ID: 680344
Sample Name: o3pLoLD7cc
Cookbook: default.jbs
Time: 12:40:09
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

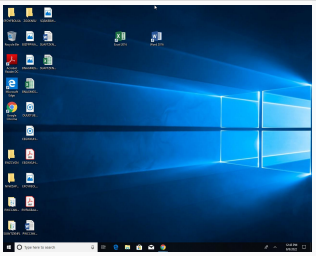
Windows Analysis Report

o3pLoLD7cc

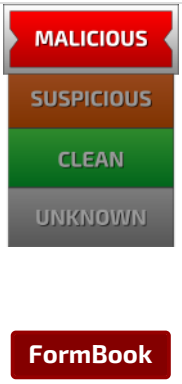
Overview

General Information

Sample Name:	o3pLoLD7cc (renamed file extension from none to exe)
Analysis ID:	680344
MD5:	0d8224c48ed19b..
SHA1:	a885be432257d2.
SHA256:	4bd0c1c5a6eb5e..
Tags:	32 exe
Infos:	



Detection



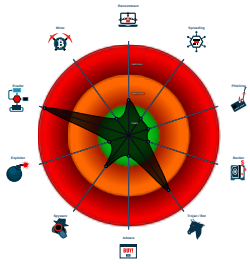
FormBook

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…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- o3pLoLD7cc.exe (PID: 980 cmdline: "C:\Users\user\Desktop\o3pLoLD7cc.exe" MD5: 0D8224C48ED19B05A91A413C69E7B4D3)
  - o3pLoLD7cc.exe (PID: 4592 cmdline: C:\Users\user\Desktop\o3pLoLD7cc.exe MD5: 0D8224C48ED19B05A91A413C69E7B4D3)
  - o3pLoLD7cc.exe (PID: 5140 cmdline: C:\Users\user\Desktop\o3pLoLD7cc.exe MD5: 0D8224C48ED19B05A91A413C69E7B4D3)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 5184 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
      - svchost.exe (PID: 4772 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: FA6C268A5B5BDA067A901764D203D433)
        - cmd.exe (PID: 5528 cmdline: /c del "C:\Users\user\Desktop\o3pLoLD7cc.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.barbaramac.com/b30i/"
  ],
  "decoy": [
    "rivacustomhomes.com",
    "foodanddessertblog.com",
    "ae-pos-package.com",
    "shantalamarr.com",
    "bangrey.xyz",
    "yourjbsaagent.com",
    "rumoastresamericas.com",
    "vetlomec.xyz",
    "israenergy.com",
    "ibuyjj.xyz",
    "redlinemuch.net",
    "plan-hub.site",
    "kosako.tech",
    "surowystorms.xyz",
    "eic.services",
    "amazoncooperative0.com",
    "4008630451.com",
    "fanfanlive.com",
    "clekgur.com",
    "3spowersolution.com",
    "szdispenser.com",
    "1stchoicemovers.uk",
    "centexfallenheroes.com",
    "rlmitte.info",
    "desertscarabe.xyz",
    "esco.website",
    "libertycontractingny.com",
    "bpcpas.online",
    "my-ar.style",
    "aster.tirol",
    "qingmu555.top",
    "arihulkkonen.info",
    "waterworksfields.co.uk",
    "zrvxr.com",
    "vfkmachine.com",
    "sekkocreativ.com",
    "goldnft.online",
    "thetrafficlist.com",
    "finpool.plus",
    "not-quite-alice.uk",
    "utblockchain.com",
    "comp-u-type.com",
    "inovasaudavel.website",
    "tlliangjia.com",
    "escolabr.website",
    "degenpotatoz.xyz",
    "miklicrp.city",
    "cryptocentury.xyz",
    "freshoutoffucks.net",
    "freemonoid.tech",
    "enchant-repining.net",
    "pvgcorp.com",
    "theskylights.co.uk",
    "637z.com",
    "ibuying.xyz",
    "nattu.info",
    "mdhzr.com",
    "rongan77.top",
    "xn--educacinenlinea-1rb.com",
    "abbeywoodlodge.com",
    "proyectosesbozo.online",
    "victormartin.xyz",
    "tind4r.com",
    "reshu-ekzamen.online"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bbb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x99bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x148a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x958a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17839:$sqlite3step: 68 34 1C 7B E1 • 0x1794c:$sqlite3step: 68 34 1C 7B E1 • 0x17868:$sqlite3text: 68 38 2A 90 C5 • 0x1798d:$sqlite3text: 68 38 2A 90 C5 • 0x1787b:$sqlite3blob: 68 53 D8 7F 8C • 0x179a3:$sqlite3blob: 68 53 D8 7F 8C
00000016.00000002.507829731.0000000000900000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.o3pLoLD7cc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.o3pLoLD7cc.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bbf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x14aa7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
5.0.o3pLoLD7cc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
5.0.o3pLoLD7cc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
0.2.o3pLoLD7cc.exe.424f558.9.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

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

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

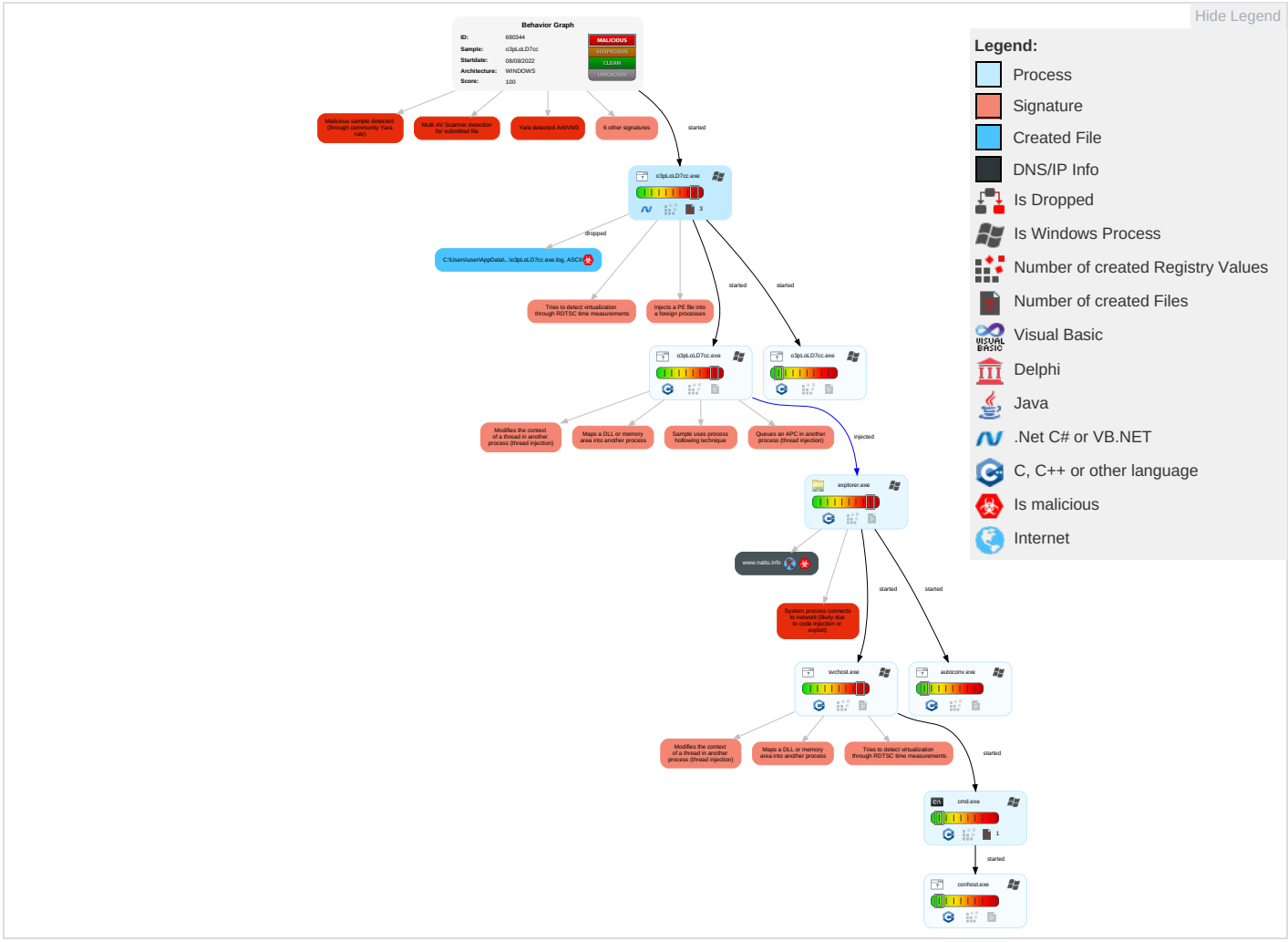
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	6 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	2 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	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 Masquerading	1 Input Capture	2 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 1 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)	3 1 Virtualization/Sandbox Evasion	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	6 1 2 Process Injection	LSA Secrets	1 1 2 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	1 1 Deobfuscate/Decode 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	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

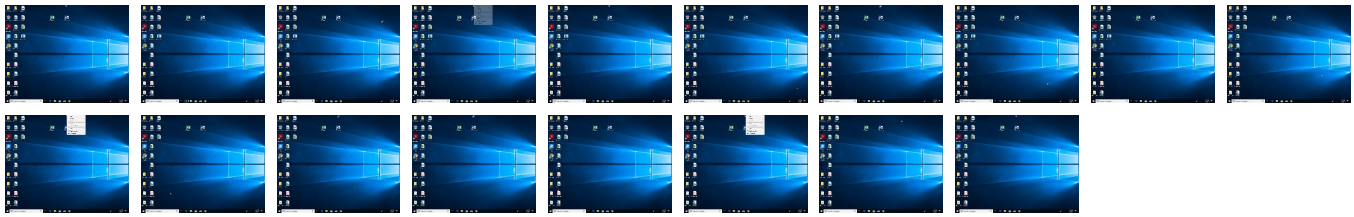
Behavior Graph



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
o3pLoLD7cc.exe	42%	Virustotal		Browse
o3pLoLD7cc.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.o3pLoLD7cc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cnJ	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comalsX	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr-c	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.founder.com.cn/cnmpat2	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/#	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comiced	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.sajatypeworks.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
www.barbaramac.com/b30i/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comk	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.founder.com.cn/cn2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/5	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.nattu.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.barbaramac.com/b30i/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com2	o3pLoLD7cc.exe, 00000000.00000003.245548384.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245979119.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247559088.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246374848.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246781545.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245108616.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244369021.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245067478.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247694806.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247023658.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246565619.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245466325.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245843164.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246820959.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247666309.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247445746.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247116878.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244398485.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244484316.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247194983.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244285528.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnJ	o3pLoLD7cc.exe, 00000000.00000003.246064355.0000000006117000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comalsX	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	o3pLoLD7cc.exe, 00000000.00000003.245548384.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245979119.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247559088.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246374848.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246781545.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245108616.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245067478.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000002.284965912.000000000732200.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247694806.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247023658.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246565619.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245466325.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245843164.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246820959.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247666309.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247445746.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247116878.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244398485.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244484316.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247194983.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244640688.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnr-c	o3pLoLD7cc.exe, 00000000.00000003.246064355.0000000006117000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.255020479.000000000611A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikipediaWt	o3pLoLD7cc.exe, 00000000.00000003.243927587.0000000006133000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnmpat2	o3pLoLD7cc.exe, 00000000.00000003.245933926.0000000006117000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/#	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.come	o3pLoLD7cc.exe, 00000000.00000003.245548384.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245979119.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247559088.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246374848.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246781545.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245108616.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245067478.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247694806.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247023658.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246565619.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245466325.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245843164.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246820959.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247666309.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247445746.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247116878.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244398485.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244484316.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247194983.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244640688.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247373240.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comiced	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.273323526.0000000006110000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.255020479.000000000611A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	o3pLoLD7cc.exe, 00000000.00000003.252641899.0000000006148000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/X	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.comt	o3pLoLD7cc.exe, 00000000.00000003.245548384.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245979119.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247559088.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246374848.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246781545.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245108616.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244369021.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245067478.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247694806.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247023658.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246565619.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245466325.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245843164.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.246820959.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247445746.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247116878.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244398485.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244484316.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.247194983.000000000612B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.244285528.000000000612B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/O	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comO	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/F	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	o3pLoLD7cc.exe, 00000000.00000003.255020479.000000000611A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	o3pLoLD7cc.exe, 00000000.00000003.244630124.0000000006116000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comk	o3pLoLD7cc.exe, 00000000.00000003.251143255.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.251497013.0000000006118000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	o3pLoLD7cc.exe, 00000000.00000003.246064355.0000000006117000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.245933926.0000000006117000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/t	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn2	o3pLoLD7cc.exe, 00000000.00000003.246064355.0000000006117000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	o3pLoLD7cc.exe, 00000000.00000002.284965912.0000000007322000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/5	o3pLoLD7cc.exe, 00000000.00000003.248134109.000000000611B000.00000004.00000800.00020000.00000000.sdmp, o3pLoLD7cc.exe, 00000000.00000003.248081608.000000000611B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680344
Start date and time: 08/08/202212:40:09	2022-08-08 12:40:09 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 40s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	o3pLoLD7cc (renamed file extension from none to 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:	32
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.evad.winEXE@10/1@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.8% (good quality ratio 82.5%) • Quality average: 72.5% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, fs.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.
- Report size getting too big, t oo many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:41:18	API Interceptor	1x Sleep call for process: o3pLoLD7cc.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\o3pLoLD7cc.exe.log

Process:	C:\Users\user\Desktop\o3pLoLD7cc.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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.77393756874727
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:	o3pLoLD7cc.exe
File size:	807936
MD5:	0d8224c48ed19b05a91a413c69e7b4d3
SHA1:	a885be432257d23d63d0ba448ec0cb6950e37370
SHA256:	4bd0c1c5a6eb5e3bb2e84db799270248f5467dfb3e6e3b1d8db14887eeecae5e
SHA512:	67b6a482b9d0dfb5b07351d05402cb10a7b1cd2724d5dc20ac9515805dd887d025b82df351201ac16cc64f71d2dd7dbcfa7e960be2de2afbc6ac1e638b1ff922
SSDEEP:	24576:5FxgV10gWvlZm4Ipn1xOFfnckCe9IbUDHDl:lgVWddIpqFpC7U
TLSH:	3B05BE1BAF147708C5A76AB4EE0BB97267F61C5D3175D0B83E647C0A4AFF301E52242A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..L.....j... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c6ace
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:	0x62F0CBF8 [Mon Aug 8 08:40:24 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc6a7c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x3a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	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	0xc4ad4	0xc4c00	False	0.813856267868488	data	7.7803803280527	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x3a8	0x400	False	0.3779296875	data	2.9367451592192806	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xca000	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	0xc8058	0x34c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 12:42:59.534740925 CEST	51391	53	192.168.2.3	8.8.8.8
Aug 8, 2022 12:43:00.008338928 CEST	53	51391	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 12:42:59.534740925 CEST	192.168.2.3	8.8.8.8	0xa4df	Standard query (0)	www.nattu.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 12:43:00.008338928 CEST	8.8.8.8	192.168.2.3	0xa4df	Server failure (2)	www.nattu.info	none	none	A (IP address)	IN (0x0001)

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

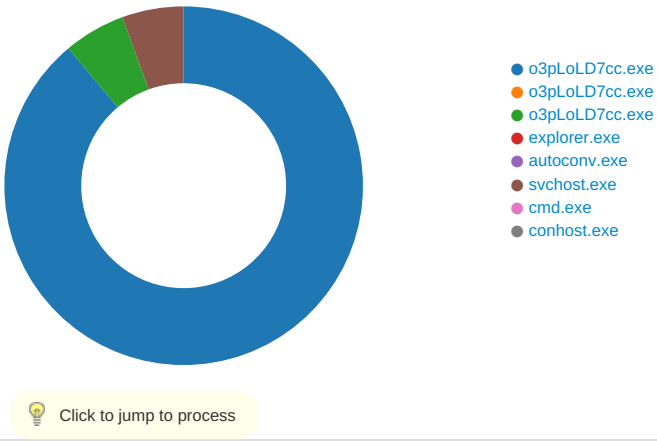
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEC
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEC
GetMessageW	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEC
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEC

Statistics

Behavior



System Behavior

Analysis Process: o3pLoLD7cc.exe PID: **980**, Parent PID: **5292**

General

Target ID:	0
Start time:	12:41:08
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\o3pLoLD7cc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\o3pLoLD7cc.exe"

Imagebase:	0xe10000
File size:	807936 bytes
MD5 hash:	0D8224C48ED19B05A91A413C69E7B4D3
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: 00000000.00000002.280526739.00000000033FA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.278817916.00000000031C3000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.281181873.000000000424F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.281181873.000000000424F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.281181873.000000000424F000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.281181873.000000000424F000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: o3pLoLD7cc.exe PID: **4592**, Parent PID: **980**

General

Target ID:	4
Start time:	12:41:20
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\o3pLoLD7cc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\o3pLoLD7cc.exe
Imagebase:	0xe0000
File size:	807936 bytes
MD5 hash:	0D8224C48ED19B05A91A413C69E7B4D3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: o3pLoLD7cc.exe PID: **5140**, Parent PID: **980**

General

Target ID:	5
Start time:	12:41:21
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\o3pLoLD7cc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\o3pLoLD7cc.exe
Imagebase:	0x4b0000
File size:	807936 bytes
MD5 hash:	0D8224C48ED19B05A91A413C69E7B4D3
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: 00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.270208888.0000000000401000.00000040.00000400.00020000.00000000.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	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **5140**

General

Target ID:	6
Start time:	12:41:28
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.352084997.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.352084997.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.352084997.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.352084997.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.331404311.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.331404311.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.331404311.000000000D756000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.331404311.000000000D756000.00000040.00000001.00040000.00000000.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: autoconv.exe PID: **5184**, Parent PID: **3968**

General

Target ID:	21
Start time:	12:42:04
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x8f0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: svchost.exe PID: 4772, Parent PID: 3968

General

Target ID:	22
Start time:	12:42:04
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x950000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.507829731.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.507829731.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.507829731.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.507829731.0000000000900000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.508959934.0000000002960000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.508959934.0000000002960000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.508959934.0000000002960000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.508959934.0000000002960000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.506902043.00000000004A0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000016.00000002.506902043.00000000004A0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.506902043.00000000004A0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.506902043.00000000004A0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4BA447	NtReadFile

Analysis Process: cmd.exe PID: 5528, Parent PID: 4772

General

Target ID:	23
Start time:	12:42:10
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\o3pLoLD7cc.exe"
Imagebase:	0xc20000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false

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

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4784**, Parent PID: **5528**

General

Target ID:	25
Start time:	12:42:11
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly