ID: 830326
Sample Name: 7pECKdsaig.exe
Cookbook: default.jbs
Time: 09:10:07
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report 7pECKdsaig.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Initial Sample 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Networking 8
E-Banking Fraud 8
System Summary 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 11
URLs 12
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 18
Public IPs 18
General Information 18
Warnings 19
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 19
IPs 19
Domains 19
ASNs 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
C:\Users\user\AppData\Local\Microsoft\PenWorkspace\DiscoverCacheData.dat 20
Static File Info 20
General 20
File Icon 20
Static PE Info 21
General 21
Entrypoint Preview 21
Rich Headers 22
Data Directories 22
Sections 23
Network Behavior 23
Snort IDS Alerts 23
Network Port Distribution 23
TCP Packets 23
UDP Packets 24
DNS Queries 24
DNS Answers 24

HTTP Request Dependency Graph 24
Code Manipulations 25
User Modules 25
Hook Summary 25
Processes 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: 7pECKdsaig.exePID: 6000, Parent PID: 3452 25
General 25
File Activities 26
Analysis Process: explorer.exePID: 3452, Parent PID: 6000 26
General 26
File Activities 27
Registry Activities 27
Analysis Process: msdt.exePID: 5148, Parent PID: 3452 27
General 27
File Activities 28
File Read 28
Analysis Process: cmd.exePID: 1328, Parent PID: 5148 28
General 28
File Activities 29
Analysis Process: conhost.exePID: 3660, Parent PID: 1328 29
General 29
Disassembly 29

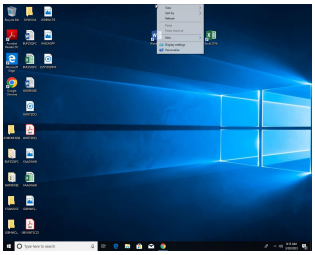
Windows Analysis Report

7pECKdsaig.exe

Overview

General Information

Sample Name:	7pECKdsaig.exe
Original Sample Name:	3343ba4097fe8..
Analysis ID:	830326
MD5:	515bf958f062fe..
SHA1:	50fbaeb36e983..
SHA256:	3343ba4097fe8..
Tags:	exe Formbook
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

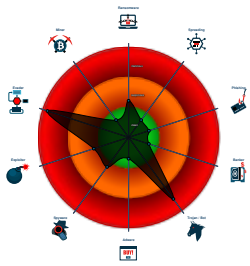
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- 7pECKdsaig.exe (PID: 6000 cmdline: C:\Users\user\Desktop\7pECKdsaig.exe MD5: 515BF958F062FEC724FBE6BDADF39485)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - msdt.exe (PID: 5148 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
      - cmd.exe (PID: 1328 cmdline: /c del "C:\Users\user\Desktop\7pECKdsaig.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 3660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.2348x.com/ar73/"
  ],
  "decoy": [
    "classgorilla.com",
    "b6817.com",
    "1wwuwa.top",
    "dgslimited.africa",
    "deepwaterships.com",
    "hkshshoptw.shop",
    "hurricanevalleyatvjamboree.com",
    "ckpconsulting.com",
    "laojiangmath.com",
    "authenticityhacking.com",
    "family-doctor-53205.com",
    "investinstgeorgeut.com",
    "lithoearthsolution.africa",
    "quickhealcareltd.co.uk",
    "delightkgrillw.top",
    "freezeclosettoilet.com",
    "coo1star.com",
    "gemgamut.com",
    "enrichednetworksolutions.com",
    "betterbeeclean.com",
    "kbmstr.com",
    "colorusainc.com",
    "five-dollar-meals.com",
    "baozhuang8.com",
    "la-home-service.com",
    "innovantexclusive.com",
    "chateaudevillars.co.uk",
    "echadholisticbar.com",
    "naijacarprices.africa",
    "4652.voto",
    "kraftheonz.com",
    "ingrambaby.com",
    "braeunungsoel.ch",
    "sweetcariadgifts.co.uk",
    "kui693.com",
    "akatov-top.ru",
    "epollresearch.online",
    "cupandsaucybooks.com",
    "arredobagno.club",
    "gt.sale",
    "dskincare.com",
    "cursosemcasa.site",
    "leaf-spa.net",
    "deathbeforedeceit.com",
    "azvvs.com",
    "laptops-39165.com",
    "ccwt.vip",
    "011965.com",
    "mtevz.online",
    "jacksontcpassettlement.com",
    "aldeajerusalen.com",
    "kellnovaglobalfood.info",
    "alphametatek.online",
    "lcssthh.com",
    "dumelogold9ja.africa",
    "d-storic.com",
    "mogi.africa",
    "ghostt.net",
    "aksharsigns.online",
    "goglucofort.com",
    "b708.com",
    "controlplus.systems",
    "lightandstory.info",
    "invstcai.sbs"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
7pECKdsaig.exe	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
7pECKdsaig.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7pECKdsaig.exe	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5651:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bfb0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9dbf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14ca7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
7pECKdsaig.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8d08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8f72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14aa5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14591:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14ba7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14d1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x998a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1380c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa683:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ad17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bd1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7pECKdsaig.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17c39:$sqlite3step: 68 34 1C 7B E1 • 0x17d4c:$sqlite3step: 68 34 1C 7B E1 • 0x17c68:$sqlite3text: 68 38 2A 90 C5 • 0x17d8d:$sqlite3text: 68 38 2A 90 C5 • 0x17c7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17da3:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.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:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x148a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.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:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17839:$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

Click to see the 48 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.7pECKdsaig.exe.a80000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
0.2.7pECKdsaig.exe.a80000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.7pECKdsaig.exe.a80000.0.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
0.2.7pECKdsaig.exe.a80000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
0.2.7pECKdsaig.exe.a80000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$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
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.634.102.136.18049707802031453 03/20/23-09:12:27.000047
SID:	2031453
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.634.102.136.18049707802031449 03/20/23-09:12:27.000047
SID:	2031449
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.6 - Destination IP: 34.102.136.180

Timestamp:	192.168.2.634.102.136.18049707802031412 03/20/23-09:12:27.000047
SID:	2031412
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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)

Stealing of Sensitive Information

Yara detected FormBook

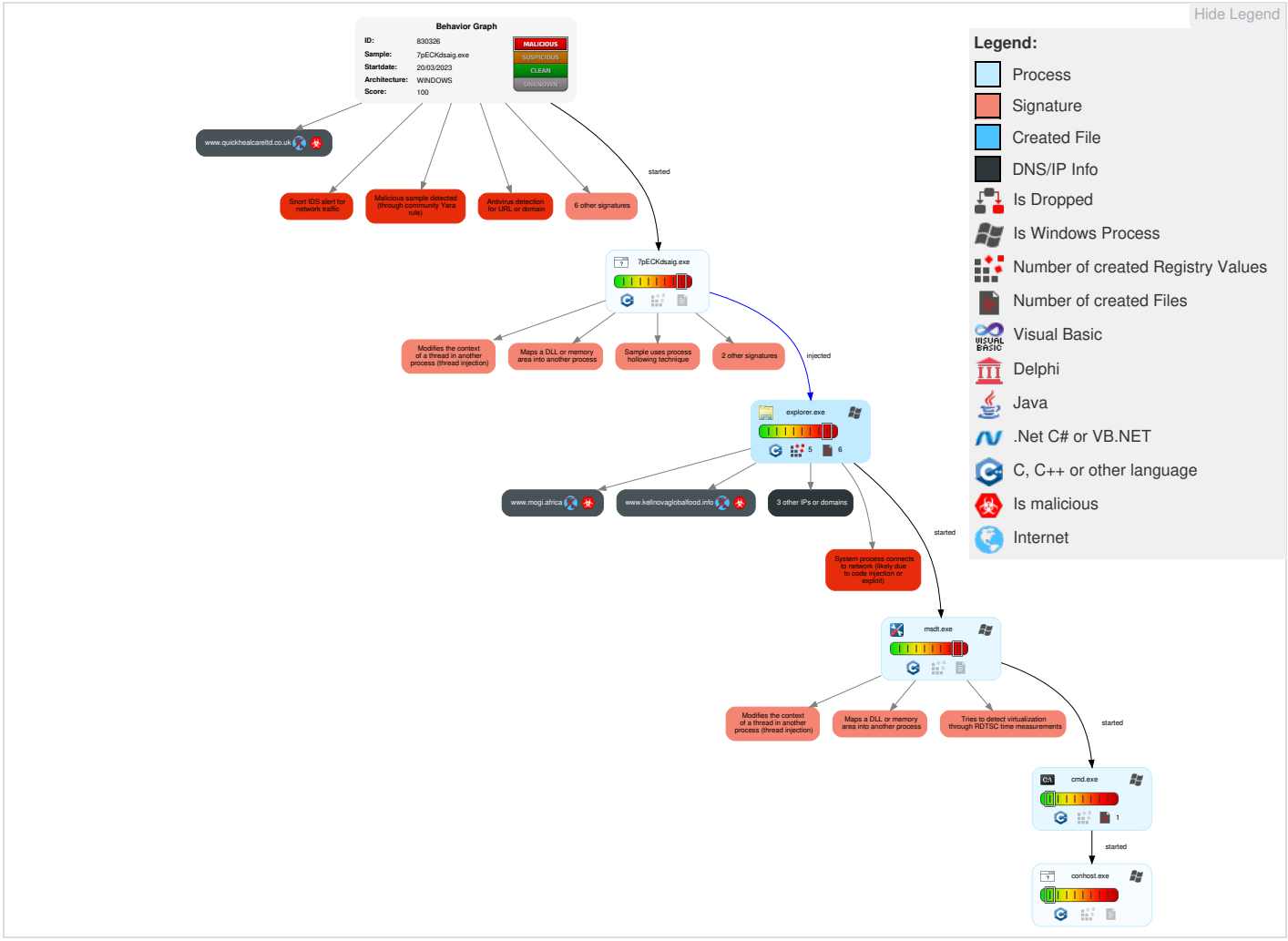
Remote Access Functionality

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	5 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 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	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	5 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Remote System 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	4 Obfuscated Files or Information	Cached Domain Credentials	1 1 System Information 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 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

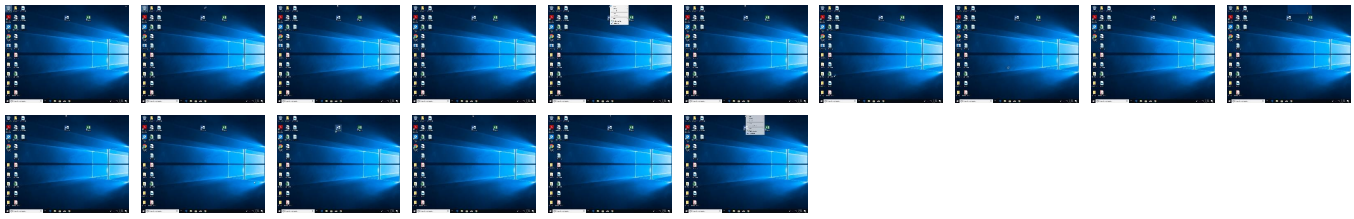
Behavior Graph



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
7pECKdsaig.exe	77%	ReversingLabs	Win32.Trojan.FormBook	
7pECKdsaig.exe	59%	Virustotal		Browse
7pECKdsaig.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
7pECKdsaig.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.7pECKdsaig.exe.a80000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.7pECKdsaig.exe.a80000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.quickhealcareltd.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jacksontcpassettlement.com/ar73/www.ingrambaby.com	100%	Avira URL Cloud	malware	
http://www.b708.com/ar73/	100%	Avira URL Cloud	malware	
http://www.ckpconsulting.com	0%	Avira URL Cloud	safe	
http://www.kellnovaglobalfood.infoReferer:	0%	Avira URL Cloud	safe	
http://www.innovantexclusive.comReferer:	0%	Avira URL Cloud	safe	
http://www.jacksontcpassettlement.comReferer:	0%	Avira URL Cloud	safe	
http://www.hurricanevalleyatvjamboree.com/ar73/www.innovantexclusive.com	100%	Avira URL Cloud	malware	
http://www.kellnovaglobalfood.info/ar73/	100%	Avira URL Cloud	malware	
http://www.2348x.com	0%	Avira URL Cloud	safe	
http://www.echadholisticbar.com/ar73/www.jacksontcpassettlement.com	100%	Avira URL Cloud	malware	
http://www.controlplus.systems	0%	Avira URL Cloud	safe	
http://www.quickhealcareltd.co.uk/ar73/	100%	Avira URL Cloud	malware	
http://www.mogi.africa/ar73/www.kellnovaglobalfood.info	100%	Avira URL Cloud	malware	
http://www.ckpconsulting.com/ar73/www.2348x.com	100%	Avira URL Cloud	malware	
http://www.kellnovaglobalfood.info/ar73/www.controlplus.systems	100%	Avira URL Cloud	malware	
http://www.controlplus.systems/ar73/www.quickhealcareltd.co.uk	100%	Avira URL Cloud	malware	
http://www.mogi.africaReferer:	0%	Avira URL Cloud	safe	
http://www.kellnovaglobalfood.info/ar73/?Qj=i6BPGBhEPZBlfl7tAP1UBBwzioJGNNDALkR90REkFgMzqoaCb5EMO/kcO5kV95GeH/kMM6gDFg==&x6=n0GdIP_	100%	Avira URL Cloud	malware	
http://www.ckpconsulting.comReferer:	0%	Avira URL Cloud	safe	
http://www.b708.comReferer:	0%	Avira URL Cloud	safe	
http://www.quickhealcareltd.co.ukReferer:	0%	Avira URL Cloud	safe	
http://www.ckpconsulting.com/ar73/	100%	Avira URL Cloud	malware	
http://www.mtevz.online/ar73/	100%	Avira URL Cloud	malware	
http://www.2348x.com/ar73/	100%	Avira URL Cloud	malware	
http://www.kellnovaglobalfood.info	0%	Avira URL Cloud	safe	
http://www.arredobagno.club/ar73/www.mtevz.online	100%	Avira URL Cloud	malware	
http://www.hurricanevalleyatvjamboree.com/ar73/	100%	Avira URL Cloud	malware	
http://www.ingrambaby.com/ar73/	100%	Avira URL Cloud	malware	
http://www.innovantexclusive.com/ar73/www.1wwuwa.top	100%	Avira URL Cloud	malware	
http://www.mogi.africa	0%	Avira URL Cloud	safe	
http://www.controlplus.systems/ar73/	100%	Avira URL Cloud	malware	
http://www.arredobagno.clubReferer:	0%	Avira URL Cloud	safe	
http://www.echadholisticbar.com/ar73/	100%	Avira URL Cloud	malware	
http://www.1wwuwa.top	0%	Avira URL Cloud	safe	
http://www.ingrambaby.com	0%	Avira URL Cloud	safe	
http://www.jacksontcpassettlement.com/ar73/	100%	Avira URL Cloud	malware	
http://www.authenticityhacking.com/ar73/	100%	Avira URL Cloud	malware	
http://www.ingrambaby.com/ar73/www.arredobagno.club	100%	Avira URL Cloud	malware	
http://www.hurricanevalleyatvjamboree.com	0%	Avira URL Cloud	safe	
http://www.1wwuwa.topReferer:	0%	Avira URL Cloud	safe	
http://www.mogi.africa/ar73/	100%	Avira URL Cloud	malware	
http://www.echadholisticbar.comReferer:	0%	Avira URL Cloud	safe	
http://www.arredobagno.club/ar73/	100%	Avira URL Cloud	malware	
http://www.mtevz.onlineReferer:	0%	Avira URL Cloud	safe	
http://www.authenticityhacking.comReferer:	0%	Avira URL Cloud	safe	
http://www.b708.com	0%	Avira URL Cloud	safe	
http://www.quickhealcareltd.co.uk	0%	Avira URL Cloud	safe	
http://www.innovantexclusive.com	0%	Avira URL Cloud	safe	
http://www.jacksontcpassettlement.com	0%	Avira URL Cloud	safe	
http://www.1wwuwa.top/ar73/www.echadholisticbar.com	100%	Avira URL Cloud	malware	
http://www.ingrambaby.comReferer:	0%	Avira URL Cloud	safe	
http://www.hurricanevalleyatvjamboree.comReferer:	0%	Avira URL Cloud	safe	
http://www.b708.com/ar73/www.hurricanevalleyatvjamboree.com	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.2348x.comReferer:	0%	Avira URL Cloud	safe	
http://www.controlplus.systemsReferer:	0%	Avira URL Cloud	safe	
http://www.controlplus.systems/ar73/?Qj=pTDthzaqblgyWHdtpzpwnulvL2qvi2wcQCOYQZrmaB3EJlnnV9x+gp8AnzNn3ZLGsW0uMr4raA==&x6=n0GdIP_	100%	Avira URL Cloud	malware	
http://www.mtevz.online	0%	Avira URL Cloud	safe	
http://www.authenticityhacking.com/ar73/www.ckpconsulting.com	100%	Avira URL Cloud	malware	
http://www.mtevz.online/ar73/r	100%	Avira URL Cloud	malware	
http://www.2348x.com/ar73/www.b708.com	100%	Avira URL Cloud	malware	
www.2348x.com/ar73/	100%	Avira URL Cloud	malware	
http://www.echadholisticbar.com	0%	Avira URL Cloud	safe	
http://www.authenticityhacking.com	0%	Avira URL Cloud	safe	
http://www.1wwuwa.top/ar73/	100%	Avira URL Cloud	malware	
http://www.arredobagno.club	0%	Avira URL Cloud	safe	
http://www.quickhealcareltd.co.uk/ar73/www.authenticityhacking.com	100%	Avira URL Cloud	malware	
http://www.innovantexclusive.com/ar73/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
controlplus.systems	34.102.136.180	true	false		unknown
kellnovaglobalfood.info	34.102.136.180	true	false		unknown
www.quickhealcareltd.co.uk	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.mogi.africa	unknown	unknown	true		unknown
www.kellnovaglobalfood.info	unknown	unknown	true		unknown
www.controlplus.systems	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.kellnovaglobalfood.info/ar73/?Qj=i6BPGBhEPZBlfl7tAP1UBBwzioJGNNDALkR90REkFgMzqoaCb5EMO/kcO5kV95GeH/kMM6gDFg==&x6=n0GdIP_	false	• Avira URL Cloud: malware	unknown
http://www.controlplus.systems/ar73/?Qj=pTDthzaqblgyWHdtpzpwnulvL2qvi2wcQCOYQZrmaB3EJlnnV9x+gp8AnzNn3ZLGsW0uMr4raA==&x6=n0GdIP_	false	• Avira URL Cloud: malware	unknown
www.2348x.com/ar73/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.b708.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.jacksontcpassettlement.com/ar73/www.ingrambaby.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.innovantexclusive.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mtevz.online/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ckpconsulting.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jacksontcpassettlement.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kellnovaglobalfood.infoReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hurricanevalleyatvjamboree.com/ar73/www.innovantexclusive.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.kellnovaglobalfood.info/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.2348x.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ckpconsulting.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.2348x.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.controlplus.systems	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.echadholisticbar.com/ar73/www.jacksontcpassettlement.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mogi.africa/ar73/www.kellnovaglobalfood.info	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.quickhealcareltd.co.uk/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ckpconsulting.com/ar73/www.2348x.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.kellnovaglobalfood.info/ar73/www.controlplus.systems	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.controlplus.systems/ar73/www.quickhealcareltd.co.uk	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.b708.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

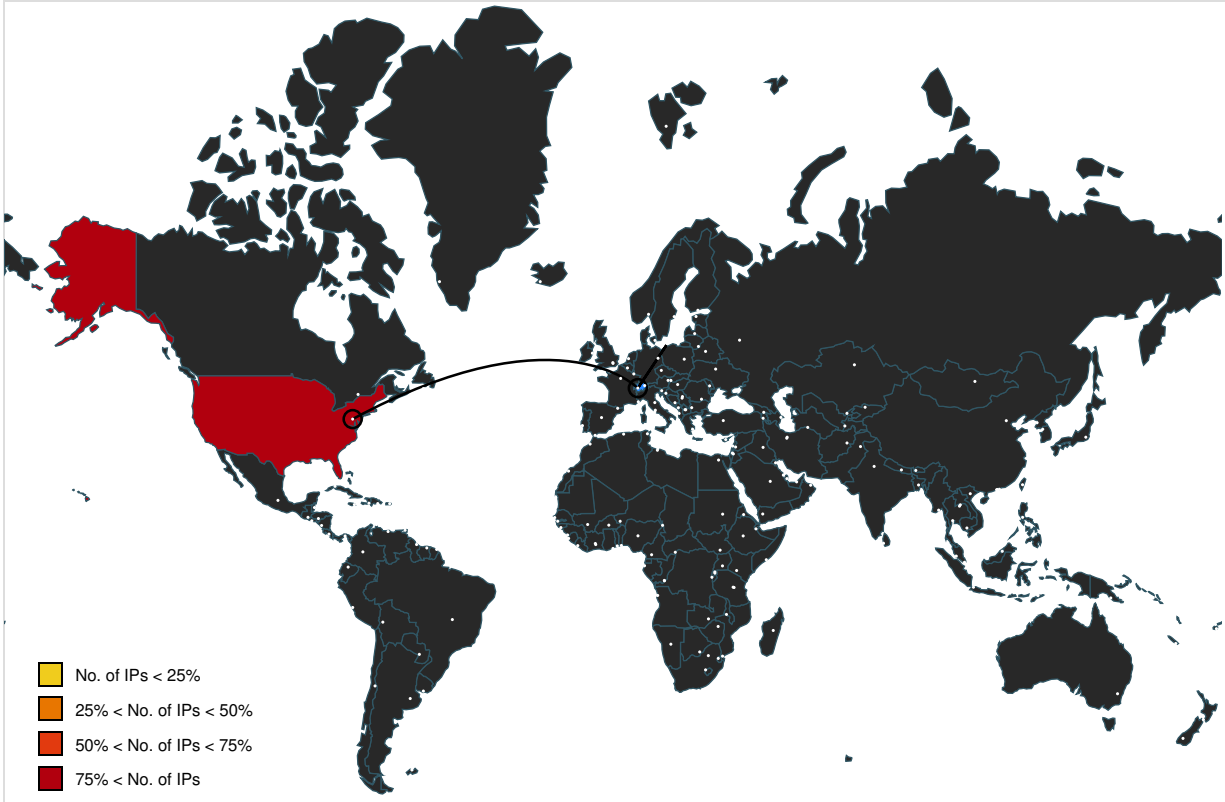
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mogi.africaReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quickhealcareltd.co.ukReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ckpconsulting.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hurricanevalleyatvjamboree.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.arredobagno.club/ar73/www.mtevz.online	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ingrambaby.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.kellnovaglobalfood.info	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mogi.africa	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.innovantexclusive.com/ar73/www.1wwuwa.top	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.controlplus.systems/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.jacksontcpassettlement.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.arredobagno.clubReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000003.46164944 8.0000000008442000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.292213498.000000000F5A7000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.461216185.000000 000F53F000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000001.0000 0000.267709513.000000000F5A7000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000003.462393796.000000000F5B30 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.254183869.000 0000000AC8000.00000004.00000020.00020000 .00000000.sdmp, explorer.exe, 00000001.0 0000003.289061192.0000000008442000.00000 004.00000001.00020000.00000000.sdmp, exp lorer.exe, 00000001.00000002.526453234.0 000000008442000.00000004.00000001.000200 00.00000000.sdmp, explorer.exe, 00000001 .00000002.517440543.0000000000AC8000.000 00004.00000020.00020000.00000000.sdmp, e xplorer.exe, 00000001.00000002.530310030 .000000000F5B6000.00000004.00000001.0002 0000.00000000.sdmp, explorer.exe, 000000 01.00000003.288711256.000000000F5A7000.0 0000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.2637358 95.0000000008442000.00000004.00000001.00 020000.00000000.sdmp	false		high
http://www.echadholisticbar.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ingrambaby.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1wwuwa.top	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.authenticityhacking.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.ingrambaby.com/ar73/www.arredobagno.club	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.hurricanevalleyatvjamboree.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1wwuwa.topReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mogi.africa/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.authenticityhacking.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.arredobagno.club/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.echadholisticbar.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.mtevz.onlineReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.b708.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quickhealcareltd.co.uk	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.innovantexclusive.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jacksontcpassettlement.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1wwuwa.top/ar73/www.echadholisticbar.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.hurricanevalleyatvjamboree.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ingrambaby.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.controlplus.systemsReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.authenticityhacking.com/ar73/www.ckpconsulting.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.b708.com/ar73/www.hurricanevalleyatvjamboree.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mtevz.online	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.2348x.comReferer:	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.2348x.com/ar73/www.b708.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.mtevz.online/ar73/r	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.authenticityhacking.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.1wwuwa.top/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.echadholisticbar.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quickhealcareltd.co.uk/ar73/www.authenticityhacking.com	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.arredobagno.club	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.innovantexclusive.com/ar73/	explorer.exe, 00000001.00000002.52571354 6.000000000833A000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 001.00000003.461649448.0000000008356000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	controlplus.systems	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl

Analysis ID:	830326
Start date and time:	2023-03-20 09:10:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	15
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
Sample file name:	7pECKdsaig.exe
Original Sample Name:	3343ba4097fe8b6b91af0ca46abb0baf6052acf1806571432cc7e9e0ba59fa2a.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/1@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 66.3% (good quality ratio 61%) • Quality average: 71.7% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:11:24	API Interceptor	563x Sleep call for process: explorer.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\PenWorkspace\DiscoverCacheData.dat

Process:	C:\Windows\explorer.exe
File Type:	JSON data
Category:	dropped
Size (bytes):	984
Entropy (8bit):	5.204081515204597
Encrypted:	false
SSDEEP:	24:Yq6CUXyhmQmnbNdB6hmxjmnz0JahmemnHZ6T06MhmDmnbxdB6hmktmn7KTdB6hm0:YqDUXyctnbNdUcAnz0JacPnHZ6T06McW
MD5:	160494591DCB3DD4E2C36F71207A87F3
SHA1:	D611935CA91C155B10A449DB72B3D5C8308A6EB7
SHA-256:	B82EC6928AAA7C30ABBE26DF13CA514DC4508C704F03EB28A4B2ABE40F60DF6E
SHA-512:	301BD7B6A4B7B2D3261C3A10FE98B2B4B811B861FCA077AF8732B7FCDFB2D106FFE82F0072CD859A4436E2EBD9347EACF44539E11AEAD2CA83703737B3030881
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"RecentItems":[{"AppID":"Microsoft.Office.OneNote_8wekyb3d8bbwe!microsoft.onenoteim","PenUsageSec":15,"LastSwitchedLowPart":3648731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.WindowsMaps_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3638731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.MSPaint_8wekyb3d8bbwe!Microsoft.MSPaint","PenUsageSec":15,"LastSwitchedLowPart":3628731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.MicrosoftEdge_8wekyb3d8bbwe!MicrosoftEdge","PenUsageSec":15,"LastSwitchedLowPart":3618731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.Windows.Photos_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3608731648,"LastSwitchedHighPart":30747937,"PrePopulated":true},{"AppID":"Microsoft.Getstarted_8wekyb3d8bbwe!App","PenUsageSec":15,"LastSwitchedLowPart":3598731648,"LastSwitchedHighPart":30747937,"PrePopulated":true}]}

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.393944417418745
TrID:	• Win32 Executable (generic) a (10002005/4) 99.98% • DOS Executable Generic (2002/1) 0.02%
File name:	7pECKdsaig.exe
File size:	185856
MD5:	515bf958f062fec724fbe6bdadf39485
SHA1:	50fbaeb36e98338dc500e252855abf0152bb6bbf
SHA256:	3343ba4097fe8b6b91af0ca46abb0baf6052acf1806571432cc7e9e0ba59fa2a
SHA512:	9b336130dc79e9dba0bdba735cc780c4c39148ca38668f660a6b6b15aeb0b8111a687ac4111a7c0bb84663b7c3ba963cefbf8fe4b4e4777fb5394b91d2272ed6
SSDEEP:	3072:F3k9Eu2PDPlFm3TiZHhJmoapMZRrr9d+/eqeibwnFUMGBY8:MkQTeHlaGZRX9K4XeY8
TLSH:	8904BF32D602C071F2B211B5F67D1B7B493D0E343295A4EAA7A225E06EF09E5B53931F
File Content Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....f...f...f.....f.....f.....f.Rich..f.....PE..L....i.?.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0xfdf140
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0xfc0000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x3F0769F8 [Sun Jul 6 00:14:48 2003 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 64h
call 00007FDF6CAC6D4Ah
mov esp, ebp
pop ebp
ret
call 00007FDF6CACA535h
pop eax
ret
call 00007FDF6CACA535h
pop eax
ret
call 00007FDF6CAC6D93h
ret
call 00007FDF6CACA535h
pop eax
ret
jmp 00007FDF6CAC6DF6h
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8764h
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8767h
ret
call 00007FDF6CACA535h
pop eax
ret

Instruction
push 88888888h
jmp 00007FDF6CAC876Ah
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC876Dh
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8770h
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8773h
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8776h
ret
call 00007FDF6CACA535h
pop eax
ret
push 88888888h
jmp 00007FDF6CAC8779h
ret
call 00007FDF6CACA535h
pop eax
ret

Rich Headers

Programming Language:	• [C++] VS2010 SP1 build 40219 • [ASM] VS2010 SP1 build 40219 • [LNK] VS2010 SP1 build 40219

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

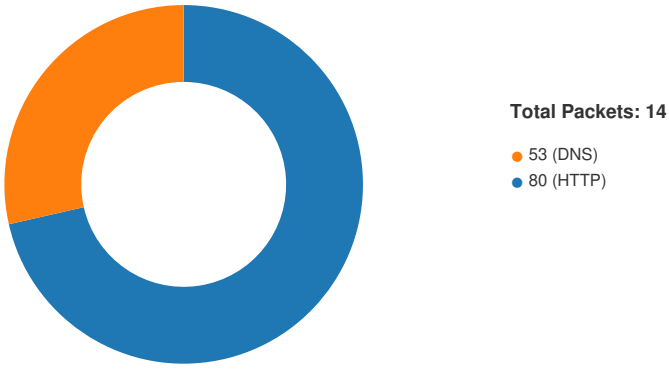
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d1a4	0x2d200	False	0.7623950398199446	data	7.409588215160137	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.634.102.136.18049707802031453 03/20/23-09:12:27.000047	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	34.102.136.180
192.168.2.634.102.136.18049707802031449 03/20/23-09:12:27.000047	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	34.102.136.180
192.168.2.634.102.136.18049707802031412 03/20/23-09:12:27.000047	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.6	34.102.136.180

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:12:26.979583979 CET	49707	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:26.998944998 CET	80	49707	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:26.999897003 CET	49707	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:27.000046968 CET	49707	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:27.019110918 CET	80	49707	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:27.245915890 CET	80	49707	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:27.245950937 CET	80	49707	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:27.246295929 CET	49707	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:27.246371031 CET	49707	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:27.263668060 CET	80	49707	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:47.472598076 CET	49708	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:47.490624905 CET	80	49708	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:47.490818977 CET	49708	80	192.168.2.6	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:12:47.491030931 CET	49708	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:47.508877993 CET	80	49708	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:47.672036886 CET	80	49708	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:47.672099113 CET	80	49708	34.102.136.180	192.168.2.6
Mar 20, 2023 09:12:47.672249079 CET	49708	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:47.672713995 CET	49708	80	192.168.2.6	34.102.136.180
Mar 20, 2023 09:12:47.690121889 CET	80	49708	34.102.136.180	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:12:03.883550882 CET	49786	53	192.168.2.6	8.8.8.8
Mar 20, 2023 09:12:04.092940092 CET	53	49786	8.8.8.8	192.168.2.6
Mar 20, 2023 09:12:26.905668974 CET	58595	53	192.168.2.6	8.8.8.8
Mar 20, 2023 09:12:26.958081961 CET	53	58595	8.8.8.8	192.168.2.6
Mar 20, 2023 09:12:47.423398018 CET	56331	53	192.168.2.6	8.8.8.8
Mar 20, 2023 09:12:47.469249010 CET	53	56331	8.8.8.8	192.168.2.6
Mar 20, 2023 09:13:18.738394976 CET	50506	53	192.168.2.6	8.8.8.8
Mar 20, 2023 09:13:18.759357929 CET	53	50506	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:12:03.883550882 CET	192.168.2.6	8.8.8.8	0xb81b	Standard query (0)	www.mogi.africa	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:26.905668974 CET	192.168.2.6	8.8.8.8	0x6157	Standard query (0)	www.kellnovaglobalfood.info	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:47.423398018 CET	192.168.2.6	8.8.8.8	0xddbb	Standard query (0)	www.controlplus.systems	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:18.738394976 CET	192.168.2.6	8.8.8.8	0x9ab2	Standard query (0)	www.quickhealcareltd.co.uk	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 09:12:04.092940092 CET	8.8.8.8	192.168.2.6	0xb81b	Server failure (2)	www.mogi.africa	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:26.958081961 CET	8.8.8.8	192.168.2.6	0x6157	No error (0)	www.kellnovaglobalfood.info	kellnovaglobalfood.info		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:12:26.958081961 CET	8.8.8.8	192.168.2.6	0x6157	No error (0)	kellnovaglobalfood.info		34.102.136.180	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:47.469249010 CET	8.8.8.8	192.168.2.6	0xddbb	No error (0)	www.controlplus.systems	controlplus.systems		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:12:47.469249010 CET	8.8.8.8	192.168.2.6	0xddbb	No error (0)	controlplus.systems		34.102.136.180	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:18.759357929 CET	8.8.8.8	192.168.2.6	0x9ab2	Name error (3)	www.quickhealcareltd.co.uk	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.kellnovaglobalfood.info
- www.controlplus.systems

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

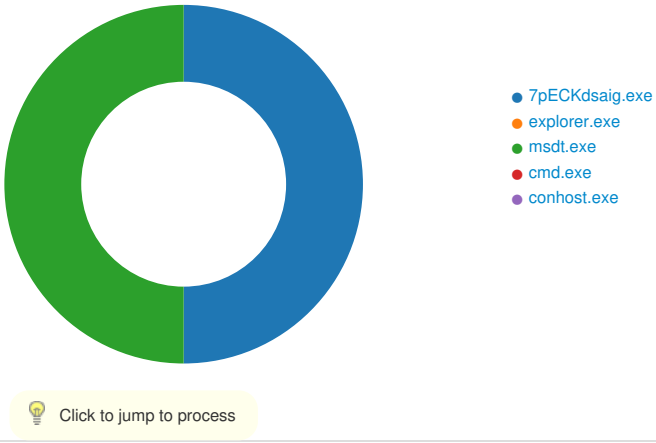
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xE1

Statistics

Behavior



System Behavior

Analysis Process: 7pECKdsaig.exe PID: **6000**, Parent PID: **3452**

General

Target ID:	0
Start time:	09:11:04
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\7pECKdsaig.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\7pECKdsaig.exe
Imagebase:	0xa80000
File size:	185856 bytes
MD5 hash:	515BF958F062FEC724FBE6BDADF39485
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.288830411.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.289101701.0000000001370000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.289101701.0000000001370000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.289101701.0000000001370000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.289101701.0000000001370000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.289101701.0000000001370000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000002.289007135.0000000001210000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.289007135.0000000001210000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.289007135.0000000001210000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.289007135.0000000001210000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.289007135.0000000001210000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000000.00000000.249149614.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.249149614.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000000.249149614.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.249149614.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.249149614.0000000000A81000.00000020.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: explorer.exe PID: **3452**, Parent PID: **6000**

General

Target ID:	1
Start time:	09:11:06
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
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_1, Description: Yara detected FormBook, Source: 00000001.00000002.531047978.000000001389F000.00000004.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.531047978.000000001389F000.00000004.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.531047978.000000001389F000.00000004.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.531047978.000000001389F000.00000004.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.531047978.000000001389F000.00000004.80000000.00040000.00000000.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	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: msdt.exe PID: **5148**, Parent PID: **3452**

General

Target ID:	2
Start time:	09:11:16
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xb60000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.520351827.0000000004FCF000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.520351827.0000000004FCF000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.520351827.0000000004FCF000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.520351827.0000000004FCF000.00000004.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.520351827.0000000004FCF000.00000004.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.518766538.0000000002EE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.518766538.0000000002EE0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.518766538.0000000002EE0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.518766538.0000000002EE0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.518766538.0000000002EE0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.518698032.0000000002EB0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.518698032.0000000002EB0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.518698032.0000000002EB0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.518698032.0000000002EB0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.518698032.0000000002EB0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.517165647.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.517165647.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.517165647.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.517165647.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.517165647.0000000000580000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000002.00000002.517610096.00000000008C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.517610096.00000000008C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000002.517610096.00000000008C4000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.517610096.00000000008C4000.00000004.00000020.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.517610096.00000000008C4000.00000004.00000020.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	59A447	NtReadFile

Analysis Process: cmd.exe PID: **1328**, Parent PID: **5148**

General

Target ID:	8
Start time:	09:11:25
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\7pECKdsaig.exe"
Imagebase:	0x1b0000
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: **3660**, Parent PID: **1328**

General

Target ID:	9
Start time:	09:11:25
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
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