ID: 828071
Sample Name:
DHL04AWB01173903102023PDF.scr.exe
Cookbook: default.jbs
Time: 18:14:07
Date: 16/03/2023
Version: 37.0.0 Beryl

Table of Contents

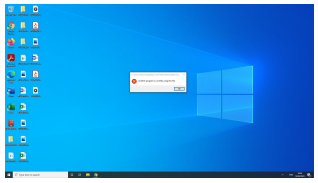
Windows Analysis Report

DHL04AWB01173903102023PDF.scr.exe

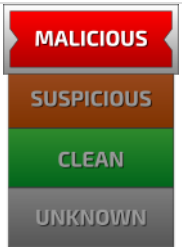
Overview

General Information

Sample Name:	DHL04AWB01173903102023PDF.scr.exe
Analysis ID:	828071
MD5:	1bf124cc783ff4..
SHA1:	b78f2ffb785071..
SHA256:	494d5735144a...
Infos:	



Detection



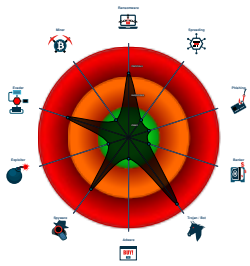
Remcos, GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- Sigma detected: Remcos
- Yara detected GuLoader
- Installs a global keyboard hook
- Drops PE files with a suspicious file…
- Tries to detect Any.run
- Creates autostart registry keys with…
- Found potential ransomware deman…
- Uses dynamic DNS services
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…

Classification



Process Tree

- **System is w10x64native**
- DHL04AWB01173903102023PDF.scr.exe (PID: 5976 cmdline: C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe MD5: 1BF124CC783FF47A91ADA4E6D4AC9E6B)
  - DHL04AWB01173903102023PDF.scr.exe (PID: 3372 cmdline: C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe MD5: 1BF124CC783FF47A91ADA4E6D4AC9E6B)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Remcos, RemcosRAT	Remcos (acronym of Remote Control & Surveillance Software) is a commercial Remote Access Tool to remotely control computers.Remcos is advertised as legitimate software which can be used for surveillance and penetration testing purposes, but has been used in numerous hacking campaigns.Remcos, once installed, opens a backdoor on the computer, granting full access to the remote user.Remcos is developed by the cybersecurity company BreakingSecurity.	• APT33 • The Gorgon Group	http://malware-traffic-analysis.net/2017/12/22/index.htmlhttps://asec.ahnlab.com/en/32376/https://asec.ahnlab.com/ko/25837/https://asec.ahnlab.com/ko/32101/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.remcos

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.10716301559.0000000004772000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000001.00000002.5987381198.0000000006C55000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: DHL04AWB0117390310 2023PDF.scr.exe PID: 3372	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	

Sigma Signatures

Stealing of Sensitive Information

Sigma detected: Remcos

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Networking

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Remcos RAT

Spam, unwanted Advertisements and Ransom Demands

Found potential ransomware demand text

Data Obfuscation

Yara detected GuLoader

Persistence and Installation Behavior

Drops PE files with a suspicious file extension

Boot Survival

Creates autostart registry keys with suspicious values (likely registry only malware)

Malware Analysis System Evasion

Tries to detect Any.run

Stealing of Sensitive Information

Yara detected Remcos RAT

Remote Access Functionality

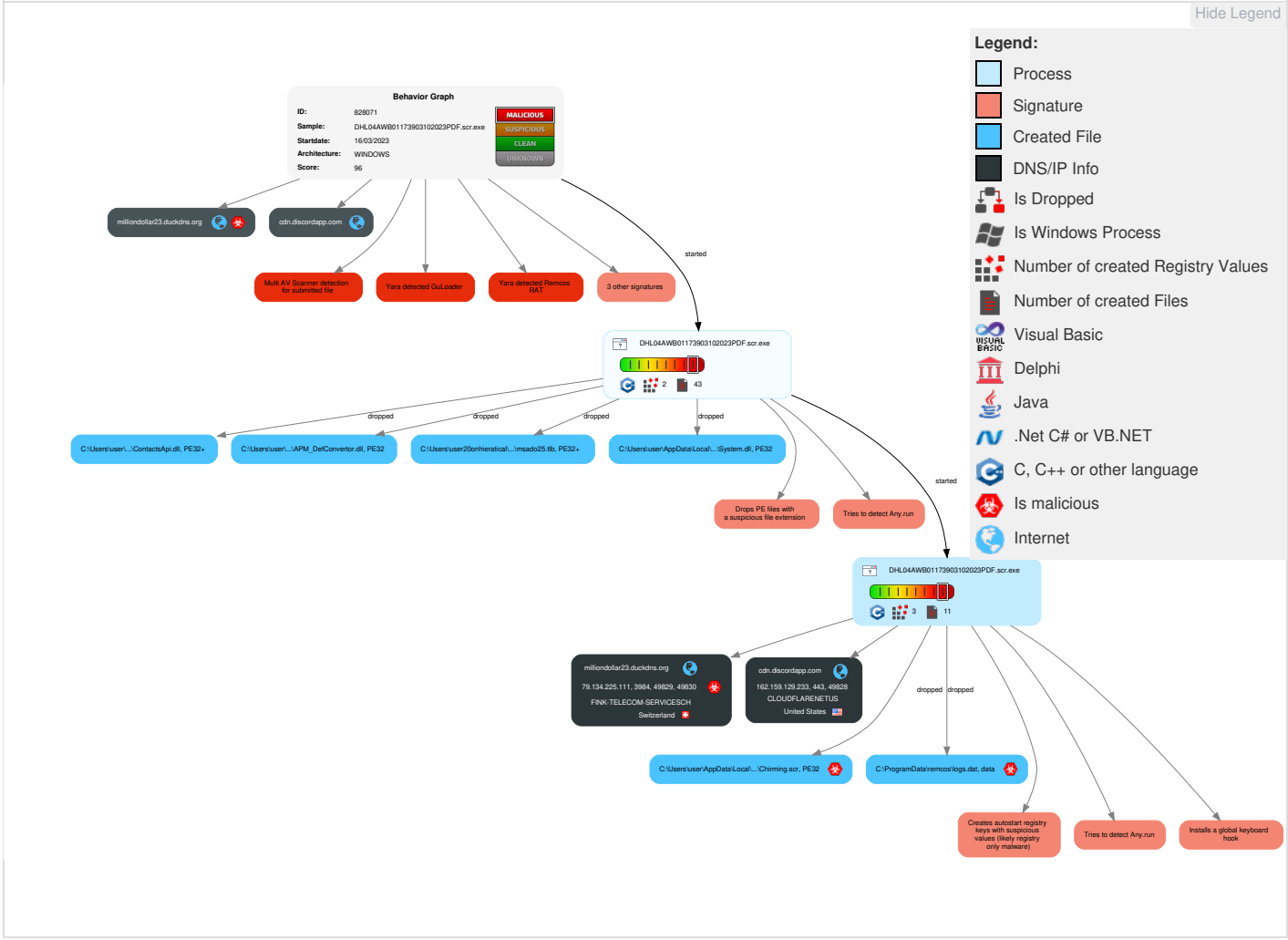
Yara detected Remcos RAT

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	1 Native API	1 1 Registry Run Keys / Startup Folder	1 2 Process Injection	1 1 1 Masquerading	1 1 Input Capture	1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 Registry Run Keys / Startup Folder	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 2 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	3 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

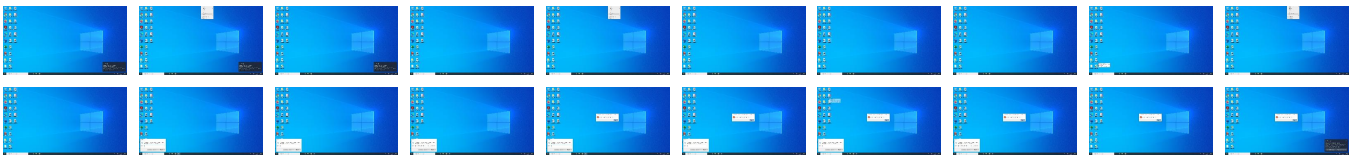
Behavior Graph

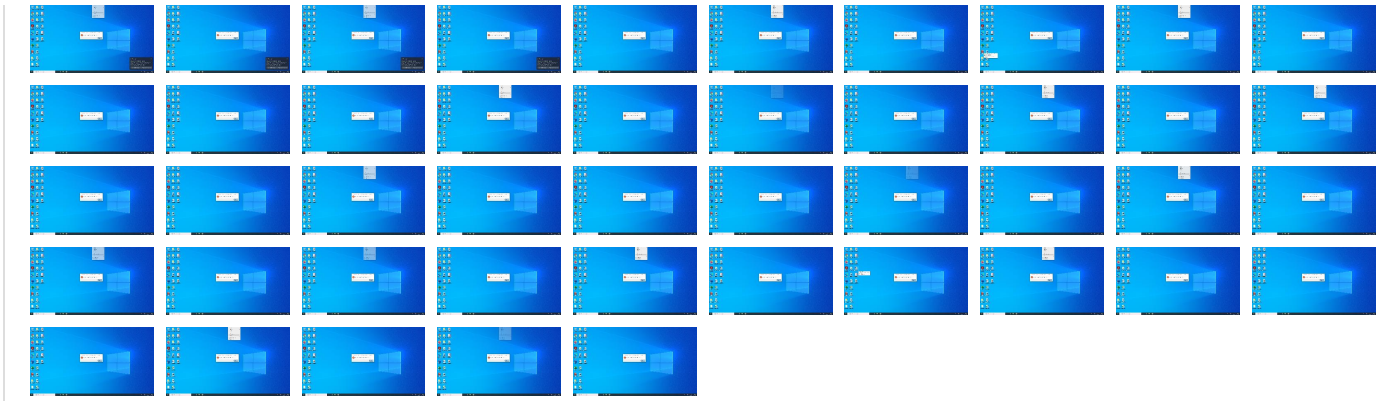


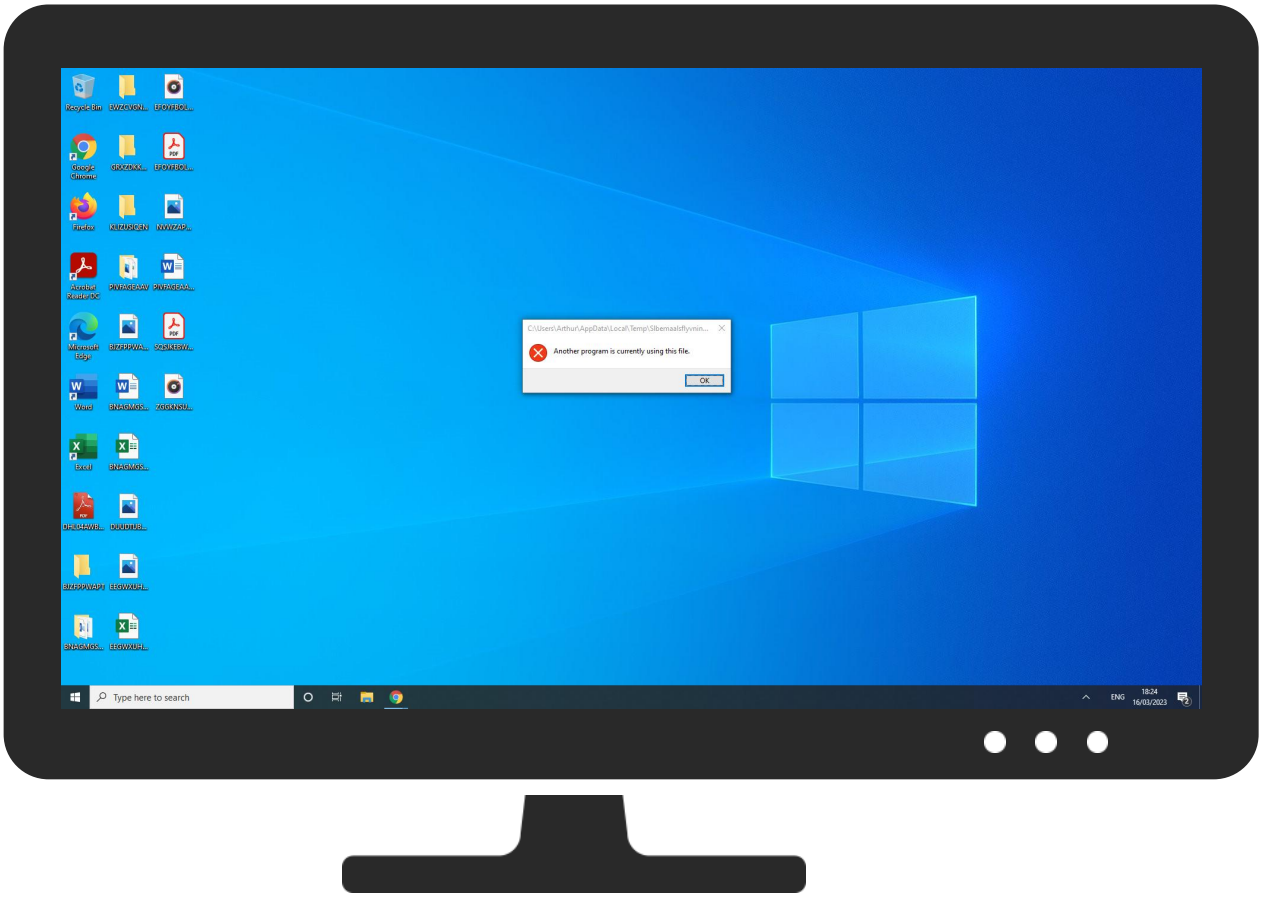
Screenshots

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
DHL04AWB01173903102023PDF.scr.exe	13%	Virustotal		Browse
DHL04AWB01173903102023PDF.scr.exe	8%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr	8%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsbBACD.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	0%	ReversingLabs		
C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Virustotal		Browse
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Virustotal		Browse
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
milliondollar23.duckdns.org	79.134.225.111	true	true		unknown
cdn.discordapp.com	162.159.129.233	true	false		high

Contacted URLs

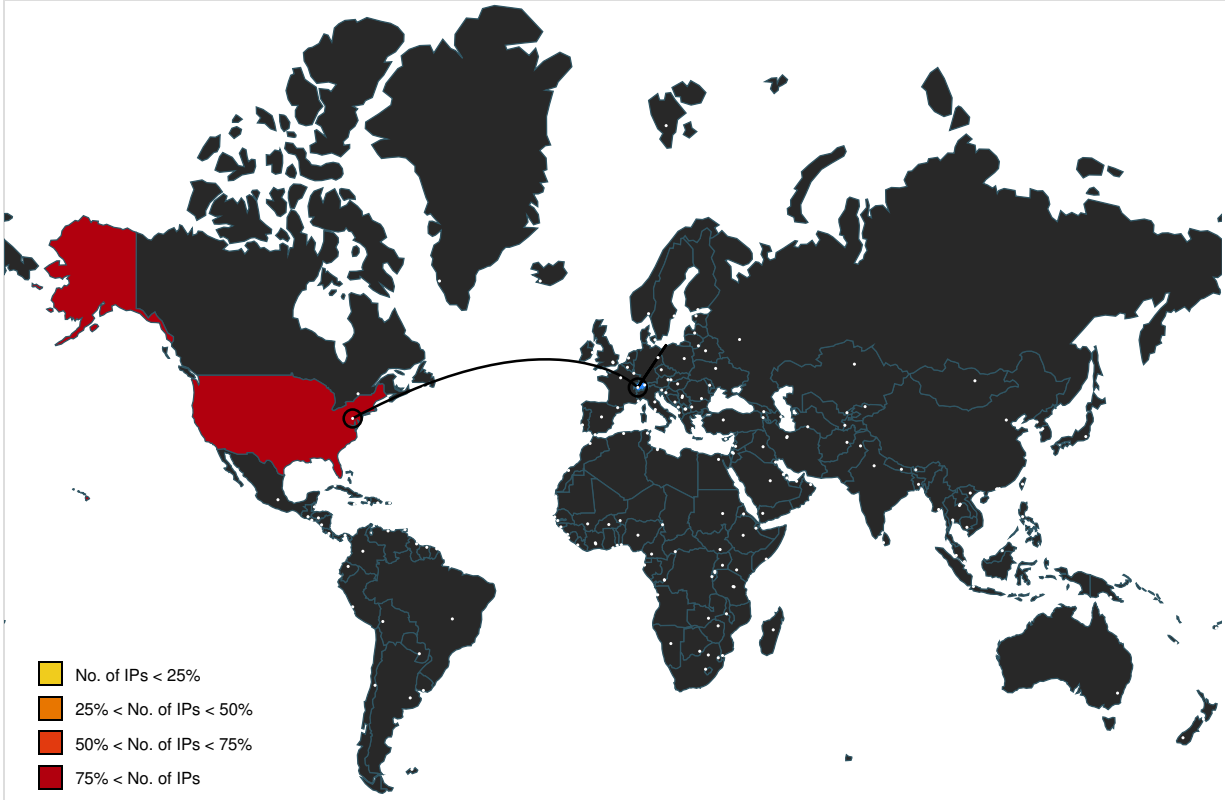
Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/503469199062990850/1085873812794523729/NxXRtUXfgqSkluV181.bin	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.00000000005F2000.00000020.00000001.01000000.00000008.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	DHL04AWB01173903102023PDF.scr.exe, 00000001.00000002.5984634399.00000000029FF000.00000004.00000020.00020000.00000000.sdmp, APM_DefConvertor.dll.1.dr, nseB51F.tmp.1.dr	false		high
http://www.symauth.com/rpa00	DHL04AWB01173903102023PDF.scr.exe, 00000001.00000002.5984634399.00000000029FF000.00000004.00000020.00020000.00000000.sdmp, APM_DefConvertor.dll.1.dr, nseB51F.tmp.1.dr	false		high
http://ocsp.thawte.com0	DHL04AWB01173903102023PDF.scr.exe, 00000001.00000002.5984634399.00000000029FF000.00000004.00000020.00020000.00000000.sdmp, APM_DefConvertor.dll.1.dr, nseB51F.tmp.1.dr	false	• Avira URL Cloud: safe	unknown
http://www.nero.com	DHL04AWB01173903102023PDF.scr.exe, 00000001.00000002.5984634399.00000000029FF000.00000004.00000020.00020000.00000000.sdmp, APM_DefConvertor.dll.1.dr, nseB51F.tmp.1.dr	false		high
http://https://cdn.discordapp.com/t	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000002.10716301559.000000004728000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.0000000000649000.00000020.00000001.01000000.00000008.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.0000000000649000.00000020.00000001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.00000000005F2000.00000020.00000001.01000000.00000008.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000002.10716301559.000000004728000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	DHL04AWB01173903102023PDF.scr.exe, Chirming.scr.4.dr	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.0000000000626000.00000020.00000001.01000000.00000008.sdmp	false		high
http://www.gopher.ftp://ftp.	DHL04AWB01173903102023PDF.scr.exe, 00000004.00000001.5844146219.0000000000649000.00000020.00000001.01000000.00000008.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	DHL04AWB01173903102023PDF.scr.exe, 00000001.00000002.5984634399.00000000029FF000.00000004.00000020.00020000.00000000.sdmp, APM_DefConvertor.dll.1.dr, nseB51F.tmp.1.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
79.134.225.111	milliondollar23.duckdns.org	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	828071
Start date and time:	2023-03-16 18:14:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	9
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:	DHL04AWB01173903102023PDF.scr.exe
Detection:	MAL
Classification:	mal96.rans.troj.spyw.evad.winEXE@3/13@10/2
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 85% (good quality ratio 83.6%) • Quality average: 87.3% • Quality standard deviation: 22%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, UserOOBEBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 40.126.32.73, 40.126.32.69, 40.126.32.132, 20.190.160.13, 20.190.160.15, 40.126.32.75, 40.126.32.137, 20.190.160.21
- Excluded domains from analysis (whitelisted): prdv6a.aadg.msidentity.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, www.tm.lg.prod.aadmsa.akadns.net, www.tm.v6.a.prd.aadg.akadns.net, login.msa.msidentity.com
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:16:31	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Postkassernes C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr
18:16:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Postkassernes C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr

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:\ProgramData\remcos\logs.dat

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	234
Entropy (8bit):	3.3531832298967457
Encrypted:	false
SSDEEP:	6:Kl/IxUlnGljqb5YcleeDAlS1gWAAe5q1gWAv:Kl/lScRUecTWFe5BW+
MD5:	78A66B0B692F4C1BCEC736DD3C0CFF22
SHA1:	EB0F85954BEC9D32CF53F875B8C0BFCB432C8444
SHA-256:	B9153E8889C6C361BD2255890E48C7CC31DAD18E1136873A3FDFF67BF50A01AA
SHA-512:	DF533E6C2696022AC4C318E3A5D970D7716CB485011802E722D56740F9A082C57A79CCE1516264B7307FB789DCE425A6FFEF9E13F279B2397D13CA8236B8D53(
Malicious:	**true**
Reputation:	low
Preview:	....[.2.0.2.3./.0.3./.1.6. .1.8.:.1.6.:.3.3. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].....[.R.u.n.].....[.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.].....[.W.i.n.].r.....[.R.u.n.].....[.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.].....

C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1211760
Entropy (8bit):	**7.9924781293877105**
Encrypted:	**true**
SSDEEP:	24576:7RNsMRW/uL9M7e36FgHRcMSbA22c91uwozF2KDQcvhNfSf7a09Xe+bUe:c4suGm6SxcD2SczF2aQcffSDb99
MD5:	1BF124CC783FF47A91ADA4E6D4AC9E6B
SHA1:	B78F2FFB785071AB785830CDD4CBC5F010B7480B
SHA-256:	494D5735144AF171CC15708B37B491B74BE1522494958E605AC348DD4897DCF9
SHA-512:	B5E35FDA41AEDB7C40961098745153EFA13470D065AC2CFB343C542011ED588694947706 15DB8A7E4B64B77AC6DD2DE4F1CFD1403EFECEEE8425993BDF6667B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1.D9u.*ju.*ju.*j..ujw.*ju.+j..*j..wjd.*j!..j..*j...jt.*jRichu.*j.....PE..L....e .Q.....`...*.....3.....p....@.....`.....t.....hs.....p.....text....^.. .....`..... ..`.rdata..T....p.....d.....@..@.data.....x.....@....ndata...@.....rsrc.....~.....@..@..... ....

C:\Users\user\AppData\Local\Temp\nsbBACD.tmp\System.dll

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.774411073650885
Encrypted:	false
SSDEEP:	192:eB2HS+ihg200uWz947Wzvxu6v0MI7JOde+Ij5Z77dslFsE+:3S62Gw947ExuGDI7J8EF7KIE
MD5:	BE2621A78A13A56CF09E00DD98488360
SHA1:	75F0539DC6AF200A07CDB056CDDDDEC595C6CFD2
SHA-256:	852047023BA0CAE91C7A43365878613CFB4E64E36FF98C460E113D5088D68EF5

SHA-512:	B80CF1F678E6885276B9A1BFD9227374B2EB9E38BB20446D52EBE2C3DBA89764AA50CB4D49DF51A974478F3364B5DBCBC5B4A16DC8F1123B40C89C01725BE3 D1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......1...u.u.u...s.u.a....r.!..q....t....t.Richu.........................PE..L....e.Q.. ....!................9'.......0..............................`......................................2.......0..P............................P.......................................................0..X..........................text.................... .......... ..`.rdata..C....0......."..............@..@.data...x....@.......&..............@....reloc..@....P.......(..............@..B... ....

C:\Users\user\AppData\Local\Temp\nseB51F.tmp

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	1831716
Entropy (8bit):	7.308492575684153
Encrypted:	false
SSDEEP:	49152:lf4WAQduqXBweZG32poHRS2tQuWikK9jM3:lJAQlnANE2tQTaM3
MD5:	9B4D8ABA094C64270F7878FAE618AC65
SHA1:	FA3D773625A7FE13C127925856A2B015C986E598
SHA-256:	CB136F81690F426D253696166DE342FF05A1C1F3C0C780BBE800A06396424751
SHA-512:	87EBE9A0C8BD59D98236943710F7A739AEE413FD8B198F1F92479434819423857252B6D160AB42A0EE8B976AAE3972185E2CC467FB9842AFEB9BF3C3D7577B73
Malicious:	false
Reputation:	low
Preview:	.3......,.........................!.......2.......3..w...........-.J... ........................G...X..............j...f... ....

C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	data
Category:	dropped
Size (bytes):	202342
Entropy (8bit):	7.5372236610693095
Encrypted:	false
SSDEEP:	3072:YTz6SobCaMo6ljmx23UrLpvJvOc9CuKjrDee/jKOVox2EclHuysfzFC64:w6SPaMo6l4XvOZ5rDtKOVoQrF0
MD5:	E2901A2B3EFA6BB00F2AD1D4AD963F52
SHA1:	1F2C771CEAE379DF9FA7FA1FA5E4ABC36638A42E
SHA-256:	FEFA0B1539475BF0ED224A8D9934FD4558DD0B1297FB661DAB776ABC96C333FF
SHA-512:	DA39BCB8E8C2BD79160B33A7767C58CC7CE204B56005B16AF6825DD6E25612D4C08E2C69A2DF288EC6635A24E740C23C5842E5DA3C08BDCCE9FC677D456C9 5E
Malicious:	false
Preview:	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAA

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\TableTextServiceYi.txt

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	45170
Entropy (8bit):	3.7626877360483184
Encrypted:	false
SSDEEP:	384:wBMdoEQYh/Iq7rwSM+jNyql218nyeEJFFCEeFe73c3+AC+mviFuqOtSS0uK3l/:wadoAr7s1+jNyqr6FFweIT0h0/
MD5:	AC05652AF93A583226FD118E23D3652F
SHA1:	DA5BB4AE245369888D1AF981AF6785FAE21C7BC9

SHA-256:	54E26FC4F586B39C4CCB6655735E8AA03AD31498EFD0119AB8406258D5561627
SHA-512:	2C24F1CBD45D5B06DF0A187793E02DA4F085E6E03CF1A697416F3F0B34FE4E96ECFCFD4E25DA3288383B98E1BC112A2418EFF5EA8E69BFBF153F28A20A687BF2
Malicious:	false
Preview:	..[.S.y.s.t.e.m.].....L.a.n.g.I.d. .=. .L.A.N.G._.Y.I.,. .S.U.B.L.A.N.G._.D.E.F.A.U.L.T.....G.u.i.d.P.r.o.f.i.l.e.=.{.4.0.9.C.8.3.7.6.-.0.0.7.B.-.4.3.5.7.-.A.E.8.E.-.2.6.3.1.6.E.E.3.F.B.0.D.}.....D.e.s.c.r.i.p.t.i.o.n.=.".Y.i. .l.n.p.u.t. .M.e.t.h.o.d.".....D.i.s.p.l.a.y. .D.e.s.c.r.i.p.t.i.o.n.=.".@.%.p.r.o.g.r.a.m.F.i.l.e.s.%.\.W.i.n.d.o.w.s. .N.T.\.T.a.b.l.e.T.e.x.t.S.e.r.v.i.c.e.\.T.a.b.l.e.T.e.x.t.S.e.r.v.i.c.e...d.l.l.,.-.1.6.".....I.c.o.n.I.n.d.e.x.=.I.C.O.N._.Y.I.....[.C.o.n.f.i.g.u.r.a.t.i.o.n.].....S.h.o.w.I.n.c.r.e.m.e.n.t.a.l.C.a.n.d.i.d.a.t.e.I.m.m.e.d.i.a.t.e.l.y.=.1.....R.e.a.d.i.n.g.W.i.n.d.o.w...W.i.d.t.h.=.3.....F.o.n.t.F.a.c.e.N.a.m.e.=.M.i.c.r.o.s.o.f.t. .Y.i. .B.a.i.t.i.....F.o.n.t.S.i.z.e.=.1.4.....[.P.r.e.s.e.r.v.e.d.K.e.y.].....G.u.i.d.I.m.e.M.o.d.e.=.{.9.8.2.1.3.4.9.4.-.3.6.7.A.-.4.8.5.5.-.9.0.A.1.-.9.7.D.9.1.7.E.3.E.C.3.D.}.....K.e.y.D.e.f.i.n.e.I.m.e.M.o.d.e.=.V.K._.S.H.I.F.T.,. .T.F._.M.O.D._.O.N._.K.E.Y.U.P._.S.H.I.F.T._.O.N.L.Y.....D.e.s.c.r.i.p.t.

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\Z_Custom2.ini

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	Generic INItialization configuration [allData0]
Category:	dropped
Size (bytes):	6221
Entropy (8bit):	4.623864089058378
Encrypted:	false
SSDEEP:	96:KGz5QTZR5ATsj5sjc9sjnljnDQcaufEjnOAvtDAvVY:BzmTZbAojyjnjljspu8jXvtMvVY
MD5:	CA003CF1D99CDF717768E88DD64BB84C
SHA1:	A0326E46EA68C4649DD6645368B43922B6126FF6
SHA-256:	44100D5F41FE4CDDD1D77EF7124FEC4F8071E5A1678339ACE0DA3DD7E826EF2F
SHA-512:	94D1EB659C22A3614F250C79D1C957876A617158BE538E35E906F12E68C6E12CCBE9C364D1F1C18D280F72FD7958D753348C056CAF320B6843EC3873B59C992
Malicious:	false
Preview:	[Config]..modeIndex=1..allIndex=1..wasdIndex=0..qwerIndex=0..fourIndex=0..syncIndex=0....[allData0]..ColorR=255..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData1]..ColorR=8..ColorG=255..ColorB=240..Color2R=255..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData2]..ColorR=255..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=0..TemperatureH=0..TemperatureL=0..StrobingRandom=0....[allData3]..ColorR=0..ColorG=0..ColorB=0..Color2R=0..Color2G=0..Color2B=0..Color3R=0..Color3G=0..Color3B=0..Color4R=0..Color4G=0..Color4B=0..SpeedType=2..DirectType=1..MusicType=3..TemperatureH=0..Tempe

C:\Users\user\Nonhieratical\Clavichordist\benenders\Actionfilm\Sortsrenheden\msado25.tlb

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	4.63717105728589
Encrypted:	false
SSDEEP:	768:5U0SzA63tPY1AcbERQzuahkbzM7hX2O4HvypROPzMiibjUsqK0M49uo:5OU63tPY114RX3M7MvPy/OPz/CF09F
MD5:	299DBB927B6390C6B925757DD5B2B7FF
SHA1:	FFCE563E42AF7B1086CB5AE92014801B2C66DC0C
SHA-256:	D9D2BD64DE6176B31A4E704D7E5D08FA9BB75A6A8AC007A61C4DF38F6FA82262
SHA-512:	E88F9DA34960BC13C27F2B236A28410AC8B71619D8175103D0BD5E7F03F395F773BCDF399E805D2150BECF2EE107147287D6FE0C00BD41AC591F868E6229634
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<..R...R...R.....R..P...R.Rich..R.PE..d....." ....0.....Z...`..... .....8.....rdata..... ....@..@.rsrc..... .....@..@.....T...8...8.....$.....8....rdata..8...x....rdata$zzzdbg.... .....rsrc$01..... .....rsrc$02.... .....A..R...)h.s.V.2..d.v.9..... .....

C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\ArtDeco_brown_22.bmp

Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, components 3
Category:	dropped
Size (bytes):	7968
Entropy (8bit):	7.906040167483731
Encrypted:	false
SSDEEP:	192:oXRXorJ1fquj4/Ms9hHCQyTscIhlMN58ZB5oEx5/U8qn8kyx:KRoqu0ksEIhCOjZU8M8kM
MD5:	162F6BB32D6D5AC380A80DA07C13E213
SHA1:	7985EAC367E0B19CC0E30B24399A37663E8436F6
SHA-256:	686310A1A5B8BB4D4EAA316FC0A3970EE878CC39F75E8C68F49ED51A5AD562DF

SHA-512:	F4DC70FB483303906CA8C4D5AE404653C7B761BEB38B3DC88ABDEBED4B28A85F3A02F6E2E1E5D28A1625F09A8EEA7A66F12959AA12E98733023CE5908B9FF199
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..5...I...K.4.....t{.k.....^SD'...g....H.7.....d....=.....RmQ..{.x.. .mj....|Z.m'.|;<l.ykc...j.0X.h...f.O,..M.K.>.xG.....K..sZ...H|U.j.Z...y?,.m.n.[...l...J.(..QUG...(...z_. ...#....Ys=....?.....>....?.}.;.V..@7.*.5..-.O...o.\F.....v.....~)...c}.O.....}b.%.....>a..Z.di.l.cH|.a

C:\Users\user\Nonhieratical\Counts\Convolution\Dottily\Iconology.Ess	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	ASCII text, with very long lines (57606), with no line terminators
Category:	dropped
Size (bytes):	57606
Entropy (8bit):	2.670628012232385
Encrypted:	false
SSDEEP:	768:lp+EachJRWeyBP/QmazA5Bnh+QuGkvrOYKT2Rrt6UptqyBcerao1CEzSkNu8R2QP:uquzgxiGXNyHlqgdeo1CtNQP
MD5:	1EE3EA9EB5F7142B93FE99689B2038A6
SHA1:	AB0D94BDBDC97EEA61B226010584C12D9AED43EA
SHA-256:	67D1985FCBEB4E6FB84785F6304B3CB63A9326B328921E04CCFD50539825FDB7
SHA-512:	BBC7EAEA47011BB96FD26ADB3B71F981AE20FDACCF1A72BAFE96EC8E3071AD29AE052B279465FA700B3AD327DC2EA97408B52FD5A0D73B716F21FCD500D30B67
Malicious:	false
Preview:	0000DB00000000B3B300008E0037373700E100DF0091910000D2D2D20000C1C100DFDF000000006A6A006F000000D8000000000000300000470000000000000373737373737006E6E003F3F000000B70000C0C00000DDDDDDDD0000DE00B50000007E0003030030034005D000900E1E1E1E1003A3A3A3A3A00E0000000A900000000D7D70000FCFC00007500F400950000515100EB00DD0000F000920000006A000018005300616100002222000072001B000010006D00B9B9B90000878787700FEFEFE0000720000000004D00CFCF00007373000000A3A3008B8B000000000000262600003E000000000000001C0000000000F50000767676000060600000101010003000000F1000000002828000000020000656500000000000000C7C70000004A005B00E1E1E1E1001A000000480056560068686800000C1000046006700B3B3008100000039007373000DA00292929000000BFBF009100005E000000131313002626000000000000460000FFFFFFFFFF00B9B9B9B9000000027000000E1E1E1000000003800F1F1F10000001F002C000000890000000061616161 00A0001F00B200002C2C2C2C2C009E00000000AC000045450063000A0A00F70000D900000003030300AF000033000101009898 00FDFD0000002424242400830056002D2D0053000000000000000000000000AB00000000EF

C:\Users\user\Nonhieratical\Extracorpuscular\APM_DefConvertor.dll	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	251376
Entropy (8bit):	5.684541726348285
Encrypted:	false
SSDEEP:	3072:njOJemjvYiYtrWTovAYYYlDvNYXzMgv9/PuMKlSOe1sWQuCyY+2JHfYavRkRYI1N:n+6v671nuMKRv1sHyaJ/YavRkRYIBYA1
MD5:	B44ED270A186763E1DA753AA39553B68
SHA1:	10390F85EA5DB841A8BC70E8ED931A5D34026BE8
SHA-256:	E24E9B9C79199B66B9F847F1E07A2769B82CB7FCCA98E5B53F28B481EEBCABD8
SHA-512:	0BF049851CBD5D29221E7C721F15E58286C030023A9BF66E88A5EE6D4D940F89CBBFB8A4E0376382472940450D631E7E3D0162C871443CA12169DFED4E7C91B5
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....43..pR..pR..pR..y*^.qR..y*N.xR....sR....}R....xR..pR..-S....wR .....JR..pR..dR.....zR.....oR.....qR.....qR..pRJ.qR.....qR..RichpR.....PE..L...L..V.....!.....@.....P.....A .....+.....8.....@...@.....text..... ..`.rdata..=A.....B.....@..@.data...D....`.....F.....@....r src..... ...V.....@..@.reloc...G.....H...v.....@..B..... .....

C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\ContactsApi.dll	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	384128
Entropy (8bit):	5.921054568677329
Encrypted:	false
SSDEEP:	6144:zJteC/kw/VKk3g6ZK5RoyPAzv2B9NAlYRuKJOllo:zreCsO3g6QRoyPAw6eRh
MD5:	7E49C04017D860D5EE299FFB104203DF
SHA1:	DDF55616BDABC91EB801CE14A45ACDAD2142B78F
SHA-256:	1AC6E64459440B6EFB03FC256E24BCCBBC512CF6E7DCD85DD3C45E1CA7584176

SHA-512:	EC125C3CD1EDE0F4C24915BC39EA641F58F1D78048E0CCB631F249839440218B02706CC8ACA785DA2B3993EDBABEFB433BF19BA29A9F1EDFB6ACACBDDC0A4F50
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....p...p...p....j..p...?...p.....p.....p.....p...p...p.....p.....p..... ..p..Rich.p.....PE..d....=.N......" ....L.....@.....@..... .....@.....0.....`E..... .....@.....|E..H.....text..... ..`.nep..... ....`.rdata..v....@.....$.....@..@.data....<.....@....pdata..@ .....@..@.rsrc..... .....@..@.reloc..`....0.....@..B.....

C:\Users\user\Nonhieratical\Thonny\Yderligheders\Samtalernes\Sikkerhedsventilen\Sports-Wallpapers-1.jpg	
Process:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x786, components 3
Category:	dropped
Size (bytes):	782753
Entropy (8bit):	7.972739118836816
Encrypted:	false
SSDEEP:	12288:1xE6g9kiViGNq+W6nQNIDO0tVGb34eaR6fUnMlkTFztQywzV0jyB4Dl9l+qfkwPN:7E6G3VibpHIdebodR6jlKFtQVUv+iP8S
MD5:	E269DECCAC13CF01A0377872E79BC676
SHA1:	54D196FDE9529310F9E5A3EBA6548DAB4F179542
SHA-256:	255874E0A6A5CA862CBAE5C783D582729B343C70C5697062D7F1E587F15F25EC
SHA-512:	08ADAD38BE3472CF8814C40F99D6DCFDA313C2FED765B872AA30C0995B027F2BEDABF75DB625F3C40F003A8EFC3F41169CBA4AF706EC637018DEEF02EC92F6CC
Malicious:	false
Preview:	.....JFIF.....`.`.....XICC_PROFILE.....HLino....mntrRGB XYZ .....1..acspMSFT....IEC sRGB.....-HP .....cprt...P...3desc.....lwtpt.. .....bkpt.....rXYZ.....gXYZ...,....bXYZ...@....dmnd...T...pdmdd.....vued...L....view.....$lumi.....meas.....$tech...0....rTRC...<....gTRC...<....bTRC...<....text....Copyright (c) 1998 Hewlett-Packard Company..desc.....sRGB IEC61966-2.1.....sRGB IEC61966-2.1.....XYZ .....Q.....XYZ .....XYZ .. ....o...8.....XYZ .....b.....XYZ .....$.....desc.....IEC http://www.iec.ch.....IEC http://www.iec.ch.....desc.....IEC 61966-2.1 Default RGB colour space - sRGB.....IEC 61966-2.1 Default RGB colour space - sRGB.....desc.....,Reference Viewing Condition in IEC61966-2.1.....,Reference Viewing Condition in IEC61966-2.1.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.9924781293877105
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	DHL04AWB01173903102023PDF.scr.exe
File size:	1211760
MD5:	1bf124cc783ff47a91ada4e6d4ac9e6b
SHA1:	b78f2ffb785071ab785830cdd4cbc5f010b7480b
SHA256:	494d5735144af171cc15708b37b491b74be1522494958e605ac348dd4897dcf9
SHA512:	b5e35fda41aedb7c40961098745153efa13470d065ac2cfb343c542011ed58869494770615db8a7e4b64b77ac6dd2de4f1cfd1403efeceee8425993bdf66670b
SSDEEP:	24576:7RNsMRW/uL9M7e36FgHRcMSbA22c91uwozF2KDQcvhNfSf7a09Xe+bUe:c4suGm6SxcD2SczF2aQcffSDb99
TLSH:	214533D212E2B0B3D690D93B5D5D6E7EE173D60014B2274B7340A8AE6F38165AB1F374
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1.D9u.*ju.*ju.*j..ujw.*ju.+j..*j..wjd.*j!..j..*j...jt.*jRichu.*j.....PE..L....e.Q.....`...*.....3.....p....@

File Icon

Icon Hash:	74f0d0c0ccd4f0c4

Static PE Info

General

Entrypoint:	0x40331c
Entrypoint Section:	.text

Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x519965DC [Sun May 19 23:53:00 2013 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:	17b7d61bda0f7478e36d9ce3d4170680

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	E=inertnesses@Forbetoning20.En, OU="Falskspillere Unrelinquishable ", O=Inalterableness, L=Montague, S=Texas, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 10/07/2022 06:04:55 09/07/2025 06:04:55
Subject Chain	• E=inertnesses@Forbetoning20.En, OU="Falskspillere Unrelinquishable ", O=Inalterableness, L=Montague, S=Texas, C=US
Version:	3
Thumbprint MD5:	B6296BD55FD696653A6ECFD645239E12
Thumbprint SHA-1:	7B9D3A3205DB42A6F338C423028B131EDDD4F064
Thumbprint SHA-256:	F7E0D7AFE23FD9E15D7B7C6CB47B4662581AE209B91E9046AE6A7AAFDC37720B
Serial:	04D25D90CEF83AEC304DC1F83B1B5CCF54893695

Entrypoint Preview
Instruction
sub esp, 000002D4h
push ebx
push ebp
push esi
push edi
push 00000020h
xor ebp, ebp
pop esi
mov dword ptr [esp+18h], ebp
mov dword ptr [esp+10h], 00409230h
mov dword ptr [esp+14h], ebp
call dword ptr [00407034h]
push 00008001h
call dword ptr [004070BCh]
push ebp
call dword ptr [004072ACh]
push 00000008h
mov dword ptr [00429298h], eax
call 00007F3C8C223C0Dh
mov dword ptr [004291E4h], eax
push ebp
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebp
push 00420690h
call dword ptr [0040717Ch]
push 0040937Ch
push 004281E0h

Instruction
call 00007F3C8C223878h
call dword ptr [00407134h]
mov ebx, 00434000h
push eax
push ebx
call 00007F3C8C223866h
push ebp
call dword ptr [0040710Ch]
cmp word ptr [00434000h], 0022h
mov dword ptr [004291E0h], eax
mov eax, ebx
jne 00007F3C8C220D6Ah
push 00000022h
mov eax, 00434002h
pop esi
push esi
push eax
call 00007F3C8C2232D4h
push eax
call dword ptr [00407240h]
mov dword ptr [esp+1Ch], eax
jmp 00007F3C8C220E29h
push 00000020h
pop edx
cmp cx, dx
jne 00007F3C8C220D69h
inc eax
inc eax
cmp word ptr [eax], dx
je 00007F3C8C220D5Bh
add word ptr [eax], 0000h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7494	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4e000	0x7fc0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x127368	0xa08	
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x2b8	.rdata
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	0x5e1c	0x6000	False	0.6542561848958334	data	6.407290112650426	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x7000	0x1354	0x1400	False	0.43046875	data	5.037834422880877	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x202d8	0x600	False	0.47265625	data	3.7587363087821926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2a000	0x24000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4e000	0x7fc0	0x8000	False	0.949371337890625	data	7.7369782578420665	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4e1d8	0x7562	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x55740	0x100	data	English	United States
RT_DIALOG	0x55840	0xf8	data	English	United States
RT_DIALOG	0x55938	0x60	data	English	United States
RT_GROUP_ICON	0x55998	0x14	data	English	United States
RT_VERSION	0x559b0	0x25c	data	English	United States
RT_MANIFEST	0x55c10	0x3b0	XML 1.0 document, ASCII text, with very long lines (944), with no line terminators	English	United States

Imports

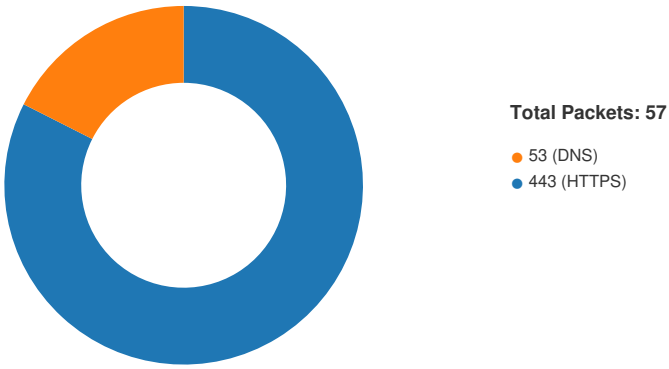
DLL	Import
KERNEL32.dll	CompareFileTime, SearchPathW, SetFileTime, CloseHandle, GetShortPathNameW, MoveFileW, SetCurrentDirectoryW, GetFileAttributesW, GetLastError, GetFullPathNameW, CreateDirectoryW, Sleep, GetTickCount, CreateFileW, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, ExitProcess, SetEnvironmentVariableW, GetWindowsDirectoryW, SetFileAttributesW, ExpandEnvironmentStringsW, SetErrorMode, LoadLibraryW, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, GlobalUnlock, GlobalLock, CreateThread, CreateProcessW, RemoveDirectoryW, lstrcmpiA, GetTempFileNameW, lstrcpyA, lstrcpyW, lstrcatW, GetSystemDirectoryW, GetVersion, GetProcAddress, LoadLibraryA, GetModuleHandleA, GetModuleHandleW, lstrcmpiW, lstrcmpW, WaitForSingleObject, GlobalFree, GlobalAlloc, LoadLibraryExW, GetExitCodeProcess, FreeLibrary, WritePrivateProfileStringW, GetCommandLineW, GetTempPathW, GetPrivateProfileStringW, FindFirstFileW, FindNextFileW, DeleteFileW, SetFilePointer, MultiByteToWideChar, FindClose, MulDiv, ReadFile, WriteFile, lstrlenA, WideCharToMultiByte
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, RegisterClassW, EnableMenuItem, GetSystemMenu, SetClassLongW, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongW, SetCursor, LoadCursorW, CheckDlgButton, GetMessagePos, LoadBitmapW, CallWindowProcW, IsWindowVisible, CloseClipboard, SetClipboardData, wsprintfW, CreateWindowExW, SystemParametersInfoW, AppendMenuW, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextW, GetDlgItemTextW, MessageBoxIndirectW, CharPrevW, CharNextA, wsprintfA, DispatchMessageW, PeekMessageW, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, GetClientRect, FillRect, DrawTextW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, GetDC, SetWindowLongW, LoadImageW, SendMessageTimeoutW, FindWindowExW, EmptyClipboard, OpenClipboard, TrackPopupMenu, EndPaint, ShowWindow, GetDlgItem, IsWindow, SetForegroundWindow
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectW, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListW, SHBrowseForFolderW, SHGetFileInfoW, ShellExecuteW, SHFileOperationW
ADVAPI32.dll	RegCloseKey, RegOpenKeyExW, RegDeleteKeyW, RegDeleteValueW, RegEnumValueW, RegCreateKeyExW, RegSetValueExW, RegQueryValueExW, RegEnumKeyW
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	CoCreateInstance, CoTaskMemFree, OleInitialize, OleUninitialize
VERSION.dll	GetFileVersionInfoSizeW, GetFileVersionInfoW, VerQueryValueW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2023 18:16:32.855799913 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:32.855892897 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:32.856173992 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:32.892891884 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:32.892925024 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:32.923475981 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:32.923746109 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:32.998830080 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:32.999624014 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:32.999752045 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.002515078 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.044373989 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149128914 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149300098 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149307966 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.149344921 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149530888 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.149555922 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149621964 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149730921 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.149741888 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149755955 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149817944 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149876118 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.149877071 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.149928093 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.149954081 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150018930 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150023937 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150115013 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150151014 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150216103 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150234938 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150258064 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150312901 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150312901 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150335073 CET	443	49828	162.159.129.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2023 18:16:33.150351048 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150408983 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150420904 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150563002 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150618076 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150651932 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150770903 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150845051 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.150863886 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.150959969 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.151051044 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.151061058 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.151249886 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.158143044 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158267975 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158310890 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.158346891 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158502102 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158526897 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.158559084 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158675909 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158715963 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.158751011 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158859968 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.158864021 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158893108 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.158914089 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159070969 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159224987 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159241915 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.159450054 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159468889 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.159490108 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.159651995 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.159673929 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159687996 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.159722090 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159722090 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.159960032 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.160126925 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.160279036 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.160310030 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.160330057 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.160459995 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.160495043 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.160514116 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.160682917 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161186934 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.161312103 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.161365032 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161365032 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161395073 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.161439896 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.161452055 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161452055 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161679029 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.161689043 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.161859989 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.167423964 CET	443	49828	162.159.129.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2023 18:16:33.167570114 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.167570114 CET	49828	443	192.168.11.20	162.159.129.233
Mar 16, 2023 18:16:33.167584896 CET	443	49828	162.159.129.233	192.168.11.20
Mar 16, 2023 18:16:33.167656898 CET	443	49828	162.159.129.233	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 16, 2023 18:16:32.845144033 CET	51269	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:16:32.848450899 CET	53	51269	9.9.9.9	192.168.11.20
Mar 16, 2023 18:16:33.308228970 CET	63295	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:16:33.572099924 CET	53	63295	9.9.9.9	192.168.11.20
Mar 16, 2023 18:17:35.652198076 CET	51788	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:17:35.834234953 CET	53	51788	9.9.9.9	192.168.11.20
Mar 16, 2023 18:18:36.607264996 CET	55925	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:18:36.712701082 CET	53	55925	9.9.9.9	192.168.11.20
Mar 16, 2023 18:19:37.093964100 CET	64270	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:19:37.198772907 CET	53	64270	9.9.9.9	192.168.11.20
Mar 16, 2023 18:20:37.471440077 CET	62628	53	192.168.11.20	9.9.9.9
Mar 16, 2023 18:20:38.486324072 CET	62628	53	192.168.11.20	1.1.1.1
Mar 16, 2023 18:20:38.593599081 CET	53	62628	1.1.1.1	192.168.11.20
Mar 16, 2023 18:21:47.112127066 CET	58853	53	192.168.11.20	1.1.1.1
Mar 16, 2023 18:21:47.225806952 CET	53	58853	1.1.1.1	192.168.11.20
Mar 16, 2023 18:22:52.644807100 CET	53532	53	192.168.11.20	1.1.1.1
Mar 16, 2023 18:22:52.755912066 CET	53	53532	1.1.1.1	192.168.11.20
Mar 16, 2023 18:23:53.178380013 CET	52315	53	192.168.11.20	1.1.1.1
Mar 16, 2023 18:23:53.289233923 CET	53	52315	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 16, 2023 18:16:32.845144033 CET	192.168.11.20	9.9.9.9	0x6e97	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:33.308228970 CET	192.168.11.20	9.9.9.9	0x43c7	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:17:35.652198076 CET	192.168.11.20	9.9.9.9	0x8ddd	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:18:36.607264996 CET	192.168.11.20	9.9.9.9	0x750b	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:19:37.093964100 CET	192.168.11.20	9.9.9.9	0x2197	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:20:37.471440077 CET	192.168.11.20	9.9.9.9	0xccb6	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:20:38.486324072 CET	192.168.11.20	1.1.1.1	0xccb6	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:21:47.112127066 CET	192.168.11.20	1.1.1.1	0xcb7e	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:22:52.644807100 CET	192.168.11.20	1.1.1.1	0xb589	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:23:53.178380013 CET	192.168.11.20	1.1.1.1	0x286	Standard query (0)	milliondollar23.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

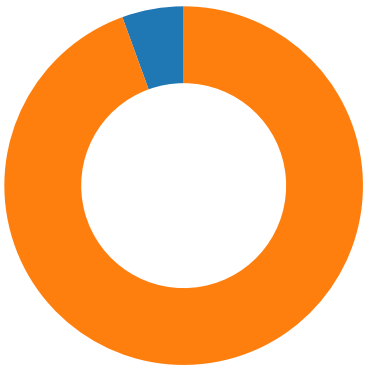
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 16, 2023 18:16:32.848450899 CET	9.9.9.9	192.168.11.20	0x6e97	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:32.848450899 CET	9.9.9.9	192.168.11.20	0x6e97	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:32.848450899 CET	9.9.9.9	192.168.11.20	0x6e97	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:32.848450899 CET	9.9.9.9	192.168.11.20	0x6e97	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:32.848450899 CET	9.9.9.9	192.168.11.20	0x6e97	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:16:33.572099924 CET	9.9.9.9	192.168.11.20	0x43c7	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:17:35.834234953 CET	9.9.9.9	192.168.11.20	0x8ddd	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:18:36.712701082 CET	9.9.9.9	192.168.11.20	0x750b	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:19:37.198772907 CET	9.9.9.9	192.168.11.20	0x2197	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:20:38.593599081 CET	1.1.1.1	192.168.11.20	0xccb6	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:21:47.225806952 CET	1.1.1.1	192.168.11.20	0xcb7e	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:22:52.755912066 CET	1.1.1.1	192.168.11.20	0xb589	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false
Mar 16, 2023 18:23:53.289233923 CET	1.1.1.1	192.168.11.20	0x286	No error (0)	milliondollar23.duckdns.org		79.134.225.111	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- cdn.discordapp.com

Statistics

Behavior



DHL04AWB01173903102023PDF.s..
DHL04AWB01173903102023PDF.s..

Click to jump to process

System Behavior

Analysis Process: DHL04AWB01173903102023PDF.scr.exe PID: 5976, Parent PID: 644

General

Target ID:	1
Start time:	18:16:00
Start date:	16/03/2023
Path:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Imagebase:	0x400000
File size:	1211760 bytes
MD5 hash:	1BF124CC783FF47A91ADA4E6D4AC9E6B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.5987381198.0000000006C55000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Nonhieratical\Apicad\Outjinx\Nonnavigableness\Competed\Coccosteid.Udr	unknown	49504256	success or wait	1	100028D5	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: DHL04AWB01173903102023PDF.scr.exe PID: 3372, Parent PID: 5976

General

Target ID:	4
Start time:	18:16:21
Start date:	16/03/2023
Path:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe
Imagebase:	0x400000
File size:	1211760 bytes
MD5 hash:	1BF124CC783FF47A91ADA4E6D4AC9E6B
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000004.00000002.10716301559.0000000004772000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	2D72E4E	CreateFileW
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	2D72E4E	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	2D72E4E	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	2D72E4E	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	2D72E4E	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	2D72E4E	InternetOpenUrlA
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	2D72E4E	InternetOpenUrlA
C:\ProgramData\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	409CF5	CreateDirectoryW
C:\ProgramData\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device	synchronous io non alert | non directory file	success or wait	2	41A9F4	CreateFileW
C:\ProgramData\remcos	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	409CF5	CreateDirectoryW

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\Temp\Slbemaalsflyvningers\Chirming.scr	0	1211760	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 31 fd 44 39 75 fd 2a 6a 75 fd 2a 6a 75 fd 2a 6a fd fd 75 6a 77 fd 2a 6a 75 fd 2b 6a fd fd 2a 6a fd fd 77 6a 64 fd 2a 6a 21 fd 1a 6a 7f fd 2a 6a fd fd 2c 6a 74 fd 2a 6a 52 69 63 68 75 fd 2a 6a 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 65 fd 51 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 60 00 00 00 2a 02 00 00 08 00 00 1c 33 00 00 00 10 00 00 00 70 00 00 00 00 40	MZ@!L!This program cannot be run in DOS mode.$1D9u*ju*ju*juj w*ju+j*jwjd*j!j*j,jt*jRichu*j PELeQ`*3p@	success or wait	2	2D50876	WriteFile
C:\ProgramData\remcos\logs.dat	0	162	0d 00 0a 00 5b 00 32 00 30 00 32 00 33 00 2f 00 30 00 33 00 2f 00 31 00 36 00 20 00 31 00 38 00 3a 00 31 00 36 00 3a 00 33 00 33 00 20 00 4f 00 66 00 66 00 6c 00 69 00 6e 00 65 00 20 00 4b 00 65 00 79 00 6c 00 6f 00 67 00 67 00 65 00 72 00 20 00 53 00 74 00 61 00 72 00 74 00 65 00 64 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 52 00 75 00 6e 00 5d 00 0d 00 0a 00 0d 00 0a 00 5b 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 4d 00 61 00 6e 00 61 00 67 00 65 00 72 00 5d 00 0d 00 0a 00	[2023/03/16 18:16:33 Offline Keylogger Started][Run][Program Manager]	success or wait	2	41AA2E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL04AWB01173903102023PDF.scr.exe	unknown	1211760	success or wait	1	2D72E4E	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Rmc-TUJMU2\	success or wait	1	4129D8	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Postkassernes	unicode	C:\Users\user\AppData\Local\Temp\Slbemaalsflyvningers\Chirming.scr	success or wait	1	2D4FC9A	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Rmc-TUJMU2	exepath	binary	5A 83 06 32 0C CA 9D CA 33 2E 4D BE 25 A5 E2 0E DD 36 8C E4 50 EA F9 73 8B 39 8B 6A 86 C3 42 CE ED E6 A6 66 A6 A4 8D 44 6B AB 18 9A 09 C2 F3 2B 08 66 7B FC 0B 9F D2 FA C6 31 36 45 B0 53 74 F9 14 F5 DB 39 EC 46 8A 29 12 0E 83 D3 4D 47 76 BB E0 11 2F 10 C0 8F F3 9D DF 77 82 FD DD 7E 6D C1 3C 1D 98 91 FE 61 BC 00 DD DE C4 64 B1 11 7F 4D 51 F3 DE F7	success or wait	1	412A00	RegSetValueExA
HKEY_CURRENT_USER\SOFTWARE\Rmc-TUJMU2	licence	unicode	06ADD78AD41271987222EF3269302DA2	success or wait	1	412A00	RegSetValueExA

Disassembly

No disassembly