ID: 831175
Sample Name:
DHL_Notice_pdf.exe
Cookbook: default.jbs
Time: 08:06:06
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

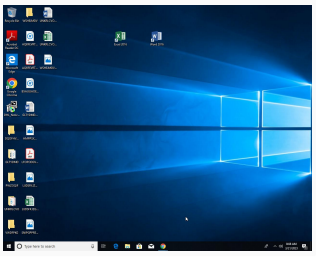
Windows Analysis Report

DHL_Notice_pdf.exe

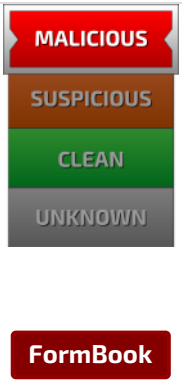
Overview

General Information

Sample Name:	DHL_Notice_pdf.exe
Analysis ID:	831175
MD5:	771508cf2751f…
SHA1:	f6d7d33b6a340..
SHA256:	652948efee89f…
Tags:	exe Formbook
Infos:	



Detection



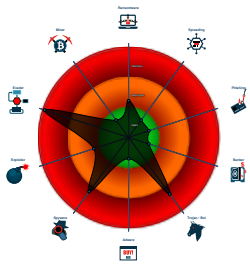
FormBook

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_Notice_pdf.exe (PID: 2080 cmdline: C:\Users\user\Desktop\DHL_Notice_pdf.exe MD5: 771508CF2751F6DABE05758E4FA25FDF)
  - zkvixbqxp.exe (PID: 6136 cmdline: "C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe" C:\Users\user\AppData\Local\Temp\thztifyh.t MD5: BE5A6985BCDCA9064A05D26CFB8D082E)
    - conhost.exe (PID: 6132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - zkvixbqxp.exe (PID: 5244 cmdline: C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe MD5: BE5A6985BCDCA9064A05D26CFB8D082E)
      - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmmon32.exe (PID: 5080 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

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp	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:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19e08:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x198a4:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x19f0a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a082:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc7ed:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18aff:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fb7a:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20b2d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.274142159.00000000008D0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.274142159.00000000008D0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1efd0:$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

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.zkvixbqxp.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.zkvixbqxp.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:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.zkvixbqxp.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19008:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.zkvixbqxp.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.zkvixbqxp.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20dc3:$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

Snort Signatures

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.38.8.8.851139532023883 03/21/23-08:08:13.337564
SID:	2023883
Source Port:	51139
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)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

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

Yara detected FormBook

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

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

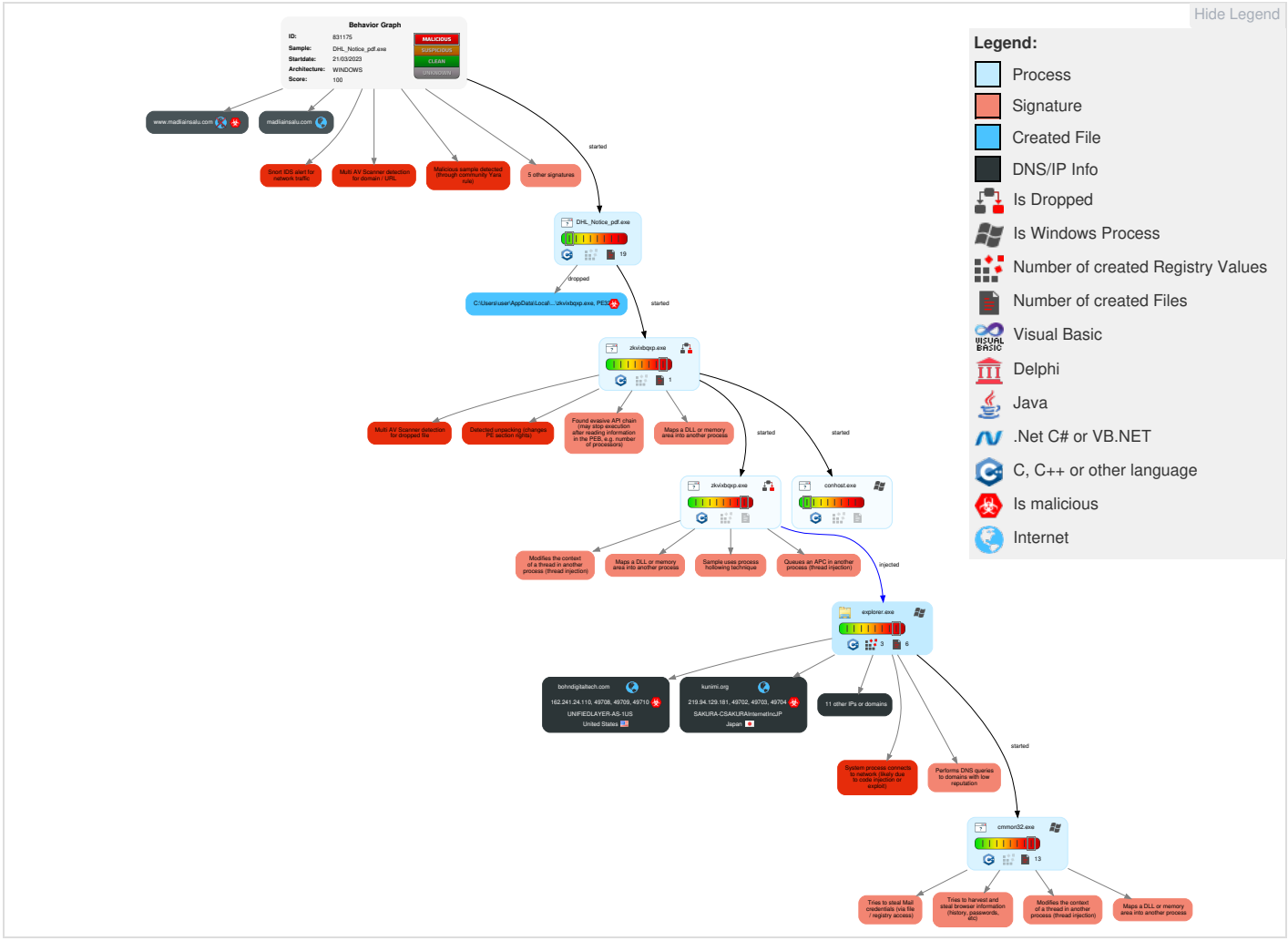
Remote Access Functionality

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 Native API	Path Interception	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	5 1 2 Process Injection	3 Obfuscated Files or Information	LSASS Memory	5 System Information 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 2 1 Security Software 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	2 Virtualization/Sandbox Evasion	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 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	1 Application Window 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 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

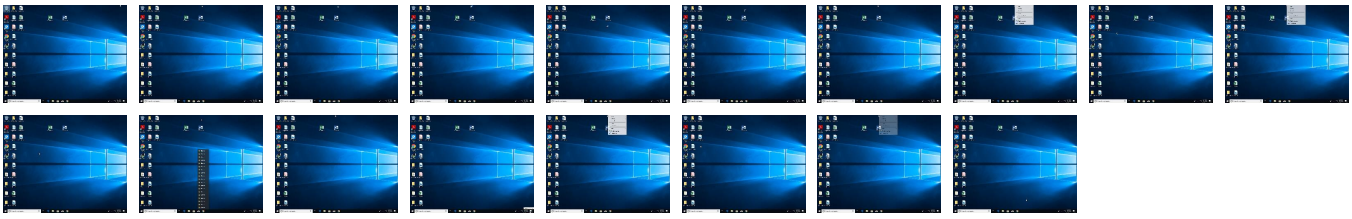
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL_Notice_pdf.exe	46%	ReversingLabs	Win32.Trojan.Fragtor	
DHL_Notice_pdf.exe	42%	Virustotal		Browse
DHL_Notice_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe	27%	ReversingLabs	Win32.Trojan.Fragtor	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.zkvixbqxp.exe.9f0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.zkvixbqxp.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

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.buymyenergy.com	0%	Avira URL Cloud	safe	
http://www.yongleproducts.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=qNzMMFnF92wYqby+PK0Ez7hJYWSZzqH1hiqfKssSJUPL9XRjbsSUYneeVaUFujlDIgVdAeBkPDqj9kdbdEfqEoULBaI9U5csBw==	100%	Avira URL Cloud	malware	
http://www.bohndigitaltech.com	0%	Avira URL Cloud	safe	
http://www.0dhy.xyz/hpb7/?bcX3Uv=BrlYCq9+qqzfybZpwXKugHGOc0m4ktDYrdhK4pNzcFj3gilCUF3BZQEP3ssdPmgNj5Kg/PdRxbVpWQCkOBnIEYQcZEeIna030A==&xN_j=yFbSaCxwQG4Y-X	100%	Avira URL Cloud	malware	
http://www.kunimi.org	0%	Avira URL Cloud	safe	
http://kunimi.org/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/ll/ds	0%	Avira URL Cloud	safe	
http://www.buymyenergy.comReferer:	0%	Avira URL Cloud	safe	
http://www.kunimi.org/hpb7/	0%	Avira URL Cloud	safe	
http://www.kunimi.org/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/ll/dsCibnuekbaxwoyPtCZtmftv1iNZwvaen+NIMKLdu8Y9hsRKcKA==	0%	Avira URL Cloud	safe	
http://www.mindsetlighting.xyz/hpb7/	100%	Avira URL Cloud	malware	
http://www.amirah.cfd/hpb7/	100%	Avira URL Cloud	phishing	
http://www.amirah.cfd	100%	Avira URL Cloud	phishing	
http://www.bisarropainting.com/hpb7/:	0%	Avira URL Cloud	safe	
http://www.0dhy.xyz/hpb7/	100%	Avira URL Cloud	malware	
http://www.admet01.clubReferer:	0%	Avira URL Cloud	safe	
http://www.adoptiveimmunotech.com/hpb7/	100%	Avira URL Cloud	malware	
http://www.bohndigitaltech.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.bohndigitaltech.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=+QEmeUzOQAV/evbBmcNZRFxNHMmEBYUw3TD399HaSALRcdrdntvE2stvjFfWDoHleQ7kMHGKc1CQfriDp0hgoRSMDh0fNxliSQ==	0%	Avira URL Cloud	safe	
http://www.traindic.top/hpb7/	100%	Avira URL Cloud	malware	
http://www.kunimi.org/hpb7/I	0%	Avira URL Cloud	safe	
http://www.creative-shield.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.madliainsalu.comReferer:	0%	Avira URL Cloud	safe	
http://www.kotelak.ru	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com/hpb7/	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.traindic.top/hpb7/?bcX3Uv=bTtFiHq0GQrF6aFlJXqsXsYFYYSgPtrX4CJLxcpJGK/F7H1QBurO56xriJCe1rAnTJlhkBPAE1A8g1vh/R7KfM22DyUBSGy/9w==&xN_j=yFbSaCxwQG4Y-X	100%	Avira URL Cloud	malware	
http://www.kotelak.ru/hpb7/	0%	Avira URL Cloud	safe	
http://www.amirah.cfdReferer:	0%	Avira URL Cloud	safe	
http://www.creative-shield.com/hpb7/:	0%	Avira URL Cloud	safe	
http://www.admet01.club	100%	Avira URL Cloud	malware	
http://www.rifleroofers.com/hpb7/?bcX3Uv=Sr1AjUgE1bmYtN0hdeH1+2eYW2bz9zJly7x8VWFTjEXaDkIuvqWhFoT+O4ddqC6+eWArdJNQDIDq/++CVSPV2yhYsiVz8XiXvw==&xN_j=yFbSaCxwQG4Y-X	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.madliainsalu.com	0%	Avira URL Cloud	safe	
http://www.kotelak.ruReferer:	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com	0%	Avira URL Cloud	safe	
http://www.madliainsalu.com/hpb7/	0%	Avira URL Cloud	safe	
http://www.rifleroofers.com	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.adoptiveimmunotech.comReferer:	0%	Avira URL Cloud	safe	
http://www.creative-shield.com	0%	Avira URL Cloud	safe	
http://www.rifleroofers.com/hpb7/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.denko-kosan.comReferer:	0%	Avira URL Cloud	safe	
http://rifleroofers.com/hpb7/?bcX3Uv=Sr1AjUgE1bmYtN0hdeH1	0%	Avira URL Cloud	safe	
http://www.traindic.top	100%	Avira URL Cloud	malware	
http://www.creative-shield.comReferer:	0%	Avira URL Cloud	safe	
http://www.adoptiveimmunotech.com	0%	Avira URL Cloud	safe	
http://www.yongleproducts.com/hpb7/	100%	Avira URL Cloud	malware	
http://www.admet01.club/hpb7/	100%	Avira URL Cloud	malware	
http://www.bisarropainting.comReferer:	0%	Avira URL Cloud	safe	
http://www.yongleproducts.com	0%	Avira URL Cloud	safe	
http://www.bisarropainting.com	0%	Avira URL Cloud	safe	
http://www.denko-kosan.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=NuHAd+vfjtmC4E+cdz1CpM6J6ScGh9KWfGXGi6oH+281UYUkr6SouFSZ7LMQAOLiSk3FYsgr8Pu9aCQzqq/bHuqb5CQESJqHRQ==	0%	Avira URL Cloud	safe	
http://www.mindsetlighting.xyz	100%	Avira URL Cloud	malware	

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
madliainsalu.com	34.120.137.41	true	false		unknown
denko-kosan.com	49.212.180.95	true	true		unknown
windowsupdatebg.s.llnwi.net	95.140.230.128	true	false		unknown
www.bohndigitaltech.com	unknown	unknown	true		unknown
www.madliainsalu.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.yongleproducts.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=qNzMMFnF92wYqby+PK0Ez7hJYWSZzqH1hiqfKssSJUPL9XRjbsSUYneeVaUFujlDIgVdAeBkPDqj9kdbdEfqEoULBaI9U5csBw==	true	• Avira URL Cloud: malware	unknown
http://www.0dhy.xyz/hpb7/?bcX3Uv=BrlYCq9+qqzfybZpwXKugHGOc0m4ktDYrdhK4pNzcFj3giICUF3BZQEP3ssdPmgNj5Kg/PdRxbVpWQCkOBnIEYQcZEeIna030A==&xN_j=yFbSaCxwQG4Y-X	true	• Avira URL Cloud: malware	unknown
http://www.0dhy.xyz/hpb7/	true	• Avira URL Cloud: malware	unknown
http://www.kunimi.org/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/ll/dsCibnuekbaxwoyPtCZtmftv1iNZwvaen+NIMKLdu8Y9hsRKcKA==	true	• Avira URL Cloud: safe	unknown
http://www.kunimi.org/hpb7/	true	• Avira URL Cloud: safe	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.bohndigitaltech.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=+QEmeUzOQAV/evbBmcNZRFxNHMmEBYUw3TD399HaSALRcdrdntvE2stvjFfWDoHleQ7kMHGKc1CQfriDp0hgoRSMDh0fNxliSQ==	true	• Avira URL Cloud: safe	unknown
http://www.denko-kosan.com/hpb7/	true	• Avira URL Cloud: safe	unknown
http://www.traindic.top/hpb7/?bcX3Uv=bTtFiHq0GQrF6aFlJXqsXsYFYYSgPtrX4CJLxcpJGK/F7H1QBurO56xriJCe1rAnTJlhkBPAE1A8g1vh/R7KfM22DyUBSGy/9w==&xN_j=yFbSaCxwQG4Y-X	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.rifleroofers.com/hpb7/?bcX3Uv=Sr1AjUgE1bmYtN0hdeH1+2eYW2bz9zJly7x8VWFTjEXaDkIuvqWhFoT+O4ddqC6+eWArdJNQDIDq/++CVSPV2yhYsiVz8XiXvw==&xN_j=yFbSaCxwQG4Y-X	true	• Avira URL Cloud: safe	unknown
http://www.rifleroofers.com/hpb7/	true	• Avira URL Cloud: safe	unknown
http://www.denko-kosan.com/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=NuHAd+vfjtmC4E+cdz1CpM6J6ScGh9KWfGXGi6oH+281UYUkr6SouFSZ7LMQAOLiSk3FYsgr8Pu9aCQzqq/bHuqb5CQESJqHRQ==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

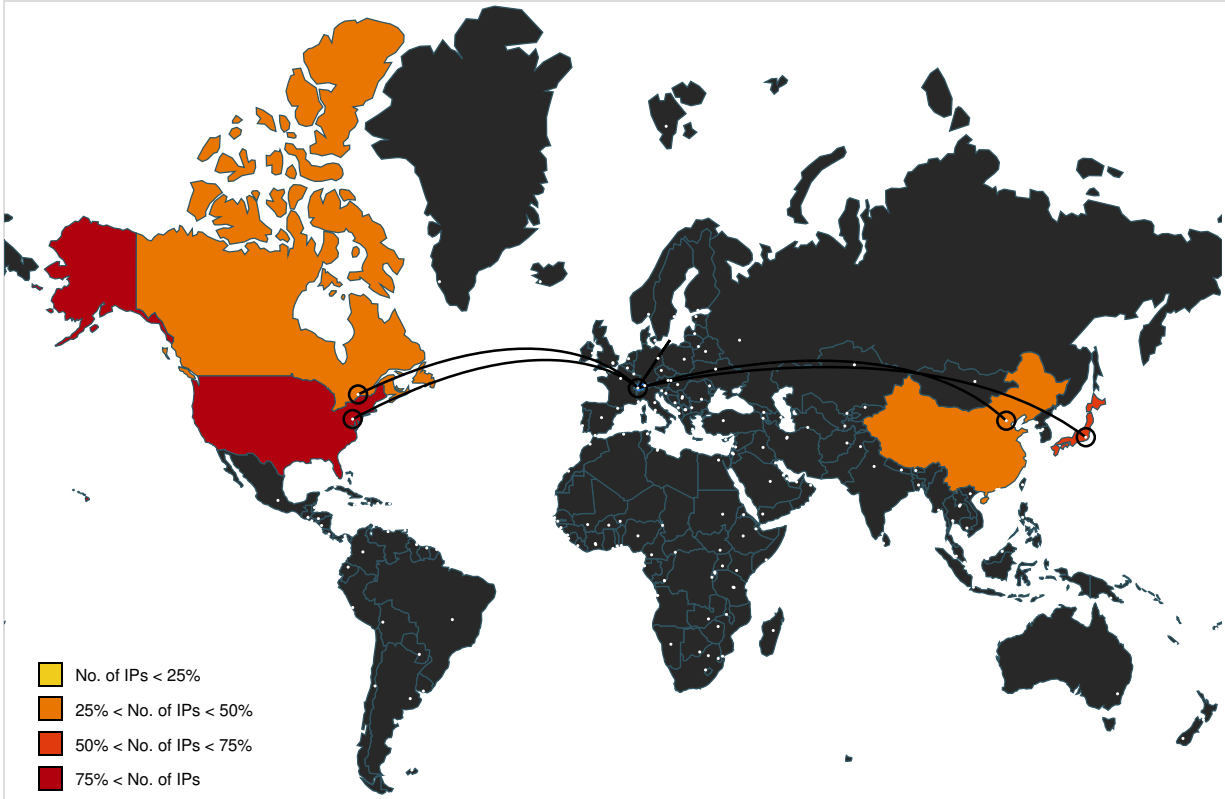
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.kunimi.org	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	cmmon32.exe, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://https://duckduckgo.com/ac/?q=	146E771M.5.dr	false		high
http://www.buymyenergy.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mindsetlighting.xyz/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.bohndigitaltech.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://kunimi.org/hpb7/?xN_j=yFbSaCxwQG4Y-X&bcX3Uv=LsyOeIgM/ET1t5hHa8GhcP6qBeQiLfhDrF81hKHttqb/ll/ds	explorer.exe, 00000004.00000002.51740443 6.000000001584A000.00000004.80000000.000 40000.00000000.sdmp, cmmon32.exe, 000000 05.00000002.506713363.0000000004EEA000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.amirah.cfd	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	cmmon32.exe, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.amirah.cfd/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: phishing	unknown
http://www.buymyenergy.comReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bisarropainting.com/hpb7/:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.admet01.clubReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adoptiveimmunotech.com/hpb7/	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.madliainsalu.comReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kunimi.org/hpb7/l	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.creative-shield.com/hpb7/	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ru	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.0dhy.xyz	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bohndigitaltech.com/hpb7/Xz.	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.amirah.cfdReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ru/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.creative-shield.com/hpb7/:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.admet01.club	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.adoptiveimmunotech.com/hpb7/j	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.bisarropainting.com/hpb7/	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 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, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.madliainsalu.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kotelak.ruReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rifleroofers.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.denko-kosan.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.513596661.000000000B74D000. 00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000004.00000003.473910844.000000 0009297000.00000004.00000001.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.madliainsalu.com/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mindsetlighting.xyzReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.buymyenergy.com/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 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, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://search.yahoo.com/favicon.icohttps://search.yah oo.com/search	cmmon32.exe, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.adoptiveimmunotech.comReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	DHL_Notice_pdf.exe	false		high
http://www.creative-shield.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 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, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://rifleroofers.com/hpb7/? bcX3Uv=Sr1AjUgE1bmYtN0hdeH1	explorer.exe, 00000004.00000002.51740443 6.0000000016024000.00000004.80000000.000 40000.00000000.sdmp, cmmon32.exe, 000000 05.00000002.506713363.00000000056C4000.0 0000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.adoptiveimmunotech.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.creative-shield.comReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 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, 00000005.00000003.315194802 .0000000000449000.00000004.00000020.0002 0000.00000000.sdmp, 146E771M.5.dr	false		high
http://www.traindic.top	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.admet01.club/hpb7/	explorer.exe, 00000004.00000003.47391084 4.0000000009297000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.yongleproducts.com/hpb7/	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.bisarropainting.comReferer:	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttp s://www.ecosia.org/search?q=	146E771M.5.dr	false		high
http://www.bisarropainting.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.yongleproducts.com	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mindsetlighting.xyz	explorer.exe, 00000004.00000002.51325349 6.0000000009297000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.473910844.0000000009297000. 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:	831175
Start date and time:	2023-03-21 08:06:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 1s
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
Sample file name:	DHL_Notice_pdf.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/5@14/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 65.2% (good quality ratio 59.3%) • Quality average: 72.2% • Quality standard deviation: 31.8%
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 IPs from analysis (whitelisted): 93.184.221.240, 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, wu.ec.azureedge.net, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net
- 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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:07:18	API Interceptor	467x 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 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\bwgyj.py

Process:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	209991
Entropy (8bit):	**7.998709566109535**
Encrypted:	**true**
SSDEEP:	3072:GOVZQocPBPtCQ8T+EZ/9vRImoqPeTVKaoQQe8esYNdoytWygtFK1b2fH3HFOM0SZ:GOXQocQ+EK9TVKEYydky+XfHPpYFZG/
MD5:	9203F8F38EDD3B6CEE9B5647706C4747
SHA1:	9EA9A90EB73A07AC7B6710D752A1A2DCC7E0ED76
SHA-256:	4B2DB80CC55681E7CD277C2DC4BD5BB67E1E4EE03F4665D214DBC9BBECCABFC8
SHA-512:	0669801D821650A9AF04D35BBAEE776B2D91A09A0E4630AB7EB22C93711FE57E9FF76268953ED918CE98F8DE22AFB0C8AAEA11BDFE91CBE245743EB273C56B69
Malicious:	false
Reputation:	low
Preview:	.....7..d..ga...}7.'.G.....#.,...b..... ..K.....X$.9..B..[...usn.....o5..}.....l.5=C.`.{..}v.b..B.....u.w...V..v1&p...P.h!.....~.7..M.....R.am..&\....P.....E....t..v.?.C....7.v....Zb&o2.. .F8.&V...Y}Q..aI.....m.`\|....gR`...7.....H."@..'D..h.A).hk..hb.D... R.K3.....v$.9..B..[.G...s..(...r..g.$X...b.Or.}.f..R.....Y^G....+m.....w...V:..6.."...W..x...<.U...f#4=MK..!..\ '..,.....E....5Y.k.?.\|.:.....!sv..Zb&o2.....d....XQ..aI.....m.`\|c...,go`...7..d....H."@=.'D....h.A?..,...b..... ..K.....X$.9..B..[.G...s..(...r..g.$X...b.Or.}.f..R.....Y^G....+m.... ....w...V:..6.."...W..x...<.U...f#4=MK..!..\'.,.....E....t..v.?."....`.v.Zb&o2.....d...}Q..aI.....m.`\|c...,go`...7..d....H."@=.'D....h.A?..,...b..... ..K.....X$.9..B..[.G...s..(. ..r..g.$X...b.Or.}.f..R.....Y^G....+m.....w...V:..6.."...W..x...<.U...f#4=MK..!..\'.,.....E....t..v.?."....`.v.Zb&o2.....d...}Q..aI...

C:\Users\user\AppData\Local\Temp\nsd7F3C.tmp

Process:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	233940
Entropy (8bit):	7.852327544537286
Encrypted:	false
SSDEEP:	3072:2sOVZQocPBPtCQ8T+EZ/9vRImoqPeTVKaoQQe8esYNdoytWygtFK1b2fH3HFOM0N:XOXQocQ+EK9TVKEYydky+XfHPpYFZGw
MD5:	CB7BDC432B7BA8C7ED8B489D5F08A081
SHA1:	A58E23586ED03EBB8B0D7670383F92C80F07D9A5
SHA-256:	81E2187A7CD1186869B5F492E68CBAC1EF8B404DD893EF9AC7295093C6C8C227
SHA-512:	5FD7458B503BA3AE3514236B2FFBE4AEED27E651994F8C2BDC50BFCAF8A7D1E5705CF7FFDE87A7BB144B72FFA2E52F3DF97B139610C5448BA91B75312188BFFB
Malicious:	false
Reputation:	low
Preview:	./.....,..... ...../.....7..... .....G.....M...j.....}.....N..... ....

C:\Users\user\AppData\Local\Temp\thztifyh.t	
Process:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	6099
Entropy (8bit):	7.134928677733547
Encrypted:	false
SSDEEP:	96:Farc6oY0Wg/DrYuDk2XO5oSw09LFQiY3XdQSkwKOYJ8CJZT0v81DJi6p:FarcRTrhX1SJ9LOn3tRkwtxE1D7
MD5:	0A06F95BA28B6704B7DBC7F68D1B5BE4
SHA1:	F1118B8640DFB7533F744FBD8CD24780D04650CD
SHA-256:	4F6DAE66BA6DC6B3EBBABD57F2A4404AF38452EC3677A779D5F41A378982B0E1
SHA-512:	417FB43A079FEC2A3702EA562E51A3E5EAEFD64D753302A3BC31AE867E2C50AE8D081883D247433F6A09C71C83EF09BFFF0B38942C1A14DEA3D60435E1B5068
Malicious:	false
Reputation:	low
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\zkvixbqxp.exe	
Process:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.4633891846895075
Encrypted:	false
SSDEEP:	96:G8wZF3bluZzQb5P4oyn/7JhpywpZ6uYHrAhBPxesU8:G8UF3bY1SP4oynl/ycZ6uYHrSBwsU8
MD5:	BE5A6985BCDCA9064A05D26CFB8D082E
SHA1:	5EB04D667D4E5A5B453ED028083423FA810EA5C4
SHA-256:	E05AF06D3928D4583C5B2B2C433B9189411EB48F39D5CBAAFED06F5CB27B3B20
SHA-512:	F2EBA81E5E658E4FF486C796F90CE80B664DA91349181B901D9B8DE96D8DA85E40F389897F5AC94228F4073ABA6B4946A5728D08A5BAE720D1FB3A592F5B105
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I...(.@.(.@.(.@.@.A.(.@.(.@.(.@K7.@.(.@ 4.@.(.@K7.@. (.@.v.A.(.@.v.A.(.@Rich.(.@.....PE..L.....d..... ....@.....@.....".....!..... ....text..... ..`.rdata..:.... .....@..@.data.....0.....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.905063780230514
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_Notice_pdf.exe
File size:	255238
MD5:	771508cf2751f6dabe05758e4fa25fdf
SHA1:	f6d7d33b6a340d2c370ca31a6f9677a2e5306486
SHA256:	652948efee89fdc5c6d3dc7f65a16aafabd0d224c9fcd55e5f86573f1b2c4aa1
SHA512:	437bca115b12044ff08264218c4ab6546a345b5fe2e6ed89d09cbbaf51f77522afc4e9004cb88e229ee3b0687faf611d30a346b953bbd8eaba0a3ece7df4fdb8
SSDEEP:	6144:/Ya6h4vRbB2TXukTFPqjpsaKncVt9I7GmmEE09z:/Yb4vRbB2Ldgjua2cplymmEE09z
TLSH:	6944124847E4E0BFE4A246701DFA62BA5BF4B52E9475410B63C02B697E726B15F0F332

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 00007F3D28E0F87Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi

Instruction
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
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F3D28E0F84Ah
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	0xcd0	.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0xcd0	0xe00	False	0.421875	data	4.212531507733574	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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	0x234	data	English	United States
RT_MANIFEST	0x3b990	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
192.168.2.38.8.8.8511395 32023883 03/21/23-08:08:13.337564	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	51139	53	192.168.2.3	8.8.8.8

Network Port Distribution

Total Packets: 52

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 08:07:24.635210037 CET	49698	80	192.168.2.3	1.13.186.125
Mar 21, 2023 08:07:24.914064884 CET	80	49698	1.13.186.125	192.168.2.3
Mar 21, 2023 08:07:24.914180994 CET	49698	80	192.168.2.3	1.13.186.125
Mar 21, 2023 08:07:24.914344072 CET	49698	80	192.168.2.3	1.13.186.125
Mar 21, 2023 08:07:25.192853928 CET	80	49698	1.13.186.125	192.168.2.3
Mar 21, 2023 08:07:25.192886114 CET	80	49698	1.13.186.125	192.168.2.3
Mar 21, 2023 08:07:25.193101883 CET	49698	80	192.168.2.3	1.13.186.125
Mar 21, 2023 08:07:25.193608046 CET	49698	80	192.168.2.3	1.13.186.125
Mar 21, 2023 08:07:25.470067978 CET	80	49698	1.13.186.125	192.168.2.3
Mar 21, 2023 08:07:35.689584017 CET	49699	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:35.807986975 CET	80	49699	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:35.808240891 CET	49699	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:35.808631897 CET	49699	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:35.926683903 CET	80	49699	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:35.927187920 CET	80	49699	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:35.927232027 CET	80	49699	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:35.927345991 CET	49699	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:37.316317081 CET	49699	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.332834005 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.451946974 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.452183008 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.452894926 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.570954084 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.571013927 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.571064949 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.571118116 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.571166992 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:38.571203947 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.571327925 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:38.689445019 CET	80	49700	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:39.957168102 CET	49700	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:40.973077059 CET	49701	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:41.091538906 CET	80	49701	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:41.091763973 CET	49701	80	192.168.2.3	198.46.160.97

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 08:07:41.091881037 CET	49701	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:41.209954977 CET	80	49701	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:41.210010052 CET	80	49701	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:41.210052967 CET	80	49701	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:41.210269928 CET	49701	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:41.210458040 CET	49701	80	192.168.2.3	198.46.160.97
Mar 21, 2023 08:07:41.328169107 CET	80	49701	198.46.160.97	192.168.2.3
Mar 21, 2023 08:07:46.758717060 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:47.058943987 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:47.059135914 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:47.061011076 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:47.360769033 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:47.398175955 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162316084 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162358046 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162380934 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162405014 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162431955 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162456036 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162482023 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162507057 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162525892 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.162532091 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162525892 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.162559032 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.162602901 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.162622929 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462626934 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462658882 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462677002 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462708950 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462730885 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462744951 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462758064 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462771893 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462784052 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462796926 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462794065 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462810993 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462824106 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462836981 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462857008 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462863922 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462878942 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462898016 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462907076 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462918043 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462928057 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462939978 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.462946892 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.462986946 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.763036966 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763091087 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763138056 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763184071 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763202906 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.763230085 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763256073 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.763283014 CET	80	49702	219.94.129.181	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 08:07:48.763330936 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763338089 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.763379097 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763426065 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763433933 CET	49702	80	192.168.2.3	219.94.129.181
Mar 21, 2023 08:07:48.763473034 CET	80	49702	219.94.129.181	192.168.2.3
Mar 21, 2023 08:07:48.763521910 CET	80	49702	219.94.129.181	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 08:07:24.608470917 CET	62704	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:07:24.629987955 CET	53	62704	8.8.8.8	192.168.2.3
Mar 21, 2023 08:07:35.665481091 CET	49977	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:07:35.687676907 CET	53	49977	8.8.8.8	192.168.2.3
Mar 21, 2023 08:07:46.422673941 CET	57840	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:07:46.707103968 CET	53	57840	8.8.8.8	192.168.2.3
Mar 21, 2023 08:07:58.808130026 CET	57990	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:07:58.829898119 CET	53	57990	8.8.8.8	192.168.2.3
Mar 21, 2023 08:07:59.838872910 CET	52387	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:07:59.860487938 CET	53	52387	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:00.867115974 CET	56924	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:00.889214993 CET	53	56924	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:05.917721033 CET	60625	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:06.065783024 CET	53	60625	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:07.086607933 CET	49302	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:07.286751986 CET	53	49302	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:08.308490992 CET	53975	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:08.328178883 CET	53	53975	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:13.337563992 CET	51139	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:13.699300051 CET	53	51139	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:24.633847952 CET	52955	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:24.783422947 CET	53	52955	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:35.742198944 CET	60582	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:35.790923119 CET	53	60582	8.8.8.8	192.168.2.3
Mar 21, 2023 08:08:48.652827978 CET	57134	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:08:48.940431118 CET	53	57134	8.8.8.8	192.168.2.3
Mar 21, 2023 08:09:08.449750900 CET	62050	53	192.168.2.3	8.8.8.8
Mar 21, 2023 08:09:08.493007898 CET	53	62050	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 08:07:24.608470917 CET	192.168.2.3	8.8.8.8	0x3abb	Standard query (0)	www.yongle products.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:35.665481091 CET	192.168.2.3	8.8.8.8	0xae75	Standard query (0)	www.0dhy.xyz	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:46.422673941 CET	192.168.2.3	8.8.8.8	0x93ef	Standard query (0)	www.kunimi.org	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:58.808130026 CET	192.168.2.3	8.8.8.8	0x395a	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:59.838872910 CET	192.168.2.3	8.8.8.8	0x60d8	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:00.867115974 CET	192.168.2.3	8.8.8.8	0x1705	Standard query (0)	www.amirah.cfd	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:05.917721033 CET	192.168.2.3	8.8.8.8	0xd3d2	Standard query (0)	www.bisarr opainting.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:07.086607933 CET	192.168.2.3	8.8.8.8	0x1bc0	Standard query (0)	www.bisarr opainting.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:08.308490992 CET	192.168.2.3	8.8.8.8	0x2433	Standard query (0)	www.bisarr opainting.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 08:08:13.337563992 CET	192.168.2.3	8.8.8.8	0x26af	Standard query (0)	www.traindic.top	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:24.633847952 CET	192.168.2.3	8.8.8.8	0x2381	Standard query (0)	www.bohndigitaltech.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:35.742198944 CET	192.168.2.3	8.8.8.8	0xd55e	Standard query (0)	www.riflerroofers.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:48.652827978 CET	192.168.2.3	8.8.8.8	0x5b9e	Standard query (0)	www.denko-kosan.com	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:09:08.449750900 CET	192.168.2.3	8.8.8.8	0xb9d5	Standard query (0)	www.madliainsalu.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 21, 2023 08:06:50.276381016 CET	8.8.8.8	192.168.2.3	0x2211	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.128	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:24.629987955 CET	8.8.8.8	192.168.2.3	0x3abb	No error (0)	www.yongleproducts.com		1.13.186.125	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:35.687676907 CET	8.8.8.8	192.168.2.3	0xae75	No error (0)	www.0dhy.xyz		198.46.160.97	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:46.707103968 CET	8.8.8.8	192.168.2.3	0x93ef	No error (0)	www.kunimi.org	kunimi.org		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 08:07:46.707103968 CET	8.8.8.8	192.168.2.3	0x93ef	No error (0)	kunimi.org		219.94.129.181	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:58.829898119 CET	8.8.8.8	192.168.2.3	0x395a	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:07:59.860487938 CET	8.8.8.8	192.168.2.3	0x60d8	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:00.889214993 CET	8.8.8.8	192.168.2.3	0x1705	Name error (3)	www.amirah.cfd	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:06.065783024 CET	8.8.8.8	192.168.2.3	0xd3d2	Name error (3)	www.bisarropainting.com	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:07.286751986 CET	8.8.8.8	192.168.2.3	0x1bc0	Name error (3)	www.bisarropainting.com	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:08.328178883 CET	8.8.8.8	192.168.2.3	0x2433	Name error (3)	www.bisarropainting.com	none	none	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:13.699300051 CET	8.8.8.8	192.168.2.3	0x26af	No error (0)	www.traindic.top		162.0.231.77	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:24.783422947 CET	8.8.8.8	192.168.2.3	0x2381	No error (0)	www.bohndigitaltech.com	bohndigitaltech.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 08:08:24.783422947 CET	8.8.8.8	192.168.2.3	0x2381	No error (0)	bohndigitaltech.com		162.241.24.110	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:35.790923119 CET	8.8.8.8	192.168.2.3	0xd55e	No error (0)	www.riflerroofers.com	rifleroofers.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 08:08:35.790923119 CET	8.8.8.8	192.168.2.3	0xd55e	No error (0)	rifleroofers.com		67.222.24.48	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:08:48.940431118 CET	8.8.8.8	192.168.2.3	0x5b9e	No error (0)	www.denko-kosan.com	denko-kosan.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 21, 2023 08:08:48.940431118 CET	8.8.8.8	192.168.2.3	0x5b9e	No error (0)	denko-kosan.com		49.212.180.95	A (IP address)	IN (0x0001)	false
Mar 21, 2023 08:09:08.493007898 CET	8.8.8.8	192.168.2.3	0xb9d5	No error (0)	www.madliainsalu.com	madliainsalu.com		CNAME (Canonical name)	IN (0x0001)	false

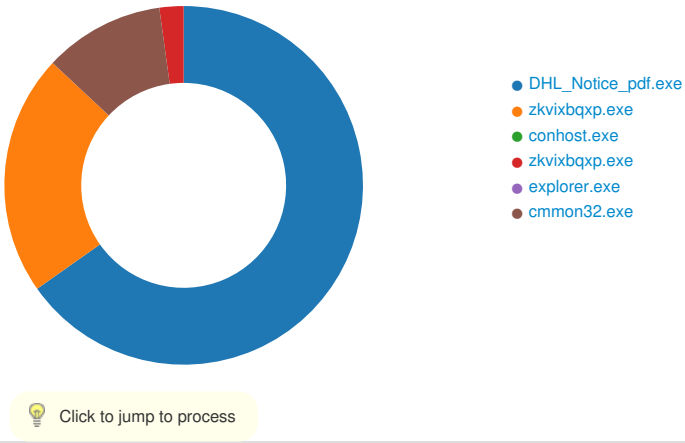
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 08:09:08.493007898 CET	8.8.8.8	192.168.2.3	0xb9d5	No error (0)	madliainsalu.com		34.120.137.41	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.yongleproducts.com
- 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_Notice_pdf.exe PID: 2080, Parent PID: 3452

General

Target ID:	0
Start time:	08:06:55
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_Notice_pdf.exe
Imagebase:	0x400000

File size:	255238 bytes
MD5 hash:	771508CF2751F6DABE05758E4FA25FDF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: zkvixbqxp.exe PID: **6136**, Parent PID: **2080**

General

Target ID:	1
Start time:	08:06:55
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe" C:\Users\user\AppData\Local\Temp\thztifyh.t
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	BE5A6985BCDCA9064A05D26CFB8D082E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 27%, ReversingLabs
Reputation:	low

File Activities

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\thztifyh.t	unknown	4096	success or wait	1	4011D6	fread
C:\Users\user\AppData\Local\Temp\thztifyh.t	unknown	4096	success or wait	1	4011D6	fread
C:\Users\user\AppData\Local\Temp\bwgyj.py	unknown	189440	success or wait	1	420A17	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	420FF4	ReadFile

Analysis Process: conhost.exe PID: **6132**, Parent PID: **6136**

General

Target ID:	2
Start time:	08:06:55
Start date:	21/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: zkvixbqxp.exe PID: **5244**, Parent PID: **6136**

General

Target ID:	3
Start time:	08:06:56
Start date:	21/03/2023
Path:	C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe
Imagebase:	0x400000
File size:	5632 bytes
MD5 hash:	BE5A6985BCDCA9064A05D26CFB8D082E
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: 00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.273874726.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.274142159.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.274142159.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.274142159.00000000008D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.273942150.0000000000560000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.273942150.0000000000560000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.273942150.0000000000560000.00000040.10000000.00040000.00000000.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: **3452**, Parent PID: **5244**

General

Target ID:	4
Start time:	08:07:00
Start date:	21/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
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	Completion	Count	Source Address	Symbol

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: **5080**, Parent PID: **3452**

General

Target ID:	5
Start time:	08:07:10
Start date:	21/03/2023
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xd0000
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: 00000005.00000002.505204819.00000000026C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.505204819.00000000026C0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505204819.00000000026C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.505473139.00000000027C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.505473139.00000000027C0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505473139.00000000027C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.504397231.0000000000240000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.504397231.0000000000240000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.504397231.0000000000240000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zkvixbqxp.exe	success or wait	1	27DC867	NtDeleteFile
C:\Users\user\AppData\Local\Temp\146E771M	object name not found	1	27DC867	NtDeleteFile
C:\Users\user\AppData\Local\Temp\146E771M	sharing violation	1	27DC867	NtDeleteFile

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\146E771M	sharing violation	1	27DC867	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	27DC837	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