

JoeSandbox Cloud BASIC



ID: 483532

Sample Name: arrival notice.exe

Cookbook: default.jbs

Time: 08:27:14

Date: 15/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report arrival notice.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: FormBook	4
Yara Overview	5
Memory Dumps	5
Unpacked PEs	6
Sigma Overview	7
System Summary:	7
Jbx Signature Overview	7
AV Detection:	7
Networking:	7
E-Banking Fraud:	7
System Summary:	7
Data Obfuscation:	7
Hooking and other Techniques for Hiding and Protection:	7
Malware Analysis System Evasion:	7
HIPS / PFW / Operating System Protection Evasion:	7
Stealing of Sensitive Information:	8
Remote Access Functionality:	8
Mitre Att&ck Matrix	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	10
Initial Sample	10
Dropped Files	10
Unpacked PE Files	10
Domains	10
URLs	10
Domains and IPs	11
Contacted Domains	11
Contacted URLs	11
URLs from Memory and Binaries	11
Contacted IPs	11
General Information	11
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASN	12
JA3 Fingerprints	12
Dropped Files	12
Created / dropped Files	12
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Data Directories	13
Sections	13
Resources	14
Imports	14
Version Infos	14
Network Behavior	14
Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	14
Analysis Process: arrival notice.exe PID: 6556 Parent PID: 6520	14
General	14
File Activities	15
File Created	15
File Written	15
File Read	15
Analysis Process: arrival notice.exe PID: 7160 Parent PID: 6556	15
General	15

Analysis Process: arrival notice.exe PID: 3436 Parent PID: 6556	15
General	15
File Activities	16
File Read	16
Analysis Process: explorer.exe PID: 3424 Parent PID: 3436	16
General	16
Analysis Process: cmstp.exe PID: 6820 Parent PID: 3436	16
General	17
File Activities	17
File Read	17
Analysis Process: cmd.exe PID: 5948 Parent PID: 6820	17
General	17
File Activities	17
Analysis Process: conhost.exe PID: 1260 Parent PID: 5948	18
General	18
Analysis Process: explorer.exe PID: 4824 Parent PID: 6068	18
General	18
File Activities	18
Registry Activities	18
Disassembly	18
Code Analysis	18

Windows Analysis Report arrival notice.exe

Overview

General Information

Sample Name:	arrival notice.exe
Analysis ID:	483532
MD5:	4196c697fa8a52e..
SHA1:	1179a7916f59fa2..
SHA256:	cfdb27a9ff39bd1...
Tags:	exe
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

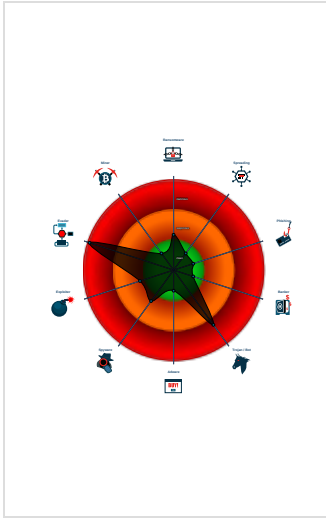
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through ...
- Yara detected AntiVM3
- Sample uses process hollowing tech...
- Maps a DLL or memory area into an ...
- Initial sample is a PE file and has a ...
- Tries to detect sandboxes and other...
- Machine Learning detection for samp...
- Self deletion via cmd delete
- .NET source code contains potentia...

Classification



Process Tree

- System is w10x64
- arrival notice.exe (PID: 6556 cmdline: 'C:\Users\user\Desktop\arrival notice.exe' MD5: 4196C697FA8A52ECDDAD63BF5AC9E8F9)
 - arrival notice.exe (PID: 7160 cmdline: C:\Users\user\Desktop\arrival notice.exe MD5: 4196C697FA8A52ECDDAD63BF5AC9E8F9)
 - arrival notice.exe (PID: 3436 cmdline: C:\Users\user\Desktop\arrival notice.exe MD5: 4196C697FA8A52ECDDAD63BF5AC9E8F9)
 - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
 - cmstp.exe (PID: 6820 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
 - cmd.exe (PID: 5948 cmdline: /c del 'C:\Users\user\Desktop\arrival notice.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
 - conhost.exe (PID: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
 - explorer.exe (PID: 4824 cmdline: 'C:\Windows\explorer.exe' /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- cleanup

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nordicbatterybelt.net/n58i/"
  ],
  "decoy": [
    "southerncircumstance.com",
    "mcsasco.com",
    "ifbrick.com",
    "societe-anonyme.net",
    "bantank.xyz",
    "dogecoin.beauty",
    "aboutacoffee.com",
    "babalandlordrealestate.com",
    "tintgta.com",
    "integrity.directory",
    "parwnr.icu",
    "poltishof.online",
    "stayandstyle.com",
    "ickjeame.xyz",
    "currentmotors.ca",
    "pond.fund",
    "petrosterzis.com",
    "deadbydaylightpoints.com",
    "hotel-balzac.paris",
    "focusmaintainance.com",
    "odeonmarket.com",
    "voeran.net",
    "lookailpop.xyz",
    "sashaignatenko.com",
    "royalgreenvillage.com",
    "airbhouse.com",
    "zl-dz.com",
    "fuwuxz.com",
    "wugupihuhepop.xyz",
    "zndhysm.com",
    "luchin.site",
    "rnchaincvkbip.xyz",
    "ffffddfrfaffrtgthhhbhfgr.com",
    "goabbasoon.info",
    "booyahbucks.com",
    "ilovecoventry.com",
    "components-electronics.com",
    "advindustry.com",
    "browandline.com",
    "hotnspicy.site",
    "marlonj26.com",
    "holidays24.net",
    "starworks.online",
    "mbchaindogbbc.xyz",
    "3wouqg.com",
    "evnfreesx.com",
    "baureihe51.com",
    "hycelassetmanagement.space",
    "photostickomni-trendyfinds.com",
    "singisa4letterword.com",
    "thklw.online",
    "menramen.com",
    "highspeedinternetinc.com",
    "beerenhunger.info",
    "hisensor.world",
    "lassurancevalence.com",
    "clementchanlab.com",
    "customia.xyz",
    "alysvera-centroestetico.com",
    "cx-xiezu.com",
    "index-mp3.com",
    "mybenefits51.com",
    "vyhozoi.site",
    "lingerista.net"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.753650396.00000000012B 0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.753650396.00000000012B 0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x85f8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8992:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14191:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1491f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93aa:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1340c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa122:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19b97:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac3a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.753650396.00000000012B 0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x16ac9:\$sqlite3step: 68 34 1C 7B E1 0x16bdc:\$sqlite3step: 68 34 1C 7B E1 0x16af8:\$sqlite3text: 68 38 2A 90 C5 0x16c1d:\$sqlite3text: 68 38 2A 90 C5 0x16b0b:\$sqlite3blob: 68 53 D8 7F 8C 0x16c33:\$sqlite3blob: 68 53 D8 7F 8C
0000000E.00000002.987277254.0000000002E0 0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.987277254.0000000002E0 0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x85f8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8992:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14191:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1491f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93aa:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1340c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa122:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19b97:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac3a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.arrival notice.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.arrival notice.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x77f8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x7b92:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x138a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x13391:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x139a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x13b1f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x85aa:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1260c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9322:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18d97:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19e3a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.arrival notice.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x15cc9:\$sqlite3step: 68 34 1C 7B E1 0x15ddc:\$sqlite3step: 68 34 1C 7B E1 0x15cf8:\$sqlite3text: 68 38 2A 90 C5 0x15e1d:\$sqlite3text: 68 38 2A 90 C5 0x15d0b:\$sqlite3blob: 68 53 D8 7F 8C 0x15e33:\$sqlite3blob: 68 53 D8 7F 8C
5.2.arrival notice.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.arrival notice.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x85f8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8992:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146a5:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14191:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147a7:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1491f:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93aa:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1340c:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa122:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19b97:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac3a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

System Summary:



Sigma detected: CMSTP Execution Process Creation

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:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected FormBook

System Summary:



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:



Self deletion via cmd delete

Malware Analysis System Evasion:



Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:



Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:



Yara detected FormBook

Remote Access Functionality:



Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 5 1 2	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Application Layer Protocol 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arrival notice.exe	30%	Virustotal		Browse
arrival notice.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	
arrival notice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.arrival notice.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adoqw	0%	Avira URL Cloud	safe	
http://crl.v	0%	URL Reputation	safe	
www.nordicbatterybelt.net/n58i/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.nordicbatterybelt.net/n58i/	true	<ul style="list-style-type: none"> Avira URL Cloud: safe 	low

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483532
Start date:	15.09.2021
Start time:	08:27:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arrival notice.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:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none"> HCA enabled EGA enabled HDC enabled AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> Successful, ratio: 19.6% (good quality ratio 17.5%) Quality average: 73.5% Quality standard deviation: 31.9%
HCA Information:	<ul style="list-style-type: none"> Successful, ratio: 100% Number of executed functions: 0 Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> Adjust boot time Enable AMSI Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:28:10	API Interceptor	1x Sleep call for process: arrival notice.exe modified
08:29:44	API Interceptor	111x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context


JA3 Fingerprints

No context

Dropped Files

No context


Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\arrival notice.exe.log		
Process:	C:\Users\user\Desktop\arrival notice.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1216	
Entropy (8bit):	5.355304211458859	
Encrypted:	false	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E	
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6	
Malicious:	true	
Reputation:	high, very likely benign file	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21	

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.378713027704192
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) Net Framework (10011505/4) 49.83%Win32 Executable (generic) a (10002005/4) 49.78%Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%Generic Win/DOS Executable (2004/3) 0.01%DOS Executable Generic (2002/1) 0.01%
File name:	arrival notice.exe
File size:	780288
MD5:	4196c697fa8a52ecddad63bf5ac9e8f9
SHA1:	1179a7916f59fa2d88829a56f3f045e1cf32c418
SHA256:	cfdb27a9ff39bd1aa5a0a43fe6e272c269a311f5748d8a13b2e705f7d66f16bd
SHA512:	8c78d2a8276fd10c118732b194865fcd40615beb8ad47459e0ce5c67097d57d66c5764c0eaf8ebdbb7591b3ff03c26f0aa90d7dd7484b8f4709c9a79c607d5a0
SSDEEP:	6144:bThvfD5IQDbCMN4K4CwdAbOo3kUnVVorbclLuKUCHWGYGSL5w2P3g6zsGJO5SVkGw:PWHCM2K4CLAOwb+uxvDfvrso6SE+7k
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......PE..L...].0.....>.....@..@..... ..@.....

File Icon

	
Icon Hash:	76d9635381490100

Static PE Info

General	
Entrypoint:	0x48c7ba
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:	0xD983B25D [Wed Aug 22 02:45:49 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8a7c0	0x8a800	False	0.766751396097	data	7.21116196113	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x8e000	0x33a9c	0x33c00	False	0.128995886171	data	2.6232852429	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	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

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: arrival notice.exe PID: 6556 Parent PID: 6520

General

Start time:	08:28:07
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\arrival notice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\arrival notice.exe'
Imagebase:	0x250000
File size:	780288 bytes
MD5 hash:	4196C697FA8A52ECDDAD63BF5AC9E8F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	<ul style="list-style-type: none"> • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.672365867.00000000035F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.672365867.00000000035F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.672365867.00000000035F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.672532960.00000000036F2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.672532960.00000000036F2000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.672532960.00000000036F2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.672048372.00000000025F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: arrival notice.exe PID: 7160 Parent PID: 6556

General

Start time:	08:28:13
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\arrival notice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\arrival notice.exe
Imagebase:	0x330000
File size:	780288 bytes
MD5 hash:	4196C697FA8A52ECDDAD63BF5AC9E8F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: arrival notice.exe PID: 3436 Parent PID: 6556

General

Start time:	08:28:13
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\arrival notice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\arrival notice.exe
Imagebase:	0xb50000
File size:	780288 bytes
MD5 hash:	4196C697FA8A52ECDDAD63BF5AC9E8F9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.753650396.00000000012B0000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.753650396.00000000012B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.753650396.00000000012B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.752247585.000000000400000.00000040.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.752247585.000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.752247585.000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.753557009.0000000001280000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.753557009.0000000001280000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.753557009.0000000001280000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 3436

General	
Start time:	08:28:15
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.712937418.000000000EC67000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.712937418.000000000EC67000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.712937418.000000000EC67000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.699881557.000000000EC67000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.699881557.000000000EC67000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.699881557.000000000EC67000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: cmstp.exe PID: 6820 Parent PID: 3436

General	
Start time:	08:28:51
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x990000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.987277254.0000000002E00000.00000004.00000001.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.987277254.0000000002E00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.987277254.0000000002E00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.986144684.00000000007B0000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.986144684.00000000007B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.986144684.00000000007B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.987219865.0000000002DD0000.00000040.00020000.sdmp, Author: Joe Security Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.987219865.0000000002DD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.987219865.0000000002DD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5948 Parent PID: 6820

General	
Start time:	08:28:53
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\arrival notice.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: 1260 Parent PID: 5948

General

Start time:	08:28:54
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 4824 Parent PID: 6068

General

Start time:	08:29:43
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\explorer.exe' /LOADSAVEDWINDOWS
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](#)

Registry Activities

[Show Windows behavior](#)

Disassembly

Code Analysis