ID: 501787
Sample Name: art-1881052385.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:08:39
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

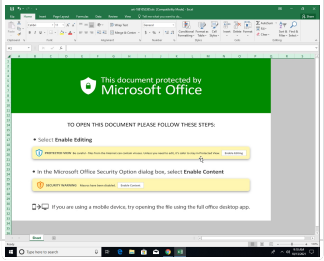
Windows Analysis Report art-1881052385.xls

Overview

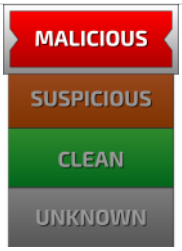
General Information

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

Most interesting Screenshot:



Detection



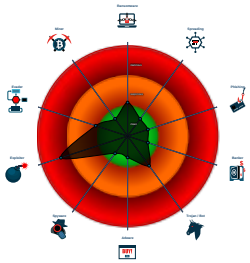
Hidden Macro 4.0

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…
- Tries to load missing DLLs
- Uses a known web browser user age…
- Document contains embedded VBA …

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 4840 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 1068 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 4140 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test MD5: 426E7499F6A7346F0410DEAD0805586B)
  - regsvr32.exe (PID: 1860 cmdline: 'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test MD5: 426E7499F6A7346F0410DEAD0805586B)
- **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)

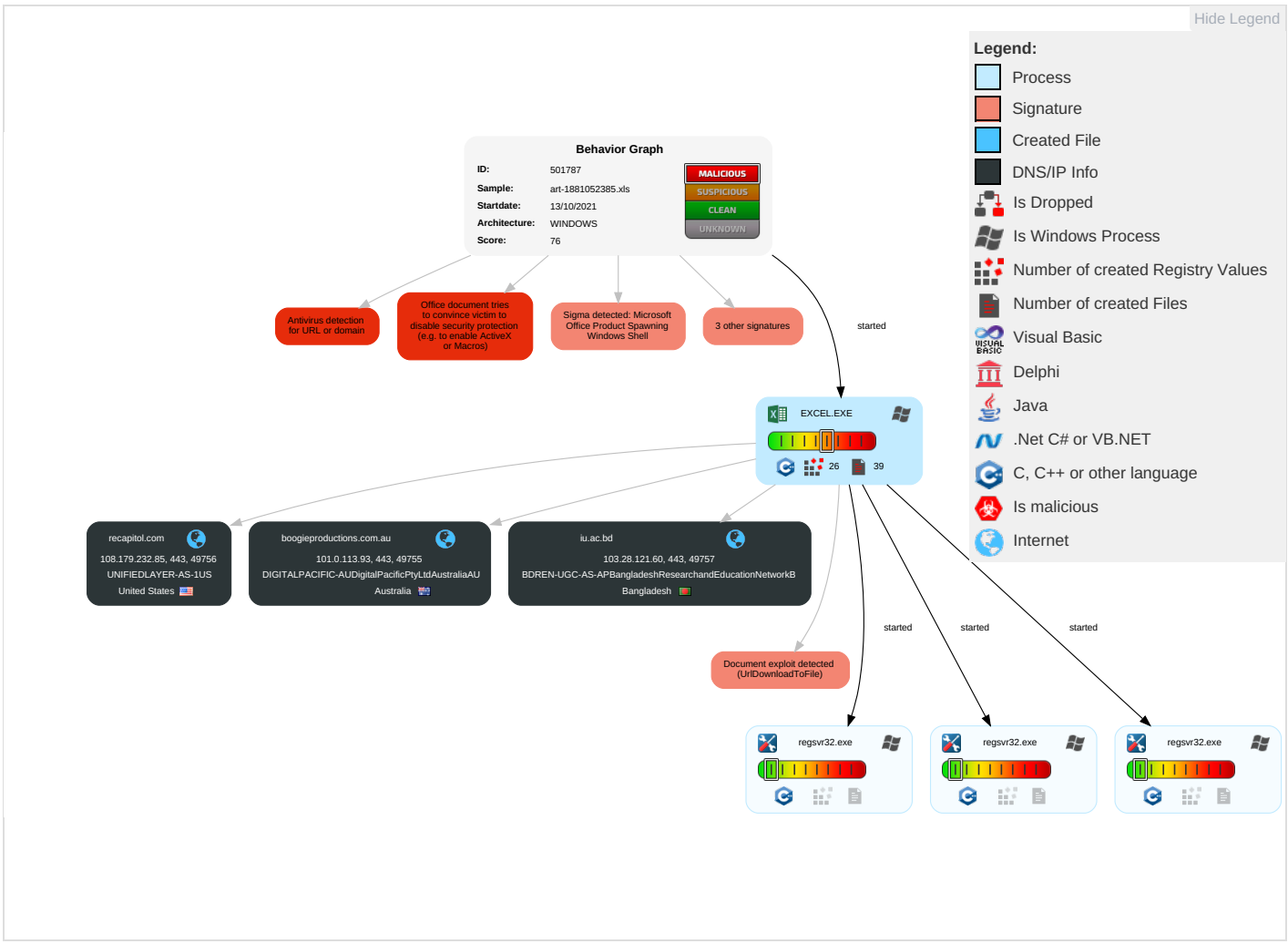
HIPS / PFW / Operating System Protection Evasion:

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	Remote Service Effects	Im
Valid Accounts	Scripting 1	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	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Exploitation for Client Execution 2 3	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	Non-Application Layer Protocol 2	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	De 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	Application Layer Protocol 1 3	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	De De Da
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 1	SIM Card Swap		Ca Bi Fr
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		M Ap Ra or

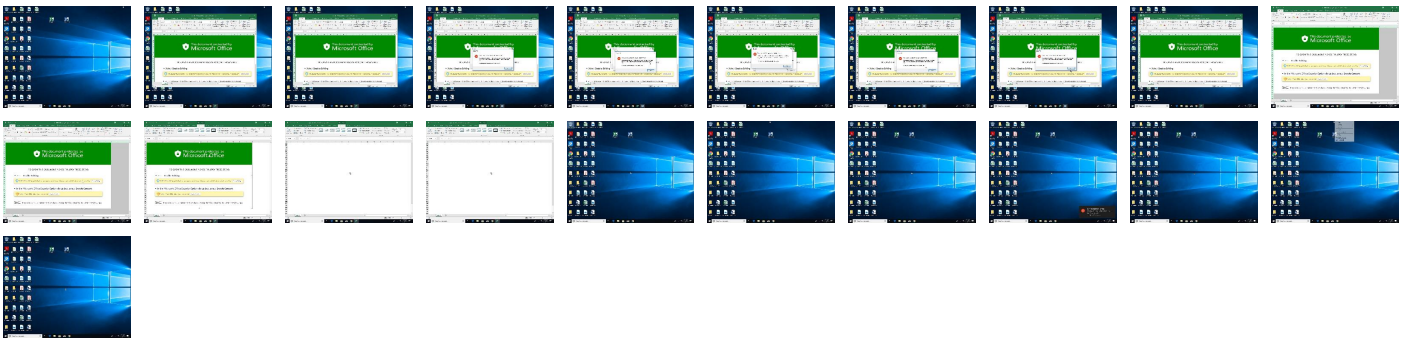
Behavior Graph

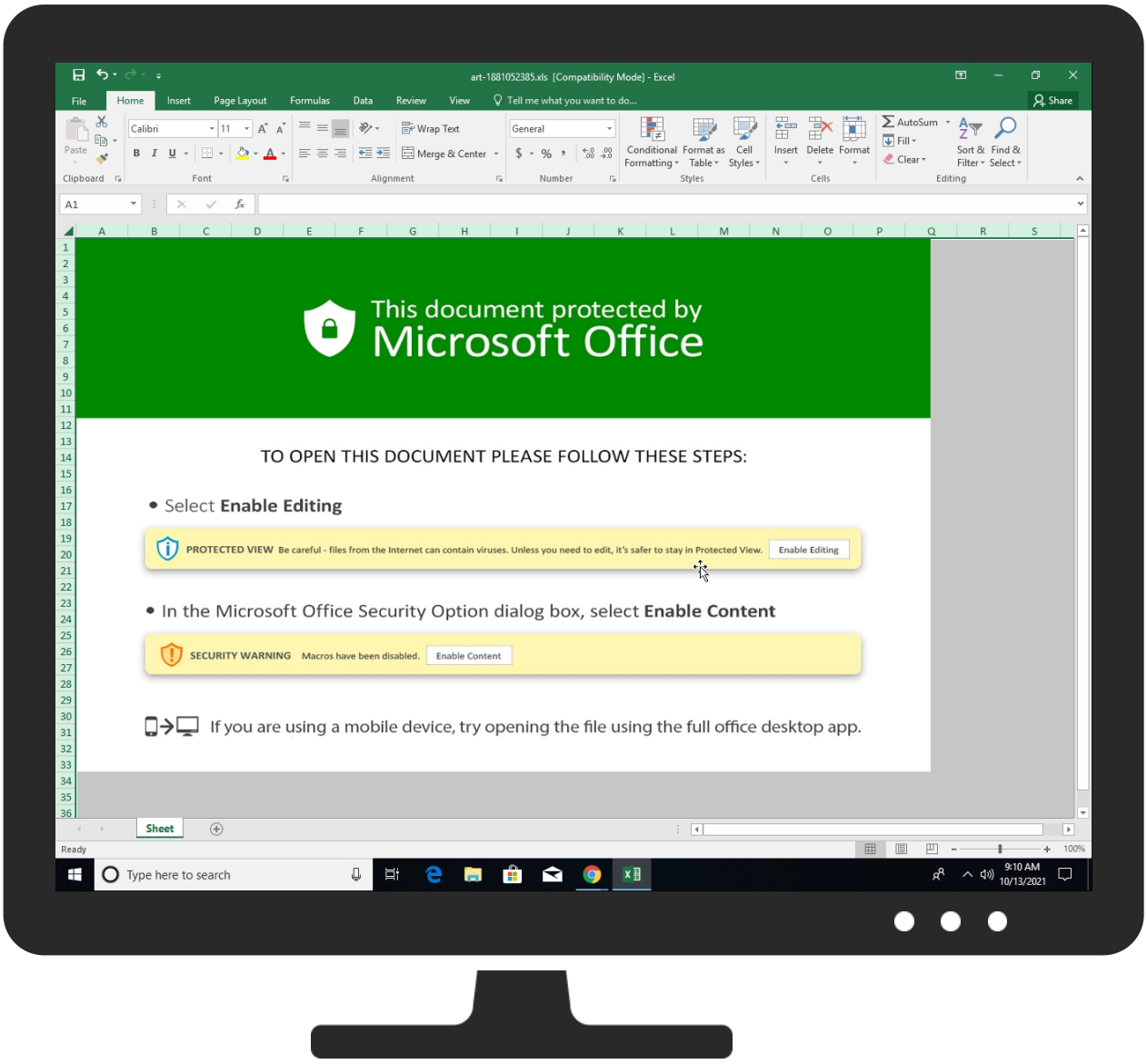


Screenshots

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

Source	Detection	Scanner	Label	Link
iu.ac.bd	0%	Virustotal		Browse
boogieproductions.com.au	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://iu.ac.bd/QpPq5lm6Xy/fikfh.html	0%	Avira URL Cloud	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://recapitol.com/pl92fIeHE11X/filht.html	100%	Avira URL Cloud	malware	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://boogieproductions.com.au/jJNW2LDF/filkfht.html	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iu.ac.bd	103.28.121.60	true	false	• 0%, Virustotal, Browse	unknown
boogieproductions.com.au	101.0.113.93	true	false	• 0%, Virustotal, Browse	unknown
recapitol.com	108.179.232.85	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://iu.ac.bd/QpPq5lm6Xy/fikfh.html	false	• Avira URL Cloud: safe	unknown
http://https://recapitol.com/pl92fIeHE11X/filht.html	true	• Avira URL Cloud: malware	unknown
http://https://boogieproductions.com.au/jJNW2LDF/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:	09:08:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	art-1881052385.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:	23
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@7/1@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 • 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
101.0.113.93	art-1881052385.xls	Get hash	malicious	Browse	

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==
108.179.232.85	art-1881052385.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
boogieproductions.com.au	art-1881052385.xls	Get hash	malicious	Browse	• 101.0.113.93
recapitol.com	art-1881052385.xls	Get hash	malicious	Browse	• 108.179.232.85
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	art-1881052385.xls	Get hash	malicious	Browse	• 101.0.113.93
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BDREN-UGC-AS-APBangladeshResearchandEducationNetworkB	art-1881052385.xls	Get hash	malicious	Browse	• 103.28.121.60
	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
37f463bf4616ecd445d4a1937da06e19	184285013-044310-sanlccjavap0003-7069_pdf (5).exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	DOC 10132021.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	WIRE ADVICE.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	WireCopy.html	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	UGS2021100716241.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	RFQ_Project 20211012 thyssenkrupp Industrial Solutions AG 6000358077_PDF.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	WireCopy.html	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	Rust_hack_v6.4.2_x64_stable.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	0810202 import Inquiry ref- November order 2021.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	Document-10122021 81258 PM.html	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	ajjVYRO.vbs	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	IMG-pic 0699821.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	HJmXSL9b6P.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	WAYBILL.EXE	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	xzH2c9tl13.exe	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
	xzH2c9tl13.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85
	538ILRcwmF.exe	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
	538ILRcwmF.exe	Get hash	malicious	Browse	• 101.0.113.93 • 103.28.121.60 • 108.179.232.85

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\4416AE68-685B-4439-B54A-0B33DBC77125	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	138049
Entropy (8bit):	5.359441538268734
Encrypted:	false
SSDEEP:	1536:acQIKNZrBdA3gBwfnQ9DQW+zBY34Zzi7nXboOidXVE6LWME9:+WQ9DQW+zbXa1
MD5:	239DBE1BBDCC17B222B5D19B4567E70F
SHA1:	88B8A5542F3313D961DEAD743E8C42280DD128CB
SHA-256:	0E702BEAE7F5B3DB1AB135A7E2F70D47A8B35266B9CBAA723873414AC2B8FD20
SHA-512:	164C5397B05BA3DE9F3CEC4BE45D4D12564CD644C2443E4D1C85191E58BF09D1A602B0E4FA475A905B003699988AB54DF39816D0ED459D68826529C6BFE6259
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-10-13T07:09:42">.. Build: 16.0.14604.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

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

File Icon

Icon Hash:	74ecd4c6c3c6c4d8

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 09:09:43.276297092 CEST	192.168.2.3	8.8.8.8	0xa25f	Standard query (0)	boogieproductions.com.au	A (IP address)	IN (0x0001)
Oct 13, 2021 09:09:47.641493082 CEST	192.168.2.3	8.8.8.8	0xcf94	Standard query (0)	recapitol.com	A (IP address)	IN (0x0001)
Oct 13, 2021 09:09:50.101304054 CEST	192.168.2.3	8.8.8.8	0x50b8	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 09:09:43.299932957 CEST	8.8.8.8	192.168.2.3	0xa25f	No error (0)	boogieproductions.com.au		101.0.113.93	A (IP address)	IN (0x0001)
Oct 13, 2021 09:09:47.782669067 CEST	8.8.8.8	192.168.2.3	0xcf94	No error (0)	recapitol.com		108.179.232.85	A (IP address)	IN (0x0001)
Oct 13, 2021 09:09:50.492285013 CEST	8.8.8.8	192.168.2.3	0x50b8	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	192.168.2.3	49755	101.0.113.93	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:09:43 UTC	0	OUT	GET /jJNW2LDF/filkfht.html 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: boogieproductions.com.au Connection: Keep-Alive
2021-10-13 07:09:47 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 07:09:47 GMT content-length: 0 date: Wed, 13 Oct 2021 07:09:47 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	192.168.2.3	49756	108.179.232.85	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:09:48 UTC	0	OUT	GET /pl92fIeHE11X/filht.html 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: recapitol.com Connection: Keep-Alive
2021-10-13 07:09:50 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 07:09:48 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	192.168.2.3	49757	103.28.121.60	443	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE

Timestamp	kBytes transferred	Direction	Data
2021-10-13 07:09:51 UTC	1	OUT	GET /QpPq5lm6Xy/fikfh.html 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: iu.ac.bd Connection: Keep-Alive
2021-10-13 07:09:53 UTC	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 07:09:50 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: 4840 Parent PID: 744

General

Start time:	09:09:39
Start date:	13/10/2021
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:	0xf70000
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

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 1068 Parent PID: 4840

General

Start time:	09:09:53
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test.test
Imagebase:	0x230000

File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 4140 Parent PID: 4840

General

Start time:	09:09:53
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test1.test
Imagebase:	0x230000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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: 1860 Parent PID: 4840

General

Start time:	09:09:54
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\regsvr32.exe' C:\Datop\test2.test
Imagebase:	0x230000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
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