ID: 553033
Sample Name: 40881-39611-05143-MT103.exe
Cookbook: default.jbs
Time: 06:27:37
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

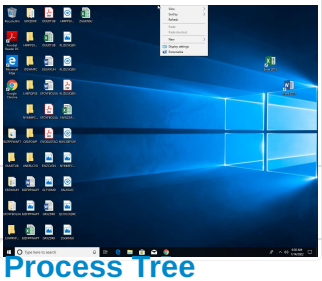
Windows Analysis Report 40881-39611-05143-MT103.exe

Overview

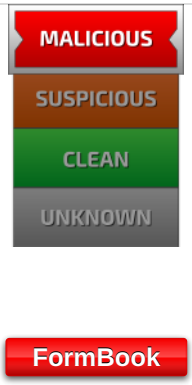
General Information

Sample Name:	40881-39611-05143-MT103.exe
Analysis ID:	553033
MD5:	a181630fd1086db.
SHA1:	e2f6974f63e07d8..
SHA256:	c026113c33af859..
Tags:	exe formbook
Infos:	

Most interesting Screenshot:



Detection



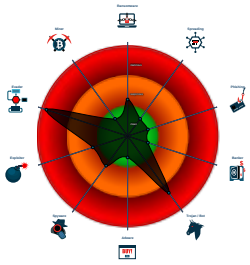
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- System process connects to networ…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete
- Injects a PE file into a foreign proce…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- 40881-39611-05143-MT103.exe (PID: 3456 cmdline: "C:\Users\user\Desktop\40881-39611-05143-MT103.exe" MD5: A181630FD1086DB2385028FA8C2CD27C)
  - 40881-39611-05143-MT103.exe (PID: 5244 cmdline: "C:\Users\user\Desktop\40881-39611-05143-MT103.exe" MD5: A181630FD1086DB2385028FA8C2CD27C)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 2924 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 1884 cmdline: /c del "C:\Users\user\Desktop\40881-39611-05143-MT103.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.watddle.com/t1y0/"
  ],
  "decoy": [
    "bovanuffelen.com",
    "yaqa.run",
    "rareanimals-mint.com",
    "nimktrading.com",
    "pansdvj.xyz",
    "duniaislam.website",
    "bangkokcrypto.com",
    "barriopyme.com",
    "empresarial0812.website",
    "fa7qi9.xyz",
    "fetch-it-incontri-online.fyi",
    "bg2eidbz.xyz",
    "fd5g6.xyz",
    "kk310.com",
    "chiacogilsonite.com",
    "fast-quotes-b3.info",
    "arcticfoxbooks.com",
    "scintillant.website",
    "bedfordshirevcs.com",
    "traverx.xyz",
    "allandlewis.com",
    "chaoliume.com",
    "stylegio.com",
    "medividecuador.com",
    "suitable-products.com",
    "gongzuo.icu",
    "gracechurchpaulina.com",
    "ambientagro.net",
    "hammerest.net",
    "commute-durable.com",
    "igwt.world",
    "hnhzgc.com",
    "gnatyuk.info",
    "1-more-watermarker.com",
    "chickenwingsnashville.com",
    "northstarliteracy.com",
    "mrcleanautowash.com",
    "listchild.com",
    "deliciasveganaz.com",
    "gteatfeet.com",
    "my-lifehack.store",
    "myevkart.com",
    "jaguar-theartofbadservice.com",
    "enerjitoptan.xyz",
    "bestroofevah.com",
    "earringsalisa.com",
    "lukewarmdefinfo.online",
    "ar-sands.com",
    "tokyosushi67.com",
    "woturxj.com",
    "bestan.xyz",
    "stockoun.com",
    "motorreizenbengsx.info",
    "jannasjewelry.com",
    "standingforfreedo.com",
    "womenxc.com",
    "venamed.store",
    "ztgnmu.com",
    "futurefarmsag.com",
    "mitchandhannah.com",
    "drnchaso.com",
    "douvip484.com",
    "tiontry.com",
    "iqamatur.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.238427747.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000000.238427747.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.40881-39611-05143-MT103.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.40881-39611-05143-MT103.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b917:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c91a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.40881-39611-05143-MT103.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$sqlite3step: 68 34 1C 7B E1 • 0x1894c:$sqlite3step: 68 34 1C 7B E1 • 0x18868:$sqlite3text: 68 38 2A 90 C5 • 0x1898d:$sqlite3text: 68 38 2A 90 C5 • 0x1887b:$sqlite3blob: 68 53 D8 7F 8C • 0x189a3:$sqlite3blob: 68 53 D8 7F 8C
1.2.40881-39611-05143-MT103.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.40881-39611-05143-MT103.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab17:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
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

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

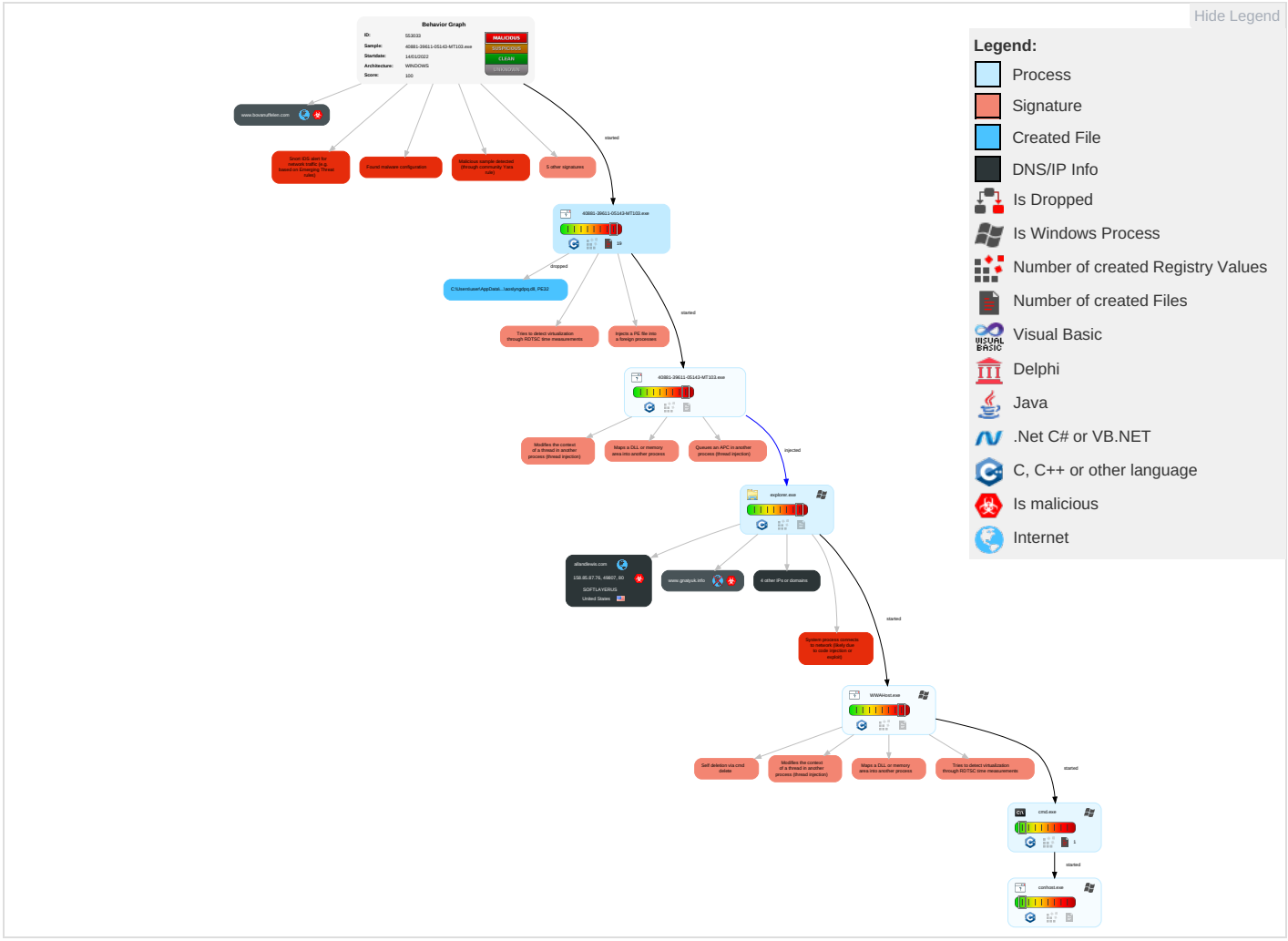
Remote Access Functionality:

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	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	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 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
40881-39611-05143-MT103.exe	32%	Virustotal		Browse
40881-39611-05143-MT103.exe	28%	ReversingLabs	Win32.Backdoor.Androm	
40881-39611-05143-MT103.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.40881-39611-05143-MT103.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.40881-39611-05143-MT103.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.40881-39611-05143-MT103.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.40881-39611-05143-MT103.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.WWAHost.exe.450f840.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.40881-39611-05143-MT103.exe.23c0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.40881-39611-05143-MT103.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.WWAHost.exe.108a368.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Domains

Source	Detection	Scanner	Label	Link
allandlewis.com	0%	Virustotal		Browse
ar-sands.com	0%	Virustotal		Browse
gnatyuk.info	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.watddle.com/t1y0/	0%	Avira URL Cloud	safe	
http://www.gnatyuk.info/t1y0/?j4eTzF=F82LBBwiF2WdFMF0PdT+LyhlKqSByZY+hePS/QYkGxd4nwGUhGJA4bF6+h/WaxW/quis&y2M=JPRlurVHW6	0%	Avira URL Cloud	safe	
http://www.allandlewis.com/t1y0/?j4eTzF=tLX95BcBGfEhqVleCXtpcNXr5hlqBy02D0w7FqhwVxcUYz1XFX4bZ6eVCxIWz+fQPry/&y2M=JPRlurVHW6	0%	Avira URL Cloud	safe	
http://www.ar-sands.com/t1y0/?j4eTzF=X3Ka+jH2pGe9JZJCakhiHHqoQGax0dVQKYvGWJh20Ylx7iFclkHqSNrYISZIlgOBNqtm&y2M=JPRlurVHW6	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
allandlewis.com	158.85.87.76	true	true	• 0%, Virustotal, Browse	unknown
ar-sands.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
gnatyuk.info	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
www.bovanuffelen.com	217.160.0.10	true	true		unknown
www.ar-sands.com	unknown	unknown	true		unknown
www.gnatyuk.info	unknown	unknown	true		unknown
www.allandlewis.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.watddle.com/t1y0/	true	• Avira URL Cloud: safe	low
http://www.gnatyuk.info/t1y0/?j4eTzF=F82LBBwiF2WdFMF0PdT+LyhlKqSByZY+hePS/QYkGxd4nwGUhGJA4bF6+h/WaxW/quis&y2M=JPRlurVHW6	false	• Avira URL Cloud: safe	unknown
http://www.allandlewis.com/t1y0/?j4eTzF=tLX95BcBGfEhqVleCXtpcNXr5hlqBy02D0w7FqhwVxcUYz1XFX4bZ6eVCxIWz+fQPry/&y2M=JPRlurVHW6	true	• Avira URL Cloud: safe	unknown
http://www.ar-sands.com/t1y0/?j4eTzF=X3Ka+jH2pGe9JZJCakhiHHqoQGax0dVQKYvGWJh20Ylx7iFclkHqSNrYISZIlgOBNqtm&y2M=JPRlurVHW6	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
158.85.87.76	allandlewis.com	United States		36351	SOFTLAYERUS	true
34.102.136.180	ar-sands.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553033
Start date:	14.01.2022
Start time:	06:27:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	40881-39611-05143-MT103.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:	27
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@7/4@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.5% (good quality ratio 22.1%) • Quality average: 74.6% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 87% • 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

No simulations

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\gy8flejfjx	
Process:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
File Type:	data
Category:	dropped
Size (bytes):	216804
Entropy (8bit):	**7.992985454496395**
Encrypted:	**true**
SSDEEP:	6144:yCixmkQwIZfn+3njjVNcZiZ4v4rGkfgjhX6q33JH:rYmTZf+3njj7ck4ArEx6q3p
MD5:	E60737235631DB824F8BFC4CE0C65893
SHA1:	A4E40A7B69038A71D7E7195D762EE57C71EC975B
SHA-256:	53E0C95D4C543F245FE578D8C8012D5F68BE4784A70CDB0AC825C3E846CD7FD5
SHA-512:	E2ADC55E2A50DB1BC2C20A26937312427A525E04911F53513A3F55BFCF5FFB1049A51EB5B80261C6AFF703772DC6C4623FDD3C1F9BDC358CEA881210C6FC2A6
Malicious:	false
Reputation:	low
Preview:	...7f.f.B,.....d.br.....Q.Q.\..3..n...E@.yx.C...r.86.|.....nU.....Q~~.....X...N.....f."..0...(...L.Z.OJ.....A)..CTe.@..+.-...Z'..\.t.8..mH.Nb..L.C.0...5....L.....Z~.VxU..R/qew.y.U.....a..V...V....c.w.Cq.....$.[}.u..n..ww][..+..X.F.7f...PF\|,.....2C.....<Q.f.\..3...nX..E@.y..C...r..6.....b.....Z..".g.W?.whU.....,...@'u..kl8g.C0z.&Ls2...+Z.OJ...%...e..D.r...8..pm<.....o)...#..Lw.....%.....L...j.+9Z~....U./.uP.yZU.....2.MX...V..\:c.w.Cq..\...$.[}....n...w.][..+...:.F.7f....PF|^.....2C.....Q.Q.\..3..n...E@.yx.C...r..6.....b.....Z..".g.W?.whU.....,...@'u..kl8g.C0z.&Ls2...+Z.OJ...%...e..D.r...8..pm<.....o)...#..Lw.....%.....L.....Z~..xU./..7.y.U.....2.MX...V..\:c.w.Cq..\...$.[}....n...w.][..+....F.7f....PF|^.....2C.....Q.Q.\..3..n...E@.yx.C...r..6.....b.....Z..".g.W?.whU.....,...@'u..kl8g.C0z.&Ls2...+Z.OJ...%...e..D.r...8..pm<.....o)...#..Lw.....%.....L.....Z~..xU./..7.y.U.....2.MX...V..\:c.w.Cq..

C:\Users\user\AppData\Local\Temp\nsgDD11.tmp	
Process:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
File Type:	data
Category:	dropped
Size (bytes):	246412
Entropy (8bit):	7.788914058550426
Encrypted:	false
SSDEEP:	6144:W3CixmkQwIZfn+3njjVNcZiZ4v4rGkfgjhX6q33JR:LYmTZf+3njj7ck4ArEx6q3
MD5:	2E4E979D88EDA0087D80AEBECB447057
SHA1:	050D9D4086182721D2F99A2A863F2655B8B436FD
SHA-256:	5A2AFE6F6311393ADC609C66748A42BCB661407B957019951E1798B2E2857DE7
SHA-512:	2737698474E92A0C8CDF488014CB1F9656EE089B74D316B30644A5FFE355904B06DD98F183BA9368295D2AC9661DA42646451ED815C6C19B124BCD3DB957AAD
Malicious:	false
Reputation:	low
Preview:	.N.....,.....9.....4M.....N.....J.....4...j.....

C:\Users\user\AppData\Local\Temp\nsgDD12.tmp\aoslyngdpq.dll	
Process:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	4.126786617959713
Encrypted:	false
SSDEEP:	48:Spo5IUvjbMnLjfFlkuW2yH+ZsQMR7/iItlRuqSQ:Z5NkLjdFuoH+Zdc5x
MD5:	4B3E6E9F3355DC3EBAB609DAE6410A5D
SHA1:	5CCC47A2929FE20876771EE8EF51788CB1A257AC
SHA-256:	9B7E58AD233B26F675636CEEEAE7493B5DA3A4979F1304AA3EC94862D5EA3A1D
SHA-512:	C845E0702CA74D83097CFAAD8CB0520CF9480F8D42B9006EA9417D5009DE14A15580EFB54276BB3A9AD8D0264E06F87428A94BE011ACF2E8BFE5F69A39994F5
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\nsgDD12.tmp\aoslyngdpq.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x-2..Ca..Ca..CaZ.Ma..Ca..B`..Ca..Ba..Ca.lG`..Ca.lC`..Ca.l.a..Ca.lA`..CaRich..Ca.....PE..L..."..a.....!..... .....P.....@..... ..H....!.....0.....@..\.....text..... ..`.rdata..h.... .....@..@.rsrc.....0.....@..@.reloc..\....@.....@..B.....

C:\Users\user\AppData\Local\Temp\xfdnpljo	
Process:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
File Type:	data
Category:	dropped
Size (bytes):	4990
Entropy (8bit):	6.144842331968714
Encrypted:	false
SSDEEP:	96:OA9ZmT5tLZuvVH9fOsGWBBFOtFiSzYHA7iQr5IHErRj1p4CTGs:OAyT550F7y/nP9cUTGs
MD5:	870459628FFCED3E7E94F580BE316FF7
SHA1:	822B4DA17A9CDD110358C202E57A8860B42655DF
SHA-256:	F5C011B67DCF4DA5B6CC9DFB82DD4980689A4DB6148BBE988B9F3EC1655E3BAA
SHA-512:	C5C832C8B869BCF8B531985DE9E4EC5A57BDAC4CE92DA51375CE044779F232500B264F6C5E4107D2192C379E5DA1C5789E567EC5806403A1A41AA9E22E3124(
Malicious:	false
Reputation:	low
Preview:	Od.<<.1P9P|...9.L<.....\.....T9.D<u.@.<<<9.H<=.=.+.D.T;<<</.d/.`=.=.+.D.TT<<</.l/.h=.=.+.D.Ti<<</.t/.p=.=.+.D.T.<<</../.x9....~...../.V.X1.9T..o/.T/.P1.T1.@+.w.f..EG1.T..@+.v/.@../.H9XL.T<<<<9...q..@=.d.=.l.=.t..=...=.\.=.T.3B...1.E../.H.9J..L=.d..1../.L..@T<<<<u....<<<9...q1.H..1.L...1S.v.<.1P.....D1.1<...1.1<1.1.w/.D1.w./.@1.1<|1./.1.D1.@1S.v.<.>r.T.<<T.<<v.<..=].T.<<T.<<v.<..!.T.<<T.<<v.<.1P9P.....Tu.D.<<<+.d/.@9.D<.1.@r<<1.@|/.@1.D./.DQXT..<<3...1.....o</..d/.`+.T...wW</..d/.`.....<+..d...=].Tg.<<.Tj;==/.HQ.+.T.=.T.===/.H9.H<.9.L<Q.u.L.<<<1.L1S.v.<.1P9P|.....Tu.D.<<<+../.@9.D<.1.@r<<1.@|/.@1.D./.DQXT.<<3..8.<<<1.....o</.../.x1....wW</.../.x1....gW/.../.x1.o...f./.../.x+.T...wW./.../.x.....<+.....>r.TR<<<.TY@==/.H9..<.1.T1./.Q.=.=.=.=.=.T.:==/.H9.H<.9.L<Q.u.L.<<<1.L1S.v.<.1P9P.u.D.<<<+.X/.@9.D<.1.@r<<1.@|/.@1.D./.DQXT.<<3...1.....o</..X/.T1....wW</..X/.T.....<+..X...!.T.<<<.T.@==/.HQ.=.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.905152088042034
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:	40881-39611-05143-MT103.exe
File size:	246624
MD5:	a181630fd1086db2385028fa8c2cd27c
SHA1:	e2f6974f63e07d8d165d7be26639d862bf2a818f
SHA256:	c026113c33af8599afd82bb769c25eea7ac5f1212576c4306347a54a8fd5ed1b
SHA512:	f20452e68bbec5426edb131cd4aaf2cae8d09730326c866793e29754a6498413d502cc57a2570520845e495e0879248832cce5204c65e4655e74ff2f5510fda9
SSDEEP:	6144:0wSXvnCUEdnwGmyea3IBAQpZi3EZ7fn/l/Qr:EvxqYyeuQ3gENUY
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE..L.....H.....Z.....%2.....

File Icon

Icon Hash:	d4e8e8f0f0e8e2c4

Static PE Info

General

Entrypoint:	0x403225
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:	0x48EFCDC9 [Fri Oct 10 21:48:57 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:	099c0646ea7282d232219f8807883be0

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5976	0x5a00	False	0.668619791667	data	6.46680044621	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.444878472222	data	5.17796812871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55078125	data	4.68983486809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x1028	0x1200	False	0.354383680556	data	3.44821615722	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-06:29:36.760410	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49776	34.102.136.180	192.168.2.5
01/14/22-06:29:57.255827	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49805	34.102.136.180	192.168.2.5
01/14/22-06:30:38.776945	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.5	217.160.0.10

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-06:30:38.776945	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.5	217.160.0.10
01/14/22-06:30:38.776945	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49809	80	192.168.2.5	217.160.0.10

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 06:29:36.584023952 CET	192.168.2.5	8.8.8.8	0xfd9e	Standard query (0)	www.gnatyuk.info	A (IP address)	IN (0x0001)
Jan 14, 2022 06:29:57.097970963 CET	192.168.2.5	8.8.8.8	0x63db	Standard query (0)	www.ar-sands.com	A (IP address)	IN (0x0001)
Jan 14, 2022 06:30:17.898581028 CET	192.168.2.5	8.8.8.8	0x32b1	Standard query (0)	www.allandlewis.com	A (IP address)	IN (0x0001)
Jan 14, 2022 06:30:38.723781109 CET	192.168.2.5	8.8.8.8	0x1403	Standard query (0)	www.bovanuffelen.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 06:29:36.614012957 CET	8.8.8.8	192.168.2.5	0xfd9e	No error (0)	www.gnatyuk.info	gnatyuk.info		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 06:29:36.614012957 CET	8.8.8.8	192.168.2.5	0xfd9e	No error (0)	gnatyuk.info		34.102.136.180	A (IP address)	IN (0x0001)
Jan 14, 2022 06:29:57.117358923 CET	8.8.8.8	192.168.2.5	0x63db	No error (0)	www.ar-sands.com	ar-sands.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 06:29:57.117358923 CET	8.8.8.8	192.168.2.5	0x63db	No error (0)	ar-sands.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 14, 2022 06:30:17.926351070 CET	8.8.8.8	192.168.2.5	0x32b1	No error (0)	www.allandlewis.com	allandlewis.com		CNAME (Canonical name)	IN (0x0001)
Jan 14, 2022 06:30:17.926351070 CET	8.8.8.8	192.168.2.5	0x32b1	No error (0)	allandlewis.com		158.85.87.76	A (IP address)	IN (0x0001)
Jan 14, 2022 06:30:38.754698038 CET	8.8.8.8	192.168.2.5	0x1403	No error (0)	www.bovanuffelen.com		217.160.0.10	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.gnatyuk.info
- www.ar-sands.com
- www.allandlewis.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49776	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 06:29:36.643239975 CET	10148	OUT	GET /t1y0/?j4eTzF=F82LBBwiF2WdFMF0PdT+LyhlKqSByZY+hePS/QYkGxd4nwGUhGJA4bF6+h/WaxW/quis&y2M=JPRlurVHW6 HTTP/1.1 Host: www.gnatyuk.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 06:29:36.760410070 CET	10149	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 14 Jan 2022 05:29:36 GMT Content-Type: text/html Content-Length: 275 ETag: "618be75c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49805	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 06:29:57.137644053 CET	11752	OUT	GET /t1y0/?j4eTzF=X3Ka+jH2pGe9JZJCakhiHHqoQGax0dVQKYvGWJh20Ylx7iFclkHqSNrYISZIlgOBNqtm&y2M=JPRlurVHW6 HTTP/1.1 Host: www.ar-sands.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 14, 2022 06:29:57.255826950 CET	11753	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 14 Jan 2022 05:29:57 GMT Content-Type: text/html Content-Length: 275 ETag: "618be735-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49807	158.85.87.76	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 06:30:18.034102917 CET	11762	OUT	GET /t1y0/?j4eTzF=tLX95BcBGfEhqVleCXtpcNXr5hlqBy02D0w7FqhwVxcUYz1XFX4bZ6eVCxIWz+fQPry/&y2M=JPRlurVHW6 HTTP/1.1 Host: www.allandlewis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 06:30:18.147511005 CET	11764	IN	HTTP/1.1 200 OK Cache-Control: private,no-cache,no-store Content-Type: text/html Server: Microsoft-IIS/8.5 Set-Cookie: ASPSESSIONIDCCTCCBCR=OAOABBHAGPPGABFDAKDGFKKD; path=/ Date: Fri, 14 Jan 2022 05:30:21 GMT Connection: close Content-Length: 7958 Data Raw: 0d 0a 3c 68 74 6d 6c 3e 0d 0a 20 3c 68 65 61 64 3e 0d 0a 20 20 3c 74 69 74 6c 65 3e 4e 61 6d 65 73 50 72 6f 2e 63 61 20 7c 20 52 65 67 69 73 74 65 72 20 77 69 74 68 20 43 6f 6e 66 69 64 65 6e 63 65 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 61 6d 65 73 50 72 6f 2e 63 61 20 7c 20 52 65 67 69 73 74 65 72 20 77 69 74 68 20 43 6f 6e 66 69 64 65 6e 63 65 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 28 64 65 73 63 72 69 70 74 69 6f 6e 29 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 2e 63 61 20 72 65 67 69 73 74 72 61 72 2c 20 2e 63 61 2c 20 2e 63 6f 6d 2c 20 2e 6f 72 67 2c 20 2e 6e 65 74 2c 20 2e 62 69 7a 2c 20 2e 75 73 2c 20 43 61 6e 61 64 61 2c 20 43 61 6e 61 64 69 61 6e 2c 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 73 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 43 6c 61 73 73 69 66 69 63 61 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 53 65 72 76 69 63 65 73 2c 20 44 6f 6d 61 69 6e 20 4e 61 6d 65 20 54 6f 70 20 4c 65 76 65 6c 20 44 6f 6d 61 69 6e 73 22 3e 0d 0a 20 20 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 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 76 69 73 69 74 2d 61 66 74 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 33 30 20 64 61 79 73 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 61 75 74 68 6f 72 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 61 6d 65 73 50 72 6f 2e 63 61 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 69 6d 61 67 65 74 6f 6f 6c 62 61 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 22 3e 0d 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 73 70 72 6f 2e 63 61 2f 69 6d 61 67 65 73 2f 6c 6f 67 6f 2d 32 30 30 78 32 30 30 2e 67 69 66 22 20 2f 3e 0d 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 3a 77 69 64 74 68 22 20 63 6f 6e 74 65 6e 74 3d 22 32 30 30 22 20 2f 3e 0d 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 69 6d 61 67 65 3a 68 65 69 67 68 74 22 20 63 6f 6e 74 65 6e 74 3d 22 32 30 30 22 20 2f 3e 0d 0a 20 20 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 43 41 22 20 2f 3e 0d 0a 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 53 74 79 6c 65 53 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 2f 69 6e 63 6c 75 64 65 2f 73 74 79 6c 65 5f 64 65 66 61 75 6c 74 2e 63 73 73 22 3e 0d 0a 0d 0a 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0d 0a 20 20 66 75 6e 63 74 69 6f 6e 20 64 65 66 61 75 6c 74 53 74 61 74 75 73 28 29 20 7b 0d 0a 20 20 20 77 69 6e 64 6f 77 2e 73 74 61 74 75 73 20 3d 20 27 4e 20 61 20 6d 20 65 20 73 20 50 20 72 20 6f 20 2e 20 63 20 61 27 3b 0d 0a 20 20 7d 0d 0a 20 Data Ascii: <html> <head> <title>NamesPro.ca | Register with Confidence</title> <meta name="title" content=" NamesPro.ca | Register with Confidence"> <meta name="description" content="(description)"> <meta name="keywords" content=".ca registrar, .ca, .com, .org, .net, .biz, .us, Canada, Canadian, domain names"> <meta name="Classification" content="Domain Name Registration Services, Domain Naming, Top Level Domains"> <meta name="robots" conte nt="index, follow"> <meta name="revisit-after" content="30 days"> <meta name="author" content="NamesPro.ca"> <meta http-equiv="imagetoolbar" content="no"> <meta property="og:image" content="https://www.namespro.ca/im ages/logo-200x200.gif" /> <meta property="og:image:width" content="200" /> <meta property="og:image:height" content="200" /> <meta property="og:locale" content="en_CA" /><link rel="StyleSheet" type="text/css" href="/include/sty le_default.css"> <script language="JavaScript" type="text/javascript"> function defaultStatus() { window.status = 'N a m e s P r o . c a'; }

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: 40881-39611-05143-MT103.exe PID: 3456 Parent PID: 1012

General

Start time:	06:28:31
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\40881-39611-05143-MT103.exe"
Imagebase:	0x400000
File size:	246624 bytes
MD5 hash:	A181630FD1086DB2385028FA8C2CD27C
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: 00000000.00000002.239409869.00000000023C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.239409869.00000000023C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.239409869.00000000023C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: 40881-39611-05143-MT103.exe PID: 5244 Parent PID: 3456

General

Start time:	06:28:32
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\40881-39611-05143-MT103.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\40881-39611-05143-MT103.exe"
Imagebase:	0x400000
File size:	246624 bytes
MD5 hash:	A181630FD1086DB2385028FA8C2CD27C
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: 00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.287858068.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.238427747.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.238427747.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.238427747.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.238938380.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.238938380.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.238938380.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.288827083.0000000000D40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.288827083.0000000000D40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.288827083.0000000000D40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.288807717.0000000000D10000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.288807717.0000000000D10000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.288807717.0000000000D10000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.237060416.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.237060416.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.237060416.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5244

General

Start time:	06:28:36
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 00000005.00000000.258001292.0000000006D55000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.258001292.0000000006D55000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.258001292.0000000006D55000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.273422701.0000000006D55000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.273422701.0000000006D55000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.273422701.0000000006D55000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: WWAHost.exe PID: 2924 Parent PID: 3472

General

Start time:	06:28:54
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x7ff797770000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 00000008.00000002.500210356.0000000003C00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.500210356.0000000003C00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.500210356.0000000003C00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.498033167.0000000001000000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.498033167.0000000001000000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.498033167.0000000001000000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.500385650.0000000003C30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.500385650.0000000003C30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.500385650.0000000003C30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1884 Parent PID: 2924

General

Start time:	06:28:59
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\40881-39611-05143-MT103.exe"
Imagebase:	0x150000
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: 6148 Parent PID: 1884

General

Start time:	06:29:00
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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