ID: 755081
Sample Name: Lakeringernes (1).exe
Cookbook: default.jbs
Time: 10:17:46
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

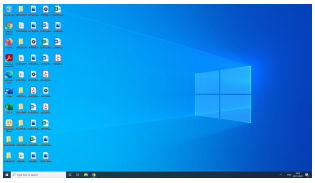
Windows Analysis Report

Lakeringernes (1).exe

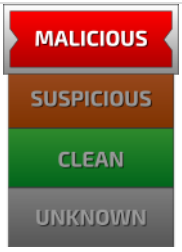
Overview

General Information

Sample Name:	Lakeringernes (1).exe
Analysis ID:	755081
MD5:	d70de507cc0d22..
SHA1:	9818fba05573d6..
SHA256:	4dbcd711f22637..
Infos:	



Detection



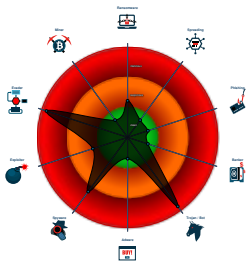
FormBook, GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for URL or domain
- Yara detected GuLoader
- 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…
- Writes to foreign memory regions
- Tries to detect Any.run

Classification



Process Tree

- **System is w10x64native**
- Lakeringernes (1).exe (PID: 2508 cmdline: C:\Users\user\Desktop\Lakeringernes (1).exe MD5: D70DE507CC0D22E43EBCF8B61A273EA5)
  - Lakeringernes (1).exe (PID: 384 cmdline: C:\Users\user\Desktop\Lakeringernes (1).exe MD5: D70DE507CC0D22E43EBCF8B61A273EA5)
    - RAVCpl64.exe (PID: 7704 cmdline: "C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s MD5: 731FB4B2E5AFBCADAABB80D642E056AC)
      - wscript.exe (PID: 3316 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 4D780D8F77047EE1C65F747D9F63A1FE)
        - explorer.exe (PID: 4684 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
        - firefox.exe (PID: 1716 cmdline: C:\Program Files\Mozilla Firefox\Firefox.exe MD5: FA9F4FC5D7ECAB5A20BF7A9D1251C851)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.techrocker.com/i036/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0c9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac41:$sqlite3step: 68 34 1C 7B E1 • 0x1a10b:$sqlite3text: 68 38 2A 90 C5 • 0x1ac86:$sqlite3text: 68 38 2A 90 C5 • 0x1a122:$sqlite3blob: 68 53 D8 7F 8C • 0x1ac9c:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17bd5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17681:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17cd7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e4f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa46a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168cc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1ddc7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6601:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f050:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa89f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17dd7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000008.00000000.2252030385.0000000000511000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 28 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 66.29.151.40	
Timestamp:	192.168.11.2066.29.151.4049856802031453 11/28/22-10:24:42.586053
SID:	2031453
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	
Timestamp:	192.168.11.2050.87.192.14449908802031453 11/28/22-10:27:29.159793
SID:	2031453
Source Port:	49908
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	
Timestamp:	192.168.11.2050.87.192.14449845802031453 11/28/22-10:22:54.782392
SID:	2031453
Source Port:	49845
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	
Timestamp:	192.168.11.2050.87.192.14449845802031412 11/28/22-10:22:54.782392
SID:	2031412

Source Port:	49845
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 66.29.151.40	−
Timestamp:	192.168.11.2066.29.151.4049856802031449 11/28/22-10:24:42.586053
SID:	2031449
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	−
Timestamp:	192.168.11.2050.87.192.14449908802031412 11/28/22-10:27:29.159793
SID:	2031412
Source Port:	49908
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	−
Timestamp:	192.168.11.2050.87.192.14449845802031449 11/28/22-10:22:54.782392
SID:	2031449
Source Port:	49845
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 66.29.151.40	−
Timestamp:	192.168.11.2066.29.151.4049856802031412 11/28/22-10:24:42.586053
SID:	2031412
Source Port:	49856
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 50.87.192.144	−
Timestamp:	192.168.11.2050.87.192.14449908802031449 11/28/22-10:27:29.159793
SID:	2031449
Source Port:	49908
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

Networking

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

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

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

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

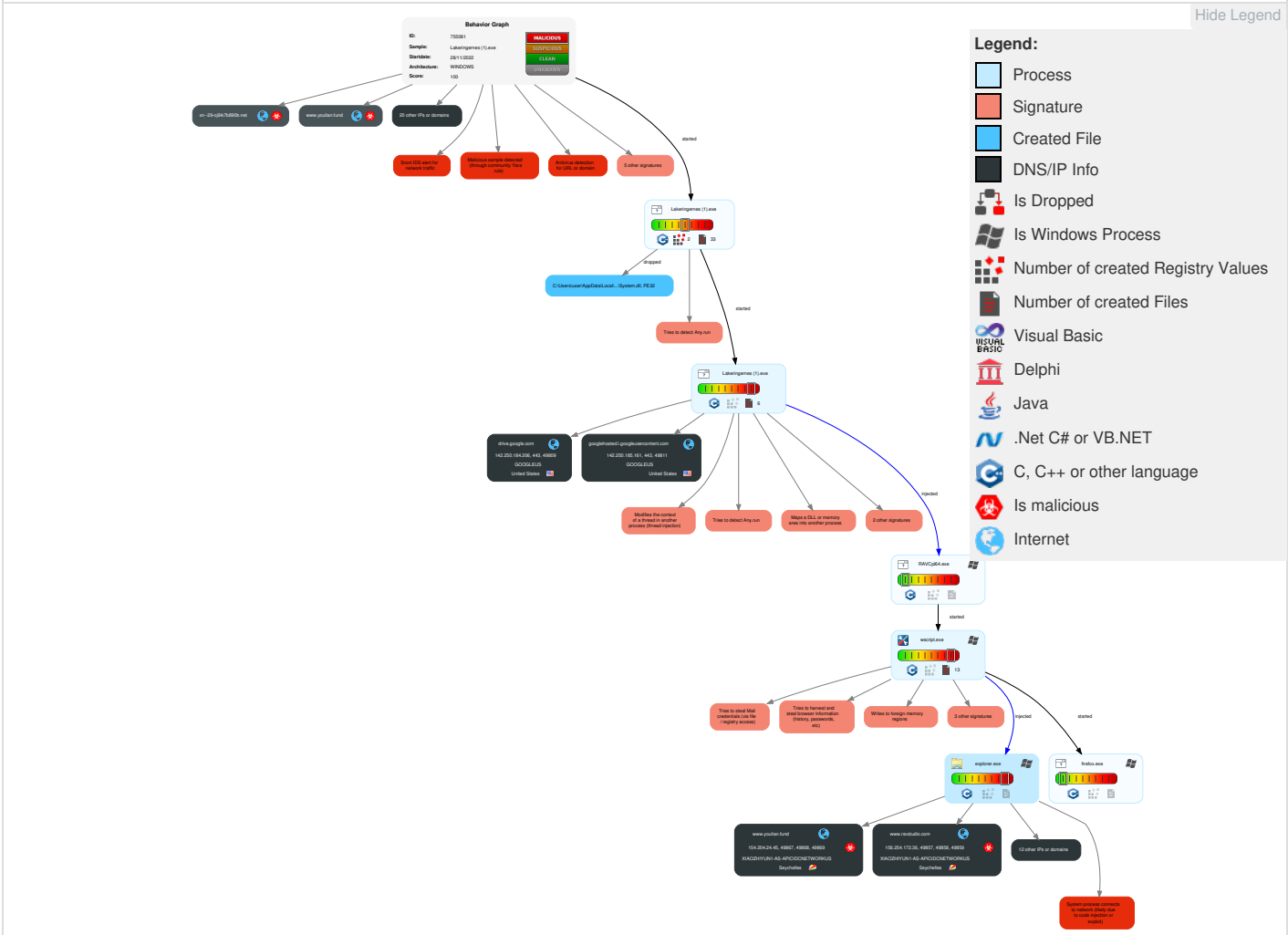
Yara detected FormBook

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 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/Reboot
Default Accounts	1 Shared Modules	1 Windows Service	1 Access Token Manipulation	3 Obfuscated Files or Information	LSASS Memory	5 System Information Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Windows Service	1 Software Packing	Security Account Manager	1 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	7 1 2 Process Injection	1 DLL Side-Loading	NTDS	1 2 Virtualization/Sandbox Evasion	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 2 Virtualization/Sandbox Evasion	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 Access Token Manipulation	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	7 1 2 Process Injection	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

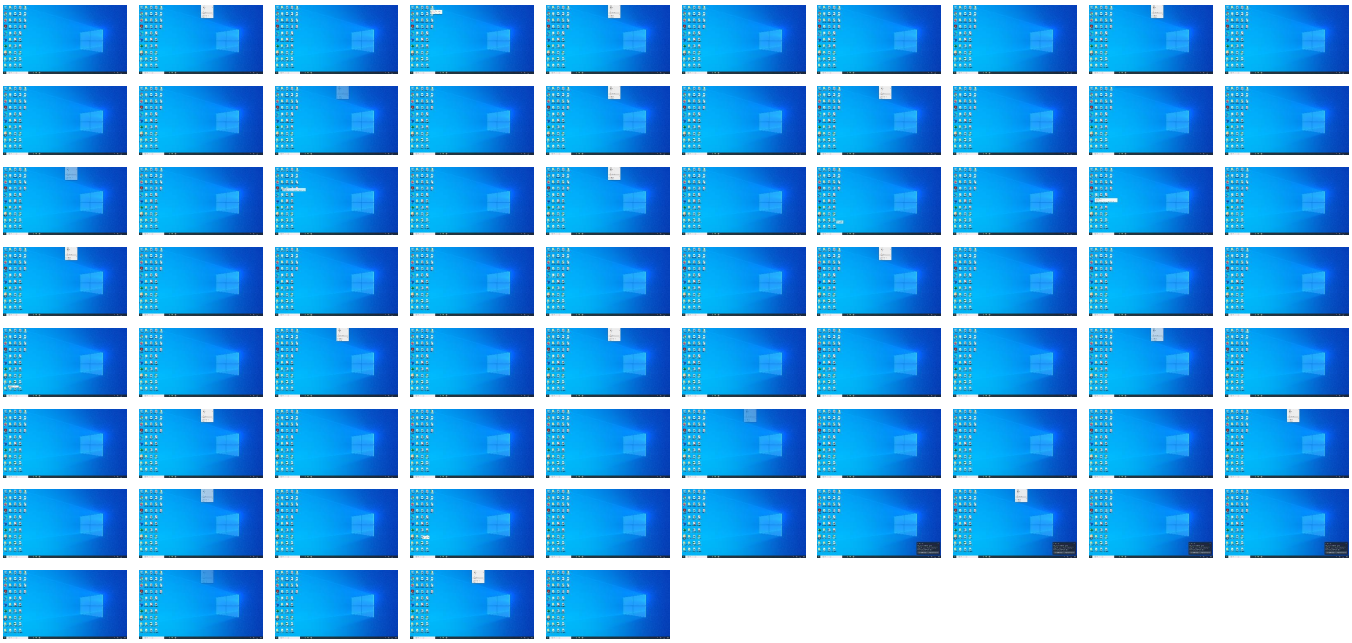
Behavior Graph



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
Lakeringernes (1).exe	35%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
Lakeringernes (1).exe	77%	ReversingLabs	Win32.Trojan.NSISInject	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsbCBD1.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Lakeringernes (1).exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
10.0.explorer.exe.13ac3814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
12.0.firefox.exe.6a93814.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.Lakeringernes (1).exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
10.0.explorer.exe.13ac3814.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.0.explorer.exe.13ac3814.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.Lakeringernes (1).exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
12.0.firefox.exe.6a93814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.wscript.exe.4d53814.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.Lakeringernes (1).exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
6.0.Lakeringernes (1).exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
12.2.firefox.exe.6a93814.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.2.wscript.exe.859208.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.Lakeringernes (1).exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
10.0.explorer.exe.13ac3814.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
xn--29-oj9ik7b890b.net	2%	Virustotal		Browse
www.005404.com	4%	Virustotal		Browse
automotiveparts-store.com	4%	Virustotal		Browse
www.youlian.fund	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://www.rsvstudio.com/i036/	0%	Avira URL Cloud	safe	
www.techrocker.com/i036/	0%	Avira URL Cloud	safe	
http://https://word.office.comle	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/wp-json/	0%	Avira URL Cloud	safe	
http://www.aceadora.shop/i036/?k0GP1N2=KIxzD5HsRZBgKJlqtD/Z5Gj6Z8qoplCrxdfuDjJNx/1c9AJO6VXMMK+63l9AWb1/ssE5X6NYSlv5byLnNWr+FpxZxtTvuFnXWw==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://www.avatarworker.com/	0%	Avira URL Cloud	safe	
http://https://outlook.comx86)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.techrocker.com/i036/?k0GP1N2=Nt7we/gwvJafOenmPtqMdMQq0A5S+F0mCo2A/o6NNSBEDFrZxTdugE3hHqQHgmQnwi6pFnnhcgi6C1+qKckarzI1zqVfAVRktw==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://www.youlian.fund/i036/?k0GP1N2=LMlqSMdQ3q0mQ0O8E4Be7P+zrPM6Gg4aprrhhSoZXl8N9fokAeXZtK7CAx7jxtppbBVDda4uu0E3KjN/+XSSDpZJ6husVXmnlg==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://www.microsoft.c-	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/comments/feed/	0%	Avira URL Cloud	safe	
http://www.rsvstudio.com/i036/?k0GP1N2=ronhS2NZk+RpAH8xyVeuvsbzfj1G+JCO7SbBJB6VTjQ5GvCPMYygorm2sXuQ6whLqX4zWjebsFwcRWcR3e6VRFoMUbeOjCqRvg==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/feed/	0%	Avira URL Cloud	safe	
http://https://outlook.comriH	0%	Avira URL Cloud	safe	
http://www.plentywindshield.com/	100%	Avira URL Cloud	malware	
http://microsoft.co	0%	Avira URL Cloud	safe	
http://www.haveusstampsale.shop/i036/	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	0%	Avira URL Cloud	safe	
http://www.planetthermo.net/i036/	0%	Avira URL Cloud	safe	
http://www.xn--29-oj9ik7b890b.net/i036/?k0GP1N2=BZwpaihTGJGWcZJSAe2sxznsnPej0JxCYfoQvgCgbuMQP061bK/C39YT663oVlO5elykthEFB/Dcn8VFPsLzlGidWMmSTKgllQ==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://https://www.automotiveparts-store.com/i036/?k0GP1N2=30w/opVeBRN2BD0	0%	Avira URL Cloud	safe	
http://www.automotiveparts-store.com/i036/	0%	Avira URL Cloud	safe	
http://www.xn--29-oj9ik7b890b.net/i036/	0%	Avira URL Cloud	safe	
http://https://excel.office.como	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/wp-content/themes/twentytwentytwo/style.css?ver=1.3	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/	0%	Avira URL Cloud	safe	
http://www.mangal20.com/i036/	0%	Avira URL Cloud	safe	
http://www.mangal20.com/i036/?k0GP1N2=Ypm+0+Vc/krk+syJRkmS/ZXdqh86ue5y1szx5SRmlweqmqT2L40Pqi55gxfwp+7cpcP0UgmrVUc/vOiRo42zU0SjFnllzv841Q==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://45.122.138.45/favicon.ico	0%	Avira URL Cloud	safe	
http://https://powerpoint.office.comCallr	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	
http://www.haveusstampsale.shop/i036/?k0GP1N2=DDTM8NTjTGQKNl9ZmiWQMqmzY5hUHu6DmELfmDs1vEv26+wpTDEFgWjPjGJv2unzSeE04u298BAHHYXe+vHUgcxZ13bZmjQmZA==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://www.techrocker.com/i036/	0%	Avira URL Cloud	safe	
http://https://www.aceadora.shop/i036/?k0GP1N2=KIxzD5HsRZBgKJlqtD/Z5Gj6Z8qoplCrxdfuDjJNx/1c9AJO6VXMMK	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/wp-includes/blocks/navigation/view.min.js?ver=c24330f635f5cb9d5e0e	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.aceadora.shop/i036/	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://www.gouldent.site/i036/	0%	Avira URL Cloud	safe	
http://www.plentywindshield.com/i036/?k0GP1N2=VaB2QWBCteskeZJAX4Hj3Mdw7Sfdvkj	100%	Avira URL Cloud	malware	
http://mangal20.com/i036/?k0GP1N2=Ypm	0%	Avira URL Cloud	safe	
http://www.livinghopedoula.com/i036/	0%	Avira URL Cloud	safe	
http://www.livinghopedoula.com/i036/?k0GP1N2=gK12bHhqEy0e4Uj/ImUnYxfT+EkUqBjjVPatb5GnWKdwUy9sF2E4a2NySHYDGj5+R015BuqmsIpMnBRMM6PNmRTNIYpZBhLGAQ==&Rzu=hV1Pon	0%	Avira URL Cloud	safe	
http://xn--299aa717y.xn--3e0b707e/wp-includes/blocks/navigation/view-modal.min.js?ver=45f05135277abf	0%	Avira URL Cloud	safe	
http://www.005404.com/i036/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.rsvstudio.com	156.254.172.36	true	true		unknown
www.avatarworker.com	3.64.163.50	true	true		unknown
xn--29-oj9ik7b890b.net	50.87.192.144	true	true	• 2%, Virustotal, Browse	unknown
www.haveusstampsale.shop	104.21.48.6	true	true		unknown
www.youlian.fund	154.204.24.45	true	true	• 1%, Virustotal, Browse	unknown
automotiveparts-store.com	162.0.238.93	true	true	• 4%, Virustotal, Browse	unknown
www.005404.com	103.63.2.175	true	true	• 4%, Virustotal, Browse	unknown
techrocker.com	23.106.120.176	true	true		unknown
www.livinghopedoula.com	168.76.162.220	true	true		unknown
www.plentywindshield.com	96.43.100.185	true	true		unknown
www.mangal20.com	156.230.149.244	true	true		unknown
www.gouldent.site	66.29.151.40	true	true		unknown
www.planetthermo.net	154.213.44.213	true	true		unknown
drive.google.com	142.250.184.206	true	false		high
www.aceadora.shop	104.21.23.41	true	true		unknown
googlehosted.l.googleusercontent.com	142.250.185.161	true	false		high
doc-00-7s-docs.googleusercontent.com	unknown	unknown	false		high
www.automotiveparts-store.com	unknown	unknown	true		unknown
www.techrocker.com	unknown	unknown	true		unknown
www.xn--29-oj9ik7b890b.net	unknown	unknown	true		unknown
www.sabzi.lol	unknown	unknown	true		unknown
www.caglaakdag.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.techrocker.com/i036/	true	• Avira URL Cloud: safe	low
http://www.rsvstudio.com/i036/	true	• Avira URL Cloud: safe	unknown
http://www.aceadora.shop/i036/?k0GP1N2=KIxzD5HsRZBgKJlqtD/Z5Gj6Z8qoplCrxdfuDjJNx/1c9AJO6VXMMK+63l9AWb1/ssE5X6NYSlv5byLnNWr+FpxZxtTvuFnXWw==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.youlian.fund/i036/?k0GP1N2=LMlqSMdQ3q0mQ0O8E4Be7P+zrPM6Gg4aprrhhSoZXI8N9fokAeXZtK7CAx7jxtppbBVDda4uu0E3KjN/+XSSDpZJ6husVXmnlg==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.techrocker.com/i036/?k0GP1N2=Nt7we/gwvJafOenmPtqMdMQq0A5S+F0mCo2A/o6NNSBEDFrZxTdugE3hHqQHgmQnwi6pFnnhcgi6C1+qKckarzI1zqVfAVRktw==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.rsvstudio.com/i036/?k0GP1N2=ronhS2NZk+RpAH8xyVeuvsbzfj1G+JCO7SbBJB6VTjQ5GvCPMYygorm2sXuQ6whLqX4zWjebsFwcRWcR3e6VRFoMUbeOjCqRvg==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.haveusstampsale.shop/i036/	true	• Avira URL Cloud: safe	unknown
http://www.planetthermo.net/i036/	true	• Avira URL Cloud: safe	unknown
http://www.xn--29-oj9ik7b890b.net/i036/?k0GP1N2=BZwpaihTGJGWcZJSAe2sxznsnPej0JxCYfoQvgCgbuMQP061bK/C39YT663oVIO5elyktthEFB/Dcn8VFPsLzIGidWMmSTKgllQ==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.automotiveparts-store.com/i036/	true	• Avira URL Cloud: safe	unknown
http://www.xn--29-oj9ik7b890b.net/i036/	true	• Avira URL Cloud: safe	unknown
http://www.mangal20.com/i036/	true	• Avira URL Cloud: safe	unknown
http://www.mangal20.com/i036/?k0GP1N2=Ypm+0+Vc/krk+syJRkmS/ZXdqh86ue5y1szx5SRmlweqmqT2L40Pqi55gxfwp+7cpcP0UgmrVUc/vOiRo42zU0SjFnllzv841Q==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.techrocker.com/i036/	true	• Avira URL Cloud: safe	unknown
http://www.haveusstampsale.shop/i036/?k0GP1N2=DDTM8NTjTGQKNl9ZmiWQMqmzY5hUHu6DmELfmDs1vEv26+wpTDEFgWjPjGJv2unzSeE04u298BAHHYXe+vHUgcxZ13bZmjQmZA==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.aceadora.shop/i036/	true	• Avira URL Cloud: safe	unknown
http://www.gouldent.site/i036/	true	• Avira URL Cloud: safe	unknown
http://www.livinghopedoula.com/i036/	true	• Avira URL Cloud: safe	unknown
http://www.livinghopedoula.com/i036/?k0GP1N2=gK12bHhqEy0e4Uj/ImUnYxfT+EkUqBjjVPatb5GnWKdwUy9sF2E4a2NySHYDGj5+R015BuqmsIpMnBRMM6PNmRTNIYpZBhLGAQ==&Rzu=hV1Pon	true	• Avira URL Cloud: safe	unknown
http://www.005404.com/i036/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	wscript.exe, 00000009.00000003.294812383 8.00000000075D7000.00000004.00000800.000 20000.00000000.sdmp, wscript.exe, 000000 09.00000002.6811526907.000000000756800 0. 00000004.00000800.00020000.00000000.sdmp, 752cuCH8.9.dr	false		high
http:// https://uk.search.yahoo.com/favicon.icohttps://uk.searc h.yahoo.com/search	wscript.exe, 00000009.00000003.294812383 8.00000000075D7000.00000004.00000800.000 20000.00000000.sdmp, wscript.exe, 000000 09.00000002.6811526907.000000000756800 0. 00000004.00000800.00020000.00000000.sdmp, 752cuCH8.9.dr	false		high
http://https://duckduckgo.com/ac/?q=	wscript.exe, 00000009.00000002.681152690 7.0000000007568000.00000004.00000800.000 20000.00000000.sdmp, 752cuCH8.9.dr	false		high
http:// https://api.msn.com:443/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2683214489.000000000D59000 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2493103703.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2743569684.000000000D590000.0000 0004.00000001.00020000.00000000.sdmp, ex plorer.exe, 0000000A.00000000.2665887889 .00000000054BC000.00000004.00000001.0002 0000.00000000.sdmp, explorer.exe, 000000 0A.00000000.2609887211.00000000054BC000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2512098330.00000 0000D590000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.2627282062.000000000D590000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://www.avatarworker.com/	wscript.exe, 00000009.00000002.680703979 5.0000000005116000.00000004.10000000.000 40000.00000000.sdmp, firefox.exe, 000000 0C.00000000.3007711714.0000000006E56000. 00000004.80000000.00040000.00000000.sdmp, firefox.exe, 0000000C.00000002.3015426236.000000 0006E56000.00000004.80000000.00040000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xn--299aa717y.xn--3e0b707e/wp-json/	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	Lakeringernes (1).exe, 00000006.00000001 .1985708428.0000000000649000.00000008.00 000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://activity.windows.com/UserActivity.ReadWrite.Cr eatedByAppam	explorer.exe, 0000000A.00000000.27373663 11.000000000D091000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2505755418.000000000D09100 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2677982824.000 000000D091000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2621240275.000000000D091000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://deff.nelreports.net/api/report?cat=msn	explorer.exe, 0000000A.00000000.27523809 90.0000000010ADC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2521656962.0000000010ADC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2692413038.000 0000010ADC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2634323900.0000000010ADC000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://excel.office.com	explorer.exe, 0000000A.00000000.26093213 81.0000000005423000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2724817110.000000000542300 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2492242615.000 0000005423000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	Lakeringernes (1).exe, 00000006.00000001 .1985503795.0000000000626000.00000008.00 000001.01000000.00000006.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://js.users.51.la/21461531.js	wscript.exe, 00000009.00000002.680718187 4.00000000052A8000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://www.gopher.ftp://ftp.	Lakeringernes (1).exe, 00000006.00000001 .1985708428.0000000000649000.00000008.00 000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://word.office.comle	explorer.exe, 0000000A.00000000.25146646 44.000000000D72B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2685356572.000000000D72B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2745951530.000 000000D72B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2629488305.000000000D72B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xn--299aa717y.xn--3e0b707e	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/us/texas-gov-abbott-sends-miles-of-cars-along-border-to-deter-migrant	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://repository.certum.pl/ctsca2021.cer0	Lakeringernes (1).exe	false		high
http://https://uk.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	wscript.exe, 00000009.00000003.294812383 8.00000000075D7000.00000004.00000800.000 20000.00000000.sdmp, 752cuCH8.9.dr	false		high
http://https://drive.google.com/	Lakeringernes (1).exe, 00000006.00000002 .2298865351.00000000018F8000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://https://uk.search.yahoo.com/sugg/chrom	wscript.exe, 00000009.00000002.681152690 7.0000000007568000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://outlook.comx86)	explorer.exe, 0000000A.00000000.25146646 44.000000000D72B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2685356572.000000000D72B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2745951530.000 000000D72B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2629488305.000000000D72B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://wns.windows.com/	explorer.exe, 0000000A.00000000.27527419 38.0000000010B3B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2692683855.0000000010B3B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2634643315.000 0000010B3B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2522098316.0000000010B3B000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://www.certum.pl/CPS0	Lakeringernes (1).exe	false		high
http://https://assets.msn.com/weathermapdata/1/static/svg/72/MostlySunnyDay.svg	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://word.office.com	explorer.exe, 0000000A.00000000.27144844 92.0000000000CF9000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2599827646.0000000000CF900 0.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2483149352.000 0000000CF9000.00000004.00000020.00020000 .00000000.sdmp	false		high

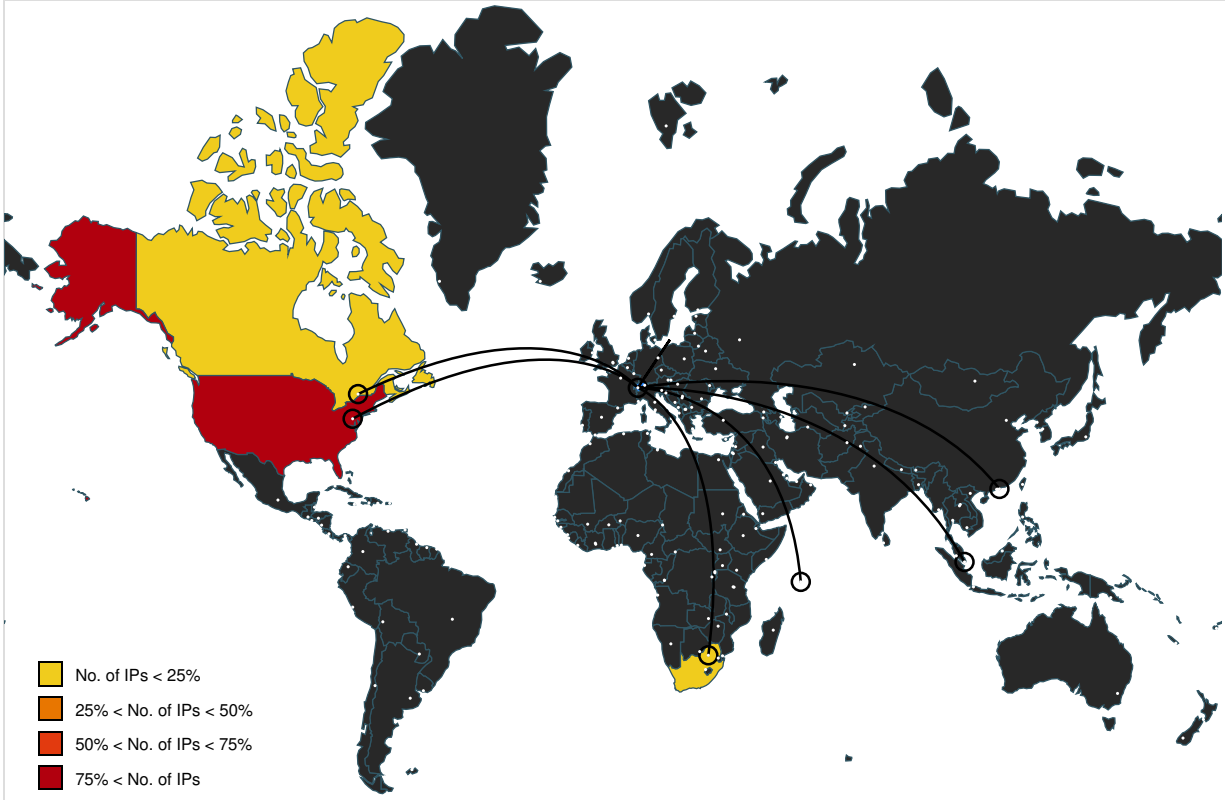
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/en-us/tv/celebrity/tarek-el-moussa-tests-positive-for-covid-19-shuts-down-filmin	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://www.microsoft.c-	explorer.exe, 0000000A.00000000.27527419 38.0000000010B3B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2692683855.0000000010B3B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2634643315.000 0000010B3B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2522098316.0000000010B3B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.certum.pl/ctnca.crl0k	Lakeringernes (1).exe	false		high
http://xn--299aa717y.xn--3e0b707e/feed/	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://microsoft.co	explorer.exe, 0000000A.00000000.27527419 38.0000000010B3B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2692683855.0000000010B3B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2634643315.000 0000010B3B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2522098316.0000000010B3B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xn--299aa717y.xn--3e0b707e/comments/feed/	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://doc-00-7s-docs.googleusercontent.com/	Lakeringernes (1).exe, 00000006.00000002 .2299774052.0000000001976000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://https://www.msn.com/en-us/news/technology/facebook-oversight-board-reviewing-xcheck-system-for-vips/	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	wscript.exe, 00000009.00000002.681152690 7.0000000007568000.00000004.00000800.000 20000.00000000.sdmp, 752cuCH8.9.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	Lakeringernes (1).exe	false		high
http://www.plentywindshield.com/	wscript.exe, 00000009.00000002.681295867 4.00000000075F8000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://outlook.comriH	explorer.exe, 0000000A.00000000.26093213 81.0000000005423000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2724817110.000000000542300 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2492242615.000 0000005423000.00000004.00000001.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com/v1/news/Feed/Windows?activityId=5696A836803C42E0B53F7BB2770E5342&timeOut=10000&o	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://doc-00-7s-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/fgrm3mfa	Lakeringernes (1).exe, 00000006.00000003 .2182121873.000000000197A000.00000004.00 000020.00020000.00000000.sdmp, Lakeringernes (1).exe, 00000006.00000002.2299626181.0000000 001961000.00000004.00000020.00020000.000 00000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://xn--299aa717y.xn--3e0b707e/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_Error	Lakeringernes (1).exe	false		high
http://https://android.notify.windows.com/iOS	explorer.exe, 0000000A.00000000.26708055 99.000000000998B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2614861942.000000000998B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2498248783.000 000000998B000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://https://www.automotiveparts-store.com/i036/?k0GP1N2=30w/opVeBRN2BD0	wscript.exe, 00000009.00000002.680752026 3.00000000055CC000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com/v1/news/Feed/Windows?	explorer.exe, 0000000A.00000000.27144844 92.0000000000CF9000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2599827646.0000000000CF900 0.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2483149352.000 0000000CF9000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://xn--299aa717y.xn--3e0b707e/wp-content/themes/twentytwentytwo/style.css?ver=1.3	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctsca2021.crl0o	Lakeringernes (1).exe	false		high
http://https://wordpress.org	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://xn--299aa717y.xn--3e0b707e/	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://excel.office.como	explorer.exe, 0000000A.00000000.25146646 44.000000000D72B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2685356572.000000000D72B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2745951530.000 000000D72B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2629488305.000000000D72B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://push.zhanzhang.baidu.com/push.js	wscript.exe, 00000009.00000002.680718187 4.00000000052A8000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://schemas.micro	explorer.exe, 0000000A.00000000.26725483 97.0000000009CC0000.00000002.00000001.00 040000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2501251606.000000000A97000 0.00000002.00000001.00040000.00000000.sdmp, explorer.exe, 0000000A.00000000.2603807323.000 00000032C0000.00000002.00000001.00040000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.aceadora.shop/i036/?k0GP1N2=KIxzD5HsRZBgKJlqtD/Z5Gj6Z8qoplCrxdfuDjJNx/1c9AJO6VXMMK	wscript.exe, 00000009.00000002.680774682 5.000000000575E000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/politics/democratic-support-for-suprem0	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://https://powerpoint.office.comCallr	explorer.exe, 0000000A.00000000.25146646 44.000000000D72B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2685356572.000000000D72B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2745951530.000 000000D72B000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2629488305.000000000D72B000.0000 0004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.msn.com/?	explorer.exe, 0000000A.00000000.26777450 22.000000000D073000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2620995953.000000000D07300 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2505511824.000 000000D073000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://45.122.138.45/favicon.ico	wscript.exe, 00000009.00000002.680718187 4.00000000052A8000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	Lakeringernes (1).exe, 00000006.00000001 .1985260298.00000000005F2000.00000008.00 000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com/Czw	Lakeringernes (1).exe, 00000006.00000002 .2298865351.00000000018F8000.00000004.00 000020.00020000.00000000.sdmp	false		high
http://subca.ocsp-certum.com05	Lakeringernes (1).exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com02	Lakeringernes (1).exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	Lakeringernes (1).exe	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	Lakeringernes (1).exe, 00000006.00000001 .1985708428.0000000000649000.00000008.00 000001.01000000.00000006.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	Lakeringernes (1).exe	false		high
http://repository.certum.pl/ctnca2.cer09	Lakeringernes (1).exe	false		high
http://xn--299aa717y.xn--3e0b707e/wp-includes/blocks/navigation/view.min.js?ver=c24330f635f5cb9d5e0e	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://android.notify.windows.com/iOSe/	explorer.exe, 0000000A.00000000.26708055 99.000000000998B000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2614861942.000000000998B00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2498248783.000 000000998B000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://xn--299aa717y.xn--3e0b707e/xmlrpc.php?rsd	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/en-us/news/politics/graham-tries-t	explorer.exe, 0000000A.00000000.26098872 11.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://mangal20.com/i036/?k0GP1N2=Ypm	wscript.exe, 00000009.00000002.680904180 3.00000000063EE000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.plentywindshield.com/i036/?k0GP1N2=VaB2QWBCteskeZJAX4Hj3Mdw7Sfdvkj	wscript.exe, 00000009.00000002.679356349 4.00000000008AB000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://repository.certum.pl/ctnca.cer09	Lakeringernes (1).exe	false		high
http://https://crash-reports.mozilla.com/submit?id=	wscript.exe, 00000009.00000003.300939308 3.0000000007F38000.00000004.00000800.000 20000.00000000.sdmp, wscript.exe, 000000 09.00000003.2948460082.0000000007642000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	wscript.exe, 00000009.00000002.681152690 7.0000000007568000.00000004.00000800.000 20000.00000000.sdmp, 752cuCH8.9.dr	false		high
http://www.litespeedtech.com/error-page	wscript.exe, 00000009.00000002.680880830 1.00000000060CA000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://aka.ms/odirmDRIVE=C	explorer.exe, 0000000A.00000000.27289445 25.000000000989C000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2613644759.000000000989C00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2496890893.000 000000989C000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://https://api.w.org/	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false		high
http://https://zz.bdstatic.com/linksubmit/push.js	wscript.exe, 00000009.00000002.680718187 4.00000000052A8000.00000004.10000000.000 40000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.foreca.com	explorer.exe, 0000000A.00000000.27254666 79.00000000054BC000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.2493103703.00000000054BC00 0.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.2665887889.000 00000054BC000.00000004.00000001.00020000 .00000000.sdmp, explorer.exe, 0000000A.0 0000000.2609887211.00000000054BC000.0000 0004.00000001.00020000.00000000.sdmp	false		high
http://xn--299aa717y.xn--3e0b707e/wp-includes/blocks/navigation/view-modal.min.js?ver=45f05135277abf	wscript.exe, 00000009.00000002.680822005 1.0000000005A82000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	wscript.exe, 00000009.00000002.681152690 7.0000000007568000.00000004.00000800.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.254.172.36	www.rsvstudio.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
154.213.44.213	www.planetthermo.net	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
154.204.24.45	www.youlian.fund	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
162.0.238.93	automotiveparts-store.com	Canada		22612	NAMECHEAP-NETUS	true
96.43.100.185	www.plentywindshield.com	United States		64050	BCPL-SGBGPNETGlobalASNSG	true
104.21.23.41	www.aceadora.shop	United States		13335	CLOUDFLARENETUS	true
156.230.149.244	www.mangal20.com	Seychelles		134705	ITACE-AS-APItaceInternationalLimitedHK	true
3.64.163.50	www.avatarworker.com	United States		16509	AMAZON-02US	true
23.106.120.176	techrocker.com	Singapore		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificpteltdSG	true
66.29.151.40	www.gouldent.site	United States		19538	ADVANTAGECOMUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.161	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
142.250.184.206	drive.google.com	United States		15169	GOOGLEUS	false
50.87.192.144	xn--29-oj9ik7b890b.net	United States		46606	UNIFIEDLAYER-AS-1US	true
103.63.2.175	www.005404.com	Hong Kong		132742	GGL-AS-APGuochaoGrouplimitedHK	true
168.76.162.220	www.livinghopedoula.com	South Africa		265240	ULTRANETSERVICOSEMINTERNETLTDABR	true
104.21.48.6	www.haveusstampsale.shop	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755081
Start date and time:	2022-11-28 10:17:46 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Lakeringernes (1).exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	16
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/6@20/16
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.8% (good quality ratio 12.9%) • Quality average: 73.2% • Quality standard deviation: 28.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe
- HTTP Packets have been reduced
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, wdcp.microsoft.com
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

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\Temp\752cuCH8

Process:	C:\Windows\SysWOW64\wscript.exe
File Type:	SQLite 3.x database, last written using SQLite version 3035005, page size 2048, file counter 5, database pages 59, cookie 0x4f, schema 4, UTF-8, version-valid-for 5
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	1.1305327154874678
Encrypted:	false
SSDEEP:	192:oLt4nKTjebGAUJp/XH9euJDvphC+KRmquPWSTVumQ6:it4nsJp/39RDhw+KRmqu+cVumQ
MD5:	D331C900DDE8ACB523C51D9448205C0A
SHA1:	BDB3366F54876E78F76A6244EDA7A4C302FEB91D
SHA-256:	F199798DF1C37E3A8F6FFF1E208F083CF687F5C6A220DCAD42BB68F2120181CD
SHA-512:	415E4F4F26D4F861063676EA786C2941DB8DB7E248E32D84595BC7D531CE19669AFDCB447BC18B0B723839984CD15269FF6E89EBCD168D8EBD0EC7AF86CC92E7
Malicious:	false
Preview:	SQLite format 3.....@ .....;.....O.....O}.....5.....

C:\Users\user\AppData\Local\Temp\Distressingly\Bloods\Ultraevangelical\Graviton\Kvle\Materialiseringerne\Antenneanlgget\Custom3.ini

Process:	C:\Users\user\Desktop\Lakeringernes (1).exe
File Type:	Generic INItialization configuration [Effect2]
Category:	dropped
Size (bytes):	5487
Entropy (8bit):	4.3524133300305206
Encrypted:	false

SSDEEP:	96:hJDu0BoU1s8G9LfGOOOOOOjOOOOOOEOOOOOOBOOOOOONsOOOOOO/OOOOOOAOOOOW:mCs8GVfGOOOOOOjOOOOOOEOOOOOOBOO4
MD5:	9D3C4AEBBDBCB28530EF93081611A33E
SHA1:	867F6A5B16638E1BFC012DFF7E63E45ADD44342E
SHA-256:	24EC6D9A80EF077A81018001F16E7D7EFE6DEB82B7BD120C8C5227BA65C63F07
SHA-512:	4E5E2ADAE00F160EBDB322B12C33582F8397B909841E76FA634D10C3BCAF90C822DA8F9F494A29FA0EA4B558B6D44BAAEBAF737156B6E38359FB5CFC36874D 2E
Malicious:	false
Preview:	..;Static - FW effect index 0..[Effect1]..ColorR=255..ColorG=0..ColorB=0..Direction=0..Random=0..Ext1=0..Speed=0..Color2R=0..Color2G=0..Color2B=0..DirectType=0. .SpeedType=0....;Breath - FW effect index 1..[Effect2]..ColorR=255..ColorG=0..ColorB=0..Direction=0..Random=0..Ext1=0..Speed=49..Color2R=8..Color2G=255..Color2 B=240..SpeedType=2..DirectType=0..MusicType=0..CometType=0..StarType=0..TriggerType=0..TemperatureH=0..TemperatureL=0....;Strobing - FW effect index 2.. [Effect3]..ColorR=255..ColorG=0..ColorB=0..Direction=0..Random=0..Ext1=0..Speed=102..Color2R=0..Color2G=0..Color2B=0..SpeedType=2..DirectType=0..Mus icType=0..CometType=0..StarType=0..TriggerType=0..TemperatureH=0..TemperatureL=0....;ColorCycle - FW effect index 4..[Effect4]..ColorR=255..ColorG=0..ColorB=0.. Direction=0..Random=0..Ext1=0..Speed=60..Color2R=0..Color2G=0..Color2B=0..SpeedType=2..DirectType=1..MusicType=0..CometType=0..StarType=0..TriggerType =0..TemperatureH=0..TemperatureL=0....;Rainbow - FW effect index 8..[E

C:\Users\user\AppData\Local\Temp\Distressingly\Bloods\Ultraevangelical\Graviton\Kvle\Materialiseringerne\Antenneanlgget\Invirility.Hus

Process:	C:\Users\user\Desktop\Lakeringernes (1).exe
File Type:	data
Category:	dropped
Size (bytes):	110043
Entropy (8bit):	**7.997895223683267**
Encrypted:	**true**
SSDEEP:	3072:A9H6LIx1K3dZjbPe8NDqL+++gZWYS0gSMr+ZuFYPPBDz:+H6e1OLNp0Wl0gSMr+ZMYPPBDz
MD5:	33CB34530F93B055803F1BD957ACD90F
SHA1:	9E446878DBEAF553AF1E693FB2B36CE2873A0E84
SHA-256:	4C6EAAB6B75A3267FB6FD26D1FF02C92C34391A32038CDCE80A09405E9EFFCBC
SHA-512:	D752959DB8F53A2EB3E5B34D9D4268ADA64E62F9ACA892EE95590367F6C3587E39CE32EDB5A6299E1638DAA56053985A3383B4D433F65DE3A4B9CBB4B6CDE3 66
Malicious:	false
Preview:	..Z.qFL...}..@...&%...7_..>7h..;....2...0.....y..l....f.J.=~."JJ....(*...T.=.....H....T:'..eK[.J.R...>.\=c=]..I..Nq/.*]nd+.~.'V......H.m{e.Z..B.=S...C...Lv9.rYqZ.e....|..G.M.....".xy.6.."... GCj...%...es....R.=.HXU51fH|ygh/.yJ..u..\......gw.....9.FF.t.,..Ln9.....".SgUy..6...%'er..L.|.yZ..f.....Uv..R.Q.R...#.o..{jd....Tj..\'...H.kX@.o.G..D.a...wU..&.A..rmbI:......7....8{.3.I} [.P.z.}..MP;%.)...4q.. .Y.O.0..Z.{....k..........o...=......Q.h.|......F.).i..HHd...7.iQ...y.......m_..dWyp.^p6.....\X..s$..2...Ub.K`.xdb.......m.P*R#.^...Z.....A...7.H..@.I..Q>C.1.Jl.=8..G..... .v...u.A....l...;q..2..C..r=..o.....P.'....d.# I........'.Y.. .pX........uxf...(6v....0..p.$HG_].HK.<J.A......":...|......f..O.mb.%T Ts..VY....Ir...;..A5..)H....A.......pU....._Yg.sQ..B5..d.G..[=.?.&.- ..U."|.8..&A. ......wB.D..J...kG...F4....dft..k".......g.6.'...*...\.......!6..y.....)|E!.l..6tHUb...Tzi/PW...U.p......0..T.<....Mh4.i0..E`..V...Hc.5..{@=.$.e..w

C:\Users\user\AppData\Local\Temp\Distressingly\Bloods\Ultraevangelical\histopathologist.Clo

Process:	C:\Users\user\Desktop\Lakeringernes (1).exe
File Type:	data
Category:	dropped
Size (bytes):	182295
Entropy (8bit):	6.675652521201867
Encrypted:	false
SSDEEP:	3072:H6TfK+T+1UeMXjFAPxIcDKYwgBN0lpwLO/KC:Oq1UeMXjFmCcDn9BNEERC
MD5:	70CA049DF0F109C19B8BA62DD648358B
SHA1:	2436AA216FC507585EAB85740593775C506C5BB0
SHA-256:	8CF9DF942C53ECCF4B4F993A86D0C2B33231533B0D78261561C1C0614BCFCFBF
SHA-512:	85C98BD0C0078D6E876ED1B314E82C141CCC87A17B52F4E79521008D70C435CDCC9B1400120BC675556F97F336689C0761893534F9C4BC6FE94A00F261199791
Malicious:	false
Preview:	RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR RRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR

C:\Users\user\AppData\Local\Temp\Dybfrossen.ini

Process:	C:\Users\user\Desktop\Lakeringernes (1).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.131687083026442

Encrypted:	false
SSDEEP:	3:pDQo7JKU2QYEJry:FQov1YEw
MD5:	09EFF7D465578AB16342D01B9115172C
SHA1:	13311B4DEBC749082CFB1A65DA02759642A9C1D7
SHA-256:	1B5F1F40B8BA4A1F6C314D8C2E1F16D138A70C0D96A3010CF4EC4D44110A443F
SHA-512:	62F99CCB5C6E936A61279DCA2AECB61D6B1B7E3E7E750B0D4C38F10BFE3EE0CE02BC58FA2B87C6784BF60BE0A700BBF179FD8905781E6B0007DE64B8B391685F
Malicious:	false
Preview:	[Decimallngdernes]..Floragrafere=Palms..

C:\Users\user\AppData\Local\Temp\nsbCBD1.tmp\System.dll

Process:	C:\Users\user\Desktop\Lakeringernes (1).exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.770803561213006
Encrypted:	false
SSDEEP:	192:vPtkumJX7zB22kGwfy0mtVgkCPOsE1un:k702k5qpdsEQn
MD5:	2AE993A2FFEC0C137EB51C8832691BCB
SHA1:	98E0B37B7C14890F8A599F35678AF5E9435906E1
SHA-256:	681382F3134DE5C6272A49DD13651C8C201B89C247B471191496E7335702FA59
SHA-512:	2501371EB09C01746119305BA080F3B8C41E64535FF09CEE4F51322530366D0BD5322EA5290A466356598027E6CDA8AB360CAEF62DCAF560D630742E2DD9BCD
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L...tc.W.. .....I.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..... ..`.rdata..S....0....."....@..@.data...h....@.....&.....@....reloc..`....P.....(.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.911285564125606
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Lakeringernes (1).exe
File size:	271824
MD5:	d70de507cc0d22e43ebcf8b61a273ea5
SHA1:	9818fba05573d67b834c90a3208faddea3446545
SHA256:	4dbcd711f2263775f0a1083e0541a07247736ba2fdaabf000654756f8c3dae67
SHA512:	7931df17ea6f9e0fb53b8158fd6f6fbdfcee2cd1aea8252815e0575e0ae993935e60ba6007635d380cb88ea80bbf6b3fb70e2846fc24a04499e84746eb9ee1a0
SSDEEP:	6144:9C2z47aQORdv5crEH4N6KOIH6e1OLNp0Wl0gSMr+ZMYPPBDqN:V47AvKEH4LOI1QlMMcMmM
TLSH:	2944130261E540BBEB811431597BDF75F7BED604541EDA0BB7202FAB3D217928B092AF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... (...F...F...F.*.....F...G.v.F.*.....F...v...F...@...F.Rich..F.....PE..L...c.W.....^.....

File Icon

Icon Hash:	f89ab6b68aa686ec

Static PE Info

General

Entrypoint:	0x4030d9
Entrypoint Section:	.text

Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5795638D [Mon Jul 25 00:55:41 2016 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:	b78ecf47c0a3e24a6f4af114e2d1f5de

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	OU="Sinicising Mohel Cop ", E=Trolovelse@Baadeplads.Dro, O=Idealets, L=Le Lauzet-Ubaye, S=Provence-Alpes-C\xf4te d'Azur, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 31/08/2022 18:52:55 30/08/2025 18:52:55
Subject Chain	• OU="Sinicising Mohel Cop ", E=Trolovelse@Baadeplads.Dro, O=Idealets, L=Le Lauzet-Ubaye, S=Provence-Alpes-C\xf4te d'Azur, C=FR
Version:	3
Thumbprint MD5:	32EBC12D71851D6198230D6A1E168F70
Thumbprint SHA-1:	5EB24F3DE7AD72BFA75BD170B307BC244FCC6E7C
Thumbprint SHA-256:	53B3B15BAA3306845DB3E5F5C435F70EC5CF893D1AEDBFC8424271734971B2CE
Serial:	52A9116BDA7A62BC

Entrypoint Preview
Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004070A8h]
call dword ptr [004070A4h]
cmp ax, 00000006h
je 00007F6CF850DAC3h
push ebx
call 00007F6CF8510A31h
cmp eax, ebx
je 00007F6CF850DAB9h
push 00000C00h
call eax
mov esi, 00407298h
push esi
call 00007F6CF85109ADh
push esi
call dword ptr [004070A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F6CF850DA9Dh
push ebp

Instruction
push 00000009h
call 00007F6CF8510A04h
push 00000007h
call 00007F6CF85109FDh
mov dword ptr [00423704h], eax
call dword ptr [00407044h]
push ebx
call dword ptr [00407288h]
mov dword ptr [004237B8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041ECC8h
call dword ptr [00407174h]
push 00409188h
push 00422F00h
call 00007F6CF8510627h
call dword ptr [0040709Ch]
mov ebp, 00429000h
push eax
push ebp
call 00007F6CF8510615h
push ebx
call dword ptr [00407154h]

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7428	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x16a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x40698	0x1f38	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x298	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5c5b	0x5e00	False	0.6603640292553191	data	6.411456379497882	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1246	0x1400	False	0.42734375	data	5.005029341587408	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1a7f8	0x400	False	0.6376953125	data	5.108396988130901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x24000	0x17000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0x16a8	0x1800	False	0.3681640625	data	4.643642871246492	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x3b238	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x3b5a0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1152, 256 important colors	English	United States
RT_DIALOG	0x3be48	0x144	data	English	United States
RT_DIALOG	0x3bf90	0x13c	data	English	United States
RT_DIALOG	0x3c0d0	0x100	data	English	United States
RT_DIALOG	0x3c1d0	0x11c	data	English	United States
RT_DIALOG	0x3c2f0	0x60	data	English	United States
RT_GROUP_ICON	0x3c350	0x14	data	English	United States
RT_MANIFEST	0x3c368	0x33d	XML 1.0 document, ASCII text, with very long lines (829), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableA, Sleep, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, GetFileAttributesA, SetFileAttributesA, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, lstrlenA, GetVersion, SetErrorMode, lstrcpynA, ExitProcess, GetFullPathNameA, GlobalLock, CreateThread, GetLastError, CreateDirectoryA, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, ReadFile, WriteFile, lstrcpyA, MoveFileExA, lstrcatA, GetSystemDirectoryA, GetProcAddress, CloseHandle, SetCurrentDirectoryA, MoveFileA, CompareFileTime, GetShortPathNameA, SearchPathA, lstrcmpiA, SetFileTime, lstrcmpA, ExpandEnvironmentStringsA, GlobalUnlock, GetDiskFreeSpaceA, GlobalFree, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, GetPrivateProfileStringA, FindClose, MultiByteToWideChar, FreeLibrary, MulDiv, WritePrivateProfileStringA, LoadLibraryExA, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, GlobalAlloc
USER32.dll	ScreenToClient, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, PostQuitMessage, GetWindowRect, EnableMenuItem, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndDialog, RegisterClassA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, GetDC, CreateDialogParamA, SetTimer, GetDlgItem, SetWindowLongA, SetForegroundWindow, LoadImageA, IsWindow, SendMessageTimeoutA, FindWindowExA, OpenClipboard, TrackPopupMenu, AppendMenuA, EndPaint, DestroyWindow, wsprintfA, ShowWindow, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegDeleteKeyA, SetFileSecurityA, OpenProcessToken, LookupPrivilegeValueA, AdjustTokenPrivileges, RegOpenKeyExA, RegEnumValueA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	OleUninitialize, OleInitialize, CoTaskMemFree, CoCreateInstance

Possible Origin

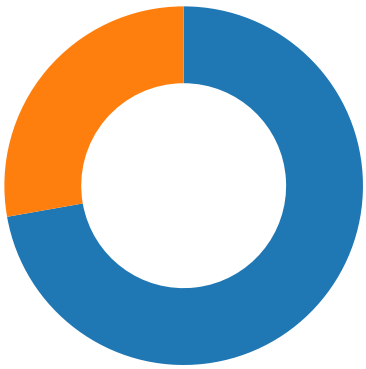
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.2066.29.151.4049856802031453 11/28/22-10:24:42.586053	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49856	80	192.168.11.20	66.29.151.40
192.168.11.2050.87.192.14449908802031453 11/28/22-10:27:29.159793	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49908	80	192.168.11.20	50.87.192.144
192.168.11.2050.87.192.14449845802031453 11/28/22-10:22:54.782392	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.11.20	50.87.192.144
192.168.11.2050.87.192.14449845802031412 11/28/22-10:22:54.782392	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.11.20	50.87.192.144
192.168.11.2066.29.151.4049856802031449 11/28/22-10:24:42.586053	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49856	80	192.168.11.20	66.29.151.40
192.168.11.2050.87.192.14449908802031412 11/28/22-10:27:29.159793	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49908	80	192.168.11.20	50.87.192.144
192.168.11.2050.87.192.14449845802031449 11/28/22-10:22:54.782392	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49845	80	192.168.11.20	50.87.192.144
192.168.11.2066.29.151.4049856802031412 11/28/22-10:24:42.586053	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49856	80	192.168.11.20	66.29.151.40
192.168.11.2050.87.192.14449908802031449 11/28/22-10:27:29.159793	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49908	80	192.168.11.20	50.87.192.144

Network Port Distribution



Total Packets: 72

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 10:20:22.837178946 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:22.837198019 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:22.837399006 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:22.850811005 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:22.850825071 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:22.889564991 CET	443	49809	142.250.184.206	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 10:20:22.889770985 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:22.889770985 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:22.890341043 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:22.890531063 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.020267010 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.020282030 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.020570040 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.020772934 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.025866032 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.068310022 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.333216906 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.333414078 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.333479881 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.333513021 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.333667994 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.335042953 CET	49809	443	192.168.11.20	142.250.184.206
Nov 28, 2022 10:20:23.335093975 CET	443	49809	142.250.184.206	192.168.11.20
Nov 28, 2022 10:20:23.471163034 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.471214056 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.471366882 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.471688986 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.471725941 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.531626940 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.531991959 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.533205032 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.533564091 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.537095070 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.537133932 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.537735939 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.537959099 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.538317919 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.580493927 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.867253065 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.867516994 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.867578030 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.867624998 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.867750883 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.867805958 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.867836952 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.868011951 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.869055986 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.869261980 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.869261980 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.869261980 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.869887114 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.870115995 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.870177984 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.870332003 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.870428085 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.870486021 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.870520115 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.870759964 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.871031046 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.871268034 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.877662897 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.877953053 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.878017902 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.878277063 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.878334999 CET	443	49811	142.250.185.161	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 10:20:23.878570080 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.878602028 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.878664017 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.878787994 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.878914118 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.878968954 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.879158974 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.879244089 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.879301071 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.879336119 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.879565001 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.879832983 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.880045891 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.880100012 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.880245924 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.880683899 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.880899906 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.880958080 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.881181955 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.881253958 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.881486893 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.881541014 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.881825924 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.882081032 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.882286072 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.882343054 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.882556915 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.882639885 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.882827997 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.882863998 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.883079052 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.883395910 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.883609056 CET	49811	443	192.168.11.20	142.250.185.161
Nov 28, 2022 10:20:23.883666992 CET	443	49811	142.250.185.161	192.168.11.20
Nov 28, 2022 10:20:23.883855104 CET	49811	443	192.168.11.20	142.250.185.161

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 10:20:22.819396019 CET	49847	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:20:22.828677893 CET	53	49847	1.1.1.1	192.168.11.20
Nov 28, 2022 10:20:23.429255962 CET	57628	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:20:23.469788074 CET	53	57628	1.1.1.1	192.168.11.20
Nov 28, 2022 10:21:36.033036947 CET	58041	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:21:36.069412947 CET	53	58041	1.1.1.1	192.168.11.20
Nov 28, 2022 10:21:51.137625933 CET	65114	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:21:51.544015884 CET	53	65114	1.1.1.1	192.168.11.20
Nov 28, 2022 10:22:03.915235043 CET	60099	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:22:03.969881058 CET	53	60099	1.1.1.1	192.168.11.20
Nov 28, 2022 10:22:12.022314072 CET	62390	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:22:12.665165901 CET	53	62390	1.1.1.1	192.168.11.20
Nov 28, 2022 10:22:24.550700903 CET	51341	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:22:24.578022957 CET	53	51341	1.1.1.1	192.168.11.20
Nov 28, 2022 10:22:35.924315929 CET	53024	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:22:35.961610079 CET	53	53024	1.1.1.1	192.168.11.20
Nov 28, 2022 10:22:47.655605078 CET	50276	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:22:48.065530062 CET	53	50276	1.1.1.1	192.168.11.20
Nov 28, 2022 10:23:00.465042114 CET	55900	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:23:00.487232924 CET	53	55900	1.1.1.1	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 10:24:29.437565088 CET	52252	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:24:29.466507912 CET	53	52252	1.1.1.1	192.168.11.20
Nov 28, 2022 10:24:35.850496054 CET	61265	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:24:35.872613907 CET	53	61265	1.1.1.1	192.168.11.20
Nov 28, 2022 10:24:47.878958941 CET	65009	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:24:48.054725885 CET	53	65009	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:00.407924891 CET	59012	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:00.473953009 CET	53	59012	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:12.342963934 CET	55130	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:12.751357079 CET	53	55130	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:25.074199915 CET	54809	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:25.490206957 CET	53	54809	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:38.055902958 CET	57486	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:38.068944931 CET	53	57486	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:46.116976976 CET	49742	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:46.335736990 CET	53	49742	1.1.1.1	192.168.11.20
Nov 28, 2022 10:25:58.410665035 CET	52605	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:25:58.855298042 CET	53	52605	1.1.1.1	192.168.11.20
Nov 28, 2022 10:26:39.666815042 CET	60882	53	192.168.11.20	1.1.1.1
Nov 28, 2022 10:26:39.808270931 CET	53	60882	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2022 10:20:22.819396019 CET	192.168.11.20	1.1.1.1	0xedb2	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:20:23.429255962 CET	192.168.11.20	1.1.1.1	0xce7c	Standard query (0)	doc-00-7s-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:21:36.033036947 CET	192.168.11.20	1.1.1.1	0xc7dd	Standard query (0)	www.avatarworker.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:21:51.137625933 CET	192.168.11.20	1.1.1.1	0x94de	Standard query (0)	www.005404.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:03.915235043 CET	192.168.11.20	1.1.1.1	0xb374	Standard query (0)	www.sabzi.lol	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:12.022314072 CET	192.168.11.20	1.1.1.1	0xfe8d	Standard query (0)	www.automotiveparts-store.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:24.550700903 CET	192.168.11.20	1.1.1.1	0x11ff	Standard query (0)	www.aceadora.shop	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:35.924315929 CET	192.168.11.20	1.1.1.1	0x10f3	Standard query (0)	www.haveusstampsale.shop	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:47.655605078 CET	192.168.11.20	1.1.1.1	0xa4c	Standard query (0)	www.xn--29-oj9ik7b890b.net	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:23:00.465042114 CET	192.168.11.20	1.1.1.1	0x70d4	Standard query (0)	www.plentywindshield.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:29.437565088 CET	192.168.11.20	1.1.1.1	0x27a	Standard query (0)	www.plentywindshield.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:35.850496054 CET	192.168.11.20	1.1.1.1	0x320e	Standard query (0)	www.gouldent.site	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:47.878958941 CET	192.168.11.20	1.1.1.1	0x906d	Standard query (0)	www.rsvstudio.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:00.407924891 CET	192.168.11.20	1.1.1.1	0x1e2d	Standard query (0)	www.techrocker.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:12.342963934 CET	192.168.11.20	1.1.1.1	0x1c50	Standard query (0)	www.youlian.fund	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:25.074199915 CET	192.168.11.20	1.1.1.1	0xeba7	Standard query (0)	www.mangal20.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:38.055902958 CET	192.168.11.20	1.1.1.1	0x556a	Standard query (0)	www.caglaakdag.xyz	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:46.116976976 CET	192.168.11.20	1.1.1.1	0x8af6	Standard query (0)	www.livinghopedoula.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:58.410665035 CET	192.168.11.20	1.1.1.1	0x4f50	Standard query (0)	www.planetthermo.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2022 10:26:39.666815042 CET	192.168.11.20	1.1.1.1	0x73ad	Standard query (0)	www.sabzi.lol	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 10:20:22.828677893 CET	1.1.1.1	192.168.11.20	0xedb2	No error (0)	drive.google.com		142.250.184.206	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:20:23.469788074 CET	1.1.1.1	192.168.11.20	0xce7c	No error (0)	doc-00-7s-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 10:20:23.469788074 CET	1.1.1.1	192.168.11.20	0xce7c	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.161	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:21:36.069412947 CET	1.1.1.1	192.168.11.20	0xc7dd	No error (0)	www.avatarworker.com		3.64.163.50	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:21:51.544015884 CET	1.1.1.1	192.168.11.20	0x94de	No error (0)	www.005404.com		103.63.2.175	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:03.969881058 CET	1.1.1.1	192.168.11.20	0xb374	Name error (3)	www.sabzi.lol	none	none	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:12.665165901 CET	1.1.1.1	192.168.11.20	0xfe8d	No error (0)	www.automotiveparts-store.com	automotivepartss-store.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 10:22:12.665165901 CET	1.1.1.1	192.168.11.20	0xfe8d	No error (0)	automotiveparts-store.com		162.0.238.93	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:24.578022957 CET	1.1.1.1	192.168.11.20	0x11ff	No error (0)	www.aceadora.shop		104.21.23.41	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:24.578022957 CET	1.1.1.1	192.168.11.20	0x11ff	No error (0)	www.aceadora.shop		172.67.208.207	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:35.961610079 CET	1.1.1.1	192.168.11.20	0x10f3	No error (0)	www.haveusstampsale.shop		104.21.48.6	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:35.961610079 CET	1.1.1.1	192.168.11.20	0x10f3	No error (0)	www.haveusstampsale.shop		172.67.175.40	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:22:48.065530062 CET	1.1.1.1	192.168.11.20	0xa4c	No error (0)	www.xn--29-oj9ik7b890b.net	xn--29-oj9ik7b890b.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 10:22:48.065530062 CET	1.1.1.1	192.168.11.20	0xa4c	No error (0)	xn--29-oj9ik7b890b.net		50.87.192.144	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:23:00.487232924 CET	1.1.1.1	192.168.11.20	0x70d4	No error (0)	www.plentywindshield.com		96.43.100.185	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:29.466507912 CET	1.1.1.1	192.168.11.20	0x27a	No error (0)	www.plentywindshield.com		96.43.100.185	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:35.872613907 CET	1.1.1.1	192.168.11.20	0x320e	No error (0)	www.gouldent.site		66.29.151.40	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:24:48.054725885 CET	1.1.1.1	192.168.11.20	0x906d	No error (0)	www.rsvstudio.com		156.254.172.36	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:00.473953009 CET	1.1.1.1	192.168.11.20	0x1e2d	No error (0)	www.techrocker.com	techrocker.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 10:25:00.473953009 CET	1.1.1.1	192.168.11.20	0x1e2d	No error (0)	techrocker.com		23.106.120.176	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:12.751357079 CET	1.1.1.1	192.168.11.20	0x1c50	No error (0)	www.youlian.fund		154.204.24.45	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:25.490206957 CET	1.1.1.1	192.168.11.20	0xeba7	No error (0)	www.mangal20.com		156.230.149.244	A (IP address)	IN (0x0001)	false

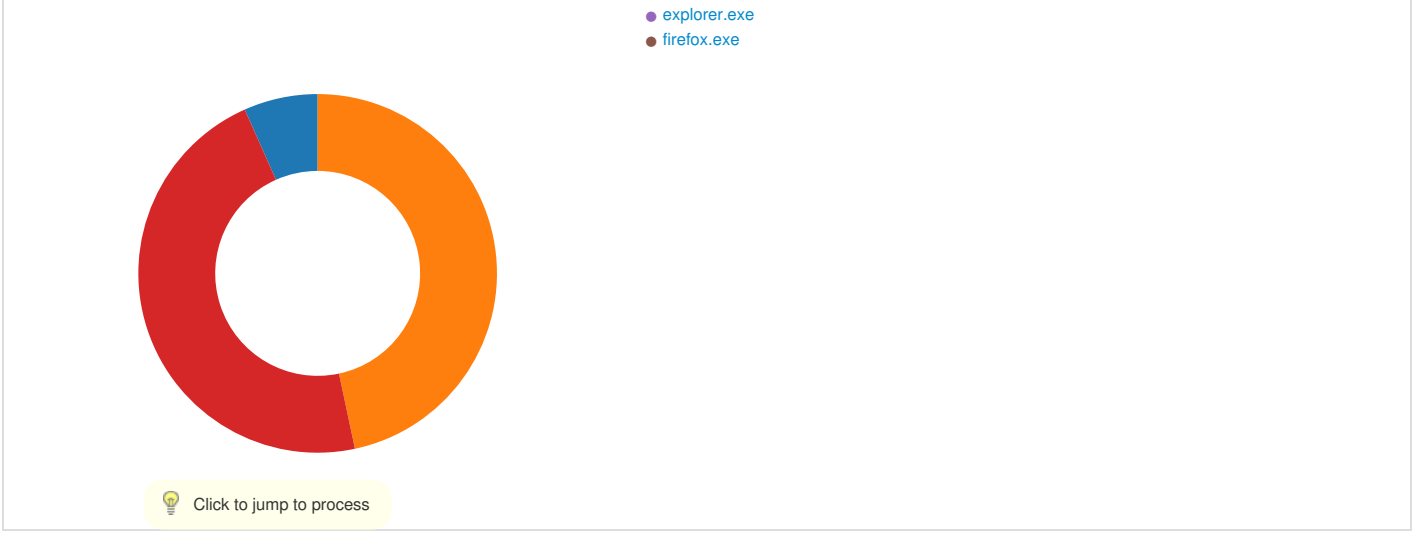
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 10:25:38.068944931 CET	1.1.1.1	192.168.11.20	0x556a	Name error (3)	www.caglaakdag.xyz	none	none	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:46.335736990 CET	1.1.1.1	192.168.11.20	0x8af6	No error (0)	www.livinghopedoula.com		168.76.162.220	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:25:58.855298042 CET	1.1.1.1	192.168.11.20	0x4f50	No error (0)	www.planetthermo.net		154.213.44.213	A (IP address)	IN (0x0001)	false
Nov 28, 2022 10:26:39.808270931 CET	1.1.1.1	192.168.11.20	0x73ad	Name error (3)	www.sabzi.lol	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-00-7s-docs.googleusercontent.com
- www.avatarworker.com
- www.005404.com
- www.automotiveparts-store.com
- www.aceadora.shop
- www.haveusstampsale.shop
- www.xn--29-oj9ik7b890b.net
- www.gouldent.site
- www.rsvstudio.com
- www.techrocker.com
- www.youlian.fund
- www.mangal20.com
- www.livinghopedoula.com
- www.planetthermo.net

Statistics

Behavior



System Behavior

Analysis Process: Lakeringernes (1).exe PID: 2508, Parent PID: 4684

General

Target ID:	2
Start time:	10:19:38
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\Lakeringernes (1).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Lakeringernes (1).exe
Imagebase:	0x400000
File size:	271824 bytes
MD5 hash:	D70DE507CC0D22E43EBCF8B61A273EA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.2211562362.00000000032B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_3, Description: Yara detected GuLoader, Source: 00000002.00000002.2210407570.0000000000624000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Lakeringernes (1).exe PID: 384, Parent PID: 2508

General

Target ID:	6
Start time:	10:20:02
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\Lakeringernes (1).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Lakeringernes (1).exe

Imagebase:	0x400000
File size:	271824 bytes
MD5 hash:	D70DE507CC0D22E43EBCF8B61A273EA5
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: 00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.2316669409.000000001D4A0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2297348771.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2297348771.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2297348771.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.2297348771.0000000000060000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000000.1983965227.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	168348D	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41DF7E	NtReadFile

Analysis Process: RAVCpl64.exe PID: 7704, Parent PID: 384

General	
Target ID:	8
Start time:	10:20:28
Start date:	28/11/2022
Path:	C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
Imagebase:	0x140000000
File size:	16696840 bytes
MD5 hash:	731FB4B2E5AFBCADAABB80D642E056AC
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: 00000008.00000000.2252030385.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.2252030385.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.2252030385.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000000.2252030385.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.2257617609.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.2257617609.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.2257617609.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000000.2257617609.0000000000511000.00000040.00000001.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

Analysis Process: wscript.exe PID: **3316**, Parent PID: **7704**

General	
Target ID:	9
Start time:	10:20:30
Start date:	28/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xec0000
File size:	147456 bytes
MD5 hash:	4D780D8F77047EE1C65F747D9F63A1FE
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: 00000009.00000002.6797344913.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.6797344913.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.6797344913.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.6797344913.0000000000C70000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.6788894111.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.6788894111.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.6788894111.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.6788894111.0000000000600000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.6797910389.0000000000CA0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.6797910389.0000000000CA0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.6797910389.0000000000CA0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.6797910389.0000000000CA0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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\Lakeringernes (1).exe	cannot delete	1	61C877	NtDeleteFile
C:\Users\user\AppData\Local\Temp\752cuCH8	object name not found	1	61C877	NtDeleteFile
C:\Users\user\AppData\Local\Temp\752cuCH8	sharing violation	1	61C877	NtDeleteFile
C:\Users\user\AppData\Local\Temp\752cuCH8	sharing violation	1	61C877	NtDeleteFile
C:\Users\user\AppData\Local\Temp\752cuCH8	sharing violation	1	61C877	NtDeleteFile
C:\Users\user\AppData\Local\Temp\752cuCH8	sharing violation	1	61C877	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	1696752	success or wait	1	61C847	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **4684**, Parent PID: **3316**

General

Target ID:	10
Start time:	10:20:52
Start date:	28/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff7be790000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: firefox.exe PID: **1716**, Parent PID: **3316**

General

Target ID:	12
Start time:	10:21:39
Start date:	28/11/2022
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Mozilla Firefox\Firefox.exe
Imagebase:	0x7ff71dcc0000
File size:	597432 bytes
MD5 hash:	FA9F4FC5D7ECAB5A20BF7A9D1251C851
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly