ID: 831160
Sample Name:
DHL_Express_Shipment_DOC.exe
Cookbook: default.jbs
Time: 07:11:09
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

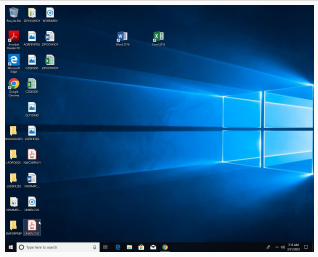
Windows Analysis Report

DHL_Express_Shipment_DOC.exe

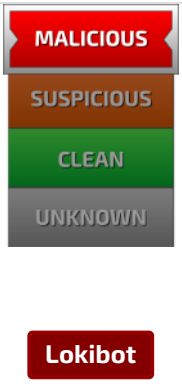
Overview

General Information

Sample Name:	DHL_Express_Shipment_DOC.exe
Analysis ID:	831160
MD5:	370ebdf4ff5036..
SHA1:	cc04ea26c136...
SHA256:	1ebedb652fa27..
Tags:	exe Loki
Infos:	



Detection



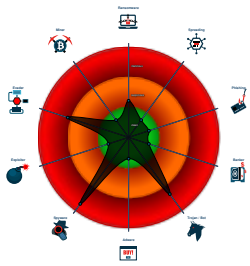
Lokibot

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Yara detected Lokibot
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi...
- Initial sample is a PE file and has a...
- Tries to harvest and steal Putty / W...
- Yara detected aPLib compressed bi...
- Tries to harvest and steal ftp login c...
- Tries to steal Mail credentials (via fi...
- Machine Learning detection for sam...
- C2 URLs / IPs found in malware con...

Classification



Process Tree

- **System is w10x64**
- DHL_Express_Shipment_DOC.exe (PID: 5396 cmdline: C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe MD5: 370EBDF4FF5036C106793994CC851779)
  - DHL_Express_Shipment_DOC.exe (PID: 5364 cmdline: C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe MD5: 370EBDF4FF5036C106793994CC851779)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
Loki Password Stealer (PWS), LokiBot	"Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets." - PhishMeLoki-Bot employs function hashing to obfuscate the libraries utilized. While not all functions are hashed, a vast majority of them are.Loki-Bot accepts a single argument/switch of -u that simply delays execution (sleeps) for 10 seconds. This is used when Loki-Bot is upgrading itself.The Mutex generated is the result of MD5 hashing the Machine GUID and trimming to 24-characters. For example: B7E1C2CC98066B250DDB2123.Loki-Bot creates a hidden folder within the %APPDATA% directory whose name is supplied by the 8th thru 13th characters of the Mutex. For example: %APPDATA%\ C98066\.There can be four files within the hidden %APPDATA% directory at any given time: .exe, .lck, .hdb and .kdb. They will be named after characters 13 thru 18 of the Mutex. For example: 6B250D. Below is the explanation of their purpose:FILE EXTENSIONFILE DESCRIPTION.exeA copy of the malware that will execute every time the user account is logged into.lckA lock file created when either decrypting Windows Credentials or Keylogging to prevent resource conflicts.hdbA database of hashes for data that has already been exfiltrated to the C2 server.kdbA database of keylogger data that has yet to be sent to the C2 serverIf the user is privileged, Loki-Bot sets up persistence within the registry under HKEY_LOCAL_MACHINE. If not, it sets up persistence under HKEY_CURRENT_USER.The first packet transmitted by Loki-Bot contains application data.The second packet transmitted by Loki-Bot contains decrypted Windows credentials.The third packet transmitted by Loki-Bot is the malware requesting C2 commands from the C2 server. By default, Loki-Bot will send this request out every 10 minutes after the initial packet it sent.Communications to the C2 server from the compromised host contain information about the user and system including the username, hostname, domain, screen resolution, privilege level, system architecture, and Operating System.The first WORD of the HTTP Payload represents the Loki-Bot version.The second WORD of the HTTP Payload is the Payload Type. Below is the table of identified payload types:BYTEPAYLOAD TYPE0x26Stolen Cryptocurrency Wallet0x27Stolen Application Data0x28Get C2 Commands from C2 Server0x29Stolen File0x2APOS (Point of Sale?)0x2BKeylogger Data0x2CScreenshotThe 11th byte of the HTTP Payload begins the Binary ID. This might be useful in tracking campaigns or specific threat actors. This value value is typically ckav.ru. If you come across a Binary ID that is different from this, take note!Loki-Bot encrypts both the URL and the registry key used for persistence using Triple DES encryption.The Content-Key HTTP Header value is the result of hashing the HTTP Header values that precede it. This is likely used as a protection against researchers who wish to poke and prod at Loki-Bots C2 infrastructure.Loki-Bot can accept the following instructions from the C2 Server:BYTEINSTRUCTION DESCRIPTION0x00Download EXE & Execute0x01Download DLL & Load #10x02Download DLL & Load #20x08Delete HDB File0x09Start Keylogger0x0AMine & Steal Data0x0EExit Loki-Bot0x0FUpgrade Loki-Bot0x10Change C2 Polling Frequency0x11Delete Executables & ExitSuricata SignaturesRULE SIDRULE NAME2024311ET TROJAN Loki Bot Cryptocurrency Wallet Exfiltration Detected2024312ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M12024313ET TROJAN Loki Bot Request for C2 Commands Detected M12024314ET TROJAN Loki Bot File Exfiltration Detected2024315ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M12024316ET TROJAN Loki Bot Screenshot Exfiltration Detected2024317ET TROJAN Loki Bot Application/Credential Data Exfiltration Detected M22024318ET TROJAN Loki Bot Request for C2 Commands Detected M22024319ET TROJAN Loki Bot Keylogger Data Exfiltration Detected M2	• SWEED • The Gorgon Group • Cobalt	http://blog.reversing.xyz/reversing/2021/06/08/lokibot.htmlhttp://reversing.fun/posts/2021/06/08/lokibot.htmlhttp://reversing.fun/reversing/2021/06/08/lokibot.htmlhttp://www.malware-traffic-analysis.net/2017/06/12/index.htmlhttps://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.lokipws

Malware Configuration

Threatname: Lokibot


```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Lokibot_1	Yara detected Lokibot	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x187f0:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk

Click to see the 7 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.DHL_Express_Shipment_DOC.exe.400000.0.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3.2.DHL_Express_Shipment_DOC.exe.400000.0.raw.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
3.2.DHL_Express_Shipment_DOC.exe.400000.0.raw.unpack	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
3.2.DHL_Express_Shipment_DOC.exe.400000.0.raw.unpack	INDICATOR_SUSPICIOUS_GENInfoStealer	Detects executables containing common artifcats observed in infostealers	ditekSHen	• 0x17936:$f1: FileZilla\recentservers.xml • 0x17976:$f2: FileZilla\sitemanager.xml • 0x15be6:$b2: Mozilla\Firefox\Profiles • 0x15950:$b3: Software\Microsoft\Internet Explorer\IntelliForms\Storage2 • 0x15afa:$s4: logins.json • 0x169a4:$s6: wand.dat • 0x15424:$a1: username_value • 0x15414:$a2: password_value • 0x15a5f:$a3: encryptedUsername • 0x15acc:$a3: encryptedUsername • 0x15a72:$a4: encryptedPassword • 0x15ae0:$a4: encryptedPassword
3.2.DHL_Express_Shipment_DOC.exe.400000.0.raw.unpack	Windows_Trojan_Lokibot_1f885282	unknown	unknown	• 0x187f0:$a1: MAC=%02X%02X%02XINSTALL=%08X%08Xk

Click to see the 11 entries

Sigma Signatures

⊘ **No Sigma rule has matched**

Snort Signatures

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212 −

Timestamp:	192.168.2.464.227.48.21249700802024313 03/21/23-07:13:25.127064

SID:	2024313
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249698802021641 03/21/23-07:13:22.578656
SID:	2021641
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249699802024318 03/21/23-07:13:23.800015
SID:	2024318
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249698802024312 03/21/23-07:13:22.578656
SID:	2024312
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249700802024318 03/21/23-07:13:25.127064
SID:	2024318
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249699802021641 03/21/23-07:13:23.800015
SID:	2021641
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249701802021641 03/21/23-07:13:27.165442
SID:	2021641
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212

Timestamp:	192.168.2.464.227.48.21249701802024313 03/21/23-07:13:27.165442
SID:	2024313
Source Port:	49701
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249698802024317 03/21/23-07:13:22.578656
SID:	2024317
Source Port:	49698
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249701802024318 03/21/23-07:13:27.165442
SID:	2024318
Source Port:	49701
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249699802024313 03/21/23-07:13:23.800015
SID:	2024313
Source Port:	49699
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249697802024317 03/21/23-07:13:21.229954
SID:	2024317
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249702802024313 03/21/23-07:13:28.916498
SID:	2024313
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249702802021641 03/21/23-07:13:28.916498
SID:	2021641
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Request for C2 Commands Detected M2 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249702802024318 03/21/23-07:13:28.916498
SID:	2024318
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	
Timestamp:	192.168.2.464.227.48.21249697802021641 03/21/23-07:13:21.229954

SID:	2021641
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot User-Agent (Charon/Inferno) - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	−
Timestamp:	192.168.2.464.227.48.21249700802021641 03/21/23-07:13:25.127064
SID:	2021641
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1 - Source IP: 192.168.2.4 - Destination IP: 64.227.48.212	−
Timestamp:	192.168.2.464.227.48.21249697802024312 03/21/23-07:13:21.229954
SID:	2024312
Source Port:	49697
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

Yara detected aPLib compressed binary

Stealing of Sensitive Information

Yara detected Lokibot

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

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

Tries to harvest and steal ftp login credentials

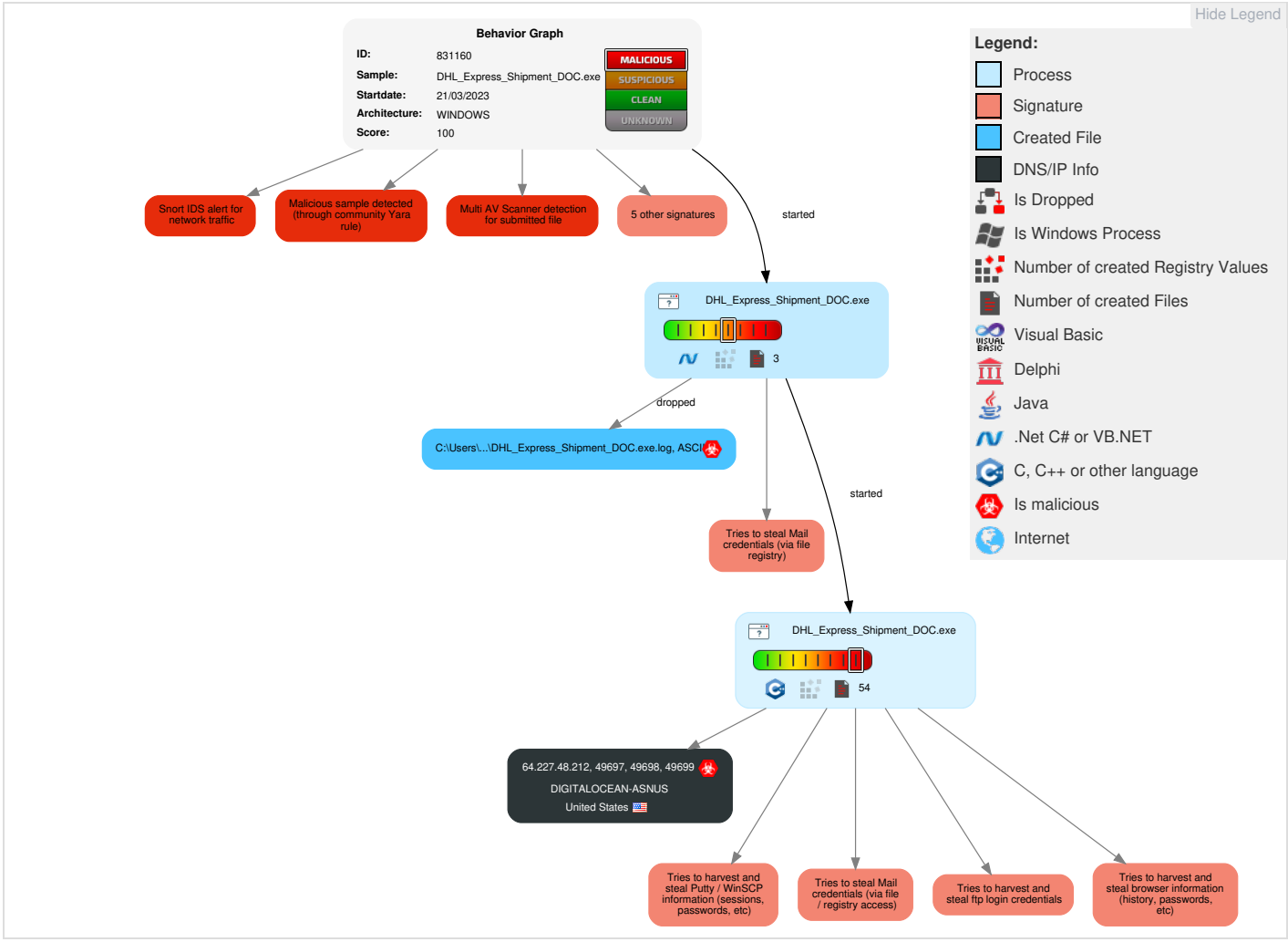
Tries to steal Mail credentials (via file registry)

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

Mitre Att&ck Matrix

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

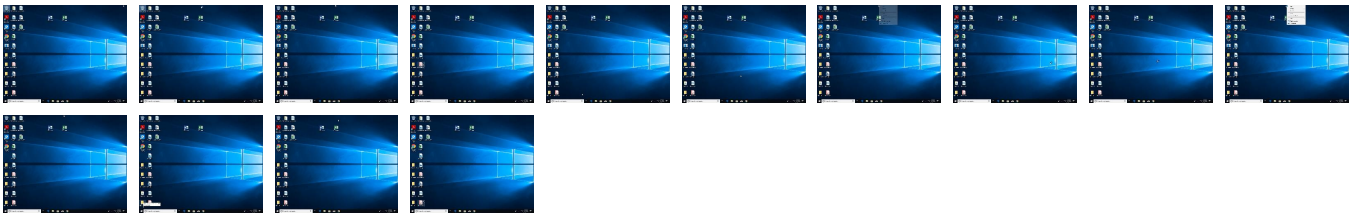
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_Express_Shipment_DOC.exe	19%	ReversingLabs		
DHL_Express_Shipment_DOC.exe	30%	Virustotal		Browse
DHL_Express_Shipment_DOC.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.DHL_Express_Shipment_DOC.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://robertmario.is/?feed=rss2	0%	Avira URL Cloud	safe	
http://robertmario.is/index.php?rest_route=/	0%	Avira URL Cloud	safe	
http://64.227.48.212/?page_id=215360	0%	Avira URL Cloud	safe	
http://robertmario.is/?feed=comments-rss2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

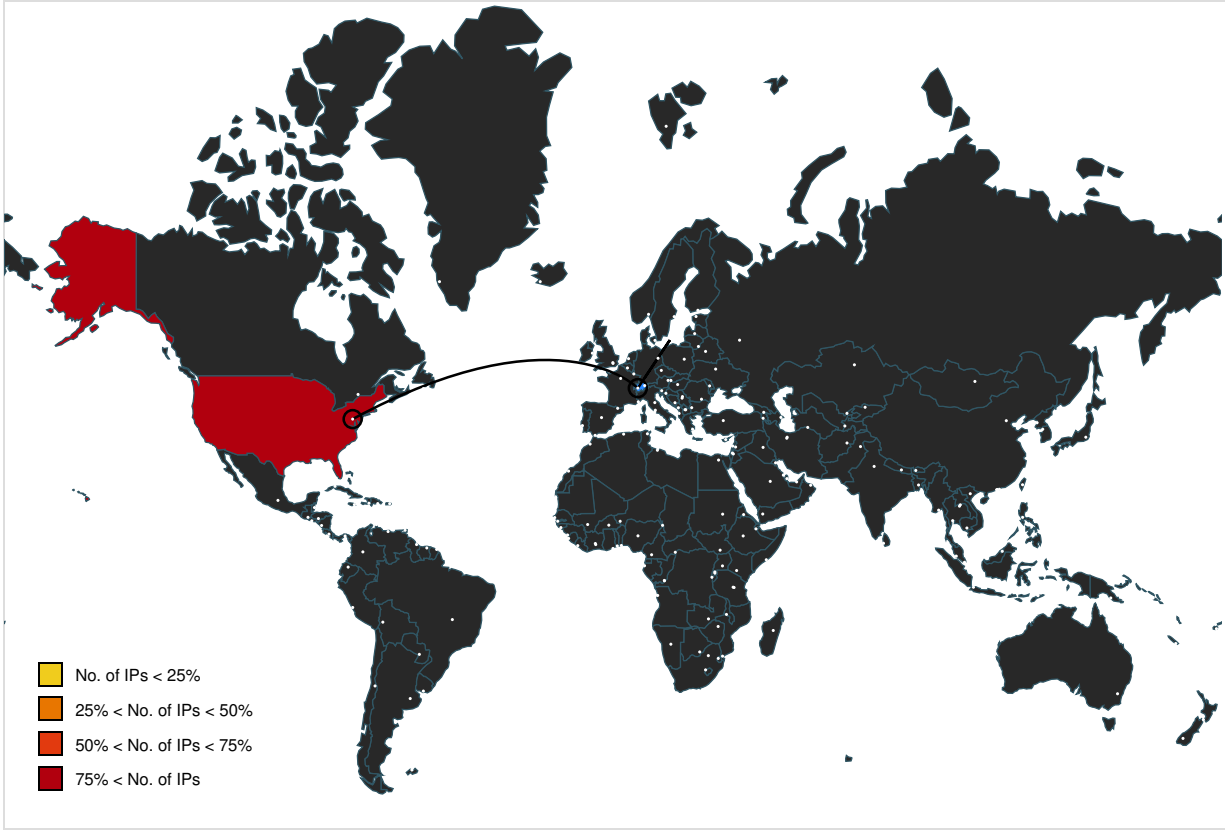
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://64.227.48.212/?page_id=215360	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://robertmario.is/?feed=rss2	DHL_Express_Shipment_DOC.exe, 00000003.00000002.486703959.0000000001678000.00000004.00000020.00020000.00000000.sdmp, DHL_Express_Shipment_DOC.exe, 00000003.00000002.487142894.0000000003519000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://robertmario.is/?feed=comments-rss2	DHL_Express_Shipment_DOC.exe, 00000003.00000002.486703959.0000000001678000.00000004.00000020.00020000.00000000.sdmp, DHL_Express_Shipment_DOC.exe, 00000003.00000002.487142894.0000000003519000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ibsensoftware.com/	DHL_Express_Shipment_DOC.exe, DHL_Express_Shipment_DOC.exe, 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://robertmario.is/index.php?rest_route=/	DHL_Express_Shipment_DOC.exe, 00000003.00000002.486703959.0000000001678000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.w.org/	DHL_Express_Shipment_DOC.exe, 00000003.00000002.486703959.0000000001678000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.227.48.212	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831160
Start date and time:	2023-03-21 07:11:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	4
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
Sample file name:	DHL_Express_Shipment_DOC.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 97.9% (good quality ratio 93.9%) • Quality average: 77% • Quality standard deviation: 28.6%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:13:18	API Interceptor	4x Sleep call for process: DHL_Express_Shipment_DOC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C

SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck

Process:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
File Type:	data
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbq:4
MD5:	8CB7B7F28464C3FCBAE8A10C46204572
SHA1:	767FE80969EC2E67F54CC1B6D383C76E7859E2DE
SHA-256:	ED5E3DCEB0A1D68803745084985051C1ED41E11AC611DF8600B1A471F3752E96
SHA-512:	9BA84225FDB6C0FD69AD99B69824EC5B8D2B8FD3BB4610576DB4AD79ADF381F7F82C4C9522EC89F7171907577FAF1B4E70B82364F516CF8BBFED99D2ADEA43AF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.414207480565285
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHL_Express_Shipment_DOC.exe
File size:	852480
MD5:	370ebdf4ff5036c106793994cc851779

SHA1:	cc04ea26c1364b9a058b55c8697a49e1c7e16970
SHA256:	1ebedb652fa27423240c3efa860e7551958811120737ee5d3ea7badf671fbacf
SHA512:	63c2c4208a7d9c3c1176167f2c015c1a0bcb8b90cbb55cbb879aa93d0d7e0e128c1662273dfb73776c29466cf87c83f84be3acd48f871a125bc2189efafd3803
SSDEEP:	12288:0wRZRbIx8nvRW3NVuf7sBF84DpHCojUzQO7auRJ0CXfmv5gn:02+xuv89V4gc4DVhhuRax
TLSH:	F00507435EBB5085E8B70F38547A76980B34E953BDD9903B3CC9B61A8FFA68360463D1
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...[..d..............0.................. ... .@.. ....`............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d16ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6419125B [Tue Mar 21 02:11:39 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd1660	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x5d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd161d	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcf6b4	0xcf800	False	0.7503800357680723	data	7.418461164070656	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5d8	0x600	False	0.4309895833333333	data	4.156248863214128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd20a0	0x34c	data		
RT_MANIFEST	0xd23ec	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.464.227.48.212 49700802024313 03/21/23-07:13:25.127064	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49700	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49698802021641 03/21/23-07:13:22.578656	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49698	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49699802024318 03/21/23-07:13:23.800015	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49699	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49698802024312 03/21/23-07:13:22.578656	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49698	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49700802024318 03/21/23-07:13:25.127064	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49700	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49699802021641 03/21/23-07:13:23.800015	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49699	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49701802021641 03/21/23-07:13:27.165442	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49701	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49701802024313 03/21/23-07:13:27.165442	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49701	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49698802024317 03/21/23-07:13:22.578656	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49698	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49701802024318 03/21/23-07:13:27.165442	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49701	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49699802024313 03/21/23-07:13:23.800015	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49699	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49697802024317 03/21/23-07:13:21.229954	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49697	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49702802024313 03/21/23-07:13:28.916498	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49702	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49702802021641 03/21/23-07:13:28.916498	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49702	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49702802024318 03/21/23-07:13:28.916498	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49702	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49697802021641 03/21/23-07:13:21.229954	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49697	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49700802021641 03/21/23-07:13:25.127064	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49700	80	192.168.2.4	64.227.48.212
192.168.2.464.227.48.212 49697802024312 03/21/23-07:13:21.229954	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49697	80	192.168.2.4	64.227.48.212

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:13:21.054405928 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:21.223337889 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:21.223686934 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:21.229954004 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:21.398396015 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:21.398611069 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:21.567040920 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199431896 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199486017 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199523926 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199561119 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199584961 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199598074 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199629068 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199635029 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199664116 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199671984 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199671984 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199696064 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199707031 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199733973 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199743986 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199749947 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199781895 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.199784994 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.199821949 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.368415117 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.368516922 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.368561983 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.368576050 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.368594885 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.368621111 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.368626118 CET	80	49697	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.368668079 CET	49697	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.405898094 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.574153900 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.574321032 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.578655958 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.746587038 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:22.746746063 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:22.914777040 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510366917 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510523081 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510556936 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510648012 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510678053 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510725021 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510727882 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.510778904 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510790110 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.510813951 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510844946 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510881901 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.510922909 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.510998011 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.629591942 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.680857897 CET	80	49698	64.227.48.212	192.168.2.4

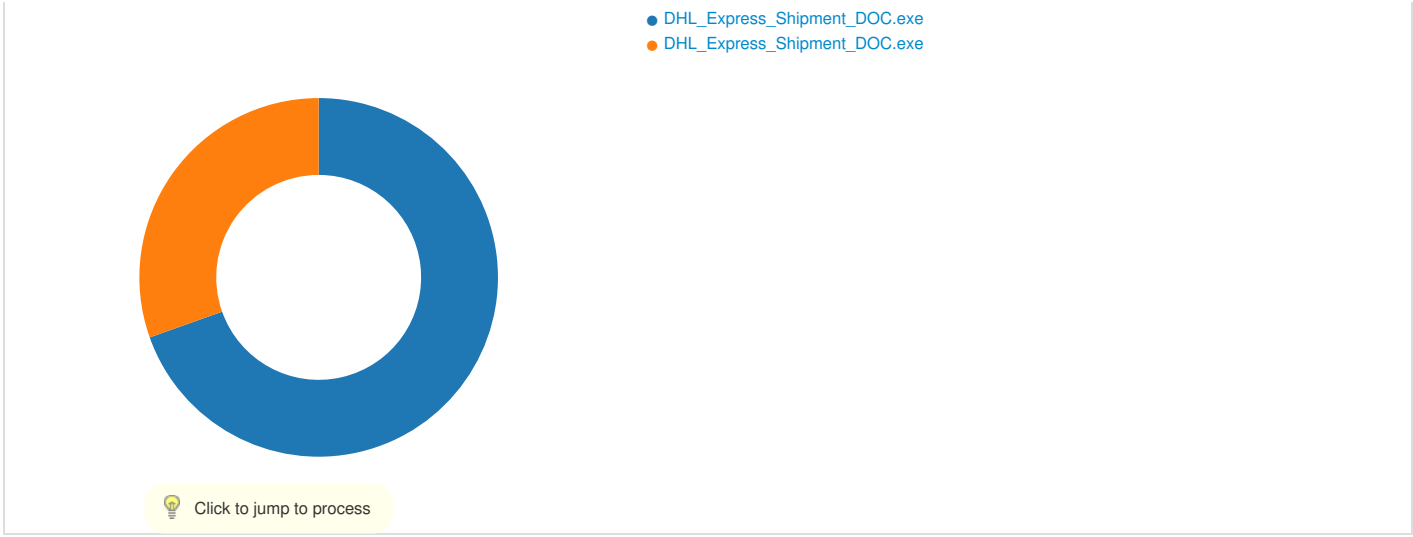
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:13:23.680969954 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.680986881 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.681025982 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.681041956 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.681066990 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.681080103 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.681107998 CET	80	49698	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.681124926 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.681175947 CET	49698	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.797202110 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.797342062 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.800014973 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:23.967341900 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:23.967590094 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.135057926 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.722923040 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.722959042 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.722980022 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723011971 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723036051 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723062038 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723079920 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723099947 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723121881 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723145962 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.723330975 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.723442078 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.723543882 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.890304089 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.890337944 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.890364885 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.890384912 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.890391111 CET	80	49699	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:24.890398979 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.890431881 CET	49699	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:24.956021070 CET	49700	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:25.124252081 CET	80	49700	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:25.124414921 CET	49700	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:25.127063990 CET	49700	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:25.295428038 CET	80	49700	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:25.296231985 CET	49700	80	192.168.2.4	64.227.48.212
Mar 21, 2023 07:13:25.464880943 CET	80	49700	64.227.48.212	192.168.2.4
Mar 21, 2023 07:13:26.076277018 CET	80	49700	64.227.48.212	192.168.2.4

HTTP Request Dependency Graph

- 64.227.48.212

Statistics

Behavior



System Behavior

Analysis Process: DHL_Express_Shipment_DOC.exe PID: 5396, Parent PID: 3528

General

Target ID:	0
Start time:	07:12:04
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
Imagebase:	0xe60000
File size:	852480 bytes
MD5 hash:	370EBDF4FF5036C106793994CC851779
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_DOC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_Express_Shipment_DOC.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7312C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: DHL_Express_Shipment_DOC.exe PID: **5364**, Parent PID: **5396**

General

Target ID:	3
Start time:	07:13:18
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe
Imagebase:	0x7ff61e220000
File size:	852480 bytes
MD5 hash:	370EBDF4FF5036C106793994CC851779
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_GENInfoStealer, Description: Detects executables containing common artifcats observed in infostealers, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Lokibot_1f885282, Description: unknown, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Lokibot_0f421617, Description: unknown, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Loki_1, Description: Loki Payload, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000003.00000002.486364234.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	403C8D	CreateDirectoryW
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	4042FB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	success or wait	1	403C1F	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL_Express_Shipment_DOC.exe	C:\Users\user\AppData\Roaming\C79A3B\B52B3F.exe	success or wait	1	403BED	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	0	1	31	1	success or wait	1	404336	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	40415C	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	40415C	ReadFile

Disassembly

No disassembly