ID: 512611
Sample Name: China Provinces-Data 31 OCT 2021.docx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 08:13:03
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

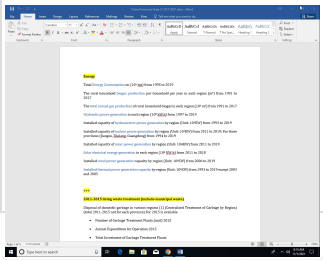
Windows Analysis Report China Provinces-Data 31 OCT…

Overview

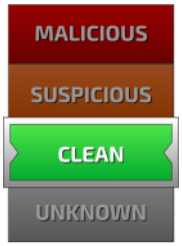
General Information

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

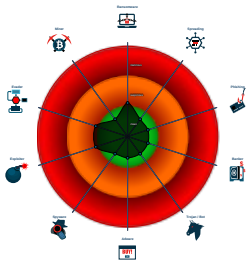


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

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

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 7012 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

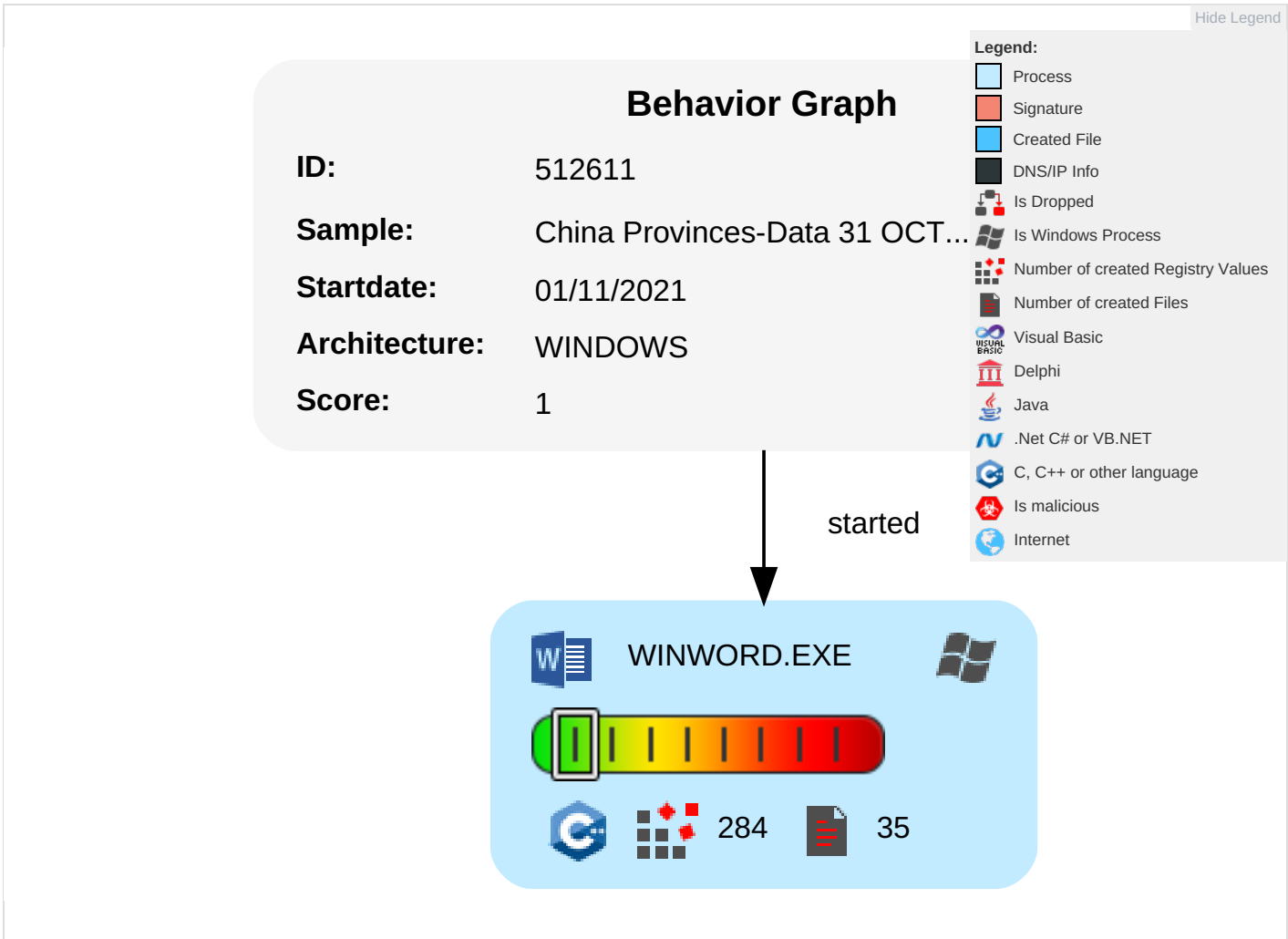
Click to jump to signature section

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	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	Data Obfuscation	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	Extra Window Memory Injection 1	LSASS Memory	System Information Discovery 2	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

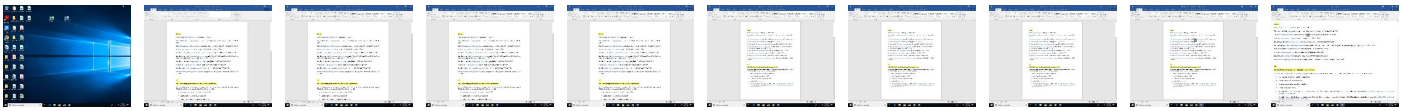
Behavior Graph

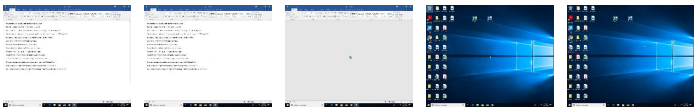


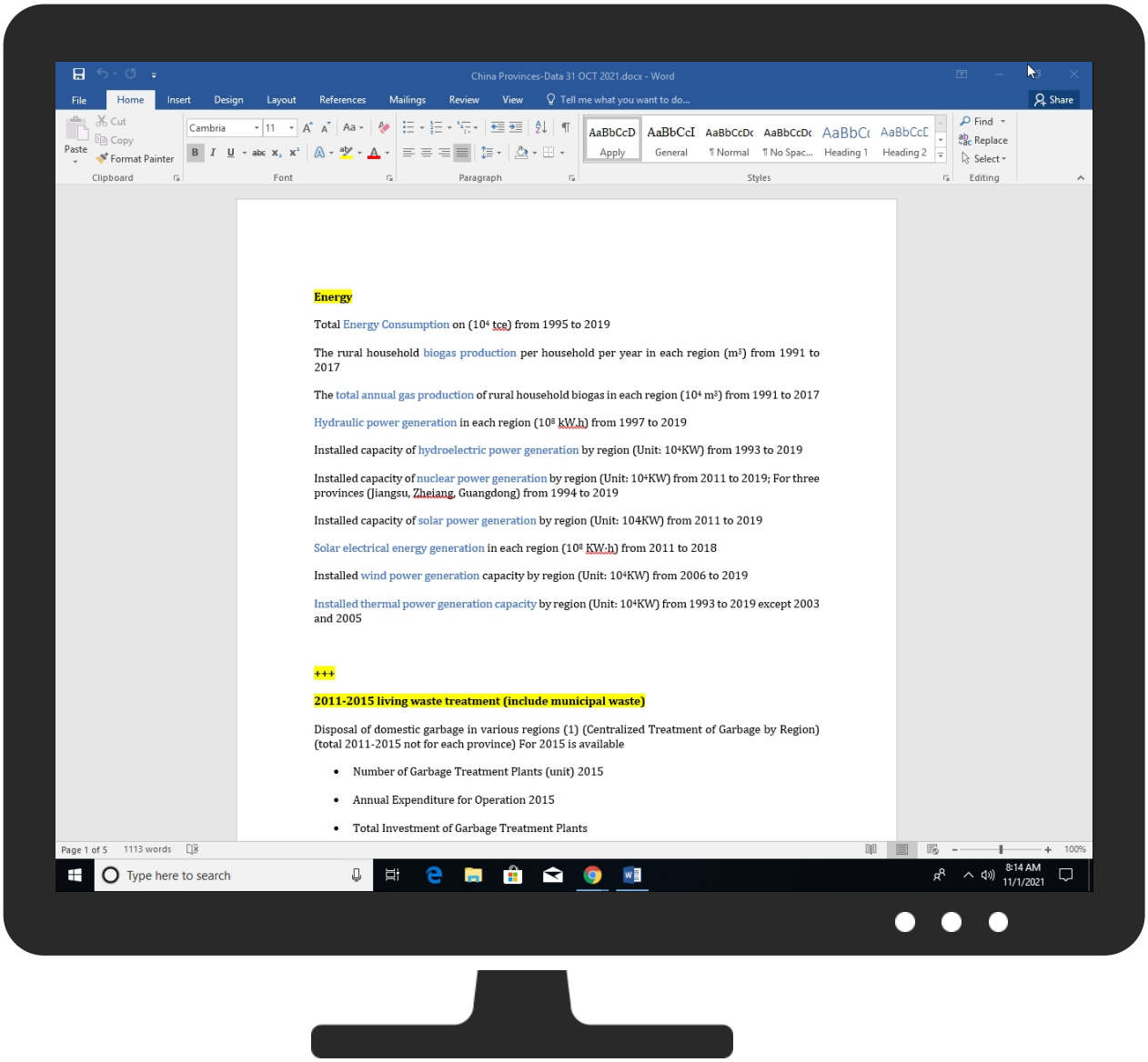
Screenshots

Thumbnails

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







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
China Provinces-Data 31 OCT 2021.docx	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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:	08:13:03
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 9s
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 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior

Number of analysed new started processes analysed:	24
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@1/10@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\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\F9CE0E30-E306-46BA-9278-F91FF6CAA486	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	139984
Entropy (8bit):	5.359101728312129
Encrypted:	false
SSDEEP:	1536:3cQIfgxrBdA3gBwfnQ9DQW+z2Y34Fi7nXboOidXVE6LWmE9:lWQ9DQW+zOXaH
MD5:	C54C915362C5D4AE26915E52B44AA2D0
SHA1:	E3E2391F6DCE7D87743D8266D102C40C6586A1FF
SHA-256:	6F7FAA68DA910ABCFB26D79B58013229AE613281D69F9AD1F49C055FAF00CBBF
SHA-512:	A96D6E78DBADC52E01654EAB99BFC59A99E2E244A438D08EEB0A2369714A6D86042A0615D3A2D9931CD30018AEEA29F95BC1F13ED4E883E6B0D25A793915365 8
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-11-01T07:13:57">.. Build: 16.0.14624.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{A9DAD24F-69A5-4999-9416-4896185140A4}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.3613836054883338
Encrypted:	false
SSDEEP:	3:YmsalTlLPltl2N81HRQjlORGt7RQ//W1XR9//3R9//3R9//:rl912N0xs+CFQXCB9Xh9Xh9X
MD5:	679672A5004E0AF50529F33DB5469699
SHA1:	427A4EC3281C9C4FAEB47A22FFBE7CA3E928AFB0
SHA-256:	205D000AA762F3A96AC3AD4B25D791B5F7FC8EFB9056B78F299F671A02B9FD21
SHA-512:	F8615C5E5CF768A94E06961C7C8BEF99BEB43E004A882A4E384F5DD56E047CA59B963A59971F78DCF4C35D1BB92D3A9BC7055BFA3A0D597635DE1A9CE06A34 6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{35CF56E4-F1E4-47F2-B569-421E607A4A4D}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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
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\INetCache\Content.Word\~WRS{CCACD415-EDEE-4DA8-8103-58CDAC2B50AF}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{CCACD415-EDEE-4DA8-8103-58CDAC2B50AF}.tmp	
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\Temp\mso42C.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	C7B765B9AFBB9810B6674DBC5C5064ED96A2682E78D5DFFAB384D81EDBC77D01E0004F230D4207F2B7D89CEE9008D79D5FBADC5CB486DA4BC43293B7AA87841
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.docx.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Thu Sep 23 14:11:36 2021, mtime=Mon Nov 1 14:13:58 2021, atime=Mon Nov 1 14:13:55 2021, length=19961, window=hide
Category:	dropped
Size (bytes):	1170
Entropy (8bit):	4.682703330203949
Encrypted:	false
SSDEEP:	24:8Bq5EAQJPc7qh8Abyvc7qBDTbXX7aB6m:8TNJPdb2FbXmB6
MD5:	03A999B6BD83A6AAD330C5497569BB92
SHA1:	A20E9C36164685CBF944D38ED83345C8735F42C4
SHA-256:	904FEC77FF8A3A9D2BE99F19C5B8B84B5232C9A5DB1C4BBE13FBC9BCEC1D33DC
SHA-512:	76948A74B942E02F38612B0457BA483F8A90C265806C00466D9A03E1DBF9B9A096AE739CA0D5F515AD6D28BB6C1B7CE9EC4346074B19B05BE8D4FD6534077FB
Malicious:	false
Reputation:	low
Preview:	L.....F.... .....M.....M.3....g..3....M.....P.O. .:i....+00.../C:\.....x.1.....N....Users.d.....L..aS.y.....:....q|..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....7Sty..user.<.....Ny.aS.y.....S.....*..h.a.r.d.z.....~.1.....7Swy..Desktop.h.....Ny.aS.y.....Y.....>.....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..|.....7SsyaS.y....h.....Q.h.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.....k.....-.....j.....>.S.....C:\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.)...As...`.....X.....841618.....!a..%.H.VZAj..."..M.....-..!a..%.H.VZAj..."..M.....-.....1SPS.XF.L8C....&.m.q.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	126
Entropy (8bit):	5.055237473169422
Encrypted:	false
SSDEEP:	3:bDuMJl+UsdIMTvFrX9MSmxWtHdIMTvFrX9MSv:bCqsDpD9MgHDpD9Mc
MD5:	037C700CCF69EA898A68CF9E22C36549

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SHA1:	5BD331F250B1553671BDC9C927BABAEAE0350E70
SHA-256:	4B41EF1DC65A17BEFCFA056A9978D3F0C461A0F2F0B5579921B143338C9E653F
SHA-512:	6A17ADE73A53E1CEFE114F60D1E6A358ECB096B41887C711C0406077B28ECBD42C450BBA74F9FFA6409E965DA45416BEB53FE3EC932CB244D9F99383C028CEC
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..China Provinces-Data 31 OCT 2021.docx.LNK=0..[misc]..China Provinces-Data 31 OCT 2021.docx.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.3848531746263366
Encrypted:	false
SSDEEP:	3:Rl/ZdJrFlqKUJzUL1tty5llX8i5lpl/t:RtZH+mdMzlLl
MD5:	BAD42AF40088F74DC553F879B321856A
SHA1:	D3F09BDEF01B618DE778AC9BCA8BB1EF0759AC0E
SHA-256:	4977C51C42DD2726531D8CCA2275C888038A21E34746574344C3D9252E68E8A3
SHA-512:	5DEB24D26008E585699675181AAE219B98F377D8A8D59640FCB3B8C6160B5A3AC2C83E79E9D3910F89D176B48ABAF2FF04B266074FB9E12D54DDBB3C7B1C300E
Malicious:	false
Reputation:	low
Preview:	.pratesh.....p.r.a.t.e.s.h.....=..G.....$.....6C.....1..G.....m.a.....5..G.....H...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D84
Malicious:	false
Preview:	..

C:\Users\user\Desktop\~$ina Provinces-Data 31 OCT 2021.docx	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.425933557540248
Encrypted:	false
SSDEEP:	3:Rl/ZdJrFlqKUJzUL1ttozlui5lpl/t:RtZH+mdszlLl
MD5:	4B57D31D4EF6CD3F10D5285A369590AB
SHA1:	A43B5A446CD32BD806658D4AC59E0F8FD92DCC7F
SHA-256:	A9BB70EE4865214ACD325EF3B82779504B3E06DCF92E58E8901DD9B27001CC5A
SHA-512:	30365AEB2F3CB9A5CEC8FFDFB9D5CB110E45310645B9B12F16D83A531E9DB82B98B768053ADB85816B2979E279848F7240FF461EFF9EC28BE300AE232B6F8C8
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....=..G.....$.....6C.....1..G.....m.a.....5..G.....H...

Static File Info

General

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:	74fcd0d2d6d6d0cc

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 7012 Parent PID: 744

General

Start time:	08:13:55
Start date:	01/11/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0xf90000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
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