ID: 532826
Sample Name: bhjRru88ej
Cookbook: default.jbs
Time: 18:24:23
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

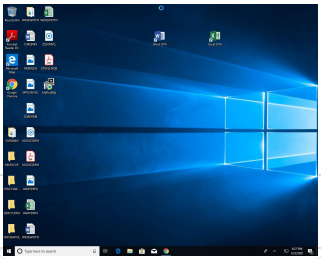
Windows Analysis Report bhjRru88ej

Overview

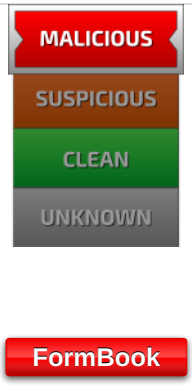
General Information

Sample Name:	bhjRru88ej (renamed file extension from none to exe)
Analysis ID:	532826
MD5:	3461688b684c14..
SHA1:	70269a15f2b27f2..
SHA256:	5869ff09468b1aa..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



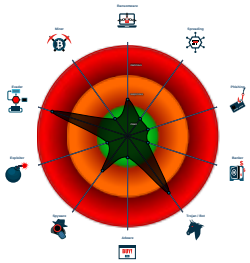
FormBook

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 …
- Multi AV Scanner detection for doma…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- Queues an APC in another process …
- Tries to detect virtualization through…
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64**
- bhjRru88ej.exe (PID: 5244 cmdline: "C:\Users\user\Desktop\bhjRru88ej.exe" MD5: 3461688B684C14BFA1B81F1A110254E4)
  - bhjRru88ej.exe (PID: 5228 cmdline: "C:\Users\user\Desktop\bhjRru88ej.exe" MD5: 3461688B684C14BFA1B81F1A110254E4)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - colorcpl.exe (PID: 5620 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 6136 cmdline: /c del "C:\Users\user\Desktop\bhjRru88ej.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 3864 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.drmichaelirvine.com/yrcy/"
  ],
  "decoy": [
    "ordermws-brands.com",
    "jkbswj.com",
    "dairatwsl.com",
    "lewismiddleton.com",
    "hevenorfeed.com",
    "kovogueshop.com",
    "cyberitconsultingz.com",
    "besrbee.com",
    "workerscompfl1.com",
    "wayfinderacu.com",
    "smplkindness.com",
    "servicesitcy.com",
    "babyvv.com",
    "fly-crypto.com",
    "chahuima.com",
    "trist-n.tech",
    "minjia56.com",
    "oded.top",
    "mes-dents-blanches.com",
    "nethunsleather.com",
    "onlinesindh.com",
    "genrage.com",
    "bhalawat.com",
    "5gwirelesszone.com",
    "semejnyjochag.com",
    "shopvintageallure.com",
    "laqueenbeautybar.supplies",
    "hominyprintingmuseum.com",
    "taksimbet13.com",
    "fairytalesinc.com",
    "loversscout.com",
    "nxn-n.com",
    "lovebydarius.store",
    "mintnft.tours",
    "snowjamproductiosmedia.com",
    "boraviajar.website",
    "cryptointelcenter.com",
    "m2momshealth.com",
    "perfectionbyinjection.com",
    "cletechsolutions.com",
    "skin4trade.com",
    "a9d7c19f0282.com",
    "waltersswholesale.com",
    "lendsoar.com",
    "virginialandsforsale.com",
    "shinepatio.com",
    "nba2klocker.team",
    "picturebookoriginals.com",
    "chatteusa.com",
    "bodevolidu.quest",
    "certidaoja.com",
    "scgxjp.com",
    "cbd-cannabis-store.com",
    "kadinisigi.com",
    "vacoveco.com",
    "hostedexchangemaintainces.com",
    "hf59184.com",
    "jingguanfm.com",
    "browsealto.com",
    "kymyra.com",
    "xrgoods.com",
    "dtsddcpj.com",
    "uptimisedmc.com",
    "redsigndesign.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.413560341.00000000009D0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.413560341.00000000009D0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.bhjRru88ej.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.bhjRru88ej.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.bhjRru88ej.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
1.0.bhjRru88ej.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.bhjRru88ej.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for domain / URL

Networking:

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:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

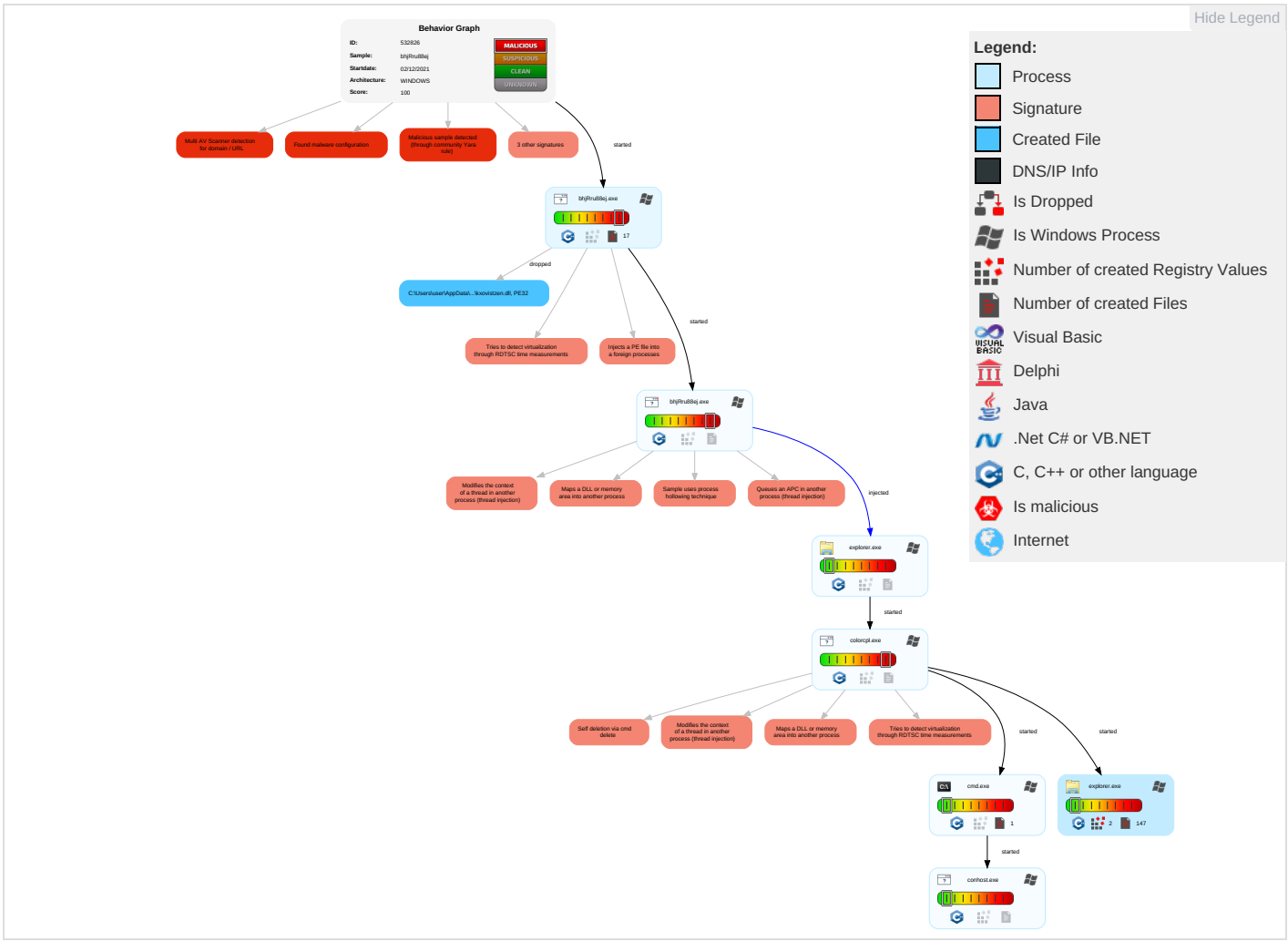
Remote Access Functionality:

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
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 6 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

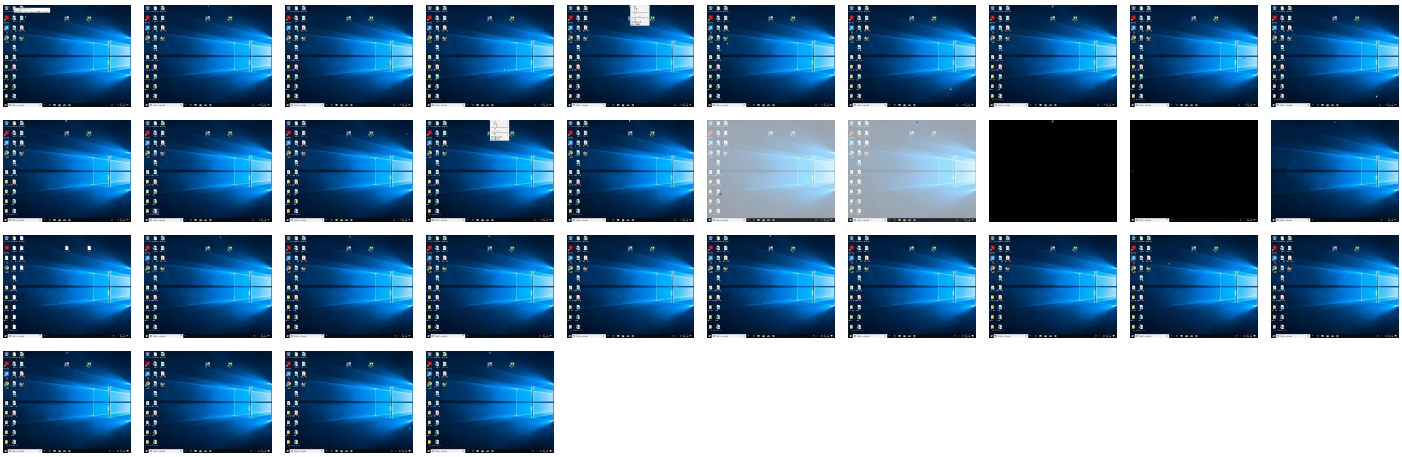
Behavior Graph



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
bhjRru88ej.exe	19%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.explorer.exe.ba3796c.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.bhjRru88ej.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.bhjRru88ej.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.bhjRru88ej.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.bhjRru88ej.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.colorcpl.exe.539796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.bhjRru88ej.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
0.2.bhjRru88ej.exe.25d0000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.colorcpl.exe.ca3240.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.bhjRru88ej.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://logo.verisign	0%	Avira URL Cloud	safe	
http://nsdobe.cM	0%	Avira URL Cloud	safe	
www.drmichaelirvine.com/yrcy/	7%	Virustotal		Browse
www.drmichaelirvine.com/yrcy/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.drmichaelirvine.com/yrcy/	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532826
Start date:	02.12.2021
Start time:	18:24:23
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	bhjRru88ej (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/2@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.9% (good quality ratio 18.9%) • Quality average: 73.6% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:26:39	API Interceptor	215x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\aenx7c9gkk268	
Process:	C:\Users\user\Desktop\bhjRru88ej.exe
File Type:	data
Category:	dropped
Size (bytes):	216882
Entropy (8bit):	**7.994298787318829**
Encrypted:	**true**
SSDEEP:	6144:6oIRGl0b+7GXCGwN5q8AJXj+yv6ZabXKtyKq:67oC+2zwN5QXYsbyyX
MD5:	11789F0E771071D04FD53F88297E2BAA
SHA1:	8DF23670A4919D8158AF1715B7F4E8A995B607C6
SHA-256:	F7CD00F4A19B9D6AC6B1DFBC1ADDB775089CB070580D7F41DE4190845FAB224C
SHA-512:	81DDADBE06EB66E1BC450F99607C1C02D8DE7A6AA1E8D228EBA66D7CD535D3E180C058E68C0F3AFF439D2DC26D34EDC32B33FFF5E295ACE639288625D4779 4F
Malicious:	false
Reputation:	low
Preview:	nI.z...v..{.Sy.....c...fq.0...bC^%E..*.w.....*..x..`P.E...q..h_.....|...fK..l.....#.....}y.B..z..R...$.Z4./.D.Ns..".2=;...t.w.....^..3.O:.i.b.Y....0..}...s.z[.s.Z...(....?'._.w....K..=-&Dr'..H.i..& H'...4..L.y...>....zo.....J/...`.*...Ot...d....v.6...Nc...c.s..(.?..bC^.E..*.w..@..*..x..`P.E.....h.Zf....#u..B.W.....y.Dl...V..jY...(..HL..{b.gX_..j....".2=;.xR.....Z.t?.|b.~...S7.....c}. /q.....P...]EC.?'=...'.~.....=-&Dr'..&...;.R..R..4..L.yi.7>....zmJ.....J/.f.`m*...Ot.r.D....v.J....Nc...crs.@.(.?>.bC^%E..*.w.....*..x..`P.E.....h.Zf....#u..B.W.....y.Dl...V..jY...(..HL.. {b.gX_..j....".2=;.xR.....Z.t?.|b.~...S7.....c}./q.....P..(....?'._.'W~..I|...=-&Dr'..&...;.&.....4..L.yi.7>....zmJ.....J/.f.`m*...Ot.r.D....v.J....Nc...crs.@.(.?>.bC^%E..*.w.....*..x..`P.E. ....h.Zf....#u..B.W.....y.Dl...V..jY...(..HL..{b.gX_..j....".2=;.xR.....Z.t?.|b.~...S7.....c}./q.....P..(....?'._.'W~..I|...=-&Dr'..&...;.&.....4..L.yi.7>....

C:\Users\user\AppData\Local\Temp\nsnC68C.tmp\kxovistzen.dll	
Process:	C:\Users\user\Desktop\bhjRru88ej.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	165376
Entropy (8bit):	6.376526911061105
Encrypted:	false
SSDEEP:	3072:kS/gkndx2PJh/XkkJJD10jpEj86LoTGUjc9:kS4k4dX7JD10j2wG
MD5:	CA01E724A81B69E7CF6613D5706917CD
SHA1:	C27C4C7F355A9B8C753D0072D8995369E70D7690
SHA-256:	602EA8D52A0CDFE9B88E865BC189728DA8DA59454C84C7F2BCF1AE93010FF6C6
SHA-512:	326DE45294389F846A30C36B0294E750304BF7C1F3730DBEFEE57224824F6D1CC2832CD4E025FF6B64C38EE56FE4DBF39A8E82610FA8F5A1388F4C7094256CCE
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A..(...{...{...{..4{$..{...{...{..5{j..{...z...{...z...{...{...{...z...{...z...{..*{...{...z ...{Rich...{.....PE..L.....a.....!..... .....e.....pf.....p`.....`..@..... .....text..... ..`.rdata..<U... ...V.....@..@.data....B.....&...^.....@....rsrc.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.939325980634555
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	bhjRru88ej.exe
File size:	329536
MD5:	3461688b684c14bfa1b81f1a110254e4
SHA1:	70269a15f2b27f2a3a33a4028d7aeb2e1094db58
SHA256:	5869ff09468b1aafa73c0a8fa15c953995495aa7144114003fdc4743860639ad

General

SHA512:	bc1ecb387ca68cf57fa1264ad6567ddca62bbf87f97362a66d3755e48496afe8f9013186dc7d03bec6c5201f0c3906715ec8a00b16bc1fa1d394256692913b93
SSDEEP:	6144:rGiG8cKLnPjzfoNvzfe67vOpnNczXDErvIJHOZabXKtyYov27XebMWHsdjE:SdKXzr6enNczXQrlJHOsbyyHFxsdE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....\.....0.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030e3
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:	
Time Stamp:	0x48EFCDCD [Fri Oct 10 21:49:01 2008 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:	7fa974366048f9c551ef45714595665e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5b68	0x5c00	False	0.67722486413	data	6.48746502716	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x129c	0x1400	False	0.4337890625	data	5.04904254867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c58	0x400	False	0.58203125	data	4.76995537906	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x900	0xa00	False	0.4078125	data	3.93441125971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: bhjRru88ej.exe PID: 5244 Parent PID: 6084

General

Start time:	18:25:22
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\bhjRru88ej.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bhjRru88ej.exe"
Imagebase:	0x400000
File size:	329536 bytes
MD5 hash:	3461688B684C14BFA1B81F1A110254E4
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: 00000000.00000002.353597466.00000000025D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.353597466.00000000025D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.353597466.00000000025D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: bhjRru88ej.exe PID: 5228 Parent PID: 5244

General

Start time:	18:25:24
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\bhjRru88ej.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\bhjRru88ej.exe"
Imagebase:	0x400000
File size:	329536 bytes
MD5 hash:	3461688B684C14BFA1B81F1A110254E4
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: 00000001.00000002.413560341.00000000009D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.413560341.00000000009D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.413560341.00000000009D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.413505967.00000000005C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.413505967.00000000005C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.413505967.00000000005C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.413413880.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.413413880.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.413413880.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.350595433.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.350595433.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.350595433.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.352601050.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.352601050.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.352601050.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.351883848.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.351883848.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.351883848.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 5228

General

Start time:	18:25:28
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.384139517.00000000075EE000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.384139517.00000000075EE000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.384139517.00000000075EE000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.397566356.00000000075EE000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.397566356.00000000075EE000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.397566356.00000000075EE000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: colorcpl.exe PID: 5620 Parent PID: 3440

General

Start time:	18:25:51
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0xac0000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.625740978.0000000000BC0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.630654958.0000000002FB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.630654958.0000000002FB0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.630654958.0000000002FB0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.630203304.0000000002EB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.630203304.0000000002EB0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.630203304.0000000002EB0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6136 Parent PID: 5620

General

Start time:	18:25:58
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\bhjRru88ej.exe"
Imagebase:	0x7ff614b90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3232 Parent PID: 6136

General

Start time:	18:25:59
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0xc70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 3864 Parent PID: 772

General

Start time:	18:26:37
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis