ID: 433531
Sample Name:
XhU4EXUp0x.exe
Cookbook: default.jbs
Time: 08:56:25
Date: 12/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

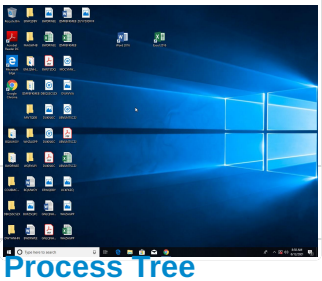
Analysis Report XhU4EXUp0x.exe

Overview

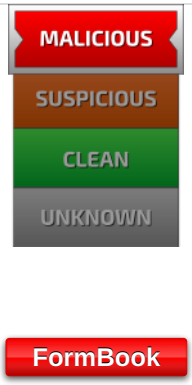
General Information

Sample Name:	XhU4EXUp0x.exe
Analysis ID:	433531
MD5:	49c83eceb8a816..
SHA1:	ead9055c813de4..
SHA256:	2f4d0e2ce90ab2c..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



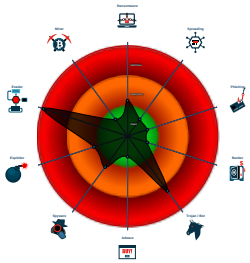
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queries sensitive video device inform…

Classification



Process Tree

- **System is w10x64**
- XhU4EXUp0x.exe (PID: 6968 cmdline: 'C:\Users\user\Desktop\XhU4EXUp0x.exe' MD5: 49C83ECEB8A816B959A778E5F2E78801)
  - XhU4EXUp0x.exe (PID: 6076 cmdline: C:\Users\user\Desktop\XhU4EXUp0x.exe MD5: 49C83ECEB8A816B959A778E5F2E78801)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 6340 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 3416 cmdline: /c del 'C:\Users\user\Desktop\XhU4EXUp0x.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.yellow-wink.com/nff/"
  ],
  "decoy": [
    "shinseikai.site",
    "creditmystartup.com",
    "howtovvbucks.com",
    "betterfromthebeginning.com",
    "oubacm.com",
    "stonalogov.com",
    "gentrypartyof8.com",
    "cuesticksandsupplies.com",
    "joelsavestheday.com",
    "llanobnb.com",
    "ecclogic.com",
    "miempaque.com",
    "cai23668.com",
    "miscdr.net",
    "twzhhq.com",
    "bloomandbrewcafe.com",
    "angcomleisure.com",
    "mafeeboutique.com",
    "300coin.club",
    "brooksranchhomes.com",
    "konversiondigital.com",
    "dominivision.com",
    "superiorshinedetailing.net",
    "thehomechef.global",
    "dating-web.site",
    "gcbsclubc.com",
    "mothererph.com",
    "pacleanfuel.com",
    "jerseryshorenflflagfootball.com",
    "roberthyatt.com",
    "wwwmacsports.com",
    "tearor.com",
    "american-ai.com",
    "mkyiyuan.com",
    "gempharmatechllc.com",
    "verdijvtc.com",
    "zimnik-bibo.one",
    "heatherdarkauthor.net",
    "dunn-labs.com",
    "automotivevita.com",
    "bersatubagaidulu.com",
    "gorillarecruiting.com",
    "mikecdmusic.com",
    "femuveewedre.com",
    "onyxmodsllc.com",
    "ooweesports.com",
    "dezeren.com",
    "foeweifgoor73dz.com",
    "sorchaashe.com",
    "jamiitulivu.com",
    "jifengshijie.com",
    "ranchfiberglas.com",
    "glendalesocialmediaagency.com",
    "icuvietnam.com",
    "404hapgood.com",
    "planetturmeric.com",
    "danfrem.com",
    "amazonautomationbusiness.com",
    "switchfinder.com",
    "diversifiedforest.com",
    "findnehomes.com",
    "rsyueda.com",
    "colombianmatrimony.com",
    "evan-dawson.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000000.652221131.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.652221131.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.XhU4EXUp0x.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.XhU4EXUp0x.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.XhU4EXUp0x.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
3.0.XhU4EXUp0x.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.XhU4EXUp0x.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

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:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

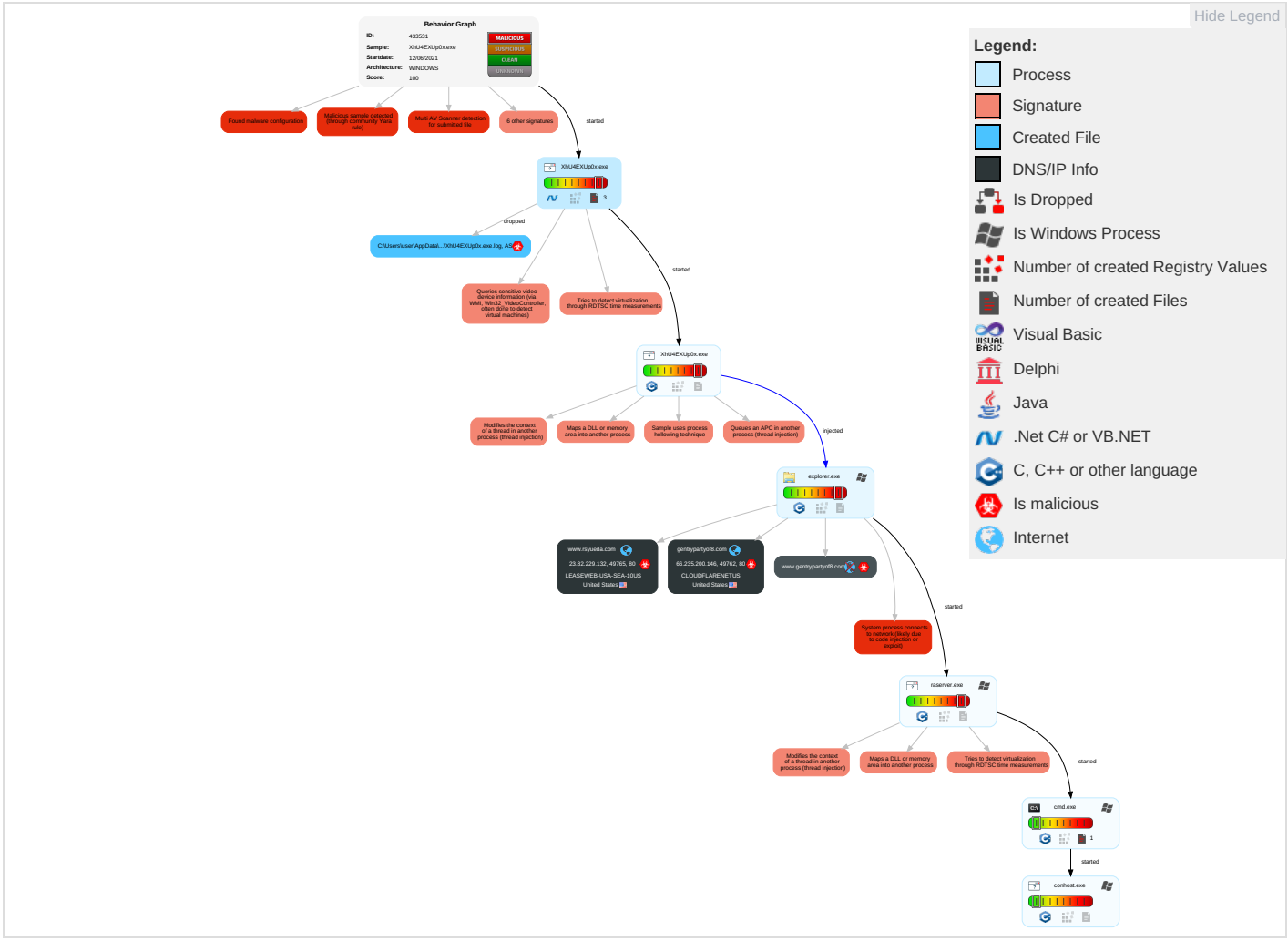
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

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
XhU4EXUp0x.exe	21%	Virustotal		Browse
XhU4EXUp0x.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
XhU4EXUp0x.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.XhU4EXUp0x.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.XhU4EXUp0x.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.gentrypartyof8.com/nff/?2dWD=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8IkF2PxixF5c&7nSX=f2MHEhOHwH	0%	Avira URL Cloud	safe	
http://www.rsyueda.com/nff/?2dWD=rcekcafpraO0sj/oaoDcLlLwOdzHntpmaKyMQqwrcrTR8fOv+tmqTlrKj/r2WTcjy7/L&7nSX=f2MHEhOHwH	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
www.yellow-wink.com/nff/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.rsyueda.com	23.82.229.132	true	true		unknown
gentrypartyof8.com	66.235.200.146	true	true		unknown
www.gentrypartyof8.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.gentrypartyof8.com/nff/?2dWD=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8IkF2PxixF5c&7nSX=f2MHEhOHwH	true	• Avira URL Cloud: safe	unknown
http://www.rsyueda.com/nff/?2dWD=rcekcafpraO0sj/oaoDcLlLwOdzHntpmaKyMQqwrcrTR8fOv+tmqTlrKj/r2WTcjy7/L&7nSX=f2MHEhOHwH	true	• Avira URL Cloud: safe	unknown
www.yellow-wink.com/nff/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.235.200.146	gentrypartyof8.com	United States		13335	CLOUDFLARENETUS	true
23.82.229.132	www.rsyueda.com	United States		396190	LEASEWEB-USA-SEA-10US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433531
Start date:	12.06.2021
Start time:	08:56:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XhU4EXUp0x.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:	21
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@7/1@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.9% (good quality ratio 16.3%) • Quality average: 73.8% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:57:13	API Interceptor	1x Sleep call for process: XhU4EXUp0x.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.235.200.146	New Purchase Order20210609.exe	Get hash	malicious	Browse	• www.anderson-anderson.com/un8c/?6lGd=HBZ81PLPUzqhOj&3f-H3H=EENVCx8DcYxC77hOTbV1SAybrq7ihl4TvqnYxLujxv6ep3jMUAl9807ilL37bAvbTVrR
	packa.....(1).exe	Get hash	malicious	Browse	• www.apexpioneer.com/wdva/?kfD4qZ=qWl9Mj/s+HilBOtVYaSZVR6j4m9BeajRzFuKOkq+ALHs1EAUycBQc15lgYPA8iZZOcHD&kr0=dbF0vFoPNvL
	New order 201534.pdf.exe	Get hash	malicious	Browse	• www.thedailymino.com/sbqi/?8pdPxFYX=jXb6weh8fwwMUEgPJJl7RJ0MRYZqFSz6owdMJ8CEOPRP4uFAZVBZ7eXod2M1Xtzg6qh0&_FNlAt=tVEl9tDHXfB4
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• www.anderson-anderson.com/un8c/?D8ODAr=EENVCx8DcYxC77hOTbV1SAybrq7ihl4TvqnYxLujxv6ep3jMUAl9807ilIXrUh/jNwCW&mJ=V6AHzvxh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Order_PO 1164_HD-F 4020 6K.exe	Get hash	malicious	Browse	• www.anderson-anderson.com/un8c/?Lh0l=EENVCx8DcYxC77hOTbV1SAybrq7ihl4TvqnYxLujxv6ep3jMUAI9807ilIXrUh/jNwCW&VTKh=vBZtYDQXqZ4DGn
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• www.taratakeson.com/oerg/?ndndnZ=UtWlYrO0rhjH&mHLD_0=dr4pMwcdhZcmPSbPHAIEo/sox+gcSbBb1FVNS74e5R2NObgAqDDHvg7Hj8ybvDNWoVhE
	bibviv.exe	Get hash	malicious	Browse	• www.milkweedmagic.com/vns/
	INVOICE PAYMENT.exe	Get hash	malicious	Browse	• www.milkweedmagic.com/vns/?nloHn6=zPqtcJu8h&OH5LRV=dxIiDTMmZIUelDEuKFBNrZVGQoGe1rqzTAT6E2MP4OmWiXtk9zOjG3OmaVxdpx2vqn8e
	BL Draft copy.exe	Get hash	malicious	Browse	• www.smallpeo.com/sx8c/?inzXrV1h=CQJBYFRSx3Pkz4hmjXzNOjG1WISSVLs1fX4LX3HiJ6zoF9rBVgsTdld9Os8/rzow8SJA&SP=cnxT3HrH
	2os1TIXTXk.exe	Get hash	malicious	Browse	• www.iidiotproof.com/mdi/?Yn=490O4/0fh9aUX7Eo1RdW8uGCBI43DKhy4NK5PQpMhOFz6rL2znJpXpofqYOF+JlL3+nX&mvKtg=Y4C4_fDHvx98fJ5
	03102021.xls	Get hash	malicious	Browse	• baxtercode.com/qkhpnucmzts/44267.5622407407.dat
	03102021.xls	Get hash	malicious	Browse	• baxtercode.com/qkhpnucmzts/44267.5507399306.dat
	03102021.xls	Get hash	malicious	Browse	• baxtercode.com/qkhpnucmzts/44267.5414023148.dat

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	orii11.exe	Get hash	malicious	Browse	• www.iidiotproof.com/mdi/?ndn4iL=490O4/0fh9aUX7Eo1RdW8uGCBI43DKhy4NK5PQpMhOFz6rL2znJpXpofqbu/uYFztZGQ&OR9=uTypBLyh3rCtd
	orii11.exe	Get hash	malicious	Browse	• www.iidiotproof.com/mdi/?8pp=490O4/0fh9aUX7Eo1RdW8uGCBI43DKhy4NK5PQpMhOFz6rL2znJpXpofqYOvh5VLz8vX&sZCx=1bYdfPf8ef5pjPm
	PO.x00991882822.xlsm	Get hash	malicious	Browse	• www.rmpcleancom/private/?-ZL=kjFT_jIXCZeHrh&FVTt=Uhbi9DfUBq2i/1fkh0yGI21N5OQMN5zBtkTJbOEZT9D8cf6FKtFeyjvu/14BaEQ5k4UB
	Parcel _009887 .exe	Get hash	malicious	Browse	• www.ocicoxford.com/csw6/?t8bHuZw=efwaGXT9IzbmNtOzDnCu+48vppNLQWQKGJFN33tYCz0tX5X/vDpmiH8bd6jrvtNwDjl3p9k8/g==&2d=llsp
	P.O-DT1692.exe	Get hash	malicious	Browse	• www.drtarver.com/g65/?hL0=/G2o2cr0v4Q8hBBM9UJDjH+yY22wUVLVelfqLGL5GIR6ySKGryVcUhqqpJFQ9LO6Iwep&Wr=LhnLHrv8d
	SAMSUNG C&T UPCOMING PROJECTS19-MP.exe.exe	Get hash	malicious	Browse	• www.elrodeorestaurantbw.com/cdl/?Mfg=/L1IlqGS5r2x+RFPi+XkQGVOlUslsJfdMM9Npew4xv9wNb7VMt18zc8R4PiLn7n17TkB&uVxpj=ojO0dJYX1B
	AWB_SHIPPING_DOCUMENT_pdf.exe	Get hash	malicious	Browse	• www.lincolnreadymeals.com/me2z/?absDxBr=WOPwKhxv/yLwNDnXBLmuN1eR3SzsT6kHFNnvJn0nwfrdF7aBYBJOwB9MozwDSP7grAKd&pPX=EFQpsLbPFZvt

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	1VTzed95Tz.exe	Get hash	malicious	Browse	• 104.21.45.72
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 104.21.19.200
	Proforma Invoice.exe	Get hash	malicious	Browse	• 104.21.19.200
	TLUN2Qvsx2.exe	Get hash	malicious	Browse	• 104.23.98.190
	rL2F1mjb2l.exe	Get hash	malicious	Browse	• 104.23.99.190
	tvijATOn6L.exe	Get hash	malicious	Browse	• 104.23.99.190
	8964532115.exe	Get hash	malicious	Browse	• 172.67.188.154
	DHL_2761228.exe	Get hash	malicious	Browse	• 162.159.13 3.233
	0900988099900000.exe	Get hash	malicious	Browse	• 172.67.188.154
	Payment Advice.exe	Get hash	malicious	Browse	• 104.21.19.200
	VM64DGCRMN5XGK.htm	Get hash	malicious	Browse	• 104.16.18.94
	1EFNborqwh.dll	Get hash	malicious	Browse	• 104.20.185.68
	OrderKLB210568.exe	Get hash	malicious	Browse	• 104.16.13.194
	Purchase_Order.exe	Get hash	malicious	Browse	• 104.21.64.212
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 172.67.188.69
	b9f5bca9a22f08aad48674bc42e4eaf72ab8aa3d652ba.exe	Get hash	malicious	Browse	• 104.26.9.187
	LsWgkxVLk1.dll	Get hash	malicious	Browse	• 104.20.184.68
	HHHyXsu7Vj.dll	Get hash	malicious	Browse	• 104.20.184.68
	7Nboq835Fc.exe	Get hash	malicious	Browse	• 104.21.19.200
	moq fob order.exe	Get hash	malicious	Browse	• 172.67.188.154
LEASEWEB-USA-SEA-10US	Product_Samples.exe	Get hash	malicious	Browse	• 23.82.229.141
	RFQ_BRAT_METAL_TECH_LTD.exe	Get hash	malicious	Browse	• 23.82.229.141
	Airwaybill # 6913321715.exe	Get hash	malicious	Browse	• 23.82.149.3
	8UsA.sh	Get hash	malicious	Browse	• 172.241.15 9.235
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• 23.82.149.3
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 23.82.229.141
	Rio International LLC URGENT REQUEST FOR QUOTATION .exe	Get hash	malicious	Browse	• 23.82.229.141
	NEW ORDER ELO-05756485.exe	Get hash	malicious	Browse	• 23.82.149.10
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• 23.82.230.186
	order samples 056-059_pdf.exe	Get hash	malicious	Browse	• 23.82.225.149
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• 23.82.225.149
	OPSzlwylj5.exe	Get hash	malicious	Browse	• 173.234.15.207
	BSG_ptf.exe	Get hash	malicious	Browse	• 23.82.225.149
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 23.82.229.136
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 23.82.229.136
	yqfUONVqpk.exe	Get hash	malicious	Browse	• 173.234.15.207
	sntU1XoQa3.exe	Get hash	malicious	Browse	• 173.234.15.207
	vvUkaRlJUJ.exe	Get hash	malicious	Browse	• 173.234.15.207
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 23.82.78.4
	hkcmd.exe	Get hash	malicious	Browse	• 173.234.15.207

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\XhU4EXUp0x.exe.log

Process:	C:\Users\user\Desktop\XhU4EXUp0x.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1406

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\XhU4EXUp0x.exe.log	
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.6744819259251145
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:	XhU4EXUp0x.exe
File size:	907264
MD5:	49c83eceb8a816b959a778e5f2e78801
SHA1:	ead9055c813de47edfec5bc46a0d896df4b4af2e
SHA256:	2f4d0e2ce90ab2c35dcba4c85e38346eae6ac2cef0f939ccdd21cade4d6343ca
SHA512:	09b42603c00de62fe0426f202a6809c0d7ed2164f6e3da1ab124a9d02e75eea115a2ad650905a2df4e9d9bbdb4347c4283eed1c161cfdf549713cbb46ca6a6d1
SSDEEP:	24576:EE4VwfX9zrNeBUdtEqTGokrWc4eJNPs2ruVc:EE4VwfX9PwBU8rWc5rGc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4decea
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:	0x60C3DF04 [Fri Jun 11 22:09:08 2021 UTC]
TLS Callbacks:	

General

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	0xdccf0	0xdce00	False	0.803978980971	data	7.68116376135	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x5dc	0x600	False	0.426432291667	data	4.164077085	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	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
Jun 12, 2021 08:58:45.281604052 CEST	192.168.2.4	8.8.8.8	0x2a48	Standard query (0)	www.gentrypartyof8.com	A (IP address)	IN (0x0001)
Jun 12, 2021 08:59:06.180969000 CEST	192.168.2.4	8.8.8.8	0x4b68	Standard query (0)	www.rsyuea.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 12, 2021 08:57:05.951527119 CEST	8.8.8.8	192.168.2.4	0x52b2	No error (0)	a-0019.a.dns.azurefd.net	a-0019.standard.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Jun 12, 2021 08:58:45.436830044 CEST	8.8.8.8	192.168.2.4	0x2a48	No error (0)	www.gentrypartyof8.com	gentrypartyof8.com		CNAME (Canonical name)	IN (0x0001)
Jun 12, 2021 08:58:45.436830044 CEST	8.8.8.8	192.168.2.4	0x2a48	No error (0)	gentrypartyof8.com		66.235.200.146	A (IP address)	IN (0x0001)
Jun 12, 2021 08:59:06.255776882 CEST	8.8.8.8	192.168.2.4	0x4b68	No error (0)	www.rsyuea.com		23.82.229.132	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.gentrypartyof8.com
- www.rsyueda.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49762	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 12, 2021 08:58:45.487462997 CEST	8357	OUT	GET /nff/?2dWD=oo8PZR09GamqRkCLHSTg5AKJvm44C+19X1uEOPW4zTuWS3c9RrL+Vx+B8IkF2PxixF5c&7nSX=f2MHEhOHwH HTTP/1.1 Host: www.gentrypartyof8.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
1	192.168.2.4	49765	23.82.229.132	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jun 12, 2021 08:59:06.452203989 CEST	8377	OUT	GET /nff/?2dWD=rcekcafpraO0sj/oaoDcLlLwOdzHntpmaKyMQqwrcrTR8fOv+tmqTlrKj/r2WTcjy7/L&7nSX=f2MHEhOHwH HTTP/1.1 Host: www.rsyueda.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jun 12, 2021 08:59:06.651827097 CEST	8378	IN	HTTP/1.1 500 Internal Server Error Cache-Control: private Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 X-AspNet-Version: 4.0.30319 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST, PUT, DELETE Date: Sat, 12 Jun 2021 06:59:03 GMT Connection: close Content-Length: 4082 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e e6 9c aa e5 b0 86 e5 af b9 e8 b1 a1 e5 bc 95 e7 94 a8 e8 ae be e7 bd ae e5 88 b0 e5 af b9 e8 b1 a1 e7 9a 84 e5 ae 9e e4 be 8b e3 80 82 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 2e 37 65 6d 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 7d 20 0d 0a 20 20 20 20 20 20 20 20 20 70 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 20 62 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 63 6f 6c 6f 72 3a 62 6c 61 63 6b 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 2d 35 70 78 7d 0d 0a 20 20 20 20 20 20 20 20 20 48 31 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 74 3b 63 6f 6c 6f 72 3a 72 65 64 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 48 32 20 7b 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 56 65 72 64 61 6e 61 22 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 34 70 74 3b 63 6f 6c 6f 72 3a 6d 61 72 6f 6f 6e 20 7d 0d 0a 20 20 20 20 20 20 20 20 70 72 65 20 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 43 6f 6e 73 6f 6c 61 73 22 2c 22 4c 75 63 69 64 61 20 43 6f 6e 73 6f 6c 65 22 2c 4d 6f 6e 6f 73 70 61 63 65 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 31 70 74 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 2e 35 65 6d 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 34 70 74 7d 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 72 6b 65 72 20 7b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 20 62 6c 61 63 6b 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 76 65 72 73 69 6f 6e 20 7b 63 6f 6c 6f 72 3a 20 67 72 61 79 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 72 72 6f 72 20 7b 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 30 70 78 3b 7d 0d 0a 20 20 20 20 20 20 20 20 2e 65 78 70 61 6e 64 61 62 6c 65 20 7b 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 75 6e 64 65 72 6c 69 6e 65 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 20 63 6f 6c 6f 72 3a 6e 61 76 79 3b 20 Data Ascii: <!DOCTYPE html><html> <head> <title></title> <meta name="viewport" content="width=device-width" /> <style> body {font-family:"Verdana";font-weight:normal;font-size: .7em;color:black;} p {font-family:"Verdana";font-weight:normal;color:black;margin-top: -5px} b {font-family:"Verdana";font-weight:bold;color:black;margin-top: -5px} H1 { font-family:"Verdana";font-weight:normal;font-size:18pt;color:red } H2 { font-family:"Verdana";font-weight:normal;font-size:14pt;color:maroon } pre {font-family:"Consolas","Lucida Console",Monospace;font-size:11pt;margin:0;padding:0.5em;line-height:14pt} .marker {font-weight: bold; color: black;text-decoration: none;} .version {color: gray;} .error {margin-bottom: 10px;} .expandable { text-decoration:underline; font-weight:bold; color:navy;

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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: XhU4EXUp0x.exe PID: 6968 Parent PID: 6016

General

Start time:	08:57:11
Start date:	12/06/2021
Path:	C:\Users\user\Desktop\XhU4EXUp0x.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\XhU4EXUp0x.exe'
Imagebase:	0x340000
File size:	907264 bytes
MD5 hash:	49C83ECEB8A816B959A778E5F2E78801
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.655856649.00000000037F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.655856649.00000000037F7000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.655856649.00000000037F7000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.654291332.00000000036B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.654291332.00000000036B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.654291332.00000000036B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.653535453.00000000026EF000.00000004.00000001.sdmp, Author: Joe Security

Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: XhU4EXUp0x.exe PID: 6076 Parent PID: 6968

General

Start time:	08:57:15
Start date:	12/06/2021
Path:	C:\Users\user\Desktop\XhU4EXUp0x.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\XhU4EXUp0x.exe
Imagebase:	0xe60000
File size:	907264 bytes
MD5 hash:	49C83ECEB8A816B959A778E5F2E78801
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: 00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.707404802.00000000015D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.652221131.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.652221131.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.652221131.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.706990052.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.706990052.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.706990052.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.707426607.0000000001600000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.707426607.0000000001600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.707426607.0000000001600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6076

General

Start time:	08:57:18
Start date:	12/06/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
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

Analysis Process: raserver.exe PID: 6340 Parent PID: 3424

General

Start time:	08:57:38
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x1370000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.911907238.0000000000A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.911907238.0000000000A90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.911907238.0000000000A90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.912137473.0000000000E80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.912137473.0000000000E80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.912137473.0000000000E80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.912162573.0000000000EB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.912162573.0000000000EB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.912162573.0000000000EB0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 3416 Parent PID: 6340

General

Start time:	08:57:42
Start date:	12/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\XhU4EXUp0x.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: 2216 Parent PID: 3416

General

Start time:	08:57:43
Start date:	12/06/2021
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