ID: 620777
Sample Name: dK0SRzWoPq
Cookbook: default.jbs
Time: 08:11:01
Date: 05/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

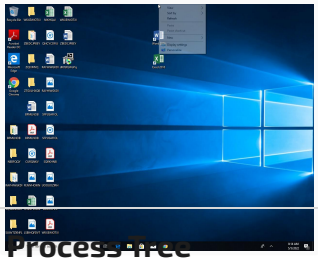
Windows Analysis Report

dK0SRzWoPq

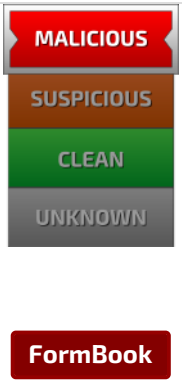
Overview

General Information

Sample Name:	dK0SRzWoPq (renamed file extension from none to exe)
Analysis ID:	620777
MD5:	6f111b596da1ac..
SHA1:	e09f8065342a4c..
SHA256:	285e772a15413a.
Tags:	32 exe Formbook trojan
Infos:	



Detection



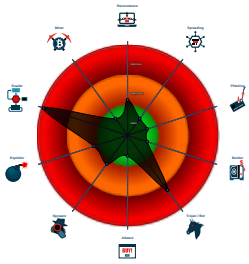
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- 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…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- dK0SRzWoPq.exe (PID: 772 cmdline: "C:\Users\user\Desktop\dK0SRzWoPq.exe" MD5: 6F111B596DA1AC7D71C4362B18309648)
  - pkypr.exe (PID: 1924 cmdline: C:\Users\user~1\AppData\Local\Temp\pkypr.exe C:\Users\user~1\AppData\Local\Temp\zpcthwca MD5: 087998162F8FBD6E48CC5AB45BE63449)
    - pkypr.exe (PID: 6380 cmdline: C:\Users\user~1\AppData\Local\Temp\pkypr.exe C:\Users\user~1\AppData\Local\Temp\zpcthwca MD5: 087998162F8FBD6E48CC5AB45BE63449)
      - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - autoconv.exe (PID: 5488 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
        - mstsc.exe (PID: 404 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
          - cmd.exe (PID: 7084 cmdline: /c del "C:\Users\user~1\AppData\Local\Temp\pkypr.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 6884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.hsf777.com/m0d4/"
  ],
  "decoy": [
    "prettyhairdivas.mobi",
    "cityblocksnft.com",
    "laraqiiz.com",
    "mubarakdigitalmedia.com",
    "perstockholm.com",
    "xn--imprio-dva.site",
    "baigouw.com",
    "support-client-video.com",
    "phomas.info",
    "dengedizayn.com",
    "zoommachone.xyz",
    "houseoflancasterhours.com",
    "petarungslot.website",
    "tyrs-it.com",
    "dalianzhuchiren.com",
    "tenthgenerationtorah.com",
    "portres.online",
    "1-minute.store",
    "shikakunazo.com",
    "veymes.store",
    "ruvedaj.xyz",
    "apremotesamsung.com",
    "palia.world",
    "you-sayso.com",
    "nftsofis.com",
    "arthamandirialkesindo.com",
    "bangkhacollections.com",
    "digitalfactoryinstitut.com",
    "aceites.info",
    "altcoinwatcher.com",
    "pearlsofgraceinc.com",
    "xianzyw.com",
    "gxclzs.com",
    "greenlighteams.com",
    "aavinya.com",
    "sans-gluten.store",
    "clanbeware.com",
    "protocolohfresco.site",
    "meredithlobrien.com",
    "cryoablation.xyz",
    "avicciibook.com",
    "toastpack.com",
    "linktosmutgoeshere.com",
    "38289.xyz",
    "xn--08s.com",
    "techkaisimi.com",
    "jllpx.com",
    "dubaicarclinic.com",
    "zhidao95.com",
    "aletterboxd.com",
    "warrantyglobe.com",
    "mindfeed.pro",
    "bhreselect.com",
    "sdfijsdjidf.xyz",
    "russetconstruction.com",
    "futternmitflo.com",
    "triumphgroup.xyz",
    "tn299td.com",
    "bulkheadsrestaurantgroup.com",
    "luvy.world",
    "h3s4.com",
    "gamewaycos.com",
    "totalbodyfit.online",
    "trendadler.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.625629256.00000000030F0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000D.00000002.625629256.00000000030F0000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.pkypr.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.pkypr.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.pkypr.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
2.2.pkypr.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.pkypr.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

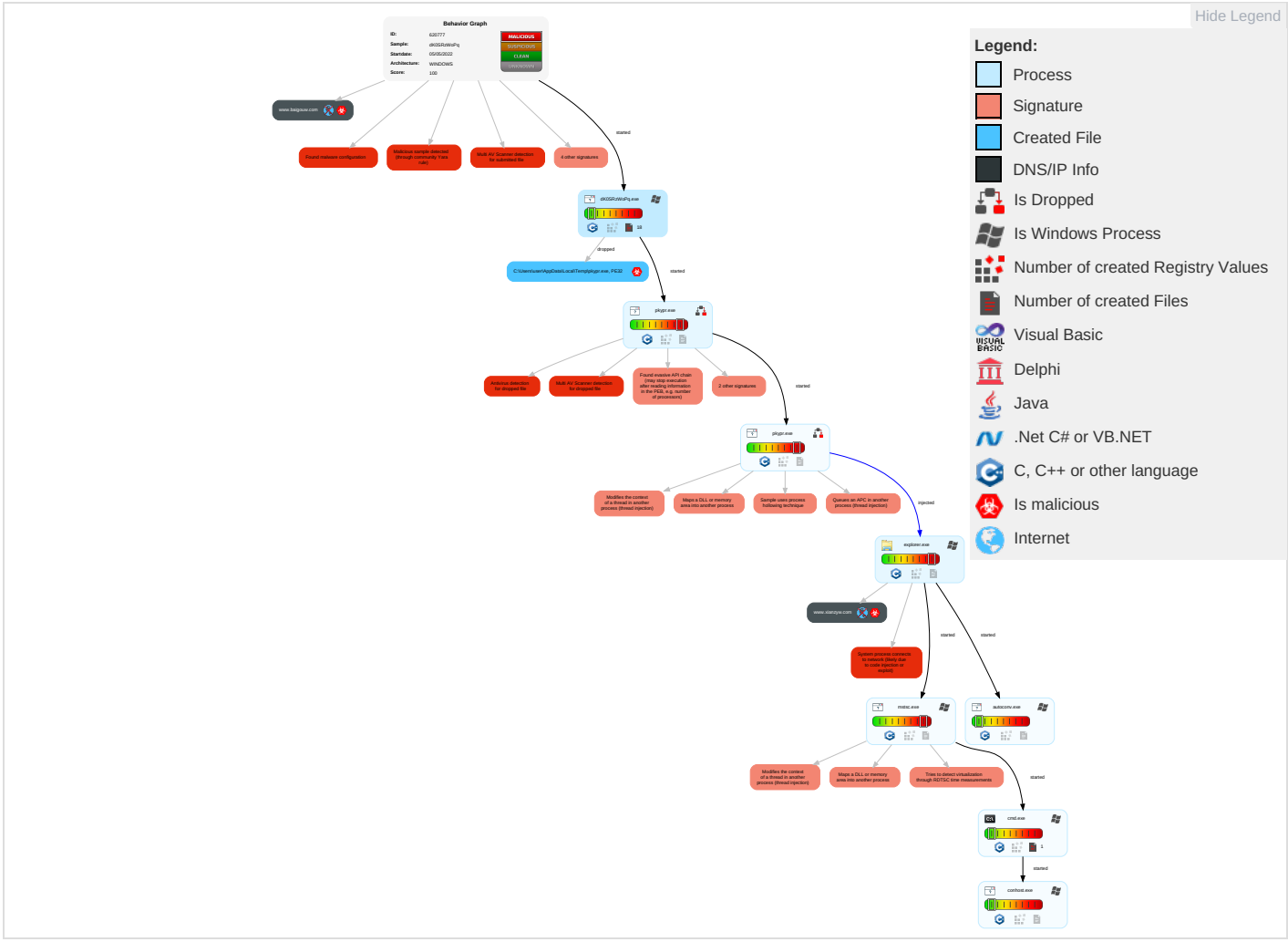
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Rootkit	1 Credential API Hooking	1 Query Registry	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	6 1 2 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	2 2 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Access Token Manipulation	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	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	3 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

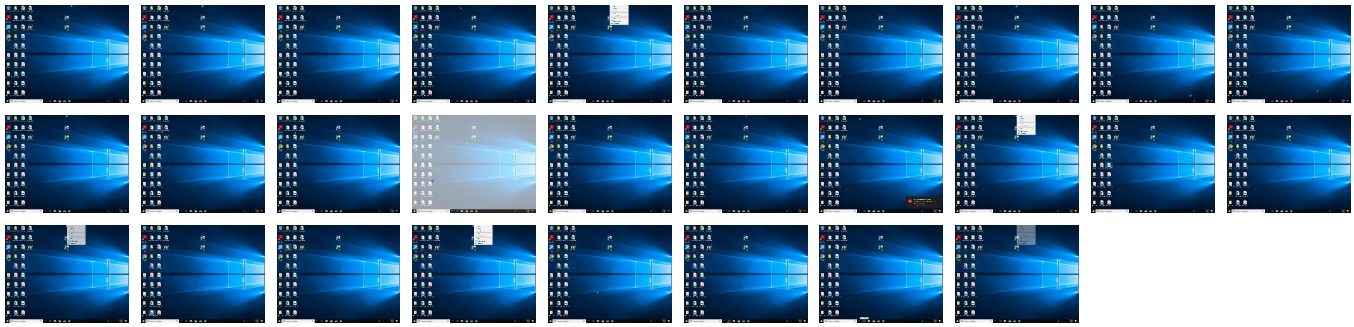
Behavior Graph



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
dK0SRzWoPq.exe	11%	Metadefender		Browse
dK0SRzWoPq.exe	62%	ReversingLabs	Win32.Trojan.LokiBot	
dK0SRzWoPq.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\pkypr.exe	100%	Avira	TR/Crypt.XPACK.Gen	
C:\Users\user\AppData\Local\Temp\pkypr.exe	44%	ReversingLabs	Win32.Trojan.FormBook	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.pkypr.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.pkypr.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.pkypr.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.pkypr.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.pkypr.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.pkypr.exe.2180000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.pkypr.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.hsf777.com/m0d4/	0%	Avira URL Cloud	safe	
http://ns.adobY	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.baigouw.com	unknown	unknown	true		unknown
www.xianzyw.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.hsf777.com/m0d4/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobY	explorer.exe, 00000003.00000000.42824371 9.00000000026D0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 003.00000000.375813124.00000000026D0000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000003.00000000.497440728.000000 00026D0000.00000004.00000001.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	dK0SRzWoPq.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620777
Start date and time: 05/05/202208:11:01	2022-05-05 08:11:01 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dK0SRzWoPq (renamed file extension from none to exe)
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/3@8/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 61.7% (good quality ratio 56.2%) • Quality average: 73.3% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.242.101.226, 40.125.122.176, 52.152.110.14, 20.54.89.106, 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.useroor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- VT rate limit hit for: dK0SRzWoPq.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ow7v8lrfalu0lz3762

Process:	C:\Users\user\Desktop\dK0SRzWoPq.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.990856274194596**
Encrypted:	**true**
SSDEEP:	3072:qjgrrRhrzo9SZLmQRZhGGa2S8nIpgjB7YwRMmcY/AoxGT4VWtKpZ6iejfz7nJ2v:q8rnrEwZCwZhGX4jB735cYLs484T8fze
MD5:	8E8024C9499E87104F27EA891A82C6A2
SHA1:	127BDF4C34CEB58C5562F86E83D1D2A085CDB5CF
SHA-256:	F11F0F6D81D98DD389B02D946FE8273591ADE4B3C7A6DA29820449EB392186FE
SHA-512:	95BE8BC870FDE8BA84728B2913B7B8A12999946DAFBE36D853662BD8D499783707F4EA1FC703D1489E244450FA1AC2BB7A93100F94794802C25B61C85FE332E
Malicious:	false
Reputation:	low
Preview:	.(3...B.'{^.....[7..r...Uu''...H:..&...".\.....-..f.....0....K....l.;l6]....|w.!..2."mX.....|.....`...m^.....>.L.@..f._[?.0..+N.pJ.~..0f.Y.])..!c.}._..;.....rSrl..F..YP.D..QSV.I.p.A....`.F.X<|S.\.T.. ....q.[X2.\....i=../Wq..a.....DPBb...B.]...g...~...6l...fg..Xb...H:..&..E".....-..f.....`:B...z.6....?d.X..F..A...l@F.y .m.U.....Is'(..k..m^.....7.....o..'j#.V..!ey.8d..$.y...}).]......n.. .n....rSr....t.YP....-.p..y..A]...`.FDX.d~.M.....q.[X.u.....i=0w/Wq..a.....DHB....B....g...c8..^l...fg..''...H:..&...".\.....-..f.....`:B...z.6....?d.X..F..A...l@F.y .m.U.....Is'(..k..m^ .....7.....o..'j#.V..!ey.8d..$.y...}).]......n...n....rSrl..F..YP4...-.p....A....`.FDX.d~.M.T.....q.[X.u.....i=0w/Wq..a.....DHB....B....g...c8..^l...fg..''...H:..&...".\.....-..f.....`:B...z.6....? d.X..F..A...l@F.y .m.U.....Is'(..k..m^.....7.....o..'j#.V..!ey.8d..$.y...}).]......n...n....rSrl..F..YP4...-.p....A....`.FDX.d~.M.T.....q.[X

C:\Users\user\AppData\Local\Temp\pkypr.exe

Process:	C:\Users\user\Desktop\dK0SRzWoPq.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	5120
Entropy (8bit):	3.9183606087237455
Encrypted:	false
SSDEEP:	48:Sp9jcdkOF5gKcByqcQigXUgdSHgeUAZ+hRP2bv0D4LS0MK0w/fcefhrRVRuqS:Ut8gVBy1TgXUgdSHgxG2K0w/ke5rpx
MD5:	087998162F8FBD6E48CC5AB45BE63449
SHA1:	42A743C81B789EAF9B3283FFA8ADBB90A4519362
SHA-256:	99B049D5615612C79DA226823C3B8D173E66E73BB1C99D0215282274685162ED
SHA-512:	12759E3CCAFF2A3D78A5008E6F96C01322EE814F0568142E09DBE0DDF30DF84C0843CAF43C34377660103CACB636ABA68F60A6903A52EFD0EBC50AB5C41967 D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 44%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;....I.J.I.J.I.J.s.J}I.J$..Kpl.J.I.JTl.J.2.K~I.J.2fJ~I.J.2.K~I.JRich.I.J .....PE..L...4prb..... ....@.....P.....!.....@..... ....text..... ..`.rdata..... .....@..@.data.....0.....@....rsrc.....@.....@..@..... ....

C:\Users\user\AppData\Local\Temp\zpcthwca

Process:	C:\Users\user\Desktop\dK0SRzWoPq.exe
File Type:	data
Category:	dropped
Size (bytes):	4971
Entropy (8bit):	6.173518476087677
Encrypted:	false
SSDEEP:	96:FmmPpZ4KuDlgjOBPv4LSuhQB2DwXQH4xShcJbfP:FmrojsqBDjYEhij
MD5:	B1BAABAF50759D3CFC8D19D3D2E20F94
SHA1:	20983C521DB67C60E18A94D31C2B41CEB2A5D7F2
SHA-256:	1FBFC239148369ED5BD7713E21CF351A45F784CB79C71EC101CF31B037F58E9C
SHA-512:	47255B15D381F1C2DFFAB6FA561E758901116A115B73029CFFC15F3252B2843CA2517199968101BB816F4B89E4AA592A78B794108E85536603CE1F60456C96F2
Malicious:	false

Preview:	.....%....@/*+.U...+.Z..5..+.Z..5..U...5.(....U...E..E.}5.0.....5..%..E..E.}5.0.....5..%..E..E.}5.0.....5.%..E..E.}5.0.....5..%..M..J.f.8g...5.q.5..%.5.....5.=.5.=.}....f.1..5..%.}...5. +*.U....f.....'U..E.1.E.6.E.Y8.E.Y1.E.3.E.2u.L.[H...[H.D. ...E..E.Y6.5....5..U.....<.....U.23.5.327....%..II.+.Z..5.5....5.O .5....=....<...%.5.5...@.=....5.%.....h..S.N....h.. ....hZ.S.`....*.....h.4wS.B....<.....%....(.+.Z..5.5.....}5..5..M..L.5....5.@.5.5.H.5....H...u.L:.5.qf.1g...<...,..}5.qf.1....<...,..f.f.8g..}<..0hZ.S.....0....5...}5.0.E..F...5..M..L..U.....5..... 5.....%....@.+.Z..5.5.(...}5..5..M..L.5....5.@.5.5.H.5....q...u..|.....5.qf.1g...<...,...5.qf.1....<...,...5.qf.1...<...,...5...f.6g...<...D.}5.qf.1....<...,..f.f.8g..}<..0h..S.....0.....5..M..L..5.=. .....E..E..E..E..E.....5..M..L..U.....5.....5.....%.....5.....}5.5..M..L.5....5.@.5.5.H.5.....u.L:.5.qf.1g...<..,..5.qf.1....<..,..f.f.8g..}<..0h.4wS.....0.$...5....E..E....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.887297413536421
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	dK0SRzWoPq.exe
File size:	219317
MD5:	6f111b596da1ac7d71c4362b18309648
SHA1:	e09f8065342a4c8664148bec4b0d9265e7e5842a
SHA256:	285e772a15413afa15e86632327faebaa56ff23d0ca19249c228b2d531e19f96
SHA512:	f3e1c725d4c0916a4856af17e272791f056595399e9970c58a4156fbd262e761b50b511cc422e41becfa86493f6248480f855df6718eeaac904d53e1ec8f1e88
SSDEEP:	6144:HNeZmLfHg6+reKq0Uzme51aUUTzC92gBE:HNlLvX+12auAVTzhg+
TLSH:	4F2412543A64C4B2D6A347722A7D43BF6B5FE21320A44B5F33182E98BD31781DA4E726
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi

Instruction
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007EFCACB7597Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007EFCACB7594Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0xa50	0xc00	False	0.402018229167	data	4.18462166815	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x2e8	data	English	United States
RT_DIALOG	0x3b478	0x100	data	English	United States
RT_DIALOG	0x3b578	0x11c	data	English	United States
RT_DIALOG	0x3b698	0x60	data	English	United States
RT_GROUP_ICON	0x3b6f8	0x14	data	English	United States
RT_MANIFEST	0x3b710	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 5, 2022 08:14:00.061939955 CEST	59856	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:01.105869055 CEST	59856	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:02.152606010 CEST	59856	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:04.199518919 CEST	59856	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:05.082415104 CEST	53	59856	8.8.8.8	192.168.2.7
May 5, 2022 08:14:06.123655081 CEST	53	59856	8.8.8.8	192.168.2.7
May 5, 2022 08:14:07.171267033 CEST	53	59856	8.8.8.8	192.168.2.7
May 5, 2022 08:14:09.217835903 CEST	53	59856	8.8.8.8	192.168.2.7
May 5, 2022 08:14:21.655561924 CEST	50560	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:22.670001030 CEST	50560	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:23.685656071 CEST	50560	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:25.701590061 CEST	50560	53	192.168.2.7	8.8.8.8
May 5, 2022 08:14:26.674069881 CEST	53	50560	8.8.8.8	192.168.2.7
May 5, 2022 08:14:27.687593937 CEST	53	50560	8.8.8.8	192.168.2.7
May 5, 2022 08:14:28.703629971 CEST	53	50560	8.8.8.8	192.168.2.7

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 5, 2022 08:14:06.123738050 CEST	192.168.2.7	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 5, 2022 08:14:07.173743010 CEST	192.168.2.7	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 5, 2022 08:14:09.218017101 CEST	192.168.2.7	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 5, 2022 08:14:27.687700033 CEST	192.168.2.7	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable
May 5, 2022 08:14:28.703749895 CEST	192.168.2.7	8.8.8.8	cff6	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 08:14:00.061939955 CEST	192.168.2.7	8.8.8.8	0xf32b	Standard query (0)	www.xianzyw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:01.105869055 CEST	192.168.2.7	8.8.8.8	0xf32b	Standard query (0)	www.xianzyw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:02.152606010 CEST	192.168.2.7	8.8.8.8	0xf32b	Standard query (0)	www.xianzyw.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 5, 2022 08:14:04.199518919 CEST	192.168.2.7	8.8.8.8	0xf32b	Standard query (0)	www.xianzyw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:21.655561924 CEST	192.168.2.7	8.8.8.8	0x8228	Standard query (0)	www.baigouw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:22.670001030 CEST	192.168.2.7	8.8.8.8	0x8228	Standard query (0)	www.baigouw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:23.685656071 CEST	192.168.2.7	8.8.8.8	0x8228	Standard query (0)	www.baigouw.com	A (IP address)	IN (0x0001)
May 5, 2022 08:14:25.701590061 CEST	192.168.2.7	8.8.8.8	0x8228	Standard query (0)	www.baigouw.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 5, 2022 08:14:05.082415104 CEST	8.8.8.8	192.168.2.7	0xf32b	Server failure (2)	www.xianzyw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:06.123655081 CEST	8.8.8.8	192.168.2.7	0xf32b	Server failure (2)	www.xianzyw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:07.171267033 CEST	8.8.8.8	192.168.2.7	0xf32b	Server failure (2)	www.xianzyw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:09.217835903 CEST	8.8.8.8	192.168.2.7	0xf32b	Server failure (2)	www.xianzyw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:26.674069881 CEST	8.8.8.8	192.168.2.7	0x8228	Server failure (2)	www.baigouw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:27.687593937 CEST	8.8.8.8	192.168.2.7	0x8228	Server failure (2)	www.baigouw.com	none	none	A (IP address)	IN (0x0001)
May 5, 2022 08:14:28.703629971 CEST	8.8.8.8	192.168.2.7	0x8228	Server failure (2)	www.baigouw.com	none	none	A (IP address)	IN (0x0001)

Code Manipulations

User Modules

Hook Summary

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

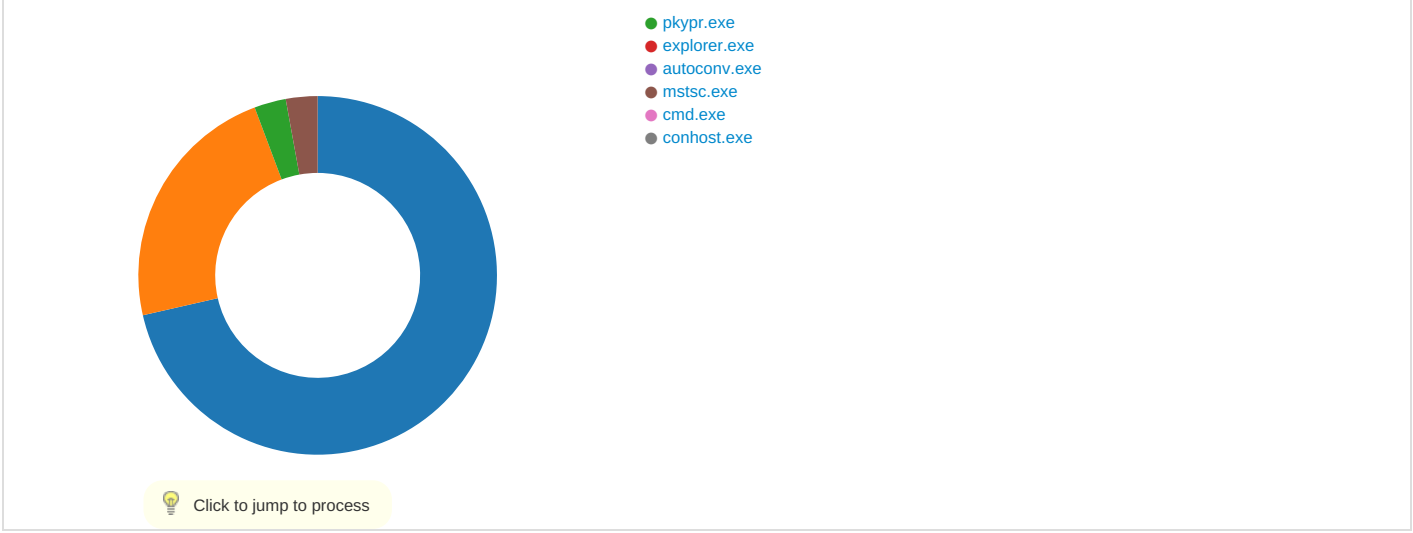
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xED
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xED
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xED
GetMessageA	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xED

Statistics

Behavior



System Behavior

Analysis Process: dK0SRzWoPq.exe PID: 772, Parent PID: 5404

General	
Target ID:	0
Start time:	08:12:15
Start date:	05/05/2022
Path:	C:\Users\user\Desktop\dK0SRzWoPq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\dK0SRzWoPq.exe"
Imagebase:	0x400000
File size:	219317 bytes
MD5 hash:	6F111B596DA1AC7D71C4362B18309648
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: pkypr.exe PID: 1924, Parent PID: 772

General	
Target ID:	1
Start time:	08:12:17
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\pkypr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\pkypr.exe C:\Users\user~1\AppData\Local\Temp\zpcthwca
Imagebase:	0x400000
File size:	5120 bytes
MD5 hash:	087998162F8FBD6E48CC5AB45BE63449
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: 00000001.00000002.372566518.0000000002180000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.372566518.0000000002180000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.372566518.0000000002180000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 44%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\zpcthwca	unknown	4096	success or wait	1	401072	fread
C:\Users\user\AppData\Local\Temp\zpcthwca	unknown	4096	success or wait	1	401072	fread
C:\Users\user\AppData\Local\Temp\ow7v8lrfalu0lz3762	unknown	189439	success or wait	1	2170A1E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	217051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	217051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	217051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	217051C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	217051C	ReadFile

Analysis Process: pkypr.exe PID: **6380**, Parent PID: **1924**

General

Target ID:	2
Start time:	08:12:18
Start date:	05/05/2022
Path:	C:\Users\user\AppData\Local\Temp\pkypr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user~1\AppData\Local\Temp\pkypr.exe C:\Users\user~1\AppData\Local\Temp\zpcthwca
Imagebase:	0x400000
File size:	5120 bytes
MD5 hash:	087998162F8FBD6E48CC5AB45BE63449
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: 00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.369225156.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.367373235.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.367373235.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.367373235.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.463016643.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.463016643.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.463016643.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.463378064.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.463378064.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.463378064.00000000009D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.463592351.0000000000A00000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.463592351.0000000000A00000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.463592351.0000000000A00000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A447	NtReadFile

Analysis Process: explorer.exe PID: **3808**, Parent PID: **6380**

General

Target ID:	3
Start time:	08:12:24
Start date:	05/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
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: 00000003.00000000.443403408.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.443403408.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.443403408.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.416140599.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.416140599.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.416140599.0000000007599000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autoconv.exe PID: **5488**, Parent PID: **3808**

General

Target ID:	12
Start time:	08:13:01
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x260000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: mstsc.exe PID: **404**, Parent PID: **3808**

General

Target ID:	13
Start time:	08:13:02
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x820000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.625629256.00000000030F0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.625629256.00000000030F0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.625629256.00000000030F0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.625466489.0000000000D30000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.625466489.0000000000D30000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.625466489.0000000000D30000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.625958951.0000000003160000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.625958951.0000000003160000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.625958951.0000000003160000.00000040.10000000.00040000.00000000.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	310A447	NtReadFile

Analysis Process: cmd.exe PID: **7084**, Parent PID: **404**

General

Target ID:	15
Start time:	08:13:07
Start date:	05/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user~1\AppData\Local\Temp\pkypr.exe"
Imagebase:	0xdd0000
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

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: **6884**, Parent PID: **7084**

General

Target ID:	16
Start time:	08:13:08
Start date:	05/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7bab80000
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

No disassembly