ID: 321436
Sample Name:
acceptable_use_policy.docm
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 06:11:03
Date: 22/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

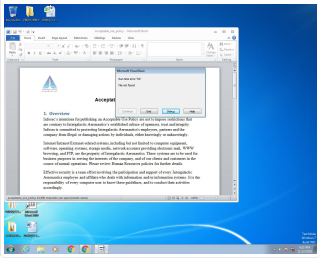
Analysis Report acceptable_use_policy.docm

Overview

General Information

Sample Name:	acceptable_use_policy.docm
Analysis ID:	321436
MD5:	d651d3331b60ee..
SHA1:	bb816e1502b0ba..
SHA256:	a0a9eca457bd72..

Most interesting Screenshot:



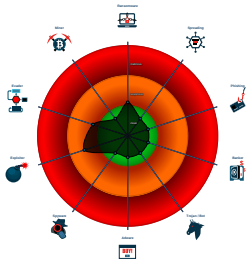
Detection

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Machine Learning detection for samp…
- Allocates a big amount of memory (p…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Document contains no OLE stream …
- Document has an unknown applicati…
- IP address seen in connection with o…
- JA3 SSL client fingerprint seen in co…
- Potential document exploit detected

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2312 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

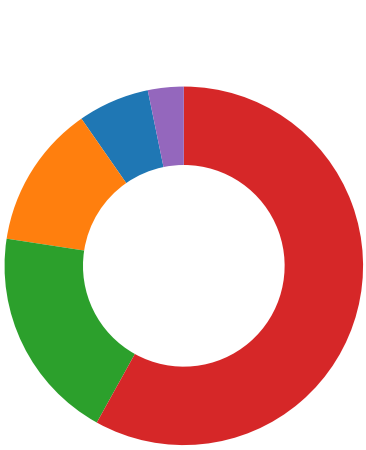
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

● AV Detection



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

System Summary:

Document contains an embedded VBA macro which may execute processes

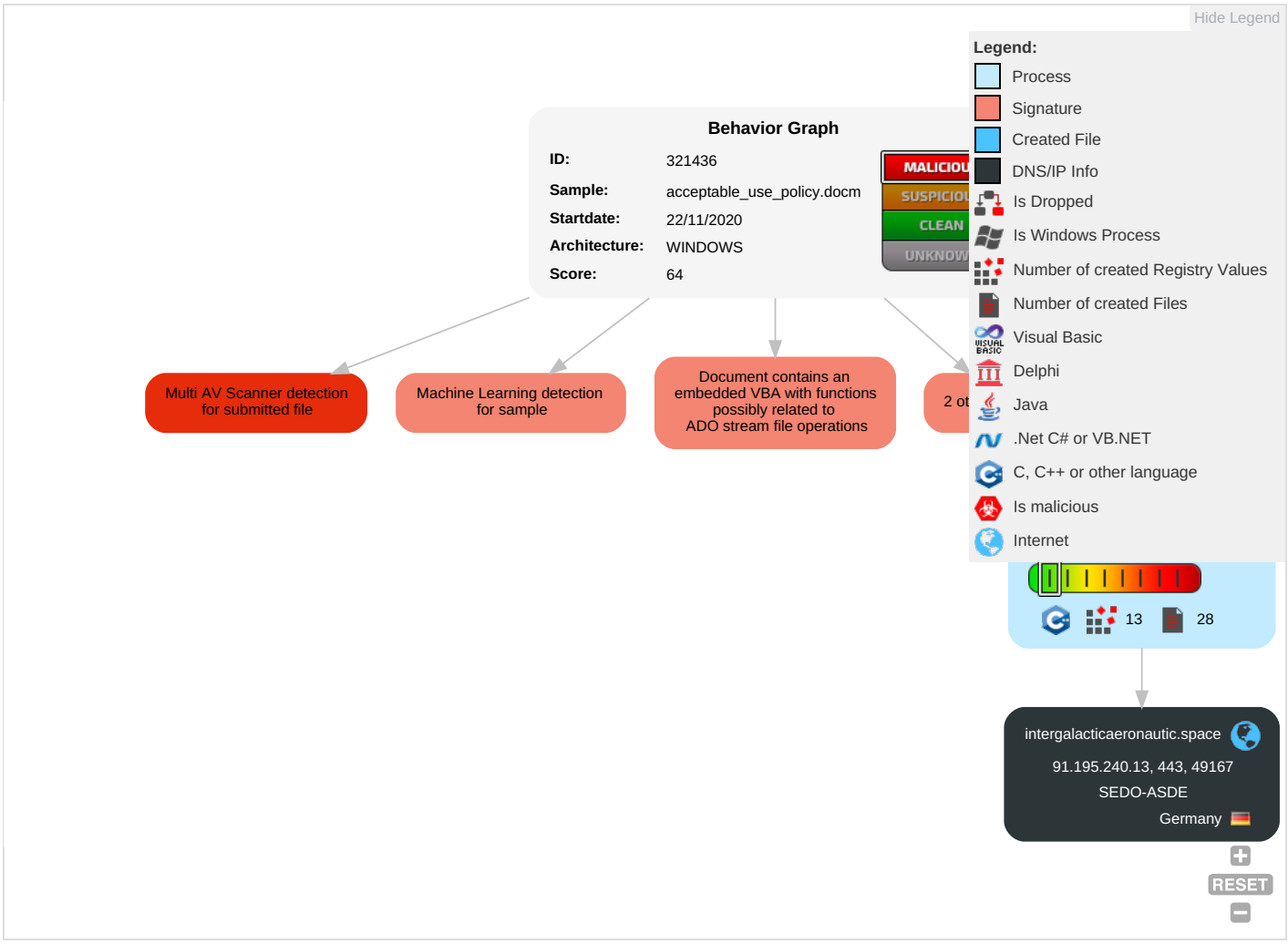
Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA with functions possibly related to HTTP operations

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Im
Valid Accounts	Scripting 3 2	Path Interception	Extra Window Memory Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mc Sy Pa
Default Accounts	Exploitation for Client Execution 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Scripting 3 2	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Extra Window Memory Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Card Swap		Ca Bil Fra

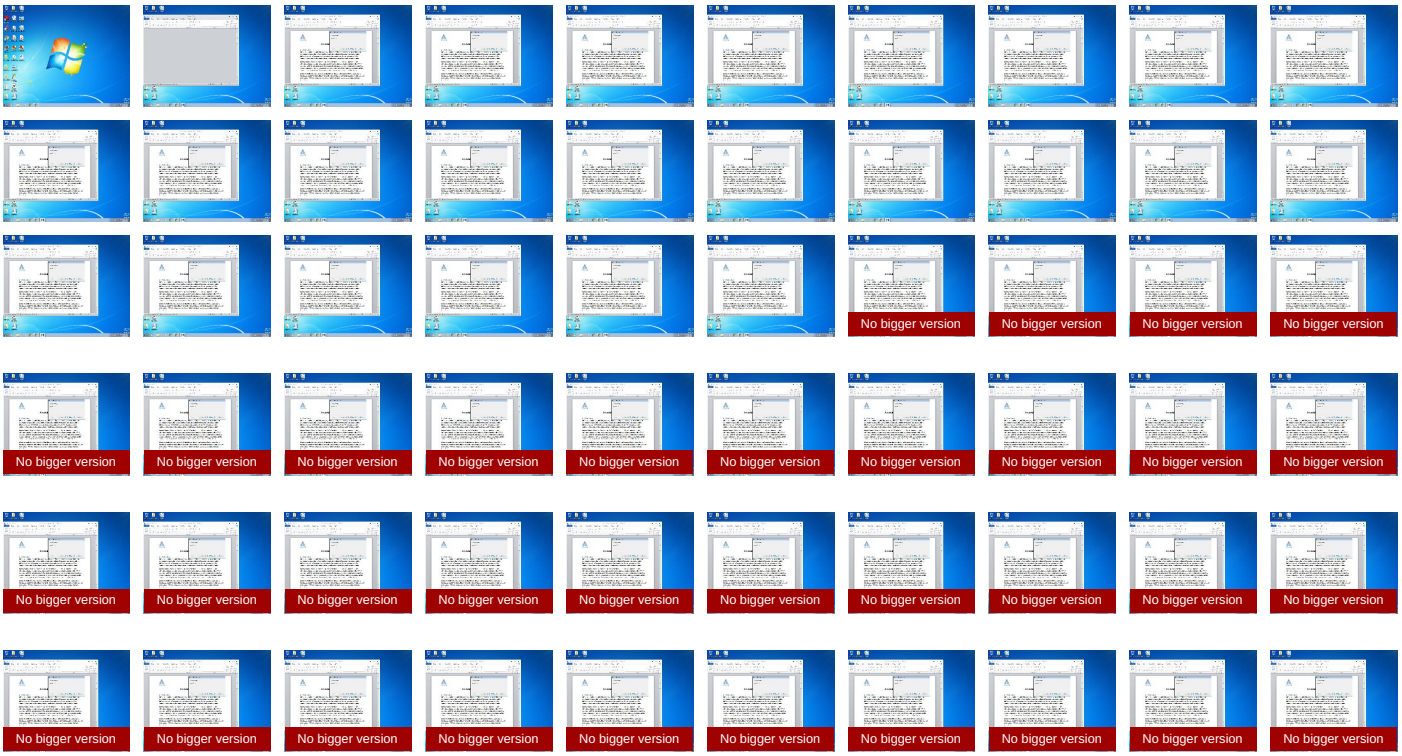
Behavior Graph

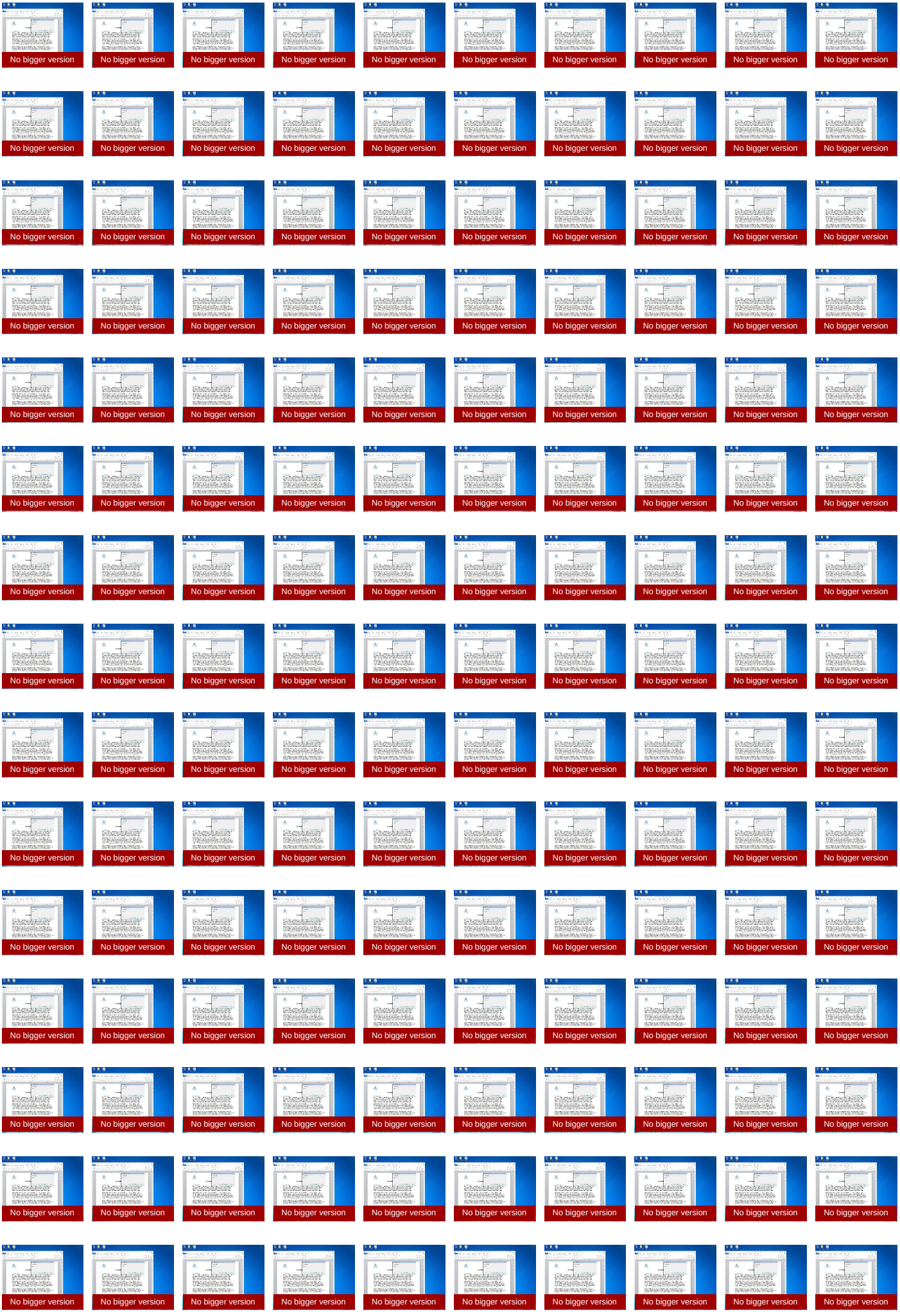


Screenshots

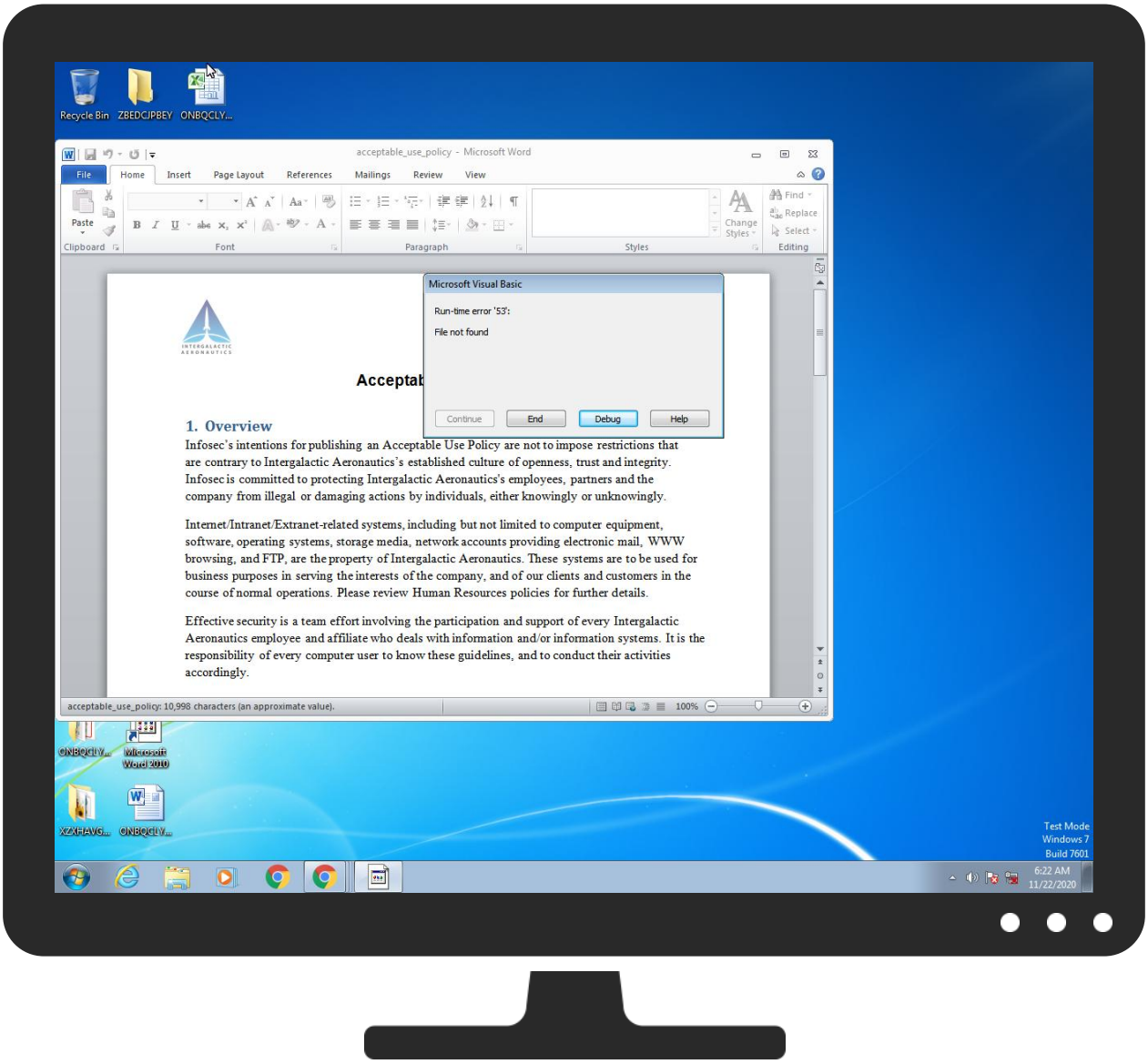
Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.






No bigger version



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
acceptable_use_policy.docm	60%	Virustotal		Browse
acceptable_use_policy.docm	48%	ReversingLabs	Script.Downloader.Obfuser	
acceptable_use_policy.docm	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
intergalacticaeronautic.space	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://intergalacticaeronautic.space/lsass.exe	2%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://https://intergalacticaeronautic.space/lsass.exe	0%	Avira URL Cloud	safe	
http://https://intergalacticaeronautic.space/win32.exe	0%	Avira URL Cloud	safe	

Domains and IPs

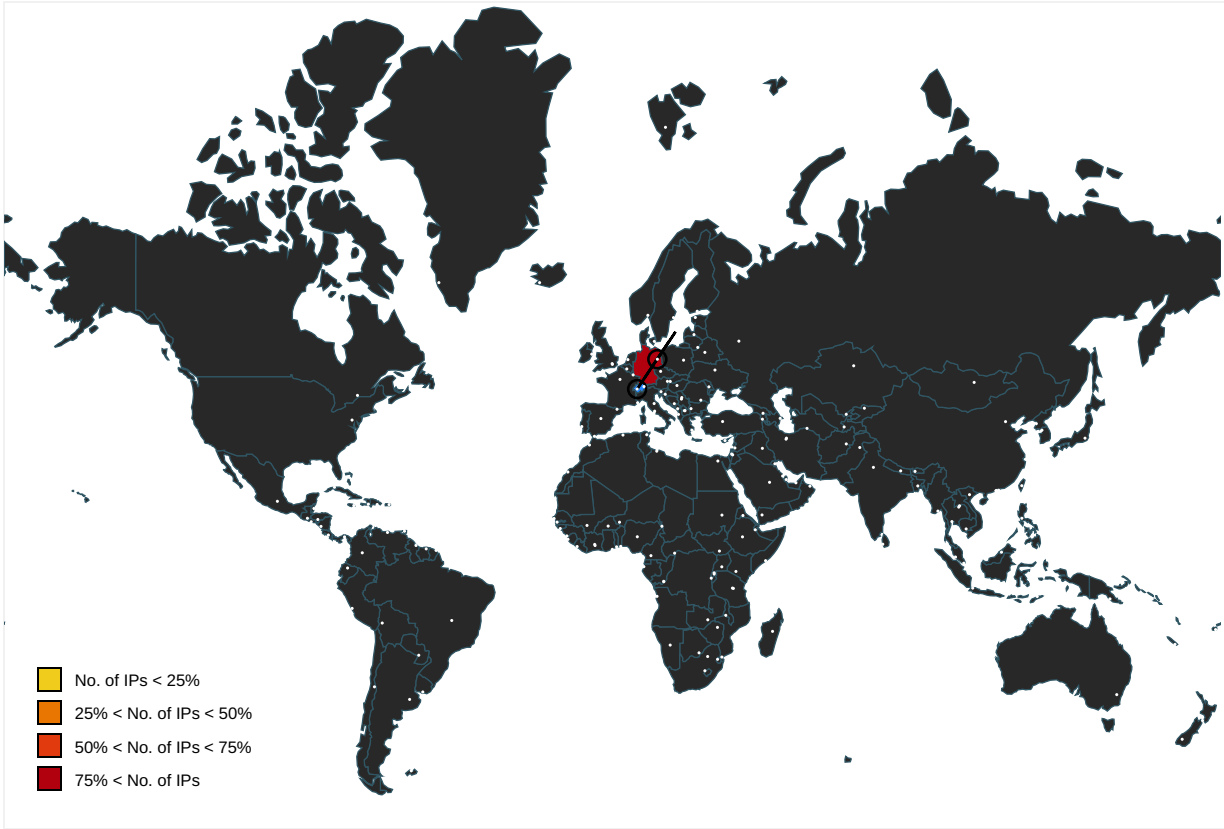
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
intergalacticaeronautic.space	91.195.240.13	true	false	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://intergalacticaeronautic.space/lsass.exe	vbaProject.bin	false	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.sans.org/security-resources/glossary-of-terms/	~WRS{EC050284-DAE8-4269-85E5-42AB58328FB4}.tmp.0.dr	false		high
http://https://intergalacticaeronautic.space/win32.exe	vbaProject.bin	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.240.13	unknown	Germany		47846	SEDO-ASDE	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321436
Start date:	22.11.2020

Start time:	06:11:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	acceptable_use_policy.docm
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	3
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:	• EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.winDOCM@1/8@1/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docm
Warnings:	Show All • Max analysis timeout: 720s exceeded, the analysis took too long • Exclude process from analysis (whitelisted): dllhost.exe • Report size exceeded maximum capacity and may have missing behavior information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.13	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• www.smobz.com/ukj/?Ezu=6QwYUCSLPFcKJYuBdUDYqHrTALkpF8bqM6rRkIucBz4KsP3ogUDK0i/zbdTcuU1sFZfY&lhuL6=Txol_LV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#Uc720#Ud2f0#Uc544#Uc774#Ud14c#Ud06c-#Ubc1c#Uc8fc#Uc11c #Uc1a1#Ubd80#Uc758#Uac74.exe	Get hash	malicious	Browse	• www.smobz.com/ukj/?BZ=6QwYUCSLPFcKJYuBdUDYqHrTALkpF8bqM6rRkIucBz4KsP3ogUDK0i/zbdT2xkFsBbXY&I48=4hOl78_
	nel.exe	Get hash	malicious	Browse	• www.office421.com/ns424/?KzrPX=kzrxP8&lJEpgpp=Cbpn9HPdnDvxKwh9tZDgvWZ3FWN5DdzTd5Eh64pT0MIinpxEBbCqVi4obr5cHTy4QQ+KEGF/dw==
	168768566-104646-sdfnt5-8.exe	Get hash	malicious	Browse	• www.app7924.com/sr1/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
intergalacticaeronautic.space	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 3.17.65.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEDO-ASDE	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• 91.195.241.137
	new file.exe.exe	Get hash	malicious	Browse	• 91.195.241.136
	Bonifico n.1101202910070714.exe	Get hash	malicious	Browse	• 91.195.241.136
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 91.195.241.136
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 91.195.241.136
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136
	http://ww1.0ffice.com/	Get hash	malicious	Browse	• 91.195.240.14
	New Additional Agreement.exe	Get hash	malicious	Browse	• 91.195.240.94
	UBEH7JEUC0.exe	Get hash	malicious	Browse	• 91.195.241.136
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• 91.195.240.13
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	ORDER7098EAR.exe	Get hash	malicious	Browse	• 91.195.241.136
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• 91.195.240.94
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	acceptable_use_policy.docm	Get hash	malicious	Browse	• 91.195.240.13
	Fennec Pharma .docx	Get hash	malicious	Browse	• 91.195.240.13
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH & WIRE REMITTANCE ADVICE.xlsx	Get hash	malicious	Browse	• 91.195.240.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 91.195.240.13
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 91.195.240.13
	http://https://www.lnepia.com.cn/app/4gnf/tiaoban.php	Get hash	malicious	Browse	• 91.195.240.13
	#U0648#U0631#U0634#U0629 #U0639#U0645#U0644 #U062a#U062f#U0631#U06cc#U0628#U06cc#U0629.doc	Get hash	malicious	Browse	• 91.195.240.13
	doc2227740.xls	Get hash	malicious	Browse	• 91.195.240.13
	POSH XANADU Order-SP-20093000-xlxs.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	d11311145.xls	Get hash	malicious	Browse	• 91.195.240.13
	MV GRAN LOBO 008.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH - WIRE PAYMENT REMITTANCE.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACHWIRE REMITTANCE ADVICE..xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH WIRE REMITTANCE PAYMENT.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH & WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 91.195.240.13
	ACH & WIRE REMITTANCE.xlsx	Get hash	malicious	Browse	• 91.195.240.13

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B298AFC8.png	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PNG image data, 2000 x 2000, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	744948
Entropy (8bit):	7.97918320978916
Encrypted:	false
SSDEEP:	12288:dw0QEKpz/X0Ud46KsXhbSPhSxIxTqwwptJ22/baZ2J/SBxgX:2UKpzMn6LB5xmTqwwLc2FSBiX
MD5:	E7A283B2CCDE766B77C60644B7F72B2C
SHA1:	4D8A980624A17367D0B2D9CCB3943F384D01B220
SHA-256:	206E88CFFEF3DEE1D444C7D9FBDB8F856006313CADC1039AEDD33A985C163D1A
SHA-512:	5C0B8237532DE1F6BEE720878B43715EFC851A97D652FA0E982A7AE20A19ABD38CA528326DEDB721916A43F695026FEB976712C5D29C47B4D19FD92B7FD8516
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....8.y.. .IDATx....r\.v..1.. Y..@U.`.....}.ghG.C.....!...G...e9|..1.b....I...U...+.@f.c"B...c..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{68A3A7DA-6F93-4194-97B0-E6749671AC21}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{EC050284-DAE8-4269-85E5-42AB58328FB4}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	39472
Entropy (8bit):	4.066178166502722
Encrypted:	false
SSDEEP:	768:+wXnxdZBHbJ5LhVgkABKEuzs3ouLORZkFzj6ShJ7VHzwNgNRIhfYXZBFQg/rV:jcZVB
MD5:	57D7AA4E6175483DDB8834C2364A477F
SHA1:	FE8050F47CBC7C948FA0F1C3F59909B1F29B99B1
SHA-256:	43A8B278C9CDC38CA5DA4158DE11859122EDB17EB77618ED0DB0824FFC5362AF
SHA-512:	9A7D6623A1C694D0EC3A9CB84E8F7731397CF8DB1FF9C7A01961F1412C1E1786AD478202DA978A96682F86FB8516009D78D4D1C9489CA7E7914324D2D8CCE29
Malicious:	false
Reputation:	low
Preview:	..... .!."#.$.%.&.'.(.).*.+.,.-.../.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>.....A.c.c.e.p.t.a.b.l.e. .U.s.e. .P.o.l.i.c.y.....O.v.e.r.v.i.e.w...I.n.f.o.s.e.c..s. .i.n.t.e.n.t.i.o.n.s. .f.o.r. .p.u.b.l.i.s.h.i.n.g. .a.n. .A.c.c.e.p.t.a.b.l.e. .U.s.e. .P.o.l.i.c.y. .a.r.e. .n.o.t. .t.o. .i.m.p.o.s.e. .r.e.s.t.r.i.c.t.i.o.n.s. .t.h.a.t. .a.r.e. .c.o.n.t.r.a.r.y. .t.o. .I.n.t.e.r.g.a.l.a.c.t.i.c. .A.e.r.o.n.a.u.t.i.c.s.. s..... .....d.....^.....d.....^.....d.....,]...^.....&..F.....E.....`..... .....^.....^.....$...K...<...[.].K.^.<.a

C:\Users\user\AppData\Local\Temp\msoC523.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	GIF image data, version 89a, 15 x 15
Category:	dropped
Size (bytes):	663
Entropy (8bit):	5.949125862393289
Encrypted:	false
SSDEEP:	12:PlrojAxh4bxdtT/CS3wkxWHMGBJg8E8gKVYQezuYEecp:trPsTTaWKbBCgVqSF
MD5:	ED3C1C40B68BA4F40DB15529D5443DEC
SHA1:	831AF99BB64A04617E0A42EA898756F9E0E0BCCA
SHA-256:	039FE79B74E6D3D561E32D4AF570E6CA70DB6BB3718395BE2BF278B9E601279A
SHA-512:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA878 41
Malicious:	false
Reputation:	high, very likely benign file
Preview:	GIF89a....w..!..MSOFFICE9.0.....sRGB.....!..MSOFFICE9.0.....msOPMSOFFICE9.0Dn&P3.!..MSOFFICE9.0.....cmPPJCmp0712.....!.....,.....'..;..b...RQ.xx.... .....,+.....yy..;..b.....qp.bb.....uv.ZZ.LL.....xw.jj.NN.A@....zz.mm.^_.....yw.....yx.xw.RR.,*.++..... .....8...>.....4567...=.../0123.....<9:.()*+,-.B.@...."#$%&'..... !..... .....C.?....A;<...HT(..;

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\acceptable_use_policy.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:13 2020, mtime=Wed Aug 26 14:08:13 2020, atime=Sun Nov 22 13:11:34 2020, length=785211, window=hide
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	4.556220219343661
Encrypted:	false
SSDEEP:	48:8JDf/XT3lkMSMh0sMtqQh2JDf/XT3lkMSMh0sMtqQ/:8Zf/XLlkMwqQh2Zf/XLlkMwqQ/
MD5:	DBE20A91BAED56A65A81054098C78FAD
SHA1:	FEB06139DFDC21DEEEB03631DCD332F27BB3DB68
SHA-256:	843CB06F07CA81F35E2CC25BEF65C47A88CA60314237F6AFB8286869DCE95B9C
SHA-512:	AF1A17E57BBD388B4907AE2AD25CA65450B1F4D8AF83FCB56ACB71A2E700F757228F213364F3C521B71B567A8D776B03BDED7DC47DD7E1FD67A6C0F19D8FC F3
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....+..{....+..{...;b....;.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....~.2.;...vQrq .ACCEPT~1.DOC..b.....Q.y.Q.y*...8.....a.c.c.e.p.t.a.b.l.e._.u.s.e._.p.o.l.i.c.y...d.o.c.m.....-...8...[.....?J.....C:\Users\..#.... .....\\928100\Users.user\Desktop\acceptable_use_policy.docm.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.a.c.c.e.p.t.a.b.l.e._.u.s.e._.p.o.l.i.c.y...d.o.c.m.....:..,.LB.)...Ag..... .....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....928100....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	103

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Entropy (8bit):	4.420825796534245
Encrypted:	false
SSDEEP:	3:HPRwcMM9ScGFcMM9SmxWPRwcMM9Sv:HPRsRtRsB
MD5:	F00316F5A9D15C15D275B9DE5D78CBDC
SHA1:	12DE6B187B39A5D2EFFEDFED5BDC82CA58387BA3
SHA-256:	2636F92F51379294E3BE95E5D7622227B77583233D00C1F9CF686332FA537D46
SHA-512:	22308C2BDDED6D8EC028C6A24121AECD15DA76D3EF26E6CA6429D6B30E4D01D7C8E72ECBE24B7331CB0B712E9D9D905772A41347F28C8C04275A5B796F8C943
Malicious:	false
Reputation:	low
Preview:	[misc]..acceptable_use_policy.LNK=0..acceptable_use_policy.LNK=0..[misc]..acceptable_use_policy.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

C:\Users\user\Desktop\~$ceptable_use_policy.docm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyokKOg5Gll3GwSKG/f2+1/ln:vdsCkWtW2IIID9l
MD5:	39EB3053A717C25AF84D576F6B2EBDD2
SHA1:	F6157079187E865C1BAADCC2014EF58440D449CA
SHA-256:	CD95C0EA3CEAEC724B510D6F8F43449B26DF97822F25BDA3316F5EAC3541E54A
SHA-512:	5AA3D344F90844D83477E94E0D0E0F3C96324D8C255C643D1A67FA2BB9EEBDF4F6A7447918F371844FCEDFCD6BBAAA4868FC022FDB666E62EB2D1BAB902891C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....w.....w.....P.w.....w.....z.....w.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.974352084549378
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	acceptable_use_policy.docm
File size:	785211
MD5:	d651d3331b60eeeb49eb0fdc17b7b1df
SHA1:	bb816e1502b0baaa77742fde8c25bbc42c717674

General

SHA256:	a0a9eca457bd72df44a7ff398b5b4469bb4d1057fd43d7906c948b99f7be51ca
SHA512:	48ab987baa051f3c95c205ff3c65f0f77389f92a74791e44195c655c4e84523112ac9e060a31679994c47e6677c7f7bde6d84521684ed3cdee86c1df16270ed6
SSDEEP:	12288:Jnw0QEKpz/X0Ud46KsXhbSPhSxIxTqwwptJ22/baZ2J/SBxgegx:JwUKpzMn6LB5xmTqwwLc2FSBi5x
File Content Preview:	PK.....!.?9.....[Content_Types].xml ...(.....

File Icon

Icon Hash:	e4e6a2a2acbcbcac

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/321436/sample/acceptable_use_policy.docm"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	False
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Title:	
Subject:	
Author:	Glenn
Keywords:	
Template:	Normal
Last Saved By:	Glenn
Revion Number:	10
Total Edit Time:	7
Create Time:	2019-10-23T16:40:00Z
Last Saved Time:	2020-06-04T00:49:00Z
Number of Pages:	7
Number of Words:	1990
Number of Characters:	11349
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Number of Lines:	94
Number of Paragraphs:	26
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	16.0000

Streams with VBA

VBA File Name: ThisDocument.cls, Stream Size: 3038

General	
Stream Path:	VBA/ThisDocument
VBA File Name:	ThisDocument.cls
Stream Size:	3038
Data ASCII:	. . . . b . . . . M . . . . < . . . . . . > I M + # $ M . G . . H . . . . y . . . . $ @ . . + . 6 = ... q 2 . P . H K . . . . / + 8 . . . . x . . . . q 2 . P . . H K . . . . / + 8 . . > I M + # $ M . G . . H . . . . M E . . . .
Data Raw:	01 16 01 00 04 00 01 00 00 16 06 00 00 e4 00 00 00 62 02 00 00 92 06 00 00 a0 06 00 00 d8 09 00 00 00 00 00 00 01 00 00 00 4d 9e bb bb 00 00 ff ff a3 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 3c 00 ff ff 00 00 c3 3e 49 4d 2b 23 24 4d ad 47 8a 0d 48 a3 bf 9c 2e 79 0d df 0e bd 24 40 b7 c5 2b ee 36 3d 86 fd 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Shell(I,
o.Close
o.Write
VB_Name
VB_Creatable
VB_Exposed
r.Status
ActiveDocument.Path
"GET",
o.SaveToFile
CreateObject("Microsoft.XMLHTTP")
String
Object
o.Type
CreateObject("ADODB.Stream")
VB_Customizable
r.send
o.Open
"https://intergalacticaeronautic.space/lsass.exe"
Document_Open()
r.Open
VB_TemplateDerived
"ThisDocument"
False
"\lsass.exe"
Attribute
Private
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
r.responseBody

VBA Code

Streams

Stream Path: PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 366

General	
Stream Path:	PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	366
Entropy:	5.32151305526
Base64 Encoded:	True
Data ASCII:	I D = " { 4 5 8 7 1 3 E 5 - 7 7 D A - 4 E C 6 - 9 0 7 7 - 0 1 1 A C 2 4 A 7 C 1 9 } " . . D o c u m e n t = T h i s D o c u m e n t / & H 0 0 0 0 0 0 0 0 . . N a m e = " P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " B 9 B B 0 6 7 E 0 A 7 E 0 A 7 E 0 A 7 E 0 A " . . D P B = " 7 2 7 0 C D 9 6 8 7 9 7 8 7 9 7 8 7 " . . G C = " 2 B 2 9 9 4 5 1 4 C 5 2 4 C 5 2 B 3 " . . . . [H o s t E x t e n d e r I n f o] . . & H 0 0

General	
Data Raw:	49 44 3d 22 7b 34 35 38 37 31 33 45 35 2d 37 37 44 41 2d 34 45 43 36 2d 39 30 37 37 2d 30 31 31 41 43 32 34 41 37 43 31 39 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 44 6f 63 75 6d 65 6e 74 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4e 61 6d 65 3d 22 50 72 6f 6a 65 63 74 22 0d 0a 48 65 6c 70 43 6f 6e 74 65 78 74 49 44 3d 22 30 22 0d 0a 56 65 72 73 69 6f 6e 43 6f 6d 70 61 74 69

Stream Path: PROJECTwm, File Type: data, Stream Size: 41

General	
Stream Path:	PROJECTwm
File Type:	data
Stream Size:	41
Entropy:	3.07738448508
Base64 Encoded:	False
Data ASCII:	T h i s D o c u m e n t . T . h . i . s . D . o . c . u . m . e . n . t . . . . .
Data Raw:	54 68 69 73 44 6f 63 75 6d 65 6e 74 00 54 00 68 00 69 00 73 00 44 00 6f 00 63 00 75 00 6d 00 65 00 6e 00 74 00 00 00 00 00

Stream Path: VBA/_VBA_PROJECT, File Type: data, Stream Size: 2765

General	
Stream Path:	VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2765
Entropy:	4.23158328116
Base64 Encoded:	False
Data ASCII:	. a . . . . , . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . .
Data Raw:	cc 61 af 00 00 01 00 ff 09 0c 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 01 00 05 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: VBA/__SRP_0, File Type: data, Stream Size: 1752

General	
Stream Path:	VBA/__SRP_0
File Type:	data
Stream Size:	1752
Entropy:	4.25450094175
Base64 Encoded:	False
Data ASCII:	. K * . . . . * \\ C N o r m a l r U . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ b . . . . H . . . . . . N . . . x | . . k . . . . E . . . . y . . . .
Data Raw:	93 4b 2a af 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 00 00 00 00 00 00 01 00 02 00 00 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 01 00 09 00 00 00 2a 5c 43 4e 6f 72 6d 61 6c 72 55 80 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 05 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00

Stream Path: VBA/__SRP_1, File Type: data, Stream Size: 102

General	
Stream Path:	VBA/__SRP_1
File Type:	data
Stream Size:	102
Entropy:	2.15571505385
Base64 Encoded:	False
Data ASCII:	r U . . . . ~ } . . . . 1 . . . . p . . . .
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 01 00 00 7e 7d 00 00 7f 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 09 00 00 00 00 00 03 00 03 00 00 09 f9 02 00 00 00 00 00 00 31 06 00 00 00 00 00 00 08 00 00 00 00 00 01 00 70 00 00 7f 00 00 00 00

Stream Path: VBA/__SRP_2, File Type: data, Stream Size: 796

General	
Stream Path:	VBA/__SRP_2
File Type:	data
Stream Size:	796
Entropy:	3.84331960003
Base64 Encoded:	False
Data ASCII:	r U . . . . . 0 . . . . . a . . . . . l . . . . . A . . . . . A . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 1e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 03 00 30 00 00 00 00 00 00 00 01 00 01 00 14 00 00 00 c1 06 00 00 00 00 00 00 61 0a 00 00 00 00 00 00 e1 07 00 00 00 00 00 00 b9 07 00 00 00 00 00 00 91 05 00 00 00 00 00 00 09 08 00 00 00 00 00 00 a1 08 00 00 00 00 00 00 49 08 00 00 00 00 00 00 99 0a 00 00 00 00

Stream Path: VBA/__SRP_3, File Type: data, Stream Size: 103

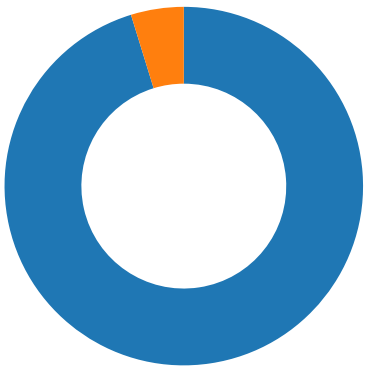
General	
Stream Path:	VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	2.08761800893
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . $ . . . . . ` . . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 40 00 00 00 04 00 24 00 01 01 00 00 00 00 02 00 00 00 04 60 00 00 00 07 1c 00 ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 1e 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: VBA/dir, File Type: shared library, Stream Size: 520

General	
Stream Path:	VBA/dir
File Type:	shared library
Stream Size:	520
Entropy:	6.28781093451
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . . P r o j e c t . Q . (. . @ . . . . . = ... l . . . . . t . ` . . . . J . < . . . . . r s t d . o l e > . . s . t . . d . o . l . e P . . . h . % ^ . . * . \\ G { 0 0 0 2 0 . 4 3 0 - . . . . C . . . . . 0 0 4 6 } # . 2 . 0 # 0 # C : . \\ W i n d o w s . \\ s y s t e m 3 . 2 \\ . e 2 . t l b . # O L E A u t . o m a t i o n . ` . . . . E N o r m a l . . E N . C r . m . a Q . F . . . . . * . \\ C . . . . . m . . .
Data Raw:	01 04 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 07 00 1c 00 50 72 6f 6a 65 63 74 05 51 00 28 00 00 40 02 14 06 02 14 3d ad 02 0a 07 02 6c 01 14 08 06 12 09 02 12 80 d4 74 c4 60 06 00 0c 02 4a 12 3c 02 0a 16 00 01 72 73 74 64 10 6f 6c 65 3e 02 19 73 00 74 00 00 64 00 6f 00 6c 00 65 50 00 0d 00 68 00 25 5e 00 03 2a 00 5c 47 7b 30 30

Network Behavior

Network Port Distribution



Total Packets: 21

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:11:52.236300945 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.257754087 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.257891893 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.274645090 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.295911074 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306190968 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306236029 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306287050 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306319952 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306360006 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.306381941 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.306490898 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.306504011 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.306510925 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.306518078 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.322204113 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.343430042 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.344146967 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.344265938 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.572088957 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:11:52.593408108 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.596224070 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:11:52.596307993 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:12:22.595403910 CET	443	49167	91.195.240.13	192.168.2.22
Nov 22, 2020 06:12:22.595664978 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:13:52.116550922 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:13:52.427846909 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:13:53.036035061 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:13:54.237385035 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:13:56.640223026 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:14:01.445242882 CET	49167	443	192.168.2.22	91.195.240.13
Nov 22, 2020 06:14:11.055818081 CET	49167	443	192.168.2.22	91.195.240.13

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 22, 2020 06:11:52.149545908 CET	52197	53	192.168.2.22	8.8.8.8
Nov 22, 2020 06:11:52.194602966 CET	53	52197	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 22, 2020 06:11:52.149545908 CET	192.168.2.22	8.8.8.8	0xbf29	Standard query (0)	intergalac ticaeronau tic.space	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2020 06:11:52.194602966 CET	8.8.8.8	192.168.2.22	0xbf29	No error (0)	intergalac ticaeronau tic.space		91.195.240.13	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 22, 2020 06:11:52.306360006 CET	91.195.240.13	443	192.168.2.22	49167	CN=intergalacticaeronautic.space CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Jun 29 02:00:00 CEST 2020 Mon Nov 27 13:46:10 CET 2017 Fri Nov 10 01:00:00 CET 2006	Wed Jun 30 14:00:00 CEST 2021 Sat Nov 27 13:46:10 CET 2027 Mon Nov 10 01:00:00 CET 2031	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=Encryption Everywhere DV TLS CA - G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Mon Nov 27 13:46:10 CET 2017	Sat Nov 27 13:46:10 CET 2027		
					CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Fri Nov 10 01:00:00 CET 2006	Mon Nov 10 01:00:00 CET 2031		

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2312 Parent PID: 584

General

Start time:	06:11:34
Start date:	22/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f470000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE91826B4	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FEE8FA683B	unknown

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE90BE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE90BE72B	RegCreateKeyExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly