ID: 433255
Sample Name: INDIV_PAYM_633854-506518488.xlsb
Cookbook: defaultwindowsofficecookbook.jbs
Time: 14:49:02
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

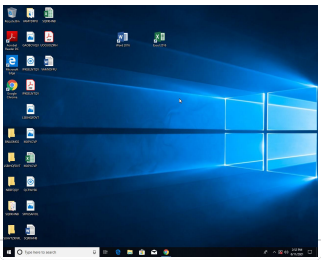
Analysis Report INDIV_PAYM_633854-506518488.xlsb

Overview

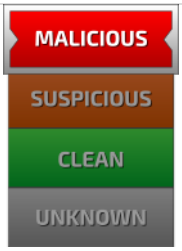
General Information

Sample Name:	INDIV_PAYM_633854-506518488.xlsb
Analysis ID:	433255
MD5:	38cab943e9882c..
SHA1:	fe99ceae30df219..
SHA256:	17c5220167efeb1.
Infos:	

Most interesting Screenshot:



Detection



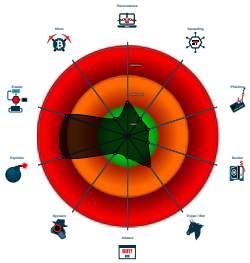
Hidden Macro 4.0

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

Signatures

- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Sigma detected: Microsoft Office Pr…
- Potential document exploit detected…
- Registers a DLL
- Tries to connect to HTTP servers, b…
- Tries to load missing DLLs
- Yara detected Xls With Macro 4.0

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6796 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6416 cmdline: regsvr32 -s ..\jbeiwmje.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

System Summary:

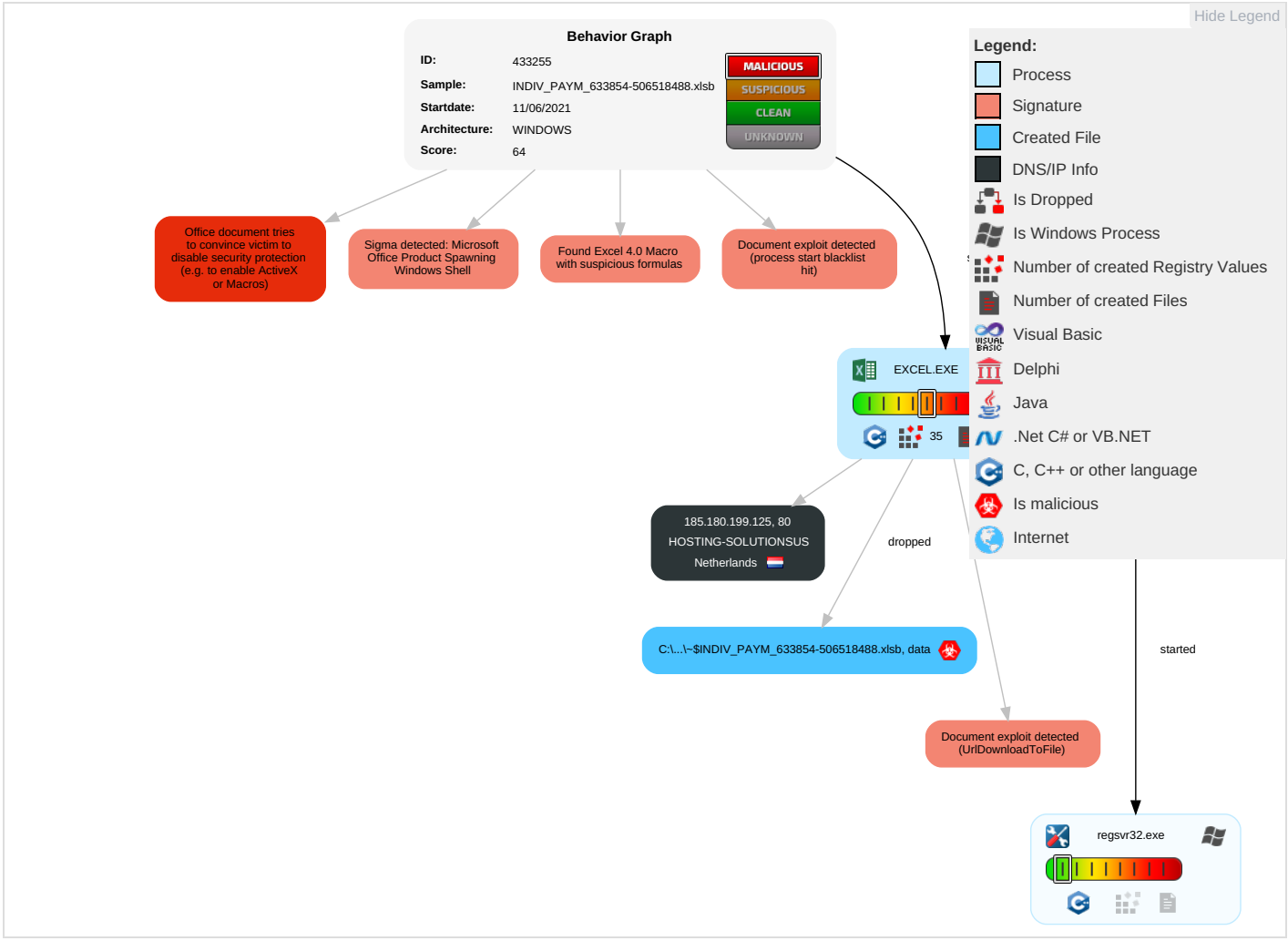
Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

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
Valid Accounts	Scripting 1	DLL Side-Loading 1	Process Injection 1	Regsvr32 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Exploitation for Client Execution 2 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

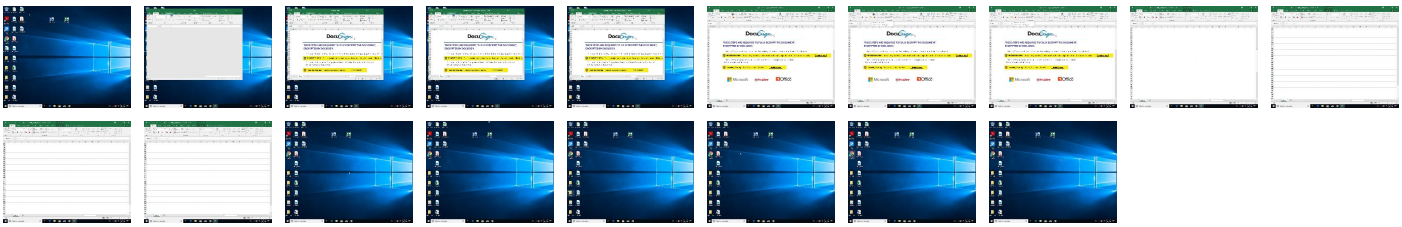
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Virustotal		Browse
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Virustotal		Browse
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Virustotal		Browse
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://api.cortana.ai	0%	URL Reputation	safe	
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Virustotal		Browse
http://https://ovisualuiapp.azurewebsites.net/pbiagave/	0%	Avira URL Cloud	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	
http://https://directory.services.	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.180.199.125	unknown	Netherlands		14576	HOSTING-SOLUTIONSUS	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433255
Start date:	11.06.2021
Start time:	14:49:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	INDIV_PAYM_633854-506518488.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal64.expl.evad.winXLSB@3/9@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.180.199.125	transfer_summ_188108012.xlsb	Get hash	malicious	Browse	
	pmnt_spec_031624191.xlsb	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTING-SOLUTIONSUS	transfer_summ_188108012.xlsb	Get hash	malicious	Browse	• 185.180.199.125
	pmnt_spec_031624191.xlsb	Get hash	malicious	Browse	• 185.180.199.125
	PO187439.exe	Get hash	malicious	Browse	• 185.162.128.35
	Order_Summary-9632850.xlsb	Get hash	malicious	Browse	• 185.180.199.121

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Total_order_data-V2434883.xlsb	Get hash	malicious	Browse	• 185.180.19 9.121
	Delivery_Information_7038598.xlsb	Get hash	malicious	Browse	• 185.180.19 9.121
	W6DkFm55kO.exe	Get hash	malicious	Browse	• 162.248.225.14
	Lma2EzVvAK.exe	Get hash	malicious	Browse	• 185.180.19 8.250
	wEcncyxrEe	Get hash	malicious	Browse	• 104.193.25 2.114
	immed_paym_req_44191988.doc	Get hash	malicious	Browse	• 185.159.82.194
	zKOi8vCorq.exe	Get hash	malicious	Browse	• 185.180.198.99
	invoice_100221.doc	Get hash	malicious	Browse	• 185.180.19 8.135
	new shippment.xlsx	Get hash	malicious	Browse	• 185.180.19 8.135
	w3QgrgNAWs.exe	Get hash	malicious	Browse	• 185.180.198.99
	yWWZnMPf9D.exe	Get hash	malicious	Browse	• 185.180.198.99
	zLjBdL6Lbk.exe	Get hash	malicious	Browse	• 185.180.19 8.141
	DHL_file094883764773845.exe	Get hash	malicious	Browse	• 162.244.32.175
	http://https://bit.ly/3547mtO	Get hash	malicious	Browse	• 162.244.32.223
	http://436095.com/cwuobmjj/lnclqsrq.html?5crjx3rlwse.eps2k	Get hash	malicious	Browse	• 162.244.32.223
	http://https://bit.ly/2H1vYuP	Get hash	malicious	Browse	• 162.244.32.223

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4B1D4E11-6555-417E-8757-1FD44D44B005	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134922
Entropy (8bit):	5.369089751778702
Encrypted:	false
SSDEEP:	1536:ncQIKNEeBXA3gBwlpQ9DQW+z7534ZliKWXboOilX5ENLWME9:TEQ9DQW+ziXOe
MD5:	C1EDAF86F426B84FAC2104ED061EA944
SHA1:	24D1CD0E890F2A4BA6930F470F50D04CE7E15920
SHA-256:	00B9E5E95119D8B5E2EB2351D7FD6492078B14A17DE6F3C0639F5D96BEF7BC99
SHA-512:	4231020218B88253F8D7D38158755539DE3E972B4163577E355EEFE6C6ADE63749613B6CDC53EEE0E2E97E81D123CEEB5366CC0F5608E2388196AE58F8111D3E
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-11T12:50:01">.. Build: 16.0.14209.30527-->.. <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:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\561637EF.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 168 x 72, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	6177
Entropy (8bit):	7.959095006853368
Encrypted:	false
SSDEEP:	96:j6KDvZ3QXkQ288GMDBm6hEeWyS8ITRIVg9gPEnbYhbY0Y4pxCpAueydMT1uZMr0a:j6KTV8WBPhqd9qqYTB6peyeT1oMr0a
MD5:	C7ED6FC355D8632DB1464BE3D56BF5CC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\561637EF.png	
SHA1:	615484A338922DDF00B903CFA48060AD60D70207
SHA-256:	26000244FBB0C6B2D76F80166CE85700BC96141C6CD80F8B399CA6F15FE3515C
SHA-512:	FB4AE09EACD15A4FE778BDF366808C4F9FE403C4054F86704C03C87C7016E7D7A5772677B69064FCB5F1B9345D80C4263A58EA8B5E9CA2B717E24E2B19B85A9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....H.....m)a....sRGB.....pHYs.....+.....IDATx^....E...1.Y. ..."3.(.D.....A..(....(.C.X.QP..b.UQAdA..9'I:Hf..f.....s....._.A..s.3...Vu.....Z.[.q.P.-9.b..q.....|.r F .....c..1.....e.->....@..;n.q..(.bt.q...>F9...[|\.1..]v..A..G..y._3...*3M.YG7.J.)..RK]u.j}.*^J.....R...j.:=}..qN .sV&..F.a.@..Vs.P...%.A.....~..w..P.Be.-].4..arss.9~.8d.@.d....''..?.G. ...z.....(.T.....G.;w.?....w....S.H.+...W.^.....E..-_.\....D-....#G.{..<r....P.K..$.{D....kzzz.R....`?..O;.....#....tb..g..gU.r>G.....:t.....a.....p..c..]..... M.6.'O.]..... 8 q...RSS.YBB.M.j..}..I.&.:%J.x..7o....d.*U..233.].....E.m}..../^..nt..X.b,..{<....=.....3....z....v..]0.e.}...?.....w..y...)S.L.F.:t..U...+F...l.....&...322.6m.../.[.J.a.=..%Kx....E...ys.....z...i.z ..g...G...e.7.|.h....!C^x.5k".....<.R..k....4iR.V-._.~....:..P.O@.y.:..:G=.\...J ...u...]%.T.n.....v..A`Y.....V...^{.X^.I`1w.q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\6496A6D2.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	956
Entropy (8bit):	7.683552542542939
Encrypted:	false
SSDEEP:	24:64ZJH5wka2YQydYiFNcincNrtNmt5xx4tRFB:JJH5fYuW5c3wPoFB
MD5:	32C83607A5C98C5A634278E5AED3AD61
SHA1:	EDE34ADEA53C413C4AC8215EA48F2F2FD59F1362
SHA-256:	4A999E919D85EDD0CD1A772CA3B29F91AEECF77D0BEB11FD1B632B7A8A0686BF
SHA-512:	AF19A013377F0F7B47E54D99D0AFA222BE46072C47944E8640B09A4993DFDDC906B7C68F7E3DAB5B3F126C9AD1090EADBF17FF7068EE8E360D0EA46811C0DB C
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d...QIDATHK.VMHTQ..2.h.X."h....A....]B...m.(h..b?.$...f.)..ta...jS..!..h.ETD.!."."C..y.....=.>8...{.s..32.0F v.F...kz..&.|_.....9.)m."......m..$9.j...E.@.:D.-..0...L.hk..(....s.'.k.A-.-.....(.....jR[m..d..O.-?:.c..70.{..sw'X.j.^j+..d....N.. .r.....Z.[[[..c...r.../.M`l.]&#.aR..[{...<O....<d...3....F...:..s9..- ...x..R...q..ON.KO;..0..^.....9.S.}..x...22.....r..f....'.....+o...A..7.....q..l...S.....s/.{.^..Pj1`.b.!t..>o..!.C.e.}....Y.....t.....r.MDq=.=..._....c..3%p...j...hl1.[.^.#..."#...e...6..l-j;.9j;o/ ...Q2...w-.?.<..r../?...0.`.;.lz.M...\. ..}x...\h^.....r..';... ...<..j..E._.E..u..g....7.X....T....7.....(&.[..... T....;V1w..,EU.W".../.....m%.u'x/.u]*....@.-.L..G.....Q.''..%fb.Z*.,...K.%BX.. ..]`J=.h".Vef...2..8.g.jX.2s..vY.u|.4p.\.h...W....(.r.....^Y....2$8F...>`p._.c..}.txq#.$.`:@...Y..?.j.IK.Fu....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\862636D5.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 178 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	5744
Entropy (8bit):	7.966496386988271
Encrypted:	false
SSDEEP:	96:4uJgumnoYk22FLjJq17cpKsv+CHI5BXjI1e+HCLDl3kjH1erj+uYU2:4CgJfkfJA7ixCxqe+GDhkT1erj+uYf
MD5:	9AD30E24270C495AE68EAF3A1EEECBFB
SHA1:	8642D256E7FFBEF5804A2D2220A1FE475A99DC36
SHA-256:	6D3EAD431ABD110369EFABC6F2E474DC24FA3D7EEC28DE43456407C5BACD6D20
SHA-512:	EB156DD0686BAAE4F46B0B0C01838DA7225529D3B31912568D36A1CC07BE006EEAD31F464B0252C3A8471ACA71E86EEE9185FE705ABAE08C56B15C63CC891A D5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....L.....FpzV....sRGB.....pHYs.....+.....IDATx^.\.tTU..u...@@. .b..su....''....+k..Aeu..rX.*.feE..(M.....b..BB.P.f&S_.~w&.I.aH...'...0.....u.2.!...`....8_ ..,.T.#.....,X...N....NN-l.....5`...Z,,..-L..k.":9..Y.,Z..c.Etrja..X.0.G.....f..ha...]..... 2`.....,..S..e...)<:v.XD'..6.E.Sxt....NN-l.....5`...Z,,..-L..k.":9..Yt.....9.{.f;...f../Mh...B..GK.....FG.. ...s...MN.vqp"+.|.m[&11..<O....?...EQ4.H...Z'M... #.T.....vS..^..p..)..... 1...JJr?.gq.V..X..h..T._Zr2g..W^...A./.W...P....q.By.49..5M--.e...5}..{.!.s4M./Xx2.....`...I>s..4U...]... (5.8o>.X.[..xS.w)../.c.Lh..a..uQ.fd.....jh.Z.d..(..=.....#.....o.y....g...-....=?..X.f./..=n\`.j..k.....{.4...b..T.-h..F..;u.x....[!.\....*'Nx^....C..b...8.....|F.$.4.....&?.>#.d.\p.R..k..>t0?.-3g.. b.....s.O..E...4o...\O=.7O=z...u1$n..6..C.]A.X...Z.tX.....I..W.....P...h.@..+q..F.kcI..x\>.....0.4..p....}.~e...).w....%Q.$W.....8.....PY.k..J....T..b.I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AFC11124.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 264 x 113, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	9924
Entropy (8bit):	7.973758306371751
Encrypted:	false
SSDEEP:	192:soXrzGktAQUkDfw4om9PEK9u27pwnJyV028/tgXEoCWoB:so9G+fnVEYu27OIW/+XEoCWoB
MD5:	B34FB4F2F0F9E70B72BA3AFD028CD97C
SHA1:	C6868336F78DEA1E718965DF3341039581DB5B5A
SHA-256:	189D420D344A694FD1928ABACBEC94D9F0EF52BE036CEB8144A9D9A6DD14EAEB
SHA-512:	4795600917F8A67A6C5CBD5713CAACE74E0483F8E6BB6D98EAB63BF24A0F71E537E7F8ABD26808630B247D454A3F467595C8343EEB4EA98AFAB49D81964158D
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\AFC11124.png	
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....q.....sRGB.....pHYs.....+....&ilDATx^.Wp.G~.{"r.. H.9s.,Q.v.....\..../wu..t.o..ru...+W]....vWa).Q.b&.@d.D.q....{0....GB....8.....X,&L1.0..... .....b...0Xa ....a..0.0.ap.@.....'.*. `.#.6.,....aX..i.b.0..b.n.k...0...J1...H..7...C...dZ....a....Z..!.kp2.R...0Rl..r.A...58.V)..C.)..f.. `....L....!...p.\k.0.a.N.U.A..F.m.Y.5....'.*. `.#.6.,....aX. .i.b.0..b.n.k...0...J1...H..7...C...dZ....a....Z..!.kp2.R...0Rl..r.A...58.V)..C.)..f.. `....L....!...p.\k.0.a.N.U.A..F.m.Y.5....'.*. ..W[....cfTDC.....V.....W`...Q!.JEaE....5O.{\N.p8b.5.#*.t .....^...p..A.+.0cC..(.v.,.....qO....-b.0.#l.....p...w...sN]m..-c.=....L....I..T...I.3....]...r.....Ae.H%..!.....O...?-.I..".4.....p...{..0..#,.....%4.;E....w..].....ga...X....#...h@.'E. '.|...I.a..J..V...!...E..?8[CQ?.'...5Qy.....X..)Y..ic 0....!..Gf..4...o.R../.^..y2.'..p.....KO..v.T....~.....-]"..u9Q..i..^e..!.i".^.....C.CKV..~Ku.4"m.$>cKP...x...7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F692DA26.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 288 x 77, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	23989
Entropy (8bit):	7.989754044300238
Encrypted:	false
SSDEEP:	384:SGjFc9Ll+HCggc/h3GXoQjZVVawDIPsTDGY9R9cNc+3JY0kEtWhfEWa92ppgMoF3:S5plMCgzGoOzVawisTDGY9Rs3JYhEtqy
MD5:	839795652A8FE78F26F4D86D757ABDE8
SHA1:	979E5B90C72EA3E5E9D9B506AFDC981BFCA61B60
SHA-256:	1A9EF0E2F66682B532D15457635920067C4F29EF762D2E8A3E0363B4CF39C13E
SHA-512:	E6D5CB06679832DE768E23EF42B9780E4E8327A057A3EA0A6CD5B76908B210078EF659CA44C8723960AB59A0DB85A052C45E7A29D7FA8A643275BA5F210F6773
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR... ...M.....sRGB.....pHYs.....+....]ZIDATx^.....{fs..|.S.....d....`...9.....8..6/.....E.BB.....yw..w.-.FF.g.5~5..ivv.'..U.Tu..8.../=..R9s.Rn....Ry.....@..V.m). bCU..n....Ue.,~b;K.Q.KUlUR.`../...:.Y.Jy..Jy8.Q.K..Xzg..a.Y....X[...s.....`...Q1b....*.....|e.a..$..(...e....e.e..i$SQ.i.y....o.@.....p..yx.b.~....Z"..Xc{,..{..o....`...9K..;.....=...%.@]? .h!.....W...Z....T.Uul..V..PS[.j.....,..W...T.Z..e..T*.J)..+.K*Wt.....W.].K..4.....{.<)...V+e....u.I..A...`o..w....jUU...b...'....EW....R\..'..b.....U.X..SKV..O&..?.)....}._....\....*..hU\..W. m.I..|.0\...o..?c.a3'.2}...u....`.9..*....q.dc....!..vq..B...9....&..rsJ.\...)..}.W./.._.g.5e....sy.....@.I.J.UgW...q..o9^O.g;V.r*v...U.0..._?.5|...x...m..Z....6...._..I.....dc.....K..`U.c+;.K.^.. .`.L...j:W(...fuB=.p..w=..D....q..&..8.V.....UU.b#z...Xyo..X...*...w..U.....sW2...d.u.~.~..)I....e.q.:#r.f.....m|...w_...1.i..bs.F..L.`.}..6V..w.....z

C:\Users\user\AppData\Local\Temp\70D40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	79256
Entropy (8bit):	7.896452643285173
Encrypted:	false
SSDEEP:	1536:9+milem3l7eO+dRRVnyYPlMVGoIahaDHTU6hryF70cAeWvijWGHL:9+wol7eO6RSYP2sTU2yF70cAijW2L
MD5:	69D8C4FE679D4CD97306A32FD7457456
SHA1:	6466079B161A8677080CE83DCFC6841C59B82350
SHA-256:	ADD2FC296BCFF22DC4247BAE39D2B7DB5BD08484CB56403A0CB2A49E3273F25C
SHA-512:	AC7BEBEE4C0888762928F01A0715FE1698ECB37D93BC2EB0022B6ED008953EC12F52567171B1EE6BBE38BD64B3B106457FE053BF52E5B93979A4A9B5BEEC5BEF
Malicious:	false
Preview:	.T.n.0....?.....C.c. ....X"...&..>CZq.8V...[.Q3....."j.Z6m&..'..k.....U..S.x.-.....n..+B;lY.R..9.....p....D...A....L~s.]...9.|v.+qoRu....:V]..R-.6..:?.Xj..!B0Z.D.....j.%(/.-.i0D.. {.dM..&...R.(.....&:.....^..Ia}..w.....0j.....z...9N...X.F.iJ...2.+'..hOh....RA"/..'$..$.O#WR.G|...:?.i3..3.eD....\O....b...o.wG:....6Q[t.n.5.....c.....s.....> ..._O...3..D.1i.w....+R..| ...u@..1>.....PK.....!.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB3342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$INDIV_PAYM_633854-506518488.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

C:\Users\user\Desktop\~$INDIV_PAYM_633854-506518488.xlsb	
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362C7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.875828596690012
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	INDIV_PAYM_633854-506518488.xlsb
File size:	63444
MD5:	38cab943e9882cad5d389e47ce0070ed
SHA1:	fe99ceae30df2196a413a0f841716ec88fdc7a7e
SHA256:	17c5220167efeb1fcaceb99e62339e7ffb904149dfad6c0f2d2b78800a329218
SHA512:	901e342dec5dbaeedf2de9a31a3e1f2fa23e97975566628dbb8544a1c70685412a1730b275f0784e6d46f92ba3c86bd789b955f54d4e4986bd2735f798159263
SSDEEP:	1536:KMTMXwc5jlMVGoIahaDHTU6hryF70liWWGH0AeWca:KMTi5j2sTU2yF70liWW20Ra
File Content Preview:	PK.....!..<.....z.....[Content_Types].xml ...(.....&&.....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "INDIV_PAYM_633854-506518488.xlsb"

Indicators

Has Summary Info:	
Application Name:	
Encrypted Document:	
Contains Word Document Stream:	
Contains Workbook/Book Stream:	
Contains PowerPoint Document Stream:	
Contains Visio Document Stream:	
Contains ObjectPool Stream:	

Indicators

Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6796 Parent PID: 800

General

Start time:	14:49:59
Start date:	11/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xd70000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6416 Parent PID: 6796

General

Start time:	14:50:25
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\jbeiwmje.dll
Imagebase:	0xb50000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis