ID: 491574
Sample Name: 3cGH9Bakuq
Cookbook: default.jbs
Time: 18:02:45
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

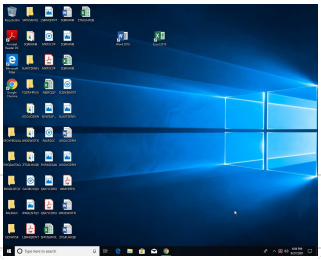
Windows Analysis Report 3cGH9Bakuq

Overview

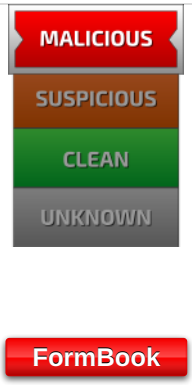
General Information

Sample Name:	3cGH9Bakuq (renamed file extension from none to exe)
Analysis ID:	491574
MD5:	0eca879131a7b1..
SHA1:	07fa4692aa15a40.
SHA256:	166559731ad153..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

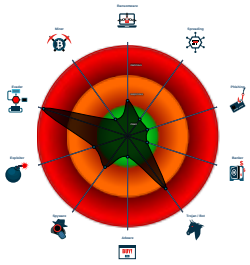


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Self deletion via cmd delete
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- 3cGH9Bakuq.exe (PID: 6452 cmdline: 'C:\Users\user\Desktop\3cGH9Bakuq.exe' MD5: 0ECA879131A7B104418B085DB7F761C3)
  - 3cGH9Bakuq.exe (PID: 6668 cmdline: C:\Users\user\Desktop\3cGH9Bakuq.exe MD5: 0ECA879131A7B104418B085DB7F761C3)
  - 3cGH9Bakuq.exe (PID: 6420 cmdline: C:\Users\user\Desktop\3cGH9Bakuq.exe MD5: 0ECA879131A7B104418B085DB7F761C3)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 5908 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - colorcpl.exe (PID: 6676 cmdline: C:\Windows\SysWOW64\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
        - cmd.exe (PID: 1472 cmdline: /c del 'C:\Users\user\Desktop\3cGH9Bakuq.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.929569610.0000000004CB0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.929569610.0000000004CB 0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$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 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.929569610.0000000004CB 0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.686725719.00000000025B 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.687646701.00000000035B 9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.3cGH9Bakuq.exe.3775cd0.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.3cGH9Bakuq.exe.3775cd0.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10f4f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10f882:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x11b595:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11b081:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x11b697:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x11b80f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x11029a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11a2fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x111012:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x120a67:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x121b0a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.3cGH9Bakuq.exe.3775cd0.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x11d999:$sqlite3step: 68 34 1C 7B E1 • 0x11daac:$sqlite3step: 68 34 1C 7B E1 • 0x11d9c8:$sqlite3text: 68 38 2A 90 C5 • 0x11daed:$sqlite3text: 68 38 2A 90 C5 • 0x11d9db:$sqlite3blob: 68 53 D8 7F 8C • 0x11db03:$sqlite3blob: 68 53 D8 7F 8C
6.2.3cGH9Bakuq.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.3cGH9Bakuq.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 10 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

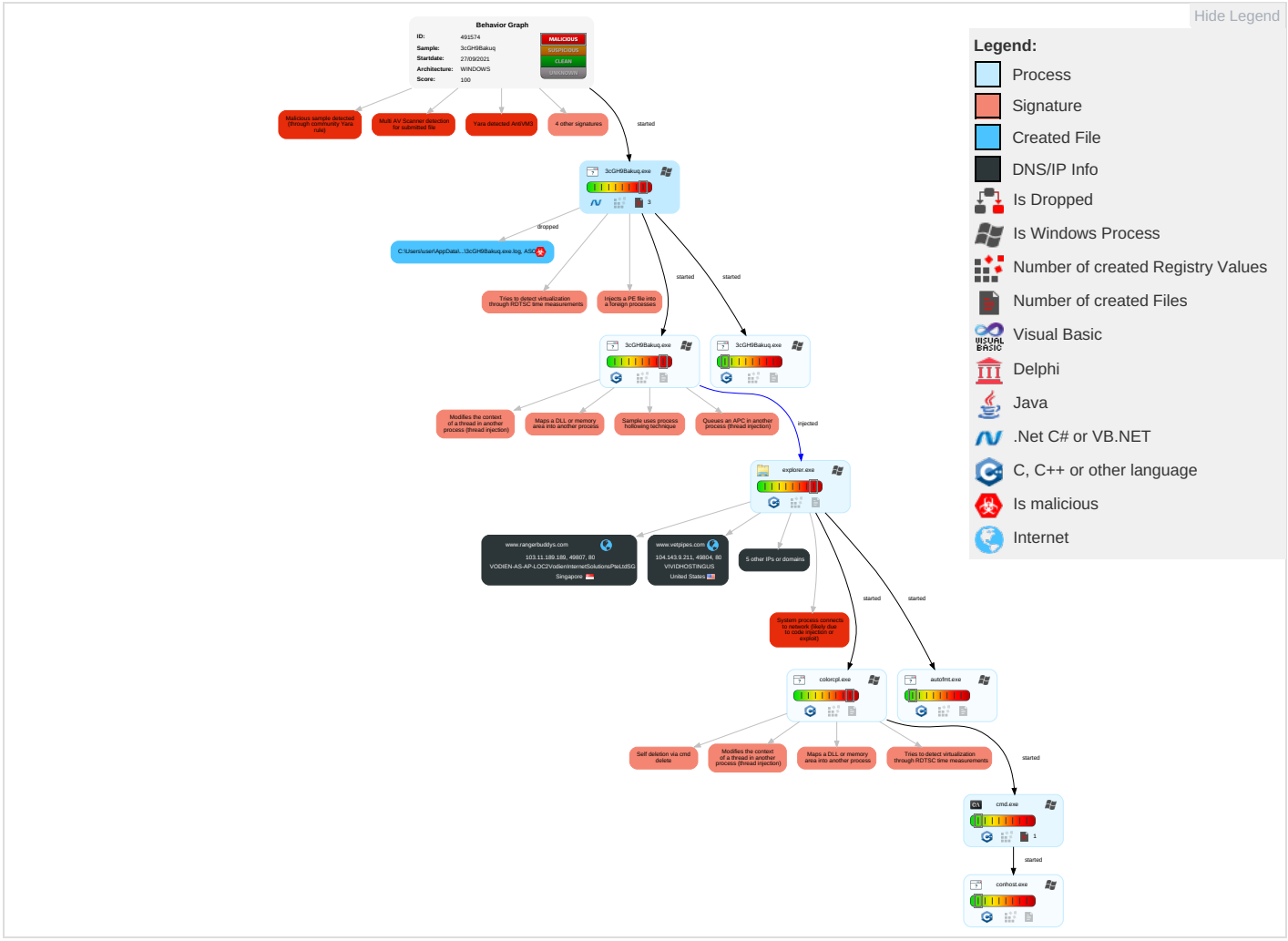
Remote Access Functionality:

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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade t Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
3cGH9Bakuq.exe	26%	Virustotal		Browse
3cGH9Bakuq.exe	22%	ReversingLabs	Win32.Trojan.Pwsx	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.3cGH9Bakuq.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnA.	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.vetpipes.com/scb0/?IN9dgxBh=gxg+zqdn+o0ww4uf8TcZaQyTsJgiXCW12nXRXcs11V7/zKzoeUyv6HeZPjVpo2wMT0Al&sVSH=CPDL8v1	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.omniriot.com/scb0/?sVSH=CPDL8v1&IN9dgxBh=beKAYpkJja+K0I/DndBFcQmb1njbIlQSoH3Y/zfbdScl712FMHF3+aANQrs36cfLB01F	0%	Avira URL Cloud	safe	
http://www.rangerbuddys.com/scb0/?sVSH=CPDL8v1&IN9dgxBh=J7r5qQFPY3cJvABn1Gs7ze2qtK7SOzbffr49jA2eoV1JiGZLpH7+KoOsOPA+gXWondlu	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnenx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoW	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnorm	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnA.	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comdiafN	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnh-c	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnenx	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cned	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.comh	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnh	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.rangerbuddys.com	103.11.189.189	true	false		high
www.omniriot.com	154.208.82.163	true	false		high
marmorariapiramide.online	143.198.15.243	true	false		high
www.vetpipes.com	104.143.9.211	true	false		high
www.marmorariapiramide.online	unknown	unknown	false		high
www.emptycc.net	unknown	unknown	false		high
www.traexcel.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.vetpipes.com/scb0/?IN9dgxBh=gxg+zqdn+o0ww4uf8TcZaQyTsJgiXCW12nXRXcs11V7/zKzoeUyv6HeZPjVpo2wMT0Al&sVSH=CPDL8v1	true	• Avira URL Cloud: safe	unknown
http://www.omniriot.com/scb0/?sVSH=CPDL8v1&IN9dgxBh=beKAYpkJja+K0I/DndBFcQmb1njbIlQSoH3Y/zfbdScl712FMHF3+aANQrs36cfLB01F	true	• Avira URL Cloud: safe	unknown
http://www.rangerbuddys.com/scb0/?sVSH=CPDL8v1&IN9dgxBh=J7r5qQFPY3cJvABn1Gs7ze2qtK7SOzbffr49jA2eoV1JiGZLpH7+KoOsOPA+gXWondlu	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.143.9.211	www.vetpipes.com	United States		64200	VIVIDHOSTINGUS	false
143.198.15.243	marmorariapiramide.online	United States		15557	LDCOMNETFR	false
154.208.82.163	www.omniriot.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	false
103.11.189.189	www.rangerbuddys.com	Singapore		58621	VODIEN-AS-AP-LOC2VodienInternetSolutionsPteLtdSG	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491574
Start date:	27.09.2021
Start time:	18:02:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3cGH9Bakuq (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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/1@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 40.3% (good quality ratio 35.4%) • Quality average: 72.3% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 100% • 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
18:03:49	API Interceptor	1x Sleep call for process: 3cGH9Bakuq.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\Microsoft\CLR_v4.0_32\UsageLogs\3cGH9Bakuq.exe.log

Process:	C:\Users\user\Desktop\3cGH9Bakuq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.294961182646713

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	3cGH9Bakuq.exe
File size:	626688
MD5:	0eca879131a7b104418b085db7f761c3
SHA1:	07fa4692aa15a409091bc6190bf33b5942db99e6
SHA256:	166559731ad15341f955bf8a16708f93542bef868c33f02f70e9b27f57b991a3
SHA512:	952420118839a1aa8fb2c498910d784aeacb2a9ed953845415e7c523c41f0d3755ec6fcda769e6045c0677d4a002d86b278876b877fc058054f95774b15332ab
SSDEEP:	12288:BB6AGIF/OXu5OtiBIZzG/NoC9NPNIQt5XyGY0:JGIF3wOI5G1oCXPzTVY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49a282
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61518E8B [Mon Sep 27 09:27:39 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x98288	0x98400	False	0.721873717159	data	7.30848087754	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x618	0x800	False	0.3349609375	data	3.46990850393	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 18:05:06.173321009 CEST	192.168.2.4	8.8.8.8	0x7514	Standard query (0)	www.emptycc.net	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:11.418425083 CEST	192.168.2.4	8.8.8.8	0xc089	Standard query (0)	www.vetpipes.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:16.769006014 CEST	192.168.2.4	8.8.8.8	0x5964	Standard query (0)	www.omniriot.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:27.743536949 CEST	192.168.2.4	8.8.8.8	0x354f	Standard query (0)	www.rangerbuddys.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:33.223629951 CEST	192.168.2.4	8.8.8.8	0x5b1e	Standard query (0)	www.traexcel.com	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:38.286906958 CEST	192.168.2.4	8.8.8.8	0x6940	Standard query (0)	www.marmorariapiramide.online	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 18:05:06.195317984 CEST	8.8.8.8	192.168.2.4	0x7514	Name error (3)	www.emptycc.net	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:11.525573015 CEST	8.8.8.8	192.168.2.4	0xc089	No error (0)	www.vetpipes.com		104.143.9.211	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:11.525573015 CEST	8.8.8.8	192.168.2.4	0xc089	No error (0)	www.vetpipes.com		104.143.9.210	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:16.955238104 CEST	8.8.8.8	192.168.2.4	0x5964	No error (0)	www.omniriot.com		154.208.82.163	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:27.852567911 CEST	8.8.8.8	192.168.2.4	0x354f	No error (0)	www.rangerbuddys.com		103.11.189.189	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:33.266285896 CEST	8.8.8.8	192.168.2.4	0x5b1e	Name error (3)	www.traexcel.com	none	none	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:38.476347923 CEST	8.8.8.8	192.168.2.4	0x6940	No error (0)	www.marmorariapiramide.online	marmorariapiramide.online		CNAME (Canonical name)	IN (0x0001)
Sep 27, 2021 18:05:38.476347923 CEST	8.8.8.8	192.168.2.4	0x6940	No error (0)	marmoraria piramide.online		143.198.15.243	A (IP address)	IN (0x0001)
Sep 27, 2021 18:05:38.476347923 CEST	8.8.8.8	192.168.2.4	0x6940	No error (0)	marmoraria piramide.online		2.57.90.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.vetpipes.com
- www.omniriot.com
- www.rangerbuddys.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49804	104.143.9.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:05:11.636744022 CEST	7941	OUT	GET /scb0/?IN9dgxBh=gxg+zqdn+o0ww4uf8TcZaQyTsJgiXCW12nXRXcs11V7/zKzoeUyv6HeZPjVpo2wMT0Al&sVSH=CPDL8v1 HTTP/1.1 Host: www.vetpipes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 18:05:11.757265091 CEST	7943	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 27 Sep 2021 16:05:11 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMLl0RJYcDS0N2xIgi01rOAcEtvCUTUq+IuNz5PA8eXYsfPLRkgnNehO+NbOZAlLoQnSpB5rXuRxRCTF+T1iU9sCAwEAAQ==_FzrU0O/DzPHwhUHqvo1zsrZd6OYhY/CKmMbfkIpM4HkqpULVsnDaZNpBRyCVeu0ugpO2Xos2NXdjGtQoX27wGQ== Data Raw: 33 31 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 6c 6f 6f 73 65 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4d 4c 6c 30 52 4a 59 63 44 53 30 4e 32 78 49 67 69 30 31 72 4f 41 63 45 74 76 43 55 54 55 71 2b 49 75 4e 7a 35 50 41 38 65 58 59 73 66 50 4c 52 6b 67 6e 4e 65 68 4f 2b 4e 62 4f 5a 41 6c 4c 6f 51 6e 53 70 42 35 72 58 75 52 78 52 43 54 46 2b 54 31 69 55 39 73 43 41 77 45 41 41 51 3d 3d 5f 46 7a 72 55 30 4f 2f 44 7a 50 48 77 68 55 48 71 76 6f 31 7a 73 72 5a 64 36 4f 59 68 59 2f 43 4b 6d 4d 62 66 6b 49 70 4d 34 48 6b 71 70 55 4c 56 73 6e 44 61 5a 4e 70 42 52 79 43 56 65 75 30 75 67 70 4f 32 58 6f 73 32 4e 58 64 6a 47 74 51 6f 58 32 37 77 47 51 3d 3d 22 3e 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 76 65 74 70 69 70 65 73 2e 63 6f 6d 20 61 74 20 44 69 72 65 63 74 6e 69 63 3c 2f 74 69 74 6c 65 3e 0a 3c 73 74 79 6c 65 3e 0a 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 69 66 72 61 6d 65 20 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 62 6f 72 64 65 72 3a 30 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 73 74 79 6c 65 3a 69 6e 68 65 72 69 74 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 69 6e 68 65 72 69 74 3b 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 7d 0a 68 74 6d 6c 2c 20 64 69 76 20 7b 68 65 69 67 68 74 3a 31 30 30 25 3b 7d 0a 62 6f 64 79 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 2e 35 3b 68 65 69 67 68 74 3a 31 30 30 25 3b 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 20 3e 3c 2f 64 69 76 3e 0a 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 30 35 30 30 30 35 2e 76 6f 6f 64 6f 6f 2e 63 6f 6d 2f 6a 73 2f 70 61 72 74 6e 65 72 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 310<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAMLl0RJYcDS0N2xIgi01rOAcEtvCUTUq+IuNz5PA8eXYsfPLRkgnNehO+NbOZAlLoQnSpB5rXuRxRCTF+T1iU9sCAwEAAQ==_FzrU0O/DzPHwhUHqvo1zsrZd6OYhY/CKmMbfkIpM4HkqpULVsnDaZNpBRyCVeu0ugpO2Xos2NXdjGtQoX27wGQ=="><head><title>vetpipes.com at Directnic</title><style>html, body, iframe {margin:0;padding:0;border:0;font-weight:inherit;font-style:inherit;font-size:100%;font-family:inherit;vertical-align:baseline;}html, div {height:100%;}body{line-height:1.5;height:100%;}</style></head><body> <script type="text/javascript" language="JavaScript" src="http://050005.voodoo.com/js/partner.js"></script></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49806	154.208.82.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:05:17.177975893 CEST	7948	OUT	GET /scb0/?sVSH=CPDL8v1&IN9dgxBh=beKAYpkJja+K0I/DndBFcQmb1njbIlQSoH3Y/zfbdScl712FMHF3+aANQrs36cfLB01F HTTP/1.1 Host: www.omniriot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49807	103.11.189.189	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 18:05:28.029920101 CEST	7950	OUT	GET /scb0/?sVSH=CPDL8v1&IN9dgxBh=J7r5qQFPY3cJvABn1Gs7ze2qtK7SOzbffr49jA2eoV1JiGZLpH7+KoOsOPA+gXWondlu HTTP/1.1 Host: www.rangerbuddys.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 18:05:28.208403111 CEST	7950	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 16:05:28 GMT Server: Apache X-Powered-By: PHP/5.6.40 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 32 39 61 0d 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 74 61 62 6c 65 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 68 65 69 67 68 74 3d 22 31 30 30 25 22 3e 0a 09 3c 74 72 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 3e 0a 09 09 3c 74 64 20 69 64 3d 22 6e 65 77 2d 62 6f 78 22 3e 3c 68 33 3e 2a 2e 63 6f 6d 20 69 73 20 61 20 72 65 67 69 73 74 65 72 65 64 20 64 6f 6d 61 69 6e 2e 3c 62 72 3e 0a 09 09 54 68 69 73 20 69 73 20 61 20 70 6c 61 63 65 68 6f 6c 64 65 72 20 66 6f 72 20 74 68 65 20 77 65 62 73 69 74 65 2e 3c 2f 74 64 3e 0a 09 3c 2f 74 72 3e 0a 09 3c 74 72 20 61 6c 69 67 6e 3d 22 63 65 6e 74 65 72 22 3e 0a 09 09 3c 74 64 3e 49 66 20 79 6f 75 20 77 6f 75 6c 64 20 6c 69 6b 65 20 74 6f 20 3c 73 74 72 6f 6e 67 3e 68 6f 73 74 20 61 20 77 65 62 73 69 74 65 3c 2f 73 74 72 6f 6e 67 3e 20 2f 20 3c 73 74 72 6f 6e 67 3e 6f 62 74 61 69 6e 20 61 20 70 65 72 73 6f 6e 61 6c 69 73 65 64 20 65 6d 61 69 6c 20 61 64 64 72 65 73 73 3c 2f 73 74 72 6f 6e 67 3e 20 2f 20 3c 73 74 72 6f 6e 67 3e 6c 69 6e 6b 20 75 70 20 74 6f 20 47 6f 6f 67 6c 65 20 61 70 70 73 3c 2f 73 74 72 6f 6e 67 3e 2e 20 44 6f 20 67 65 74 20 69 6e 20 74 6f 75 63 68 20 77 69 74 68 20 75 73 2e 3c 62 72 3e 0a 09 09 20 56 6f 64 69 65 6e 20 6f 66 66 65 72 73 20 53 69 6e 67 61 70 6f 72 65 20 68 6f 73 74 65 64 20 73 65 72 76 65 72 73 20 66 6f 72 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 76 6f 64 69 65 6e 2e 63 6f 6d 2f 22 3e 53 69 6e 67 61 70 6f 72 65 20 57 65 62 20 48 6f 73 74 69 6e 67 3c 2f 61 3e 20 61 6e 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 76 6f 64 69 65 6e 2e 63 6f 6d 2f 73 69 6e 67 61 70 6f 72 65 2d 65 6d 61 69 6c 2d 68 6f 73 74 69 6e 67 2e 70 68 70 22 3e 53 69 6e 67 61 70 6f 72 65 20 45 6d 61 69 6c 20 48 6f 73 74 69 6e 67 3c 2f 61 3e 20 73 65 72 76 69 63 65 73 2e 3c 2f 74 64 3e 0a 09 3c 2f 74 72 3e 0a 3c 2f 74 61 62 6c 65 3e 0a 0a 0d 0a Data Ascii: 29a<head><meta name="robots" content="noindex, nofollow"></head><table width="100%" height="100%"><tr align="center"><td id="new-box"><h3>*.com is a registered domain. This is a placeholder for the website.</td></tr><tr align="center"><td>If you would like to host a website / obtain a personalised email address / link up to Google apps. Do get in touch with us. Vodien offers Singapore hosted servers for Singapore Web Hosting and Singapore Email Hosting services.</td></tr></table>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 3cGH9Bakuq.exe PID: 6452 Parent PID: 6556

General

Start time:	18:03:39
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\3cGH9Bakuq.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\3cGH9Bakuq.exe'
Imagebase:	0x240000
File size:	626688 bytes
MD5 hash:	0ECA879131A7B104418B085DB7F761C3
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.686725719.00000000025B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.687646701.00000000035B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.687646701.00000000035B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.687646701.00000000035B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.686799799.0000000002604000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 3cGH9Bakuq.exe PID: 6668 Parent PID: 6452

General

Start time:	18:03:49
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\3cGH9Bakuq.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\3cGH9Bakuq.exe
Imagebase:	0xa0000
File size:	626688 bytes
MD5 hash:	0ECA879131A7B104418B085DB7F761C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 3cGH9Bakuq.exe PID: 6420 Parent PID: 6452

General

Start time:	18:03:50
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\3cGH9Bakuq.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3cGH9Bakuq.exe
Imagebase:	0x440000
File size:	626688 bytes
MD5 hash:	0ECA879131A7B104418B085DB7F761C3
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: 00000006.00000002.779648624.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.779648624.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.779648624.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.780291616.0000000000BA0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.780291616.0000000000BA0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.780291616.0000000000BA0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.780216392.0000000000A10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.780216392.0000000000A10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.780216392.0000000000A10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6420

General

Start time:	18:03:52
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000007.00000000.716031426.000000000DA49000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.716031426.000000000DA49000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.716031426.000000000DA49000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.738903713.000000000DA49000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.738903713.000000000DA49000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.738903713.000000000DA49000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autofmt.exe PID: 5908 Parent PID: 3424

General

Start time:	18:04:29
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x10f0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: colorcpl.exe PID: 6676 Parent PID: 3424

General

Start time:	18:04:30
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\colorcpl.exe
Imagebase:	0xdc0000
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: 0000000F.00000002.929569610.0000000004CB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.929569610.0000000004CB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.929569610.0000000004CB0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.928514787.0000000000CD0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.928514787.0000000000CD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.928514787.0000000000CD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.929541418.0000000004C80000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.929541418.0000000004C80000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.929541418.0000000004C80000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1472 Parent PID: 6676

General

Start time:	18:04:36
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\3cGH9Bakuq.exe'
Imagebase:	0x11d0000
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: 6028 Parent PID: 1472

General

Start time:	18:04:36
Start date:	27/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis