ID: 1550253
Sample Name:
Anfrage_244384.exe
Cookbook: default.jbs
Time: 16:09:43
Date: 06/11/2024
Version: 41.0.0 Charoite

Table of Contents

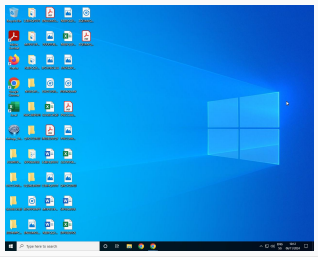
Windows Analysis Report

Anfrage_244384.exe

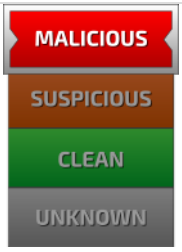
Overview

General Information

Sample name:	Anfrage_244384.exe
Analysis ID:	1550253
MD5:	b03f23199ae98..
SHA1:	f454c8de72926..
SHA256:	eda014e3b658...
Tags:	exe user-threatcat_ch
Infos:	



Detection



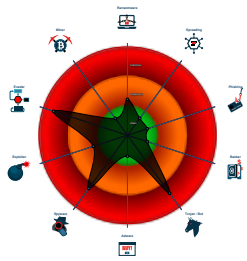
FormBook, GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected FormBook
- Yara detected GuLoader
- AI detected suspicious sample
- Found direct / indirect Syscall (likely…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Switches to a custom stack to bypa…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fi…

Classification



Process Tree

- **System is w10x64**
- Anfrage_244384.exe (PID: 5308 cmdline: "C:\Users\user\Desktop\Anfrage_244384.exe" MD5: B03F23199AE987A7BCE0FF1A0D742E3E)
  - Anfrage_244384.exe (PID: 5608 cmdline: "C:\Users\user\Desktop\Anfrage_244384.exe" MD5: B03F23199AE987A7BCE0FF1A0D742E3E)
    - dptLotHBnXg.exe (PID: 3052 cmdline: "C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLlVOlVfQTf\dptLotHBnXg.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
      - verclsid.exe (PID: 1056 cmdline: "C:\Windows\SysWOW64\verclsid.exe" MD5: 190A347DF06F8486F193ADA0E90B49C5)
        - dptLotHBnXg.exe (PID: 3916 cmdline: "C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLlVOlVfQTf\dptLotHBnXg.exe" MD5: 32B8AD6ECA9094891E792631BAEA9717)
        - firefox.exe (PID: 1832 cmdline: "C:\Program Files\Mozilla Firefox\Firefox.exe" MD5: C86B1BE9ED6496FE0E0CBE73F81D8045)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://0xmrmagnezi.github.io/malware%20analysis/FormBook/https://any.run/cybersecurity-blog/xloader-formbook-encryption-analysis-and-malware-decryption/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africahttps://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://any.run/cybersecurity-blog/deobfuscating-guloader/https://asec.ahnlab.com/en/55978/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.3362363415.0000000000960000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000007.00000002.3361086022.00000000003B0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000007.00000002.3362535904.00000000009B0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.3361838593.00000000007B0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000004.00000002.3122242151.0000000034330000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Suricata Signatures

ET EXPLOIT Possible CVE-2016-2211 Symantec Cab Parsing Buffer Overflow

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-11-06T16:10:51.193850+0100	2022930	1	A Network Trojan was detected	52.149.20.212	443	192.168.2.6	49753	TCP
2024-11-06T16:11:29.888003+0100	2022930	1	A Network Trojan was detected	52.149.20.212	443	192.168.2.6	49926	TCP

ETPRO MALWARE Common Downloader Header Pattern UHCa

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-11-06T16:11:29.973578+0100	2803270	2	Potentially Bad Traffic	192.168.2.6	49927	188.40.95.144	443	TCP

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Yara detected FormBook

AI detected suspicious sample

E-Banking Fraud

Yara detected FormBook

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Switches to a custom stack to bypass stack traces

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Found direct / indirect Syscall (likely to bypass EDR)

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

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

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

Remote Access Functionality

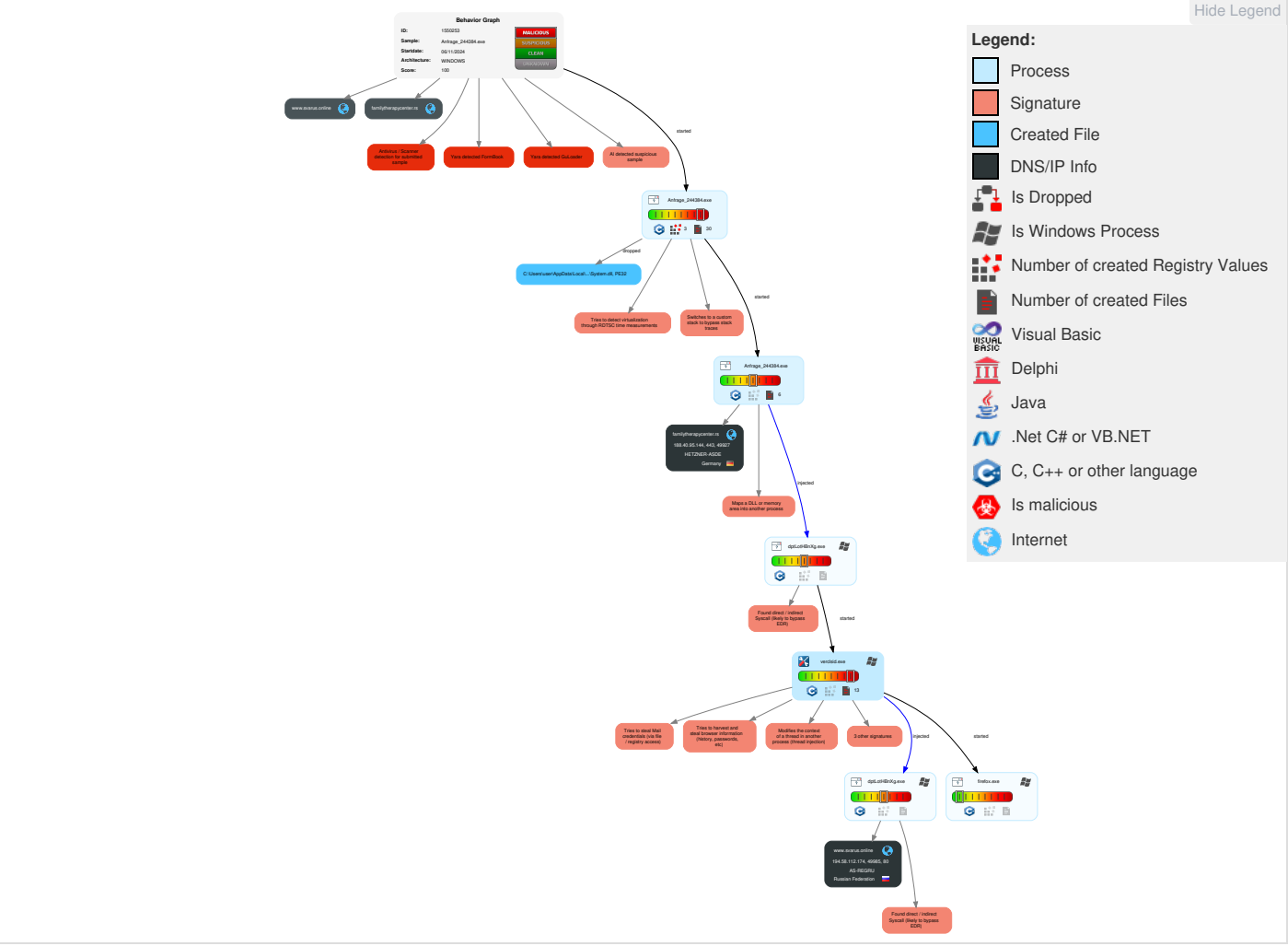
Yara detected FormBook

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 1 Masquerading	1 OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Email Collection	1 1 Encrypted Channel	Exfiltration Over Other Network Medium	1 System Shutdown/Reboot

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Credentials	Domains	Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	3 1 2 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	3 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 Abuse Elevation Control Mechanism	1 Access Token Manipulation	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Data from Local System	3 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	1 DLL Side-Loading	3 1 2 Process Injection	NTDS	2 File and Directory Discovery	Distributed Component Object Model	1 Clipboard Data	4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 4 System Information Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 Abuse Elevation Control Mechanism	Cached Domain Credentials	Wi-Fi Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Remote System Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

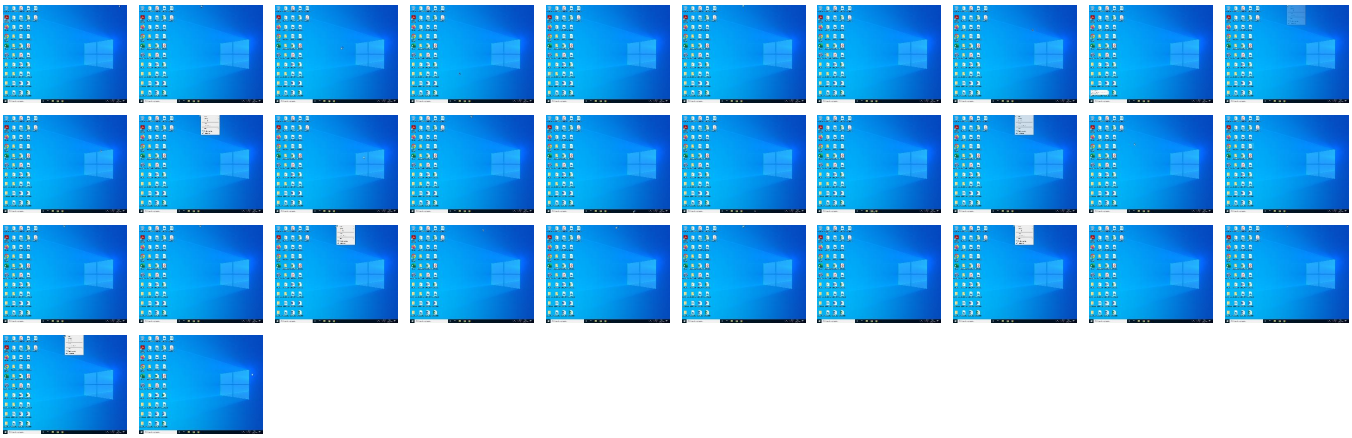
Behavior Graph



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
Anfrage_244384.exe	11%	ReversingLabs	Win32.Trojan.InjectorX	
Anfrage_244384.exe	100%	Avira	HEUR/AGEN.1361137	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsgA6C3.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://familytherapycenter.rs/	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.bins	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.bin2	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.bink	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.bin	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.binl	0%	Avira URL Cloud	safe	
http://https://familytherapycenter.rs/LxuQG254.binA	0%	Avira URL Cloud	safe	
http://https://parking.reg.ru/script/get_domain_data?domain_name=www.svarus.online&rand=	0%	Avira URL Cloud	safe	
http://www.svarus.online/sa87/?LJ=0zbXYrx&6X64=UqcT3NX6Xc6Oa5c5HtJN6Sm3jRGrdUDSppl2CYCGZerglEzU6CQj7u00+cYUshbCTVWQ/5Gc6Lshk9bP6yg8AmPqwLiPHc0f1bybms24K+7m7zNAaNQIZa1j2XstdwJ+GTV4HpA=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
familytherapycenter.rs	188.40.95.144	true	false		high
www.svarus.online	194.58.112.174	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://familytherapycenter.rs/LxuQG254.bin	false	• Avira URL Cloud: safe	unknown
http://www.svarus.online/sa87/?LJ=0zbXYrx&6X64=UqcT3NX6Xc6Oa5c5HtJN6Sm3jRGrdUDSppl2CYCGZerglEzU6CQj7u00+cYUshbCTVWQ/5Gc6Lshk9bP6yg8AmPqwLiPHc0f1bybms24K+7m7zNAaNQIZa1j2XstdwJ+GTV4HpA=	false	• Avira URL Cloud: safe	unknown

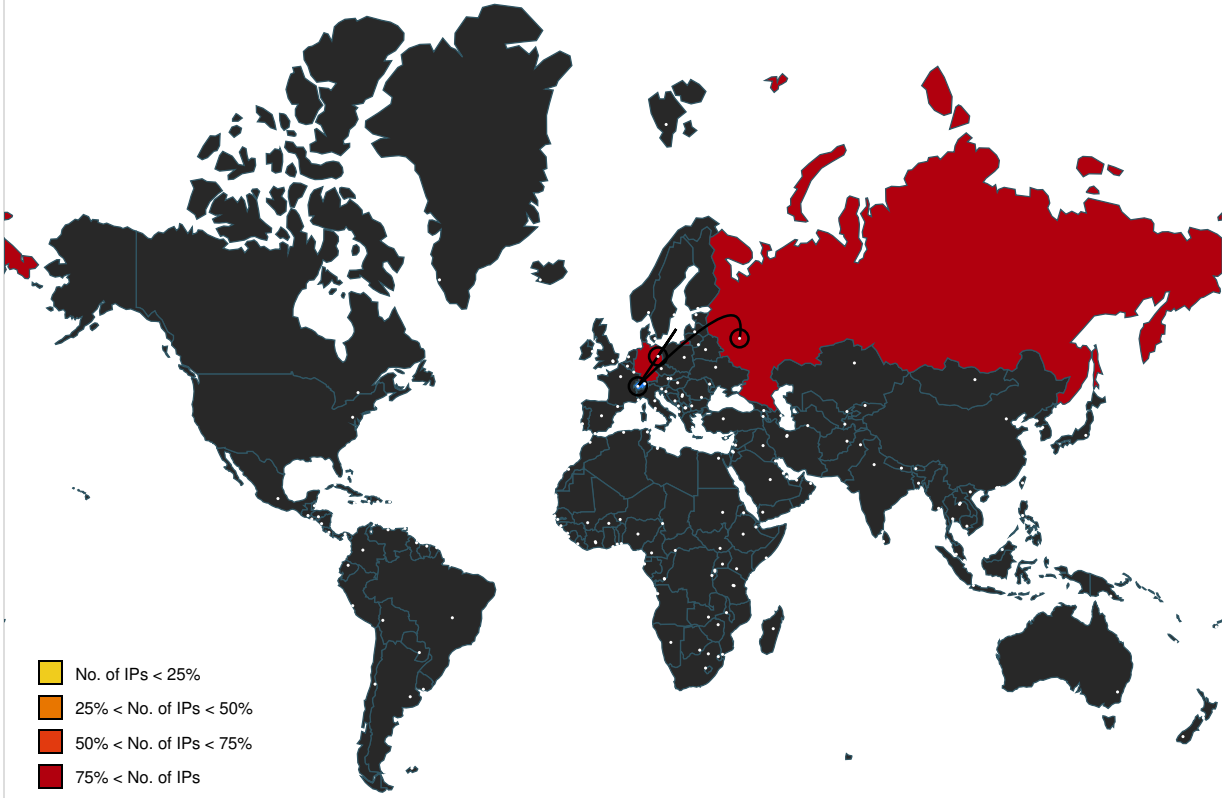
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	verclsid.exe, 00000007.00000002.3365232559.00000000076E8000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	verclsid.exe, 00000007.00000002.3365232559.00000000076E8000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://reg.ru	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://familytherapycenter.rs/	Anfrage_244384.exe, 00000004.00000002.30 92148007.00000000043B3000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.reg.ru/dedicated/?utm_source=www.svarus.online&utm_medium=parking&utm_campaign=s_land_se	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.reg.ru/domain/new/?utm_source=www.svarus.online&utm_medium=parking&utm_campaign=s_land_n	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://www.ftp.ftp://ftp.gopher.	Anfrage_244384.exe, 00000004.00000001.25 96303421.0000000000649000.00000020.00000 001.01000000.00000007.sdmp	false		high
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://familytherapycenter.rs/LxuQG254.bin2	Anfrage_244384.exe, 00000004.00000002.30 92148007.0000000004378000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://familytherapycenter.rs/LxuQG254.bins	Anfrage_244384.exe, 00000004.00000002.30 92148007.00000000043B3000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	Anfrage_244384.exe	false		high
http://https://help.reg.ru/support/ssl-sertifikaty/1-etap-zakaz-ssl-sertifikata/kak-zakazat-besplatnyy-ssl-	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://www.ecosia.org/newtab/	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://www.reg.ru/whois/?check=&dname=www.svarus.online&reg_source=parking_auto	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://familytherapycenter.rs/LxuQG254.bink	Anfrage_244384.exe, 00000004.00000002.30 92148007.00000000043B3000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://familytherapycenter.rs/LxuQG254.binl	Anfrage_244384.exe, 00000004.00000002.30 92148007.0000000004378000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://familytherapycenter.rs/LxuQG254.binA	Anfrage_244384.exe, 00000004.00000002.30 92148007.00000000043B3000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	Anfrage_244384.exe, 00000004.00000001.25 96303421.00000000005F2000.00000020.00000 001.01000000.00000007.sdmp	false		high
http://nsis.sf.net/NSIS_Error	Anfrage_244384.exe	false		high
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://parking.reg.ru/script/get_domain_data?domain_name=www.svarus.online&rand=	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	Anfrage_244384.exe, 00000004.00000001.25 96303421.0000000000649000.00000020.00000 001.01000000.00000007.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.reg.ru/sozdanie-saita/	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	Anfrage_244384.exe, 00000004.00000001.25 96303421.00000000005F2000.00000020.00000 001.01000000.00000007.sdmp	false		high
http://https://www.reg.ru/hosting/?utm_source=www.svarus.online&utm_medium=parking&utm_campaign=s_land_host	verclsid.exe, 00000007.00000002.33634142 48.0000000005024000.00000004.10000000.00 040000.00000000.sdmp, dptLotHBnXg.exe, 0 0000008.00000002.3362833809.0000000002A9 4000.00000004.00000001.00040000.00000000.sdmp	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	verclsid.exe, 00000007.00000002.33652325 59.00000000076E8000.00000004.00000020.00 020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.40.95.144	familytherapycenter.rs	Germany		24940	HETZNER-ASDE	false
194.58.112.174	www.svarus.online	Russian Federation		197695	AS-REGRU	false

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1550253
Start date and time:	2024-11-06 16:09:43 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 9m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01

Number of analysed new started processes analysed:	9
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	Anfrage_244384.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/11@2/2
EGA Information:	• Successful, ratio: 75%
HCA Information:	• Successful, ratio: 85% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, ocsp.digicert.com, otelrules.azureedge.net, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- VT rate limit hit for: Anfrage_244384.exe

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\02-E8420l

Process:	C:\Windows\SysWOW64\verclsid.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x37, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1239949490932863
Encrypted:	false
SSDEEP:	384:g2qOB1nxCkvSA1LyKOMq+8iP5GDHP/0j:9q+n0E91LyKOMq+8iP5GLP/0
MD5:	271D5F995996735B01672CF227C81C17
SHA1:	7AEAACD66A59314D1CBF4016038D3A0A956BAF33
SHA-256:	9D772D093F99F296CD906B7B5483A41573E1C6BD4C91EF8DBACDA79CDF1436B4
SHA-512:	62F15B7636222CA89796FCC23FC5722657382FAAAFEDC937506CAB3286AA696609F2A5A8F479158574D9FB92D37C0AA74EA15F7A172EBF1F3D260EF6124CF8B
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....Y.....7.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\nsgA6C3.tmp\System.dll

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.7711167426271945
Encrypted:	false
SSDEEP:	192:OPtkumJX7zB22kGwfy0mtVgkCPOsX1un:/702k5qpdsXQn
MD5:	3F176D1EE13B0D7D6BD92E1C7A0B9BAE
SHA1:	FE582246792774C2C9DD15639FFA0ACA90D6FD0B
SHA-256:	FA4AB1D6F79FD677433A31ADA7806373A789D34328DA46CCB0449BBF347BD73E
SHA-512:	0A69124819B7568D0DEA4E9E85CE8FE61C7BA697C934E3A95E2DCFB9F252B1D9DA7FAF8774B6E8EFD614885507ACC94987733EBA09A2F5E7098B774DFC8524B6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L.....MX.. .....!.....'.....0.....`.....2.....0..P.....P.....0..X.....text...O..... ..`.rdata..S....0....."....@..@.data...h....@.....&.....@....reloc..`....P.....(.....@..B..... .....

C:\Users\user\AppData\Roaming\secretaryships\Angoragedernes\nilgedde.mes

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	Matlab v4 mat-file (little endian) Y, numeric, rows 0, columns 0
Category:	dropped
Size (bytes):	354845
Entropy (8bit):	1.2446363869824946
Encrypted:	false
SSDEEP:	768:E2oz5FNvncy2DZRau7W0sxOvPfSfpg5rWuWAAUldde/FwPPMk/FOuyQv9biuPia6:opho02mYrKiKLFyJ1AIu2
MD5:	DF7A44909B03AB5BC45910B405D9977A
SHA1:	3D0583A7DFB39E559827189E02123F2C983A21D5
SHA-256:	5A3B61A0BC8E81E756374D2A9FF5087FA4496543A635738ACA8911E95D6340D9
SHA-512:	C2B4E951A185FC3FB75109B5CAA554431C1517588D04B8F2BA865F75BE448A0448364BCB84253C9B44579078787DDA616F33666C0C1BF902EC644EBC9A6FE62
Malicious:	false
Reputation:	low
Preview:	.....%.Y.....[.....z.....8.....{.....b.....W.....#.....%.... z.....7.....x.i...+.....8.....- ..3.....|.....T.....#.....\.....A.....7.....'..... .....]..... .J.J.....s.....g.....W.....$...g.....

C:\Users\user\AppData\Roaming\secretaryships\Angoragedernes\selefant.kri

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	298017
Entropy (8bit):	1.245520550165085
Encrypted:	false
SSDEEP:	768:nLoDoRi0SWvTrmnVqvh6dzfCaci65UhXqjMctTGA3QBgdRWqrw3q3LFPRvx7H155:DStBsLk6gsifeQIGA0iYRwvy8n
MD5:	B4C9FC75BAB8C9F006A7D9DDBC249F79
SHA1:	70D4047E7E3BB10CF237B82775C89A1D92700162
SHA-256:	1D84F9462C244A4500C213DF8DD79971B286392CA02BC536F5F6C3EEBC94E7E3
SHA-512:	2E2279CB3755AC5708ABB30E8342235B7F0A24223E3D6F4B2B21B62E59012A5126ADC1BD73D7B64E72634728DECCE7A049D3E6F5055F8D74E959BEE54EDBEA4C
Malicious:	false
Preview:	....._.,.....;.....7...O.....'.....P.....L.....@..... ....8.....v.....G.....h.....m..+b.....m.....C.....i..... .....,.....C.....a.....Y.....,.....q..... .....p.....S.....L.....).....kF.....^.....E.....

C:\Users\user\AppData\Roaming\secretaryships\Angoragedernes\speil.int

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	497497
Entropy (8bit):	1.2525295412969446
Encrypted:	false
SSDEEP:	1536:rbNZ/Rg8JCCgxT2eIgde/lBWTTBwGceukAdTYz91n6n:9NRg836IVLWHeGxKYQ
MD5:	F3F6C6E37EAB51D3B9B9C059C1EB874C
SHA1:	401E5740CCFBC1DA83BD9B426C11020C812986F2
SHA-256:	B5A607F50C65E41B2BFF7F852F27373177D326D9DFA1040E1C2B3AF62F757BAB
SHA-512:	060B328595ADAF9E85B390AA2AACEEFE4C6197294B7C45594798755C5E04BE1E2110F617B51E38D7DF423CD807FA81B30702CE2548563980B9CA195ECF2C11A7
Malicious:	false
Preview:	.....o.....j.....c..6...../.....m.....r.D..... ...T.....8.....x.....!....O....\.....G.....G.....n....."....:..... .....@.....<.....i.....k..... .....=.....g.....k.....A.....[.....).....e.....b.....6.....

C:\Users\user\AppData\Roaming\secretaryships\Hemmeligt70.Bly

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	58676
Entropy (8bit):	4.585503260397429
Encrypted:	false
SSDEEP:	768:hUm9EMv+RHOORqqYH3VEwnRnXNcmhdmPJPU9FLd86+qWhTeFVk6t6MmaEEXrDH9S:Om9chszXJlVdmPJuTWcJ6+3O9Rh
MD5:	CED0BE5E2D0028EFD3F1249AC1126BA3
SHA1:	3902CD952EA81D8A7D9E0FC1F17972967DDD917D
SHA-256:	4B029ECD2CE2EB26D9686573D7D891E689A717672BB8F76903BC44EC43DA2955
SHA-512:	7F14E8FD856D1D1E2FD89C692685EB70C462BC1C202C4946CC1B0D27E59264278264C3C7EA72E63F9B9BA35C434FAAB305724827A4C8D63ADBE78D8C4E4759D
Malicious:	false
Preview:	..ll..__.....|.....VVVVVV.*.....b.....YY...33333333333.A.KK.---.....].{{{{...KK.....T.....rr.....333.....*..Q..5.....11.....'..... 7...||||||.....V.....j.E.....}..../////.....""".....y...>.....YYYY...ff.<.....WWWW.....H.....qq..'". ~..Y.....@.....mmm....;..kkkk.....RRRRR.....zz.....UU.....7777.....jj....n.....9.p....,.....Z....s.;.....BBBBBBBB..>.Q.....W.....CC CC.xxxx.....FFFF.....).....,.....:::...[[[.....TTT.[.....PPPP.....S.....////.....^.....!..JJ.,.\\\.....ff....._..... .....hh.....``..... ..kkkkkk.....f.Z.....DDDD...z.....R.].;.....R...OO.....

C:\Users\user\AppData\Roaming\secretaryships\Tingid.pig

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped

Size (bytes):	476422
Entropy (8bit):	1.2552031449987011
Encrypted:	false
SSDEEP:	1536:zGmPxn4XjZOVebnJjvYbTUBhGKcjnO/EeMHPm:Sm6zYVb849nH6
MD5:	F236A74F28F6F32F81F1347D9F129268
SHA1:	D5BE521661EE4BF3C186C3EAA0411DD5DF6F3EBA
SHA-256:	BEED12F00B12156FF9FA63595DE11A5C01493CF5F85488CB2E159CF1A8236778
SHA-512:	D6AD37DDF7B6B38B90F09186AC81C6A76F16F9A4613D6113F10D7B2A4F68129E570EFFC77A19B04F276277B7A569EBD5FD4A48D2E2E72CEA8CEE5A8F67CC5E F4
Malicious:	false
Preview:	.....7.....).....$....%.....#.....M.....6.....N.....)..... .....a.....t.....T.....@.....+..U.....A'.....L..... .....2.....k.....&.....>.....|.....? .....&.....n.q.....}.....E.....p.....6.....

C:\Users\user\AppData\Roaming\secretaryships\anya.por

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	448073
Entropy (8bit):	1.2554221597008608
Encrypted:	false
SSDEEP:	1536:i9EUBeeNEu//hQg77ea6OP/B1p7to4APRUYZAkxe:qFZO5u/B1pBo510
MD5:	3AD8D5763CA124C7392D1F4F53D24F0E
SHA1:	17D48EF1AB8D52A31821A069C225D45201535899
SHA-256:	3965D74DBD296AA8E7524C773FE81FE63A78355145502153CB577E9CB136DDA0
SHA-512:	EE8BDE196A33297BFD4E51ED01E7D0178CF457497E822771D2BE3C58A97681AC52CD19A2BBBB71220F06F6D936A6AA67966295DF3C676104B9643F07CBE37E0 8
Malicious:	false
Preview:	.....y...k..... ....L.....c.....d.....p.....R.....5.....f.....{..... .....J.....@.....E...h.....0.....M.....'.....-.....Z.....{.....T..... ...c.W.....n.....H.....|.....^.....w.....c.....).....y.....<..... .....T.....3.....S..<.....?.....1!.....^.....t.....G.....

C:\Users\user\AppData\Roaming\secretaryships\besiddertrang.gra

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	362911
Entropy (8bit):	1.2562704713226092
Encrypted:	false
SSDEEP:	768:uFKWW9YiDIIMhmjVacve6tEvHBLNB3tQsrTpPH8mZLAUFwsahGF48hDpWRcKthwz:u5W9yMJLNbJ1CbFV3Gd6Ie48dPs
MD5:	8AB9852274FA64E09B5711A2E7D94AAB
SHA1:	2C39272B969040B4C185EE4A69A5F04FD1F7C0DB
SHA-256:	FCD149788A3530E5E2CF5E17A09B1DE51EB67B51F3E8941E7091F88B610373F1
SHA-512:	6761208A22E8D93D70465E6DD9CF1B53826AA6BF0418DCCB0A6E5816A183790A61AD67EDCF52D213669750147011075 63CE47A0465CEE801300493AEB566CC6
Malicious:	false
Preview:	....-.....?d.....\.a.....8.....x.....e.....).....+.....i..... .....4.....j.....".....Z.....%..... .....F.....g.....E./..... .....Y.....#.....F.....n.M.....W.....

C:\Users\user\AppData\Roaming\secretaryships\darbyite.txt

Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	497
Entropy (8bit):	4.296439217688297
Encrypted:	false
SSDEEP:	12:kdESMQrs7ZnIyxrqlLIRF0+UAkN0lCGsMqejQlJ8:QjMfpluqPAEsOi
MD5:	1560371431CEB91914AF5B9D0D307EE1
SHA1:	182B8979D4D0F9F26366653638A9C92FDAFF0D56

SHA-256:	72A2010CDB6ED407FCA17CDB181D5F01801F16040C2C9443BD7CB5032CDAAEF7
SHA-512:	865EF0F7636149A47043183583635C2A4306BF49565166760672B88F0F9DA89A529FE4166DFF496327304E56A8A460B8113E5F3D58601C0B8A3EFAABD792AF3D
Malicious:	false
Preview:	avenging piktogrammernes duecento korsedderkop skurvognsudlejningernes fnges ranaria..kavitet ubetalelige forhalingen passado nautically formaalsbestemmelsernes admiralsuniformers..franchot unimposing rimfire.bemba barsac unflaked skbnesvanger.tige backchats leveret viktualieforretningernes processal dignitas altica ep oxyharpikset sergenter forureningsbegrnsedes..sforsvaret antiquating photomechanically enighedernes firepot megrez almon aeneus madrassen thrallborn denoteres s lipup tvebakken..

C:\Users\user\AppData\Roaming\secretaryships\straffespark.Sek	
Process:	C:\Users\user\Desktop\Anfrage_244384.exe
File Type:	data
Category:	dropped
Size (bytes):	284322
Entropy (8bit):	7.771418895856943
Encrypted:	false
SSDEEP:	6144:fOiGjlSjER8DMKEzL4eNm6Vkg9XNf805ft+MODD+T:GCjEa4/zLD+05ek
MD5:	301AF874579F9CE64FCE51A01F616625
SHA1:	6D35516DA84E4342C8E094023B60175BAB5EDCEB
SHA-256:	35BE42786F6EF050A3BAEA615517E40958E6140A089E7D4A83283F1708994C03
SHA-512:	3275C3B39115C29FE923C415D36F4932C279018994E636CE6606C5604B6FA5DA984C7244BE7017AC78204F6F8D90AE7706B1E729FAD91EAEB3C2020A610755E4
Malicious:	false
Preview:	.....00.....WW...:...GGG..ll.....;;;....U.....<.....M.....JJ.....K.....I...###.....;;...\\.t.999.llllll..ee.LL..... .^^^.....CC...@.....(.....4.....9.....tt.....'.....1.....\....GGG.....^.....3.ZZ.:.w.....----...C.....ccccc...d.&&.....I..>>>>...www.... ...k.....o...~~.....9.....F.A...XX.....dd.....A..00...++.....%%%%.....NNNN....QQ.[[[.....fffffff.....0.....@.r..|.i.....KK.....y...,,,,,,,....TTTTT... a.....CCC.....`....((.....RR.....7...x.....#.y.....1....._.....TTTT.gg.....k.....HHHH.....$$.....b.....((.?.=====..... .....M.B.j.!.....sss....U..__.....$..;;...../////...x....WW.BB..3

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.578007574835592
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:	Anfrage_244384.exe
File size:	1'240'824 bytes
MD5:	b03f23199ae987a7bce0ff1a0d742e3e
SHA1:	f454c8de72926ee9f98db7056fa89f0c3ada9666
SHA256:	eda014e3b658bfbbfd141c1459a3414d9ee8b7c139a3976fe732141fa9cf3f80
SHA512:	01ccdc0f586a8926a56f0d3bfee91c5e882bff5df84cbb5363df6681fb62863a8075af8261bb72ecf2360d9d4dc4552dddb4e1ec1da002c24b9416ff0d3f95be
SSDEEP:	24576:aCAoDyk/vnt3h1CzLuTIv08yZVk7ku8h7w6/t338euHdB4bU4VD4C:aCAfqvtx1UuTIMfg7ku8Vfx3/uHHSU4t
TLSH:	E4451243376604A5D45984F7D75ACD30BFA3BC7B018006EB325CB71A9ABA3F0452B539
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...<.MX.....b...|.....

File Icon

Icon Hash:	076d76bb4c713307

Static PE Info

General

Entrypoint:	0x4031a3
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:	0x584DCA3C [Sun Dec 11 21:50:52 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:	CN=immechanical, O=immechanical, L=Montiers, 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	• 26/07/2024 11:01:31 26/07/2027 11:01:31
Subject Chain	• CN=immechanical, O=immechanical, L=Montiers, C=FR
Version:	3
Thumbprint MD5:	8DCDBA681539229FD7339C836C203A51
Thumbprint SHA-1:	9C6E1EF295C999DBD8E2212BF532CD5F5E425BC0
Thumbprint SHA-256:	E345B14576959ED8D4BF59A4660594FC647CCA9157F84BFFB114D15B60339C48
Serial:	313E1C1AB85C6CF76B122FEB885EF111CAA7CE29

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], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080A8h]
call dword ptr [004080A4h]
cmp ax, 00000006h
je 00007F1534C242F3h
push ebx
call 00007F1534C27261h
cmp eax, ebx
je 00007F1534C242E9h
push 00000C00h
call eax
mov esi, 00408298h
push esi
call 00007F1534C271DDh
push esi
call dword ptr [004080A0h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F1534C242CDh
push ebp
push 00000009h
call 00007F1534C27234h
push 00000007h

Instruction
call 00007F1534C2722Dh
mov dword ptr [0042F404h], eax
call dword ptr [00408044h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4B8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429828h
call dword ptr [00408174h]
push 0040A188h
push 0042EC00h
call 00007F1534C26E57h
call dword ptr [0040809Ch]
mov ebp, 00435000h
push eax
push ebp
call 00007F1534C26E45h
push ebx
call dword ptr [00408154h]

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	0x8534	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4b000	0x64f00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x12cc18	0x22e0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6071	0x6200	86ec2a2da0012903b23e33f511180572	False	0.6687659438775511	data	6.434342820031866	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1352	0x1400	cd090b7c5bd9ae3da2a43d4f02ef98b7	False	0.4599609375	data	5.237297010093776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x254f8	0x600	e98382d1559cdefaafaf45200fe1faf0	False	0.4544270833333333	data	4.037252180314336	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x30000	0x1b000	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x4b000	0x64f00	0x65000	4b35ddad0638afdc14d8651f31f9f72e	False	0.5893022896039604	data	6.144636705094013	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
RT_BITMAP	0x4b400	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States	0.23623853211009174
RT_ICON	0x4b768	0x4180c	Device independent bitmap graphic, 255 x 510 x 32, image size 260100	English	United States	0.5566530003727171
RT_ICON	0x8cf78	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States	0.6340796167041287
RT_ICON	0x9d7a0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States	0.6664652091654404
RT_ICON	0xa6c48	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States	0.6956188001889466
RT_ICON	0xaae70	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States	0.6902489626556016
RT_ICON	0xad418	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States	0.724437148217636
RT_ICON	0xae4c0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States	0.7479508196721312
RT_ICON	0xaee48	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States	0.799645390070922
RT_DIALOG	0xaf2b0	0x144	data	English	United States	0.5216049382716049
RT_DIALOG	0xaf3f8	0x13c	data	English	United States	0.5506329113924051
RT_DIALOG	0xaf538	0x100	data	English	United States	0.5234375
RT_DIALOG	0xaf638	0x11c	data	English	United States	0.6091549295774648
RT_DIALOG	0xaf758	0xc4	data	English	United States	0.5918367346938775
RT_DIALOG	0xaf820	0x60	data	English	United States	0.7291666666666666
RT_GROUP_ICON	0xaf880	0x76	data	English	United States	0.7457627118644068
RT_VERSION	0xaf8f8	0x2c8	data	English	United States	0.5084269662921348
RT_MANIFEST	0xafbc0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States	0.5542168674698795

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

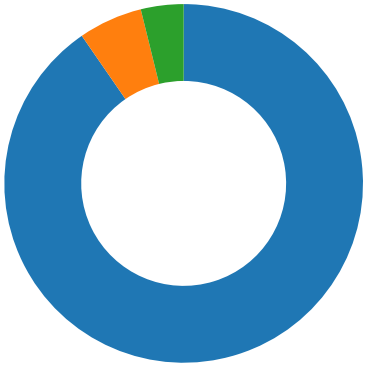
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Suricata IDS Alerts

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-11-06T16:10:51.193850+0100	2022930	ET EXPLOIT Possible CVE-2016-2211 Symantec Cab Parsing Buffer Overflow	1	52.149.20.212	443	192.168.2.6	49753	TCP
2024-11-06T16:11:29.888003+0100	2022930	ET EXPLOIT Possible CVE-2016-2211 Symantec Cab Parsing Buffer Overflow	1	52.149.20.212	443	192.168.2.6	49926	TCP
2024-11-06T16:11:29.973578+0100	2803270	ETPRO MALWARE Common Downloader Header Pattern UHCa	2	192.168.2.6	49927	188.40.95.144	443	TCP

Network Port Distribution



Total Packets: 52

- 53 (DNS)
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 6, 2024 16:11:28.768946886 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:28.768976927 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:28.769068003 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:28.780911922 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:28.780921936 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.657499075 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.657598972 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:29.708969116 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:29.708998919 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.709355116 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.709409952 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:29.713604927 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:29.755340099 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.973598957 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.973630905 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.973704100 CET	49927	443	192.168.2.6	188.40.95.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 6, 2024 16:11:29.973727942 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:29.974431038 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.090436935 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.090507030 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.108393908 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.108469963 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.224955082 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.225029945 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.226656914 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.226733923 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.342242956 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.342363119 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.343491077 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.343590021 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.459671974 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.459764004 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.460283041 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.460346937 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.576864004 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.577044964 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.578058004 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.578149080 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.693831921 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.693994045 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.694691896 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.694760084 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.811450005 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.811522007 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.811695099 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.811753988 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.812539101 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.812597990 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.928647995 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.928831100 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:30.928858995 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.928873062 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:30.928920984 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.045684099 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.045768023 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.045856953 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.045918941 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.046528101 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.046591043 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.162657022 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.162900925 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.163398027 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.163460970 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.163692951 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.163753033 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.279798985 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.279913902 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.280013084 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.280071020 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.280838013 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.281049013 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.397082090 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.397152901 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.397691965 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.397759914 CET	49927	443	192.168.2.6	188.40.95.144

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 6, 2024 16:11:31.398647070 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.398708105 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.516211987 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.516320944 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.516426086 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.516480923 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.516498089 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.516556978 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.633235931 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.633323908 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.633493900 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.633542061 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.634280920 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.634358883 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.634495020 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.649395943 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.649420023 CET	443	49927	188.40.95.144	192.168.2.6
Nov 6, 2024 16:11:31.649429083 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:11:31.652431965 CET	49927	443	192.168.2.6	188.40.95.144
Nov 6, 2024 16:12:25.578471899 CET	49985	80	192.168.2.6	194.58.112.174
Nov 6, 2024 16:12:25.583801985 CET	80	49985	194.58.112.174	192.168.2.6
Nov 6, 2024 16:12:25.583904982 CET	49985	80	192.168.2.6	194.58.112.174
Nov 6, 2024 16:12:25.592947960 CET	49985	80	192.168.2.6	194.58.112.174
Nov 6, 2024 16:12:25.598653078 CET	80	49985	194.58.112.174	192.168.2.6
Nov 6, 2024 16:12:26.524735928 CET	80	49985	194.58.112.174	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 6, 2024 16:11:28.557219028 CET	53943	53	192.168.2.6	1.1.1.1
Nov 6, 2024 16:11:28.763389111 CET	53	53943	1.1.1.1	192.168.2.6
Nov 6, 2024 16:12:25.464119911 CET	61751	53	192.168.2.6	1.1.1.1
Nov 6, 2024 16:12:25.571099043 CET	53	61751	1.1.1.1	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 6, 2024 16:11:28.557219028 CET	192.168.2.6	1.1.1.1	0xb39	Standard query (0)	familyther apycenter.rs	A (IP address)	IN (0x0001)	false
Nov 6, 2024 16:12:25.464119911 CET	192.168.2.6	1.1.1.1	0x5ba6	Standard query (0)	www.svarus .online	A (IP address)	IN (0x0001)	false

DNS Answers

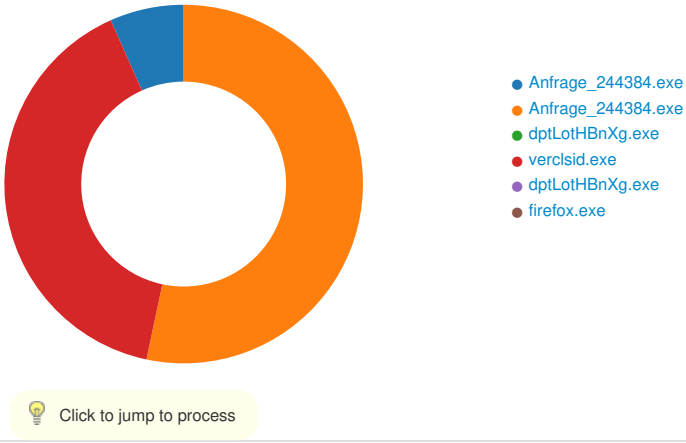
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 6, 2024 16:11:28.763389111 CET	1.1.1.1	192.168.2.6	0xb39	No error (0)	familyther apycenter.rs		188.40.95.144	A (IP address)	IN (0x0001)	false
Nov 6, 2024 16:12:25.571099043 CET	1.1.1.1	192.168.2.6	0x5ba6	No error (0)	www.svarus .online		194.58.112.17 4	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- familytherapycenter.rs
- www.svarus.online

Statistics

Behavior



System Behavior

Analysis Process: Anfrage_244384.exe PID: 5308, Parent PID: 4004

General

Target ID:	0
Start time:	10:10:32
Start date:	06/11/2024
Path:	C:\Users\user\Desktop\Anfrage_244384.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Anfrage_244384.exe"
Imagebase:	0x400000
File size:	1'240'824 bytes
MD5 hash:	B03F23199AE987A7BCE0FF1A0D742E3E
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: 00000000.00000002.2597198603.0000000004A03000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

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

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

Analysis Process: Anfrage_244384.exe PID: 5608, Parent PID: 5308

General

Target ID:	4
Start time:	10:11:21
Start date:	06/11/2024
Path:	C:\Users\user\Desktop\Anfrage_244384.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Anfrage_244384.exe"
Imagebase:	0x400000
File size:	1'240'824 bytes
MD5 hash:	B03F23199AE987A7BCE0FF1A0D742E3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.3122242151.0000000034330000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000004.00000002.3123079037.0000000035D90000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	true

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	38D0C76	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	38D0C76	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	38D0C76	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	38D0C76	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	38D0C76	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	38D0C76	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1699896	success or wait	1	40A9F0	NtReadFile
C:\Windows\SysWOW64\verclsid.exe	0	11776	success or wait	1	40A9F0	NtReadFile

Analysis Process: dptLotHBnXg.exe PID: **3052**, Parent PID: **5608**

General

Target ID:	6
Start time:	10:12:03

Start date:	06/11/2024
Path:	C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLIVOIVfQTf\dptLotHBnXg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLIVOIVfQTf\dptLotHBnXg.exe"
Imagebase:	0x9c0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000006.00000002.3362392086.0000000004560000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: verclsid.exe PID: 1056, Parent PID: 3052

General

Target ID:	7
Start time:	10:12:04
Start date:	06/11/2024
Path:	C:\Windows\SysWOW64\verclsid.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\verclsid.exe"
Imagebase:	0xbe0000
File size:	11'776 bytes
MD5 hash:	190A347DF06F8486F193ADA0E90B49C5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000007.00000002.3362363415.0000000000960000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000007.00000002.3361086022.00000000003B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000007.00000002.3362535904.00000000009B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\02-E8420I	object name not found	1	3D9288	NtDeleteFile
C:\Users\user\AppData\Local\Temp\02-E8420I	sharing violation	1	3D9288	NtDeleteFile
C:\Users\user\AppData\Local\Temp\02-E8420I	sharing violation	1	3D9288	NtDeleteFile
C:\Users\user\AppData\Local\Temp\02-E8420I	sharing violation	1	3D9288	NtDeleteFile
C:\Users\user\AppData\Local\Temp\02-E8420I	sharing violation	1	3D9288	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	1699896	success or wait	1	3D91DB	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: dptLotHBnXg.exe PID: **3916**, Parent PID: **1056**

General

Target ID:	8
Start time:	10:12:19
Start date:	06/11/2024
Path:	C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLIVOIVfQTf\dptLotHBnXg.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\tAKCTYeJpmZahMqbkmAXToQDqRYfFQfhdsmegOOXsToYOGIuLIVOIVfQTf\dptLotHBnXg.exe"
Imagebase:	0x9c0000
File size:	140'800 bytes
MD5 hash:	32B8AD6ECA9094891E792631BAEA9717
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.3361838593.00000000007B0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security
Reputation:	high
Has exited:	false

Analysis Process: firefox.exe PID: **1832**, Parent PID: **1056**

General

Target ID:	10
Start time:	10:12:31
Start date:	06/11/2024
Path:	C:\Program Files\Mozilla Firefox\firefox.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Mozilla Firefox\Firefox.exe"
Imagebase:	0x7ff728280000
File size:	676'768 bytes
MD5 hash:	C86B1BE9ED6496FE0E0CBE73F81D8045
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

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