ID: 501787
Sample Name: art-1881052385.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:01:19
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

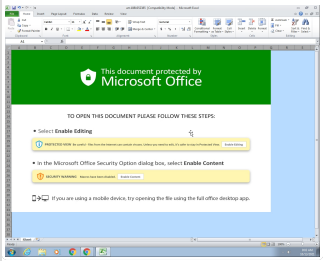
Windows Analysis Report art-1881052385.xls

Overview

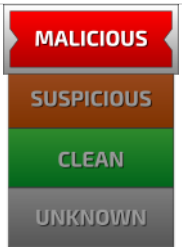
General Information

Sample Name:	art-1881052385.xls
Analysis ID:	501787
MD5:	d8b24f156013e77.
SHA1:	bf3de63943d78a1.
SHA256:	0361b3ee64c579..
Infos:	

Most interesting Screenshot:



Detection



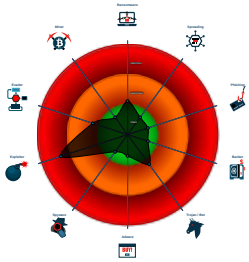
Hidden Macro 4.0

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Antivirus detection for URL or domain
- Sigma detected: Regsvr32 Comman…
- Sigma detected: Microsoft Office Pr…
- Document exploit detected (process…
- Document exploit detected (UrlDown…
- Yara detected hidden Macro 4.0 in E…
- Yara signature match
- Potential document exploit detected…
- Uses a known web browser user age…
- May sleep (evasive loops) to hinder …
- Document contains embedded VBA …
- JA3 SSL client fingerprint seen in co…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1208 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
  - regsvr32.exe (PID: 292 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 2140 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
  - regsvr32.exe (PID: 1876 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 59BCE9F07985F8A4204F4D6554CFF708)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
art-1881052385.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x3bf57:$s1: Excel • 0x34eb:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 0 0 00 00 00 00 00 00 00 01 3A
art-1881052385.xls	JoeSecurity_HiddenMacro	Yara detected hidden Macro 4.0 in Excel	Joe Security	

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

AV Detection:

Antivirus detection for URL or domain

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)

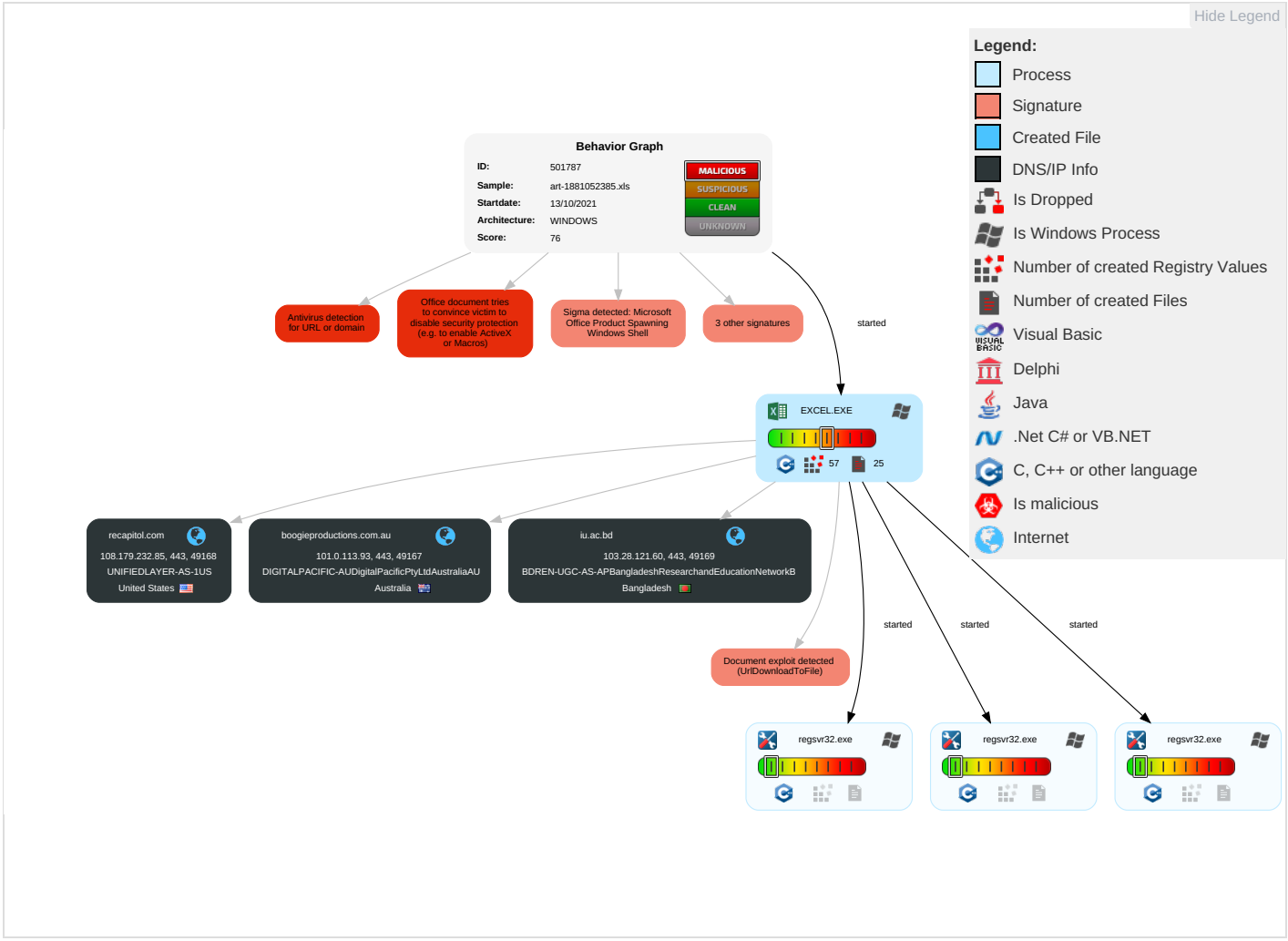
HIPS / PFW / Operating System Protection Evasion:

Yara detected hidden Macro 4.0 in Excel

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Scripting 1	Path Interception	Process Injection 1	Disable or Modify Tools 1	OS Credential Dumping	Virtualization/Sandbox Evasion 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Exploitation for Client Execution 2 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	System Information Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 2	SIM Card Swap	

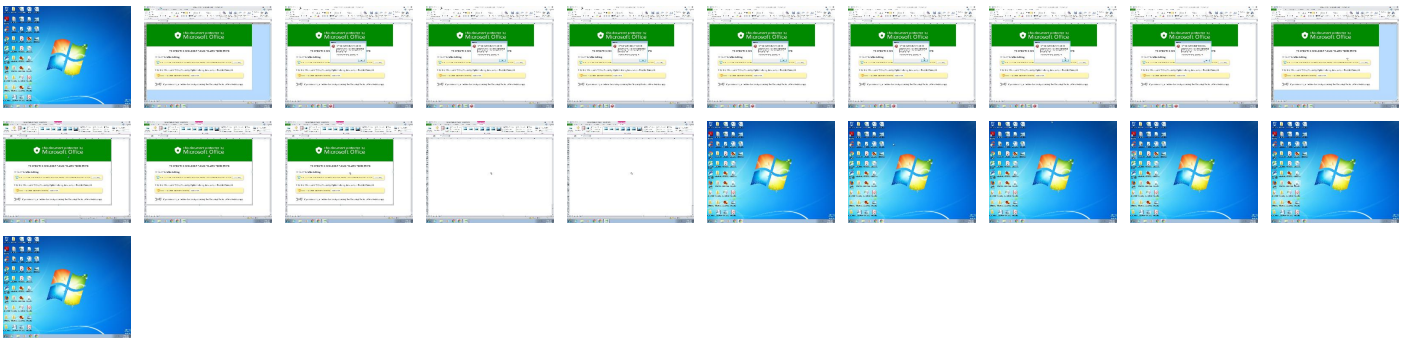
Behavior Graph

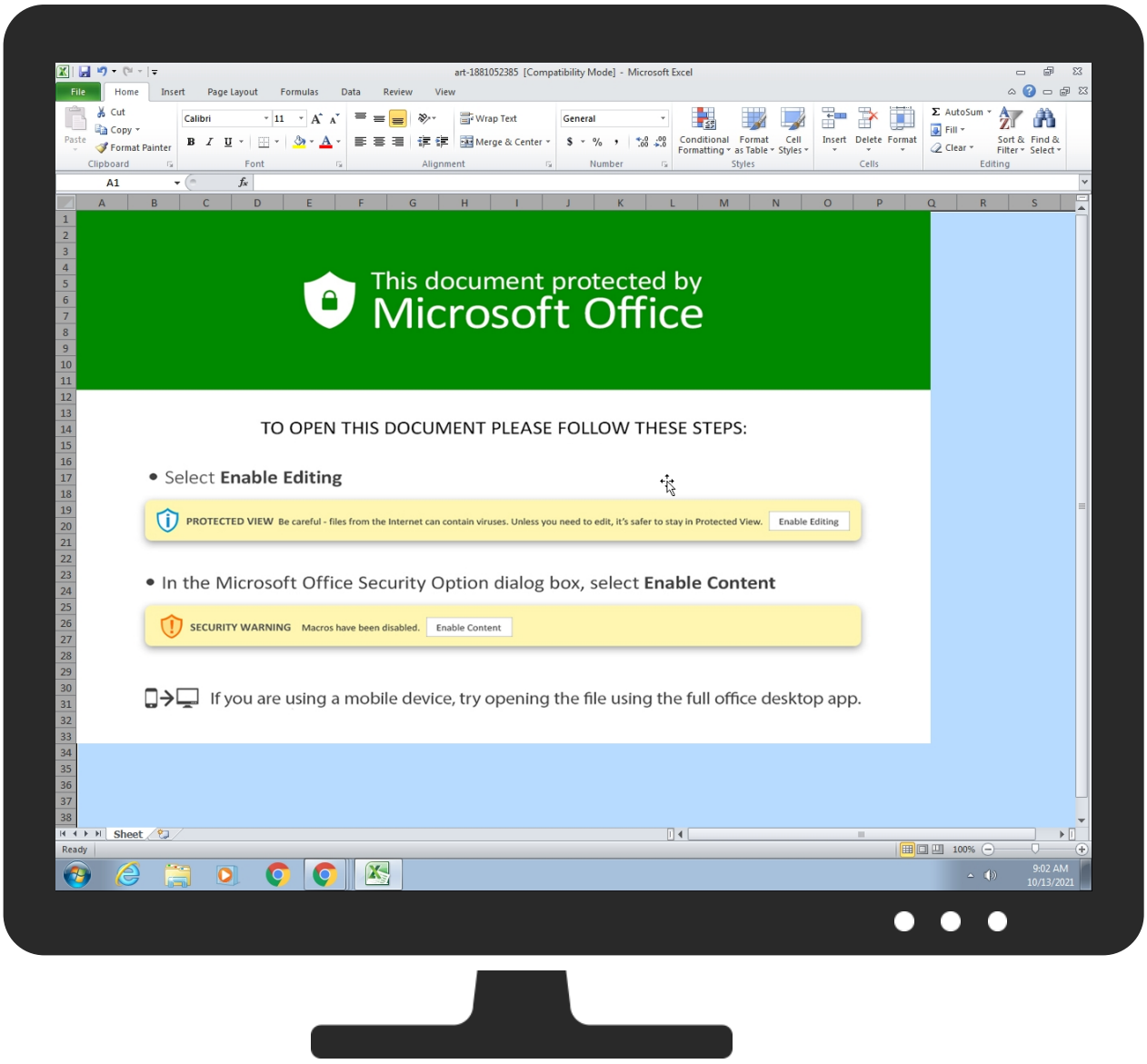


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://recapitol.com/pl92fIeHE11X/filht.html	100%	Avira URL Cloud	malware	
http://https://iu.ac.bd/QpPq5lm6Xy/fikfh.html	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://boogieproductions.com.au/jNW2LDF/filkfht.html	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iu.ac.bd	103.28.121.60	true	false		unknown
boogieproductions.com.au	101.0.113.93	true	false		unknown
recapitol.com	108.179.232.85	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://recapitol.com/pl92fIeHE11X/filht.html	true	• Avira URL Cloud: malware	unknown
http://https://iu.ac.bd/QpPq5lm6Xy/fikfh.html	false	• Avira URL Cloud: safe	unknown
http://https://boogieproductions.com.au/jNW2LDF/filkfht.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.0.113.93	boogieproductions.com.au	Australia		55803	DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	false
103.28.121.60	iu.ac.bd	Bangladesh		63961	BDREN-UGC-AS-APBangladeshResearchandEducationNetworkB	false
108.179.232.85	recapitol.com	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501787
Start date:	13.10.2021
Start time:	09:01:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	art-1881052385.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:	8
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:	mal76.expl.winXLS@7/0@3/3
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 • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:01:34	API Interceptor	312x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.28.121.60	g7NoKI5667.dll	Get hash	malicious	Browse	• bengali.iu.ac.bd/xNM4FTUzqRRk/ICguHncbARsgBD8NCSA2Bx8nL0Z6c3lifn1yZX5heA==
	qsdqqsd.dll	Get hash	malicious	Browse	• bengali.iu.ac.bd/xNM4FTUzqRRk/fXMKNg0nKzN/DA15DggBI0N6dX1le310YXlkfw==
	090921.dll	Get hash	malicious	Browse	• bengali.iu.ac.bd/xNM4FTUzqRRk/fXMKNg0nKzN/DA15DggBI0N6dX1le310YXlkfg==
	diagram-595.doc	Get hash	malicious	Browse	• bengali.iu.ac.bd/xNM4FTUzqRRk/GAUAID5zCzE+BzoOJAtGenN5Yn59cmV+YXl4
	diagram-378.doc	Get hash	malicious	Browse	• bengali.iu.ac.bd/xNM4FTUzqRRk/cxMTCDUBQ3p1fWV7fXRheWR5fg==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iu.ac.bd	g7NoKI5667.dll	Get hash	malicious	Browse	• 103.28.121.60
	qsdqqsd.dll	Get hash	malicious	Browse	• 103.28.121.60
	090921.dll	Get hash	malicious	Browse	• 103.28.121.60
	diagram-595.doc	Get hash	malicious	Browse	• 103.28.121.60
	diagram-378.doc	Get hash	malicious	Browse	• 103.28.121.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALPACIFIC-AUDigitalPacificPtyLtdAustraliaAU	doc-379851424.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-379851424.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.112.4
	ITT - PPCL-2021-0515-PKG4 - pipping and drilling Services.doc	Get hash	malicious	Browse	• 116.90.56.138
	Inquiry-Doors.exe	Get hash	malicious	Browse	• 101.0.91.38
	product specification.exe	Get hash	malicious	Browse	• 101.0.117.102
	7PUgGUWM2l	Get hash	malicious	Browse	• 182.160.170.135
	Attached Quotation.exe	Get hash	malicious	Browse	• 101.0.117.102
	Cd9EA600XXdm0tl.exe	Get hash	malicious	Browse	• 101.0.117.102
	E8ljMuBj9L	Get hash	malicious	Browse	• 111.67.13.18
	QcXQmNSaSp	Get hash	malicious	Browse	• 49.156.27.62
	arm7	Get hash	malicious	Browse	• 111.67.13.28
	QYUNlRkkn1.exe	Get hash	malicious	Browse	• 203.16.60.34
	6Y5P9BoimMLclbt.exe	Get hash	malicious	Browse	• 101.0.117.102
	gunzipped.exe	Get hash	malicious	Browse	• 101.0.117.102
	SecuriteInfo.com.Variant.Bulz.627351.21436.exe	Get hash	malicious	Browse	• 101.0.117.102
	ENQUIRY.exe	Get hash	malicious	Browse	• 101.0.117.102
	16wKmiVoPj05ynr.exe	Get hash	malicious	Browse	• 101.0.117.102
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 101.0.117.102
BDREN-UGC-AS-APBangladeshResearchandEducationNetworkB	g7NoKI5667.dll	Get hash	malicious	Browse	• 103.28.121.60
	qsdqqsd.dll	Get hash	malicious	Browse	• 103.28.121.60
	090921.dll	Get hash	malicious	Browse	• 103.28.121.60
	diagram-595.doc	Get hash	malicious	Browse	• 103.28.121.60
	diagram-378.doc	Get hash	malicious	Browse	• 103.28.121.60

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	JrZcKXgWcl.vbs	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	doc-379851424.xls	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	doc-220808714.xls	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	INV.ppt	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	Purchase Order .xlsx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	MV JOLLY EXPRESS.docx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	DHL_Delivery_Notification.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	FedEx AWB 884174658339.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	UPDATE INVOICE FM K & S INDUSTRY.docx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 347391.docx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	swift.Telex.xls	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	Invoice number 1257MAJAKFVII2021 incl. VAT.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	Consignment Notification.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	RFQ87976VF.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	RFQPTD0075453423.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	F#U0130YAT TEKL#U0130F#U0130 FORMU.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	CONTRACT 0902021.doc	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	PO006237_2nd Shipment.docx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	sample.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	avec.xlsx	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Tue Oct 12 17:38:05 2021, Security: 0
Entropy (8bit):	7.345299074583062
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	art-1881052385.xls
File size:	251904
MD5:	d8b24f156013e7722bfbba988da25e07
SHA1:	bf3de63943d78a14a07604c90bb6e523c8bf717b
SHA256:	0361b3ee64c579db66c932ff110836fd4ade16f68eb6a18cabc9c60c96d86b59
SHA512:	6d68601bb032f0765c14cd1a7e55d5aad064b8567ee504307f72b03b87a8abdbd161a680b0931de5dfb7a4dac2d38080e23c41fd8c4c8bdb3e08ec073a5b2507
SSDEEP:	6144:nKpb8rGYrMPe3q7Q0XV5xtuEsi8/dgJ93WPcZZRRrq1RObTwvOkPDklgvS3+nQ7p:893tDrmcbTwvzD63fLvfP1GOn

General

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

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "art-1881052385.xls"

Indicators

Has Summary Info:	True
Application Name:	unknown
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:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2021-10-12 16:38:05
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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 09:02:15.234417915 CEST	192.168.2.22	8.8.8.8	0x2484	Standard query (0)	boogieproductions.com.au	A (IP address)	IN (0x0001)
Oct 13, 2021 09:02:20.100203991 CEST	192.168.2.22	8.8.8.8	0xf4d3	Standard query (0)	recapitol.com	A (IP address)	IN (0x0001)
Oct 13, 2021 09:02:22.541899920 CEST	192.168.2.22	8.8.8.8	0x8d81	Standard query (0)	iu.ac.bd	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 09:02:15.569689989 CEST	8.8.8.8	192.168.2.22	0x2484	No error (0)	boogieproductions.com.au		101.0.113.93	A (IP address)	IN (0x0001)
Oct 13, 2021 09:02:20.242722988 CEST	8.8.8.8	192.168.2.22	0xf4d3	No error (0)	recapitol.com		108.179.232.85	A (IP address)	IN (0x0001)
Oct 13, 2021 09:02:22.919787884 CEST	8.8.8.8	192.168.2.22	0x8d81	No error (0)	iu.ac.bd		103.28.121.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- boogieproductions.com.au
- recapitol.com
- iu.ac.bd

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	101.0.113.93	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:02:16 UTC	0	OUT	GET /jJNW2LDF/filkfht.html 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: boogieproductions.com.au Connection: Keep-Alive
2021-10-13 07:02:20 UTC	0	IN	HTTP/1.1 200 OK Connection: close x-powered-by: PHP/5.6.40 content-type: text/html; charset=UTF-8 cache-control: public, max-age=604800 expires: Wed, 20 Oct 2021 07:02:19 GMT content-length: 0 date: Wed, 13 Oct 2021 07:02:19 GMT server: LiteSpeed vary: User-Agent alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46"

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	108.179.232.85	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:02:20 UTC	0	OUT	GET /pl92fIeHE11X/filht.html 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: recapitol.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:02:22 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 07:02:20 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	103.28.121.60	443	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:02:23 UTC	1	OUT	GET /QpPq5lm6Xy/fikfh.html 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: iu.ac.bd Connection: Keep-Alive
2021-10-13 07:02:26 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 07:02:22 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1208 Parent PID: 596

General

Start time:	09:01:22
Start date:	13/10/2021
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:	0x13f800000
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 292 Parent PID: 1208

General

Start time:	09:01:34
Start date:	13/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0xffa60000
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

Analysis Process: regsvr32.exe PID: 2140 Parent PID: 1208

General

Start time:	09:01:34
Start date:	13/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0xffa60000
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

Analysis Process: regsvr32.exe PID: 1876 Parent PID: 1208

General

Start time:	09:01:35
Start date:	13/10/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0xffa60000
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

Disassembly

Code Analysis