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
.text	0x2000	0xc89f8	0xc8a00	False	0.8177667445482866	data	7.787205536847968	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x3d0	0x400	False	0.3837890625	data	3.0440429899176986	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

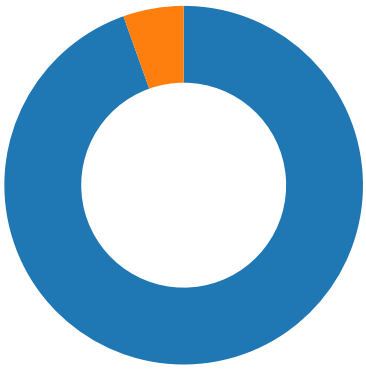
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xcc058	0x374	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:55:46.548738956 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:46.716939926 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:46.717205048 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:50.893640995 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:50.893995047 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.061827898 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.062006950 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.062292099 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.230369091 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.275805950 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.444633007 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.444693089 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.444734097 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.444762945 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.444789886 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.444809914 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.448621988 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.543545008 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.614767075 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:51.657484055 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:51.826605082 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.043581963 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.085932970 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.254144907 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.255610943 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.426814079 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.430459023 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.603749990 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.604528904 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.773387909 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.773827076 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:52.965123892 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:52.976968050 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:53.145898104 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:53.147037029 CEST	49744	587	192.168.2.3	208.91.199.225

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:55:53.147173882 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:53.147833109 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:53.147933006 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:55:53.314980030 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:53.317739964 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:53.440301895 CEST	587	49744	208.91.199.225	192.168.2.3
Aug 8, 2022 12:55:53.637490988 CEST	49744	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:34.683269024 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:34.849540949 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:34.851684093 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:35.456537008 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:35.547338009 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:35.593027115 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:35.759546995 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:35.759733915 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:35.844222069 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:35.846904993 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.013546944 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.234888077 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.406636953 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.572982073 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.573018074 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.573040962 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.573056936 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.573084116 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.573133945 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.575385094 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.735094070 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:36.741107941 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:36.844441891 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:37.074443102 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:37.241643906 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:37.344326973 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:39.497345924 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:39.664825916 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:39.665436983 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:39.835731030 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:39.836378098 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.006812096 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.007275105 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.175622940 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.178391933 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.369616032 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.370012045 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.537209034 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.538456917 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.538657904 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.538769960 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.538887978 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:40.704484940 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.706026077 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:40.835095882 CEST	587	49777	208.91.199.225	192.168.2.3
Aug 8, 2022 12:56:41.047856092 CEST	49777	587	192.168.2.3	208.91.199.225
Aug 8, 2022 12:56:49.444216013 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:49.610522032 CEST	587	49780	208.91.198.143	192.168.2.3
Aug 8, 2022 12:56:49.612788916 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:50.155709028 CEST	587	49780	208.91.198.143	192.168.2.3
Aug 8, 2022 12:56:50.156405926 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:50.322803974 CEST	587	49780	208.91.198.143	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:56:50.322856903 CEST	587	49780	208.91.198.143	192.168.2.3
Aug 8, 2022 12:56:50.323129892 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:50.490689039 CEST	587	49780	208.91.198.143	192.168.2.3
Aug 8, 2022 12:56:50.548585892 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:50.574191093 CEST	49780	587	192.168.2.3	208.91.198.143
Aug 8, 2022 12:56:50.740653038 CEST	587	49780	208.91.198.143	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:55:46.484108925 CEST	57723	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:55:46.509882927 CEST	53	57723	8.8.8.8	192.168.2.3
Aug 8, 2022 12:56:34.583363056 CEST	58625	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:56:34.602864981 CEST	53	58625	8.8.8.8	192.168.2.3
Aug 8, 2022 12:56:49.363284111 CEST	50778	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:56:49.385094881 CEST	53	50778	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:55:46.484108925 CEST	192.168.2.3	8.8.8.8	0xafa7	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:34.583363056 CEST	192.168.2.3	8.8.8.8	0xe8be	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:49.363284111 CEST	192.168.2.3	8.8.8.8	0xa9b6	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:55:46.509882927 CEST	8.8.8.8	192.168.2.3	0xafa7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Aug 8, 2022 12:55:46.509882927 CEST	8.8.8.8	192.168.2.3	0xafa7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Aug 8, 2022 12:55:46.509882927 CEST	8.8.8.8	192.168.2.3	0xafa7	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Aug 8, 2022 12:55:46.509882927 CEST	8.8.8.8	192.168.2.3	0xafa7	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:34.602864981 CEST	8.8.8.8	192.168.2.3	0xe8be	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:34.602864981 CEST	8.8.8.8	192.168.2.3	0xe8be	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:34.602864981 CEST	8.8.8.8	192.168.2.3	0xe8be	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:34.602864981 CEST	8.8.8.8	192.168.2.3	0xe8be	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:49.385094881 CEST	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:49.385094881 CEST	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:49.385094881 CEST	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Aug 8, 2022 12:56:49.385094881 CEST	8.8.8.8	192.168.2.3	0xa9b6	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

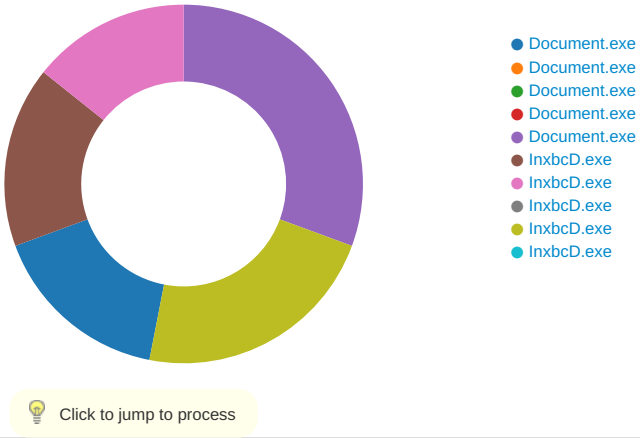
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 12:55:50.893640995 CEST	587	49744	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 8, 2022 12:55:50.893995047 CEST	49744	587	192.168.2.3	208.91.199.225	EHLO 035347

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 8, 2022 12:55:51.062006950 CEST	587	49744	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Aug 8, 2022 12:55:51.062292099 CEST	49744	587	192.168.2.3	208.91.199.225	STARTTLS
Aug 8, 2022 12:55:51.230369091 CEST	587	49744	208.91.199.225	192.168.2.3	220 2.0.0 Ready to start TLS
Aug 8, 2022 12:56:35.456537008 CEST	587	49777	208.91.199.225	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 8, 2022 12:56:35.593027115 CEST	49777	587	192.168.2.3	208.91.199.225	EHLO 035347
Aug 8, 2022 12:56:35.759733915 CEST	587	49777	208.91.199.225	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Aug 8, 2022 12:56:35.846904993 CEST	49777	587	192.168.2.3	208.91.199.225	STARTTLS
Aug 8, 2022 12:56:36.013546944 CEST	587	49777	208.91.199.225	192.168.2.3	220 2.0.0 Ready to start TLS
Aug 8, 2022 12:56:50.155709028 CEST	587	49780	208.91.198.143	192.168.2.3	220 us2.outbound.mailhostbox.com ESMTP Postfix
Aug 8, 2022 12:56:50.156405926 CEST	49780	587	192.168.2.3	208.91.198.143	EHLO 035347
Aug 8, 2022 12:56:50.322856903 CEST	587	49780	208.91.198.143	192.168.2.3	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Aug 8, 2022 12:56:50.323129892 CEST	49780	587	192.168.2.3	208.91.198.143	STARTTLS
Aug 8, 2022 12:56:50.490689039 CEST	587	49780	208.91.198.143	192.168.2.3	220 2.0.0 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: Document.exe PID: 5756, Parent PID: 5148

General

Target ID:	0
Start time:	12:55:11
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Document.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Document.exe"
Imagebase:	0x20000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.284409305.0000000002533000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286387486.000000000277A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.287031983.00000000035EB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.287031983.00000000035EB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.287031983.00000000035EB000.00000004.00000800.00020000.00000000.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	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Document.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D10C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Document.exe.log	0	1308	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D10C907	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile

Analysis Process: Document.exe PID: **5156**, Parent PID: **5756**

General

Target ID:	4
Start time:	12:55:25
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Document.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Document.exe
Imagebase:	0xc0000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: Document.exe PID: **4140**, Parent PID: **5756**

General	
Target ID:	5
Start time:	12:55:25
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Document.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Document.exe
Imagebase:	0x50000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Document.exe PID: **5076**, Parent PID: **5756**

General	
Target ID:	6
Start time:	12:55:26
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Document.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Document.exe
Imagebase:	0x3a0000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Document.exe PID: **6128**, Parent PID: **5756**

General	
Target ID:	8
Start time:	12:55:27
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Document.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Document.exe
Imagebase:	0xeb0000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
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: 00000008.00000000.279787688.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000000.279787688.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000008.00000000.279787688.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.527070208.00000000032E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.527070208.00000000032E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Roaming\InxbcD	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BC4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BC4DD66	CopyFileW
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BC4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe:Zone.Identifier	success or wait	1	63D622A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 22 fd fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 06 00 00 00 00 00 00 fd 0c 00 00 20 00 00 00 fd 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL"b0 @ @	success or wait	4	6BC4DD66	CopyFileW
C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6BC4DD66	CopyFileW

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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\05b98e77-fe4c-4961-9081-bc8c3f45dec3	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	InxbcD	unicode	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe	success or wait	1	6BC4646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	InxbcD	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BC4DE2E	RegSetValueExW

Analysis Process: InxbcD.exe PID: **2136**, Parent PID: **3968**

General

Target ID:	18
Start time:	12:55:43
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe"
Imagebase:	0x760000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.356439070.0000000002E2A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.350967308.0000000002BE3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, Virustotal, Browse • Detection: 17%, ReversingLabs
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	6CDFCF06	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	6CDFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InxbcD.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D10C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InxbcD.exe.log	0	1308	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 30 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	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D10C907	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile

Analysis Process: InxbcD.exe PID: **5532**, Parent PID: **3968**

General

Target ID:	21
Start time:	12:55:52
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe"
Imagebase:	0x6e0000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	false
Has administrator privileges:	false
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	6CDFCF06	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	6CDFCF06	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile

Analysis Process: InxbcD.exe PID: **4684**, Parent PID: **2136**

General

Target ID:	22
Start time:	12:55:54
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Imagebase:	0x250000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: InxbcD.exe PID: **3396**, Parent PID: **2136**

General

Target ID:	24
Start time:	12:55:55
Start date:	08/08/2022

Path:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Imagebase:	0x7ff73c930000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.524941648.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.524941648.0000000002BC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6CDFCF06	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	6CDFCF06	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	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CDD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\69a5bb94-495b-4fa8-967b-f04b05c4a6bf	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile

Analysis Process: InxbcD.exe PID: 1656, Parent PID: 5532

General	
Target ID:	25
Start time:	12:56:09
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\InxbcD\InxbcD.exe
Imagebase:	0x520000
File size:	823808 bytes
MD5 hash:	7ED91A8A05D340670440C48390AABA1C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000019.00000002.529474477.00000000029BC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

No disassembly