ID: 680337
Sample Name: Technical Specifications & Drawings.exe
Cookbook: default.jbs
Time: 12:26:09
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

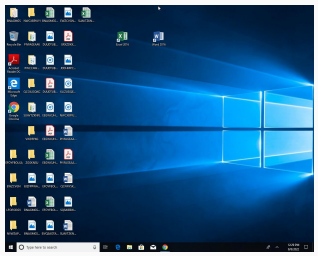
Windows Analysis Report

Technical Specifications & Drawings.exe

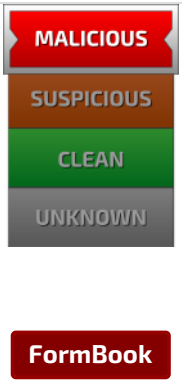
Overview

General Information

Sample Name:	Technical Specifications & Drawings.exe
Analysis ID:	680337
MD5:	9b94f751e8cc14…
SHA1:	f12af989efe2b3b..
SHA256:	893a0b655917a1..
Tags:	exe Formbook
Infos:	



Detection



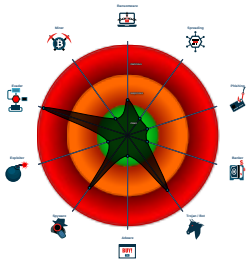
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- 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…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Technical Specifications & Drawings.exe (PID: 6080 cmdline: "C:\Users\user\Desktop\Technical Specifications & Drawings.exe" MD5: 9B94F751E8CC145058DB9F428C2AD571)
  - Technical Specifications & Drawings.exe (PID: 5084 cmdline: C:\Users\user\Desktop\Technical Specifications & Drawings.exe MD5: 9B94F751E8CC145058DB9F428C2AD571)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 1896 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.tomoptique.fr/02pi/"
  ],
  "decoy": [
    "M3tfGJmJRxnXx2v38A==",
    "m4b8szAh7fn1GFTQt32C+uKxPpY=",
    "aq5+I6igUigQzHUz",
    "4lHg1pN4fbZQ8Hg5",
    "pZgq+XdYRJZGtZpXb/gobxk=",
    "ngmngHIN+PJf3danjt0=",
    "aWHnw0nyXCgQzHUz",
    "Qa+KQe7PL5g83V8q",
    "lX0/3lMZHyGWQPyVm46Q9eKxPpY=",
    "syPESuXcWyQQzHUz",
    "ULeDOo1rfqvVcCs=",
    "COFEArOnRS4JMdemgP8DLQqSNA==",
    "OqdvdWhJyOqVPg==",
    "ANt3czoMin1DUZcstDUe",
    "rKFuM+S9pv/riVlgxBgU",
    "xzso5SN63kL1Ltanjt0=",
    "hu2RdTMU7NZL0ZeqvEGH7OKxPpY=",
    "phmUZhkO/d6ZTx6mWMQ=",
    "Wj2oYxTKjw68jMwazrQW",
    "lv2aiTsU6N7OqJUTBj2Y+uKxPpY=",
    "5L0q4IlGEpRTlSYstDUe",
    "FvK8ah8qZ6vVcCs=",
    "abtoVRsE4tE6sNIRwiGUA+KxPpY=",
    "y8Gdr3IxeuRASI4Jy+8KaA==",
    "N7Em3E0iRrJy3danjt0=",
    "OBWvoWlwJbCSGdanjt0=",
    "kHkzKtyb51bk65cS+g==",
    "BVkF/LV3JBY+srgvS9U=",
    "fd2hjkcgFnNDp9ilV9U=",
    "edamUMWCAMievvdJA4WztmMX",
    "h/qtrJyTWSJL/PxJHllzWAg=",
    "kWe7Ro0IyOqVPg==",
    "QrAe3YpmUGlDSXfy/wMvSTmfNg==",
    "ZWHgx4I+k/iuEUaNFmBIl0c0Hiy9",
    "iPlzLaJyecBx3tanjt0=",
    "Fo9S+XIwpyB1byMstDUe",
    "SkLiwnZYrCYQrGBeaKYibhE=",
    "XcysZNaTMwWxq2OmTRULYA==",
    "aNu4UwbkA17EoBLXgP02mT00Hiy9",
    "Mo8yuSKja+g9",
    "607Ad/rXD5aMLt2xfIZ2e1NnoZ4=",
    "pXk25GIbEhR4+i13QkI+STmfNg==",
    "uysGFdukYWM8/QtMBEyc/uKxPpY=",
    "fmH+9tKRYRD/oVthN3aztmMX",
    "TbWDRDb0g9Ciq2OmTRULYA==",
    "tqF7KKme4y7gKNanjt0=",
    "6+CEgnJVgQLuirED1LIRexM=",
    "YFTOiPnMSI9rJw==",
    "k/yeppGCO9fBv/c8",
    "Kqk+FsSThJHxaSMiNY+ztmMX",
    "HezQg/rXDY51FtXgrAd8lkv0sCmtHTtGnw==",
    "GWjsvjb3CHtxvjlKOYiztmMX",
    "QCnkguifwkk/mCkstDUe",
    "zTm3ZwwBFoJjoigstDUe",
    "4VQ4+q5U0aUIx2v38A==",
    "7c038ndW7jMCtjw=",
    "8d6NjFQhZqvVcCs=",
    "xqJFQfyja+g9",
    "iHDxwkgzyOqVPg==",
    "OSu/mIgimCB8X9MWJixbvWOuqdoDwaU=",
    "Sq1WTzwwyOqVPg==",
    "huZUE5ZZNtqY/wlhy+8KaA==",
    "g27epFQnkhaSqe1sRB2ztmMX",
    "b9WRoY5wEffprIkPy+8KaA=="
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x65b1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1dbe0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa53f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16de7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16be5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16691:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16ce7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16e5f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa10a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x158ac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xae52:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c837:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d94a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x19289:$sqlite3step: 68 34 1C 7B E1 • 0x193bc:$sqlite3step: 68 34 1C 7B E1 • 0x192cb:$sqlite3text: 68 38 2A 90 C5 • 0x19413:$sqlite3text: 68 38 2A 90 C5 • 0x192e2:$sqlite3blob: 68 53 D8 7F 8C • 0x19435:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.314845901.000000000B546000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 29 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.Technical Specifications & Drawings.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.Technical Specifications & Drawings.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x57b1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cde0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x973f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x15fe7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
4.0.Technical Specifications & Drawings.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x15de5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15891:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15ee7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1605f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x930a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14aac:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa052:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ba37:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1cb4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.Technical Specifications & Drawings.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18489:$sqlite3step: 68 34 1C 7B E1 • 0x185bc:$sqlite3step: 68 34 1C 7B E1 • 0x184cb:$sqlite3text: 68 38 2A 90 C5 • 0x18613:$sqlite3text: 68 38 2A 90 C5 • 0x184e2:$sqlite3blob: 68 53 D8 7F 8C • 0x18635:$sqlite3blob: 68 53 D8 7F 8C
0.2.Technical Specifications & Drawings.exe.39fd758.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.23.226.119	
Timestamp:	192.168.2.367.23.226.11949803802031412 08/08/22-12:28:44.161490
SID:	2031412
Source Port:	49803
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.23.226.119	
Timestamp:	192.168.2.367.23.226.11949803802031453 08/08/22-12:28:44.161490
SID:	2031453
Source Port:	49803
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.223.117.72	
Timestamp:	192.168.2.367.223.117.7249809802031449 08/08/22-12:28:49.631208
SID:	2031449
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.223.117.72	
Timestamp:	192.168.2.367.223.117.7249809802031412 08/08/22-12:28:49.631208
SID:	2031412
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.223.117.72	
Timestamp:	192.168.2.367.223.117.7249809802031453 08/08/22-12:28:49.631208
SID:	2031453
Source Port:	49809
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.3 - Destination IP: 67.23.226.119	
Timestamp:	192.168.2.367.23.226.11949803802031449 08/08/22-12:28:44.161490
SID:	2031449
Source Port:	49803
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Machine Learning detection for sample

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)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

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

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

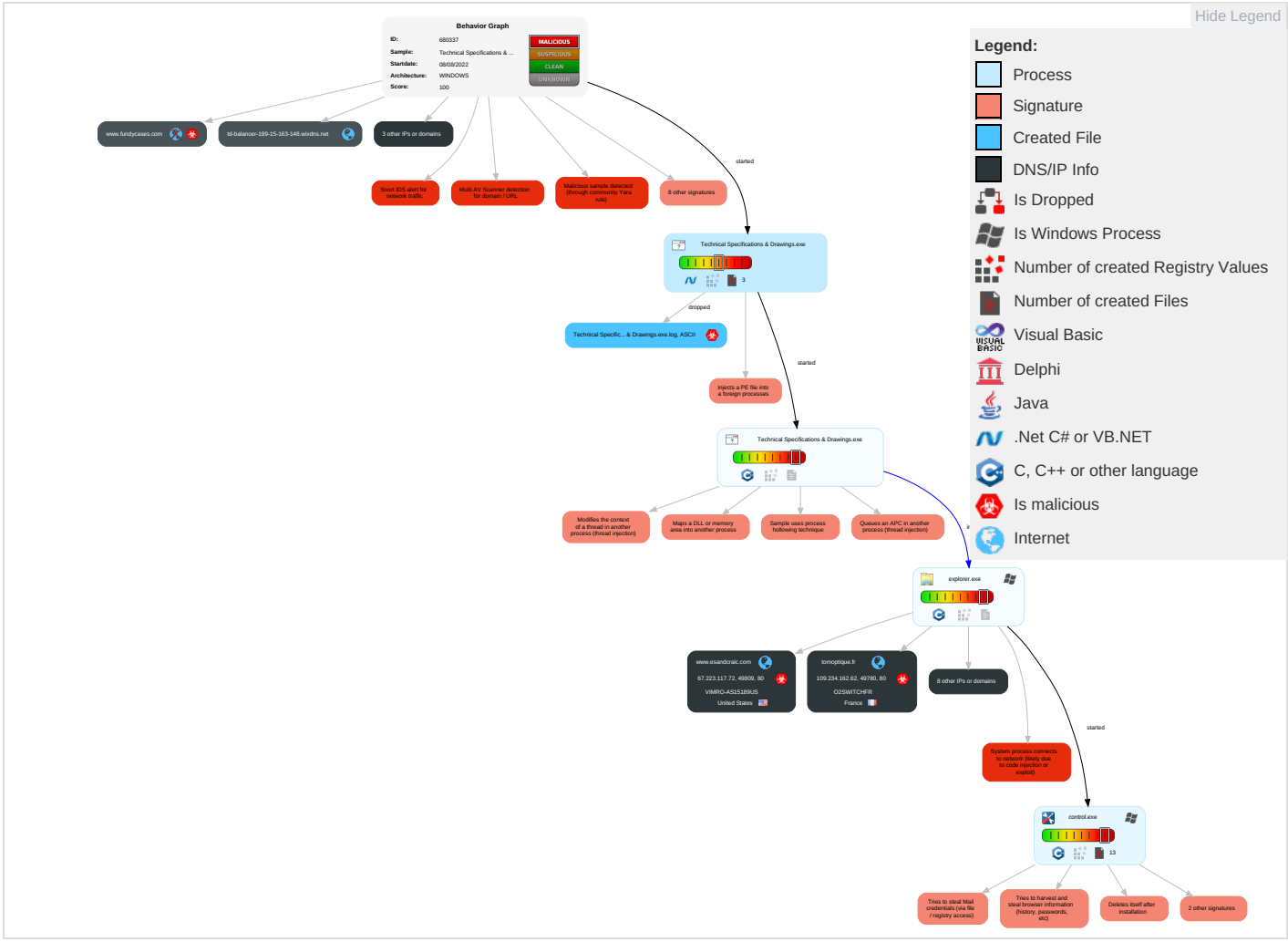
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 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	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	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)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information 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	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	1 3 Software Packing	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 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Technical Specifications & Drawings.exe	32%	Virustotal		Browse
Technical Specifications & Drawings.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	
Technical Specifications & Drawings.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.Technical Specifications & Drawings.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
boshi-eg.online	12%	Virustotal		Browse
mexc-event-partner.site	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.kirchhoff-darryl.com/02pi/?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91+KgqpPGSJqKC7J3zS0r1gze3M+2qFZl2NsX2aSbasAE+ZE0SL8u6zgnew==&wRtdp=ETVPg0_	100%	Avira URL Cloud	malware	
http://www.tomoptique.fr/02pi/?ZL0=thvfohwi7xD8LUPTC+PvURbDlMdrWv6G+kdQz5W5EjaeNcjaAM/7YzWabXa+Emqnmxa+j2rvyn8aQKdomTvD7NHn7LH6m5q/aw==&wRtdp=ETVPg0_	100%	Avira URL Cloud	malware	
http://www.mexc-event-partner.site/02pi/?ZL0=OtaEbXX4ObCoLhtF/lWLZX2dLDLBfFgcjwhWC5AcKk5LEysMwPLPLl+t4RfX0ATi8hGNnWUlfKNR4DoGgewcnJOxYMoo89i/Ow==&wRtdp=ETVPg0_	100%	Avira URL Cloud	malware	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.esandcraic.com/02pi/?ZL0=H3j/zDn1cik0H8aEc4JTyOZmy0u09IlpCgxUGgbrjIcqKZuTm1TQkyEN0mTnJzpMGdd8V9PF4iBs4MdYqflf8PDJEP40yO/f8Q==&wRtdp=ETVPg0_	100%	Avira URL Cloud	malware	
http://www.kirchhoff-darryl.com/02pi?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91	100%	Avira URL Cloud	malware	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.mexc-event-partner.site/02pi/	100%	Avira URL Cloud	malware	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.tomoptique.fr/02pi/	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boshi-eg.online	67.23.226.119	true	true	• 12%, Virustotal, Browse	unknown
tomoptique.fr	109.234.162.62	true	true		unknown
mexc-event-partner.site	184.168.107.80	true	true	• 6%, Virustotal, Browse	unknown
www.kirchhoff-darryl.com	107.155.208.43	true	true		unknown
www.esandcraic.com	67.223.117.72	true	true		unknown
td-balancer-199-15-163-148.wixdns.net	199.15.163.148	true	false		unknown
www.mexc-event-partner.site	unknown	unknown	true		unknown
www.fundycases.com	unknown	unknown	true		unknown
www.gzkanglongkeji.com	unknown	unknown	true		unknown
www.boshi-eg.online	unknown	unknown	true		unknown
www.tomoptique.fr	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.kirchhoff-darryl.com/02pi/?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91+KgqpPGSJqKC7J3zS0r1gze3M+2qFZl2NsX2aSbasAE+ZE0SL8u6zgnew==&wRtdp=ETVPg0_	true	• Avira URL Cloud: malware	unknown
http://www.tomoptique.fr/02pi/?ZL0=thvfohwi7xD8LUPTC+PvURbDlMdrWv6G+kdQz5W5EjaeNcjaAM/7YzWabXa+Emqnmxa+j2rvyn8aQKdomTvD7NHn7LH6m5q/aw==&wRtdp=ETVPg0_	true	• Avira URL Cloud: malware	unknown

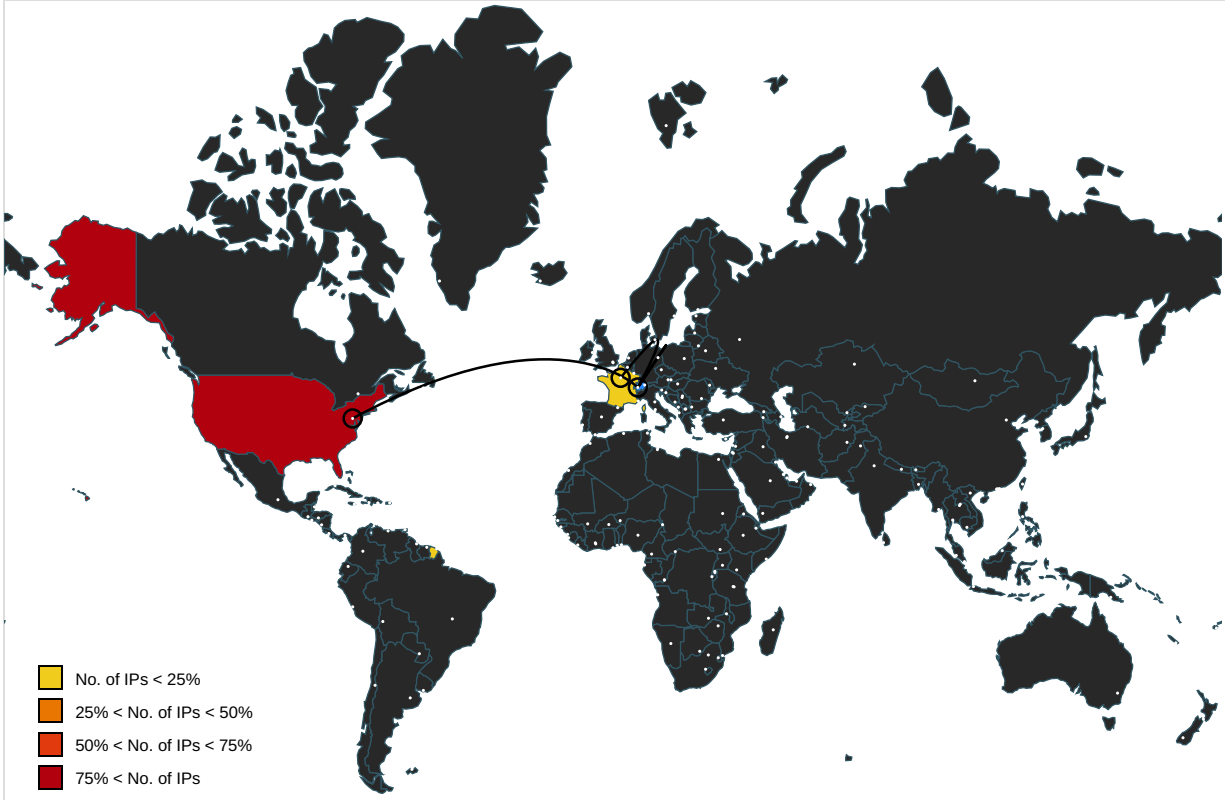
Name	Malicious	Antivirus Detection	Reputation
http://www.mexc-event-partner.site/02pi/?ZL0=OtaEbXX4ObCoLhtF/lWLZX2dLDLBfFgcjwhWC5AcKk5LEysMwPLPLl+t4RfX0ATi8hGNnWUlfKNR4DoGgewcnJOxYMoo89i/Ow==&wRtdp=ETVPg0_	true	• Avira URL Cloud: malware	unknown
http://www.esandcraic.com/02pi/?ZL0=H3j/zDn1cik0H8aEc4JTyOZmy0u09IlpCgxUGgbrjIcqKZuTm1TQkyEN0mTnJzpMGdd8V9PF4iBs4MdYqflf8PDJEP40yO/f8Q==&wRtdp=ETVPg0_	true	• Avira URL Cloud: malware	unknown
http://www.mexc-event-partner.site/02pi/	true	• Avira URL Cloud: malware	unknown
www.tomoptique.fr/02pi/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.kirchhoff-darryl.com/02pi?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91	control.exe, 00000013.00000002.518695747.0000000004AB2000.00000004.10000000.00040000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.goodfont.co.kr	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Technical Specifications & Drawings.exe, 00000000.00000002.271439563.00000000068F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.234.162.62	tomoptique.fr	France		50474	O2SWITCHFR	true
107.155.208.43	www.kirchhoff-darryl.com	United States		4686	BEKKOAMEBEKKOAMEINTERNETINCJP	true
67.223.117.72	www.esandcraic.com	United States		15189	VIMRO-AS15189US	true
184.168.107.80	mexc-event-partner.site	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
67.23.226.119	boshi-eg.online	United States		33182	DIMENOCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680337
Start date and time: 08/08/202212:26:09	2022-08-08 12:26:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Technical Specifications & Drawings.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:	29
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.spyw.evad.winEXE@4/2@14/6
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.3% (good quality ratio 81.7%) • Quality average: 72% • Quality standard deviation: 33.1%
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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 NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:27:15	API Interceptor	1x Sleep call for process: Technical Specifications & Drawings.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Technical Specifications & Drawings.exe.log

Process:	C:\Users\user\Desktop\Technical Specifications & Drawings.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\207G7-97P

Process:	C:\Windows\SysWOW64\control.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.774223579181345
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:	Technical Specifications & Drawings.exe
File size:	800256
MD5:	9b94f751e8cc145058db9f428c2ad571
SHA1:	f12af989efe2b3b11e4784899ca4c6794da17879
SHA256:	893a0b655917a18e5886348b39f6023fa851cf3d89e5b8709219ad3d2766fa97
SHA512:	02660cedcbf7d4a6d075eaa8bbd79bd560fc88ae1bbe5032348240f499432294f9c889b55f96e5f2e4214b7fe838df647a0cf4afefe2778b831af0d7dfd4e3dd
SSDEEP:	24576:hFxgV10E4B8aMrhPemfzId4MaZAOzje9IbUDHDl:tgVWES8z04eOzj7U
TLSH:	1805BE0BAF147708C5A76AB5EE0BBD76A7F61C5D3135D0B83A617C0A4AFF301E51242A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...@..b.....0.....L... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c4cea
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0AC40 [Mon Aug 8 06:25:04 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xc4c98	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc6000	0x390	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	0xc	.reloc
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	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	0xc2cf0	0xc2e00	False	0.8121780287844772	data	7.780783068719605	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc6000	0x390	0x400	False	0.369140625	data	2.8640931166907952	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc6058	0x334	data		

Imports

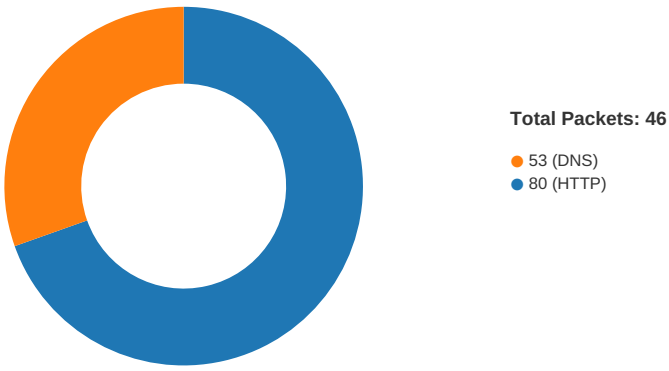
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.367.23.226.119 49803802031412 08/08/22-12:28:44.161490	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49803	80	192.168.2.3	67.23.226.119
192.168.2.367.23.226.119 49803802031453 08/08/22-12:28:44.161490	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49803	80	192.168.2.3	67.23.226.119
192.168.2.367.223.117.72 49809802031449 08/08/22-12:28:49.631208	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.3	67.223.117.72
192.168.2.367.223.117.72 49809802031412 08/08/22-12:28:49.631208	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.3	67.223.117.72
192.168.2.367.223.117.72 49809802031453 08/08/22-12:28:49.631208	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.3	67.223.117.72
192.168.2.367.23.226.119 49803802031449 08/08/22-12:28:44.161490	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49803	80	192.168.2.3	67.23.226.119

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:28:32.463253975 CEST	49776	80	192.168.2.3	107.155.208.43
Aug 8, 2022 12:28:32.755367041 CEST	80	49776	107.155.208.43	192.168.2.3
Aug 8, 2022 12:28:32.755527020 CEST	49776	80	192.168.2.3	107.155.208.43
Aug 8, 2022 12:28:32.786432028 CEST	49776	80	192.168.2.3	107.155.208.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:28:33.078504086 CEST	80	49776	107.155.208.43	192.168.2.3
Aug 8, 2022 12:28:33.078955889 CEST	80	49776	107.155.208.43	192.168.2.3
Aug 8, 2022 12:28:33.078989983 CEST	80	49776	107.155.208.43	192.168.2.3
Aug 8, 2022 12:28:33.079127073 CEST	49776	80	192.168.2.3	107.155.208.43
Aug 8, 2022 12:28:33.302218914 CEST	49776	80	192.168.2.3	107.155.208.43
Aug 8, 2022 12:28:33.595402002 CEST	80	49776	107.155.208.43	192.168.2.3
Aug 8, 2022 12:28:38.335200071 CEST	49780	80	192.168.2.3	109.234.162.62
Aug 8, 2022 12:28:38.365019083 CEST	80	49780	109.234.162.62	192.168.2.3
Aug 8, 2022 12:28:38.365221024 CEST	49780	80	192.168.2.3	109.234.162.62
Aug 8, 2022 12:28:38.365463018 CEST	49780	80	192.168.2.3	109.234.162.62
Aug 8, 2022 12:28:38.395041943 CEST	80	49780	109.234.162.62	192.168.2.3
Aug 8, 2022 12:28:38.864422083 CEST	80	49780	109.234.162.62	192.168.2.3
Aug 8, 2022 12:28:38.864464045 CEST	80	49780	109.234.162.62	192.168.2.3
Aug 8, 2022 12:28:38.864614010 CEST	49780	80	192.168.2.3	109.234.162.62
Aug 8, 2022 12:28:38.864650965 CEST	49780	80	192.168.2.3	109.234.162.62
Aug 8, 2022 12:28:38.894378901 CEST	80	49780	109.234.162.62	192.168.2.3
Aug 8, 2022 12:28:44.019023895 CEST	49803	80	192.168.2.3	67.23.226.119
Aug 8, 2022 12:28:44.154835939 CEST	80	49803	67.23.226.119	192.168.2.3
Aug 8, 2022 12:28:44.157953978 CEST	49803	80	192.168.2.3	67.23.226.119
Aug 8, 2022 12:28:44.161489964 CEST	49803	80	192.168.2.3	67.23.226.119
Aug 8, 2022 12:28:44.297408104 CEST	80	49803	67.23.226.119	192.168.2.3
Aug 8, 2022 12:28:44.300245047 CEST	80	49803	67.23.226.119	192.168.2.3
Aug 8, 2022 12:28:44.300311089 CEST	80	49803	67.23.226.119	192.168.2.3
Aug 8, 2022 12:28:44.300527096 CEST	49803	80	192.168.2.3	67.23.226.119
Aug 8, 2022 12:28:44.300573111 CEST	49803	80	192.168.2.3	67.23.226.119
Aug 8, 2022 12:28:44.436374903 CEST	80	49803	67.23.226.119	192.168.2.3
Aug 8, 2022 12:28:49.458475113 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:49.628911018 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.631028891 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:49.631207943 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:49.801218033 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902386904 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902443886 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902481079 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902518988 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902545929 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:28:49.902592897 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:49.902663946 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:51.640513897 CEST	49809	80	192.168.2.3	67.223.117.72
Aug 8, 2022 12:28:51.810667992 CEST	80	49809	67.223.117.72	192.168.2.3
Aug 8, 2022 12:29:01.721714973 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:01.971877098 CEST	80	49817	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:01.972079039 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:01.972229004 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:01.972253084 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:01.972655058 CEST	49818	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.222067118 CEST	80	49817	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.227452040 CEST	80	49818	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.227598906 CEST	49818	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.227710009 CEST	49818	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.232486010 CEST	80	49817	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.232532978 CEST	80	49817	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.232578039 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.232604027 CEST	49817	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.482373953 CEST	80	49818	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.489057064 CEST	80	49818	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.489123106 CEST	80	49818	184.168.107.80	192.168.2.3
Aug 8, 2022 12:29:02.489309072 CEST	49818	80	192.168.2.3	184.168.107.80
Aug 8, 2022 12:29:02.489403963 CEST	49818	80	192.168.2.3	184.168.107.80

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:29:02.744102001 CEST	80	49818	184.168.107.80	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:28:32.168889046 CEST	52985	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:28:32.449382067 CEST	53	52985	8.8.8.8	192.168.2.3
Aug 8, 2022 12:28:38.314755917 CEST	52810	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:28:38.334137917 CEST	53	52810	8.8.8.8	192.168.2.3
Aug 8, 2022 12:28:43.877885103 CEST	55151	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:28:44.018109083 CEST	53	55151	8.8.8.8	192.168.2.3
Aug 8, 2022 12:28:49.332912922 CEST	64816	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:28:49.456350088 CEST	53	64816	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:01.681569099 CEST	49723	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:01.719481945 CEST	53	49723	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:07.523072958 CEST	52581	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:08.532000065 CEST	52581	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:09.578977108 CEST	52581	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:11.663458109 CEST	52581	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:12.542298079 CEST	53	52581	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:12.571427107 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:13.551590919 CEST	53	52581	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:13.579313993 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:14.594968081 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:14.598031998 CEST	53	52581	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:16.610747099 CEST	50152	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:16.682765961 CEST	53	52581	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:17.592346907 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:18.598768950 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:19.614202976 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:21.629395008 CEST	53	50152	8.8.8.8	192.168.2.3
Aug 8, 2022 12:29:22.596843958 CEST	56639	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:29:22.630506992 CEST	53	56639	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Aug 8, 2022 12:29:13.551677942 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 8, 2022 12:29:14.598773003 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 8, 2022 12:29:16.682864904 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 8, 2022 12:29:18.598884106 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 8, 2022 12:29:19.614459038 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable
Aug 8, 2022 12:29:21.629515886 CEST	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:28:32.168889046 CEST	192.168.2.3	8.8.8.8	0x260e	Standard query (0)	www.kirchhoff-darryl.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:38.314755917 CEST	192.168.2.3	8.8.8.8	0x93ae	Standard query (0)	www.tomoptique.fr	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:43.877885103 CEST	192.168.2.3	8.8.8.8	0xd4b1	Standard query (0)	www.boshi-eg.online	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:49.332912922 CEST	192.168.2.3	8.8.8.8	0x603	Standard query (0)	www.esandcraic.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:01.681569099 CEST	192.168.2.3	8.8.8.8	0x7af8	Standard query (0)	www.mexc-event-partner.site	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:29:07.523072958 CEST	192.168.2.3	8.8.8.8	0x6d06	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:08.532000065 CEST	192.168.2.3	8.8.8.8	0x6d06	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:09.578977108 CEST	192.168.2.3	8.8.8.8	0x6d06	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:11.663458109 CEST	192.168.2.3	8.8.8.8	0x6d06	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:12.571427107 CEST	192.168.2.3	8.8.8.8	0x4d10	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:13.579313993 CEST	192.168.2.3	8.8.8.8	0x4d10	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:14.594968081 CEST	192.168.2.3	8.8.8.8	0x4d10	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:16.610747099 CEST	192.168.2.3	8.8.8.8	0x4d10	Standard query (0)	www.gzkanglongkeji.com	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:22.596843958 CEST	192.168.2.3	8.8.8.8	0xdf98	Standard query (0)	www.fundycases.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:28:32.449382067 CEST	8.8.8.8	192.168.2.3	0x260e	No error (0)	www.kirchhoff-darryl.com		107.155.208.43	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:38.334137917 CEST	8.8.8.8	192.168.2.3	0x93ae	No error (0)	www.tomoptique.fr	tomoptique.fr		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:28:38.334137917 CEST	8.8.8.8	192.168.2.3	0x93ae	No error (0)	tomoptique.fr		109.234.162.62	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:44.018109083 CEST	8.8.8.8	192.168.2.3	0xd4b1	No error (0)	www.boshi-eg.online	boshi-eg.online		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:28:44.018109083 CEST	8.8.8.8	192.168.2.3	0xd4b1	No error (0)	boshi-eg.online		67.23.226.119	A (IP address)	IN (0x0001)
Aug 8, 2022 12:28:49.456350088 CEST	8.8.8.8	192.168.2.3	0x603	No error (0)	www.esandcraic.com		67.223.117.72	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:01.719481945 CEST	8.8.8.8	192.168.2.3	0x7af8	No error (0)	www.mexc-event-partner.site	mexc-event-partner.site		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:29:01.719481945 CEST	8.8.8.8	192.168.2.3	0x7af8	No error (0)	mexc-event-partner.site		184.168.107.80	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:12.542298079 CEST	8.8.8.8	192.168.2.3	0x6d06	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:13.551590919 CEST	8.8.8.8	192.168.2.3	0x6d06	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:14.598031998 CEST	8.8.8.8	192.168.2.3	0x6d06	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:16.682765961 CEST	8.8.8.8	192.168.2.3	0x6d06	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:17.592346907 CEST	8.8.8.8	192.168.2.3	0x4d10	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:18.598768950 CEST	8.8.8.8	192.168.2.3	0x4d10	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:19.614202976 CEST	8.8.8.8	192.168.2.3	0x4d10	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:21.629395008 CEST	8.8.8.8	192.168.2.3	0x4d10	Server failure (2)	www.gzkanglongkeji.com	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 12:29:22.630506992 CEST	8.8.8.8	192.168.2.3	0xdf98	No error (0)	www.fundycases.com	gcdn0.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:29:22.630506992 CEST	8.8.8.8	192.168.2.3	0xdf98	No error (0)	gcdn0.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:29:22.630506992 CEST	8.8.8.8	192.168.2.3	0xdf98	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:29:22.630506992 CEST	8.8.8.8	192.168.2.3	0xdf98	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-199-15-163-148.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 12:29:22.630506992 CEST	8.8.8.8	192.168.2.3	0xdf98	No error (0)	td-balancer-199-15-163-148.wixdns.net		199.15.163.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.kirchhoff-darryl.com
- www.tomoptique.fr
- www.boshi-eg.online
- www.esandcraic.com
- www.mexc-event-partner.site

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49776	107.155.208.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:32.786432028 CEST	7566	OUT	GET /02pi/?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91+KgqpPGSJqKC7J3zS0r1gze3M+2qFZl2NsX2aSbasAE+ZE0SL8u6zgnew==&wRtdp=ETVPg0_ HTTP/1.1 Host: www.kirchhoff-darryl.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 12:28:33.078955889 CEST	7566	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 10:28:32 GMT Server: Apache/2.2.15 (CentOS) Location: http://www.kirchhoff-darryl.com/02pi?ZL0=JO9pwDAFX0pE08ZhB6JsQfIKbq32cMNHUs94bAK91+KgqpPGSJqKC7J3zS0r1gze3M+2qFZl2NsX2aSbasAE+ZE0SL8u6zgnew==&wRtdp=ETVPg0_ Content-Length: 457 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6b 69 72 63 68 68 6f 66 66 2d 64 61 72 72 79 6c 2e 63 6f 6d 2f 30 32 70 69 3f 5a 4c 30 3d 4a 4f 39 70 77 44 41 46 58 30 70 45 30 38 5a 68 42 36 4a 73 51 66 49 4b 62 71 33 32 63 4d 4e 48 55 73 39 34 62 41 4b 39 31 2b 4b 67 71 70 50 47 53 4a 71 4b 43 37 4a 33 7a 53 30 72 31 67 7a 65 33 4d 2b 32 71 46 5a 6c 32 4e 73 58 32 61 53 62 61 73 41 45 2b 5a 45 30 53 4c 38 75 36 7a 67 6e 65 77 3d 3d 26 61 6d 70 3b 77 52 74 64 70 3d 45 54 56 50 67 30 5f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 32 2e 31 35 20 28 43 65 6e 74 4f 53 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 6b 69 72 63 68 68 6f 66 66 2d 64 61 72 72 79 6c 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.2.15 (CentOS) Server at www.kirchhoff-darryl.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49780	109.234.162.62	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:38.365463018 CEST	7583	OUT	GET /02pi/?ZL0=thvfohwi7xD8LUPTC+PvURbDlMdrWv6G+kdQz5W5EjaeNcjaAM/7YzWabXa+Emqnmxa+j2rvyn8aQKdomTvD7NHn7LH6m5q/aw==&wRtdp=ETVPg0_ HTTP/1.1 Host: www.tomoptique.fr Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:38.864422083 CEST	7587	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 10:28:38 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://tomoptique.fr/02pi/?ZL0=thvfohwi7xD8LUPTC+PvURbDlMdrWv6G+kdQz5W5EjaeNcjaAM/7YzWabXa+Emqnmxa+j2rvyn8aQKdomTvD7NHn7LH6m5q/aw==&wRtdp=ETVPg0_ Server: o2switch-PowerBoost-v3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49803	67.23.226.119	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:44.161489964 CEST	7676	OUT	GET /02pi/?ZL0=4npjF3s9G6uWNp4ceBGqcNUcjkX96JEG8J4d3OAuWw45Kxpl9gSb2BHY5Eg4Nc6InaukRaYVJuT4y0aleUHPUlqgoOBFmRDZHQ==&wRtdp=ETVPg0_ HTTP/1.1 Host: www.boshi-eg.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 12:28:44.300245047 CEST	7677	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 10:28:44 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49809	67.223.117.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:49.631207943 CEST	7769	OUT	GET /02pi/?ZL0=H3j/zDn1cik0H8aEc4JTyOZmy0u09IlpCgxUGgbrjIcqKZuTm1TQkyEN0mTnJzpMGdd8V9PF4iBs4MdYqflf8PDJEP40yO/f8Q==&wRtdp=ETVPg0_ HTTP/1.1 Host: www.esandcraic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:28:49.902386904 CEST	7770	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 10:28:49 GMT Server: Apache Content-Length: 5278 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 09 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 22 3e 0a 0a 09 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 0a 0a 09 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4d 6f 6e 74 73 65 72 72 61 74 3a 32 30 30 2c 34 30 30 2c 37 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 0a 0a 09 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 63 73 73 2f 34 30 34 2e 63 73 73 22 20 2f 3e 0a 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 3e 3c 2f 64 69 76 3e 0a 3c 73 76 67 20 69 64 3d 22 73 76 67 57 72 61 70 5f 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 78 3d 22 30 70 78 22 20 79 3d 22 30 70 78 22 20 76 69 65 77 42 6f 78 3d 22 30 20 30 20 37 30 30 20 32 35 30 22 3e 0a 20 20 3c 67 3e 0a 20 20 20 20 3c 70 61 74 68 20 69 64 3d 22 69 64 33 5f 32 22 20 64 3d 22 4d 31 39 35 2e 37 20 32 33 32 2e 36 37 68 2d 33 37 2e 31 56 31 34 39 2e 37 48 32 37 2e 37 36 63 2d 32 2e 36 34 20 30 2d 35 2e 31 2d 2e 35 2d 37 2e 33 36 2d 31 2e 34 39 2d 32 2e 32 37 2d 2e 39 39 2d 34 2e 32 33 2d 32 2e 33 31 2d 35 2e 38 38 2d 33 2e 39 36 2d 31 2e 36 35 2d 31 2e 36 35 2d 32 2e 39 35 2d 33 2e 36 31 2d 33 2e 38 39 2d 35 2e 38 38 73 2d 31 2e 34 32 2d 34 2e 36 37 2d 31 2e 34 32 2d 37 2e 32 32 56 32 39 2e 36 32 68 33 36 2e 38 32 76 38 32 2e 39 38 48 31 35 38 2e 36 56 32 39 2e 36 32 68 33 37 2e 31 76 32 30 33 2e 30 35 7a 22 2f 3e 0a 20 20 20 20 3c 70 61 74 68 20 69 64 3d 22 69 64 32 5f 32 22 20 64 3d 22 4d 34 37 30 2e 36 39 20 31 34 37 2e 37 31 63 30 20 38 2e 33 31 2d 31 2e 30 36 20 31 36 2e 31 37 2d 33 2e 31 39 20 32 33 2e 35 38 2d 32 2e 31 32 20 37 2e 34 31 2d 35 2e 31 32 20 31 34 2e 32 38 2d 38 2e 39 39 20 32 30 2e 36 2d 33 2e 38 37 20 36 2e 33 33 2d 38 2e 34 35 20 31 31 2e 39 39 2d 31 33 2e 37 34 20 31 36 2e 39 39 2d 35 2e 32 39 20 35 2d 31 31 2e 30 37 20 39 2e 32 38 2d 31 37 2e 33 35 20 31 32 2e 38 31 61 38 35 2e 31 34 36 20 38 35 2e 31 34 36 20 30 20 30 20 30 20 31 2d 32 31 2e 36 37 20 32 2e 38 33 48 33 31 39 2e 33 63 2d 37 2e 34 36 20 30 2d 31 34 2e 37 33 2d 2e 39 34 2d 32 31 2e 38 31 2d 32 2e 38 33 2d 37 2e 30 38 2d 31 2e 38 39 2d 31 33 2e 37 36 2d 34 2e 36 2d 32 30 2e 30 34 2d 38 2e 31 34 61 38 38 2e 32 39 32 20 38 38 2e 32 39 32 20 30 20 30 20 30 20 31 2d 31 37 2e 33 35 2d 31 32 2e 38 31 63 2d 35 2e 32 39 2d 35 2d 39 2e 38 34 2d 31 30 2e 36 37 2d 31 33 2e 36 36 2d 31 36 2e 39 39 2d 33 2e 38 32 2d 36 2e 33 32 2d 36 2e 38 2d 31 33 2e 31 39 2d 38 2e 39 32 2d 32 30 2e 36 2d 32 2e 31 32 2d 37 2e 34 31 2d 33 2e 31 39 2d 31 35 2e 32 37 2d 33 2e 31 39 2d 32 33 2e 35 38 76 2d 33 33 2e 31 33 63 30 2d 31 32 2e 34 36 20 32 2e 33 34 2d 32 33 2e 38 38 20 37 2e 30 31 2d 33 34 2e 32 37 20 34 2e 36 37 Data Ascii: <!DOCTYPE html><html lang="en"><head><meta charset="utf-8"><meta http-equiv="X-UA-Compatible" content="IE=edge"><meta name="viewport" content="width=device-width, initial-scale=1"><title>404 Not Found</title><link href="https://fonts.googleapis.com/css?family=Montserrat:200,400,700" rel="stylesheet"><link type="text/css" rel="stylesheet" href="/css/404.css" /></head><body> <svg id="svgWrap_2" xmlns="http://www.w3.org/2000/svg" x="0px" y="0px" viewBox="0 0 700 250"> <g> <path id="id3_2" d="M195.7 232.67h-37.1V149.7H27.76c-2.64 0-5.1-.5-7.36-1.49-2.27-.99-4.23-2.31-5.88-3.96-1.65-1.65-2.95-3.61-3.89-5.88s-1.42-4.67-1.42-7.22V29.62h36.82v82.98H158.6V29.62h37.1v203.05z"/> <path id="id2_2" d="M470.69 147.71c0 8.31-1.06 16.17-3.19 23.58-2.12 7.41-5.12 14.28-8.99 20.6-3.87 6.33-8.45 11.99-13.74 16.99-5.29 5-11.07 9.28-17.35 12.81a85.146 85.146 0 0 1-20.04 8.14 83.637 83.637 0 0 1-21.67 2.83H319.3c-7.46 0-14.73-.94-21.81-2.83-7.08-1.89-13.76-4.6-20.04-8.14a88.292 88.292 0 0 1-17.35-12.81c-5.29-5-9.84-10.67-13.66-16.99-3.82-6.32-6.8-13.19-8.92-20.6-2.12-7.41-3.19-15.27-3.19-23.58v-33.13c0-12.46 2.34-23.88 7.01-34.27 4.67

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49817	184.168.107.80	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:29:01.972229004 CEST	8097	OUT	POST /02pi/ HTTP/1.1 Host: www.mexc-event-partner.site Connection: close Content-Length: 409 Cache-Control: no-cache Origin: http://www.mexc-event-partner.site User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.mexc-event-partner.site/02pi/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 5a 4c 30 3d 44 76 79 6b 59 68 57 49 4d 35 4c 42 4a 6a 4d 50 6a 54 75 63 62 57 6d 55 44 47 6a 73 66 32 46 4f 72 53 64 48 57 70 34 47 61 33 74 68 66 6a 38 75 79 5f 54 78 59 47 53 44 75 33 62 4c 39 42 7a 62 39 47 57 70 74 79 46 63 62 75 70 69 6f 68 6f 32 6d 5a 51 56 77 5a 7e 45 62 35 42 51 71 64 43 78 66 72 6f 78 42 49 62 70 39 44 47 75 43 31 5a 30 69 52 7a 49 4d 53 7a 7a 32 78 43 77 6d 76 61 52 4e 31 7a 49 62 44 50 49 4d 5f 62 72 31 33 36 6b 6d 7a 39 35 4e 67 61 62 55 51 4a 31 6b 50 63 62 41 55 71 63 37 55 45 52 32 73 48 51 55 66 46 65 5a 46 4f 7a 35 4e 4e 35 7a 68 6b 4a 6b 50 6b 35 57 53 37 6a 28 47 52 42 41 71 49 7a 64 74 78 42 54 72 46 39 36 4c 77 2d 57 32 63 52 66 32 63 57 74 31 28 5f 4b 43 54 63 65 35 74 43 76 64 59 53 45 5f 6f 36 59 31 59 2d 41 79 45 43 4f 36 6e 73 66 6e 71 72 39 4d 35 34 6d 44 79 6f 39 47 71 66 4f 48 6c 58 37 74 41 41 7a 32 51 4a 71 51 41 63 33 52 49 4f 45 2d 42 64 71 4a 48 6c 69 37 6b 68 41 6c 45 4f 6d 68 6a 72 35 37 6b 71 6e 4e 55 6f 6e 4e 66 4f 51 70 48 43 58 79 67 71 66 58 67 68 77 34 71 52 56 47 6c 61 38 50 50 57 5a 63 4c 6c 7e 38 65 44 72 52 57 79 48 4a 59 70 30 53 4a 41 56 59 6c 76 6d 33 33 33 6c 6f 4f 2d 6b 6b 54 2d 63 69 57 52 79 36 54 35 7a 51 79 71 52 6f 44 4c 6d 41 29 2e 00 00 00 00 00 00 00 00 Data Ascii: ZL0=DvykYhWIM5LBJjMPjTucbWmUDGjsf2FOrSdHWp4Ga3thfj8uy_TxYGSDu3bL9Bzb9GWptyFcbu pioho2mZQVwZ~Eb5BQqdCxfroxBIbp9DGuC1Z0iRzIMSzz2xCwmvaRN1zIbDPIM_br136kmz95NgabUQJ1kPcbAUqc 7UER2sHQUfFeZFOz5NN5zhkJkPk5WS7j(GRBAqIzdtxBTrF96Lw-W2cRf2cWt1(_KCTce5tCvdYSE_o6Y1Y-AyECO6 nsfnqr9M54mDyo9GqfOHIX7tAAz2QJqQAc3RIOE-BdqJHli7khAlEOmhjr57kqnNUonNfOQpHCXygqfXghw4qRVGla 8PPWZcLl~8eDrRWyHJYp0SJAVYlvm333loO-kkT-ciWRy6T5zQyqRoDLmA).

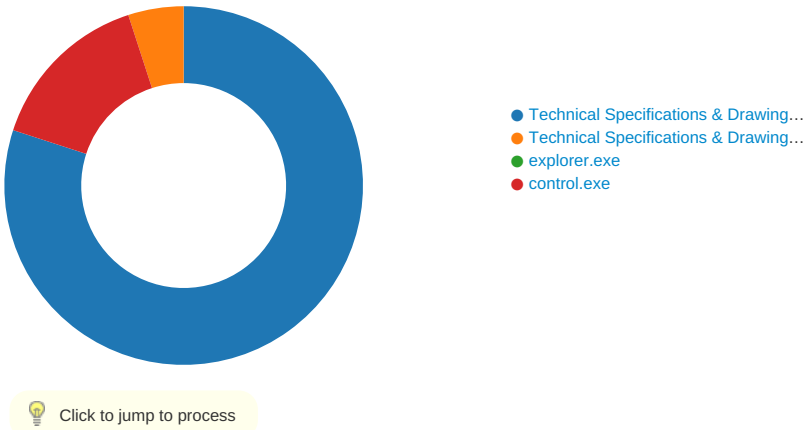
Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:29:02.232486010 CEST	8099	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 10:29:02 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49818	184.168.107.80	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 12:29:02.227710009 CEST	8098	OUT	GET /02pi/?ZL0=OtaEbXX4ObCoLhtF/lWLZX2dLDLBfFgcjwhWC5AcKk5LEysMwPLPLl+t4RfX0ATi8hGNnWUlfKNR4DoGgewcnJOxYMoo89i/Ow==&wRtdp=ETVPg0_ HTTP/1.1 Host: www.mexc-event-partner.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 12:29:02.489057064 CEST	8100	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 10:29:02 GMT Server: Apache Content-Length: 315 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 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 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Statistics

Behavior



System Behavior

Analysis Process: Technical Specifications & Drawings.exe PID: **6080**, Parent PID: **5240**

General

Target ID:	0
Start time:	12:27:07
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Technical Specifications & Drawings.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Technical Specifications & Drawings.exe"
Imagebase:	0x400000
File size:	800256 bytes
MD5 hash:	9B94F751E8CC145058DB9F428C2AD571
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.264997908.0000000002BA2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.265706280.00000000039FD000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.265706280.00000000039FD000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.265706280.00000000039FD000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.265706280.00000000039FD000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.263808361.0000000002973000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Analysis Process: Technical Specifications & Drawings.exe PID: **5084**, Parent PID: **6080**

General

Target ID:	4
Start time:	12:27:16
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Technical Specifications & Drawings.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Technical Specifications & Drawings.exe
Imagebase:	0xd20000
File size:	800256 bytes
MD5 hash:	9B94F751E8CC145058DB9F428C2AD571
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: 00000004.00000000.260249710.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000004.00000000.260249710.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.260249710.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.260249710.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
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	41B297	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5084**

General

Target ID:	5
Start time:	12:27:19
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.314845901.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.314845901.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.314845901.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.314845901.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.333361957.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.333361957.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.333361957.000000000B546000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.333361957.000000000B546000.00000040.00000001.00040000.00000000.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: control.exe PID: **1896**, Parent PID: **3968**

General

Target ID:	19
Start time:	12:27:54
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x1c0000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.508193652.00000000024C0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.513252120.0000000004260000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.513252120.0000000004260000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.513252120.0000000004260000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.513252120.0000000004260000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.510569655.0000000002A30000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.510569655.0000000002A30000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.510569655.0000000002A30000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.510569655.0000000002A30000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Technical Specifications & Drawings.exe	success or wait	1	24DB2C7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\207G7-97P	object name not found	1	24DB2C7	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	24DB297	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