ID: 830435
Sample Name:
DHL_Notification_pdf.exe
Cookbook: default.jbs
Time: 11:27:15
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report DHL_Notification_pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Yara Signatures 5
Memory Dumps 5
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 14
Public IPs 15
General Information 15
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 16
ASNs 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
C:\Users\user\AppData\Local\Temp\146E771M 16
C:\Users\user\AppData\Local\Temp\ldndbi.exe 17
C:\Users\user\AppData\Local\Temp\nsw10F5.tmp 17
C:\Users\user\AppData\Local\Temp\qlqjt.de 17
C:\Users\user\AppData\Local\Temp\tfnqr.hy 18
Static File Info 18
General 18
File Icon 18
Static PE Info 19
General 19
Entrypoint Preview 19
Rich Headers 20
Data Directories 20
Sections 20
Resources 20
Imports 21
Possible Origin 21
Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 22

Copyright Joe Security LLC 2023

UDP Packets 24
DNS Queries 24
DNS Answers 24
HTTP Request Dependency Graph 25
Statistics 25
Behavior 25
System Behavior 26
Analysis Process: DHL_Notification_pdf.exePID: 5084, Parent PID: 3320 26
General 26
File Activities 26
Analysis Process: ldndbi.exePID: 3008, Parent PID: 5084 26
General 26
File Activities 26
File Read 27
Analysis Process: conhost.exePID: 4584, Parent PID: 3008 27
General 27
Analysis Process: ldndbi.exePID: 6108, Parent PID: 3008 27
General 27
File Activities 27
File Read 28
Analysis Process: explorer.exePID: 3320, Parent PID: 6108 28
General 28
File Activities 28
Registry Activities 28
Analysis Process: cmmon32.exePID: 5228, Parent PID: 3320 28
General 28
File Activities 29
File Created 29
File Deleted 30
File Read 30
Registry Activities 30
Disassembly 30

Copyright Joe Security LLC 2023

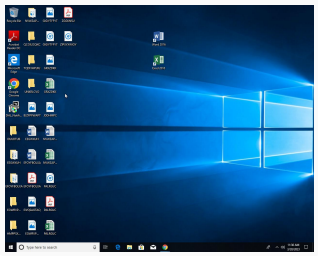
Windows Analysis Report

DHL_Notification_pdf.exe

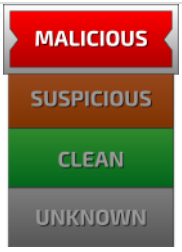
Overview

General Information

Sample Name:	DHL_Notification_pdf.exe
Analysis ID:	830435
MD5:	06f7894017e8f…
SHA1:	fab1cbdbbb5fc…
SHA256:	bbfb2aacf1ff43…
Tags:	DHL exe Formbook
Infos:	



Detection



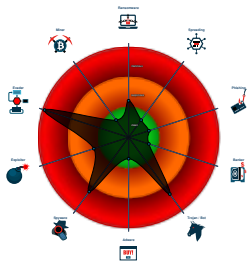
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w10x64**
- DHL_Notification_pdf.exe (PID: 5084 cmdline: C:\Users\user\Desktop\DHL_Notification_pdf.exe MD5: 06F7894017E8F6737D228ADC14480C83)
  - ldndbi.exe (PID: 3008 cmdline: "C:\Users\user~1\AppData\Local\Temp\ldndbi.exe" C:\Users\user~1\AppData\Local\Temp\qlqjt.de MD5: C99B9B59B44F7789DD46E5230C22A9CD)
    - conhost.exe (PID: 4584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - ldndbi.exe (PID: 6108 cmdline: C:\Users\user~1\AppData\Local\Temp\ldndbi.exe MD5: C99B9B59B44F7789DD46E5230C22A9CD)
      - explorer.exe (PID: 3320 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmmon32.exe (PID: 5228 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	**http://** blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Copyright Joe Security LLC 2023

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1efd0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae2f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18217:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x18015:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17ab1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x18117:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1828f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa9fa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16d0c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1dd87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ed3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.508740330.0000000000C00000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000005.00000002.508740330.0000000000C00000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1efd0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae2f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x18217:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.ldndbi.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.ldndbi.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1ffc3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbe22:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1920a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.ldndbi.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19008:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18aa4:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1910a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x19282:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xb9ed:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17cff:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1ed7a:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1fd2d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.ldndbi.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.ldndbi.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20dc3:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcc22:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a00a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Copyright Joe Security LLC 2023

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.7 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.78.8.8.850513532023883 03/20/23-11:29:43.795616
SID:	2023883
Source Port:	50513
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- Performs DNS queries to domains with low reputation

E-Banking Fraud

- Yara detected FormBook

System Summary

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation

- Detected unpacking (changes PE section rights)

HIPS / PFW / Operating System Protection Evasion

- System process connects to network (likely due to code injection or exploit)
- Sample uses process hollowing technique
- Maps a DLL or memory area into another process
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Copyright Joe Security LLC 2023

Yara detected FormBook

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

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

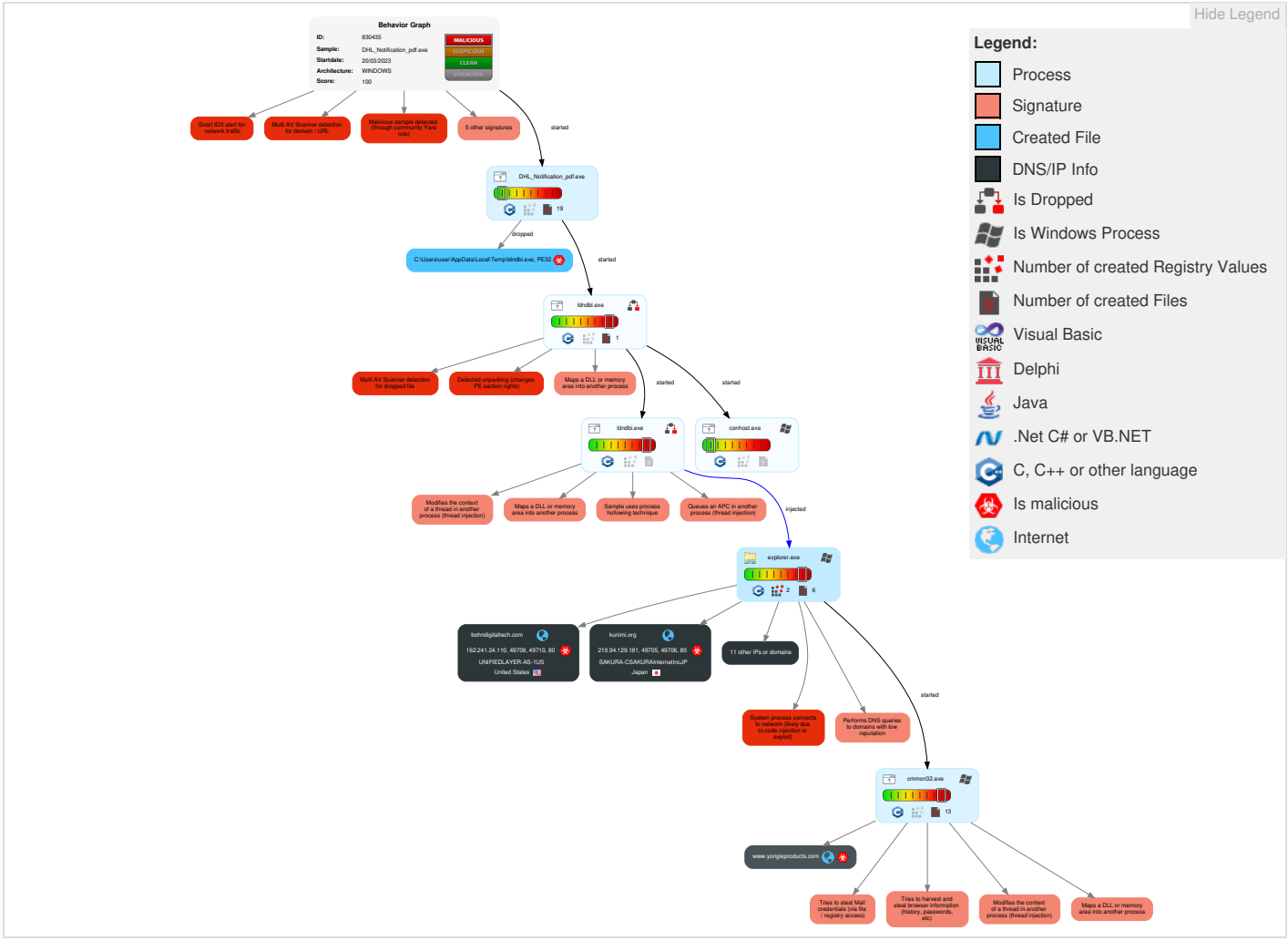
Remote Access Functionality

Yara detected FormBook

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 Shared Modules	Path Interception	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	5 1 2 Process Injection	3 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Software Packing	Security Account Manager	1 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 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 Masquerading	NTDS	1 4 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Virtualization/Sandbox Evasion	LSA Secrets	2 Virtualization/Sandbox Evasion	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 Access Token Manipulation	Cached Domain Credentials	2 Process 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	5 1 2 Process Injection	DCSync	1 Application Window Discovery	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	Indicator Removal from Tools	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

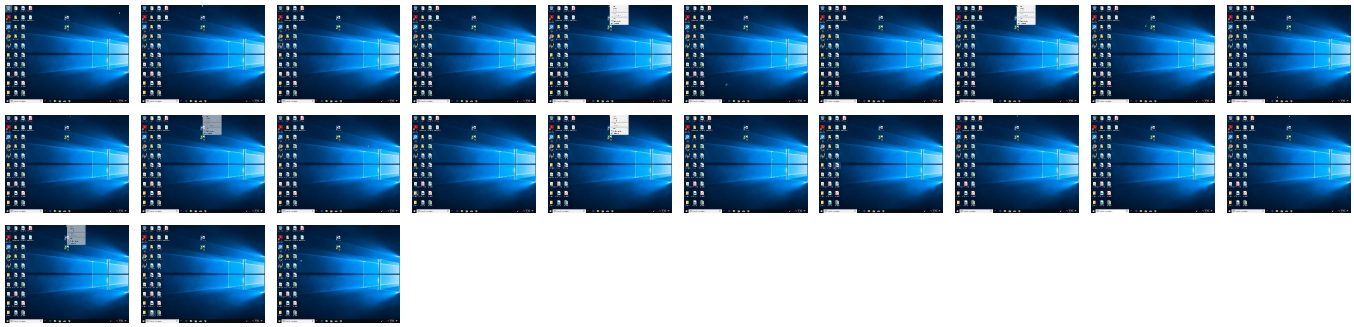
Behavior Graph



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_Notification_pdf.exe	54%	ReversingLabs	Win32.Trojan.FormBook	
DHL_Notification_pdf.exe	46%	Virustotal		Browse
DHL_Notification_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ldndbi.exe	19%	ReversingLabs	Win32.Trojan.Lazy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.ldndbi.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.ldndbi.exe.5d0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
kunimi.org	4%	Virustotal		Browse
bohndigitaltech.com	5%	Virustotal		Browse
rifleroofers.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.kunimi.org	0%	Avira URL Cloud	safe	
http://kunimi.org/hpb7/?MWgiD_=Gt_ludmBZP&pgoMAr2=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/II/dsC	0%	Avira URL Cloud	safe	
http://www.buymyenergy.com	0%	Avira URL Cloud	safe	
http://www.bohndigitaltech.com	0%	Avira URL Cloud	safe	
http://www.rifleroofers.com/hpb7/?pgoMAr2=Sr1AjUgE1bmYtN0hdeH1+2eYW2bz9zJIy7x8VWFTjEXaDkIuvqWhFoT+O4ddqC6+eWArdJNQDIDq/++CVSPCikRZslZ7vUOEqSXS/sLR9FgE&MWgiD_=Gt_ludmBZP	0%	Avira URL Cloud	safe	
http://www.yongleproducts.com/hpb7/?MWgiD_=Gt_ludmBZP&pgoMAr2=qNzMMFnF92wYqby	100%	Avira URL Cloud	malware	
http://www.buymyenergy.comReferer:	0%	Avira URL Cloud	safe	
http://www.admet01.clubReferer:	0%	Avira URL Cloud	safe	
http://www.kunimi.org/hpb7/	0%	Avira URL Cloud	safe	
http://www.traindic.top/hpb7/?pgoMAr2=bTtFiHq0GQrF6aFlJXqsXsYFYYSgPtrX4CJLxcpJGK/F7H1QBurO56xriJCe1rAnTJlhkBPAE1A8g1vh/R7dLaG3D1YJBFes4W4zIdoETPhG&MWgiD_=Gt_ludmBZP	100%	Avira URL Cloud	malware	
http://www.adoptiveimmunotech.com/hpb7/	100%	Avira URL Cloud	malware	
http://www.mindsetlighting.xyz/hpb7/	100%	Avira URL Cloud	malware	
http://www.0dhy.xyz/hpb7/	100%	Avira URL Cloud	malware	
http://www.amirah.cfd/hpb7/	100%	Avira URL Cloud	phishing	
http://www.bisarropainting.com/hpb7/:	0%	Avira URL Cloud	safe	
http://www.amirah.cfd	100%	Avira URL Cloud	phishing	
http://www.traindic.top/hpb7/	100%	Avira URL Cloud	malware	
http://www.bohndigitaltech.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.madliainsalu.comReferer:	0%	Avira URL Cloud	safe	
http://www.0dhy.xyz	0%	Avira URL Cloud	safe	
http://www.bohndigitaltech.com/hpb7/Xz.	0%	Avira URL Cloud	safe	
http://www.creative-shield.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.kotelak.ru	0%	Avira URL Cloud	safe	
http://www.kunimi.org/hpb7/I	0%	Avira URL Cloud	safe	
http://www.amirah.cfdReferer:	0%	Avira URL Cloud	safe	
http://www.kotelak.ru/hpb7/	0%	Avira URL Cloud	safe	
http://www.admet01.club	100%	Avira URL Cloud	malware	
http://www.0dhy.xyz/hpb7/?pgoMAr2=BrlYCq9+qqzfybZpwXKugHGOc0m4ktDYrdhK4pNzcFj3gilCUF3BZQEP3ssdPmgNj5Kg/PdRxbVpWQCkOBnfQOgdZDSA0ZYkxsRLP7vho3iJ&MWgiD_=Gt_ludmBZP	100%	Avira URL Cloud	malware	
http://www.creative-shield.com/hpb7/:	0%	Avira URL Cloud	safe	
http://www.adoptiveimmunotech.com/hpb7/j	100%	Avira URL Cloud	malware	
http://www.bisarropainting.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.kotelak.ruReferer:	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com/hpb7/?MWgiD_=Gt_ludmBZP&pgoMAr2=NuHAd+vfjtmC4E+cdz1CpM6J6ScGh9KWfGXGi6oH+281UYUkr6SouFSZ7LMQAOLiSk3FYsgr8Pu9aCQzqq/MT4aa5FcMBKGUU6DgJQXharGK	0%	Avira URL Cloud	safe	
http://www.madliainsalu.com	0%	Avira URL Cloud	safe	
http://www.rifleroofers.com	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com	0%	Avira URL Cloud	safe	
http://www.rifleroofers.comReferer:	0%	Avira URL Cloud	safe	
http://www.denko-kosan.comReferer:	0%	Avira URL Cloud	safe	
http://www.buymyenergy.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.mindsetlighting.xyzReferer:	0%	Avira URL Cloud	safe	
http://www.madliainsalu.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.adoptiveimmunotech.comReferer:	0%	Avira URL Cloud	safe	
http://www.creative-shield.com	0%	Avira URL Cloud	safe	
http://www.adoptiveimmunotech.com	0%	Avira URL Cloud	safe	
http://www.rifleroofers.com/hpb7/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.creative-shield.comReferer:	0%	Avira URL Cloud	safe	
http://rifleroofers.com/hpb7/?pgoMAr2=Sr1AjUgE1bmYtN0hdeH1	0%	Avira URL Cloud	safe	
http://www.bisarropainting.comReferer:	0%	Avira URL Cloud	safe	
http://www.traindic.top	100%	Avira URL Cloud	malware	
http://www.yongleproducts.com/hpb7/	100%	Avira URL Cloud	malware	
http://www.admet01.club/hpb7/	100%	Avira URL Cloud	malware	
http://www.bisarropainting.com	0%	Avira URL Cloud	safe	
http://www.yongleproducts.com	0%	Avira URL Cloud	safe	
http://www.mindsetlighting.xyz	100%	Avira URL Cloud	malware	
http://www.bohndigitaltech.comReferer:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kunimi.org	219.94.129.181	true	true	• 4%, Virustotal, Browse	unknown
bohndigitaltech.com	162.241.24.110	true	true	• 5%, Virustotal, Browse	unknown
www.0dhy.xyz	198.46.160.97	true	true		unknown
rifleroofers.com	67.222.24.48	true	true	• 0%, Virustotal, Browse	unknown
www.yongleproducts.com	1.13.186.125	true	true		unknown
www.traindic.top	162.0.231.77	true	true		unknown
denko-kosan.com	49.212.180.95	true	true		unknown
www.bohndigitaltech.com	unknown	unknown	true		unknown
www.denko-kosan.com	unknown	unknown	true		unknown
www.rifleroofers.com	unknown	unknown	true		unknown
www.kunimi.org	unknown	unknown	true		unknown
www.amirah.cfd	unknown	unknown	true		unknown
www.bisarropainting.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.rifleroofers.com/hpb7/?pgoMAr2=Sr1AjUgE1bmYtN0hdeH1+2eYW2bz9zJIy7x8VWFTjEXaDkluvqWhFoT+O4ddqC6+eWArdJNQDIDq/++CVSPCikRZslZ7vUOEqSXS/sLR9FgE&MWgiD_=Gt_ludmBZP	true	• Avira URL Cloud: safe	unknown
http://www.kunimi.org/hpb7/	true	• Avira URL Cloud: safe	unknown
http://www.traindic.top/hpb7/?pgoMAr2=bTtFiHq0GQrF6aFlJXqsXsYFYYSgPtrX4CJLxcpJGK/F7H1QBurO56xriJCe1rAnTJlhkBPAE1A8g1vh/R7dLaG3D1YJBFes4W4zIdoETPhG&MWgiD_=Gt_ludmBZP	true	• Avira URL Cloud: malware	unknown
http://www.traindic.top/hpb7/	true	• Avira URL Cloud: malware	unknown
http://www.bohndigitaltech.com/hpb7/	true	• Avira URL Cloud: safe	unknown
http://www.denko-kosan.com/hpb7/	true	• Avira URL Cloud: safe	unknown
http://www.0dhy.xyz/hpb7/?pgoMAr2=BrlYCq9+qqzfybZpwXKugHGOc0m4ktDYrdhK4pNzcFj3gIlCUF3BZQEP3ssdPmgNj5Kg/PdRxbVpWQCkOBnfQOgdZDSA0ZYkxsRLP7vho3iJ&MWgiD_=Gt_ludmBZP	true	• Avira URL Cloud: malware	unknown
http://www.denko-kosan.com/hpb7/?MWgiD_=Gt_ludmBZP&pgoMAr2=NuHAd+vfjtmC4E+cdz1CpM6J6ScGh9KWfGXGi6oH+281UYUkr6SouFSZ7LMQAOLiSk3FYsgr8Pu9aCQzqq/MT4aa5FcMBKGUU6DgJQXharGK	true	• Avira URL Cloud: safe	unknown
http://www.rifleroofers.com/hpb7/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

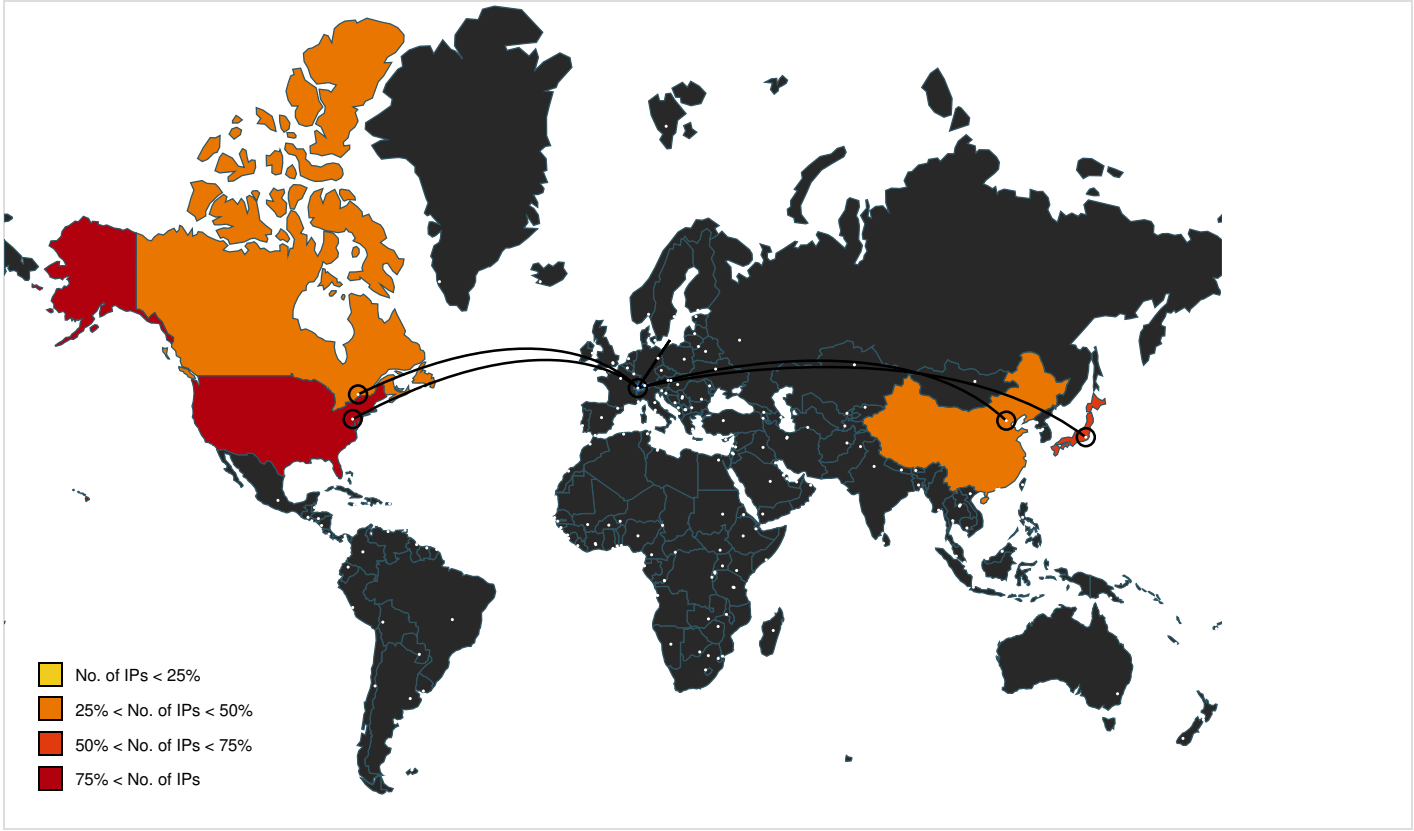
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.kunimi.org	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://https://duckduckgo.com/ac/?q=	146E771M.5.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.buymyenergy.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mindsetlighting.xyz/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://kunimi.org/hpb7/?MWgiD_=Gt_IudmBZP&pgoMAr2=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/II/dsC	explorer.exe, 00000004.00000002.52373040 3.0000000014FCA000.00000004.80000000.000 40000.00000000.sdmp, cmmon32.exe, 000000 05.00000002.510648252.00000000056BA000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bohndigitaltech.com	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.amirah.cfd	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://www.yongleproducts.com/hpb7/?MWgiD_=Gt_IudmBZP&pgoMAr2=qNzMMFnF92wYqby	cmmon32.exe, 00000005.00000002.509147113 .0000000000F05000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.0dhy.xyz/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.amirah.cfd/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://www.buymyenergy.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bisarropainting.com/hpb7/:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.admet01.clubReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adoptiveimmunotech.com/hpb7/	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.madliainsalu.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kunimi.org/hpb7/I	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.creative-shield.com/hpb7/	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ru	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.0dhy.xyz	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.bohndigitaltech.com/hpb7/Xz.	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.amirah.cfdReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ru/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.creative-shield.com/hpb7/:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.admet01.club	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.adoptiveimmunotech.com/hpb7/j	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.bisarropainting.com/hpb7/	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.google.com/images/branding/product/ico/googleg_lodp.ico	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.madliainsalu.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ruReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rifleroofers.com	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.denko-kosan.com	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.511253808.00000000047AE000. 00000040.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.madliainsalu.com/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mindsetlighting.xyzReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rifleroofers.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.buymyenergy.com/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	146E771M.5.dr	false		high
http://www.denko-kosan.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.adoptiveimmunotech.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	DHL_Notification_pdf.exe	false		high
http://www.creative-shield.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.adoptiveimmunotech.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.creative-shield.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	146E771M.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	cmmon32.exe, 00000005.00000003.381521454 .0000000007C36000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.traindic.top	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.admet01.club/hpb7/	explorer.exe, 00000004.00000002.52108236 0.0000000007D45000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.yongleproducts.com/hpb7/	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://rifleroofers.com/hpb7/?pgoMAr2=Sr1AjUgE1bmYtN0hdeH1	explorer.exe, 00000004.00000002.52373040 3.00000000157A4000.00000004.80000000.000 40000.00000000.sdmp, cmmon32.exe, 000000 05.00000002.510648252.0000000005E94000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bisarropainting.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bohndigitaltech.comReferer:	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	146E771M.5.dr	false		high
http://www.bisarropainting.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yongleproducts.com	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mindsetlighting.xyz	explorer.exe, 00000004.00000003.46253544 0.0000000007D57000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.521082360.0000000007D45000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.46.160.97	www.0dhy.xyz	United States		36352	AS-COLOCROSSINGUS	true
67.222.24.48	rifleroofers.com	United States		63410	PRIVATESYSTEMSUS	true
49.212.180.95	denko-kosan.com	Japan		9371	SAKURA-CSAKURAInternetIncJP	true
1.13.186.125	www.yongleproducts.com	China		13335	CLOUDFLARENETUS	true
162.241.24.110	bohndigitaltech.com	United States		46606	UNIFIEDLAYER-AS-1US	true
219.94.129.181	kunimi.org	Japan		9371	SAKURA-CSAKURAInternetIncJP	true
162.0.231.77	www.traindic.top	Canada		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830435
Start date and time:	2023-03-20 11:27:15 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 22s
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:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Copyright Joe Security LLC 2023

Sample file name:	DHL_Notification_pdf.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/5@12/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 71.7% (good quality ratio 66.2%) • Quality average: 75.2% • Quality standard deviation: 30.7%
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- 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
11:28:23	API Interceptor	619x Sleep call for process: explorer.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\Temp\146E771M

Process:	C:\Windows\SysWOW64\cmmon32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	modified

Size (bytes):	94208
Entropy (8bit):	1.2889923589460437
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJP/6oVuss8Ewn7PrH944:QS/inXrVuss8Ewn7b944
MD5:	7901DD9DF50A993306401B7360977746
SHA1:	E5BA33E47A3A76CC009EC1D63C5D1A810BE40521
SHA-256:	1019C8ADA4DA9DEF665F59DB191CA3A613F954C12813BE5907E1F5CB91C09BE9
SHA-512:	90C785D22D0D7F5DA90D52B14010719A5554BB5A7F0029C3F4E11A97AD72A7A600D846174C7B40D47D24B0995CDBAC21E255EC63AC9C07CF6E106572EA181D5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\ldndbi.exe

Process:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	95744
Entropy (8bit):	6.22620721848125
Encrypted:	false
SSDEEP:	1536:X0ZIV4KXc4OxQEsGZDmS+jtBaK/eRuZocSZUpxwkyBp+NnFsSW81kxgsWJjcdvhk:Ed4KALsGZDN+x/yuZocSTkyBw9y8eASK
MD5:	C99B9B59B44F7789DD46E5230C22A9CD
SHA1:	A4551975A1003A0309AE3EEF35FF0183E388707B
SHA-256:	FC5D8E04A8C7A63B993963ABB0A4BA5DD1203818CCA5A04221A0E0470F2A3D1A
SHA-512:	DE8ED5C68B001D32D71DFAE1D9A30D1128848131F77A2FDD64B5E8C047D0E796B52335033F718BC89F0BFEED15517AE038468D227F4ED4A43E63CB51BD75F7E
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 19%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7...s...s...s...8...y...8.....8...g.....U.....b.....`...8...j...s.....r.....r..Richs.....PE..L.....d.....!.....|.....".....@.....|k.....^.....]..@..... .....text..... ..`.rdata...f.....h.....@..@.data...l.....l.....@..... ....

C:\Users\user\AppData\Local\Temp\nsw10F5.tmp

Process:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	326174
Entropy (8bit):	7.563897951059429
Encrypted:	false
SSDEEP:	6144:1d/7iDj8MH9T02nVWHI/MPkICJa6D22lOqwNjuGKGsGZExocCm:PgjH9A2UH05ICwjw/wNjuGKGsHG
MD5:	E835C61DF57229CDB9D3E96D0C7E8201
SHA1:	79E878C0BD2109C17F1273D61856822AFE949E60
SHA-256:	5F43497768944110E3B665872721D20A11F40A0691DD6FCA543A782FE47060D3
SHA-512:	42E90C700FDBAD71D280F1755DEF646BA74AB2D0485F5B07DBF4E6F4FB843C378B923D1049F17CE10C0BE52770418813E82BBE028938BBFEC3EA45882344E22E
Malicious:	false
Preview:	X7.....,.....t...&.....6.....X7..... .....G.....j.....L.....6..... ....

C:\Users\user\AppData\Local\Temp\qlqjt.de

Process:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	5950
Entropy (8bit):	7.1560009193344385

Encrypted:	false
SSDEEP:	96:Farc6oYhg/DrYuAk2XO5oSw0i3D9pdn4m3dwnHgzU15FE9ORPmCsCmbvrfjXC:FarcRRIhX1SJaDNn4maAzU15gJLrLXC
MD5:	A994E285DD19803FB9EC4341608FA3BD
SHA1:	D5D88C4A0C0DD00CF6120AAC684492BC28203088
SHA-256:	95E31DD67CAED4C3E24EAA150BBF40B380AE7DCB308639D45539675A66D827E4
SHA-512:	3BEAFB9225621703067B76099FCA5A9D012F9CB9078F2FB32B6EB803EA2BCE7E6D75598D5DADA3D721F50CA67FFBA3850BCB21A3AADAB73414052F3A03B8E1C6
Malicious:	false
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.;.q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\tfnqr.hy

Process:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	210296
Entropy (8bit):	**7.998895711202933**
Encrypted:	**true**
SSDEEP:	6144:kd/7iDj8MH9T02nVWHI/MPkICJa6D22lOq4:mgjH9A2UH05ICwjw/4
MD5:	1A4214B2D0C61B85EAB942BAA8B90A45
SHA1:	48AEB34FBB99C2AC55961F17F84E1C3EE0740EAF
SHA-256:	B12B5EB17E8DC4DBC3A9FB16736BCE60E097346E92367195081185 10CC9092E1
SHA-512:	E1BD0FA394F3B555A43D62C294EEA6385AE57A1254994FA34644DABFD6BB4208E16A032DA00C8656FC1AEDC9A57DD3FA72599B03FF098FC39EC085B4C90E445C
Malicious:	false
Preview:	.%A.....<^...dz3..'..k.Vp.....;J..8.ubm._rl./.h....1..&..Xg.5JN.....P.%A.h.j.\...8..j.....T...y!..:...s....E.V"..9.R,..r~.X.~...b.EE.&.jt...KG.>.J.p..f..*.r.\M.....!..V..Xv).Y..a"..... J..\..j.T.....@.T.V.s...r...u..&A.vR_.8B..KR.G.L.....W...N.X.'..P-..s...-J.8..bm._#l.#.h....H1..&..Xh.5J..A...,YY.).=....|df.!..\.....].. ..i...3../[..M.kX....."..9.R,..T.P....*z.....F.Q*.U. ..]....I...x.....!..\...v).1.ba..8.....J....=LT/....@.T.V.s-..r.r.u..sA.v._..B...R.?.L.....W...N.T'.h.P-..s...;J..8.ubm._rl./.h....1..&..Xh.5J..A...,YY.).=....|df.!..\.....].. ..i...3../[..M.kX....."..9.R,..T.P....*z.....F.Q*.U...]....I...x.....!..V..Xv)....a..8.....J....=LT.....@.T.V.s-..r.r.u..sA.v._..B...R.?.L.....W...N.T'.h.P-..s...;J..8.ubm._rl./.h....1..&..Xh.5J..A...,YY.) .=....|df.!..\.....].. ..i...3../[..M.kX....."..9.R,..T.P....*z.....F.Q*.U...]....I...x.....!..V..Xv)....a..8.....J....=LT.....@.T.V.s

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.92568389123595
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:	DHL_Notification_pdf.exe
File size:	299346
MD5:	06f7894017e8f6737d228adc14480c83
SHA1:	fab1cbdbbb5fc2e76de2622948a02c3e8af17c18
SHA256:	bbfb2aacf1ff431d0ed71b54c499d3a56b6bcc90d5137cd78097b40c354c2353
SHA512:	a88448b4853746bb49d2640e5f23796187e6234f744ee006c687e93197f9dee86cf826259b2480879dcf00dad0b98355dd49298ece63f0bc32f1d356b3f3d8d6
SSDEEP:	6144:PYa6brXt83aw4ZaNEQRd0SyjNmzvw/gAn/lfVuMqs6sV3jQl:PYRrXtCJ4Zazd0SyxEvwYA/l9l6s1je
TLSH:	C654128023E4C4EADCE10E316E3ADAAEA5FFDA251064564F37953F8679617D2DD0E302
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FA6B0ABA0EAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx

Instruction
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FA6B0ABA0BAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

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	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xce8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.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	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0xce8	0xe00	False	0.4224330357142857	data	4.238068683037627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country

Copyright Joe Security LLC 2023

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b1d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x3b4c0	0x100	data	English	United States
RT_DIALOG	0x3b5c0	0x11c	data	English	United States
RT_DIALOG	0x3b6e0	0x60	data	English	United States
RT_GROUP_ICON	0x3b740	0x14	data	English	United States
RT_VERSION	0x3b758	0x24c	data	English	United States
RT_MANIFEST	0x3b9a8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

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

Possible Origin

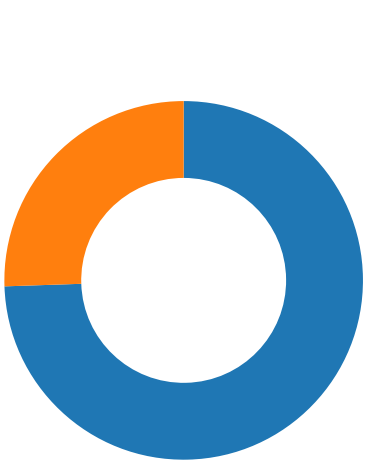
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.78.8.8.8.8505135 32023883 03/20/23-11:29:43.795616	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	50513	53	192.168.2.7	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:28:47.445717096 CET	49702	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:28:50.459781885 CET	49702	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:28:56.460304022 CET	49702	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:29:10.232919931 CET	49703	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:29:13.243027925 CET	49703	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:29:16.992034912 CET	49704	80	192.168.2.7	198.46.160.97
Mar 20, 2023 11:29:17.113477945 CET	80	49704	198.46.160.97	192.168.2.7
Mar 20, 2023 11:29:17.113718033 CET	49704	80	192.168.2.7	198.46.160.97
Mar 20, 2023 11:29:17.113889933 CET	49704	80	192.168.2.7	198.46.160.97
Mar 20, 2023 11:29:17.235318899 CET	80	49704	198.46.160.97	192.168.2.7
Mar 20, 2023 11:29:17.235604048 CET	80	49704	198.46.160.97	192.168.2.7
Mar 20, 2023 11:29:17.235634089 CET	80	49704	198.46.160.97	192.168.2.7
Mar 20, 2023 11:29:17.235824108 CET	49704	80	192.168.2.7	198.46.160.97
Mar 20, 2023 11:29:17.235997915 CET	49704	80	192.168.2.7	198.46.160.97
Mar 20, 2023 11:29:17.357302904 CET	80	49704	198.46.160.97	192.168.2.7
Mar 20, 2023 11:29:19.259192944 CET	49703	80	192.168.2.7	1.13.186.125
Mar 20, 2023 11:29:22.527839899 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:22.803483963 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:22.803628922 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:22.803774118 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.079303980 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.119358063 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407063007 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407105923 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407131910 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407161951 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407191038 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407196999 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.407217026 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407244921 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407264948 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.407269955 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407298088 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407324076 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.407330990 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.407362938 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.407388926 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.682904005 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.682940960 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.682967901 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.682996035 CET	80	49705	219.94.129.181	192.168.2.7

Copyright Joe Security LLC 2023

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:29:23.683026075 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683053017 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683075905 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683082104 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683108091 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683132887 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683157921 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683182955 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683187962 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683187962 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683211088 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683228970 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683242083 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683258057 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683273077 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683300972 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683331966 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683339119 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683373928 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683398008 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.683401108 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683425903 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.683479071 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.958991051 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959032059 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959053040 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959073067 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959094048 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959114075 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959135056 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959157944 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959163904 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959177971 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959197998 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959218025 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959237099 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959239006 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959259033 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959268093 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959280968 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959300995 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959311008 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959321976 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959353924 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959366083 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959374905 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959393978 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959394932 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959415913 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959438086 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959456921 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959458113 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959480047 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959494114 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959506989 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959526062 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959533930 CET	49705	80	192.168.2.7	219.94.129.181
Mar 20, 2023 11:29:23.959547043 CET	80	49705	219.94.129.181	192.168.2.7
Mar 20, 2023 11:29:23.959559917 CET	80	49705	219.94.129.181	192.168.2.7

Copyright Joe Security LLC 2023

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 11:28:47.359352112 CET	56588	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:28:47.383311033 CET	53	56588	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:10.199090004 CET	60326	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:10.222804070 CET	53	60326	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:16.961611032 CET	50835	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:16.990191936 CET	53	50835	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:22.251379967 CET	50505	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:22.526632071 CET	53	50505	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:31.374200106 CET	61178	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:31.394165993 CET	53	61178	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:32.418570995 CET	63926	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:32.440613031 CET	53	63926	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:37.463385105 CET	53336	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:37.600847006 CET	53	53336	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:38.619600058 CET	51007	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:38.787115097 CET	53	51007	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:43.795615911 CET	50513	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:43.897444963 CET	53	50513	8.8.8.8	192.168.2.7
Mar 20, 2023 11:29:56.792202950 CET	60765	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:29:56.933132887 CET	53	60765	8.8.8.8	192.168.2.7
Mar 20, 2023 11:30:05.017503023 CET	58283	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:30:05.039990902 CET	53	58283	8.8.8.8	192.168.2.7
Mar 20, 2023 11:30:12.980236053 CET	50024	53	192.168.2.7	8.8.8.8
Mar 20, 2023 11:30:13.238567114 CET	53	50024	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 11:28:47.359352112 CET	192.168.2.7	8.8.8.8	0x130a	Standard query (0)	www.yongle products.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:10.199090004 CET	192.168.2.7	8.8.8.8	0xab4b	Standard query (0)	www.yongle products.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:16.961611032 CET	192.168.2.7	8.8.8.8	0xcde2	Standard query (0)	www.0dhy.xyz	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:22.251379967 CET	192.168.2.7	8.8.8.8	0xf8f6	Standard query (0)	www.kunimi.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:31.374200106 CET	192.168.2.7	8.8.8.8	0x6e51	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:32.418570995 CET	192.168.2.7	8.8.8.8	0x5c46	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:37.463385105 CET	192.168.2.7	8.8.8.8	0xad3c	Standard query (0)	www.bisarr opainting.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:38.619600058 CET	192.168.2.7	8.8.8.8	0xd44d	Standard query (0)	www.bisarr opainting.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:43.795615911 CET	192.168.2.7	8.8.8.8	0x217e	Standard query (0)	www.traindic.top	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:56.792202950 CET	192.168.2.7	8.8.8.8	0xd494	Standard query (0)	www.bohndi gitaltech.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:30:05.017503023 CET	192.168.2.7	8.8.8.8	0xf4bd	Standard query (0)	www.rifler oofers.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:30:12.980236053 CET	192.168.2.7	8.8.8.8	0x89bd	Standard query (0)	www.denko-kosan.com	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 20, 2023 11:28:47.383311033 CET	8.8.8.8	192.168.2.7	0x130a	No error (0)	www.yongle products.com		1.13.186.125	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:10.222804070 CET	8.8.8.8	192.168.2.7	0xab4b	No error (0)	www.yongle products.com		1.13.186.125	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2023

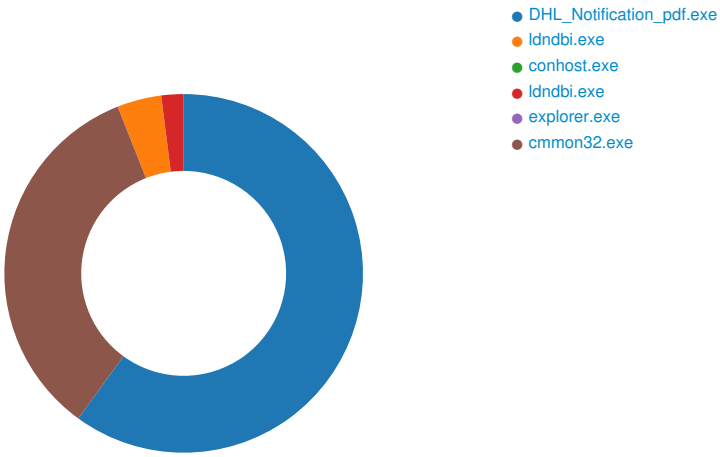
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 11:29:16.990191936 CET	8.8.8.8	192.168.2.7	0xcde2	No error (0)	www.0dhy.xyz		198.46.160.97	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:22.526632071 CET	8.8.8.8	192.168.2.7	0xf8f6	No error (0)	www.kunimi.org	kunimi.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:29:22.526632071 CET	8.8.8.8	192.168.2.7	0xf8f6	No error (0)	kunimi.org		219.94.129.181	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:31.394165993 CET	8.8.8.8	192.168.2.7	0x6e51	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:32.440613031 CET	8.8.8.8	192.168.2.7	0x5c46	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:37.600847006 CET	8.8.8.8	192.168.2.7	0xad3c	Name error (3)	www.bisarropainting.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:38.787115097 CET	8.8.8.8	192.168.2.7	0xd44d	Name error (3)	www.bisarropainting.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:43.897444963 CET	8.8.8.8	192.168.2.7	0x217e	No error (0)	www.traindic.top		162.0.231.77	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:29:56.933132887 CET	8.8.8.8	192.168.2.7	0xd494	No error (0)	www.bohndigitaltech.com	bohndigitaltech.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:29:56.933132887 CET	8.8.8.8	192.168.2.7	0xd494	No error (0)	bohndigitaltech.com		162.241.24.110	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:30:05.039990902 CET	8.8.8.8	192.168.2.7	0xf4bd	No error (0)	www.rifleroofers.com	rifleroofers.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:30:05.039990902 CET	8.8.8.8	192.168.2.7	0xf4bd	No error (0)	rifleroofers.com		67.222.24.48	A (IP address)	IN (0x0001)	false
Mar 20, 2023 11:30:13.238567114 CET	8.8.8.8	192.168.2.7	0x89bd	No error (0)	www.denko-kosan.com	denko-kosan.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 11:30:13.238567114 CET	8.8.8.8	192.168.2.7	0x89bd	No error (0)	denko-kosan.com		49.212.180.95	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.0dhy.xyz
- www.kunimi.org
- www.traindic.top
- www.bohndigitaltech.com
- www.rifleroofers.com
- www.denko-kosan.com

Statistics

Behavior



System Behavior

Analysis Process: DHL_Notification_pdf.exe PID: 5084, Parent PID: 3320

General

Target ID:	0
Start time:	11:28:11
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_Notification_pdf.exe
Imagebase:	0x400000
File size:	299346 bytes
MD5 hash:	06F7894017E8F6737D228ADC14480C83
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: ldndbi.exe PID: 3008, Parent PID: 5084

General

Target ID:	1
Start time:	11:28:11
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\ldndbi.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user~1\AppData\Local\Temp\ldndbi.exe" C:\Users\user~1\AppData\Local\Temp\qlqjt.de
Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	C99B9B59B44F7789DD46E5230C22A9CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 19%, ReversingLabs
Reputation:	low

File Activities

Copyright Joe Security LLC 2023

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qlqjt.de	unknown	4096	success or wait	1	407824	ReadFile
C:\Users\user\AppData\Local\Temp\qlqjt.de	unknown	4096	success or wait	1	407824	ReadFile

Analysis Process: conhost.exe PID: **4584**, Parent PID: **3008**

General

Target ID:	2
Start time:	11:28:12
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6edaf0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ldndbi.exe PID: **6108**, Parent PID: **3008**

General

Target ID:	3
Start time:	11:28:13
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\ldndbi.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\ldndbi.exe
Imagebase:	0x400000
File size:	95744 bytes
MD5 hash:	C99B9B59B44F7789DD46E5230C22A9CD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.290138385.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.290138385.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.290138385.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.290222663.0000000000490000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.290222663.0000000000490000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.290222663.0000000000490000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.292007151.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.292007151.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.292007151.0000000000D20000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E62A	NtReadFile

Analysis Process: explorer.exe PID: **3320**, Parent PID: **6108**

General

Target ID:	4
Start time:	11:28:18
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff75ed40000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmmon32.exe PID: **5228**, Parent PID: **3320**

General

Target ID:	5
Start time:	11:28:31
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x1200000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.508997363.0000000000E50000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.508740330.0000000000C00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.508740330.0000000000C00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.508740330.0000000000C00000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.509702408.00000000011A0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.509702408.00000000011A0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.509702408.00000000011A0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA

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	C1CF4E	HttpSendRequestA
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	C1CF4E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	C1CF4E	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user~1\AppData\Local\Temp\ldndbi.exe	success or wait	1	C1C867	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\146E771M	object name not found	1	C1C867	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\146E771M	sharing violation	1	C1C867	NtDeleteFile
C:\Users\user~1\AppData\Local\Temp\146E771M	sharing violation	1	C1C867	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	C1C837	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly