ID: 778234
Sample Name: New Years Quiz.pptx
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 09:07:04
Date: 05/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

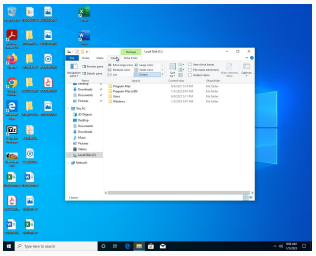
Windows Analysis Report

New Years Quiz.pptx

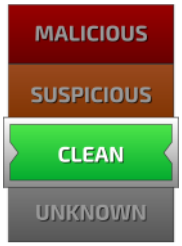
Overview

General Information

Sample Name:	New Years Quiz.pptx
Analysis ID:	778234
MD5:	aaef4b88a07861..
SHA1:	97191fc7bb61c6...
SHA256:	84108e3fdd2d92..



Detection

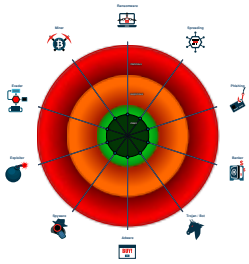


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

No high impact signatures.

Classification



Process Tree

- **System is w10x64_ra**
- POWERPNT.EXE (PID: 1004 cmdline: C:\Program Files\Microsoft Office\Root\Office16\POWERPNT.EXE" "C:\Users\alfredo\Desktop\New Years Quiz.pptx" /ou " MD5: 51D7379A407A1D7A5B0D1C4F61165269)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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

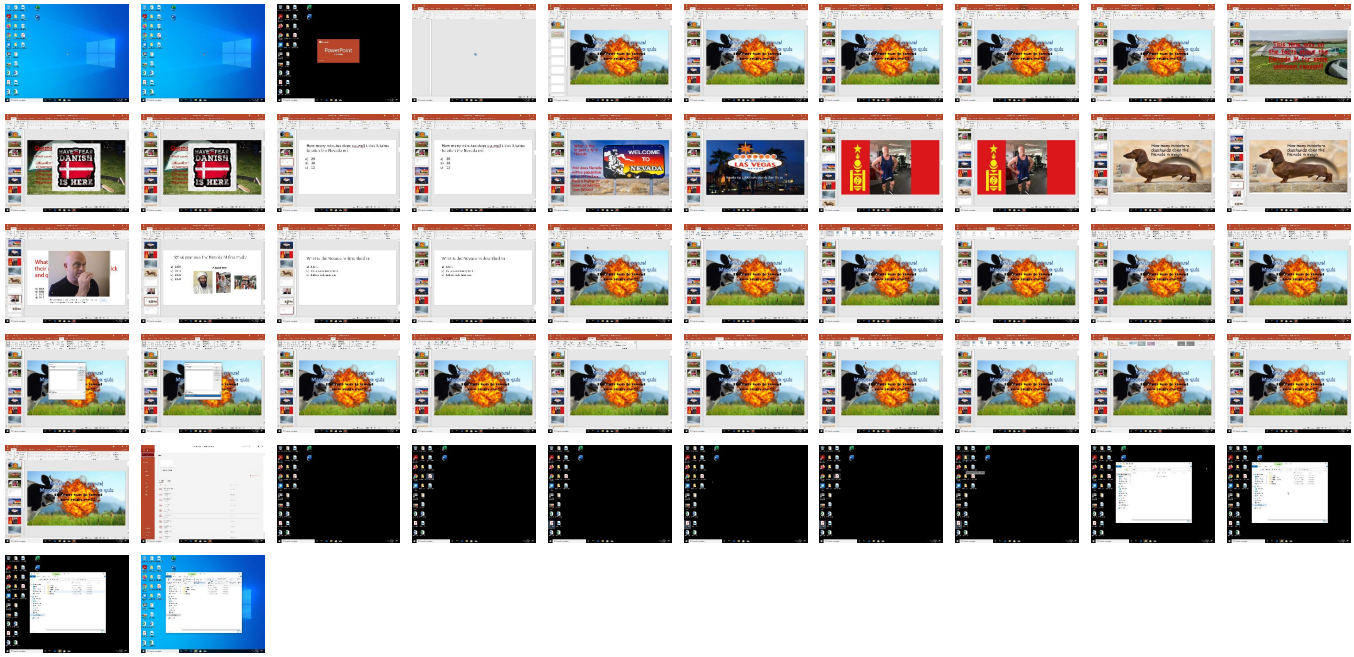
Mitre Att&ck Matrix

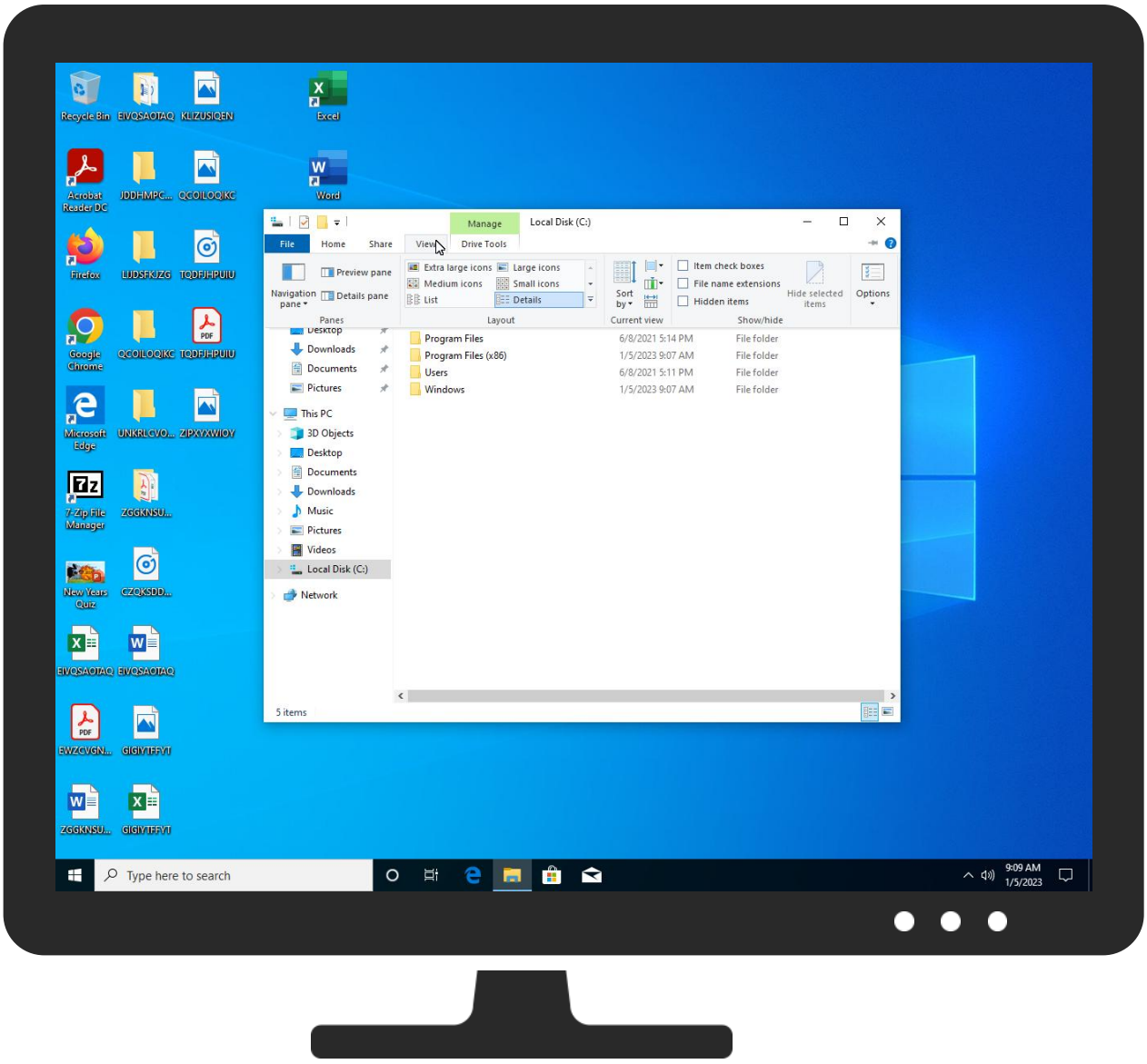
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Extra Window Memory Injection	1 Masquerading	OS Credential Dumping	1 File and Directory Discovery	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	1 Extra Window Memory Injection	LSASS Memory	1 System Information Discovery	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

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
New Years Quiz.pptx	0%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

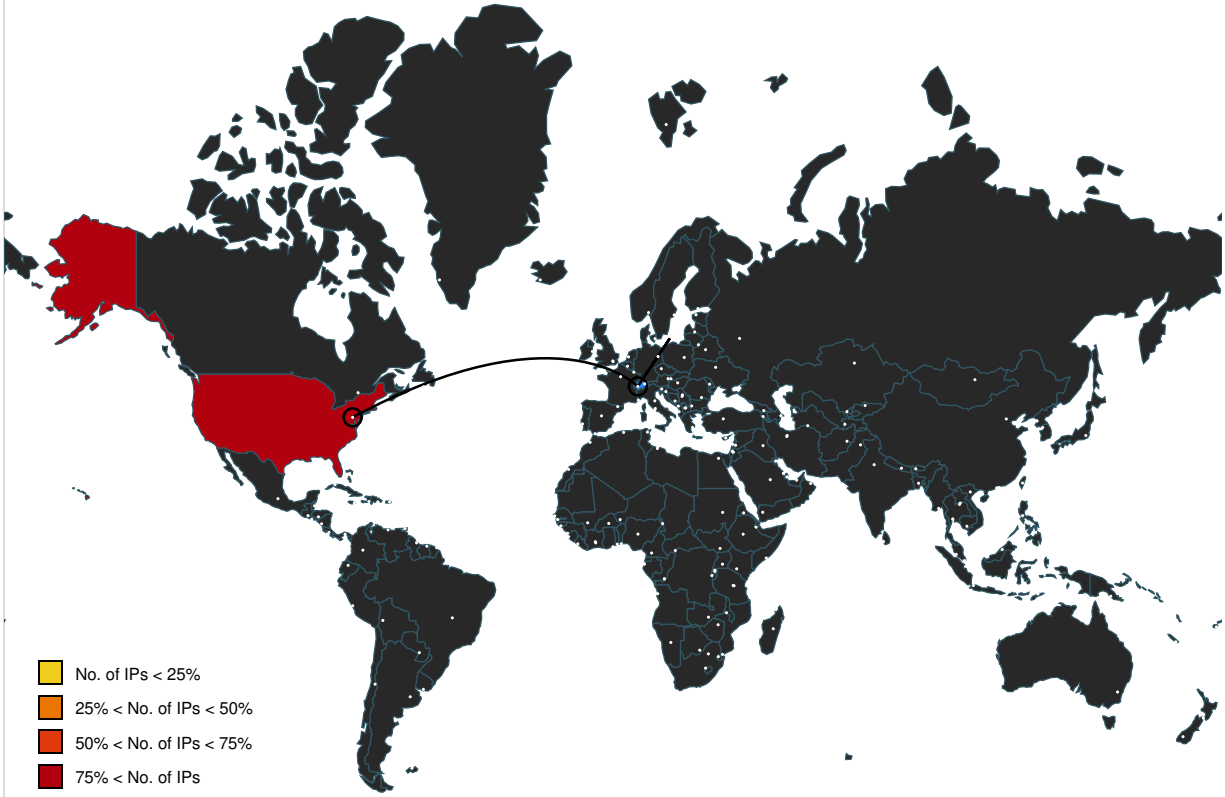
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.113.194.132	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.32.24	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.89.14	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
2.23.192.37	unknown	European Union		1273	CWVodafoneGroupPLCEU	false
2.16.238.28	unknown	European Union		20940	AKAMAI-ASN1EU	false
52.109.13.64	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.168.112.66	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.111.243.5	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
88.221.168.226	unknown	European Union		16625	AKAMAI-ASUS	false
2.17.100.210	unknown	European Union		4230	CLAROSABR	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	778234
Start date and time:	2023-01-05 09:07:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	New Years Quiz.pptx
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	16
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
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean0.winPPTX@1/243@0/57
Cookbook Comments:	• Found application associated with file extension: .pptx

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe
- Created / dropped Files have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.32.24, 52.109.89.14, 52.113.194.132, 52.109.13.64, 88.221.168.226, 52.168.112.66, 2.17.100.210, 2.17.100.200, 2.16.238.28, 2.16.238.14
- Excluded domains from analysis (whitelisted): binaries.templates.cdn.office.net.edgesuite.net, slscr.update.microsoft.com, templatesmetadata.office.net.edgekey.net, eur.roaming1.live.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1847.dscg2.akamai.net, ecs-office.s-0005.s-msedge.net, roaming.officeapps.live.com, login.live.com, e16604.g.akamaiedge.net, officeclient.microsoft.com, prod.fs.microsoft.com.akadns.net, ecs.office.com, self-events-data.trafficmanager.net, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, self.events.data.microsoft.com, onedscolprdeus01.eastus.cloudapp.azure.com, prod.roaming1.live.com.akadns.net, s-0005-office.config.skype.com, e26769.b.akamaiedge.net, prod.nexusrules.live.com.akadns.net, s-0005.s-msedge.net, config.officeapps.live.com, metadata.templates.cdn.office.net, ecs.office.trafficmanager.net, nexusrules.officeapps.live.com, europe.configsvc1.live.com.akadns.net, binaries.templates.cdn.office.net
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtCreateKey calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtSetValueKey calls found.

Created / dropped Files

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CatalogCacheMetaData.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (1284), with no line terminators
Category:	dropped
Size (bytes):	1284
Entropy (8bit):	5.170594889414003
Encrypted:	false
SSDEEP:	
MD5:	D4C8F765A71AA04279C21384706BA348
SHA1:	49BBBB440E8B5F79A150D9A6884C5E620A551AF1
SHA-256:	62BD85B88C58A79FD644AE6A1AFC84E6ED154C7D9E0394348A08EC03DA549D0A
SHA-512:	47EE46131D92620ED05F756EE55C90A5699E76FA79A6C55CF0AE75E7102EE3E252076DDC656F049606EAFDF627881A68C127D4D264E424BD0B349938E7FC56F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><root><version>1</version><Count>8</Count><Resource><Id>Broadway_26215680</Id><LAT>2023-01-05T08:07:38Z</LAT><key>27289878557.ttf</key><folder>Broadway</folder><type>4</type></Resource><Resource><Id>Gill Sans MT_26215680</Id><LAT>2023-01-05T08:08:34Z</LAT><key>31805007993.ttf</key><folder>Gill Sans MT</folder><type>4</type></Resource><Resource><Id>Tw Cen MT_26215168</Id><LAT>2023-01-05T08:08:34Z</LAT><key>29602640380.ttf</key><folder>Tw Cen MT</folder><type>4</type></Resource><Resource><Id>Tw Cen MT_26215680</Id><LAT>2023-01-05T08:08:34Z</LAT><key>35523432091.ttf</key><folder>Tw Cen MT</folder><type>4</type></Resource><Resource><Id>Rockwell_26215680</Id><LAT>2023-01-05T08:08:36Z</LAT><key>34805489950.ttf</key><folder>Rockwell</folder><type>4</type></Resource><Resource><Id>Calisto MT_26215680</Id><LAT>2023-01-05T08:08:41Z</LAT><key>30111742330.ttf</key><folder>Calisto MT</folder><type>4</type></Resource><Resource><Id>Century Schoolb

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JSON data
Category:	dropped
Size (bytes):	379722

Entropy (8bit):	4.9088149211082355
Encrypted:	false
SSDEEP:	
MD5:	E9FB5A0DF105C6F7F80E8B650DF56AAB
SHA1:	0B7F6ADA05673F2535E61267C3CB428489ECEB55
SHA-256:	A24470762A1F9F5F069C0F70EF53D693D08B7C99797935800FF294BD3B2566F3
SHA-512:	65C83135CE550981ED88CB4A83127CB3C94D5C616F26B05185FCC129E5201A88EB0A1351D144E1511B50ADB388071BFCC60388FDD613EBBA5B202FFC76F7D42B
Malicious:	false
Reputation:	low
Preview:	{"MajorVersion":4,"MinorVersion":17,"Expiration":14,"Fonts":[{"a":[4294966911],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32696,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23643452060","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22180,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17656736728","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294966911],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54372,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"31150835240","p":[2,11,8,4,2,2,2,2,2,4],"sub":[],"t":"ttf","u":[3,0,0,0],"v":67502,"w":45875968},{"c":[536870913,0],"dn":"Agency FB","fs":52680,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"29260917085","p":[2,11,5,3,2,2,2,2,

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Broadway\27289878557.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 14 tables, 1st "OS/2", 39 names, Macintosh, Data copyright \251 URW Software & Type GmbH, additional data copyright \251 The Monotype Corpor
Category:	dropped
Size (bytes):	54068
Entropy (8bit):	6.837393037047299
Encrypted:	false
SSDEEP:	
MD5:	FF4B052F2B0A1BD9910889E21C922948
SHA1:	108386FEE49DB0AE3F26439D4952E341A5B70511
SHA-256:	418160D917FFC40D113CB626C5A48175EBD30A4EBC1818BCF6E2D04E2D720DEB
SHA-512:	E40DA82737416B252355E27A974670D0814C8331D0BEF0285CDB4F28D044FFF7A5B00A1D4217A2A242CA317ED4A04A1CAFC3BD064F51C0E3D9AE3903BD63808
Malicious:	false
Reputation:	low
Preview:	.....`OS/2.;.....h...`cmapc.g.....cvt 3.J....X....fpgm...4.....glyf*;.....0....head.T.....6hhea._.N...$...$hmtx.\F.....kern.G.[...@...^loca!gJj...H....maxp.....H... name.2|2.....tpost...d..... prep <.....\J.y._.<.....v.....`.....1.M.....M.>...>.....1.....p...T.....A.....9.....Z.....3.....3...&.d.....URW .@. .....M.. .....`.h... .....3.....Y...Y.,.:.,...&.0...0...Y...f.....(.6.,.b...L.....[...=.,.6.,...,...,...,(.,.%.,.9.,.0.,.C.,.-...[...K...J.,.`...K.m.J...Q.?.....t...7...t.[.t.8.t...7...u.L.t.....t.[.t.....`...7...t...7...t...D.....t.E.....3.....a.0...t...=...t.....0...t...0...0...0.....}.=...t...t.-.....t...t.>.t...t...0...t...0.>.t...8.v.....f.....?...,.....z.,...U...?...?.....7.[.t...`...7...t...0...0...0...0...0...0...0...0...0...0...0...t...N.....t...0...0...0...0...0...f...f...f...f.,.`...6.,...,.K.,.t.U..

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Calisto MT\30111742330.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 16 tables, 1st "OS/2", 49 names, Macintosh, Digitized data copyright (C) 1991-1997 The Monotype Corporation. All rights reserved. Calisto\25
Category:	dropped
Size (bytes):	72184
Entropy (8bit):	6.905579645036388
Encrypted:	false
SSDEEP:	
MD5:	4F7371BA417EACF6DD5B62E47407C82A
SHA1:	EA1759A2EFA734ACD881EAF19D462AFFB2D6C031
SHA-256:	6C68E9444AC0974A055FF7A2EED3E1FBE482075203AA05A9FF47336D538C01A2
SHA-512:	484BE7CEBE505AA2F19258E648E73705836041D3DE888D8EAD1FEA95FE814FC625D32FE0123D0751AC03CBD6E0EC7A4FC7D8F20A6ADA4C86D6F95B13B8BEA342
Malicious:	false
Reputation:	low
Preview:	.....OS/2x..#.....`cmap...D..#.....cvt .U3..1$...<fpgm...1..&....?gasp.....glyf.....;L...^hdmxAt.b.....head.Tn.....6hhea.s.k...D...$hmtx+.A.....kernECK.....locaF^yR..9`....maxp.....h... namem..!...`...gpost.O.f..... prep.....+<.....G*m!1_.<.....!H.....`....F.h.\.....f.*.....h.....b...^.....A....._.....+.....".+.....f.f.....MONO.@. .....R...f.. ....?...?...V.X...I...K.?.;.j.Q...I...+...<.V...?...V.7.?...?.u...L.....0...h.....k...@...q...h...S.?...?...V...V...V.....0.V.a.+...+.2..._...0.V.(...*...Y.j.,...4...8.+.!.?.....V.`....,V.\_...'.j.p.?.*.j.....V.....-.....?.X.....?.t...:...%.....w...I.....D.V.S...J.j.4.....j...?.8...t.....+.....+.j...V.M.?...+.K... ...R.j...j.....+.....>.....?.....V...+...+.....\_.V.(.....V.`.j.....I...I...I...I...I...D...J...J...J.?.8.?.8.?...?...j...V.M.V.M.V.M.V.M.V.M.j...j..

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Century Schoolbook\39048582419.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 18 tables, 1st "LTSH", 47 names, Macintosh, Typeface \251 The Monotype Corporation plc. Data \251 The Monotype Corporation plc / Type Soluti
Category:	dropped
Size (bytes):	148828

Entropy (8bit):	6.965995473329857
Encrypted:	false
SSDEEP:	
MD5:	277FE10CF3A8F3AD7F76B56E7BB2C237
SHA1:	748EA8F59CC1072D5F6AC20123A165BC844A2998
SHA-256:	13938B851436C6CF7A7EBC1D8C1B83B55176997CBC6C7FE9E09F8C0BE23B9C4A
SHA-512:	F1294DCB946CF4FBEACAA9C0D62516032418BED2FF9D90C77F30A2A8429B8D04148A0ED022647EA013057B4AA0EBB13CA3D3B7EEC8267689D5AF394C6BB75(EC
Malicious:	false
Reputation:	low
Preview:	..... LTSHV.....|....OS/2z.p.....`VDMX.&..... ...ncmap.B.7..e....Jcvt .?....v.....fpgm.<.:..k.....gasp.....EL....glyf!s.....Zhdmx.}...&...?.head.....,...6hhea.....d...$hmtx .....tkern.+.-..3P...vloca.G...{....<maxp..... name7=....5....bpost.6.f..E,... prephL|...ph...4.....^.^p.._.<.....8.0....`.....F...N.....<.q.. .....#.;...Z.4.....3.....3....f.....MONO.@. .....q..... ....9...9...^.....o.s...s.....i.....k.....b...E.9.....9...9...s.e.s...s.`.s...s.m.s...s.u.s...s.|.s.v .9...9.....F...E...F...Q.....a.....9.F.....V.j.9.h...`.B.L.s...9.S.V.@..."...T.9.o.V.P.9.t...4.....V.:...6.....#...%.....J....."....s.e.s.....=...m...W.../.L.c...+...1.^.....3...2...e.. .C...E...=.s.k...4...q...3...8.L...9.5.L.0.L.+...b...m...*.....I.....T.9.o...6.s.e.s.e.s.e.s.e.s.e.s.e...=...W...W...W...W...1...1...-....

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Gill Sans MT\31805007993.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 18 tables, 1st "LTSH", 51 names, Macintosh, Digitized data copyright The Monotype Corporation 1991-1995. All rights reserved. Gill Sans\250
Category:	dropped
Size (bytes):	60276
Entropy (8bit):	6.677529334455376
Encrypted:	false
SSDEEP:	
MD5:	819FC8B7DAD24A4923E5A21D10CFD1DA
SHA1:	89DB48291FD6DACA993DEB179D8308EA4C41E3A3
SHA-256:	55ECC8624601C62D9A6EFE78DA98B93AF49BFA0025E23C09DC686C8B449AC00F
SHA-512:	7AF62A9C7D4A6E744F79B314DFC014C6EAB73B987A76AAA9B941D31E7E3C40E253C00951B34F5DDD02E792629EE7D00967F94E79A091884F6F22D904812A148
Malicious:	false
Reputation:	low
Preview:	..... LTSH_2.D.....0OS/2r.....`VDMXo.wD.....cmapBh....2.....cvt -.A...>.....fpgm.....6T...igasp.....d....glyf.....C....Phdmx...1.....$.head.^....,...6hhea.z._...d...$hmtx.. ^.....kern.h.W...T....loca..d...@....Zmaxp..... name.. .....(post.i.f...D... prep..W...;.....\_.<.....x.....`.....T.X.....o.(...V.....T.....,.....,.Q...D...../... .....B.....3.....3.....f.....MONO.@. .....).1.o.. .....u... .....9...9...+.....^.....V.h.h.3...;...Z.....V.#...r...N...R...f.?.....?.....F.....f...\...d...B...J...^...f. ..p...r...p.....n.V.....d.....h.....?.....?...?.....\.....Z.....T...#...}.....V.....+.....?.....5.j.....{.j.7...y...N...Z...T.....j.....}...u.....+.y...}.j.L...u...H.+.....T..... }.....V.....9...../...V.V...V.....d.....?.....\...}.j.7.j.7.j.7.j.7.j.7...N...T...T...T...T.....

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Rockwell\22994219909.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 14 tables, 1st "OS/2", 45 names, Macintosh, Digitized data copyright (C) 1992 - 1996 The Monotype Corporation. All rights reserved. Rockwell
Category:	dropped
Size (bytes):	47604
Entropy (8bit):	6.76349595744851
Encrypted:	false
SSDEEP:	
MD5:	AD1D66027DA137FC2BC98CD71CAA150D
SHA1:	DEF81492202C62DCD0E4F4B8FB4E3343226B44AE
SHA-256:	1004A6D9595010CADE12660E559BDC5EDE0460F74FF8EFEE1181E24023EFAC52
SHA-512:	6E740A9A57519C78A6DC318DEB38023E539A03620E2E8FE13A9E65BAB180B228BF0AFB75346EB3CA62BFA0DB9E8F276E4CA015B4A31C9EDC1C43F6F49ACDC AF0
Malicious:	false
Reputation:	low
Preview:	.....`OS/2u.....h...`cmap%T.\.....Lcvt ..9....0....fpgm.&.o.....glyf.qoK.....Thead.G.....6hhea.o.....$...$hmtx7.A.....kern"q!....$....loca.u.....maxp.....H... na me.\|.l.....post.6.f..... prepL}O$... .....J..__.<.....-5.....`.....r.....O...?.....9...n.....3.....3.....f.....MONO.@. .....5..... ..... .....V.D...N.X.T...?...!...=...`...d...+...3.V...V.1...7.V.D...\...H.....3...N...#...?...R...-...H...?.V.D.V.1.V...V...V.....H.....#.j./.?.N...J.+./.../.?.N.../...-..... ../...1...-...5.V.N.V.1.V.N...!...R.j.-...#.....!.....3.....\...-...5.....y...D...)...F...1...D...9...B...)...?.....)...).j.).../...F.....R.?.+...9.....+.?.....+.?.....5...T.7.....y.?.....#...#.?.N. +./...5.V.N...#...D...D...D...D...D...F...D...D...D...D...?...../...F...F...F...F...F...+...+...+...+...5.3.....F.+.9...F...m

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Rockwell\34805489950.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 18 tables, 1st "LTSH", 45 names, Macintosh, Digitized data copyright (C) 1992 - 1997 The Monotype Corporation. Rockwell\250 is a trademark
Category:	dropped
Size (bytes):	64128
Entropy (8bit):	6.7834746442259215

Encrypted:	false
SSDEEP:	
MD5:	19688646462F503EEE2236317063181C
SHA1:	3CE5FCADDFE60AF34D1F6AE3D8A9E60535655EFF
SHA-256:	FDD9AECCBA119696D748B6D0BF743AB0F7C3D5352C25A09D2411E90E47D8893F
SHA-512:	AC306A4952CAF157976E63F8A1C6CA22698B09520BEADBAF3424ADCEE157B96F380A7FD4537D6688FCBDC41AD3C54D62A07F40A3F590E7FCD9E86AFA64D37A54
Malicious:	false
Reputation:	low
Preview:	..... LTSH.....OS/2I<.....`VDMXO`g.....cmap.,.B..6p....cvt 2oB...B.....fpgm.h-@..9.....gasp.....p....glyf..-m..F....Phdmx..*....`....head..5C...,...6hhea.....d...$hmtx2fC.....kern.b.....loca.....D.....maxp.n..... name.....post.c.f...P... prep0.0...>....E.....XH.v_.<.....Q.....`.....u.M.....,.....u.....A...A.....#.8...%.q.....P.P...,.P.P...H.f.....MT .@. .....8.<.... .....o... .....V...?...V.U.V.?.....j.?.j.Q.....9.+.C.V...V.....?.V.....V.H.V.'.V.R.V.D.V.<.V.I.V.d.V.y.V.D.V.^.V...V...V...V.....>...r.....W.....8.j.%.j.c...7...@.....%.+.....2.....j.f...).j.f.....?.B....j.....?...+.....3.....;...6.....o.?.^.+.6.+.H...Z...J.V.8...H...*.V.B.V.....2.V.)...6...7...N.....J.V.-...T.j.>...5.V...+...j.$.....!....:.7.....-...1.....W...8.....j.f.j...?.^.?.^.?.^.?.^.?.^.?.^.+.H...J...J...J...J.V.B.V...V...V..

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Tw Cen MT\29602640380.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 18 tables, 1st "LTSH", 51 names, Macintosh, Digitized data copyright The Monotype Corporation 1991-1997. All rights reserved. Twentieth Cent
Category:	dropped
Size (bytes):	61112
Entropy (8bit):	6.651555118650965
Encrypted:	false
SSDEEP:	
MD5:	EC30C7137295826590ED7893E7BC416A
SHA1:	DE0109C7F802446DA6FDD1175A80D903D9253B5A
SHA-256:	C2702C214118910040F2D4CE5AFFB1C5EBB3CE06D36350387037282C4BCA579F
SHA-512:	7F0405D8C70C4793E82C1791FCD8A8EBF80213806E3E2A0C3FBB2058B000DE6AED7B13E0131972D6D17351B4BFF1D2BF7D5A77B75197A63442A6BA43B6DB350
Malicious:	false
Reputation:	low
Preview:	..... LTSH.L.....-OS/2s..C.....`VDMXm.t.....cmap+..x..2.....cvt ..&5..=(....fpgm.&.o..5.....gasp. .....glyf.T.z..A ....hdmx.....$\head.....,...6hhea.M.....d...$hmtx.?n4.....kernF.H$... ...JlocaGAl...>....Tmaxp..... name.....l....post.i.x..... prepF.....:....B.....,_.<.....<.....`.....V.....z.....).....)..\...6...../.9.....).....h.....3.....3.....x.....MONO.@. ...9..... .....j..... .....u...u.....u...^.X.Z...P.....h...\...%...+...V.V.....P...X...m.+.;...d.....L...d...d...P...h.....f...h...m...=.V...V...V.....o...u.V.d.....V.....X...V.....+.5.V.....\.V.}.....T...B.V.....;.j.N...1...;...P.....+.....D...5.....X...m.....+.h...q...u...;...s...}...y...s.....j.....y...j.....q.+.y.....=...{...Z...m...B...B...T...9.7...../.?...V.d.V.d.....V.\.....V.....m...m...Y...R...C...m.+.`...u...u...9...B...L.....

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\CloudFonts\Tw Cen MT\35523432091.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 18 tables, 1st "LTSH", 51 names, Macintosh, Digitized data copyright The Monotype Corporation 1991-1997. All rights reserved. Twentieth Cent
Category:	dropped
Size (bytes):	70608
Entropy (8bit):	6.638401506377789
Encrypted:	false
SSDEEP:	
MD5:	9A5D7DCE2D86E010DFF5CF19F17C5F6A
SHA1:	F2E071956980C2529C578053393E0EB30F3A53CF
SHA-256:	E32ABBEB5B314CBAB5CEE0F7A9022AA51E37AABC02CD39F78B0194A7B2A86CCA
SHA-512:	380E9DB9550A19D2CDA1FE48306D95138ED76A14B467A2AADB0C6D0A3AA9AC19F44829828B30994F18AF7A07C0B5C998498923F3E93C6D7E01AF818FF6E4E47D
Malicious:	false
Reputation:	low
Preview:	..... LTSH..{.....-OS/2w.....`VDMXm.uF.....cmap+..x..2.....cvt .{*...>.....fpgm.&.o..5.....gasp. .....glyfa..s..B.....hdmx.Wu,.....$\head.?1...,...6hhea.....d...$hmtx..a.....kern`.b.....loca..:...@,...Tmaxp..... nameZ..7.....post.k.x..... prep.....:.....,_.<.....`.....m.V.....#...?.....m.....).....).a...4.....#.9...b.....1.....3.....3.....x.....MONO.@. .....}..... .....9..... .....5...5.....s...^.X.Z.j.....;.V.R...\.+.m.+.X...V.V.....m...V...5.j.T.j...j.m.j.{.j...j.?.j.b.j.5.j.}.j.f...V.+.H.V...V...V.....1...u.....H.....w...w.+.N.....F.j.....+.).V.{.+.P.....+.N.....L...7...../.j.F.j.9...B.+.....D.+.!...5.....X.j.f.j.....1.j.`...N...;.j.\...N...T...V...j.....V.d...T...F.j...j.`.....3.+.#...V.....V.7...;...?...)...9.7...../.?.....H...w.V.{.+.P.....j.f.j.f.j.f.j.f.j.f.j.f...1...N...N...N...N...j.....

C:\Users\alfredo\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview_4_17.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	TrueType Font data, 10 tables, 1st "OS/2", 7 names, Microsoft, language 0x409, \251 2018 Microsoft Corporation. All Rights Reserved.msofp_4_17RegularVersion 4.17;O365
Category:	dropped
Size (bytes):	672416
Entropy (8bit):	6.566110770587873

Encrypted:	false
SSDEEP:	
MD5:	4DFB7AADD4771ADDF1BA168C12DEDBF3
SHA1:	B379DC0E19FE0F51E77305BE0A7F3421B80E8A0F
SHA-256:	DB9B46CC2132D76EF90CA9A59AF03CB478BB91EA2CDA3E8E42DD0801873416E2
SHA-512:	1C5AE2C794017A81A4232A2EF43725A0DA30F9672123940D85D34A4A77744D2D7ECA5FFE9A91E2FEDDBDBADE4EEAD6AB80E565C1F8FBB813C5A2BC25F7F0A 359
Malicious:	false
Reputation:	low
Preview:	.... OS/29.P...(...`cmap.s.........pglyf..e.......0.head-@;,.......6hheaE.@B.......$hmtx...........ploca..@....h...tmaxp........... name.T+...A\|....post...<..B.... ....Me.._.<...........<.. ....Aa.x.................Q....Aa....Aa.........................~...........................j.......................3.............................MS .@.......(...Q................. ....d.......0...J.......8...>..........+a..# ...,.................K.......z...............N......*...!...-...+....z.......h..%^..3...&j..+...+%..".....................l......$A...,.......g...&...=.......X..&........*......&...(B...............#.......j...............+...P...5. ..@...)..........#...........*...N...7......<...;>.............]...........5......#....s.......$.......$.......^..................H.......%...7.......6.......O...V...........K.......c......!...........$...&...*p..+<..+...-.... q.......O..................F..(....5..0K..$...0V...k..*e...o...........S...*...0..0...*M......9...

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{238C290D-0C97-46DE-BD64-9F14ED6C027A}mi33552983.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33626
Entropy (8bit):	7.965887842736553
Encrypted:	false
SSDEEP:	
MD5:	62AC3DEE6787F06749ABC64859935C49
SHA1:	6420D089E14541F4E53E3AD5E267C06D860C2FD9
SHA-256:	32E2B26C0C073EAB9C0B22A76044B9B331AB0DC7BEBBB38D3C71F87F4AD54DA8
SHA-512:	CBFB57AE929F781D5DE4A57FD496C242F4AE57C708E8AAE6197434A68F3CC93CE88BD3AEE49AF218909E67E62BFC6CD23F6D0A55379DBD32E33FD2F9568D3 4D
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...`..........SZ.....sRGB.........gAMA......a.....pHYs..........(J.....IDATx^....uGU>|...+.....4)......4.Q..)" .#(]E........... H/...I(.;.....q.iy.'^....s..3k..gM..../....^.'...2d..*.B ........NW...X...C......N'..".c>....w..t.?..t.?..3...6.....?..../.....;]...~.e..r..u..0..mNG.....>.......3.<.GO.z......\o.b/...G?6]...e...2].JW.r...\............<..7?..C.........:C..~...?.....qC............~n..m.......L...k...<.C.r...p....r...........N.~......::..'GR........'>cz.S.=..*.{.3......;~..m...s..N<q:...r..N.N<.C.6M'}...._...AV...._.../... .b/......8...<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@.. <000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p@.. <000p@..<000p@..<000p@..<000p@..<000p@..<000p@..<000p

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{43A445D3-7727-4F2E-9472-F92BACF22F60}mi78438558.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	17077
Entropy (8bit):	7.955496041674705
Encrypted:	false
SSDEEP:	
MD5:	89491620526FB557381C97F5159F36ED
SHA1:	1394C15301FC23A6163B4B405F5C2A493C4A4A06
SHA-256:	EE8D00409134C1FAE8AA63489CEDCB49977B80DB8A51F63BAA7C2232BACC4DC3
SHA-512:	4A57CD62A7545C8C083173AAF456B0655E42D2F4F86D7EC4DBDE61FC4C0E932B0929A952F7E9600F05621BDFC263CECDB4F03BE66EBFBE9D86A57DBC7F76D 42B
Malicious:	false
Reputation:	low
Preview:	.PNG........IHDR...`..........SZ.....sRGB.........gAMA......a.....pHYs..........o.d..BJIDATx^..|....y...7o.:...0..!!......Z.. @...z.@h......{.....w.M.$..{.%W....7..F..=i.twz.....g.......).LY ..mBrV..E..0.9.@............e.n...\|Ef.........Vm;%iY..U.4q..&L...o..Q..0..*...W...t.........\|(sB...E..0.9.......s$..`..Mq........a\.....Y....0.......8.X......,.....0.,..`....`.1`....p...3..../X.....a.X.}....,.. c.......`.f...`_.....0.......8.X......,.....0.,..`....`.1`....p...3..../X.....a.X.}....,..c.......`.f...`_.....0.......8.X......,.....0.,..`....`.1`....p...3..../X.....a.X.}....,..c.......`.f...`_.....0.......8.X......,.....0.,..` ....`.1`....p...3..../X.....a.X.}....,.5Ca~vX..`"..../X....88l.iR.w.........`_.....px......[.....O.vN..../X.....M...6S..p.^.....p......t.....k5,..`....`.].l.....(T...4.`.K}6...Lt[`.>...`_...@m.`%8.D..........<.r .0...1.u{3.v....`_...@m.`]TL.qCO.....3.m..-.=.,K....M.=\a....../X.. ..X..S\B...y.a........3?.Y..(.=.<61m.8..N.X.}.....(..H(..../..*

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{46D8A058-AD83-4418-BC1B-14B5F1063F02}mi12214701.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE

File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	141414
Entropy (8bit):	7.97730194336646
Encrypted:	false
SSDEEP:	
MD5:	9314E2C904CB70E9F42929E0BA74415E
SHA1:	7CFDBD0BC37BBD19470289A315041F0309B7C72A
SHA-256:	CEA729DE164BFB8295E37A7DE3290CD3515D32A6AFB6524DBB04DA5DB25EE400
SHA-512:	E5B1F7339DB29858C8ADC7B4F5DD452CE5E5BF7E5845D2914D2D985C6A04DE863607F786E7F6E4957ECF295A6F0A6B18214EB06B30AEF1A4CE8810EF843899 7
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...`.....SZ.....sRGB.....gAMA.....a.....pHYs.....(J.....IDATx^...z$I.....teepp.9wp.9.@..9.4#.TuO..{....<.....1u.....@.37.f..~**...+W....._....-.....Y ..>...&&....V.V.6.6..6v....vd.....U...kg.d.G'g..g.On.....n7X^.yv..X^.....[g.o.>.s.....;..n.9.+..-.}.6v7[.9{p'.Y..?.s....{...{.....e.?t....<..e.9..Z..:.&.}.k.....^v...g....s...W.... ....z..g...g..gK..gs.Kg..sg...Y..<+.kgc#.....`.lp0.600...7|6.?t..?.o./#.....e...X.6Y....Y^.t.....].z...gO...x.....g._:{.....>~.p.....?.}.....n.?.>../..r...W7.{-..;...[:...m..c~.Z~ .}8.....w..>..w...K.~u.....]8{..>{.]={s2~.|.r.t.x.r.~.b.v..t.....^.O.=^....p.....Kg...>.={s<s.N.^_.?{#{.{...<.>{..>{.?q.|.y.l.q.t.~.h.|.`.tv{.pvK.p.zv]....;S.[.....Qe.l.4r...:[..<...8[..8.- ..]k....#g.....x..j;.vm.rvm.|vk.~.`{.....g7w..z.....g.n..=.n..=.}M.....g/.>9{.....X.....}.wo..{.N.....?x.x....:i!Li...G.."Mh....O.6

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{8495E18B-412D-4B1B-8704-42D9816247F3}mi56535239.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	45741
Entropy (8bit):	7.906583578601499
Encrypted:	false
SSDEEP:	
MD5:	62E3A125CC1380C07A17CADB62885A5F
SHA1:	1B14FA60F0324F9EFA0FB8596E3870D3AA7392DB
SHA-256:	28D60D922C2FE6D983631EEE48458CE314C05D3BF27D59D40969557E6A520916
SHA-512:	43DBFFCBF92B1DAF68E5050A896999E9BEA9662A95C957ED81AFF2CFAF4FBDA657C54A427C3392F47EFF209F52B03109D71E67DF95CCDB62E35F009B087239 D
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...`.....SZ.....sRGB.....gAMA.....a.....pHYs.....(J....BIDATx^....&.U.q.pw....{p..,.H.....wwwX...B.....t.LO[.Z{.SG....].=.>.....k..~....X..u.]|.. z<b.h9.6?.....c.[.....;Z{...|....=.....?.... |"z..{....\.o.q....;.N.q.t.[.vmn....u..o4....;.Lm.|..z....:~..Ve..F<Zs.u.=.z.}..-..y..>..Q >...xGs.Z..h....7....X..5....!.=R.,..=r..>P...x.P.E..7..*R.0.b. .]....;...F.lm...Lx...o.Qt.cd.....OZ./.56.o4...i....X....`9ot.e..t#.\6.+...k..r~..C@m.?i.,.....*.....W!NnF...1...}..9.....-.f[.,h.'.B...mt.h....s.u..].7:..p..F..w...K.. FY.?...g]$.,v9..4...6.k6. .4.o.....[D...j..[...t.t].....nL.lm|I.....8..mt..8.;O....4..n...#.....\_.M.....V._1.Lk.Mgu.y...~..'-.....x...\_....=.6..o.....y.s|..#..6..@p.|... f.l..F..$..8.s.Bc..*.pZ...4y..:;...k..mt...s.u..4.- .6:.....Ew....l..6..4.2...A.IG.m...z....}..].'...F.mt{.F.V>...7.;MP\>..m....#..[...t.t=....Fsn.u.|k.K.....Mw..).6~.h..F'.e...?.6:....yml...:.S`m.".E.}..'~?.

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{A046CC4D-7B23-4B53-8616-1CDEBE4EFE24}mi56160789.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	71880
Entropy (8bit):	7.977631623268977
Encrypted:	false
SSDEEP:	
MD5:	14F2A95B1D0C1A2F1643280AF8B27B7B
SHA1:	11AF2540E50851B6BE93E00DA0895BF9C945045D
SHA-256:	C107DD95B3286A4BC540D5860AB9AB3BC3E1C6232D7F92C3129B2FA16AD57B7D
SHA-512:	7192C880B24D29F163F54ED35ECCD6F2EFAC7B1CE5260FE7582E2A843FB48CA8C3D869DE0DB2F075D968D55C7C7CFCA1B2B5FAC724588E08160C2375D6BE6 2F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...`.....SZ.....sRGB.....gAMA.....a.....pHYs.....(J.....IDATx^.....y.....M.6i.a;q...33K.$.,fZ.....+f.ll.....9Z'f.....u.P.....o....<.9...7.Y.....6.....f,Xwl..c7.^vl .c..f...&..U...,O>6ki..V..[.....w.....zIU...y..N...Z.....9.f,.?6{E.....f._sl..cl|..l..V...[.V.....ck3.-.Pxl}F.....sk.%...[.Tp,!..X|v.^W.cd.[.R....5.K)l.....e...K.=.S.q,)..XbN....cy....e.4. .]~,...XNi..7...c.%..R.....:F..yU.....Vv.K.k.r+[.....K-..~..R.%f...[},).R.Z....5.y....XZq.o..-[..}n..|...ck....\.U.&....s...Syle.s.L..k.:.....c...%.....4...:..K...\...e|.l.....mU.....].=v..%..>.. s.^|.....b..m_y.m+...Tm.D..t...\....E.M`4..u.gs.'.`iK..lq\.ns}..m....f.u....[.\d..lej.....u[bq9...mEb..L*.Vd.....2./6..6..Y|V.....[...eT..J.~]F..N).kJm.BK....6...uY.;...2.,..S..[.e...._. .;.|.%..x..._.a...z...Z}.|.].8..q....,ek6...3.-1...k-)..6...._..'.~Ny....ZFI..._g..o9.]~.>.....:^..M+.[z...{...eV.:)[..Z.^n.R.I]V...uK.

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{A9368E30-AB01-4AE6-85D7-0976C7B52F44}mi56410444.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 352 x 198, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	43242
Entropy (8bit):	7.983454839708982
Encrypted:	false
SSDEEP:	
MD5:	C1F7D8EC22091D84E2806C62D1D560F5
SHA1:	0149186A7C9B4EABF36361AC0EC36F082081ABF1
SHA-256:	337897A933AFA31C14343E6CBF74781001C5DE77C85C46BD0591D67F114D0B32
SHA-512:	7A2729B208797216CEA563D91A6CA33C6AEE309BDB01028FB13E7A1C2EFAD66EB0B8387AA0D42545AC6FD9CD92EC68520B37C4C323C5E90001C32EC8210CADD
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...`.....SZ.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..et].-....}..k.....k..a03...;.c;ffK.....,Y..`...S.q...jJ..(YI,{.....sL.....U..ou=....._..T\q..W..x.@.....o..u..a4..*...+.....i...b...w._..W\q..7.....+..y..y..~x...f..8.v]O7.K..._.s...h.=E.i..O...m...xp.....;Fq....V.9v..6...q.....t.7.....W.....M.....f!...^..N....=.....>.n.,.O...GA_q....V..t.E.....".2...%8Q....pd.....w'.MCL...Z.P...H..d.....H;.K.K..?...H.....5=...Y.i.b.'F..a....V.....uu.....f....}.500Z.S....5...~.F; 6.....ENI.r.s..w..y.....^...e.4....]v..N.iL.t.u x..'S.....W4.) .....?..!.^....DRV...6.t.C...02].}....]....pq?.....#v....)..QTS....x..@Jn.1.&:v?.m.!>=..g...Ez~".<..(;.e`.....P.%.N10.....W|"W.X.....8..24..V....O.1<|u`...~.9.>.. .....Qv..1.....j...{.^~.PR_.....:l....j;[P.P..H;xx....#.<.mg..^gi.....4....GC?9.W.'...+.....2....N....u.....9....5A|.7.-..n.g....0.Co..]S...b=bS<q.,

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{D0AA75E6-088B-4A97-AEA4-DEE27432CA3A}mt16411177.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 200 x 113, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	11224
Entropy (8bit):	7.9614300831372695
Encrypted:	false
SSDEEP:	
MD5:	B4A0AE40C2B3D3285360CFC77B11838F
SHA1:	EBE8BCB8C84FE9E2E04F9A73653242B512853DCE
SHA-256:	389A976126320BD3B24525C2388F3EE00FD489B1B1491F9B759FE1D706EF3EF0
SHA-512:	EB390A12EEDF971A9C80F7840516DC46F8F10445E524FEE952A47F73E1BFB52BB451BCF8032759D80A660EAB56F82432FB0131BA372BE14EBC643A156365F02A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....q.....#....sRGB.....gAMA.....a.....pHYs.....o.d..+mIDATx^.g.]..}..f.....`@....."R+..!.L..(.I...cl..p.9.=.c....\..6...RK.!..f.....V.>..>}$A. A.x...W_U}o.W .....k..SPPP.x.u.....&.....0"^0...."JAAA...E!HA..(.)(.B....(.)(.B....(.)(.B....(.)(.B....(.)(.B....(.)(.B....(.)(.B.....0..=..a...S.j...N.;...O...."....P.P.{.@?.Au..6iv.../.....d.....3..3..k....i.=.....:Wy.g.+tw..H(.e....=s.z..#.!...)...i..a.....i...9fY._{.[+b..?4t.~.K.s.(.;A...O.....S..%<../.-....+.S.9..a.w..s&Gc .f..*9.P.....HF.....IX7.6.5.}c...GI.kO\|...n@...2..~.?.....F..\|...f.+.i.....:.g..V.y.t.e.C.Q.Z...;$.....'Y.h...z...V..?.S..../..I..jGP+.....a..&. ....[?.@x.....8F.....3. ..!..._..6....I.(....5!.g.T..c.....C.2.]qZ...G|..i.Y.[...8..YO.1T..zO=\.....~.?.g >.....i..?.....?z<.9.m..-.gR.]x...F..."..O=]....t.$.}_...A...k&.5lX.8<..u/.dY..cY.....|...].0z.'.....i..U9.....f....h....Ya.g.3A0.g..i..

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\DTS\en-US{98DE69B2-6F80-47C2-AC66-AA353EC06934}\{F094975A-ACAD-4B10-8B84-3BB8626B1ED2}mt10001108.png

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	PNG image data, 200 x 113, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	4792
Entropy (8bit):	7.919519824286398
Encrypted:	false
SSDEEP:	
MD5:	0487A314ED07DBC89E92E8F17F7DFED1
SHA1:	F01A61125FF490AE2107CEB7D275C0EEFA87F5FC
SHA-256:	1E37A0FB4AFAED6EED7ECA76992EF1DD67749DA8B3CD9CBA7603E6EBA24DCA03
SHA-512:	394278BFA2C4DE420FA00DC62518D5D60F962274C9207251B8E2D827C6B4A699A46162823F1BE341626E045CF02BD5F2427C57CE5074C38D357F9650A0C90243
Malicious:	false
Reputation:	low

Preview:	.PNG.....IHDR.....q.....#....sRGB.....gAMA.....a.....pHYs.....(J....MIDATx^.i.U....ku...CKTp.(.D..d...g.E.e...E....'&E!.8...v.&...e.v.R.5.EQ@1.h.....o.w.WEqR.+T.. .....v.hU.?.....E....!.%.P+.q.p.*...q.:.@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q..@.'...q.|..iQ.1.....J..^,Yi?..v .....sQ.r../....b.....u0V.WF....tL....vqR{.....T2{i..;.|.4X .w..>.?..qC....S.{`V..K.h.P..vE.....L..[...4....n]p..S.J.[e...K..#...m.v|O.X..'...I.Y..9.....j).s|.....}t....|s.,.<V.]..../....?1..?..|..c=. ..os..y..y.u.5.....4.t./...m..<...F.<:.{K.(^.. j.c.....MD+..wd.....Z....|.}..r.n..z'.J".K....:...5R2o....3..5Q_.(..}.fu.0.1...~.].....^M..{...m....'WJ....x.uR....h.D..=m.:.n."...O...?....;"...>.. ...i...b..%..y.5.D$<..*+..i.$..?..&..g...W....(..gK.q..r.^..^.I....L..dF[.ud.9.....J.[....1..... :[].3.KF.s.t.R~....tY....n.+.X.3.%...*...|..m)[z.y.n.J..!Q[..=!.dt=G.....k.a.yw

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4636D7E0-DF9D-422B-96D7-0AA1309D86F8

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	152820
Entropy (8bit):	5.3552592415743705
Encrypted:	false
SSDEEP:	
MD5:	4151EBE6150A50F304D0C89CD403F6B8
SHA1:	1F83FEC2A15FDFF3DF08F659C691AA8946EB1D5C
SHA-256:	E861F51D904BB288A73D8DD919DE62EC7404C4B73417CBB54E3CA300FBC042D5
SHA-512:	A63C2EEFB546DE76F2DF30AC7CF94900C8DC9C4DF7A762A1179BE5E637CFDDEA5911D1CEDECA7B896297BC29D8DAF47183A954BC892828B63B2D950A5FFF E66
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="2023-01-05T08:07:35">.. Build: 16.0.16012.30527-->.. <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:au thentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:h eaderValue="Passport1.4 from-PP='{}&p=" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAu thorityU

C:\Users\alfredo\AppData\Local\Microsoft\Office\16.0\powerpnt.exe_Rules.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	232945
Entropy (8bit):	5.12845402951343
Encrypted:	false
SSDEEP:	
MD5:	A59DF65BA101FF3F9EE92D36D1777318
SHA1:	A55D663EDC0E4A75762576BDB2B81D14B40CE911
SHA-256:	ABF046F7126CED276F961EFBE48D19E4303C244FC1A280CDF9F10C7D56636999
SHA-512:	337C9EA5E6BD5A00202544885DBC19C9198DE96D3F88129CD2060D74EADD0E02A5356D60BD66ADB2DF8D054847FB1F32CCEBC02D103142BAB333E7447FE7D 56
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d 448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159 " G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L> <R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N=" ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

C:\Users\alfredo\AppData\Local\Microsoft\Office\OTele\powerpnt.exe.db-journal

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	SQLite Rollback Journal
Category:	dropped
Size (bytes):	4616
Entropy (8bit):	0.13760166725504608
Encrypted:	false
SSDEEP:	
MD5:	455C6B37CF40D5437E23E404E92ECC6E
SHA1:	01A5FF99F424D4BE604358F0A2565120F53E7591
SHA-256:	049C2701C0F8983325113E36C947B3D2CEBBF9B674A28048BDBB9BE0E1054C59

SHA-512:	FA610167E23DE41313D837CBF8BC0E880D65B340E45ABD7C0940F467E0C87F720049ECD39878C456B80EEDE9188784B653587CFDBE007636E2D1EE29635B5D6D
Malicious:	false
Reputation:	low
Preview:	.... .c.....}q.....SQLite format 3.....@ .....

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.842548705375362
Encrypted:	false
SSDEEP:	
MD5:	4A69C0F7097BCFC99AE99614ADC2392D
SHA1:	6823038586E3A0784ABA604432B11217CF066272
SHA-256:	49C28A700C260184E85AA3862C62B2DEA0609DB23C2E64EF13062D65F11EDC41
SHA-512:	9D2B8FFFB51AB510C5F1DB6B86C2D9D983D415BA54C6638A50B7C6AB1E3812465E2864CEF3861DF12BDBB63D6EF966A4A026286F4EA8BEA7B516E277B6BE544F
Malicious:	false
Reputation:	low
Preview:	{".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{".H.e.a.d.e.r.".:.{".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{".R.e.q.u.e.s.t.I.n.d.e.x.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".C.J.1.m.u.g.S.o.z.s.S.9.x.S.Z./.Q.v.O.c.+.E.J.4.u.2.c.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.O.I.O.K.O.U.g.2.Q.E.=.".},.,".S.t.a.t.u.s.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.5.S.c.x.0.U.

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	2684
Entropy (8bit):	3.9005353256550435
Encrypted:	false
SSDEEP:	
MD5:	A1BC73130737D82E54866B5427EC474B
SHA1:	EB494E65A2E05E36DBB112FB77F4564F0237CB32
SHA-256:	D82E49F54C0079CF3965ED96BFC13BE4B91E9225148CEE67B22541AAD19359A8
SHA-512:	5BBBEDB9C376582C088EC5665E08C8153CC27CB97AD314828D9ECCED3E88359511C0C9B21183DC869F1DF9442BCFCDCBB92B7FDE0E17D42E8641400DB2823A0
Malicious:	false
Reputation:	low
Preview:	{".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{".H.e.a.d.e.r.".:.{".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{".R.e.q.u.e.s.t.I.n.d.e.x.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".V.H.X.L.G.R.5.H.j.D.k.3.C.i.F.b.L.a.m.K.N.+.n.c.g.T.0.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".Q.u.4.l.Q.a.4./.2.g.E.=.".},.,".S.t.a.t.u.s.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.5.S.c.x.0.U.

C:\Users\alfredo\AppData\Local\Microsoft\TokenBroker\Cache\9aad439831564ef9f88438a70a63c87e26ef3852.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	3902
Entropy (8bit):	3.9894358014824247
Encrypted:	false
SSDEEP:	
MD5:	1BC223474CE43E344DB28355CDE1B024
SHA1:	049E6F5D87AB8A1AD2600C35F3CB115E291184D4
SHA-256:	95B0854C03F0D54823500421975F75F5F88266917C5ACBB06AD69D0FACE296E9

SHA-512:	794CD4FC6C5FAB98A446FCB0A0B38F25DD45AB6DED0D16A4E7C45ABB12B639E69B1853CBB859F2C0BCFC5671F0256DEEF2EF8C4BA744E0E20DACC4D61FE4EEFE
Malicious:	false
Reputation:	low
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:{.".H.e.a.d.e.r.".:{.".O.b.j.e.c.t.T.y.p.e.".:".T.o.k.e.n.R.e.s.p.o.n.s.e.".,".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:2.,".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:1.},.,".O.b.j.e.c.t.D.a.t.a.".:{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:{.".R.e.q.u.e.s.t.I.n.d.e.x.".:{.".T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".m.q.1.D.m.D.F.W.T.v.n.4.h.D.i.n.C.m.P.I.f.i.b.v.O.F.I.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:{.".T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".r.S.F.8.D.d.0.g.2.Q.E.=.".},.,".S.t.a.t.u.s.".:{.".T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".A.w.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:{.".T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:t.r.u.e.,".V.a.l.u.e.":.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.5.S.c.x.0.U.

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2A1F0D83.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	216909
Entropy (8bit):	7.904234639639555
Encrypted:	false
SSDEEP:	
MD5:	F2FCE02C8E3C1F69C6462E8F50518B92
SHA1:	6B3A1A6B6679C8DF1D0B81FDBD46368FC82FA2A1
SHA-256:	C118A62559E0D16441F20928A9EB68581F46890487944F39CAE530512F23EBBC
SHA-512:	DC480DF5BD72044E548B0CD9550A185250AE098596AE86CF22013B299C43C16EA4BD963500709139A231D71269456BB95F81AE1BB09CA0D11DBC7B6150DA9F6
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....U.....C.....C.....8.....?.....!.1A.Qa"2..q...B#.....Rb3rC..S.c$..s4.....!1.AaQq.....?...Q.....(I~D[}L...p.t...0#.mz...c.x.....q.....U..]Z.O..G...1.....=k...2.....r=,K0.@...6<...p.t....5n.....WJ....Y..@...q.k.7.D.....*....8.VM....9...U{..K;..^G^.+....:Z.9....(._.x...2^.X..6.....Z..A..\y..... .k.....T..(...>B....O].:....@..?h.@E.;...).o.30.7=:.8....G.:@. .V.....G...4.....P....a..w...l.....8b8. N...o..%R....B.j.?..V.....\.n.1...`.R..60....i..T.x.....j...0.(a.)]....mH.....o#..@.(4..H....{..E.9WJ. ..(....7.K.....d`...N.....,.8.0.R..c.S.E.@RK5R.0.A..N...F. Y2...E....\..G^.*.).,z@.".4.....`....C..._. .....+.@..?h.@...X.

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\379F7A11.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	698841
Entropy (8bit):	7.948223172892605
Encrypted:	false
SSDEEP:	
MD5:	5B6CEBC52A32FBB69153430736A977AD
SHA1:	59563C8AFFE36D46BBBBBB1F5581B01ACBC04DCE
SHA-256:	FB796009FA6034727156769A44BA6CD8C82A6ABB1BC0E526C70BF321E5801F34
SHA-512:	41C03836618A5D6F2F6F1BA5618EE12055B42C23A12EFD9DF29451E716D12CFF7CF73D00232E8DBC7E6E5DC1DC9E59DA10A5F5E4F781CCD165F4123BF6B4C22
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....K.....C.....C.....8.....E.....!.1A.Q".a2q.B#..R..3...b$...rC.S4.%.c...Ds.....?..t...R.8.[.'`.?...Vj>U...x&$...X..#B2.`..@...`...I.L...H.....Rt.a2..UM.....zO.h+{....p.$..h....unZU..%vfx..L...@>b..A.8...F..7..E..j...).C.C..A..=.....}...z...].i..JD.@8VG.....@04.YjREy..=.@..Du=;h<....G...-....{m.....V.x`|..e.....}.s...1..v3..;..@.y.g..+.v)..7.....9..`.H...o.....mp=...F.a...t...9.m.,....^....E/pz...U.#.$L..c..Z.S...._p"....L.^F:.5.q...}.....k..`G^...A...(ed.....L.w].NEl.....f0&d.?^..7..B3MI`.[w... l.r..M....p$....._.....G.....s...kS.H....F...x.m...d].'..]..=.^....O.r.Qe...d.TKp.Du.... P.....g....x..w1..G....T..._l.b..OS..EQp>...k

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3946BDF6.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	528727
Entropy (8bit):	7.942279931323295
Encrypted:	false
SSDEEP:	
MD5:	5610340C45AC614CECC4B45A260A41ED

SHA1:	4774619D33A8714E1E4061F99F5DC1C1BD45017D
SHA-256:	A54A9ED63B284B6438301F1DC098DA87D66C00C3F9BBE80A7F31CB6DB331A324
SHA-512:	09A8BD9ED8CE2538F2474DBDABA80F3AF67883B11C8B190A037BEB37F63F357A0F513AA66BA4E4DC594CE43A5A14084308722969355C559C5251E2D20B37F2B4
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....K.....C.....C.....8..... .....@.....!.1..AQ"aq2.....B#.....Rb3.rC$.....S%.c4.....&.....!1Aa..qQ...."..2.....?...X.PNUr..1...>./._u.]...._.X..du4..M.. .^aT.....x.rT.....w..c..F.q.V.....0.pF.~:tb.....K^C...E{'.)B.~.|.y(.....?.N.....}.@...'d.....f..=...V7..b.].:..6..9.-w...#w...%..+.o.Z...P..#..o.n.....u.u....f.[....'.....J(.....t._..... ....:.G.W..W.'.....?.C.....F.{'3....mE....'....X-....I... ....6.....y|~rj.p...~.....hv.3..d....-G.a..'..._.^....i.KPv@...p.....Q..-g.....u.;....U...L.6.....=...}.w.....-.....|O.j.:..?p..%..x....D..E .W.....Wa....R.(~Em7.V..r)....u...8Y.kS..N.0.E.g.S..}...q._....VK...q^.z.Z{....c..R..u...

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4964F8DE.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 57x56, components 3
Category:	dropped
Size (bytes):	2406
Entropy (8bit):	7.350722063542453
Encrypted:	false
SSDEEP:	
MD5:	DE9E2081CA419F1F313DEF734E92B3C2
SHA1:	E78FB1997A3CCE6F5AF763F2ACE1CFA1761B9980
SHA-256:	393D6596C0845C8E24D64BC731A35425377E952C164BDEC551F798DB48270E14
SHA-512:	D5FF7A33A3986F54CA6555126299CE6067B68870DE084FA0F18221CF8B36F78932BF65D842DB694DAC87940C7CFA9F8F7F4D8054F17784B0B7770A686A2121A2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C.....C.....8.9.."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....*..V.....>..3../.X.....o...G.. .Y...o....m.g.....?.)...{... ..<w.[..'.!.....l...o...?.....[.}.g.....3.....J..I<m.|F.?....Z|5...O.&.m...p....2.::,.$.C..$a.1....;,.....o4..G.....!..?e....)..X..+..?...%...G.ggm.y_b.v>.~.3.F..... .....|1...o.+o.W..6..%....h....o.../.[...y.....O.....H...z?.....O.....H...z.....\.....O...?.B.

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\4DAE6E50.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	278917
Entropy (8bit):	7.858243593920861
Encrypted:	false
SSDEEP:	
MD5:	335E607D2CC7BB1E8CB5B1C3BD59CBF9
SHA1:	ED555AA9DE4737D7A225EEC37C08C71BBABE7619
SHA-256:	6CA1E4602E9B1F90460CBBBFA4069E79F7B11D2571602980207655CA25661F06
SHA-512:	864B60811F10C8C1EF92193B2335F2B5725454B6C67793B6457E63342A70769A89FA4D0F3978C7D5AB91E2163BBEA04653E0FEEB857CCB4131EFAC30C2E5443A
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....X.....C.....C.....8..... .....>.....!1.A.Qaq"..2.....B...R#b3r..C...S..cs.....?.... .".. .".. .".. .".. .".. .".. .".. .".. .)..A.{ ...~..2.....BKpt...t..... ....Ah"..._.A.6d..Y.8...:..?...}uAtA[...9..(WW..@@.82.t...y..z .4q~(.5k...r....A..... ...BPU.....T.T.r.....f...~.....!.SV..v.-..D.Z..N/.....$...A.t....c^(%.p..].A.....=...iR.=..P] OC..^..A..w.L.^.+qA_..PR...Nh".A: .AH".. .".. ."...z:..-....WAE....A.D..A.D.....2:...\.A>.).A.D..7...4...t...A.D...@./....v..;...".K.b.}PB]. ."..!.8z...=.47@.N.4.....D.H...+..2%. .%.8 .d...s.. .....).A..H.....].JA..m.r@.o..:..:}u@....f.wr@$. ..Kh..,....]..J..&[...../T....m..z..,.hmJ .x.h.... .L.P-.?..

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5A5BBD72.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 10x1, components 3
Category:	dropped
Size (bytes):	651
Entropy (8bit):	6.584685575659917
Encrypted:	false
SSDEEP:	
MD5:	A646BB573B7C5AEB4EBEC789D384A2B5
SHA1:	9AC454BE8B3173E1A7D5591FE38796427E0E3E4E

SHA-256:	BC4ADD3C3D2A97243818BB1464C7C8426643696348B91EB27299CEFC5BF96E98
SHA-512:	1060ED1E3DC2690DCAD06AECBD475704CB294BD8E7390300252B46CD5815F0E36A42A594177FE682528C53AF1903E4E6422155E1478C65751C244CE06EC95F7
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....\..:...?.?...._...P...

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7A1D47ED.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 2540x1429, components 3
Category:	dropped
Size (bytes):	221286
Entropy (8bit):	7.673562418106071
Encrypted:	false
SSDEEP:	
MD5:	96621688ADD6E84DB55045D657EA054D
SHA1:	674A71EB639FF99097924471AFC9DFA165C0BB5A
SHA-256:	E8575111AEFD2D78CD37A703704EDBF63760A34BDAC48A030913E17BBD468D44
SHA-512:	62B6E94CD5B5128D610AE60F6FB4FF3E0DA8D6A816CC9AC8F962E2D7CDF6B7C46BD5414C951582C5A215678F6B98A09F432E0D0BF7F61921F076B3E0B9F713B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....C.....C.....s... ....!.1AQ..a"q..2.....B#.R..3.b.$r..%C4S...cs.5D'...6.Tdt....&.....EF..V.U(.....eu.....fv.....7GWgw.....8HXhx.....)9IYiy.....*:JZjz..... ..m.....!.1A.Q.a".q..2.....#B.Rbr.3$4C...S%.c...s.5.D..T.....&6E.'dtU7..().....eu.....FVfv.....GWgw.....8HXhx.....9IYiy.....*:JZjz.....>.....?..9..0.U..b...]...o. 'b.....]....*.b.S...+....v*.*.U.....v*.P.U.U.R.....]...5...p...T.#..E|1E,...G....b..[.....'..8.+p.ZX...n.;.8.t...|P.....ZF.R.U..;...m+.WF78B..Y.w8.....q..b..E).....k....b.NE.G.4zaB.U. P..v*..Z..7LP..KG....O*.....`K.LV.p...B.j`J.*.....*T.,... .h]....-=qKX.Bq....0..[.!.;.....P.P.U..]...&..)....4.<qJ.).....

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\7C5B5FA2.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	820038
Entropy (8bit):	7.957734979229796
Encrypted:	false
SSDEEP:	
MD5:	1924AC53015DA65542BB42E40FD962EA
SHA1:	8AB31F61B7B82C036AB844E5C6888CD8D9D45180
SHA-256:	D01CE8FFE0965853F207CA0829AAC69AAAF4C764A2D9CF35E23837F190C63E8D
SHA-512:	8D33FFE1CE4756491A55E09E158C0FB7201C0A58E100244D3FAF06EF595E8D82F04CAB64A2F2991355866A814F1EDD531FB607A54F7F0C7CD5AEF47F4A0E893B
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....P.....C.....C.....8..... .....F.....!...1AQ".aq....2..B#....$R3b.4.rC%...SD5..cs.....?...N~...Z5f.mbxY...!'S.t....>.,...Ib...Gn.\k.....R(I.^..\(&df... 2@$..#8.:.a.....k.u.t{.....v..k<...,...;.X...._...@a..*..c.=.. `..(.P..>].I9nW...nGq..tQ.F....O@1.f.a.....I..3.v..A.wg.b...;....`.....Ai'Jj...X$.r..>=...|.~Ek.VG.....i...?.....A.e?...S.%,.c.\..... =j.xz1r0.nJ..q.`s..9..A....y.z.....c`...i...5..z.....D....o+.....G.....oI.....8.....9C.e.b.....M=..[.(...p..v$...AY`).g.c..I.....:.^.[V.dQ.d...3....#..b3:.....m{.>.].nz..Q.|Vv.!1.8m.. .k.H..@..K.....b.].6.Q.....J...rJr.RO1>...I...7...<5,..r.... .!..]..Ca>.Y@...z....5..a.!Bx.b.K....<.Gc....J..X

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\860FEEE5.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 10x3, components 3
Category:	dropped
Size (bytes):	650
Entropy (8bit):	6.587598234229773
Encrypted:	false
SSDEEP:	
MD5:	8B502486F7CB690DC0F8F474363C1404
SHA1:	843F1350C1F773D425FB4167A01A1C21F71D1D4D
SHA-256:	DD289CE38BBB5E97E2A18A4BAAB3B2FEA571CE6492CDB3793CBA4010D00DD2AF

SHA-512:	C06DC1289FB485CE33BBCA7DC17248F36B24E6DAF5F47A051D1E166900B5E39DA5B1E3F1282C954C2742E2EA605EBBC3C7AAF6C306C667E5A6837B1D51F240 31
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C.....C.....".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....r.....9i...E....

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A38B76C6.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	558041
Entropy (8bit):	7.9426360654130646
Encrypted:	false
SSDEEP:	
MD5:	4E718B48B0DA3FC918FF52BDF58A79C7
SHA1:	04CBE4EC63AA9813C0705C94BA1782798D86CB78
SHA-256:	068A5CB556887FAE17A67DACF36CCC0EE1D578D8822A95E5ABE9EBFAB3F5096D
SHA-512:	C19D82B4D20CA9C509B7A5EAC85AF253F701FA5A67F9D305B2B4BD470510B1F7BAE95792218BD007D4A694CA85C8F32BDEBFD03B763370D4D62D47AD4827B4 03
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....P.....C.....C.....8..... .....@.....!.1..AQ"aq2.....B#...Rb3.rC...S$.4.c..D.....?..=.%...Q.....M.W..+^R.\|.....[./+d.~:..b....r.3.....R.....h....[+V.g. .....b/Z.[m.....x..Z.....!ot...&.#..a^".....3r}...C1....2..),.....-.UxY}.wF.U.#@.<-`I.;n..2..Tl.B.&E..M.0q'8G23....uK...D.r...'x.m(Y..T...O....UF..I_0...\|> .....6.S.fWg....V.2.....+B.-. {...q.....0...f...;..6^p5...a.....h:.b....8...._..k@..>....8.}.....9..>.}7..@eM.B.-..Lh6.^6..p.K.....C.qX.....dX.+.....2.I.....}.V.5g\|G..h6..^..1...O._:.*G;5*.Tgh`.....%.-....-_..X...5.. .u#.1.:...zR.)....?....$.A....~....{.=.$0nl/....F.....!...%.....A...6.q...@.6.Z.6.V..y...@_o...T}.;.?...5..M.Vm..Vgo>.h

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A4460ACB.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	264405
Entropy (8bit):	7.930410397393636
Encrypted:	false
SSDEEP:	
MD5:	5AC4A5F3DC3713108189228077312139
SHA1:	78DD5CFA187B2DE8D963CF60B67D2066C2248188
SHA-256:	51BDC7D7F70702980CFC01864C9BF2128972730D9C199A247F728A75EA2AB685
SHA-512:	642AE0C44D8C5DD345BFC3952548182E79540ADC961BE9ADAB6F46FCD61651068C685C4EBD33015E2FE9BB6D4CDE3CD0117A345B078054170EEDEFB85B684 38
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....U.....C.....C.....8..... .....=.....!.1A.Q"aq2.....B..#.....Rb3.r..C$.S%c.....$.....!1A..aQ"q.....?....o..{W....X....L.v.M...Q..).S.9;E.&.#.. p..kX..&..t.LC.n$w....-...HM...Z..LkY...N...I."..J..$L.@..&.mQ.....t.J.X.zl.J..Z..Q.Z..",./!..TZ..F.:4...@A$q',QQ..0t.4&..p..V.u~F..A.....CCA....._f.Sz..$G.f....5..c-rb...2m.@. J.5D.c...0...F...7..A..PW...}i.T.M..}.....<..Wf.....-..:../..Y...$t5.Z....M4..QJ.MeEF.|e.^.+q.XE.....v...h.....GU.....>eL.....4...I.M.I..j..w..;W.:...:.....{I...TA.....j0..I..v.4.E....]j..'. ...m.C..R:..:.*Q...J.v|..|a.zH....,w..=..o._.."]k...9c...q...C[q..;.41...!..p....x...P..t...d....<.j+4.o4..M.:...q..N../.6.....V.....1.(....n.

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\A54DA97F.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	70603
Entropy (8bit):	7.140447789990316
Encrypted:	false
SSDEEP:	
MD5:	5887BC78EAC0C8D784C5898D4913FEBD
SHA1:	8B72A130479222C0DB48C1EB3529B1F9C37EC70C
SHA-256:	26E736EB8B7FB54B6FCF9A681BC7092AED59FF711ACFF4886CE668383AD0D060

SHA-512:	27197C9B253CDDCD5C939710F24B2D2CDAEF9612165D300BE1DB8BF12D03E3C2E058794515CBD24BC58B928EC9BE6F363B02706C90DB605A56F4918113DA32 8
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....L.....C.....C.....8..... .....!.....1AQ...a!q.....?.....A.@..s}.....P\. ` `\.....(0000000000000000.....<.....y...@... \..d..x ....@... \....(.....<.....x..@.s.... @P.y.....'.....'.(,.@.r....N..d.....Pi9...`_ .>....P^...7.....q...N..h7.....N..P@`n '.....}.<.y.....`.k9...N9...O .p.....,...%...Y..@I...@A,.....K.@ I...@@I...@.,.....MOP...OP@..6.....:...A./.@M.... .....K..0,..@.R...../.@.R.....^...../.@.....0000000000000.....0.AA.. `0`0i...y.....|.....`....A@....x.... Y.... @P.>@...Y...N ... \.PP98..@.r..' @.r....N.....^8.....g.....Az...A.....Pn(7.....u....u..P@`N..X..r.e...>.

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\D4C0E1A8.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 1920x1080, components 3
Category:	dropped
Size (bytes):	1177633
Entropy (8bit):	7.949732545805057
Encrypted:	false
SSDEEP:	
MD5:	42B7913ADEA6A320F6B667A072E0E4EF
SHA1:	18ED27C14BF85708CD97CC9EB7107D33E70EEA48
SHA-256:	B0CA80CF95664A89DB69895AB3E4D7B122FC3A63A3847BD59B1140F2C8F8E353
SHA-512:	0DB02309479375D769C5856AF6760723B777662B377C3775627BAC567B9B20CD9BF5AD9C0D9AC2940125A972BE1168BBE657B372DD878F5F12D1EBF886776F6D
Malicious:	false
Reputation:	low
Preview:	......JFIF.....Adobe.d.....Exif..MM.*.....Ducky.....U.....C.....C.....8..... .....B.....!...1..AQ".a.q.2#.....B..R...3$br..C4%.....?...r.;..f..`K.2.)N%.:...-(..n)-.%.....$..5..{..!].1d.n.8..N6..r..... .H$..E... f<K.}.....T..K..../..tq..^.(.).....K.p..<N..I..C..Bu..j.].6.H..JT...z..E.....{...].S....B..%H...qp.Z..*.....o]p.t...'$bK.V....(0..v.@x)....PR.>{t.r.rq...).-.".G..95....\.i.....:.....+.r? ..v.!W..e?...0^y..8.E... ...5$...{.{..y.YN4..R<...-.~?.y...BA+.".$jt..c....y....G.....3.%Ky.....Y.....F....Ne'..I}..a....S3X.....D..Z(j5.(.....;.e.E...T.....%...G..4....s.9...z.WKK.7...4...p. 8..&....R.t...8W...q..x.d.-mF&K.).VKl2P....QSMI.A..|c.^3.Yo6....mJ....:...i..'...PGq.E.o..~.N=o.6E.IPJ.i..C`U

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\DB29F6C4.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=4, software=Adobe ImageReady], baseline, precision 8, 174x138, components 3
Category:	dropped
Size (bytes):	9054
Entropy (8bit):	7.871446681431426
Encrypted:	false
SSDEEP:	
MD5:	7027A1BF5F1026419278DE39A7DEDB49
SHA1:	2846234BDE825EBE0250140F0D5D9E94D62A8287
SHA-256:	EE0E328A138B5E5BBA977BE895178762B7F49985A28764C7EC43B04F22C7A683
SHA-512:	405BDC38592E72C8A2076A7ACDD0BEA41C193D22157A0BA36C036048EFB808326B942B2857ACDA640F076E464A9B61C5BE29D4945682DDA0320BB79E57D0D5 3
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....XExif..MM.*.....1.....>Q.....Q.....Q.....Adobe ImageReady.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!22 2222222222222222222222222222222222222222222222222222.....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CD EFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*5 6789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..9vy....._...F.....c.A.....JZ..v..c..+.B..=3.v.)...)'eu<..',O.v..G. .2[.^...&.!"X.s.w8.=Gn..m.`Y..O6...@}O...E&.yT./T.2.....CL&..H...f.....P.P.."T.@..g.". ..#...$.I%_.i.6$.....<v....T..e. '6.#.....,`../...{t4.O..C..|... .S..B=.h..F.2.z.....

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E3E13574.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.02, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 176x176, components 3
Category:	dropped
Size (bytes):	28392
Entropy (8bit):	7.935956341093106
Encrypted:	false
SSDEEP:	
MD5:	D7B5B9ACC51AE4D1952D0807CD730479
SHA1:	35B34F36DBD22312E260588EFFCD60E67296B1D1
SHA-256:	7569ED3DE1DA6389AF57FD52B839DEDE743C69B340338CA2F363E422F8E2AD0A

SHA-512:	09266F2DB97C56759E8EFF656089E5E041D3EDD97990485D0445D8D320C7D3CBFB85DD1DCCD71C4E99CA19496CC2950166501964FAAEC3EEAC7598CFF03A3 B
Malicious:	false
Reputation:	low
Preview:	......JFIF.............Adobe.d.........Ducky......._.....C..C...-....... ....%..#.bCc..F(A3..?..}..^!.!....%c.<|.w....._'#....X.1.z.[.+....[..&Q#.'Q.<.^.....cV.h&.9..."....8.<.D....IF..S3....%...R...."N.'.e. 1.3 .M.......=^....W.%a...S T*......Z.np..l`u.^ ...y.o.x..v.h...`h.^....."..*a..yU2.B.P..7p.V.g...F..D"%.o......6o..3juWV.K....4..&(..(....8.FY.l..J5..hi.?F.(.D..*.!.t.=..$Q....u.S.....q'.....:U J...w......qZ9.T...}D-......H%./...(.C.H.x./n...v.Fw.........Cc'T.D.S.$t...Y..fa.\..@..s"h.....j.........W....-....'[..aT..p.FHD`.E.K-i..n..*.........$\|..#.#[.............^...o.w.._.Eos..5:Vl.k.....@ Q\....u.&e0.l(..#E.M.Q......VV.=..*......`.>^...._...$f.~..........2eQ3,..q.v..xf.Yhi.P..P:.dM!.@VtS.x.......I....

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E44A150A.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=0], baseline, precision 8, 100x100, components 3
Category:	dropped
Size (bytes):	3922
Entropy (8bit):	7.825059024683028
Encrypted:	false
SSDEEP:	
MD5:	D526A7CFE31880576A7EFD82B16C6B0A
SHA1:	D8B1FA76C45174BDF8083402E4D8AF7F4945217A
SHA-256:	E8E64B926CB24F6D2E7C4641E3F1B8225C803306858CDB5881DBF5A071E1BCC8
SHA-512:	AC328A8DC1803D6C70BF8435DF32A677EE1D0C87228B78B1F0264CABAFC25249C78691374FC3FD9B70DABCEFC7B68208F54C37439B676863DDF60639E44503I 4
Malicious:	false
Reputation:	low
Preview:	......JFIF.............Adobe.d.........Exif..MM.*.............Ducky.......F.....C..C...d.d............. ....7......................!.1..A"Qa2.q.B#..R3..b..$..C..?...@0XI.=t..L&..?#.,5Yr.[....N.....h.._.....7;..\c....8.%.I^3...r......-...]...... ....G.k.e...sX{.8.$..4..~........Lk...6*...X9.(.....=',.b...q..."X..J.(..5)..F.....G.6.v^U.Mg...k..v...A~.E9..v4..O..DlT.b...Un.Fe.-...*Vz...t....^.cA}kF5kR1..T...F.X..h.b./.c..1...))`{.T.E v.I....t..........rOc.^s....}.t..W....)k...RH..L.;.....L.-...[A..+(.)U.Y.&...Gy.......I6... ..<A.t...>....U..[#..3.....S.!..*Ic. ....4...9...P.V;.z.L.......h..U3...f.>Ek...!Z.X.....r.c@{...2(....#.....F.....0A. ... ..y!...u...Z..kr..P5..`:..!...m.Ac.|......OTJU.h.....a....@o.{.G?.}bzN...X..T..+...o..#..<....=.9"....x.a

C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F90673B.jpeg

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=5], baseline, precision 8, 352x208, components 3
Category:	dropped
Size (bytes):	32811
Entropy (8bit):	7.951114825435616
Encrypted:	false
SSDEEP:	
MD5:	FEAAED7027775E59B74A76257D7EE600
SHA1:	837F0EC190E480D976B0E4F26EE2BA59C0A801B4
SHA-256:	8C39120FD4C18F370674148DAA3EB2C80050B2C04B17260227CA6E9BB89CDC54
SHA-512:	EA0CAB0B0E9E95FE0CADF355F8279D45A6B61C247D877A10982D42552321DA4B145C97266BB9A493738E62557A29BE89EDAADA718057BFCF8DC6FDFFA38969 36
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....ZExif..MM.*................J............Q...........Q..........Q..........................C.................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!2222222222 22222222222222222222222222222222222222222........`.."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJST UVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDE FGHIJSTUVWXYZcdefghijstuvwxyz..?....Z....'M..W9`B.F8..3..Cy..i..6W..om..#i..B..y....z.Y`.r84.ydivwc.f9$..@.....k.... .m....P....".~.!,<..16...l.....c<....?.?..w.l..9....t1.1u+&....c.l....^M0..5.N...%.:....@......K....Z\"\...^.....<...}).*.e...Q%..u.3..l.;..A.g.x..{B.h.\....1C..Q...e.Xm.u..F...../,.O{..

C:\Users\alfredo\AppData\Local\Temp\Diagnostics\POWERPNT\App_1672906054575304400_623894A8-1F58-4A5C-98D1-A45B3C2C368D.log

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	ASCII text, with very long lines (15196), with CRLF line terminators
Category:	dropped
Size (bytes):	72622
Entropy (8bit):	5.549400388194359
Encrypted:	false
SSDEEP:	
MD5:	E156FB22A7413BBA1AF0A896DD77C54E
SHA1:	651403DB062880D8FB0AD0EF7CEA0D27D0D92D47

SHA-256:	09C0103CB59779644DED5CA32DE5770E7425C02E28CC667E740E64F6188E9781
SHA-512:	9D57AB7903B21C0EA1F75636161662E2C76ADEFE47567ADC41CE113065BFB009BE5133CAC19EE397A22BDDF3EA23B0C449D07F79763D23919072B16FE0DAA39
Malicious:	false
Reputation:	low
Preview:	Timestamp.Process.TID.Area.Category.EventID.Level.Message.Correlation..01/05/2023 08:07:35.471.POWERPNT (0x3EC).0xE10.Microsoft PowerPoint.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Canvas.GraphImport.EntryPointAppear","Flags":30962256044949761,"InternalSequenceNumber":28,"Time":"2023-01-05T08:07:35.471Z","Contract":"Office.System.Activity","Activity.CV":"qJQ4YlgfXEqY0aRbPCw2jQ.1.14.1.3","Activity.Duration":54,"Activity.Count":1,"Activity.AggMode":0,"Activity.Success":true,"Activity.Result.Code":-6,"Activity.Result.Type":"EntryPointResult","Data.DetachedDuration":23,"Data.GoLocalRequestSent":false}...01/05/2023 08:07:36.371.POWERPNT (0x3EC).0xE10.Microsoft PowerPoint.Telemetry Event.b7vzq.Medium.SendEvent {"EventName":"Office.Text.GDIAssistant.RegisterCloudFontCallback","Flags":30962256044949761,"InternalSequenceNumber":38,"Time":"2023-01-05T08:07:36.371Z","Contract":"Office.System.Activity","Activity.CV":"qJQ4YlgfXEqY0aRbPCw2jQ.14.2","Activity.Duration":22,"Activity.C

C:\Users\alfredo\AppData\Local\Temp\TCD4405.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	242
Entropy (8bit):	3.4938093034530917
Encrypted:	false
SSDEEP:	
MD5:	A6B2731ECC78E7CED9ED5408AB4F2931
SHA1:	BA15D036D522978409846EA682A1D7778381266F
SHA-256:	6A2F9E46087B1F0ED0E847AF05C4D4CC9F246989794993E8F3E15B633EFDD744
SHA-512:	666926612E83A7B4F6259C3FFEC3185ED3F07BDC88D43796A24C3C9F980516EB231BDEA4DC4CC05C6D7714BA12AE2DCC764CD07605118698809DEF12A71F1FD
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.a.b.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4405.tmp\TabList.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	4888
Entropy (8bit):	7.8636569313247335
Encrypted:	false
SSDEEP:	
MD5:	0A4CA91036DC4F3CD8B6DBF18094CF25
SHA1:	6C7EED2530CD0032E9EEAB589AFBC296D106FBB9
SHA-256:	E5A56CCB3B3898F76ABF909209BFAB401B5DDCD88289AD43CE96B02989747E50
SHA-512:	7C69426F2250E8C84368E8056613C22977630A4B3F5B817FB5EA69081CE2A3CA6E5F93DF769264253D5411419AF73467A27F0BB61291CCDE67D931BD0689CB66
Malicious:	false
Reputation:	low
Preview:	PK.....e.>.....]>.....diagrams/layout1.xmlz.....Z..6....;..{.....lw.E.o....i..T....&...G.+...$..(.6..>Y.pf8C.|3.?..m....xA8v.`.hW..@..Zn..(kb..(.....`.+....Y`...\..qh.0.!&w..)|...<..]Q.._....m..Z.{3..~..5..R..d..A.O....gU.M..0..#...;.>$...T.....T..z.Z.\a.+...?#.~.....1.>?...*..DD.1...'.,..(...5B...M..]..>.C..<[....,L.p..Q.v.v^q.Y...5.~^c..5.....3.j.....BgJ.nv.. .....tt.....Q..p..K....(M.(]@..E..~z.~...8...49.t.Q..Q.n..+.....*J.#J.... .P...P.1...!.#&...?A..&..".:|..D.I...:.....~/.....b..]..... .nI7.IC.a..%...9.....4...r....b..q....@o.....O...y...d@+~.<.\....f.a`:...Qy/^..P....[....@i.I._.?.X.x.8....)..s....I.0...|.....t...;...q=k.=..N.%!.(.1....B.Ps/."...#.%..&...j<..2x.=<.....s.....h..?..]?Y?...C.}E.O.....{..6.d....I...A.....JN..w+....2..m>9.T7...t.6.}.i..f.Ga..t.].->...8U.....G.D`.....p..f.. ...qT.YX.t.F..X.u=.3r..4....4Q.D..I.6.+PR...+..T..h: H.&.1~....n.....).....2J.. O.W+vd..f....0.....6..9QhV..

C:\Users\alfredo\AppData\Local\Temp\TCD44A3.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	280
Entropy (8bit):	3.484503080761839
Encrypted:	false
SSDEEP:	
MD5:	1309D172F10DD53911779C89A06BBF65
SHA1:	274351A1059868E9DEB53ADF01209E6BFBDFADFB
SHA-256:	C190F9E7D00E053596C3477455D1639C337C0BE01012C0D4F12DFCB432F5EC56
SHA-512:	31B38AD2D1FFF93E03BF707811F3A18AD08192F906E36178457306DDAB0C3D8D044C69DE575ECE6A4EE584800F827FB3C769F98EA650F1C208FEE84177070339

Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .I.n.t.e.r.c.o.n.n.e.c.t.e.d.B.l.o.c.k.P.r.o.c.e.s.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD44A3.tmp\InterconnectedBlockProcess.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	9191
Entropy (8bit):	7.93263830735235
Encrypted:	false
SSDEEP:	
MD5:	08D3A25DD65E5E0D36ADC602AE68C77D
SHA1:	F23B6DDB3DA0015B1D8877796F7001CABA25EA64
SHA-256:	58B45B9DBA959F40294DA2A54270F145644E810290F71260B90F0A3A9FCDEBC1
SHA-512:	77D24C272D67946A3413D0BEA700A7519B4981D3B4D8486A655305546CE6133456321EE94FD71008CBFD678433EA1C834CFC147179B31899A77D755008FCE489
Malicious:	false
Reputation:	low
Preview:	PK.....]w>....<...5.....diagrams/layout1.xmlz.....].r.F.}.....1w`.J..'.....w..Dn. d....~.....pw...O.....s...?...p7.t>e.r<.]u.e..d..|8..\uo.....K...._.Y..E6.|..y;.....y.*/:o./...:[.o.+/.....?.....Z.?..s..d}...S.`...b.^o9.e.ty9_d...y>M.....7...e....."...<.v.u...e:].N.t....a....0..}..bQ.Y..>.~..~...U.|..Ev.....N...bw....{...O..Y.Y.&.....A.8Ik...N.Z.P.[}t.....|m...E..v...6......_?..."..K<.=x....$..%@.e..%....$=F..G..e.....<F..G51...;.....=...e.e.q..d.....A...&9'.N.\%.=N.Z.9.s.....y.4.Q.c.....|8.....Eg.:.ky.z.h.....).O...mz...N.wy.m...yv....~8.?Lg..o.l.y:.....z.i..j.irxl.w...r.....|.=....s};.\u.{t;i~S.....U7..mw...<.vO...M.o...W.U.....}.`V<|..%....l..`>]..".].I.i.N..Z..~Lt.....}?..E~:..>$.....x...%.....N....'C.m.=...w.=.Y...+'M.].2>.]_~...'.?...:.....z.O..Y.....6..5...sj?.....).B..>.3...G...p.9.K!..[H..1$v../...E V..?`....+[...C.....h..!.QI5....<.>...A.d.....

C:\Users\alfredo\AppData\Local\Temp\TCD4503.tmp\BracketList.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4026
Entropy (8bit):	7.809492693601857
Encrypted:	false
SSDEEP:	
MD5:	5D9BAD7ADB88CEE98C5203883261ACA1
SHA1:	FBF1647FCF19BCEA6C3CF4365C797338CA282CD2
SHA-256:	8CE600404BB3DB92A51B471D4AB8B166B566C6977C9BB63370718736376E0E2F
SHA-512:	7132923869A3DA2F2A75393959382599D7C4C05CA86B4B27271AB9EA95C7F2E80A16B45057F4FB729C9593F506208DC70AF2A635B90E4D8854AC06C787F6513D
Malicious:	false
Reputation:	low
Preview:	PK.....YnB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`...nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....bnB;?.....f....._rels/.rels...J.1.._%..f....m/.,x...&.lt.dV.y.\|..."v....q..\|.....r..F..)..;.T5g.eP..O..Z.^-.8...<.Y....Q..."....*D.%.!9.R&#"."0(.u}).!..l....b..J..rr....P.L.w..0.-.....A..w..x.7U...Fu<mT.....^s...F./ ..(.4L..`.....}...O..4.L...+H.z...m..j[].=.....oY}.PK.....J.L6...m....,.....diagrams/layout1.xml.X.n.8.}N.....PG.....wZ,..R.%.K...J.H]....y.3..9...O..5."J.1.\.1....Q....z.....e.5].)...$b.C)...Gx!...J3..N..H...s....9.~...#..$...W.8..l`\|..0xH}.....L.\|..(V;..1...kF..O=...j...G.X.....T.,d>.w.Xs.....3L.r..er\o..D..^....O.F.{:.>.R'....Y-...B.P.;....X.'c...{x*.M7..><\|.1.w..{].46.>.z.E.J.....G.....Hd..$..7....E.

C:\Users\alfredo\AppData\Local\Temp\TCD4503.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	250
Entropy (8bit):	3.4916022431157345
Encrypted:	false
SSDEEP:	
MD5:	1A314B08BB9194A41E3794EF54017811
SHA1:	D1E70DB69CA737101524C75E634BB72F969464FF
SHA-256:	9025DD691FCAD181D5FD5952C7AA3728CD8A2CAF20DEA14930876419BED9B379
SHA-512:	AB29C8674A85711EABAE5F9559E9048FE91A2F51EB12D5A46152A310DE59F759DF8C617DA248798A7C20F60E26FBB1B0FC8DB47C46B098BCD26CF8CE78989ACA
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .B.r.a.c.k.e.t.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD45D3.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.4721586910685547
Encrypted:	false
SSDEEP:	
MD5:	4DD225E2A305B50AF39084CE568B8110
SHA1:	C85173D49FC1522121AA2B0B2E98ADF4BB95B897
SHA-256:	6F00DD73F169C73D425CB9895DAC12387E21C6E4C9C7DDCFB03AC32552E577F4
SHA-512:	0493AB431004191381FF84AD7CC46BD09A1E0FEEC16B3183089AA8C20CC7E491FAE86FE0668A9AC677F435A203E494F5E6E9E4A0571962F6021D6156B288B28A
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .c.h.e.v.r.o.n.a.c.c.e.n.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD45D3.tmp\chevronaccent.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4243
Entropy (8bit):	7.824383764848892
Encrypted:	false
SSDEEP:	
MD5:	7BC0A35807CD69C37A949BBD51880FF5
SHA1:	B5870846F44CAD890C6EFF2F272A037DA016F0D8
SHA-256:	BD3A013F50EBF162AAC4CED11928101554C511BD40C2488CF9F5842A375B50CA
SHA-512:	B5B785D693216E38B5AB3F401F414CADACCDCB0DCA4318D88FE1763CD3BAB8B7670F010765296613E8D3363E47092B89357B4F1E3242F156750BE86F5F7E9B8D
Malicious:	false
Reputation:	low
Preview:	PK.....NnB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`...nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....TnB;..d.....h....._rels/.rels...J.0.._%.n..)"....<.w.&.4..!...y.|.....|.&3.o...S..K.T5g.U....g..n.f....T*.hcf...D.V..Ft....d....c2".z.....N.s._2....7.0.V.]P.CO?...`...8....4&....._i..Y.T...Z...g....{-...]..pH..@.8....}tP.)..B>..A...S&.....9..@...7.....b_.PK.....r};5.z.....diagrams/layout1.xml.X.n.8.}.....4.+.(...@.....(..J..._.!)..b..v.}.H..zf8...dhM....E..I.H..V.Y.R..2zw5L~....^..]...J_..4.\.\.....8..z..2T..".X.l.F#.....5....*....c....r.kR.I.E..,.2...&%..".qF.R.2.....T;F...W.. ...3...AR.OR.O..J}.w6..<...,.x..x....`g?.t.I.{.I...|X..g.....<BR..^...Q.6..m.kp...ZuX.?.z.YO.g...$.....'.]..I.#...]$/~`${.

C:\Users\alfredo\AppData\Local\Temp\TCD4603.tmp\Dividend.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	570901
Entropy (8bit):	7.674434888248144
Encrypted:	false
SSDEEP:	
MD5:	D676DE8877ACEB43EF0ED570A2B30F0E
SHA1:	6C8922697105CEC7894966C9C5553BEB64744717
SHA-256:	DF012D101DE808F6CD872DFBB619B16732C23CF4ABC64149B6C3CE49E9EFDA01
SHA-512:	F40BADA680EA5CA508947290BA73901D78DE79EAA10D01EAEF975B80612D60E75662BDA542E7F71C2BBA5CA9BA46ECAFE208FD6E40C1F929BB5E407B10E89FBD
Malicious:	false
Reputation:	low
Preview:	PK.....1AE,.{E...#P.....[Content_Types].xml..Mo.0.....Z..N7.=l.....V0.-o..j?...H..sa...../UCb.'...r...w.i..e..<[....{2..U.m..N.{...r.....3.fj.o.....2.*....;.L.6..&,D.Cld8...a.gZf.....r-v..><....~/.....|Zk.....a.R&.d.(.$..6..}.:.....3.....1..[.p.....?..+....R...y,.fod.....e...-.|..#..]j....n:...f...-J...i.^.:Y....T.....m^..~GNp../e}...N....a..5.d.8YcN..5.d.8Y...7..A..e...7Q."3.....sL._...v...n..b..2].v....n.t....Z...Uk...j.&.Z....im|.r....B.....7DaBuN.... ...>..>..>..>..>..>.....V}-.....Q}#.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7FaBuN.... ...>..>..>..>..>..>.....V}-...Q}..&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7EaBuN.... ...>..>..>..>..>..>.....V}-...Q}3.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b.\}..)....A.....[..PK.....1A.s@.....O....._rels/.rels...J.1.._%..d...t.....}...n2!..}6.>..`(.v...K`2...70.....84P....

C:\Users\alfredo\AppData\Local\Temp\TCD4603.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE

File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.5459495297497368
Encrypted:	false
SSDEEP:	
MD5:	76340C3F8A0BFCEDAB48B08C57D9B559
SHA1:	E1A6672681AA6F6D525B1D17A15BF4F912C4A69B
SHA-256:	78FE546321EDB34EBFA1C06F2B6ADE375F3B7C12552AB2A04892A26E121B3ECC
SHA-512:	49099F040C099A0AED88E7F19338140A65472A0F95ED99DEB5FA87587E792A2D11081D59FD6A83B7EE68C164329806511E4F1B8D673BEC9074B4FF1C09E3435D
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .D.i.v.i.d.e.n.d...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4604.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	3.494357416502254
Encrypted:	false
SSDEEP:	
MD5:	6F8FE7B05855C203F6DEC5C31885DD08
SHA1:	9CC27D17B654C6205284DECA3278DA0DD0153AFF
SHA-256:	B7F58DF058C938CCF39054B31472DC76E18A3764B78B414088A261E440870175
SHA-512:	C518A243E51CB4A1E3C227F6A8A8D9532EE111D5A1C86EBBB23BD4328D92CD6A0587DF65B3B40A0BE2576D8755686D2A3A55E10444D5BB09FC4E0194DB70AF E6
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.h.e.m.e.P.i.c.t.u.r.e.G.r.i.d...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4604.tmp\ThemePictureGrid.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	6193
Entropy (8bit):	7.855499268199703
Encrypted:	false
SSDEEP:	
MD5:	031C246FFE0E2B623BBBD231E414E0D2
SHA1:	A57CA6134779D54691A4EFD344BC6948E253E0BA
SHA-256:	2D76C8D1D59EDB40D1FBBC6406A06577400582D1659A544269500479B6753CF7
SHA-512:	6A784C28E12C3740300883A0E690F560072A3EA8199977CBD7F260A21E8346B82BA8A4F78394D3BB53FA2E98564B764C2D0232C40B25FB6085C36D20D70A39D1
Malicious:	false
Reputation:	low
Preview:	PK.....X..<..Zn|.....diagrams/layout1.xmlz.....]..H.}.....M,l#g.j:.G-eu.*S=.$.....T_6..I...6...d.NJ....r.p.p.....|.z.K.M..L.T.(.....<..ks.....o...t}...P..*.7...`.+.[...H..._..X. u.....N....n....n|..=.....K.:.G7.u....."g.n.h...O.,...c...f.b.P.....>[l.....j.*.?..mxk..n..|A...,\o..j..wQ.....lw.~].Lh..{3Y..D..5.Y..n..Mh.r..J....6*.<.kO...Alv.._.qdKQ.5...-FMN.....;.~.. ._..pv..&...%"Nz].n.....vM.`..k..a.:.f]...a.....y.....g0..`.....|V...Yq.....#...8....n..i7w<2Rp...R.@.]..%.b%..~...a..<.j...&....?...Qp..Ow|&4>...d.O.|.|...Fk;t.P[A..i.6K.~...Y. N..9.....~<Q..f...i.....6..U...l. ..E..4$Lw..p..Y%NR..;...B|B.U...\e.....S...=...B{A.]..*....5Q.....FI..w....q.s{.K....(.]...HJ9.....(.....[U|.....d71.Vv.....a.8...L.....k;1%.T.@+..uv.~v.]`.V.... Z.....`.M.@..Z|.r...../C..Z.n0.....@.YQ.8..q.h.....c.%...p..<..zl.c..FS.D..fY..z..=O..%L..MU..c.:.~.....F]c.....5.=.8.r...0....Y.\o.o....U.~n..`...Wk..2b.....I~

C:\Users\alfredo\AppData\Local\Temp\TCD48A1.tmp\Celestial.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	3295051
Entropy (8bit):	7.9549249539064
Encrypted:	false
SSDEEP:	

MD5:	5978107C3CB2A4A8427E643D0A5587EB
SHA1:	A3A865B6D128E7C9C5821DF03B9EDFE136F53D17
SHA-256:	DDCEAEC2A8E652B60CFA4D5D4C7895D70AD25A214D70DE884302C8FE18F53910
SHA-512:	D9E0B9D52665F4C1E4B6CC32E6DEBA4C0CBC9309728415AC9588DDD84CAD47A90567192D24BF7FF2F5DD7836A559F396B5015ABF3E085ABC9B813FF365388D65
Malicious:	false
Reputation:	low
Preview:	PK.....1A.f}.....p.....[Content_Types].xml..n.@.._.....8i.'.....}.....(y...H}.....3Fi..%.....3..._...j.`.2....cod.(...r...w{s..)...]..3..APF.61...6ug.Y..... 7.....d<..Q.V6.N.....{.0.U5 ...>.-..Ko.nw.f...'.....!.s.=fw.{PaW.. ..82.;.<..os....n....>...w..%....P...v...v...'....m.m..3.[.._...:[,...h..!~s..^..Y..E.....^.9Y.j.....#x.....3....=....b}4O.*....k7.+.&.Xg.X.X..XSN.KN .+N.7.X....!..CR....I]...>....L...!=...9..!L.0.v.gEo\.....w..No.a.C.q.}<.....a..n./.....e.-)h9a..}i.}.."-..C.C.Xq..0?..M4.....r.A.+..\...r.>.... .W.\...re?..%.-/hiA..ZR.r.W.D.\}.E K..kZ.>.....4....&T.....Wlw.b....}..+.A\...q.....~.WK.Z^.....>.h..`.....}.....k..s.L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-}..i..`..G.....(.P.'....B\...}..+.A\...q.....~..+.!\-1hyAK .ZV..... ...-Z.>X.2.....>8..S.L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-}..i..`..G....(.P.'....B\...}..+.A\...q.....~..+.!\-1hyAK.ZV..... ..

C:\Users\alfredo\AppData\Local\Temp\TCD48A1.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	284
Entropy (8bit):	3.5058612801050892
Encrypted:	false
SSDEEP:	
MD5:	1F4035219DC6A0E9FD3A3164C6B6D0E6
SHA1:	C6CFB52EC8764F3B27782310DD74A71AB8EFD34C
SHA-256:	6AC194049AB034406AD36F9C4436CFC74BF03664A3C025F91D642779D15B9DFC
SHA-512:	1D86B380200A41547E2FF9A00CEFAB5895F88BD777EAF3981A0406B1CFD2139069D922A88963431EA781FB766A8410957A33816F8E27F57C1EBA85507540F715
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .C.e.l.e.s.t.i.a.l...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4940.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	260
Entropy (8bit):	3.4895685222798054
Encrypted:	false
SSDEEP:	
MD5:	63E8B0621B5DEFE1EF17F02EFBFC2436
SHA1:	2D02AD4FD9BF89F453683B7D2B3557BC1EEEE953
SHA-256:	9243D99795DCDAD26FA857CB2740E58E3ED581E3FAEF0CB3781CBCD25FB4EE06
SHA-512:	A27CDA84DF5AD906C9A60152F166E7BD517266CAA447195E6435997280104CBF83037F7B05AE9D4617323895DCA471117D8C150E32A3855156CB156E15FA5864
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .V.a.r.y.i.n.g.W.i.d.t.h.L.i.s.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4940.tmp\VaryingWidthList.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	3075
Entropy (8bit):	7.716021191059687
Encrypted:	false
SSDEEP:	
MD5:	67766FF48AF205B771B53AA2FA82B4F4
SHA1:	0964F8B9DC737E954E16984A585BDC37CE143D84
SHA-256:	160D05B4CB42E1200B859A2DE00770A5C9EBC736B70034AFC832A475372A1667
SHA-512:	AC28B0B4A9178E9B424E5893870913D80F4EE03D595F587AA1D3ACC68194153BAFC29436ADFD6EA8992F0B00D17A43CFB42C529829090AF32C3BE591BD41776D
Malicious:	false

Reputation:	low
Preview:	PK.....nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....nB;O.....k....._rels/.rels...J.@.._e..4...i/.,x..Lw'....v'.<....WpQ.. ,.....7?....u.y..;bL../..3t.+.t.G....Y.v8.eG.MH,....(\..d..R....t>Z.<F-..G.(..\.x...I?..M..:#.....2.#.[..H7..#g{...._j...(.....q.....;.5'..Nt..."...A.h.....>....\.'...L..D..DU<.....C.TKu.5Tu.. ..bV..;PK.....C26.b.....diagrams/layout1.xml.T.n. .}N....).je./m.+u...`{..0P.....p..U}c.9g..3....=h.(.."..D-.&....~.....y..I...(r.aJ.Y..e..;.YH...P.{b.....hz.-..>k.i5..z>.l...f...c..Y. ..7.ND...=.%..1...Y.-.o.=)(1g.{."E.>2.=...]Y..r0.Q...e.E.QKal,.....{f...r..9-.mH..C..\.w....c.4.JUbx.p Q...R.....,...G.F...uPR...\|um.+g..?..C..gT...7.0.8l$.*.=qx.....-8..8.

C:\Users\alfredo\AppData\Local\Temp\TCD4971.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	256
Entropy (8bit):	3.4842773155694724
Encrypted:	false
SSDEEP:	
MD5:	923D406B2170497AD4832F0AD3403168
SHA1:	A77DA08C9CB909206CDE42FE1543B9FE96DF24FB
SHA-256:	EBF9CF474B25DDFE0F6032BA910D5250CBA2F5EDF9CF7E4B3107EDB5C13B50BF
SHA-512:	A4CD8C74A3F916CA6B15862FCA83F17F2B1324973CCBCC8B6D9A8AEE63B83A3CD880DC6821EEADFD882D74C7EF58FA586781DED44E00E8B2ABDD367B47CE 45B7
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .C.o.n.v.e.r.g.i.n.g.T.e.x.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p. l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4971.tmp\ConvergingText.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	11380
Entropy (8bit):	7.891971054886943
Encrypted:	false
SSDEEP:	
MD5:	C9F9364C659E2F0C626AC0D0BB519062
SHA1:	C4036C576074819309D03BB74C188BF902D1AE00
SHA-256:	6FC428CA0DCFC27D351736EF16C94D1AB08DDA50CB047A054F37EC028DD08AA2
SHA-512:	173A5E68E55163B081C5A8DA24AE46428E3FB326EBE17AE9588C7F7D7E5E5810BFCF08C23C3913D6BEC7369E06725F50387612F697AC6A444875C01A2C94D0F
Malicious:	false
Reputation:	low
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....| ...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~CI.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'.. ..z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,.L.3.#e...wZpZ.]S..:....t.....{..6.7.|..,dH.e..K 7-}.~.v...5.....b..PK.....q.~<.6..9 ...e.....diagrams/layout1 .xml..r.....{.]..u...xv7b.....HPd....t.q...b.i_a.'..P.f.3..F..1...U.u.*.2.....?}..O..V.....yQ.Mf.....w.....O....N.....t3;...e....j.^.o&.....w...../.w.....e.....O.../..6...8>^ .^.....ru5...\.=>[M?.....g.....w.N....i.....iy6.?.....>.....>{yT.....x.....-...z5.L./.g....._.l.1.....#...|...pr.q

C:\Users\alfredo\AppData\Local\Temp\TCD4A01.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	254
Entropy (8bit):	3.4845992218379616
Encrypted:	false
SSDEEP:	
MD5:	E8B30D1070779CC14FBE93C8F5CF65BE
SHA1:	9C87F7BC66CF55634AB3F070064AAF8CC977CD05
SHA-256:	2E90434BE1F6DCEA9257D42C331CD9A8D06B848859FD4742A15612B2CA6EFACB
SHA-512:	C0D5363B43D45751192EF06C4EC3C896A161BB11DBFF1FC2E598D28C644824413C78AE3A68027F7E622AF0D709BE0FA893A3A3B4909084DF1ED9A8C1B8267FC A
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .H.e.x.a.g.o.n.R.a.d.i.a.l...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l. a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4A01.tmp\HexagonRadial.glox	
Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	6024
Entropy (8bit):	7.886254023824049
Encrypted:	false
SSDEEP:	
MD5:	20621E61A4C5B0FFEEC98FFB2B3BCD31
SHA1:	4970C22A410DCB26D1BD83B60846EF6BEE1EF7C4
SHA-256:	223EA2602C3E95840232CACC30F63AA5B050FA360543C904F04575253034E6D7
SHA-512:	BDF3A8E3D6EE87D8ADE0767918603B8D238CAE8A2DD0C0F0BF007E89E057C7D1604EB3CCAF0E1BA54419C045FC6380ECBDD070F1BB235C44865F1863A8FA7EEA
Malicious:	false
Reputation:	low
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....|...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~Cl.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'.....z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,.L.3.#e...wZpZ.]S..:.....t.....{..6.7.\|..,dH.e..K 7-}.~.v...5.....b..PK.....2..<..]#.....'.....diagrams/layout1.xml.].r.8...V.;0.;..aO.....{.....V..3].d{.....\. .#.t... .....x<...@7o.]..7.N..@.NF..../....S.../.xC..U...<..Q.=...\|..v.....cQ..Y=.....i`.. ..?.;...Go....x.O.$....7s..0..qg....|..r..l.w.a..p.3.Em7v...N.....3..7...N.\\..f...9...U$..7...k.C..M.@\.s....G/..?...I...t.Yos...p..z...6.Inqi.6..<..1qg+.....#]....|C/N..K\}.....#..".

C:\Users\alfredo\AppData\Local\Temp\TCD4A6F.tmp\Content.inf	
Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.48087342759872
Encrypted:	false
SSDEEP:	
MD5:	69757AF3677EA8D80A2FBE44DEE7B9E4
SHA1:	26AF5881B48F0CB81F194D1D96E3658F8763467C
SHA-256:	0F14CA656CDD95CAB385F9B722580DDE2F46F8622E17A63F4534072D86DF97C3
SHA-512:	BDA862300BAFC407D662872F0BFB5A7F2F72FE1B7341C1439A22A70098FA50C81D450144E7570877783964967777410ADCE4B11B655455BEDC3D128B80CFB472A
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .P.i.c.t.u.r.e.F.r.a.m.e...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4A6F.tmp\PictureFrame.glox	
Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	4326
Entropy (8bit):	7.821066198539098
Encrypted:	false
SSDEEP:	
MD5:	D32E93F7782B21785424AE2BEA62B387
SHA1:	1D5589155C319E28383BC01ED722D4C2A05EF593
SHA-256:	2DC7E71759D84EF8BB23F11981E2C2044626FEA659383E4B9922FE5891F5F478
SHA-512:	5B07D6764A6616A7EF25B81AB4BD4601ECEC1078727BFEAB4A780032AD31B1B26C7A2306E0DBB5B39FC6E03A3FC18AD67C170EA9790E82D8A6CEAB8E7F564447
Malicious:	false
Reputation:	low
Preview:	PK.....n.A...#.....docProps/thumbnail.jpgz.....{4.i....1.n.v)..#.*....A+..Q(."..D.....#Q)...SQ....2c.ei.JC...N.{.....}.s.s..y>....d.(:.;.....q.....$.OBaPbl..(.V...o.....'..b..edE.J.+....."..tq..dqX.....8...CA.@.....0.G.O.$Ph...%i.Q.CQ.>.%!j..F..."?@.1J.Lm$..`..*oO...}..6.....(%....^CO..p.....-,....w8..t.k.#....d..'...O...8....s1....z.r...rr...,(.)...*.]Q]S.{X.SC{GgWw..O....X./FF9._&..L.....[z..^..*....C...qI.f... .Hq....d*.d..9.N{{.N.6..6)..n<...iU]3.._.....%./.?.....(H4<.....}..%..Z..s...C@.d>.v...e.'WGW.....J..:....`....n..6.....]W~/.JX.Qf..^...}...._Sg.-.p..a..C_:..F..E.....k.H.....-Bl$._5...B.w2e...2...c2/y3.U...7.8[.S}H..r/..^...g...|...I..\M..8p$]..poX-/.2}..}z\.|.d<T.....1....2...{P...+Y...T...!.....p..c.....D..o..%.d.f.~.;.;=4.J..]1"("`.....d.0.....L.f0.I..r8..M....m,.p..Y.f....\2.q. ...d9q....P...K..o!..#o...=.....{.p..l.n.....&..o...!J..|)..q4.Z.b..PP....U.K..|.i.$v

C:\Users\alfredo\AppData\Local\Temp\TCD4AFF.tmp\Content.inf	
Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE

File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.4680595384446202
Encrypted:	false
SSDEEP:	
MD5:	D79B5DE6D93AC06005761D88783B3EE6
SHA1:	E05BDCE2673B6AA8CBB17A138751EDFA2264DB91
SHA-256:	96125D6804544B8D4E6AE8638EFD4BD1F96A1BFB9EEF57337FFF40BA9FF4CDD1
SHA-512:	34057F7B2AB273964CB086D8A7DF09A4E05D244A1A27E7589BDC7E5679AB5F587FAB52A2261DB22070DA11EF016F7386635A2B8E54D83730E77A7B142C2E392
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .a.r.c.h.i.t.e.c.t.u.r.e...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4AFF.tmp\architecture.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	5783
Entropy (8bit):	7.88616857639663
Encrypted:	false
SSDEEP:	
MD5:	8109B3C170E6C2C114164B8947F88AA1
SHA1:	FC63956575842219443F4B4C07A8127FBD804C84
SHA-256:	F320B4BB4E57825AA4A40E5A61C1C0189D808B3EACE072B35C77F38745A4C416
SHA-512:	F8A8D7A6469CD3E7C31F3335DDCC349AD7A686730E1866F130EE36AA9994C52A01545CE73D60B642FFE0EE49972435D183D8CD041F2BB006A6CAF31BAF4924C
Malicious:	false
Reputation:	low
Preview:	PK.....A;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.Bl...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL....XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]....v..{.M&.].>`....nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....pnB;.M.:.....g....._rels/.rels...J.0.._%.n....xp..,{.i2M.....G.....7...3o/.....d.kyU....^..[>Q....j.#P.H.....Z>..+!...B*\|@...G...E....E]..".3.....!..7....;.,.....Ot..0r....Z..&1..U..p.U-.[Uq&.....Gyy.}n.(.C(i.x.....?.vM..}..%.7.b.>L..]..PK.....EV:5K..4....H.....diagrams/layout1.xml.Yo.6.....S.`.....$M...Q8A...R..T.k...K.4CQG..}.A..9..?R....!&...Q..ZW.....Q....<8..z..g....4{d.>..;.{.>.X.....Y.2.....cR....9e.. ..}L.....yv&.&...r..h...._..M. e...[..}.>.k.....3.`.ygN...7.w..3..W.S.....w9....r(....Zb..1....z...&WM.D<.....D9...ge.....6+.Y....$f.....wJ$O..N..FC..Er.....?..is...-Z

C:\Users\alfredo\AppData\Local\Temp\TCD4B6E.tmp\CircleProcess.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	16806
Entropy (8bit):	7.9519793977093505
Encrypted:	false
SSDEEP:	
MD5:	950F3AB11CB67CC651082FEBE523AF63
SHA1:	418DE03AD2EF93D0BD29C3D7045E94D3771DACB4
SHA-256:	9C5E4D8966A0B30A22D92DB1DA2F0DBF06AC2EA75E7BB8501777095EA0196974
SHA-512:	D74BF52A58B0C0327DB9DDCAD739794020F00B3FA2DE2B44DAAEC9C1459ECAF3639A5D761BBBC6BDF735848C4FD7E124D13B23964B0055BB5AA4F6AFE76DE00
Malicious:	false
Reputation:	low
Preview:	PK.....T.>.....[Content_Types].xmlz.....=N.1...b.Eko(.B....(.Pp..=.u.?.....#q..ND.!$.J{.o....G..[Cv.....+.R.Nx.....0."u..S...$&.....Je..B..x.....m.....M^z....f....|...N..Q..z.!.- .2.9y.i.8j.....0.AE..p.s~@../jw.#8.I.#....4.~Cl.:#h..f.PU.s.~.....(.)F..Y.....^x..PK.....T.>...V....L....._rels/.rels...J.@.._e..]AD.....x....3.t..T.w.\ZpA<x.....v..'...z.....Y..[...<..2.TT....Q$.!.=.....&C....b".F.q.7...X3...7.8.N.}.. ?..8...#...,.L.3.#e...wZpZ.]S..:.....t.....{..6.7.|..,dH.e..K 7-}.~.v...5.....b..PK.....Ul.<..<"l5...&.....diagrams/layout1.xml.}.r.l..s.....~Y.f.gzfv.....E."w.K..J5m.e...4.0..Q... A.!...%...<...3.....O.....t~.u{...5.G.....?,.....N.....L.....~.:....^,..r=./~7_..8.....o.y.....oo.3.f.....f.....r.7../....qr r.v9.....,?...._O.....?9.O~]..zv.l'.W.....;..\..~...../.....?~..n.....\}pt.....b,~...;>.=;>:..u.....?.....2]..]....i.....9..<.p..4D..

C:\Users\alfredo\AppData\Local\Temp\TCD4B6E.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	254

Entropy (8bit):	3.4720677950594836
Encrypted:	false
SSDEEP:	
MD5:	D04EC08EFE18D1611BDB9A5EC0CC00B1
SHA1:	668FF6DFE64D5306220341FC2C1353199D122932
SHA-256:	FA60500F951AFAF8FFDB6D1828456D60004AE1558E8E1364ADC6ECB59F5450C9
SHA-512:	97EBCCAF64FA33238B7CFC0A6D853EFB050D877E21EE87A78E17698F0BB38382FCE7F6C4D97D550276BD6B133D3099ECAB9CFCD739F31BFE545F4930D896EE C3
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .C.i.r.c.l.e.P.r.o.c.e.s.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l. a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4BCF.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	238
Entropy (8bit):	3.472155835869843
Encrypted:	false
SSDEEP:	
MD5:	2240CF2315F2EB448CEA6E9CE21B5AC5
SHA1:	46332668E2169E86760CBD975FF6FA9DB5274F43
SHA-256:	0F7D0BD5A8CED523CFF4F99D7854C0EE007F5793FA9E1BA1CD933B0894BFBD0D
SHA-512:	10BA73FF861112590BF135F4B337346F9D4ACEB10798E15DC5976671E345BC29AC8527C6052FEC86AA7058E06D1E49052E49D7BCF24A01DB259B5902DB091182
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .r.i.n.g.s...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m. a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4BCF.tmp\rings.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	5151
Entropy (8bit):	7.859615916913808
Encrypted:	false
SSDEEP:	
MD5:	6C24ED9C7C868DB0D55492BB126EAFF8
SHA1:	C6D96D4D298573B70CF5C714151CF87532535888
SHA-256:	48AF17267AD75C142EFA7AB7525CA48FAB579592339FB93E92C4C4DA577D4C9F
SHA-512:	A3E9DC48C04DC8571289F57AE790CA4E6934FBEA4FDDC20CB780F7EA469FE1FC1D480A1DBB04D15301EF061DA5700FF0A793EB67D2811C525FEF618B997BC/ BD
Malicious:	false
Reputation:	low
Preview:	PK.....nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....5nB;.ndX....`....._rels/.rels...J.1.._%..f.J.J..x..AJ.2M&.....g..#..... .....|.c..x{_._..^0e.|.gU..z.....#.._..[..JG.m.....(...e..r."....P)....3..M].E:..SO.;D..c..J..rt...c.,.....a.;....$.../5..D.Ue.g...Q3.....5.':...@...~t{.v..QA>.P.R.A~..^AR.S4G.....].n.. .x41....PK.....^5..s.V....Z.....diagrams/layout1.xml.[]o.F.}N~..S.....VU.U+m6R.....&.d.}...{M....Q.S....p9.'./O..z."..t>q....."[..j>y..?...u....[.}..j-...?Y..Bdy.I./.....0.._.....-.s...rj... I..=..<..9.|>YK.....o.|.my.F.LIB..be/E.Y!.$6r.f/.p%.....U....e..W.R..fK....`+?.rwX.[.b..|..O>o.|.....>1.....trN`7g..Oi.@5..^...]4.r...-y...T.h...[.j1..v....G.....nS..m..E"L...s

C:\Users\alfredo\AppData\Local\Temp\TCD4D00.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	286
Entropy (8bit):	3.4670546921349774
Encrypted:	false
SSDEEP:	
MD5:	3D52060B74D7D448DC733FFE5B92CB52
SHA1:	3FBA3FFC315DB5B70BF6F05C4FF84B52A50FCCBC

SHA-256:	BB980559C6FC38B703D1E9C41720D5CE8D00D2FF86D4F25136DB02B1E54B1518
SHA-512:	952EF139A72562A528C1052F1942DAE1C0509D67654BF5E7C0602C87F90147E8EE9E251D2632BCB5B511AB2FF8A3734293D0A4E3DBD3D187F5E3C042685F9A0
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.h.e.m.e.P.i.c.t.u.r.e.A.l.t.e.r.n.a.t.i.n.g.A.c.c.e.n.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4D00.tmp\ThemePictureAlternatingAccent.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	5630
Entropy (8bit):	7.87271654296772
Encrypted:	false
SSDEEP:	
MD5:	2F8998AA9CF348F1D6DE16EAB2D92070
SHA1:	85B13499937B4A584BEA0BFE60475FD4C73391B6
SHA-256:	8A216D16DEC44E02B9AB9BBADF8A11F97210D8B73277B22562A502550658E580
SHA-512:	F10F7772985EDDA442B9558127F1959FF0A9909C7B7470E62D74948428BFFF7E278739209E8626AE5917FF728AFB8619AE137BEE2A6A4F40662122208A41ABB2
Malicious:	false
Reputation:	low
Preview:	PK.....<..W8...j.....diagrams/layout1.xmlz.....].....Hy..{...n .I.:.D.vvW..s....-a..fg&.}.\..+.....4M..'=...(._.U]U....._.....U...k}.y.,.....C..._^.....w/."7....v..Ea.....Q..u..D{..{v.x.]....AtB15u..o...w..o.1...f.L...l<[zk7..7^..,.h.&l3...#..)..'H..d.r.#w=b...Ocw.y.&.v..t.>.s..m^M7..8I?o7.....H...b....Qv.;'..%.f..#vR....V.H.),g..`...)(..m...[l...b...,.....U...Q.{.y.y.....G.I.tT.n..N.....A.tR..tr....i.<.....,.n:.#.A..a!X.....DK..;v..._M..ISc../n...v.....}.....I.|8.!b.C..v..|.....4l..n.;<9.i./..}!&2.c/.r...>.X02[..|.a.-.....$#-....>...{.M].>3.,\o.x....X%;.F.k.)*".I8<.0..#.....?.h..-..O.2.B.s..v....{Abd...h0....H..I.. ...%...$1.Fyd..Y....U...S.Y.#.V.....TH(....%..nk.3Y.e.m.-.S..Q...j.Ai..E..v.....4.t.|..&"...{..4.!.h.....C.P.....W...d[.....U<Yb;B.+W.!.@B....!.=.....b"...Y.N;.#..Q...0G.IW...]7:...#9!z.....|f..r..x.....t.....`.uL1u.:.....U.D.n.<Q.[%...ngC./..|...!..q;;.w.".D..lt.".I.4".mt...E..mt

C:\Users\alfredo\AppData\Local\Temp\TCD4D6F.tmp\Retrospect.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	1623260
Entropy (8bit):	7.867463315196704
Encrypted:	false
SSDEEP:	
MD5:	126269588DEC71F54D53B563106D0500
SHA1:	E4E27B005A9728617832F0F2645980CC2CE6EC52
SHA-256:	0C11107C6CF799125DB9352E2F3A0D2B9ED5D55CBBEAED66D79464058598D94B
SHA-512:	667F9CA3929926397ED5B43DF4859B8C52973F2603405763308D931C32C4DA831A144ED7041096AFC7CDD291B2978622DED5DD4C16C6BFB0F18235E05B212E5
Malicious:	false
Reputation:	low
Preview:	PK.....Z&A.....a.....[Content_Types].xml...r.`...[a.:%..R.v..p.gh..$d...^../.[0.e..=d....B...c.._?~._>$..}...2.t]...D.ty...I....._....T.M.I.,,..APLo.$,z.,J.wf.<...e>..p.=.G.....eZFiyT...8....E...P}y}..,w;...\]k.....o.....9(.E<.....>..I;....|.Lq.g....]..g.....~>W.<....0/?.I.....g...U.V..3....I.O.....m.I...T.....h.GE.....'K....$...z.E..(.Gc.....N.....>...b....Z...Y.f.13k..:af..Y..13.....8L....o...s.....k...l.k....K.Z..i[..7mk...m._.....~.../.^...{..Z...r@.....P.@.....Z..d....R..e.O..jY.S.,..Z..T-K}....Z-^}.}iyS_C.C}.6.w.`.zNd-K}2...e.O..jY.S.,..Z..T-K }...>U.R_.....}iyS_C.C}C...*....Y.R..uwY.S.,..Z..T-K}...>U.R..e.O..W..o./-o.kha....N.LP..e.O...,..Z..T-K}...>U.R..e.O..jY....w./-o.kha.odC}#...s"kY....K}...>U.R..e.O..jY.S.,..Z..j.x.....M}.-....P....9...,..\[w..>U.R..e.O..jY.S.,..Z..T-K}.Z..N...M}.-...m.o.`.zNd-K}2...e.O..jY.S.,..Z..T-K}...>U.R_.....3..;S0A='...>.k...jY.S.,..Z..T-K}...>U.R..e..V.W.

C:\Users\alfredo\AppData\Local\Temp\TCD4D6F.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	286
Entropy (8bit):	3.51951639572024
Encrypted:	false
SSDEEP:	
MD5:	77DEBFBA0B5B6B234F571A6A97E744F3
SHA1:	51DD22B67F86F9F21E791D7B08810C297DE4756B
SHA-256:	DDEA979C345BDB9F5D33D673CD74C84B2C25A16DE1CAC1D2311FBB52E011C786
SHA-512:	428E2C1D370D783B481EA64E3700942F9F74E4B1693793078C8F51E8644A5A8B39DEEFF79A84E3A2C1EBF6A6A5694C26F86D19542FD3DC334A81FA94386E19A0
Malicious:	false
Reputation:	low

Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .R.e.t.r.o.s.p.e.c.t...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4E00.tmp\Mesh.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	3078052
Entropy (8bit):	7.954129852655753
Encrypted:	false
SSDEEP:	
MD5:	CDF98D6B111CF35576343B962EA5EEC6
SHA1:	D481A70EC9835B82BD6E54316BF27FAD05F13A1C
SHA-256:	E3F108DDB3B8581A7A2290DD1E220957E357A802ECA5B3087C95ED13AD93A734
SHA-512:	95C352869D08C0FE903B15311622003CB4635DE8F3A624C402C869F1715316BE2D8D9C0AB58548A84BBB32757E5A1F244B1014120543581FDEA7D7D9D502EF9C
Malicious:	false
Reputation:	low
Preview:	PK.....1AS'.....ip.....[Content_Types].xml..n.@.._.....8ie'.....}.....(y...H}.....3Fi..%2.v?..3..._...d=..E.g.....7.i.-.t5.6.....}}.m9r.....m...ML.g.M.eV$.r..*.M..l0...A...M..j;.w={o.f..F....i..v.....5..d;..D.ySa...M&..qd*w>.O.{h...|w..5.]..'.CS<.:8C}.g.|E.../..>..].Tnml..I.....r.Gv.E....7.;.E.....4/l.....6.K.C?1qz.O.v_..r.....\c.c.>..lS.....X.N.3N.sN..N.)'.%'..'..N.pL.E...T.!..CR....Ie..k.o..M..w.B.0}..3....v..+....,q..pz.....v{.;....s3.|..V..ZZ.....0.[.....x.....!.!~.8.e..n..&.}p....s.i.. ..[]...q.r....~..+.A\...q.....e.-)h9..."Z.>...5-C..`..g.}.....r.A.+..\...r.>.... .W.\...re?..%.-/hiA..ZR.r.W.D.\}.EK..kZ.>.....5..9.&T.....Wlu.b....}..+.A\...q.....~.WK.Z^.....>.h..`.....}.....^h....L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-}..i..`..G..j..).&T.....Wlu.b....}..+.A\...q.....~.WK.Z^.....>.h..`.....}.....^j..K.L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-}..i.

C:\Users\alfredo\AppData\Local\Temp\TCD4E00.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.5303110391598502
Encrypted:	false
SSDEEP:	
MD5:	8D1E1991838307E4C2197ECB5BA9FA79
SHA1:	4AD8BB98DC9C5060B58899B3E9DCBA6890BC9E93
SHA-256:	4ABA3D10F65D050A19A3C2F57A024DBA342D1E05706A8A3F66B6B8E16A980DB9
SHA-512:	DCDC9DB834303CC3EC8F1C94D950A104C504C588CE7631CE47E24268AABC18B1C23B6BEC3E2675E8A2A11C4D80EBF020324E0C7F985EA3A7BBC77C1101C23D01
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .M.e.s.h...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4E41.tmp\Frame.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	523048
Entropy (8bit):	7.715248170753013
Encrypted:	false
SSDEEP:	
MD5:	C276F590BB846309A5E30ADC35C502AD
SHA1:	CA6D9D6902475F0BE500B12B7204DD1864E7DD02
SHA-256:	782996D93DEBD2AF9B91E7F529767A8CE84ACCC36CD62F24EBB5117228B98F58
SHA-512:	B85165C769DFE037502E125A04CFACDA7F7CC36184B8D0A54C1F9773666FFCC43A1B13373093F97B380871571788D532DEEA352E8D418E12FD7AAD6ADB75A150
Malicious:	false
Reputation:	low
Preview:	PK.....1AE,.{E...#P.....[Content_Types].xml..Mo.0.....Z..N7.=l.....V0.-o..j?...H..sa...../UCb.'...r...w.i..e..<[....{2..U.m..N.{...r.....3.fj.o.....2.*....;.L.6..&,D.Cld8...a.gZf.....r-v..><....~/.....|Zk.....a.R&.d.(.$..6..}.:.....3.....1..[.p.....?..+....R...y,.fod.....e...-.|..#..]j....n:...f...-J...i.^.:Y....T.....m^..~GNp../e}...N....a..5.d.8YcN..5.d.8Y...7..A..e...7Q."3.....sL._....v...n..b..2].v....n.t....Z...Uk...j.&.Z....im|.r....B.....7DaBuN.... ...>..>..>..>..>..>.....V}-.....Q}#.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7FaBuN.... ...>..>..>..>..>..>.....V}-...Q}..&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b....7EaBuN.... ...>..>..>..>..>..>.....V}-...Q}3.&T..j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o.,-k..b.\}..)...A.....[..PK.....1A.s@.....O....._rels/.rels...J.1.._%..d...t.....}...n2!..}6.>..`(.v...K`2...70.....84P....

C:\Users\alfredo\AppData\Local\Temp\TCD4E41.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.5159096381406645
Encrypted:	false
SSDEEP:	
MD5:	71CCB69AF8DD9821F463270FB8CBB285
SHA1:	8FED3EB733A74B2A57D72961F0E4CF8BCA42C851
SHA-256:	8E63D7ABA97DABF9C20D2FAC6EB1665A5D3FDEAB5FA29E4750566424AE6E40B4
SHA-512:	E62FC5BEAEC98C5FDD010FABDAA8D69237D31CA9A1C73F168B1C3ED90B6A9B95E613DEAD50EB8A5B71A7422942F13D6B5A299EB2353542811F2EF9DA7C3A1 5DC
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .F.r.a.m.e...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. . {.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4ED1.tmp\Wood_Type.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	1649585
Entropy (8bit):	7.875240099125746
Encrypted:	false
SSDEEP:	
MD5:	35200E94CEB3BB7A8B34B4E93E039023
SHA1:	5BB55EDAA4CDF9D805E36C36FB092E451BDDB74D
SHA-256:	6CE04E8827ABAEA9B292048C5F84D824DE3CEFDB493101C2DB207BD4475AF1FD
SHA-512:	ED80CEE7C22D10664076BA7558A79485AA39BE80582CEC9A222621764DAE5EFA70F648F8E8C5C83B6FE31C2A9A933C814929782A964A47157505F4AE79A3E2F
Malicious:	false
Reputation:	low
Preview:	PK.....1A..u._....P.....[Content_Types].xml..Ms.@.....!...=.7....;a.h.&Y..l..H~..`;...d..g/..e..,M..C...5...#g/."L..;...#.]..f...w../._.2Y8..X.[..7._.[...K3..#.4.....D.]l.?...~.&J&....p..wr- v.r.?...i.d.:o....Z.a|._....|.d...A....A".0.J.....nz....#.s.m.....(.]........~..XC..J.....+.|...(b}...K!._.D....uN....u..U..b=.^..[...f...f,...eo..z.8.mz.....".D..SU.}ENp.k.e}.O.N....:^....5.d.9Y. N..5.d.q.^s..}R...._E..D...o..o...o...f.6;s.Z]...Uk6d.j..MW....5[C].f#...l;u.M..Z.../iM|...b...S.....0.zN.... ...>..>..>..>..>..>.....e...,..7...F(L.....>.ku...i...i...i...i...i...i.....yi.....G... 1.....j...r.Z]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..i.o|^Z....Q}.;.o...9.Z..\.V.....jZ.....k.pT...0.zN.... ...>..>..>..>..>..>.....e...,..7...f(L.....>.ku...i...i...i...i...i...i...i... .....yi.....n.....{..._f...0...PK.....1A.s@.....O....._rels/.rels...J.1.._%..d...t.....}...n2!..}6.>..`(.v...

C:\Users\alfredo\AppData\Local\Temp\TCD4ED1.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	284
Entropy (8bit):	3.5552837910707304
Encrypted:	false
SSDEEP:	
MD5:	5728F26DF04D174DE9BDFF51D0668E2A
SHA1:	C998DF970655E4AF9C270CC85901A563CFDBCC22
SHA-256:	979DAFD61C23C185830AA3D771EDDC897BEE87587251B84F61776E720ACF9840
SHA-512:	491B36AC6D4749F7448B9A3A6E6465E8D97FB30F33EF5019AF65660E98F4570711EFF5FC31CBB8414AD9355029610E6F93509BC4B2FB6EA79C7CB09069DE7362
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .W.o.o.d._.T.y.p.e...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t. i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD4F6E.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	246

Entropy (8bit):	3.5039994158393686
Encrypted:	false
SSDEEP:	
MD5:	16711B951E1130126E240A6E4CC2E382
SHA1:	8095AA79AEE029FD06428244CA2A6F28408448DB
SHA-256:	855342FE16234F72DA0C2765455B69CF412948CFBE70DE5F6D75A20ACDE29AE9
SHA-512:	454EAA0FD669489583C317699BE1CE5D706C31058B08CF2731A7621FDEFB6609C2F648E02A7A4B2B3A3DFA8406A696D1A6FA5063DDA684BDA4450A2E9FEFB0EF
Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .T.a.b.b.e.d.A.r.c...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD4F6E.tmp\TabbedArc.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	3683
Entropy (8bit):	7.772039166640107
Encrypted:	false
SSDEEP:	
MD5:	E8308DA3D46D0BC30857243E1B7D330D
SHA1:	C7F8E54A63EB254C194A23137F269185E07F9D10
SHA-256:	6534D4D7EF31B967DD0A20AFFF092F8B93D3C0EFCBF19D06833F223A65C6E7C4
SHA-512:	88AB7263B7A8D7DDE1225AE588842E07DF3CE7A07CBD937B7E26DA7DA7CFED23F9C12730D9EF4BC1ACF26506A2A96E07875A1A40C2AD55AD1791371EE674A09B
Malicious:	false
Reputation:	low
Preview:	PK.....a9;lq.ri...#.....diagrams/layout1.xmlz.....WKn.0.];.`..J..AP...4E..!..hi$..I.....z..D.d;...m.d...f.3o.._....9'.P.I1.F.C...d.D:.....Q..Z..5$..BO...e..(.9..2..+.Tsjp.. Vt.f.<...gA.h...8...>..p4..T...9.c...'.G.;.@.;xKE.A.uX.....1Q...>...B...!T.%.* ...0.....&.....(.R.u..BW.yF.Grs...)..$..p^.s.c._..F4.*. .<%.BD..E....x... ..@...v.7f.Y.....N.|.qW'..m.....i m.?.64w..h...UI...J....;.0..[....G..\...?:.7.0.fGK.C.o^....j4.....p...w:...V....cR..i...I...J=...%. &..#..[M....YG...u...I)F.I>.j.....f..6.....2.]..$7.....Fr..o.0...I&..6U...M.....%..47.a.[..s.....[..r....Q./}.-.(.\..#. ..y`...a2..*....UA.$K.nQ:e!bB.H.-Q-a.$La.%.Z!...6L...@...j.5.....b..S.\c..u...R..dXWS.R.8"....o[..V...s0W..8:...U.#5..hK....ge.Q0$>...k.<...YA.g..o5...3... ..~re.....>.....:..$.~.....pu ._Q..|Z...r...E.X.....U....f)s^.?...%.....459..XtL:M.).....x..n9..h...c...PK.....Ho9<"..%.....diagrams/layoutHeader1.xmlMP.N.0.>oOa.

C:\Users\alfredo\AppData\Local\Temp\TCD50CB.tmp\Quotable.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	966946
Entropy (8bit):	7.8785200658952
Encrypted:	false
SSDEEP:	
MD5:	F03AB824395A8F1F1C4F92763E5C5CAD
SHA1:	A6E021918C3CEFFB6490222D37ECEED1FC435D52
SHA-256:	D96F7A63A912CA058FB140138C41DCB3AF16638BA40820016AF78DF5D07FAEDD
SHA-512:	0241146B63C938F11045FB9DF5360F63EF05B9B3DD1272A3E3E329A1BFEC5A4A645D5472461DE9C06CFE4ADB991FE96C58F0357249806C341999C033CD88A7A
Malicious:	false
Reputation:	low
Preview:	PK.....1A.....F`.....[Content_Types].xml..n.@.._.y.ac $..,.....-..g@.u.G.+t.:.....D1...itgt>...k..lz;].8Kg^....N.I.....0.~}....ykk.A`..N..\...2+.e.c..r..P+....I.e.....\|.^/.vc{....s..z....f^...8...'.zcN&.<....}.K.'h..X..y.c.qnn.s%...V('~v.W.....I%nX`.....G.....r.Gz.E..M..".M....6n.a..V.K6.G?Qqz.....\e.K.>..lkM..`...k.5...sb.rbM8..8..9..pb..R..{>$..C .>.....X..iw.'..a.09CPk.n...v....5n..Uk\...SC...j.Y.....Vq..vk>mi.....z..t....v.]...n...e(.....s.i.....]...q.r....~.WV/.j.Y.....K..-.. Z..@.\..P..W...A..X8.`$C.F(.P..H...W..r.>... .W.C..z AV+.....@.\..h....r)...R..-.....c..0F...@Z.....v.+.A\...q.....ZAV'p)...R.D....K..-...h....eP.....(.P..H...W..r.>... .W.C..zAV+.....@.\..h....r)...R..-.....0A...@Z.....v.+.A\...q... ....ZAV'p)...R.D....K..-...h....eP.....w(.P..H...W..r.>... .W.C..zAV+.....@.\..h....r)...R..-.....T..Gl..~.....~....PK.....1A.s@.....O....._rels/.rels...J.

C:\Users\alfredo\AppData\Local\Temp\TCD50CB.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	282
Entropy (8bit):	3.5323495192404475
Encrypted:	false
SSDEEP:	

MD5:	BD6B5A98CA4E6C5DBA57C5AD167EDD00
SHA1:	CCFF7F635B31D12707DC0AC6D1191AB5C4760107
SHA-256:	F22248FE60A55B6C7C1EB31908FAB7726813090DE887316791605714E6E3CEF7
SHA-512:	A178299461015970AF23BA3D10E43FCA5A6FB23262B0DD0C5DDE01D338B4959F222FD2DC2CC5E3815A69FDDCC3B6B4CB8EE6EC0883CE46093C6A59FF2B042C1
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .Q.u.o.t.a.b.l.e...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD5139.tmp\Berlin.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	976001
Entropy (8bit):	7.791956689344336
Encrypted:	false
SSDEEP:	
MD5:	9E563D44C28B9632A7CF4BD046161994
SHA1:	D3DB4E5F5B1CC6DD08BB3EBF488FF05411348A11
SHA-256:	86A70CDBE4377C32729FD6C5A0B5332B7925A91C492292B7F9C636321E6FAD86
SHA-512:	8EB14A1B10CB5C7607D3E07E63F668CFC5FC345B438D39138D62CADF335244952FBC016A311D5CB8A71D50660C49087B909528FC06C1D10AF313F904C06CBD5C
Malicious:	false
Reputation:	low
Preview:	PK.....{MB.f}.....p.....[Content_Types].xml..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~|.?"....|.{.[..e^7E.....Gi..V.by..G..|.....U..t.|..mW...m..|.5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c.v...(=.v.....F_..U..G...T.e.y)[..b.....3.m....6.X5.P....._...b../..}.-.....~.-..z..d.....j.^.+c..E.V..~3}..U.7..~p.>.E..9^d....4%}.E.$....N..r....<....%...%.?....w.u...h.....D...w.....h.....Dkw...x..T....T....T....T....T....j...."[.J.....;..!4...M.....t.n-.{..skp...[;.....F...j.7...4fC...K1..K/..K-..K+..K)..K'..f9.....FI._....d0...?7K7].....A.....FI.....Ft....u.....Ft.....\.....w....R.....R.....R.....o...].`.....A....#.`..\....S.._...4...o.....W<x#.....w#...r.nD..]....\.~....|.....b...^...Z...V...R...N..W<x.....I._...I..?.A.....xp_Q..y<h..tL.i.?HNn...].....r.nD..]~.....wy~7.....Ft.....E/|c.

C:\Users\alfredo\AppData\Local\Temp\TCD5139.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	278
Entropy (8bit):	3.5270134268591966
Encrypted:	false
SSDEEP:	
MD5:	327DA4A5C757C0F1449976BE82653129
SHA1:	CF74ECDF94B4A8FD4C227313C8606FD53B8EEA71
SHA-256:	341BABD413AA5E8F0A921AC309A8C760A4E9BA9CFF3CAD3FB2DD9DF70FD257A6
SHA-512:	9184C3FB989BB271B4B3CDBFEFC47EA8ABEB12B8904EE89797CC9823F33952BD620C061885A5C11BBC1BD3978C4B32EE806418F3F21DA74F1D2DB9817F6E167E
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .B.e.r.l.i.n...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD51F6.tmp\Content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	data
Category:	dropped
Size (bytes):	258
Entropy (8bit):	3.4692172273306268
Encrypted:	false
SSDEEP:	
MD5:	C1B36A0547FB75445957A619201143AC
SHA1:	CDB0A18152F57653F1A707D39F3D7FB504E244A7
SHA-256:	4DFF7D1CEF6DD85CC73E1554D705FA6586A1FBD10E4A73EEE44EAABA2D2FFED9
SHA-512:	0923FB41A6DB96C85B44186E861D34C26595E37F30A6F8E554BD3053B99F237D9AC893D47E8B1E9CF36556E86EFF5BE33C015CBBDD31269CDAA68D6947C47F5F

Malicious:	false
Reputation:	low
Preview:	[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .p.i.c.t.u.r.e.o.r.g.c.h.a.r.t...g.l.o.x.....C.o.m.p.o.n.e.n.t.:. .W.o.r.d.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.\.S.m.a.r.t.A.r.t. .G.r.a.p.h.i.c.s.....

C:\Users\alfredo\AppData\Local\Temp\TCD51F6.tmp\pictureorgchart.glox

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	7370
Entropy (8bit):	7.9204386289679745
Encrypted:	false
SSDEEP:	
MD5:	586CEBC1FAC6962F9E36388E5549FFE9
SHA1:	D1EF3BF2443AE75A78E9FDE8DD02C5B3E46F5F2E
SHA-256:	1595C0C027B12FE4C2B506B907C795D14813BBF64A2F3F6F5D71912D7E57BC40
SHA-512:	68DEAE9C59EA98BD597AE67A17F3029BC7EA2F801AC775CF7DECA292069061EA49C9DF5776CB5160B2C24576249DAF817FA463196A04189873CF16EFC4BEDC62
Malicious:	false
Reputation:	low
Preview:	PK.....;nB;.h.....F.....[Content_Types].xmlz.....MN.0...by.b.,.BI...X `...{..O.S...H\.'.XTP..K{.o.....rg..bL...XM.:.v..c.k...}.D....9.....Bb>.+..G.....+(.u}.w.]...v..{.M&.].>`... .nB..B0Z@.e.u..R.....-.&#....aR..`.a..|. 1^.....&..|..s.A.t..b..A.i7...7.&....bQK$O.....9....V....Wt_PK.....HnB;..I)....j.....\_rels/.rels...J.@.._e..&6E.i/.,x..Lw'.j.....G..\..... .....)...Y.3)..`...9r{v!.....z...#>5.g.WJ%..T..>'m ..K.T.....j6[(:f.)S....C.mk5^.=:...X.....C.... I.....&5..e..H.1...).P.cw.kjT.....C.....=.....}G!7E.y$.(...}b.....b=.<..^.....U..Y..PK..... ....^5a.2u.....diagrams/layout1.xml..ko.8..+x.t.l..J.n.t.Mnw.x. ....B.t$.,.(&i.....(..d.mY.....g.../[.<!.{ap>...L...p....G.9z?...._...e..`..%.....8....G!..B8.....o...b.....Q.>\|.....g..O\B ...i.h...0B.}.....z...k...H..t~r.v.....7o.E....$....Z.....ZDd..~.....>.....O.3.SI.Y.".O&I....#."._c.$.r..z.g0`...0...q:...^0.EF...%(.Ao$.#.o6..c'....$%.}

C:\Users\alfredo\AppData\Local\Temp\TCD5264.tmp\Ion_Boardroom.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	1593982
Entropy (8bit):	7.907400454215888
Encrypted:	false
SSDEEP:	
MD5:	407ACAACDD935B4C82A2D4AF73D07744
SHA1:	E7AB195DF6F9BFD7676C34503E337194DC7631DD
SHA-256:	ED85105C65F81EC015215B76ECBD46BEE4CAAA17AD716393DFD15D5DCD57A3E4
SHA-512:	03D30E2357319A8153D242EEE035DDFDA718CE93E00C0D99ECF82C1387D1FE1A436111E13AD1CE67214C87CF4709D68FF452C041772A43CB242786ED4090370
Malicious:	false
Reputation:	low
Preview:	PK.....AS'.....ip.....[Content_Types].xml..n.@.._.....8ie'.....}.....(y...H}.....3Fi..%2.v?..3..._...d=..E.g.....7.i.-.t5.6.....}}.m9r.....m...ML.g.M.eV$.r..*.M..l0...A...M..j;.w={o.f.. F....i..v.....5..d;..D.ySa...M&..qd*w>.O.{h...|w..5.]..'.CS<.:8C}.g.|E.../..>..].Tnml..I.....r.Gv.E....7.;.E.....4/l.....6.K.C?1qz.O.v_..r.....\c.c.>..lS.....X.N.3N.sN..N.)'.%'..'..N .pL.E...T.!..CR....Ie..k.o..M..w.B.0}..3....v..+.....,q..pz.....v{.;....s3.|..V..ZZ.....0.[.....x.....!.!~.8.e..n..&.}p....s.i.. ..[]...q.r....~..+.A\...q.....e.-)h9..."Z.>...5-C..`..g.}.....r.A.+. .\...r.>.... .W.\....re?..%.-/hiA..ZR.r.W.D.\}.EK..kZ.>.....5..9.&T.....Wlu.b....}..+.A\...q.....~.WK.Z^.....>.h..`.....}.....^h....L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-} ..i..`..G..j..).&T.....Wlu.b....}..+.A\...q.....~.WK.Z^.....>.h..`.....}.....^j..K.L...H...!...r.>... .W...\...rE?.....-+hIA..\}..r...-}..i.

C:\Users\alfredo\AppData\Local\Temp\TCD5264.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	292
Entropy (8bit):	3.549050193282821
Encrypted:	false
SSDEEP:	
MD5:	D7052608155B2599CDB50B8F9AAD7BD2
SHA1:	F7213641CDC854DD1E7812BCCF9BD918188149F1
SHA-256:	577A765CD1FBE2B62887AD32EE0CF7DCD6FCF166772AFB5895F5E11C0C1386AB
SHA-512:	173AA81483025EE6A2FA042C8B281226D27E0AB4CF7E61A09FDA3897445CE90D300C9E2173AE10BC051F60CD3576B343F963FB482DC7C6529488AE8E82A5A10
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .l.o.n._.B.o.a.r.d.r.o.o.m...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L. o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD52C3.tmp\Depth.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	2332136
Entropy (8bit):	7.9547975506532795
Encrypted:	false
SSDEEP:	
MD5:	2AECC99B664F840799028A20703C3E21
SHA1:	0018EAB0CE4900220607F4F80B506AA2F7F89C17
SHA-256:	DF93F14304E35E460EEC7F8464AE2C2B0BFFA84D860D4857F41E0F07A3F023E3
SHA-512:	E0BD3A86C7AF6B7202E8FBA42BCA27FBB17A21AC94A685A38C8A45F5AE35F350AE18D6B107F553DC95774FAE47F8BD8926F76DDD840BB7EB8E51E5CF2269A A1C
Malicious:	false
Reputation:	low
Preview:	PK.....fdlB.f}.....p.....[Content_Types].xml..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~\|.?"....\|.{.[..e^7E.....Gi..V.by..G..\|.....U..t.\|..mW...m..\|. 5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c.v...(=.v.....F_..U..G...T.e.y)[..b.....3.m....6.X5.P....._...b../..}.-.....`~.-..z..d.....j.^.+c..E.V..~3}..U.7..~p.>.E..9^d....4%}.E.$....N..r.... <....%...%.?....w.u...h.....D...w.....h.....Dkw...x..T....T....T....T....T....j...."[.J.....;..!4...M.....t.n-.{..skp...[;.....F...j.7...4fC...K1..K/..K-..K+..K)..K'..f9.....Fl._.... .....d0...?7K7].....A.....Fl.....Ft....u.....Ft.....\.....w....R.....R.....R.....o...].`.....A....#.`..\.....S._...4...o.....W<x#.....w#...r.nD..]....\.~....|.....b...^...Z...V. ..R...N..W<x.....I._...I..?.A.....xp_Q..y<h..tL.i.?HNn...]..........r.nD..]~.....wy~7.....Ft.....E/|c.

C:\Users\alfredo\AppData\Local\Temp\TCD52C3.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.5344681868414707
Encrypted:	false
SSDEEP:	
MD5:	C601540411B7C0E6DE93621C69A0B71D
SHA1:	B1F855540B73B163B6FD15B227C0B1D0EDC51AA9
SHA-256:	6690E31622155199015B15E94B39C52BEBD081611F4AE0A9E3299CC56AF8EE33
SHA-512:	90B14C2D325A091CA3A8CAAE2B4888F79BE0CD9C7E73E3B27A73F5043BB26491ABEEBEC9E25BB27F0E11B7E8F3E5E706F7D0623759301C4FAF0BCA7BCA8F6 6E2
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .D.e.p.t.h...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. . {.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD5360.tmp\View.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	486596
Entropy (8bit):	7.668294441507828
Encrypted:	false
SSDEEP:	
MD5:	0E37AECABDB3FDF8AAFEDB9C6D693D2F
SHA1:	F29254D2476DF70979F723DE38A4BF41C341AC78
SHA-256:	7AC7629142C2508B070F09788217114A70DE14ACDB9EA30CBAB0246F45082349
SHA-512:	DE6AFE015C1D41737D50ADD857300996F6E929FED49CB71BC59BB091F9DAB76574C56DEA0488B0869FE61E563B07EBB7330C8745BC1DF6305594AC9BDEA4A6 BF
Malicious:	false
Reputation:	low
Preview:	PK.....V'BE,.{....#P.....[Content_Types].xml..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..!....?~\|.?"....\|.{.[..e^7E.....Gi..V.by..G..\|.....U..t.\|..mW...m..\|. 5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c...W..G.4D_.}T,.@...}....R.Z..4k.....Y..mEkLor.f^..O..P...`.../.\|u1..Y.....nK.....u=..2.tu~^L.Y5]/...~+.v...o....j.`?.S...../.by.\|..>."kZbs... .H.9..m.z.]W.V.?~v.....;...N.....w....;.z..N.....w.....R.~n..Ofu.-..K.e....{..A.~.8.#D..)o.7.....:2.....=.....f...u....[..}...u.6b...xz.[...G..\|#...$....)J./.....7.....oQ..]^.M..... wy}7a.....&l.....w.....l._...l..?.A.....r..9.|.8.....{w.....n...]^.M.....wy}7a.....&l.....`..z..`.....2.o...wx}.....>..c.M..Arr#.....nD..[.....w.....n...]^.M.....wy}7a.....& l.....w..... ..Fp....w_Q....g..tL.i.?H.o...]^.....n...]^.M.....wy}7a.....&l.....`..z..`

C:\Users\alfredo\AppData\Local\Temp\TCD5360.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	274
Entropy (8bit):	3.535303979138867
Encrypted:	false
SSDEEP:	
MD5:	35AFE8D8724F3E19EB08274906926A0B
SHA1:	435B528AAF746428A01F375226C5A6A04099DF75
SHA-256:	97B8B2E246E4DAB15E494D2FB5F8BE3E6361A76C8B406C77902CE4DFF7AC1A35
SHA-512:	ACF4F124207974CFC46A6F4EA028A38D11B5AF40E55809E5B0F6F5DABA7F6FC994D286026FAC19A0B4E2311D5E9B16B8154F8566ED786E5EF7CDBA8128FD62AF
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .V.i.e.w...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD548A.tmp\Savon.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	1204049
Entropy (8bit):	7.92476783994848
Encrypted:	false
SSDEEP:	
MD5:	FD5BBC58056522847B3B75750603DF0C
SHA1:	97313E85C0937739AF7C7FC084A10BF202AC9942
SHA-256:	44976408BD6D2703BDBE177259061A502552193B1CD05E09B698C0DAC3653C5F
SHA-512:	DBD72827044331215A7221CA9B0ECB8809C7C79825B9A2275F3450BAE016D7D320B4CA94095F7CEF4372AC63155C78CA4795E23F93166D4720032ECF9F932B8E
Malicious:	false
Reputation:	low
Preview:	PK.....1A..d T....P.....[Content_Types].xml..Ms.@.....!...=.7....kX 5o.,L..<.....d..g/..dw.]...C...9...#g/."L..;...#.]..f...w../._.3Y8..X.[..7._.[...K3..3.4.....D.]l.?...~.&J&.. .s...;...H9...e.3.q.....k-.0>Lp:.7..eT...Y...P...OVg.....G..).aV...\Z.x...W.>f...oq.8.....I?Ky...g..."...J?....A$zL.].7.M.^..\....C..d/;.J0.7k.X4.e..?N{....r.."LZx.H?. .....;r.+...A<.;U.... .4...!'k...s.&..)'k...d..d....._E..D...o..o...o...f.7;s..]...Uk6d.j..MW....5[C].f#...l;u.M..Z.../iM|...b...s.....0..O.... ...>..>..>..>..>..>.>.....2V}.....Q}#.&T...rU....\..\..\..\..\..\..\..\.W..W.^Z....Q}c;.o...>.Z..\.v.....*Z....K.X.5X8.obG.MP.P.'P.U}.k..rU..rU..rU..rU..rU..rU..rU..rU_EK_}.zi.....G.M.).....j...r..]..CZ..CZ..CZ..CZ..CZ..CZ..CZ..h.oZ/-c..`....7CaBu.@-W.A.]..U}H.U}H.U}H.U}H.U}H.U}H.U}H.U}.-}...e...,...|...].k.....PK.....1A.s@.....O....._rels/.rels...J.1.._%..d...t....}...n2!..}6.>..`(.v...K`2...70...

C:\Users\alfredo\AppData\Local\Temp\TCD548A.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	276
Entropy (8bit):	3.5364757859412563
Encrypted:	false
SSDEEP:	
MD5:	CD465E8DA15E26569897213CA9F6BC9C
SHA1:	9EA9B5E6C9B7BF72A777A21EC17FD82BC4386D4C
SHA-256:	D4109317C2DBA1D7A94FC1A4B23FA51F4D0FC8E1D9433697AAFA72E335192610
SHA-512:	869A42679F96414FE01FE1D79AF7B33A0C9B598B393E57E0E4D94D68A4F2107EC58B63A532702DA96A1F2F20CE72E6E08125B38745CD960DF62FE539646EDD8
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .S.a.v.o.n...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD5556.tmp\Metropolitan.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	777647
Entropy (8bit):	7.689662652914981
Encrypted:	false

SSDEEP:	
MD5:	B30D2EF0FC261AECE90B62E9C5597379
SHA1:	4893C5B9BE04ECBB19EE45FFCE33CA56C7894FE3
SHA-256:	BB170D6DE4EE8466F56C93DC26E47EE8A229B9C4842EA8DD0D9CCC71BC8E2976
SHA-512:	2E728408C20C3C23C84A1C22DB28F0943AAA960B4436F8C77570448D5BEA9B8D53D95F7562883FA4F9B282DFE2FD07251EEEFDE5481E49F99B8FEDB66AAAAB68
Malicious:	false
Reputation:	low
Preview:	PK.....V'B.._<....-.....[Content_Types].xml..`.I.%&/m.{.J.J..t...`.$.@.....iG#).*..eVe]f.@....{...{...;.N'...?\fd.l..J..l....?~\|.?"....\|.{.[..e^7E.....Gi..V.by..G..\|.....U..t.\|..mW...m..\|.5.j./..^d-.Y_.]e..E~wog...j...v.....?..u....c...W..G.4D_.}T,.@...}....R.Z..4k.....Y..mEkLor.f^..O..P...`.../.\|u1..Y.....nK.....u=..2.tu~^L.Y5]/...~+.v...o....j.`?.S...../.by.\|..>."kZbs....H.9..m.z.]W.V.?~v.....;...N.....w....;.z..N.....w.....R.~n..Ofu.-..K.e....{..A.~.8.#D..)o.7.....:2.....=.....f...u....[..}...u.6b...xz.[...G..\|#...$....)J./.....7.....oQ..]^.M.....wy}7a.....&l.....w.....l._...l..?.A.....r..9.|.8.....{w.....n...]^.M.....wy}7a.....&l.....`..z..`.....2.o...wx}.....>..c.M..Arr#.....nD..[.....w.....n...]^.M.....wy}7a.....&l.....w..... ..Fp....w_Q....g..tL.i.?H.o...]^.....n...]^.M.....wy}7a.....&l.....`..z..`

C:\Users\alfredo\AppData\Local\Temp\TCD5556.tmp\content.inf

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	290
Entropy (8bit):	3.5091498509646044
Encrypted:	false
SSDEEP:	
MD5:	23D59577F4AE6C6D1527A1B8CDB9AB19
SHA1:	A345D683E54D04CC0105C4BFFCEF8C6617A0093D
SHA-256:	9ADD2C3912E01C2AC7FAD6737901E4EECBCCE6EC60F8E4D78585469A440E1E2C
SHA-512:	B85027276B888548ECB8A2FC1DB1574C26FF3FCA7AF1F29CD5074EC3642F9EC62650E7D47462837607E11DCAE879B1F83DF4762CA94667AE70CBF78F8D45534
Malicious:	false
Reputation:	low
Preview:	..[.F.i.l.e.].....O.r.i.g.i.n.a.l.N.a.m.e.:. .M.e.t.r.o.p.o.l.i.t.a.n...t.h.m.x.....C.o.m.p.o.n.e.n.t.:. .P.P.T.F.i.l.e.s.....R.e.q.V.e.r.:. .1.4.....E.x.e.c.u.t.a.b.l.e.:. .{.P.P.}.....S.t.o.r.e.L.o.c.a.t.i.o.n.:. .{.M.y. .T.e.m.p.l.a.t.e.s.}.....C.o.m.m.a.n.d.:. .{.F.i.l.e.P.a.t.h.}.....

C:\Users\alfredo\AppData\Local\Temp\TCD55B5.tmp\Facet.thmx

Process:	C:\Program Files\Microsoft Office\root\Office16\POWERPNT.EXE
File Type:	Microsoft OOXML
Category:	dropped
Size (bytes):	738429
Entropy (8bit):	7.8235726750504355
Encrypted:	false
SSDEEP:	
MD5:	8EBD58005DAF9C4EC15AC2530D3A4A30
SHA1:	D11B9F2B85F20EB3DB28C4D9C9FDD909848E3E05
SHA-256:	D3AB94FDC32B10903AD444F6F3518F93C3D7348FB945168DD8140C74BB7D7E26
SHA-512:	00A3A6F8A8D10F4BAD87C3BEAE299D0E28931593EF0FB4145711B1D164A3351A8EF131DA0F26AAB9C3EB7AC214B69E1F03CB52E0E1EA95EB444664D5B0B998E9
Malicious:	false
Reputation:	low
Preview:	PK.....e.$A}.4+.....k.....[Content_Types].xml..n.@.E_.y.ac $..,.....-..g@.u.G.+t.:.....A1.....=..._..d.....Y:.B...t.e.8]..].....s.M.=.....6...&Z.D.?.u..,."Q.].. W.....p0..Q.Z.....Rm7....}\.{.W^.....Z3/N...o.....1'.T.o.HYw?....._,.<<c.qnn...8.:.B9.."^...U.O*q.....>..-]..O...-.q..Y.M...:.M+...}..y..{.0..V'K6.K?Qqz.....c^..~GN.*s_..Q=g[k.....8..XCN..'....k.u.u....+..r...!.A....!.Q....a...7U.*uH...!gi=..Y.[.v{&.....q.=.[.v{....k.5.....4Y9..3Y).....v..mi...Wi.~.=G.....t.?.S.....bB..H.%X.W..r.>.... .W.\...rU?.++i..&+g.b&+e\..h....r.V..^.JZ..j`.....bB..H.%X.W..r.>.... .W.\...rU?.++i..&+g.b&+e\..h....r.V..^.JZ..j`.....bB..H.%X.W..r.>.... .W.\...rU?.++i..&+g.b&+e\..h....r.V..^.JZ..j`...[..u...UN -.`A\a..U. .W.\...r5?..U.....q.....,D.%X5Zz.*i.....C.&2.k...UN -.`A\a..U. .W.\...r5?..U.....q.....,D.%X5Zz.*i.....C..d...*&T9..\..q...W.\...r.?.... .W.C...&+h.r&+f.R.%X..K..-.`.h....e.....zu9JR..7..Y=..6.?PK..

Static File Info

General

File type:	Microsoft PowerPoint 2007+
Entropy (8bit):	7.997266324981801
TrID:	• PowerPoint Microsoft Office Open XML Format document (133004/1) 76.66% • Microsoft PowerPoint Macro-enabled Open XML add-in (32504/1) 18.73% • ZIP compressed archive (8000/1) 4.61%

File name:	New Years Quiz.pptx
File size:	3698551
MD5:	aaef4b88a0786189d40ef96e7c6c7dfc
SHA1:	97191fc7bb61c677785d316cd8bb4a7c36f34fa4
SHA256:	84108e3fdd2d9270764c51ae9e8012448173cfd82e95e6aa22365d3cf1fe97a1
SHA512:	a361727e0f5e2e878c2564cf9c70c2a6d79c6cef86d966863f9f4f65126a9129c57ff41f8738aa033503758efa450519da5eb6f257f464ae7a2aa64100d3d761
SSDEEP:	98304:dtoIOTcFkbsoi9QhaYuU7myfTRfr6yqj5:sLcssoFB7mEs
TLSH:	DC0633F49DD8AD5EE61B113E4CE7C7E8D9E02CB7D5810A292AF85518FF2EB12324C194
File Content Preview:	PK.....!.....ppt/presentation.xml...n.0...'....N48. BU.e..I....&.Du..6.:..w..0D.....9.....v_SgG..8.\t3v...^V.5s...Q.:RaVb.....Y3m...).`..n..... (.L=O..Rcy...@[sQc.].....z.x.{5..... .....u".5y.M.....3..Y\.$..../...3%..;.

File Icon

Icon Hash:	74f4c4ccc6c6c0d4