ID: 512611
Sample Name: China Provinces-Data 31 OCT 2021.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:08:11
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

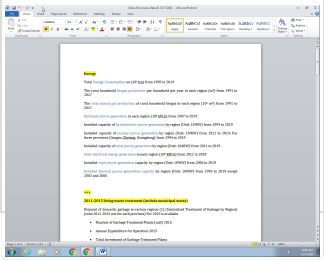
Windows Analysis Report China Provinces-Data 31 OCT…

Overview

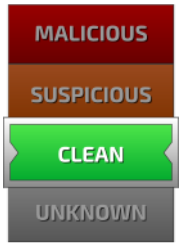
General Information

Sample Name:	China Provinces-Data 31 OCT 2021.docx
Analysis ID:	512611
MD5:	eb301c0e30ef6a2.
SHA1:	f84552cf901c25f…
SHA256:	eea693eb90d88e..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

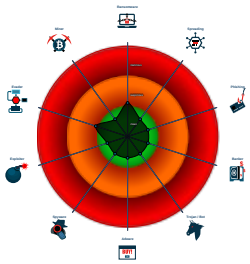


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Document contains no OLE stream …
- Document has an unknown applicati…
- Document misses a certain OLE str…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2096 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

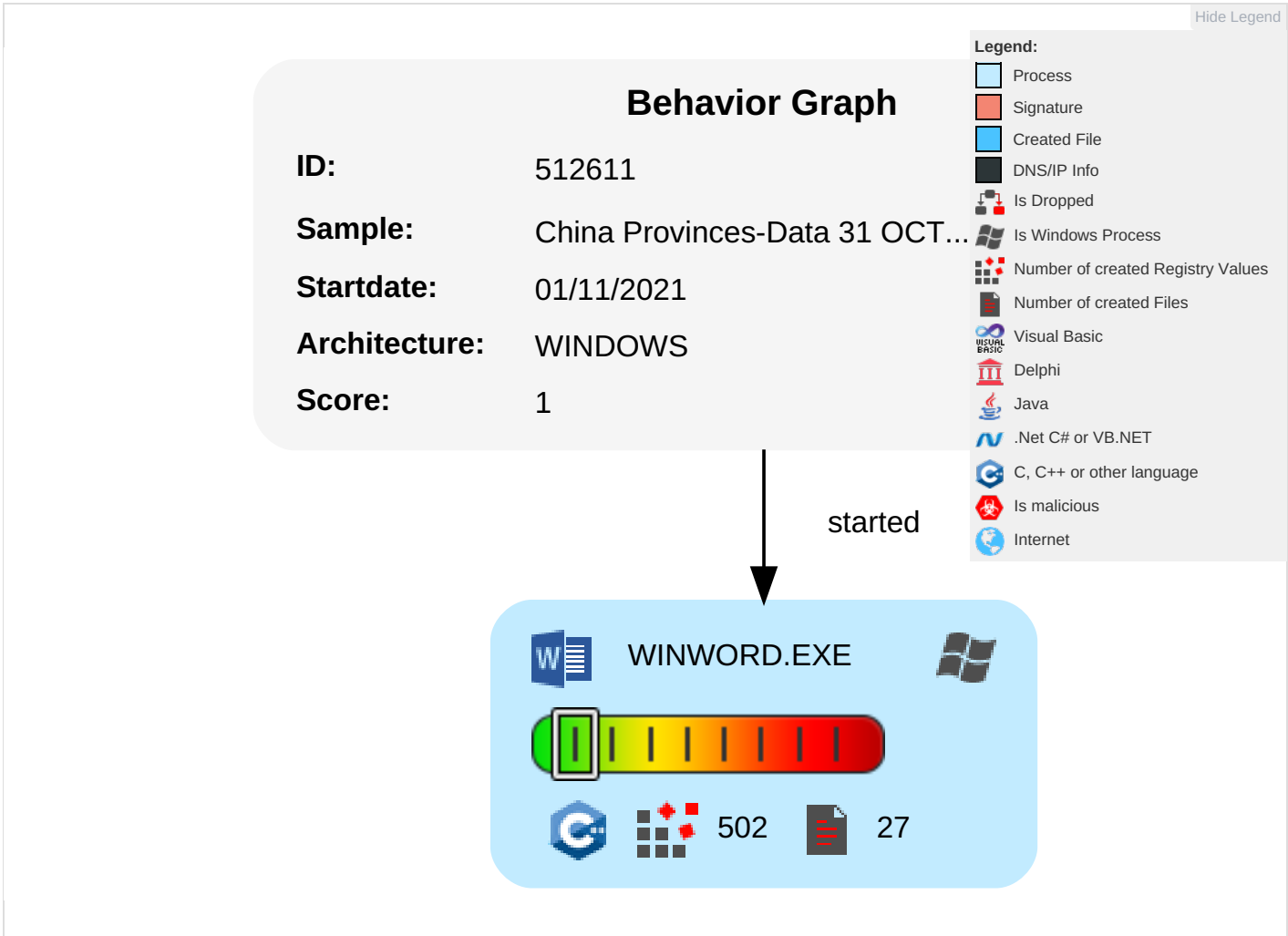
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

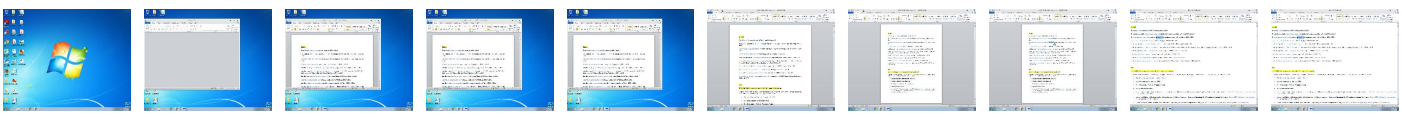
Behavior Graph

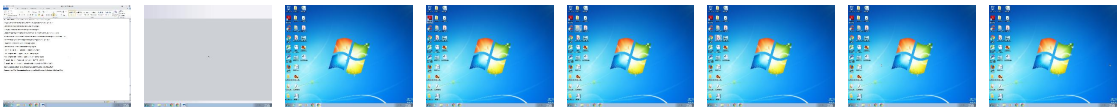


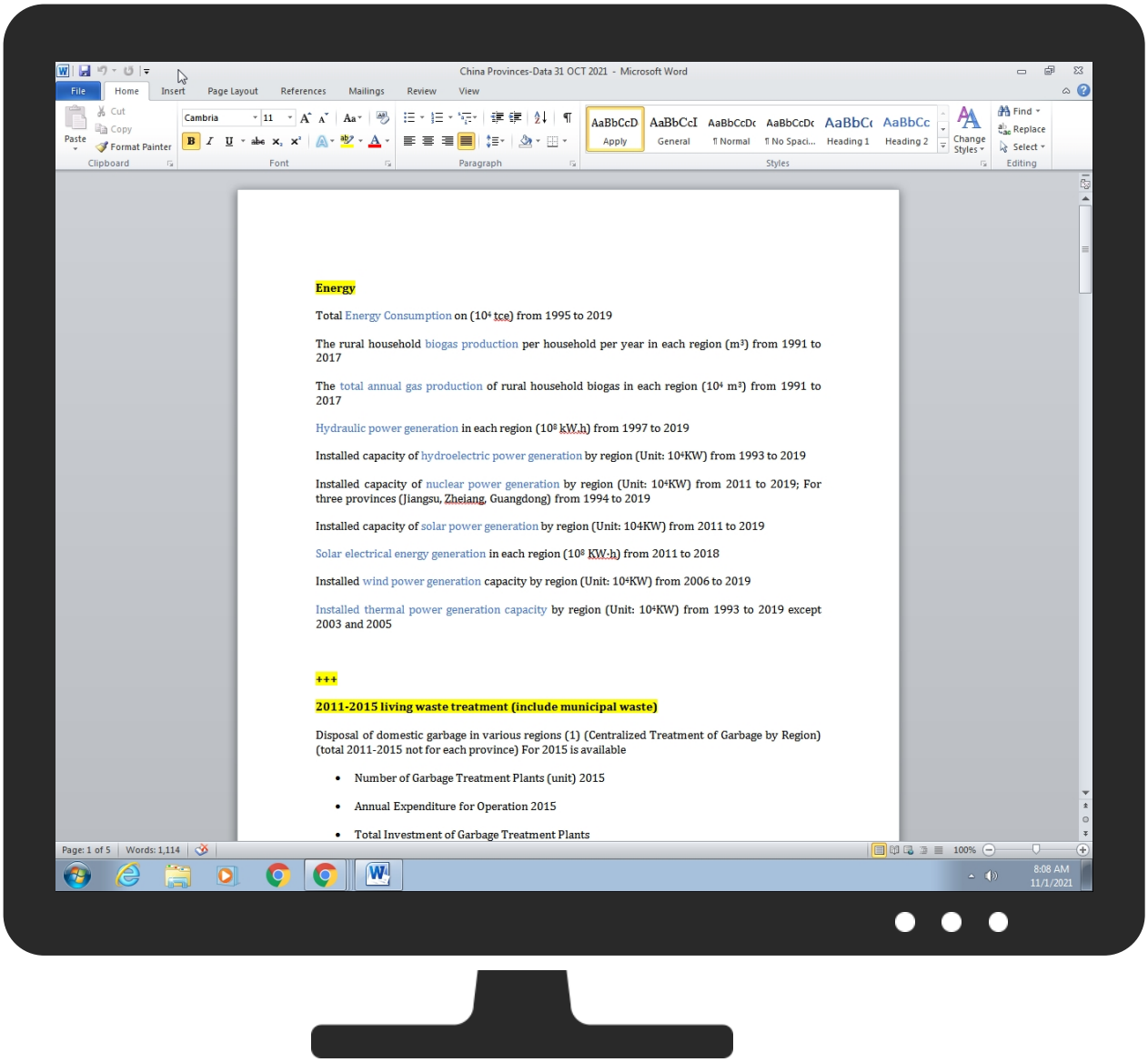
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512611
Start date:	01.11.2021
Start time:	08:08:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	China Provinces-Data 31 OCT 2021.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@1/9@0/0
EGA Information:	Failed
HDC Information:	Failed
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: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{32A009B3-E3BF-4300-BF80-F6867CD7AE39}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	2560
Entropy (8bit):	1.4293855632973755
Encrypted:	false
SSDEEP:	6:rl912N0xVN+CFQXPJpw9X4qyCyp9X4qyCyp9XCw9Xz49Xz49XCw9XCw9XCB9Xh9r:rl3lTpFQBpINWNWCIzgzgCICICb77
MD5:	76CDA6BF10B121C761AB4C5014466415
SHA1:	E99FC79D582DFFF0EC5DA0027CB8CC6086A55411
SHA-256:	794B3C615861E5E0B5799832E4ABB243BD0D3296F5B2635088863E757A61707E
SHA-512:	8DA2130CEE2F0E4B61A77B6AB6EC5F551EBC44BB0A0370957A130C0C8808B861EA97E98AA5BCD48C84DF18448D3ABD0E64C609C6AAB4634A2758AB4557DAC 25
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6BB2BC61-620F-417C-BDF8-A963CA13DE9C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	21504
Entropy (8bit):	4.053957472085887
Encrypted:	false
SSDEEP:	384:6RgA/jWqfZgSYvmxfuiPvbMpx3w0hsZjuj1IgtHxm7:6RxXhsi7Mpx39Wuj1Igvm7
MD5:	42690178DCCA8D66C32E1A990CEE159D
SHA1:	990399086D2F86E9AFE8CE8F5EAE20D9E3E218AC
SHA-256:	2FAEDE99F6BA7473E75832DD477296701E0283C4C0773FFAF2834CB8F73EF26B
SHA-512:	2829FA636BE2F20A7B076FE726F60C16D09F19DA3EC9AB08BAC90F53041501233E669A77EA99A0DF91B9C40C05DF0BD68BA4F1BC62CCA905A61159EF1233220 C
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{6BB2BC61-620F-417C-BDF8-A963CA13DE9C}.tmp	
Preview:	..E.n.e.r.g.y. ...T.o.t.a.l. .E.n.e.r.g.y. .C.o.n.s.u.m.p.t.i.o.n. .o.n. .(.1.0.4. .t.c.e.). .f.r.o.m. .1.9.9.5. .t.o. .2.0.1.9...T.h.e. .r.u.r.a.l. .h.o.u.s.e.h.o.l.d. .b.i.o.g.a.s. .p.r.o.d.u.c.t.i.o.n. .p.e.r. .h.o.u.s.e.h.o.l.d. .p.e.r. .y.e.a.r. .i.n. .e.a.c.h. .r.e.g.i.o.n. .(.m.3.). .f.r.o.m. .1.9.9.1. .t.o. .2.0.1.7...T.h.e. .t.o.t.a.l. .a.n.n.u.a.l. .g.a.s. .p.r.o.d.u.c.t.i.o.n. .o.f. .r.u.r.a.l. . h.o.u.s.e.h.o.l.d. .b.i.o.g.a.s. .i.n. .e.a.c.h. .r.e.g.i.o.n. .(.1.0.4. .m.3.). .f.r.o.m. .1.9.9.1. .....H.....\.....F.....h...j...r.....&.....*...\..... .....&..F ..gd.S.....&..F..gd.^.....&..F..gd.M.....&..F..gd.{.....&..F..gd.k.....gd.N|.....gd..V.....gd..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{88097168-8014-4F50-9F5B-FCD16AD8ED4B}.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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Temp\msoDB90.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\China Provinces-Data 31 OCT 2021.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=Mon Aug 30 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Mon Nov 1 14:08:15 2021, length=19961, window=hide
Category:	dropped
Size (bytes):	1129
Entropy (8bit):	4.57880709050258
Encrypted:	false
SSDEEP:	24:8q5/XTuzLIZFwc7qnrefOQc7qBDv3qRAQd7Qy:86/XTkGFwLFQoOUj
MD5:	549C0BCB61EE0736D9FCBD15FEBED340
SHA1:	5EA21B6214D5180E8AFFE31B003345863148BAE2
SHA-256:	57C214BB69A67206C03123B43BE86E8F39978B25F37F1865D61E85D7215768B9
SHA-512:	745DB0F3869CB675C038F94B3B01C3A297B462AE22D7C4D693E5416470AC99D686EFAABABE917DB56A520BD5DE7ECF748C52386F1FB8EF15639DB46B878457 8 4
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...A;.>...A;.>...B.K2....M.....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.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1. 7.6.9.....2..M..aS.y .CHINAP~1.DOC..x.....S...S..*.....C.h.i.n.a. .P.r.o.v.i.n.c.e.s.-.D.a.t.a. .3.1. .O.C.T. .2.0.2.1...d.o.c.x.....-...8...[.....?J.. ....C:\Users\..#.....\\399601\Users.user\Desktop\China Provinces-Data 31 OCT 2021.docx.<.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C.h.i.n.a. .P.r.o.v.i.n.c.e.s.-.D.a.t.a. .3.1. .O.C.T. .2.0.2.1...d.o.c.x.....:.,.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

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\China Provinces-Data 31 OCT 2021.LNK	

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:	dropped
Size (bytes):	116
Entropy (8bit):	5.005755113035686
Encrypted:	false
SSDEEP:	3:bDuMJl+UsdIMTvFrX9rlmxWtHdIMTvFrX9rlv:bCqsDpD9rzHDpD9r1
MD5:	C0F0ABBD769EC76849E9D6EF4376AED6
SHA1:	D8BCD3464E824B8B6053FB9B0696D828B49074BA
SHA-256:	EFAC0741B2FC7B3909EC6934FD272CD623036C73E4330F30DA9B015C2FEE4D70
SHA-512:	AD3FD78F3D15D5BBA4775F9EC714183D7BE8818F3CA387123D6AC23C5D359924C26C3DCBE928A0932EA655435BADC0F0018E1E0E505F40495FA599DA3097B7 F
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..China Provinces-Data 31 OCT 2021.LNK=0..[misc]..China Provinces-Data 31 OCT 2021.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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA83 2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\Desktop\~$ina Provinces-Data 31 OCT 2021.docx	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false

C:\Users\user\Desktop\~$ina Provinces-Data 31 OCT 2021.docx	
SSDEEP:	3:vrJlaCkWtVyDFH5UKycWT5yAi/lln:vdsCkWtgZ2YAyll
MD5:	6525B5171CE36A6D7EDB3E4DFD5CB579
SHA1:	70AFC3864539BCF8F1C4CD336F6096534A6268FA
SHA-256:	617E1415F4483DAE29072F8E5A042E9EB3446F53F9AC2F26180AECD1D93151CF
SHA-512:	700AEAE11F026EDE01A59B5CC1166D041E1B100E91F84F984D072CDB154251AD15A11C629B8CD7314CB0B2FF8669C3C52EB592020FBA2502CB35BDE6D1EA832
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.556485042738815
TrID:	• Word Microsoft Office Open XML Format document (49504/1) 49.01% • Word Microsoft Office Open XML Format document (43504/1) 43.07% • ZIP compressed archive (8000/1) 7.92%
File name:	China Provinces-Data 31 OCT 2021.docx
File size:	19961
MD5:	eb301c0e30ef6a2a5107882989ba9aba
SHA1:	f84552cf901c25fc7f33796607e6ffa87c8858ac
SHA256:	eea693eb90d88e2a4f809918d2e5f200b267fcb8b6e6941cb6067714e75a167f
SHA512:	453027624b4c3f75b28d13476d282fc038cd42c1d12199ecd00e4e01f822bace76387bc6ab4f8e7f2e1b484bdc6444f0e08828f8964565d44ceb91c510be7a57
SSDEEP:	384:dds5u8TyDNONDWpGqibNxt/ZtNNgN2SlQsliE8Qv9620GaPxlKyChi31X:4g8TykB6biBxllNnSys8E8Qvk7pcyCyV
File Content Preview:	PK.....!.2.oWf.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	e4e6a2a2a4b4b4a4

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2096 Parent PID: 596

General

Start time:	08:08:15
Start date:	01/11/2021
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:	0x13f550000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Disassembly

Code Analysis