ID: 635250
Sample Name: DHL_29028263 receipt document of the purchase,pdf.exe
Cookbook: default.jbs
Time: 17:49:58
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

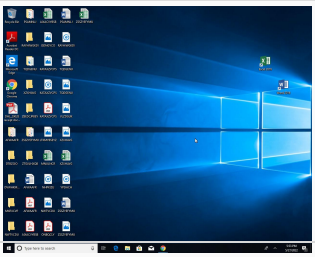
Windows Analysis Report

DHL_29028263 receipt document of the purchase,pdf.exe

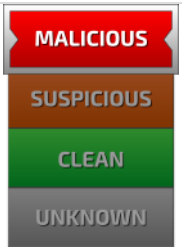
Overview

General Information

Sample Name:	DHL_29028263 receipt document of the purchase,pdf.exe
Analysis ID:	635250
MD5:	c97dfff9af3555c…
SHA1:	efc71d34d01661..
SHA256:	bd89fe68b099ed..
Tags:	DHL exe Formbook
Infos:	



Detection



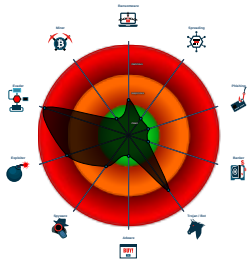
FormBook

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

Signatures

- Found malware configuration
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Icon mismatch, binary includes an i…
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- DHL_29028263 receipt document of the purchase,pdf.exe (PID: 7020 cmdline: "C:\Users\user\Desktop\DHL_29028263 receipt document of the purchase,pdf.exe" MD5: C97DFFF9AF3555CA25082CC686715C76)
  - tcmsetup.exe (PID: 7084 cmdline: C:\Windows\SysWOW64\tcmsetup.exe MD5: EBCB8BE0CD1C5FEC861B53CDE71F009D)
  - find.exe (PID: 7092 cmdline: C:\Windows\SysWOW64\find.exe MD5: 9BCB215932501B45D204DC8E592EA996)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - svchost.exe (PID: 5564 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 6868 cmdline: /c del "C:\Windows\SysWOW64\find.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bestofsouthbeach.guide/mrw6/"
  ],
  "decoy": [
    "car-kit.store",
    "localbrewsislamorada.com",
    "jaykamins.art",
    "babeswant.com",
    "tubularyhvlpu.online",
    "psychomindsofficial.com",
    "jmsls.net",
    "nxeifycssut.mobi",
    "paraquatinducedparkinsons.com",
    "trancendentalastroshop.store",
    "modaskayita.com",
    "reeventos.com",
    "loueofficial.com",
    "sentlogisticsja.com",
    "umiyan.com",
    "getvirtualaddress.com",
    "beargreasers.com",
    "kyousaku.net",
    "prospectdatasolutions.com",
    "16gjm.xyz",
    "range4tis.com",
    "doholiz.com",
    "techno-delights.com",
    "commercewholesale.com",
    "delcobilly.com",
    "artificial-pigment.wiki",
    "hashv.one",
    "weichuang-pifa.com",
    "cafehavanacigars.club",
    "misantaparticulares.online",
    "frontierwindpowerllc.com",
    "howellandassocinc.com",
    "cherylwoya.com",
    "platinumridge.art",
    "corporatesupplygroup.online",
    "blog-ikusachi-life.com",
    "946abg.net",
    "djfest.net",
    "haiye88.com",
    "koedayuuki.net",
    "jagapps.tech",
    "metanask.online",
    "southtm.com",
    "mcalpinindustries.com",
    "unifonic.agency",
    "quarhu.com",
    "jxrszp.com",
    "itasetembro-consulte.digital",
    "ff4cn15ck.xyz",
    "xd16880.com",
    "btcminers.bet",
    "laborchcg.com",
    "tanran.online",
    "shuddhiorganics.com",
    "numi.quest",
    "fortuscare.com",
    "fromleadertomastercoach.com",
    "xn--eltemplodehcate-lnb.com",
    "activeton.com",
    "morningvibecoffee.com",
    "uhk.academy",
    "finestrecitaltolearn-today.info",
    "citie-dct.com",
    "xn--xcr352cxsd.net"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x583a8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x58742:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x64455:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x63f41:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x64557:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x646cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x5915a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x631bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x59ed2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x69947:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x6a9ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x66879:$sqlite3step: 68 34 1C 7B E1 • 0x6698c:$sqlite3step: 68 34 1C 7B E1 • 0x668a8:$sqlite3text: 68 38 2A 90 C5 • 0x669cd:$sqlite3text: 68 38 2A 90 C5 • 0x668bb:$sqlite3blob: 68 53 D8 7F 8C • 0x669e3:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000000.527619880.0000000005187000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000000.527619880.0000000005187000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 41 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.find.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.find.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.find.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
2.0.find.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.0.find.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 209.99.64.43

Timestamp:	192.168.2.5209.99.64.4349816802031412 05/27/22-17:53:28.062546
SID:	2031412
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 209.99.64.43

Timestamp:	192.168.2.5209.99.64.4349816802031453 05/27/22-17:53:28.062546
SID:	2031453
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.5 - Destination IP: 209.99.64.43

Timestamp:	192.168.2.5209.99.64.4349816802031449 05/27/22-17:53:28.062546
SID:	2031449
Source Port:	49816
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Exploits

Yara detected UAC Bypass using CMSTP

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

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

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Contains functionality to hide user accounts

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

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

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

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

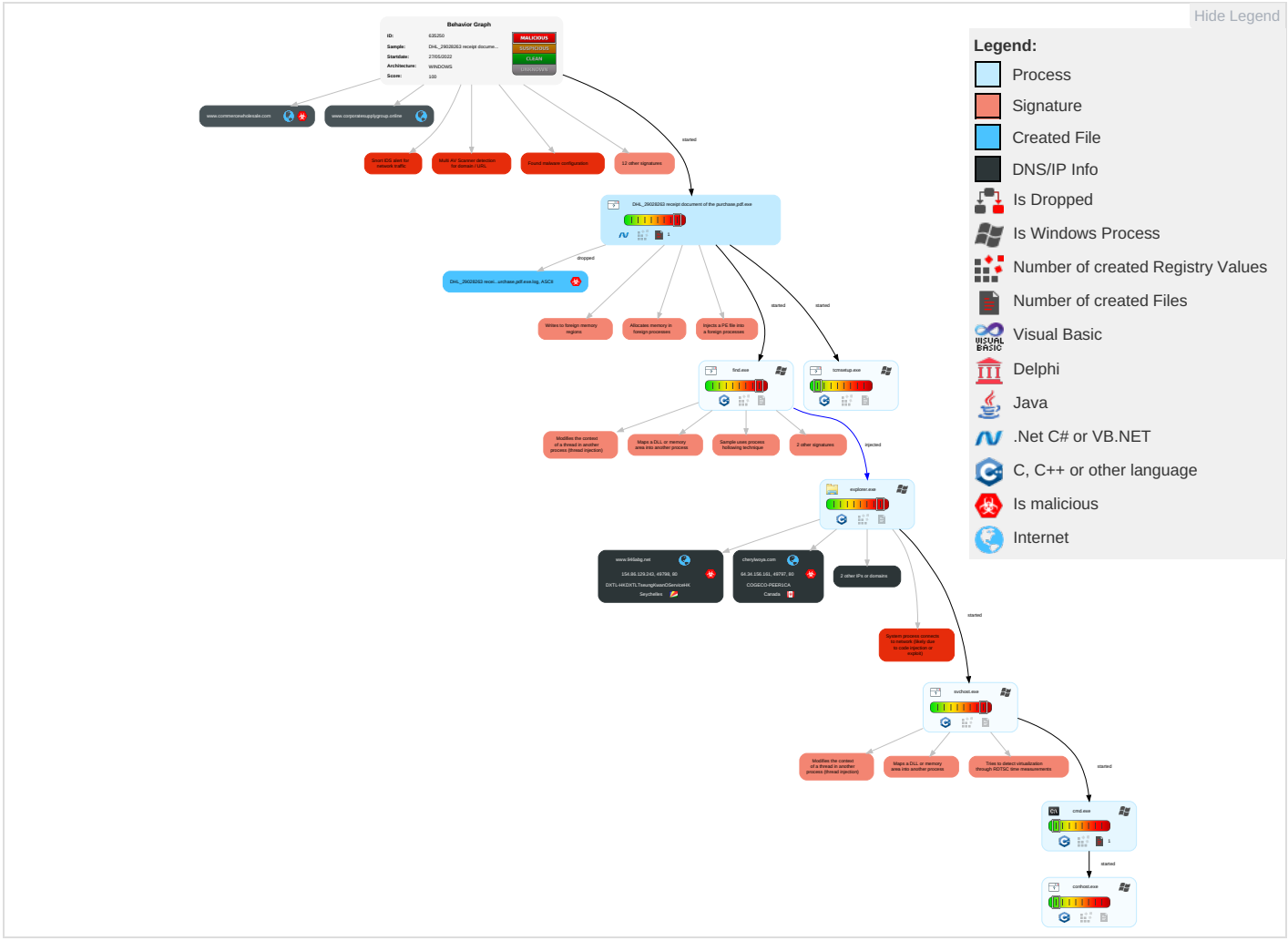
Remote Access Functionality

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 Scheduled Task/Job	1 Scheduled Task/Job	8 1 2 Process Injection	1 1 Masquerading	1 Input Capture	1 Query Registry	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 3 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 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)	8 1 2 Process Injection	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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 Hidden Users	Cached Domain Credentials	1 1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

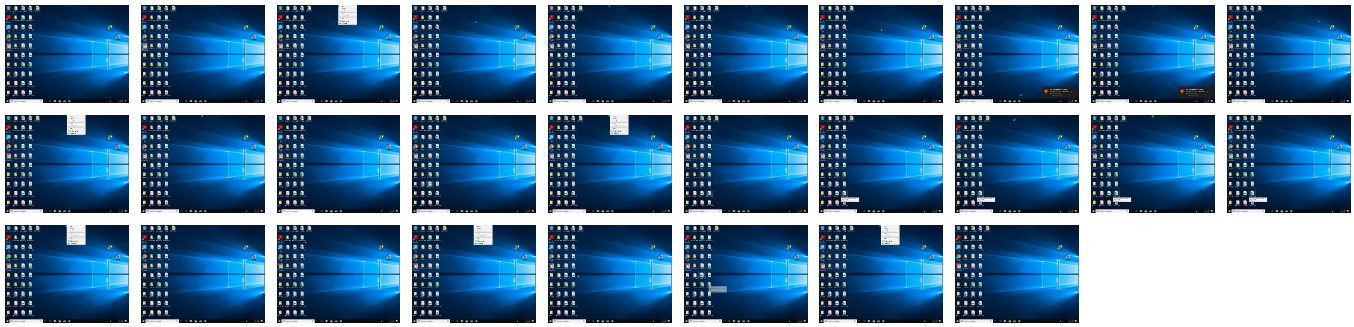
Behavior Graph



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_29028263 receipt document of the purchase,pdf.exe	22%	ReversingLabs	ByteCode-MSIL.Trojan.Tedy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.find.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
2.2.find.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
2.0.find.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
2.0.find.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
2.0.find.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

Source	Detection	Scanner	Label	Link
cherylwoya.com	10%	Virustotal		Browse
www.946abg.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.cherylwoya.com/mrw6/?5j=-Z8hhJu0CH1&kZL=6fZEMEdK0EUsHT8poDGbU1zs+0N96qjYHzalTR2tuqMjY7ixAH4WqcSwjImDfJQ+xirU	100%	Avira URL Cloud	phishing	
http://www.946abg.net/mrw6/?kZL=serf4G2fT23AQqvD11FW0e5UhnaipW+P1SIFRHWKX7vOHQGiYIAk+83ijhEv+8S8z0gu&5j=-Z8hhJu0CH1	100%	Avira URL Cloud	malware	
www.bestofsouthbeach.guide/mrw6/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.commercewholesale.com	209.99.64.43	true	true		unknown
cherylwoya.com	64.34.156.161	true	true	• 10%, Virustotal, Browse	unknown
www.946abg.net	154.86.129.243	true	true	• 1%, Virustotal, Browse	unknown
www.corporatesupplygroup.online	203.170.80.250	true	false		unknown
www.cherylwoya.com	unknown	unknown	true		unknown
www.kyousaku.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cherylwoya.com/mrw6/?5j=-Z8hhJu0CH1&kZL=6fZEMEdK0EUsHT8poDGbU1zs+0N96qjYHzalTR2tuqMjY7ixAH4WqcSwjImDfJQ+xirU	true	• Avira URL Cloud: phishing	unknown
http://www.946abg.net/mrw6/?kZL=serf4G2fT23AQqvD11FW0e5UhnaipW+P1SIFRHWKX7vOHQGiYIAk+83ijhEv+8S8z0gu&5j=-Z8hhJu0CH1	true	• Avira URL Cloud: malware	unknown
www.bestofsouthbeach.guide/mrw6/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.random.org/sequences/	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2019-08-01/managementGroupDeploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2019-08-01/tenantDeploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2014-04-01-preview/deploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://json-schema.org/draft-04/schema#Lhttp://json-schema.org/draft-04/schema	DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://json-schema.org/draft-04/schema	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://aka.ms/arm-tools-apiversion.	DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json	DHL_29028263 receipt document of the purchase,pdf.exe, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high
http://https://schema.management.azure.com/schemas/2019-08-01/tenantDeploymentTemplate.json.2014	DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000000.435567902.00000000010E2000.00000020.00000001.01000000.00000003.sdmp, DHL_29028263 receipt document of the purchase,pdf.exe, 00000000.00000002.479557672.00000000010E2000.00000020.00000001.01000000.00000003.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.34.156.161	cherylwoya.com	Canada		13768	COGECO-PEER1CA	true
154.86.129.243	www.946abg.net	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635250
Start date and time: 27/05/202217:49:58	2022-05-27 17:49:58 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_29028263 receipt document of the purchase,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
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
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@9/1@5/2
EGA Information:	• Successful, ratio: 66.7%

HDC Information:	• Successful, ratio: 64.4% (good quality ratio 58.7%) • Quality average: 71.5% • Quality standard deviation: 31.7%
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 • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target DHL_29028263 receipt document of the purchase,pdf.exe, PID 7020 because it is empty
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_29028263 receipt document of the purchase,pdf.exe.log

Process:	C:\Users\user\Desktop\DHL_29028263 receipt document of the purchase,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	522
Entropy (8bit):	5.348034597186669
Encrypted:	false
SSDEEP:	12:Q3La/hz92n4M9tDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9l0ZKhav:MLU84qpE4Ks2wKDE4KhK3VZ9pKhk

MD5:	D4AF6B20AEA9906B4FF574A174E96287
SHA1:	81655019BB100FAADD5B36755F798EE5FB09E672
SHA-256:	DD8AE93DA079839B31327D22A2408E0C3EA4DDE92FD389CD5B96AD57CCE7B2E1
SHA-512:	6D912AC17876D9C21E61ED8C1B435AEA0FBB27FB97626A40903B4DFFC1204BEF3A43B02805DEDD2531822FD6F62CF06F0D758C1B2CA07258E82F95225D71C1E
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.208402474565558
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL_29028263 receipt document of the purchase,pdf.exe
File size:	2419712
MD5:	c97dfff9af3555ca25082cc686715c76
SHA1:	efc71d34d01661436ef23e2af1a36f7f96319122
SHA256:	bd89fe68b099ed00bea985dbdf7c8c0d87deb5a85c29d7a27f09764ab5b9d04d
SHA512:	7a10d62a1f0ba0ada604822ac15d2172af65b521d9fbe14bc559eb1f9a01547034981a837fe8e9e0f3d835f5e2519ee498cb7838fe73e32c3cbbf1e86db6d301
SSDEEP:	24576:Wmnp0sdiKbb62RNH6AyM1l/+rRa53ruU:IKbb62RNaKsF6
TLSH:	B5B5B337DF344E2592F9A719A9644912FE30A78F4A41870FBA7D060C1F3B77A114B72A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0...$..B.....$.. ....$...@.. .....@%.....`.....

File Icon

Icon Hash:	c49a0894909c6494

Static PE Info

General

Entrypoint:	0x64c703
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xD7CA2EE6 [Thu Sep 21 05:15:18 2084 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x24c5fc	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24e000	0x3fe8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x252000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x24c646	0x38	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x24a709	0x24a800	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x24e000	0x3fe8	0x4000	False	0.453125	data	5.64147469867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x252000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x24e148	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x24e5b0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 1134929317, next used block 44344484		
RT_ICON	0x24f658	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x251c00	0x30	data		
RT_VERSION	0x251c30	0x3b6	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

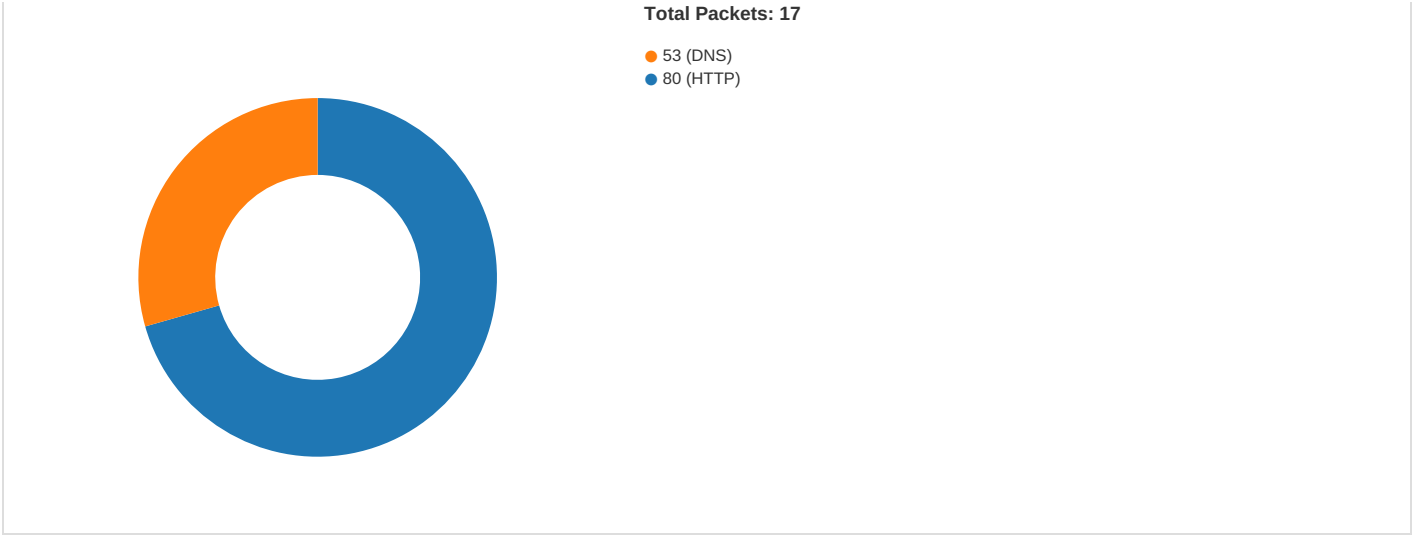
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	? Microsoft Corporation. All rights reserved.
Assembly Version	16.0.0.0
InternalName	Microsoft.WebTools.Languages.Json.dll
FileVersion	16.6.936.3669
CompanyName	Microsoft Corporation
LegalTrademarks	
ProductVersion	16.6.936-preview3+550e59c1ad
FileDescription	
OriginalFilename	Microsoft.WebTools.Languages.Json.dll

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5209.99.64.434 9816802031412 05/27/22-17:53:28.062546	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.5	209.99.64.43
192.168.2.5209.99.64.434 9816802031453 05/27/22-17:53:28.062546	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.5	209.99.64.43
192.168.2.5209.99.64.434 9816802031449 05/27/22-17:53:28.062546	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.5	209.99.64.43

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:53:01.227459908 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.337821007 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.337915897 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.338088036 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.448623896 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.452982903 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453003883 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453022003 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453039885 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453057051 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453073978 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453090906 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453109026 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453125000 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.453128099 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453186035 CEST	80	49797	64.34.156.161	192.168.2.5
May 27, 2022 17:53:01.453228951 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.453255892 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:01.453469992 CEST	49797	80	192.168.2.5	64.34.156.161
May 27, 2022 17:53:06.815435886 CEST	49798	80	192.168.2.5	154.86.129.243
May 27, 2022 17:53:07.025321960 CEST	80	49798	154.86.129.243	192.168.2.5
May 27, 2022 17:53:07.025649071 CEST	49798	80	192.168.2.5	154.86.129.243
May 27, 2022 17:53:07.025675058 CEST	49798	80	192.168.2.5	154.86.129.243
May 27, 2022 17:53:07.227186918 CEST	80	49798	154.86.129.243	192.168.2.5
May 27, 2022 17:53:07.227204084 CEST	80	49798	154.86.129.243	192.168.2.5
May 27, 2022 17:53:07.227215052 CEST	80	49798	154.86.129.243	192.168.2.5
May 27, 2022 17:53:07.227734089 CEST	49798	80	192.168.2.5	154.86.129.243
May 27, 2022 17:53:07.227752924 CEST	49798	80	192.168.2.5	154.86.129.243
May 27, 2022 17:53:07.429177999 CEST	80	49798	154.86.129.243	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:53:01.072865009 CEST	63538	53	192.168.2.5	8.8.8.8
May 27, 2022 17:53:01.219815016 CEST	53	63538	8.8.8.8	192.168.2.5
May 27, 2022 17:53:06.473618031 CEST	61478	53	192.168.2.5	8.8.8.8
May 27, 2022 17:53:06.814008951 CEST	53	61478	8.8.8.8	192.168.2.5
May 27, 2022 17:53:12.240880966 CEST	55355	53	192.168.2.5	8.8.8.8
May 27, 2022 17:53:12.280710936 CEST	53	55355	8.8.8.8	192.168.2.5
May 27, 2022 17:53:22.301239967 CEST	54463	53	192.168.2.5	8.8.8.8
May 27, 2022 17:53:22.336560011 CEST	53	54463	8.8.8.8	192.168.2.5
May 27, 2022 17:53:27.801031113 CEST	50393	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:53:27.909094095 CEST	53	50393	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 17:53:01.072865009 CEST	192.168.2.5	8.8.8.8	0x1bd5	Standard query (0)	www.cherylwoya.com	A (IP address)	IN (0x0001)
May 27, 2022 17:53:06.473618031 CEST	192.168.2.5	8.8.8.8	0x4e8e	Standard query (0)	www.946abg.net	A (IP address)	IN (0x0001)
May 27, 2022 17:53:12.240880966 CEST	192.168.2.5	8.8.8.8	0x813c	Standard query (0)	www.kyousaku.net	A (IP address)	IN (0x0001)
May 27, 2022 17:53:22.301239967 CEST	192.168.2.5	8.8.8.8	0xd0	Standard query (0)	www.corporatesupplygroup.online	A (IP address)	IN (0x0001)
May 27, 2022 17:53:27.801031113 CEST	192.168.2.5	8.8.8.8	0xc623	Standard query (0)	www.commercewholesale.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 17:53:01.219815016 CEST	8.8.8.8	192.168.2.5	0x1bd5	No error (0)	www.cherylwoya.com	cherylwoya.com		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 17:53:01.219815016 CEST	8.8.8.8	192.168.2.5	0x1bd5	No error (0)	cherylwoya.com		64.34.156.161	A (IP address)	IN (0x0001)
May 27, 2022 17:53:06.814008951 CEST	8.8.8.8	192.168.2.5	0x4e8e	No error (0)	www.946abg.net		154.86.129.243	A (IP address)	IN (0x0001)
May 27, 2022 17:53:12.280710936 CEST	8.8.8.8	192.168.2.5	0x813c	Name error (3)	www.kyousaku.net	none	none	A (IP address)	IN (0x0001)
May 27, 2022 17:53:22.336560011 CEST	8.8.8.8	192.168.2.5	0xd0	No error (0)	www.corporatesupplygroup.online		203.170.80.250	A (IP address)	IN (0x0001)
May 27, 2022 17:53:27.909094095 CEST	8.8.8.8	192.168.2.5	0xc623	No error (0)	www.commercewholesale.com		209.99.64.43	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cherylwoya.com
- www.946abg.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49797	64.34.156.161	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:53:01.338088036 CEST	9264	OUT	GET /mrw6/?5j=-Z8hhJu0CH1&kZL=6fZEMEdK0EUsHT8poDGbU1zs+0N96qjYHzalTR2tuqMjY7ixAH4WqcSwjImDfJQ+xirU HTTP/1.1 Host: www.cherylwoya.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

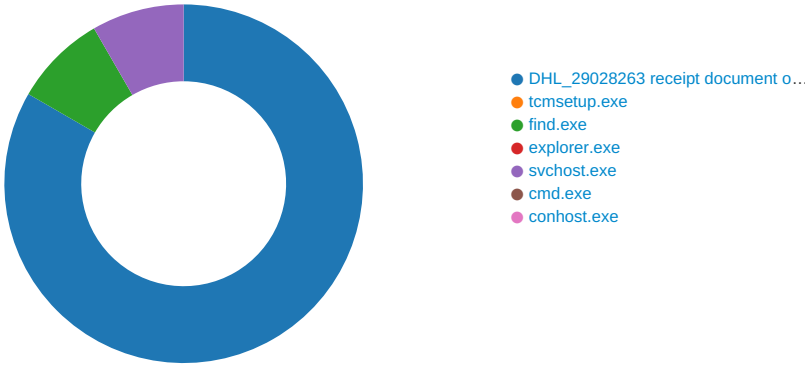
Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:53:01.452982903 CEST	9265	IN	HTTP/1.1 404 Not Found Date: Fri, 27 May 2022 15:53:01 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Cache-Control: no-cache, no-store, must-revalidate Pragma: no-cache Expires: 0 Transfer-Encoding: chunked Content-Type: text/html Data Raw: 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 0d 0a 0a 0d 0a 31 35 37 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 6 3 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 0d 0a 33 0d 0a 34 30 34 0d 0a 31 0d 0a 20 0d 0a 39 0d 0a 4e 6f 74 20 46 6f 75 6e 64 0d 0a 31 66 63 61 0d 0a 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 2c 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 72 65 73 70 6f 6e 73 65 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 43 43 43 43 43 43 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 2e 73 74 61 74 75 73 2d 63 6f 64 65 20 7b 0a 20 20 20 Data Ascii: 111157<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; chars et=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0"> <tit le>34041 9Not Found1fca</title> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; pa dding: 0; margin: 0; } section, footer { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .response-info { color: #CCCCCC; } .status-code {

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49798	154.86.129.243	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:53:07.025675058 CEST	9276	OUT	GET /mrw6/?kZL=serf4G2fT23AQqvD11FW0e5UhnaipW+P1SIFRHWKX7vOHQGiYIAk+83ijhEv+8S8z0gu&5j=-Z8 hhJu0CH1 HTTP/1.1 Host: www.946abg.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:53:07.227204084 CEST	9276	IN	HTTP/1.1 404 Not Found Server: nginx Date: Fri, 27 May 2022 15:53:07 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr><c enter>nginx </body></html>

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: DHL_29028263 receipt document of the purchase,pdf.exe PID: **7020**, Parent PID: **5576**

General

Target ID:	0
Start time:	17:51:13
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL_29028263 receipt document of the purchase,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL_29028263 receipt document of the purchase,pdf.exe"
Imagebase:	0x10e0000
File size:	2419712 bytes
MD5 hash:	C97DFFF9AF3555CA25082CC686715C76
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.490164346.00000000048A4000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.487275778.0000000004472000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.487275778.0000000004472000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.487275778.0000000004472000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.487559942.00000000044F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.487559942.00000000044F0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.487559942.00000000044F0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.486933021.0000000004396000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000000.00000002.486933021.0000000004396000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: tcmsetup.exe PID: **7084**, Parent PID: **7020**

General	
Target ID:	1
Start time:	17:51:28
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\tcmsetup.exe
Imagebase:	0x9e0000
File size:	14848 bytes
MD5 hash:	EBCB8BE0CD1C5FEC861B53CDE71F009D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: find.exe PID: **7092**, Parent PID: **7020**

General	
Target ID:	2
Start time:	17:51:29
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\find.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\find.exe
Imagebase:	0x1030000
File size:	14848 bytes
MD5 hash:	9BCB215932501B45D204DC8E592EA996
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.471183159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.471183159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.471183159.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.571277848.0000000000D40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.571277848.0000000000D40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.571277848.0000000000D40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.470820106.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.470820106.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.470820106.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.570977775.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.570977775.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.570977775.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.470421147.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.470421147.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.470421147.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.570002580.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.570002580.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.570002580.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **7092**

General

Target ID:	4
Start time:	17:51:33
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.527619880.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.527619880.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.527619880.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.508992436.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.508992436.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.508992436.0000000005187000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5564, Parent PID: 684

General

Target ID:	14
Start time:	17:52:10
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x8a0000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.705413123.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.705413123.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.705413123.0000000003210000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.704496254.00000000029D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.704496254.00000000029D0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.704496254.00000000029D0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.705527409.0000000003240000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.705527409.0000000003240000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.705527409.0000000003240000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	29E86E7	NtReadFile

Analysis Process: cmd.exe PID: 6868, Parent PID: 5564

General

Target ID:	16

Start time:	17:52:19
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\SysWOW64\find.exe"
Imagebase:	0x1100000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3856**, Parent PID: **6868**

General

Target ID:	17
Start time:	17:52:20
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly