ID: 552744
Sample Name: m3A3k6ajlu.exe
Cookbook: default.jbs
Time: 17:33:31
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

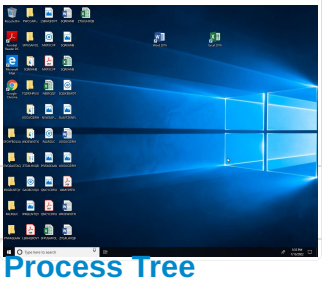
Windows Analysis Report m3A3k6ajlu.exe

Overview

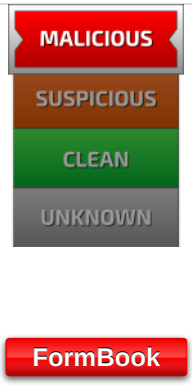
General Information

Sample Name:	m3A3k6ajlu.exe
Analysis ID:	552744
MD5:	6ff998ebcfcb9d4…
SHA1:	affe47369a5d858..
SHA256:	1d5e0028a025d7..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

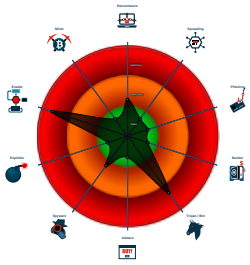


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Machine Learning detection for samp…
- 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**
- m3A3k6ajlu.exe (PID: 6980 cmdline: "C:\Users\user\Desktop\m3A3k6ajlu.exe" MD5: 6FF998EBCFCB9D4FF3B39E9179DCD068)
  - m3A3k6ajlu.exe (PID: 7016 cmdline: "C:\Users\user\Desktop\m3A3k6ajlu.exe" MD5: 6FF998EBCFCB9D4FF3B39E9179DCD068)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 5884 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 5552 cmdline: /c del "C:\Users\user\Desktop\m3A3k6ajlu.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - explorer.exe (PID: 4188 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.rthearts.com/nk6l/"
  ],
  "decoy": [
    "cbnextra.com",
    "entitysystemsinc.com",
    "55midwoodave.com",
    "ebelizzi.com",
    "khojcity.com",
    "1527brokenoakdrive.site",
    "housinghproperties.com",
    "ratiousa.com",
    "lrcrepresentacoes.net",
    "tocoec.net",
    "khadamatdemnate.com",
    "davidkastner.xyz",
    "gardeniaresort.com",
    "qiantangguoji.com",
    "visaprepaidprocessing.com",
    "cristinamadara.com",
    "semapisus.xyz",
    "mpwebagency.net",
    "alibabasdeli.com",
    "gigasupplies.com",
    "quantumskillset.com",
    "eajui136.xyz",
    "patsanchezelpaso.com",
    "trined.mobi",
    "amaturz.info",
    "approveprvqsx.xyz",
    "fronterapost.house",
    "clairewashere.site",
    "xn--3jst70hg8f.com",
    "thursdaynightthriller.com",
    "primacykapjlt.xyz",
    "vaginette.site",
    "olitusd.com",
    "paypal-caseid521.com",
    "preose.xyz",
    "ferbsqlv28.club",
    "iffiliatefreedom.com",
    "okdahotel.com",
    "cochuzyan.xyz",
    "hotyachts.net",
    "diamond-beauties.com",
    "storyofsol.com",
    "xianshucai.net",
    "venusmedicalarts.com",
    "energiaorgonu.com",
    "savannah.biz",
    "poeticdaily.com",
    "wilddalmatian.com",
    "kdydkyqksqucyuyen.com",
    "meanmod.xyz",
    "kaka.digital",
    "viewcision.com",
    "wowzerbackupandrestore-us.com",
    "hydrogendatapower.com",
    "427521.com",
    "ponto-bras.space",
    "chevalsk.com",
    "hnftdl.com",
    "nanasyhogar.com",
    "createacarepack.com",
    "wildkraeuter-wochenende.com",
    "uchihomedeco.com",
    "quintongiang.com",
    "mnbvending.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.360679274.0000000002400000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.360679274.0000000002400000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.360679274.0000000002400000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18839:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.428523251.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.428523251.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.m3A3k6ajlu.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.m3A3k6ajlu.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.m3A3k6ajlu.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a39:$sqlite3step: 68 34 1C 7B E1 • 0x17b4c:$sqlite3step: 68 34 1C 7B E1 • 0x17a68:$sqlite3text: 68 38 2A 90 C5 • 0x17b8d:$sqlite3text: 68 38 2A 90 C5 • 0x17a7b:$sqlite3blob: 68 53 D8 7F 8C • 0x17ba3:$sqlite3blob: 68 53 D8 7F 8C
0.2.m3A3k6ajlu.exe.2400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.m3A3k6ajlu.exe.2400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$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
Multi AV Scanner detection for domain / URL
Multi AV Scanner detection for dropped file
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:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique
Maps a DLL or memory area into another process
Injects a PE file into a foreign processes
Queues an APC in another process (thread injection)
Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

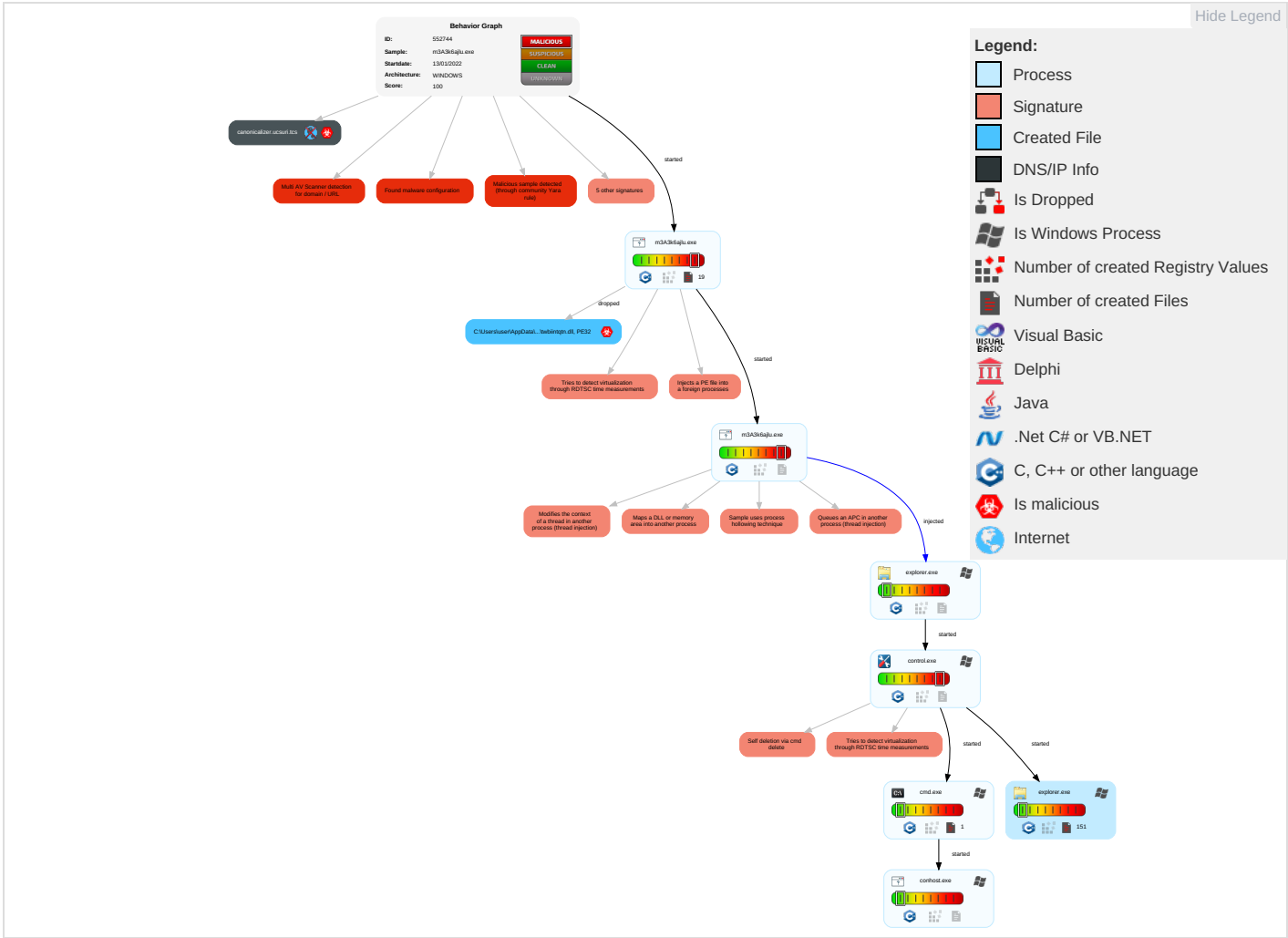
Yara detected FormBook

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	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	File Deletion 1	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
m3A3k6ajlu.exe	39%	Virustotal		Browse
m3A3k6ajlu.exe	41%	ReversingLabs	Win32.Trojan.Tnega	
m3A3k6ajlu.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsaD190.tmp\twbiintqtn.dll	28%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsaD190.tmp\twbiintqtn.dll	36%	ReversingLabs	Win32.Trojan.Tnega	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.m3A3k6ajlu.exe.2400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.1.m3A3k6ajlu.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.m3A3k6ajlu.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.m3A3k6ajlu.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.m3A3k6ajlu.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.m3A3k6ajlu.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.rthearts.com/nk6l/	6%	Virustotal		Browse
www.rthearts.com/nk6l/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
canonicalizer.ucsuri.tcs	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.rthearts.com/nk6l/	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552744
Start date:	13.01.2022
Start time:	17:33:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	m3A3k6ajlu.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:	24
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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/4@5/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 22.4% (good quality ratio 20.9%) • Quality average: 77.7% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 79% • 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\afrykf2i1n03fpc5

Process:	C:\Users\user\Desktop\m3A3k6ajlu.exe

C:\Users\user\AppData\Local\Temp\afrykf2i1n03fpc5	
File Type:	data
Category:	dropped
Size (bytes):	217196
Entropy (8bit):	**7.992350964417339**
Encrypted:	**true**
SSDEEP:	3072:/uxdCyaJCp9Pgtm5S3F+Tt+pSVAvr5QdDeo/tesUtU1R6nbXaMqaIzL29Bdr:/4Cykn3Fct8j5AD9VJUG6mta/r
MD5:	492C0B3F8E7DA6E807279FBDF3653293
SHA1:	8BCB777CBDB94C26A79CD4407EFA6D3CEDEBAA90
SHA-256:	7F6A197449C1D9ADEA4A7EAD887D9E2F33784C94706D1A7B971A0888279C6E3A
SHA-512:	9584078D6672ED63CFD24D08B298F24F4492D7743DD1349099DD0AAD96B7CAF853B5307DBB2E54DC91A76C4BF5A5210D56CD4F576A9D59109D7C0C2F3F543E
Malicious:	false
Reputation:	low
Preview:	..Il.R...g6X...=Ia)?."[.....S.0*...0+...vTE.Y...B.&.I..Q}.w]..?.{t_...s...6..L}__..$.u9.....ygu.:.Y.%../$?.a...."x._.{.5D..'".N.....a...'P.e8..... ..{?.sL8.....v.....IW.>.....v._=.I...3..-...5....q.0S.N^9.....drG7.>I...#...WY.M.J.G.|c..OS...R.6x.te.....).;.`...y&B.*..0-...v{E.....B.&.I..Q}.w4..?c.g..+.o.`.....>.....\.{.Ls...z.9. .w..qR8~..>|.Wx.5D..Z..V..1.g%*]v...w.Z...sA. ..D.?D^....5J..\.d...IW.>...L..h.v..K3I..3...S5....qB0....A...).....drG*.\I...#.}.WY...J.G..c.O....R..x.te...M.).Y;.`....&.0*...0+...vTE.Y...B.&.I..Q}.w4..?c.g..+.o.`.....>.....\.{.Ls...z.9. .w..qR8~..>|.Wx.5D..Z..V..1.g%*]v...w.Z...sA...D.?D^....5J..\.d...IW.>.....v....I.D.3.R..5....qB0....A...).....drG*.\I...#.}.WY...J.G..c.O....R..x.te...M.).Y;.`....&.0*...0+...vTE.Y...B. &.I..Q}.w4..?c.g..+.o.`.....>.....\.{.Ls...z.9. .w..qR8~..>|.Wx.5D..Z..V..1.g%*]v...w.Z...sA...D.?D^....5J..\.d...IW.>.....v....I.D.3.R..5....qB0....A...).....drG

C:\Users\user\AppData\Local\Temp\entjucon	
Process:	C:\Users\user\Desktop\m3A3k6ajlu.exe
File Type:	data
Category:	dropped
Size (bytes):	5244
Entropy (8bit):	6.121856063921895
Encrypted:	false
SSDEEP:	96:V+W0fvRq4Qjca2l1RWgjJhUIpVbGnUsl0ptmCuS9wSPfSYP3Txv2YV:V+NRFQVaLjrUIXGnMuS9/SkZ2K
MD5:	7D238BBFDF1017D7F0100F56F12907F9
SHA1:	7BC67E3D025507551A580B5557AB9DE2EB50C8F7
SHA-256:	9CB16A18C15E621D9465C37D1ABA82CD04ECB64238EC385BF6BFD5995F69670A
SHA-512:	7E6526A884AD599316A6405E130FD6F33D3F6B9DBCF34EA11BF8AE6890B2AB1CC982D33077AEB631631C4FE8452F3629184F7917366E13C98627E70992784D5B
Malicious:	false
Reputation:	low
Preview:	&3.....'.'.....+...[....;..[....#....D......../.....#.....3..7.....##.....K..O.....#P.....C..G.....#Y.....[..._.....[..v..;..?....#..F..#..'..#.....^.M.....# ....]...../.?+..#.....H....3...K...C... [...;...#...../..)..+..3.....+ ..#....D.....H../....+....".]....'....[.....^.....^.....".].....A.#....#....]....<.#....#....]....x.#....#....]....'.'...[....#D.....3.....A..... .....(?#.....[.....v....F....3...7..#v...^>....3...7.....[....3...<.#N....#I...../(...#....#...../../.....+.(.D.+.....+.".].....'.'...[....#D.....[.....A.....(?#.....[.....v....F....[..._...v...^>....[. ..._...v...N>...[..._....F....M ...[..._..#v...^>....[..._.....[....[...A.#!....#@...../.....#....(.....#...../../.....+.(.D.+.....+.".].....'.'.D.....?.....A.....(?#. ...[.....v....F....?...#...v. ..^>....?...#.....[....?...x.#.....#...../(...

C:\Users\user\AppData\Local\Temp\nsaD18F.tmp	
Process:	C:\Users\user\Desktop\m3A3k6ajlu.exe
File Type:	data
Category:	dropped
Size (bytes):	452173
Entropy (8bit):	7.081240704036401
Encrypted:	false
SSDEEP:	6144:n0u4Cykn3Fct8j5AD9VJUG6mta/wUtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:0xt8N69VJUSaonCYFD6TG9pjni6v
MD5:	E195AE799CE29E50A3DB9CCF0853F380
SHA1:	409B4A8645FDA4BAEC9679703F0F69A1D16E0C03
SHA-256:	4BE5FDEB58D410FB91680841B78286BCAB2F3FDE860FC25FF846E5AC182A0148
SHA-512:	0D00A845E233716337881E4A6610FA0CAD46741EF815C81C334CE977064B8895F7F1C092D3F74CDBD76D30BC8637EAF6D45B4A96EF6E274A936ACCEBD4072F4
Malicious:	false
Reputation:	low
Preview:	Uw.....,.....\.....ov.....=w.....2..... .....J.....j.....Q.....H..... ....

C:\Users\user\AppData\Local\Temp\nsaD190.tmp\twbiintqtn.dll	
Process:	C:\Users\user\Desktop\m3A3k6ajlu.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199168
Entropy (8bit):	5.818225992861307
Encrypted:	false
SSDEEP:	6144:+UtJEr7mQNzZ/vDXqxnfNahvFp1cck4X3rm6v:+nCYFD6TG9pjni6v

C:\Users\user\AppData\Local\Temp\nsaD190.tmp\twbiintqtn.dll	
MD5:	835007A7E91DC05F1DFFAB07F1032942
SHA1:	7B2553283FF1000FF5B3E5CB2093FBEDBDB38456
SHA-256:	BB411A18C9CAB163E8BED9CBB17E71D71A42A2A18E7838964EA26E3A525DAF5D
SHA-512:	47E4494FCDC4482E3CFBCCFDCE043E8D442D5271F7F8487B906A325F8F65EB57F51E3C0F7CC0580B6E11190667E72A79396B4852AB4A66E53E157B53B14D74F
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 28%, Browse • Antivirus: ReversingLabs, Detection: 36%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...B...B...B.....B..C...B...C...B.a.F...B.a.B...B.d.....B.a.@...B.R ich..B.....PE..L.....a.....!.....@.....@.....0..x..... .....text...k..... ..`.rdata.....@..@.rsrc..... .....@..@.reloc..x....0.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.961651041066942
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:	m3A3k6ajlu.exe
File size:	368319
MD5:	6ff998ebcfcb9d4ff3b39e9179dcd068
SHA1:	affe47369a5d85864c64783eae960d59782aa841
SHA256:	1d5e0028a025d76c09fbf798a8a3311ed7477c985b16ae8078b110e762778154
SHA512:	646d8d72d9e8e897c3804fda817f515fd6c211c9404a64ae9cd53cef744ed55f9b56cc8f995babe1ebdb5bbe9bec383d737641e1912d65a660e5384dfe055019
SSDEEP:	6144:ow1pLD7oRXWVfah8cj3g7s7b1dFY6E0s2bzxU89YPbP2jOf/f28pqwNgPSe:3/7SWtQ8u3gsBfE0bbzxtubPwOusFSPV
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:	b2a88c96b2ca6a72

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

General

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	0x900	0xa00	False	0.409375	data	3.94693169534	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
01/13/22-17:35:59.956418	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.6

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 17:37:01.568332911 CET	192.168.2.6	8.8.8.8	0x7a17	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Jan 13, 2022 17:37:02.576399088 CET	192.168.2.6	8.8.8.8	0x7a17	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 17:37:03.576450109 CET	192.168.2.6	8.8.8.8	0x7a17	Standard query (0)	canonicali zer.ucsuri.tcs	A (IP address)	IN (0x0001)
Jan 13, 2022 17:37:05.592150927 CET	192.168.2.6	8.8.8.8	0x7a17	Standard query (0)	canonicali zer.ucsuri.tcs	A (IP address)	IN (0x0001)
Jan 13, 2022 17:37:09.608030081 CET	192.168.2.6	8.8.8.8	0x7a17	Standard query (0)	canonicali zer.ucsuri.tcs	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: m3A3k6ajlu.exe PID: 6980 Parent PID: 5228

General

Start time:	17:34:31
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\m3A3k6ajlu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\m3A3k6ajlu.exe"
Imagebase:	0x400000
File size:	368319 bytes
MD5 hash:	6FF998EBCFCB9D4FF3B39E9179DCD068
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: 00000000.00000002.360679274.0000000002400000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.360679274.0000000002400000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.360679274.0000000002400000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: m3A3k6ajlu.exe PID: 7016 Parent PID: 6980

General

Start time:	17:34:33
Start date:	13/01/2022
Path:	C:\Users\user\Desktop\m3A3k6ajlu.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\m3A3k6ajlu.exe"
Imagebase:	0x400000
File size:	368319 bytes
MD5 hash:	6FF998EBCFCB9D4FF3B39E9179DCD068
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: 00000001.00000002.428523251.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.428523251.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.428523251.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.429655920.0000000000D40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.429655920.0000000000D40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.429655920.0000000000D40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.356571950.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.356571950.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.356571950.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.358044530.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.358044530.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.358044530.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.359077478.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.359077478.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.359077478.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.428966747.00000000009E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.428966747.00000000009E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.428966747.00000000009E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 7016

General

Start time:	17:34:37
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.397979738.000000000F648000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.397979738.000000000F648000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.397979738.000000000F648000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: control.exe PID: 5884 Parent PID: 3440

General

Start time:	17:35:03
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0x210000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5552 Parent PID: 5884

General

Start time:	17:35:09
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\m3A3k6ajlu.exe"
Imagebase:	0x2a0000
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: 5392 Parent PID: 5552

General

Start time:	17:35:11
Start date:	13/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 4188 Parent PID: 2932

General

Start time:	17:35:42
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Modified

Disassembly

Code Analysis