ID: 528618
Sample Name:
cK1g5gckZR9VHjj.exe
Cookbook: default.jbs
Time: 15:09:16
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report cK1g5gckZR9VHjj.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 18
ICMP Packets 18
DNS Queries 18
DNS Answers 18
HTTP Request Dependency Graph 19
HTTP Packets 19
Code Manipulations 21

Statistics 21
Behavior 21
System Behavior 21
Analysis Process: cK1g5gckZR9VHjj.exe PID: 7160 Parent PID: 6012 22
General 22
File Activities 22
File Created 22
File Written 22
File Read 22
Analysis Process: cK1g5gckZR9VHjj.exe PID: 1312 Parent PID: 7160 22
General 22
Analysis Process: cK1g5gckZR9VHjj.exe PID: 6104 Parent PID: 7160 22
General 22
File Activities 23
File Read 23
Analysis Process: explorer.exe PID: 3440 Parent PID: 6104 23
General 23
File Activities 24
Analysis Process: netsh.exe PID: 6904 Parent PID: 3440 24
General 24
File Activities 24
File Read 24
Analysis Process: cmd.exe PID: 6900 Parent PID: 6904 25
General 25
File Activities 25
Analysis Process: conhost.exe PID: 6992 Parent PID: 6900 25
General 25
Disassembly 25
Code Analysis 25

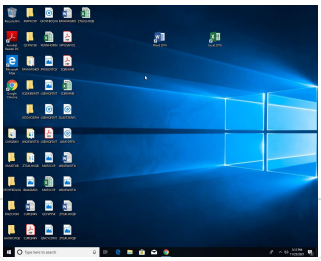
Windows Analysis Report cK1g5gckZR9VHjj.exe

Overview

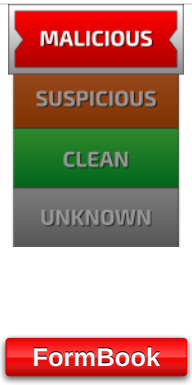
General Information

Sample Name:	cK1g5gckZR9VHjj.exe
Analysis ID:	528618
MD5:	5f19b9a3e41ef2e..
SHA1:	25638b49edf7444.
SHA256:	afac806262706ae.
Tags:	exe Formbook xloader
Infos:	

Most interesting Screenshot:



Detection



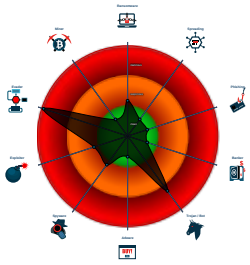
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- 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…
- Uses netsh to modify the Windows n…
- Tries to detect sandboxes and other…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- cK1g5gckZR9VHjj.exe (PID: 7160 cmdline: "C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe" MD5: 5F19B9A3E41EF2E6EC3200BF4A246CEC)
  - cK1g5gckZR9VHjj.exe (PID: 1312 cmdline: C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe MD5: 5F19B9A3E41EF2E6EC3200BF4A246CEC)
  - cK1g5gckZR9VHjj.exe (PID: 6104 cmdline: C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe MD5: 5F19B9A3E41EF2E6EC3200BF4A246CEC)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 6904 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 6900 cmdline: /c del "C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.spoiledzone.com/udeh/"
  ],
  "decoy": [
    "pimpyoursmile.com",
    "mibikeshops.com",
    "blueprintroslyn.com",
    "onlinedatingthaiweb.com",
    "filmweltruhr.com",
    "apprigutimaunrpgroup.com",
    "prolineautoservices.com",
    "thejohnmatt.com",
    "predialisbolivia.com",
    "pittsburghdata.center",
    "janeflwr.com",
    "usxigroup.com",
    "canurfaliogli.net",
    "securebankofamericalog.site",
    "concernedclimatecitizen.com",
    "756256.xyz",
    "blaclyteproductions.com",
    "chaturey.com",
    "mesoftbilisim.com",
    "crochetastitch.com",
    "biggirlrantz.com",
    "trenddoffical.com",
    "eureka.quest",
    "syuanbao.com",
    "auspicious.tech",
    "mypc.host",
    "hemeishun.com",
    "3973rollingvalleydrive.com",
    "lovebydarius.store",
    "z1liner.com",
    "pspoint.com",
    "skincell-advanced.website",
    "937281.com",
    "mygranitepro.com",
    "masterlotz.com",
    "electricidadygasmx.com",
    "mmcyxx.com",
    "fixmetech.com",
    "teesworkshop.com",
    "topshelfbudshop.com",
    "ccnet.club",
    "myfranciscanshoe.com",
    "kyrstensinema2024.com",
    "selectioncoeur.com",
    "nrgd1.club",
    "qzttb.net",
    "ouidles.com",
    "royaldears.com",
    "downingmunroe.online",
    "seawooenc.com",
    "flagfootballcoaches.com",
    "tremblock.com",
    "finsits.com",
    "rcepjobs.com",
    "web-control.biz",
    "notvaccinatedjobs.com",
    "glueandstack.com",
    "modularbuildingsolutions.net",
    "sosibibyslot.website",
    "dragonmodz.net",
    "turkishdelightday.xyz",
    "dentalhealth24.com",
    "celtabet153.xyz",
    "pigsandbees.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000000.355165380.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.355165380.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.cK1g5gckZR9VHjj.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.cK1g5gckZR9VHjj.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.0.cK1g5gckZR9VHjj.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
2.0.cK1g5gckZR9VHjj.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.0.cK1g5gckZR9VHjj.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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:

Self deletion via cmd delete

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

Queues an APC in another process (thread injection)

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

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

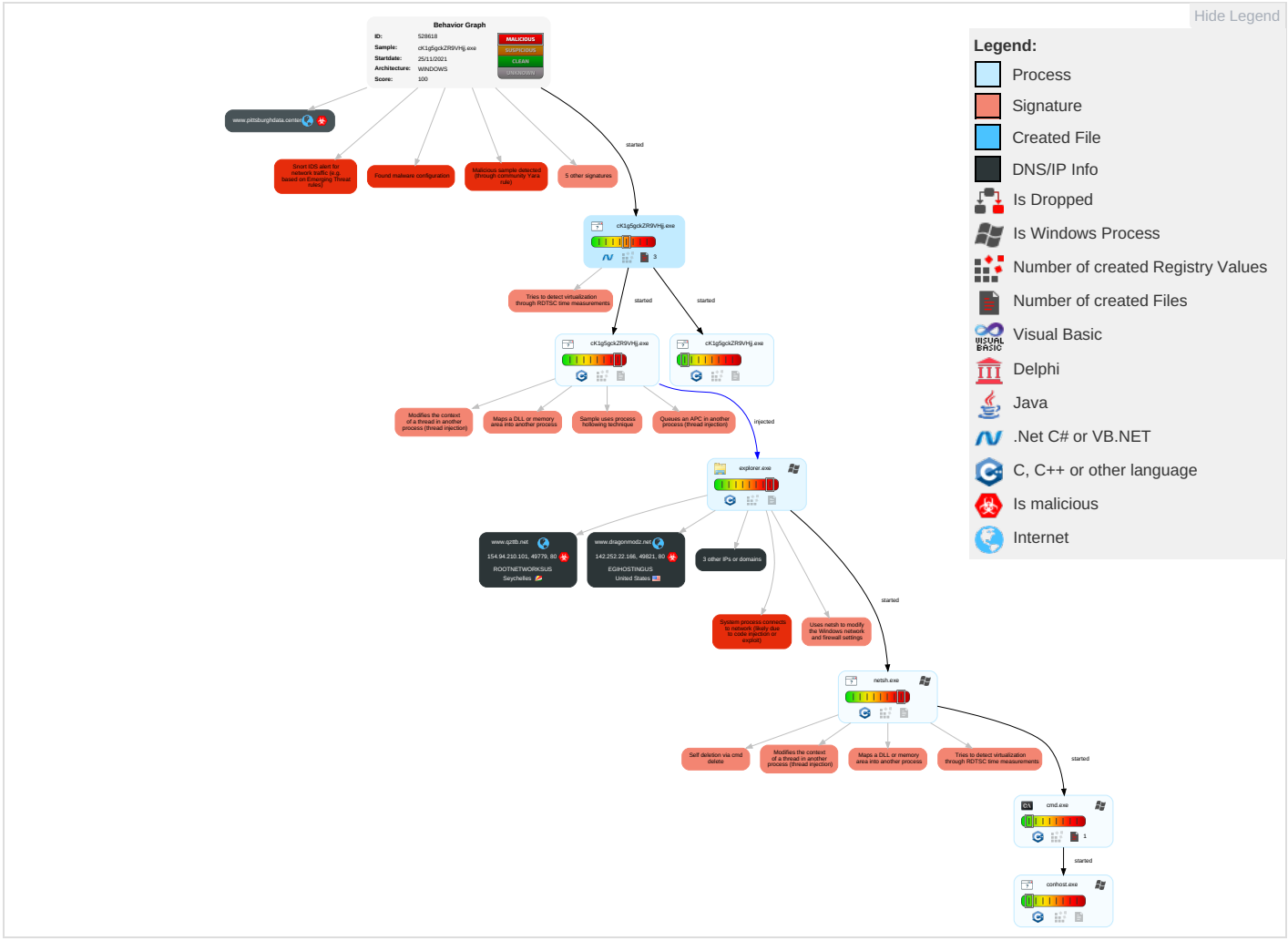
Remote Access Functionality:

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
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.cK1g5gckZR9VHjj.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.cK1g5gckZR9VHjj.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.cK1g5gckZR9VHjj.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.cK1g5gckZR9VHjj.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.dragonmodz.net/udeh/?Ipp=dUteF4ZXLzuJCUcYdQc1YLLQWaT61UR38kyqHblZtlDA/JK3c3P/1iwgVtH+FS5JjCNv5C6f7A==&w8e=oTrd	0%	Avira URL Cloud	safe	
http://www.qzttb.net/udeh/?Ipp=0GJ3uF0xqxUvxNgo0ZAG0/AKZrovZvEja3W0Pwl2ZRVpe8mYbBKREVo+7yTMDi1lrzUfYpfKkw==&w8e=oTrd	0%	Avira URL Cloud	safe	
http://www.royaldears.com/udeh/?Ipp=v0MSI9GJGiZ1sOz/LzfG2QhElsQnBWapnw3k3ldXy2xTual36y4oBDIxb66ss1xce1kRKjOJbQ==&w8e=oTrd	0%	Avira URL Cloud	safe	
www.spoiledzone.com/udeh/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.qzttb.net	154.94.210.101	true	true		unknown
www.royaldears.com	3.64.163.50	true	true		unknown
www.dragonmodz.net	142.252.22.166	true	true		unknown
www.pittsburghdata.center	209.17.116.163	true	true		unknown
www.blueprintroslyn.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.dragonmodz.net/udeh/?Ipp=dUteF4ZXLzuJCUcYdQc1YLLQWaT61UR38kyqHblZtlDA/JK3c3P/1iwgVtH+FS5JjCNv5C6f7A==&w8e=oTrd	true	• Avira URL Cloud: safe	unknown
http://www.qzttb.net/udeh/?Ipp=0GJ3uF0xqxUvxNgo0ZAG0/AKZrovZvEja3W0Pwl2ZRVpe8mYbBKREVo+7yTMDi1lrzUfYpfKkw==&w8e=oTrd	true	• Avira URL Cloud: safe	unknown
http://www.royaldears.com/udeh/?Ipp=v0MSI9GJGiZ1sOz/LzfG2QhElsQnBWapnw3k3ldXy2xTual36y4oBDIxb66ss1xce1kRKjOJbQ==&w8e=oTrd	true	• Avira URL Cloud: safe	unknown
www.spoiledzone.com/udeh/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.252.22.166	www.dragonmodz.net	United States		18779	EGIHOSTINGUS	true
154.94.210.101	www.qzttb.net	Seychelles		32708	ROOTNETWORKSUS	true
3.64.163.50	www.royaldears.com	United States		16509	AMAZON-02US	true
209.17.116.163	www.pittsburghdata.center	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528618
Start date:	25.11.2021
Start time:	15:09:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cK1g5gckZR9VHjj.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:	24
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@9/1@7/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.9% (good quality ratio 12.4%) • Quality average: 72.5% • Quality standard deviation: 32.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:10:15	API Interceptor	27x Sleep call for process: cK1g5gckZR9VHjj.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3.64.163.50	Nuevo Pedido.exe	Get hash	malicious	Browse	• www.rcepjobs.com/udeh/?2dYxhfjx=Sh2Frx7Ne5Gbf0GZF0aHN0EyZlj99LhHOr4v0jLu0VOTkpyLoQ3tHVxja8cQ+qoaRshC&s6AD=5jltOBY8-rN
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• www.inklusion.online/n8ds/?6ldD=4XwYGzmPDVH3THQXSPknmfdazToDAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&v6Mt=3fxxA4Z

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xDG1WDcI0o.exe	Get hash	malicious	Browse	• www.warriorsouls.com/imnt/?w4=173jVSvDSoGUE2AW1ivoK5ykCyKPADg/LonPGNHNCQX2BYegbwJ7vTJYHkxtjawzsEfN&nHNxLR=Q48l
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?0v=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&kTGXE2=5jpDxBr8jNJ0VnGP
	Xl1gbEIo0b.exe	Get hash	malicious	Browse	• www.teachermeta.com/btn2/?nRk=QvINNIMzsRYf/0qmivF6Dmovk+WpXAaZUAI4egrxWGuGQnhzgyC+G4dLS9x+/CyjCjh9&sFN0Yx=JL0hlxBhSB
	Rev_NN doccument.doc	Get hash	malicious	Browse	• www.brettneoheroes.com/e6b3/
	202111161629639000582.exe	Get hash	malicious	Browse	• www.sketchnfts.com/wkgp/?4h5=jdmv8BZZ/B46r0we2YWB0KZ3uGSoSKuz6a4pN1QKcZ2F8xRxcAMtTOc/gzvsbCezLg9G&2dX=P6APITtHDX2tmpK
	Ez6r9fZIXc.exe	Get hash	malicious	Browse	• www.battlegroundxr.com/ad6n/?G8a0vHm=ZcTQfm3E3Bis9O+U1J+3C+jUHMxN8jyTuxkjib6Q0pkS+Pn4CLfVing+78WMbf+swImY&6lrHq=5jktfN6hH6
	New Order INQ211118.exe	Get hash	malicious	Browse	• www.cleversights.com/ng6c/?JBGdjn1=EPV2/NoACT8dHOR9v1gyCHceGsyPjrlJM+UK8aQEsksszrMl224UALhiEE2fgJmZ+elx&8pB8=1bqLQxdXG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quote.exe	Get hash	malicious	Browse	• www.sandspringsrambl ers.com/g2fg/?1btd=IfCDV&CTEp9H=ge+LGbGWprSeotpzV0+Q+kydhBjB2swQkk5yFtO6ceAAyVR8yEXyjgFWO6AISkVeqI4m
	111821 New Order_xlxs.exe	Get hash	malicious	Browse	• www.methodicalservices.com/oae0/?UDKtfT=0pSD8r20Ixf8_&9rGxtBkx=0YzjOyVp+Yb6xacNTkTkmGCYCJkm2COrsGtOu7+4k+P6CiNE0Q3WT0+8/3B2OogfveoZ
	rEC0x536o5.exe	Get hash	malicious	Browse	• www.evaccines.com/s3f1/?XZeT=mbzqDKJ3zGVZXRXzBR45Cgdnnesr2+nRJSwniRIMGUaPxNPQA+ji5LfWApDcm/CqO18J&_dlpGp=dTiPIlmXgVLtX
	Booking Confirmation 548464656_pdf.exe	Get hash	malicious	Browse	• www.metaversealive.com/cfb2/?4hGdfRT=Agu3xtL1ZQO5CFfrtHOGjgVP3skWkN/ViqH4UJ4za8OjNS089a88X4B7IihWeXraBDmd&2dM4Gf=e4hhCbFxvtz0ztm
	Purchase Order Ref No_ Q51100732.xlsx	Get hash	malicious	Browse	• www.fondoflouisville.com/dyh6/?NL0hl=kQyzM0Wln+3leUBi0Wmn3eENdAam7BCJPPELL5jXxpKBYvrw3jMhvOGuqF2XIvtdQ71vEA==&v2M=r0DdC04HWpDX
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.inklusion.online/n8ds/?9rJT=4XwYGzmPDVH3THQXSPknmfdazTodAXDlHas2KNX7n/UXs4ghRUZWEGvkVm0hYsfSCvUh&at=WtR4GZm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order-2021-PO.Pdf.exe	Get hash	malicious	Browse	• www.godrejs-windsor.com/vocn/?5jYXyzb=pnlTJGUzE5gMj2POSUsxOYM9XX/o1stqBdRTzx6fWnpbF/A27HO5FUQYdB9AbrLCdWzy&IL08W8=d6AXkVBHUjyXZ
	Inquiry Sheet.doc	Get hash	malicious	Browse	• www.babehairboutique.com/cy88/?7nLpW=-ZKlyLs0ebYdGfJ&QZ=K8MP/gXd9fA79gQ3nARZg5fl4N3QoqdUhkC4TU9uNhwqyFbAVwd8tffptZPcvcemife8Lg==
	PO-No 243563746 Sorg.exe	Get hash	malicious	Browse	• www.webmakers.xyz/seqa/?tvv=ihZT8RaXnH5DP6&R48TL=PArQXewhCLQ/aGYQG57zH1nhkqDi1nj517Xyl5njozHkl0sb3Vjromuzr7tZwLe6Yf/2
	ORDER REMINDER.doc	Get hash	malicious	Browse	• www.questaylor.com/zaip/?r2JPlFDH=HAqh6cOe6LTcTwCBF16MZHaJ4csidjMHsZ2CzJlUzLX8i4OfANm4LybqNg7cEAPcNuVe8g==&Ozu8Z=qxoHsxEPs4u
	Order Specification.doc	Get hash	malicious	Browse	• www.vestamobile.com/c28n/?-Zl=BwxsM8rRu+R6ZjIadp4KdiQptkWWHTzqe5Z/ld4s21xj8K8eoUYG89NnPoNyzSQlYa401Q==&Rnjl=fpapUTW

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EGIHOSTINGUS	or4ypx7Ery	Get hash	malicious	Browse	• 172.120.223.197
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 172.120.157.187
	SOA.exe	Get hash	malicious	Browse	• 45.39.212.96
	Swift Copy TT.doc	Get hash	malicious	Browse	• 142.111.110.248
	Product Offerety44663573.xlsx	Get hash	malicious	Browse	• 68.68.98.160
	Env#U00edo diciembre.exe	Get hash	malicious	Browse	• 104.253.94.109
	IAENMAI.xlsx	Get hash	malicious	Browse	• 23.27.137.70

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	jydygx.arm7	Get hash	malicious	Browse	• 107.165.18.79
	202111161629639000582.exe	Get hash	malicious	Browse	• 166.88.19.181
	w8aattzDPj	Get hash	malicious	Browse	• 172.121.95.168
	XxMcevQr2Z	Get hash	malicious	Browse	• 172.120.10 8.136
	sora.arm	Get hash	malicious	Browse	• 136.0.238.242
	x3mKjigp7j	Get hash	malicious	Browse	• 216.172.14 5.226
	588885.xlsx	Get hash	malicious	Browse	• 107.187.86.150
	New Order INQ211118.exe	Get hash	malicious	Browse	• 23.230.105.118
	REltoQA3nv.exe	Get hash	malicious	Browse	• 107.164.10 2.213
	uranium.x86	Get hash	malicious	Browse	• 136.0.81.164
	SHIPPPING-DOC.xlsx	Get hash	malicious	Browse	• 50.118.200.122
	order-2021-PO.Pdf.exe	Get hash	malicious	Browse	• 142.111.56.40
	zhaP868fw5	Get hash	malicious	Browse	• 23.27.237.204
ROOTNETWORKSUS	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 154.94.229.8
	eh.arm	Get hash	malicious	Browse	• 154.82.151.141
	l1z4rdsQu4D.x86	Get hash	malicious	Browse	• 154.27.158.217
	d8Hs7X8HGP	Get hash	malicious	Browse	• 154.27.246.223
	y2NMF6ulOI	Get hash	malicious	Browse	• 154.82.103.232
	Hilix.arm	Get hash	malicious	Browse	• 154.82.151.120
	document.exe	Get hash	malicious	Browse	• 154.82.127.19
	yXTRZQmYdr	Get hash	malicious	Browse	• 154.94.148.183
	Owari.arm7	Get hash	malicious	Browse	• 154.82.103.252
	JuihXmkZGF	Get hash	malicious	Browse	• 154.94.148.170
	2gRh8To5o9	Get hash	malicious	Browse	• 154.27.246.214
	zFDNFIXYHn	Get hash	malicious	Browse	• 103.211.168.19
	peach.arm	Get hash	malicious	Browse	• 156.236.248.47
	zgV2Uq4fmu	Get hash	malicious	Browse	• 156.236.225.9
	7fic3HM8I3	Get hash	malicious	Browse	• 156.236.225.7
	mixazed_20210816-155711.exe	Get hash	malicious	Browse	• 154.82.111.78
	M8XFTAqveT	Get hash	malicious	Browse	• 154.82.151.133
	RR8K3UpQdt	Get hash	malicious	Browse	• 38.240.210.8
	Qka3fi8NpL	Get hash	malicious	Browse	• 154.82.151.169
	Z7bNxhhS7y	Get hash	malicious	Browse	• 154.82.151.124

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cK1g5gckZR9VHjj.exe.log	
Process:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cK1g5gckZR9VHjj.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.842673281078141
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:	cK1g5gckZR9VHjj.exe
File size:	445440
MD5:	5f19b9a3e41ef2e6ec3200bf4a246cec
SHA1:	25638b49edf7444005e1e02fb5d972da5920e1d8
SHA256:	afac806262706aea36f8c34cb56ffa94f49da9b39b752cfd077f9b921e972c1d
SHA512:	9819afc87fe9dc827cfdaf7a676ab8e01f7e419ac09e354cbb3270e167527db2ffea6d61fbe46469c14e3a8a2689f26c98712606e0878294167ed7e15e6fb2c5
SSDEEP:	12288:G/NdU0VixBFmkJ+W/wCCGBRG5F2ZBGutgq:G/vU0Vi1nJ+dCPukAuJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...hI.a.....0..... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46e0b6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4968 [Thu Nov 25 08:29:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6c0cc	0x6c200	False	0.883977601156	data	7.85526570093	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x5c4	0x600	False	0.4296875	data	4.13349213194	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-15:11:39.736402	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
11/25/21-15:11:41.436557	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49801	80	192.168.2.6	3.64.163.50
11/25/21-15:11:41.436557	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49801	80	192.168.2.6	3.64.163.50
11/25/21-15:11:41.436557	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49801	80	192.168.2.6	3.64.163.50

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 15:11:34.718662977 CET	192.168.2.6	8.8.8.8	0xa06c	Standard query (0)	www.qzttb.net	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:35.732012987 CET	192.168.2.6	8.8.8.8	0xa06c	Standard query (0)	www.qzttb.net	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:41.348179102 CET	192.168.2.6	8.8.8.8	0xe11f	Standard query (0)	www.royaldears.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:46.591064930 CET	192.168.2.6	8.8.8.8	0x209c	Standard query (0)	www.dragonmodz.net	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:57.075520992 CET	192.168.2.6	8.8.8.8	0x35bb	Standard query (0)	www.blueprintroslyn.com	A (IP address)	IN (0x0001)
Nov 25, 2021 15:12:02.135910988 CET	192.168.2.6	8.8.8.8	0x140	Standard query (0)	www.pittsburghdata.center	A (IP address)	IN (0x0001)
Nov 25, 2021 15:12:23.801845074 CET	192.168.2.6	8.8.8.8	0xe244	Standard query (0)	www.pittsburghdata.center	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 15:11:35.928148031 CET	8.8.8.8	192.168.2.6	0xa06c	No error (0)	www.qzttb.net		154.94.210.101	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:39.736213923 CET	8.8.8.8	192.168.2.6	0xa06c	Server failure (2)	www.qzttb.net	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:41.409744024 CET	8.8.8.8	192.168.2.6	0xe11f	No error (0)	www.royaldears.com		3.64.163.50	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:46.682406902 CET	8.8.8.8	192.168.2.6	0x209c	No error (0)	www.dragonmodz.net		142.252.22.166	A (IP address)	IN (0x0001)
Nov 25, 2021 15:11:57.112966061 CET	8.8.8.8	192.168.2.6	0x35bb	Name error (3)	www.blueprintroslyn.com	none	none	A (IP address)	IN (0x0001)
Nov 25, 2021 15:12:02.309823036 CET	8.8.8.8	192.168.2.6	0x140	No error (0)	www.pittsburghdata.center		209.17.116.163	A (IP address)	IN (0x0001)
Nov 25, 2021 15:12:23.989738941 CET	8.8.8.8	192.168.2.6	0xe244	No error (0)	www.pittsburghdata.center		209.17.116.163	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.qzttb.net
- www.royaldears.com
- www.dragonmodz.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49779	154.94.210.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:11:36.125092030 CET	11598	OUT	GET /udeh/?lpp=0GJ3uF0xqxUvxNgo0ZAG0/AKZrovZvEja3W0Pwl2ZRVpe8mYbBKREVo+7yTMDi1lrzUfYpfKkw==&w8e=oTrd HTTP/1.1 Host: www.qzttb.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:11:36.336148024 CET	12007	IN	HTTP/1.1 404 Not Found Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/10.0 X-Powered-By: PHP/7.0.33 X-Powered-By: ASP.NET Date: Thu, 25 Nov 2021 14:11:35 GMT Connection: close Content-Length: 7447 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 53 79 73 74 65 6d 20 45 72 72 6f 72 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 6e 6f 66 6f 6c 6c 6f 77 22 20 2f 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 2f 2a 20 42 61 73 65 20 2a 2f 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 33 33 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 31 34 70 78 20 56 65 72 64 61 6e 61 2c 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 68 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 27 4d 69 63 72 6f 73 6f 66 74 20 59 61 48 65 69 27 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 30 70 78 20 32 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 6f 72 64 2d 62 72 65 61 6b 3a 20 62 72 65 61 6b 2d 77 6f 72 64 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 68 31 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 30 70 78 20 30 20 30 3b 0d 0a 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 32 38 70 78 3b 0d 0a 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 35 30 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 33 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 68 32 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0d 0a 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 34 30 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 36 70 78 20 30 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0d 0a 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 38 70 78 3b 0d 0a 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 31 70 78 20 73 6f 6c 69 64 20 23 65 65 65 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 68 33 2e 73 75 62 68 65 61 64 69 6e 67 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 34 32 38 38 63 65 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 36 70 78 20 30 20 30 3b 0d 0a 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 34 30 30 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 20 20 20 20 20 20 20 20 68 33 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 31 32 70 78 3b 0d 0a 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 36 70 78 3b 0d 0a 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 62 6f 6c 64 3b 0d 0a 20 Data Ascii: <!DOCTYPE html><html><head> <meta charset="UTF-8"> <title>System Error</title> <meta name ="robots" content="noindex,nofollow" /> <meta name="viewport" content="width=device-width, initial-scale=1, user-scal able=no"> <style> /* Base */ body { color: #333; font: 14px Verdana, "Helvetica Neue", helvetica, Arial, 'Microsoft YaHei', sans-serif; margin: 0; padding: 0 20px 20px; word-break: break-word; } h1{ margin: 10px 0 0; font-size: 28px; font-weight: 500; line-height: 32px; } h2{ color: #4288ce; font-weight: 400; padding: 6px 0; margin: 6px 0 0; font-size: 18px; border-bottom: 1px solid #eee; } h3.subheading { color: #4288ce; margin: 6px 0 0; font-weight: 400; } h3{ margin: 12px; font-size: 16px; font-weight: bold;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49801	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:11:41.436557055 CET	15048	OUT	GET /udeh/?lpp=v0MSI9GJGiZ1sOz/LzfG2QhElsQnBWapnw3k3ldXy2xTual36y4oBDIxb66ss1xce1kRKjOJbQ==&w8e=oTrd HTTP/1.1 Host: www.royaldears.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:11:41.456082106 CET	15049	IN	HTTP/1.1 410 Gone Server: openresty Date: Thu, 25 Nov 2021 14:11:41 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 65 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 79 61 6c 64 65 61 72 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 61 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 72 6f 79 61 6c 64 65 61 72 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4e <meta http-equiv='refresh' content='5; url=http://www.royaldears.com/' />a </head>9 <body>3a You are being redirected to http://www.royaldears.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49821	142.252.22.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 15:11:46.852530956 CET	16564	OUT	GET /udeh/?lpp=dUteF4ZXLzuJCUcYdQc1YLLQWaT61UR38kyqHblZtlDA/JK3c3P/1iwgVtH+FS5JjCNv5C6f7A==&w8e=oTrd HTTP/1.1 Host: www.dragonmodz.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 15:11:47.031126976 CET	16565	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 14:11:46 GMT Content-Type: text/html Content-Length: 1886 Connection: close Vary: Accept-Encoding Data Raw: 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 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 ba a3 b6 ab c3 c3 ba b1 c6 fb b3 b5 ce ac d0 de cd b6 d7 ca d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 31 35 33 32 3b 26 23 31 39 39 36 38 3b 26 23 38 33 3b 26 23 36 39 3b 26 23 32 34 37 37 33 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 33 39 36 34 30 3b 26 23 32 38 31 36 35 3b 26 23 32 32 32 36 39 3b 26 23 33 35 38 32 31 3b 26 23 33 33 32 35 38 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 30 31 33 35 3b 26 23 32 30 38 3b 26 23 32 31 33 30 36 3b 26 23 32 32 33 31 32 3b 26 23 34 34 3b 26 23 33 33 33 39 34 3b 26 23 33 39 33 32 31 3b 26 23 33 34 31 32 31 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 30 31 30 38 3b 26 23 32 31 33 30 36 3b 26 23 32 32 33 31 32 3b 26 23 34 34 3b 26 23 33 33 33 39 34 3b 26 23 33 39 33 32 31 3b 26 23 33 34 31 32 31 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 32 33 31 32 3b 26 23 33 32 34 34 37 3b 26 23 32 34 34 33 33 3b 26 23 33 35 32 37 30 3b 2c 26 23 32 33 35 34 35 3b 26 23 33 30 35 32 38 3b 26 23 33 38 32 33 36 3b 26 23 32 33 33 37 36 3b 26 23 32 30 38 33 37 3b 26 23 32 33 35 36 37 3b 26 23 32 38 31 36 35 3b 26 23 32 36 30 33 32 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 31 35 33 32 3b 26 23 31 39 39 36 38 3b 26 23 38 33 3b 26 23 36 39 3b 26 23 32 34 37 37 33 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 33 39 36 34 30 3b 26 23 32 38 31 36 35 3b 26 23 32 32 32 36 39 3b 26 23 33 33 33 39 34 3b 26 23 33 39 33 32 31 3b 26 23 33 34 31 32 31 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 2c 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 26 23 32 30 31 32 32 3b 26 23 32 37 39 35 34 3b 26 23 33 31 35 33 32 3b 26 23 31 39 39 36 38 3b 26 23 38 33 3b 26 23 36 39 3b 26 23 32 34 37 37 33 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 26 23 34 34 3b 26 23 33 39 36 34 30 3b 26 23 32 38 31 36 35 3b 26 23 32 32 32 36 39 3b 26 23 33 35 38 32 31 3b 26 23 33 33 32 35 38 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 33 35 32 37 30 3b 26 23 33 39 30 35 37 3b 26 23 32 30 31 30 38 3b 26 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title="';</script><title>亚洲第一SE情网站,高清国语自产精品视频二区在,色香蕉视频,久久国产精品在线影视,对着镜子后入小清新国产精品</title><meta name="keywords" content="亚洲第一SE情网站,高清国语自产精品视频二区在,色香蕉视频,久久国产精品在线影视,对着镜子后入小清新国产精品" /><meta name="description" content="亚洲第一SE情网站,高清国语自产精品视频二&

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cK1g5gckZR9VHjj.exe PID: 7160 Parent PID: 6012

General

Start time:	15:10:13
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe"
Imagebase:	0x8e0000
File size:	445440 bytes
MD5 hash:	5F19B9A3E41EF2E6EC3200BF4A246CEC
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: 00000000.00000002.357245488.0000000002BD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.357490796.0000000002C9A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.358483058.0000000003DF6000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.358483058.0000000003DF6000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.358483058.0000000003DF6000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cK1g5gckZR9VHjj.exe PID: 1312 Parent PID: 7160

General

Start time:	15:10:16
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
Imagebase:	0x2f0000
File size:	445440 bytes
MD5 hash:	5F19B9A3E41EF2E6EC3200BF4A246CEC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: cK1g5gckZR9VHjj.exe PID: 6104 Parent PID: 7160

General

Start time:	15:10:18

Start date:	25/11/2021
Path:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe
Imagebase:	0x560000
File size:	445440 bytes
MD5 hash:	5F19B9A3E41EF2E6EC3200BF4A246CEC
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: 00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.354564190.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.355165380.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.355165380.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.355165380.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.433824497.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.433824497.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.433824497.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.434217315.0000000000F80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.434217315.0000000000F80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.434217315.0000000000F80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.434604641.00000000012F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.434604641.00000000012F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.434604641.00000000012F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6104

General

Start time:	15:10:20
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: 00000005.00000000.407619289.000000000E6B1000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.407619289.000000000E6B1000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.407619289.000000000E6B1000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.392202181.000000000E6B1000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.392202181.000000000E6B1000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.392202181.000000000E6B1000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: netsh.exe PID: 6904 Parent PID: 3440

General

Start time:	15:10:53
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x9e0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 0000000C.00000002.612178801.00000000033D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.612178801.00000000033D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.612178801.00000000033D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.611462047.0000000003090000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.611462047.0000000003090000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.611462047.0000000003090000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.611332367.0000000002DC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.611332367.0000000002DC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.611332367.0000000002DC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6900 Parent PID: 6904

General

Start time:	15:10:57
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\cK1g5gckZR9VHjj.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6992 Parent PID: 6900

General

Start time:	15:10:58
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis