JoeSandbox Cloud PRO

ID: 1125217
Sample Name: test1234.docx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:29:13
Date: 01/05/2020
Version: 28.0.0 Lapis Lazuli

Table of Contents

Analysis Report test1234.docx

Overview

General Information

Joe Sandbox Version:	28.0.0 Lapis Lazuli
Analysis ID:	1125217
Start date:	01.05.2020
Start time:	22:29:13
Joe Sandbox Product:	Cloud
Overall analysis duration:	0h 3m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	test1234.docx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016** Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean1.winDOCX@1/11@0/1
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .docx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, WMIADAP.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.107.3.128, 8.253.207.120, 67.27.235.254, 67.26.73.254, 8.253.95.249, 67.27.234.126, 23.210.248.85 • Excluded domains from analysis (whitelisted): fs.microsoft.com, config.edge.skype.com.trafficmanager.net, s-0001.s-msedge.net, mobile.pipe.aria.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, config-edge-skype-com.s-0001.s-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, audownload.windowsupdate.nsatc.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, mobile.events.data.trafficmanager.net • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

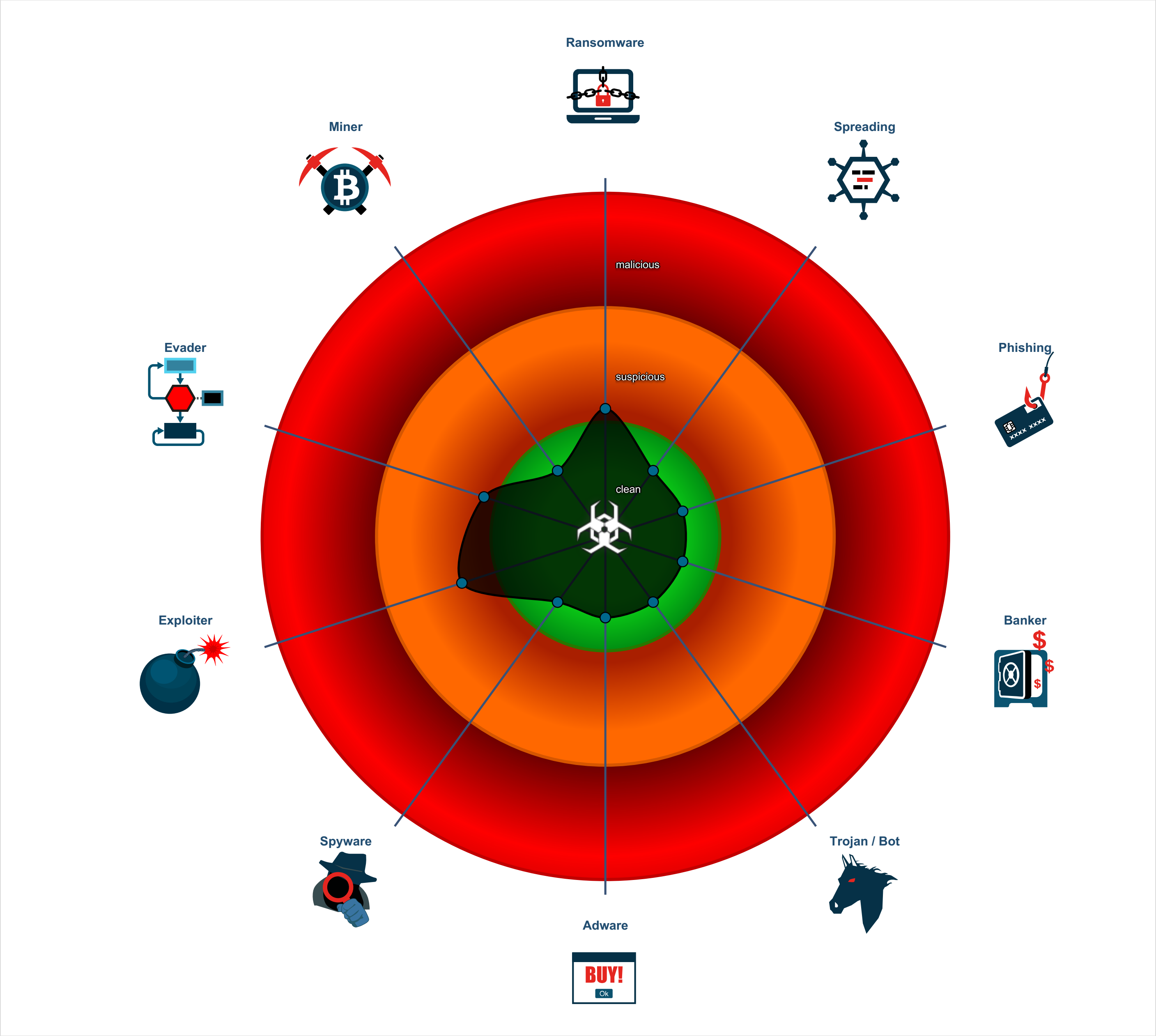
Detection

Strategy	Score	Range	Reporting	Whitelisted	Detection
Threshold	1	0 - 100	Report FP / FN	**false**	MALICIOUS SUSPICIOUS [✓ CLEAN] UNKNOWN

Confidence

Strategy	Score	Range	Further Analysis Required?	Confidence
Threshold	3	0 - 5	true	99% 80% [✓ 60%] 40% 20% 5%

Classification Spiderchart



Analysis Advice

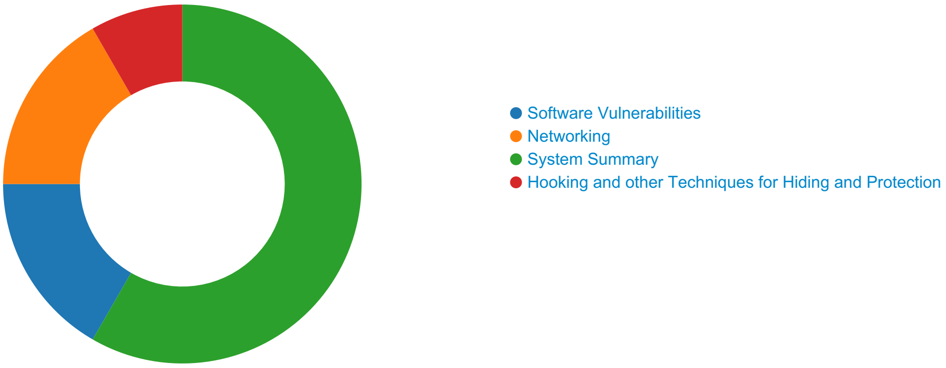
No malicious behavior found, analyze the document also on other version of Office / Acrobat

Uses HTTPS for network communication, use the 'Proxy HTTPS (port 443) to read its encrypted data' cookbook for further analysis

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	Impa
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Port Monitors	Masquerading 1	Credential Dumping	File and Directory Discovery 1	Application Deployment Software	Data from Local System	Data Compressed	Standard Cryptographic Protocol 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Mod Syst Parti
Replication Through Removable Media	Exploitation for Client Execution 2	Port Monitors	Accessibility Features	Binary Padding	Network Sniffing	System Information Discovery 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock

Signature Overview



Click to jump to signature section

Software Vulnerabilities:

Potential document exploit detected (performs HTTP gets)

Potential document exploit detected (unknown TCP traffic)

Networking:

IP address seen in connection with other malware

Uses HTTPS

System Summary:

Classification label

Creates files inside the user directory

Creates temporary files

Reads ini files

Found graphical window changes (likely an installer)

Checks if Microsoft Office is installed

Uses new MSVCR Dlls

Hooking and other Techniques for Hiding and Protection:

Disables application error messsages (SetErrorMode)

Malware Configuration

No configs have been found

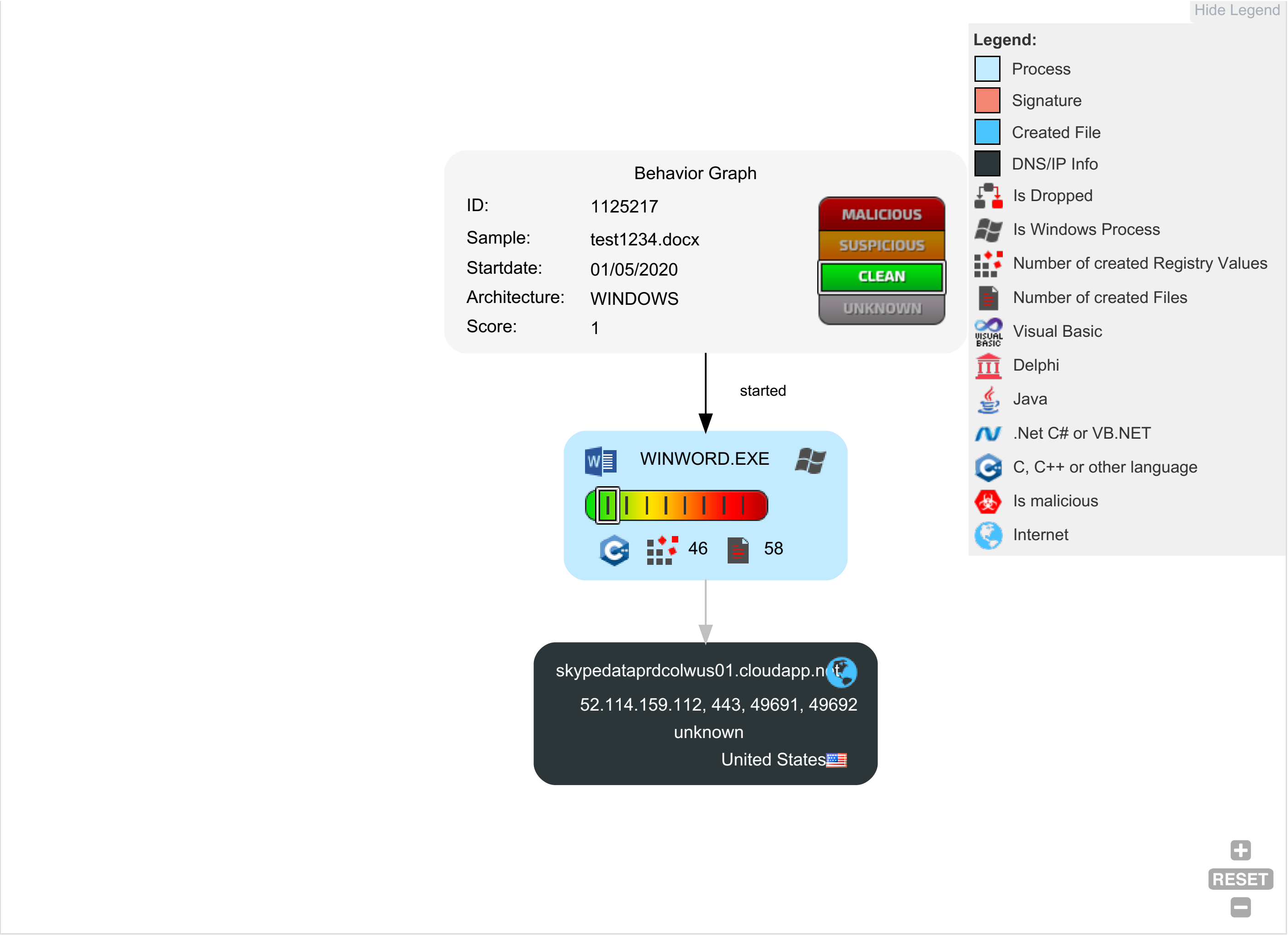
Similar Samples

Samplename	Analysis ID	SHA256	Similarity
test1234.docx	1125217		
CyberFT_CB.pdf	822892	Get hash	
CyberFT_MSEx_compare.pdf	822894	Get hash	
SAPURA 900 - POB - 08 - MARCH - 2020.xlsx	1086990	Get hash	

52292.pdf	76726	Get hash	
Invoice #527579.pdf	79955	Get hash	
SignedBankAuthorization_166819_BrightView Landscape.pdf	78651	Get hash	
K-40631 Offer.xls	1092555	Get hash	
rmStmt_ASA_00.pdf	1016338	Get hash	
First Notice - MMFR Noncompliance Q2 2020(7001).docx	1116774	Get hash	
091118Noblebank.pdf	76580	Get hash	
DOC200918.pdf	541066	Get hash	
Project Recommended doc2.pdf	79660	Get hash	
Invoice # 3161802.pdf	79927	Get hash	
Grand Thornton.pdf	509579	Get hash	
zajavka rus.doc	1093457	Get hash	
Payment_Advice.xls	1112828	Get hash	
Purchase Order Receiving Copy 70 for Colorcon Inc..pdf	1024959	Get hash	
CV STEVY F6T6.docx	1110110	Get hash	
KCS Prepay_ Schedule Form_v7.2019ydh.docx	1093462	Get hash	
DS_GE SENSING EMEA UNLIMITED COMPANY_ENG_254828.docx	1108853	Get hash	
Tsys presentation eXXpedition Feb 2020.pptx	1074785	Get hash	
New Classification of Temperament, Character, Behavior and Personality types.docx	100461	Get hash	
Anexos_Informes_Periciales_20180713_000509_0999f69286a6648e_1537532702652.pdf	79521	Get hash	
y3255591.pdf	734785	Get hash	
Docs.pdf	76798	Get hash	
Project Recommended doc2.pdf	79655	Get hash	
Ga6rS1qqnf.pdf	47428	Get hash	
d4a54d660163e25e35cd0c3e110947ca73292e39e4437b63cb0aa0bd9b4bcf2.pdf	294280	Get hash	
Verify Icloud 8272-8821-3922-8772.pdf	30835	Get hash	
SKKNI Inspektur Bahan Peledak (Final).pdf	91654	Get hash	
RO-2018.docx	1115541	Get hash	
Tool Box Talks Sign in Sheet 2020.docx	1102333	Get hash	
Solirwinds Bootcamp Discount.docx	930539	Get hash	
CreateSpace.Hacker.Jun.2015.ISBN.1512214566.pdf	79393	Get hash	
TEST SHAY.docx	105540	Get hash	
shippingmanifest.docx	698884	Get hash	
05-04-18.pdf	547831	Get hash	
0910.pdf	735412	Get hash	
q2866742.pdf	734781	Get hash	
z7812421.pdf	734793	Get hash	
PO_88239.pdf	77077	Get hash	
LawLLC_TPReportsx2363018.pdf	734567	Get hash	
SKM_C554e17060706560.pdf	287571	Get hash	
FINAL NOTICE.pdf	309673	Get hash	
Chase Security Alert.pdf	291848	Get hash	
new file.pdf	30415	Get hash	
uofc_parking.pdf	997148	Get hash	
#Payment-Receipt 1.docx	102273	Get hash	
ET44 ET45 series Benchtop digital bridge.docx	68201	Get hash	
clickable.docx	105644	Get hash	
Installation Guide for i4cut 1D.doc	881171	Get hash	
shippingmanifest.docx	698884	Get hash	
Closing_documents.docx	703120	Get hash	

correction.docx	718914	Get hash	
SVC_08393002293.pdf	545667	Get hash	
Invoice_00387.pdf	733437	Get hash	
Policy Request - File #2018-313 ORT File #18117359.pdf	64883	Get hash	
Swift Copy.mht	54072	Get hash	
FedEx_10031917.pdf	30979	Get hash	
IT SUPPORT.pdf	30012	Get hash	
NOTICE.pdf	30627	Get hash	
Panerisco Investment.pdf	30453	Get hash	
pdfIB.pdf	30813	Get hash	
Micro-Voice.pdf	30847	Get hash	
scan000131.pdf	30699	Get hash	
pdfIB.pdf	30811	Get hash	
voice msg.pdf	30834	Get hash	
Office-Voicemail.pdf	30873	Get hash	
pdfIB.pdf	30812	Get hash	
Help_Desk.pdf	30274	Get hash	
SECURITY DOCUMENT.pdf	30895	Get hash	
Invoice_PDF.mht	833649	Get hash	
HR policy review..docx	101898	Get hash	
A28273.docx	102559	Get hash	
02 Microsoft Teams PowerPoint Guide for Quick Start.pptx	101553	Get hash	
validate (2).pdf	76252	Get hash	
DocuSign Invoice.docx	105176	Get hash	
CV_ AURORA AVIGNONI.docx	105178	Get hash	
New Doc1.docx	64862	Get hash	
2018 Transfer List.mht	68779	Get hash	
scotworkusa.pdf	31169	Get hash	
scotworkusa.pdf	31172	Get hash	
scotworkusa.pdf	31171	Get hash	
scotworkusa.txt.pdf	31168	Get hash	
Helpdesk Notification.docx	102510	Get hash	
Doc-32569008.docx	104051	Get hash	
You have new voice note.doc	101530	Get hash	
A28273.docx	102557	Get hash	
A28273.docx	102558	Get hash	
rQe3q2EnyT.docx	103699	Get hash	
Docs 01.pdf	76680	Get hash	
2160244 - Invoice for customer.doc	882264	Get hash	
Remittance Advice0023.doc	852217	Get hash	
New Doc1.docx	64864	Get hash	
trenddata.0065.xls	71053	Get hash	
2018 Transfer List.mht	67732	Get hash	
X-Apple-BillingVerify85123.docx	103175	Get hash	
Helpdesk Notification.docx	102510	Get hash	
ReviewID#363[7861202].doc	102019	Get hash	
Scanned010.AdvantechTerms.pdf	78475	Get hash	

Behavior Graph



Simulations

Behavior and APIs

No simulations

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

No Antivirus matches

Yara Overview

Initial Sample

No yara matches

PCAP (Network Traffic)

No yara matches

Dropped Files

No yara matches

Memory Dumps

No yara matches

Unpacked PEs

No yara matches

Sigma Overview

No Sigma rule has matched

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.114.159.112	http://https://wgyates-my.sharepoint.com/:o:/g/personal/jennifer_james_ellissteel_com/Es6mzWRZZQNEm5AZnW2VLBUB1_YDdvqUgbPhIMHrCV8Flg?e=eaM6fl	Get hash	malicious	Browse	
	http://https://onedrive.live.com/redir?resid=1A7E049B54189AB3%21103&authkey=%21AO2HrrVv4r4880U&page=View&wd=target%28Untitled%20Section.one%7Cd2499090-a97b-4bc4-9172-9c66580c17a3%2FRon%20shared%20a%20document%20with%20you.%7C45e6b0d3-7720-4a10-be29-3649d223ec0e%	Get hash	malicious	Browse	
	order-927337.xls	Get hash	malicious	Browse	
	Projekt.wbk	Get hash	malicious	Browse	
	incoming-invoice-0888.xls	Get hash	malicious	Browse	
	Covid2019_Test_A2039.doc	Get hash	malicious	Browse	
	Descr_858525.doc	Get hash	malicious	Browse	
	Guidelines 513.xls	Get hash	malicious	Browse	
	Info_695.xls	Get hash	malicious	Browse	
	http://https://onedrive.live.com/redir?resid=A37258A5832F32B8%214689&authkey=%21AKowXqG92E9h4gE&page=View&wd=target%28Quick%20Notes.one%7C14f4b0c2-0aad-4257-9e8a-0045367c9d14%2FReview%20Document%20No.%20CLT9070281%7Ccfadc8cf-140f-4bee-b6da-6b8d044e29f4%2F%29	Get hash	malicious	Browse	
	Attachment.slk	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
skypedataprdcolwus01.cloudapp.net	http://https://wgyates-my.sharepoint.com/:o:/g/personal/jennifer_james_ellissteel_com/Es6mzWRZZQNEm5AZnW2VLBUB1_YDdvqUgbPhIMHrCV8Flg?e=eaM6fl	Get hash	malicious	Browse	52.114.159.112
	http://https://onedrive.live.com/redir?resid=1A7E049B54189AB3%21103&authkey=%21AO2HrrVv4r4880U&page=View&wd=target%28Untitled%20Section.one%7Cd2499090-a97b-4bc4-9172-9c66580c17a3%2FRon%20shared%20a%20document%20with%20you.%7C45e6b0d3-7720-4a10-be29-3649d223ec0e%	Get hash	malicious	Browse	52.114.159.112
	order-927337.xls	Get hash	malicious	Browse	52.114.159.112
	Projekt.wbk	Get hash	malicious	Browse	52.114.159.112
	incoming-invoice-0888.xls	Get hash	malicious	Browse	52.114.159.112
	Covid2019_Test_A2039.doc	Get hash	malicious	Browse	52.114.159.112
	Descr_858525.doc	Get hash	malicious	Browse	52.114.159.112
	Guidelines 513.xls	Get hash	malicious	Browse	52.114.159.112
	Info_695.xls	Get hash	malicious	Browse	52.114.159.112
	http://https://onedrive.live.com/redir?resid=A37258A5832F32B8%214689&authkey=%21AKowXqG92E9h4gE&page=View&wd=target%28Quick%20Notes.one%7C14f4b0c2-0aad-4257-9e8a-0045367c9d14%2FReview%20Document%20No.%20CLT9070281%7Ccfadc8cf-140f-4bee-b6da-6b8d044e29f4%2F%29	Get hash	malicious	Browse	52.114.159.112
	Attachment.slk	Get hash	malicious	Browse	52.114.159.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
unknown	http://https://drive.google.com/file/d/1hWlc7SfuuWxEI1a0x6y_KJ66-39gJNDp/view?usp=sharing_eil&ts=5eac8483	Get hash	malicious	Browse	183.90.228.14
	CONFIDENTIAL.docx	Get hash	malicious	Browse	52.1.139.84
	CONFIDENTIAL.docx	Get hash	malicious	Browse	34.200.138.208
	May Invoice.doc	Get hash	malicious	Browse	205.185.122.246
	Rejected_Stimulus.jar	Get hash	malicious	Browse	89.208.198.226
	1QaCEWBhON.dll	Get hash	malicious	Browse	177.60.96.231
	#Ud83d#UdcdeAeriestechnology.com Audio_4544.htm	Get hash	malicious	Browse	50.87.153.185
	http://https://sks-high-performance-fax-message.webflow.io	Get hash	malicious	Browse	157.240.20.35
	http://xmsecu.com:8080/ocx/NewActive.exe	Get hash	malicious	Browse	120.92.86.126
	http://https://childtesrackscup1904.blogspot.lu/	Get hash	malicious	Browse	67.199.248.10
	http://https://tolongjagadia.com/wp-content/plugins/hw/english.php?email=bill.rebarick@austalusa.com	Get hash	malicious	Browse	162.241.114.220
	http://holfve.se/zlrllwff/vf62r5gk.Scott_Carter&hwzbddkypg	Get hash	malicious	Browse	108.177.126.157
	linqer_4.6.0.1_trial.exe	Get hash	malicious	Browse	137.135.70.79
	http://https://u15900461.ct.sendgrid.net/ls/click?upn=9A-2BxpfZZtss8CnrMI9mpkQTuKb7DiPT-2FlQIbiypLNnv264n2A7yHaegr-2BN843AVSs3trtsgXwxZsZhlLuLqADmWsKTgnUYEibWDLQIPK-2FQ4oaggydGJC1pfcNWd2EYKNNHdwe2rOpHq3XM8HvG-2FYqw-3D-3DNuqk_VIH3-2Bha1squ3Hk0F8PoA7GiLLPEmJLyL8ngaCy0ydg0D1jFVMarq55fWn2L4SuilRmjDCW7XV7ctfRvZVYBSCmQPwlF9vRwojNakJh6uIT-2FR9ct-2FqWe4QRCGaDYCludkqWz3T8KjU7Hnuawi4raaoEa4j8yqooOxOjULgJHizXVw4mW8mDo2uOajkSvwq-2B1xl8jkkAwnVrGGkrB6aDQVXNTR2vJVeq9s33Lr7nVxGmk-3D	Get hash	malicious	Browse	104.250.174.61
	http://https://onerts.glitch.me	Get hash	malicious	Browse	151.101.12.193
	Scan 202015 pdf.exe	Get hash	malicious	Browse	192.185.5.62
	Scan 202015 pdf.exe	Get hash	malicious	Browse	192.185.5.62
	http://https://www.mycirclehealth.com/FTsang@victoria.com5me5/;RlRzYW5nQHZpY3RvcmlhLmNvbQ==	Get hash	malicious	Browse	151.101.12.157
	http://https://create.piktochart.com/output/46205199-my-visual	Get hash	malicious	Browse	151.101.12.157
	http://https://sunshinestreams.net?email=Pablo.Saballos@seaboardmarine.com	Get hash	malicious	Browse	87.238.248.176

JA3 Fingerprints

No context

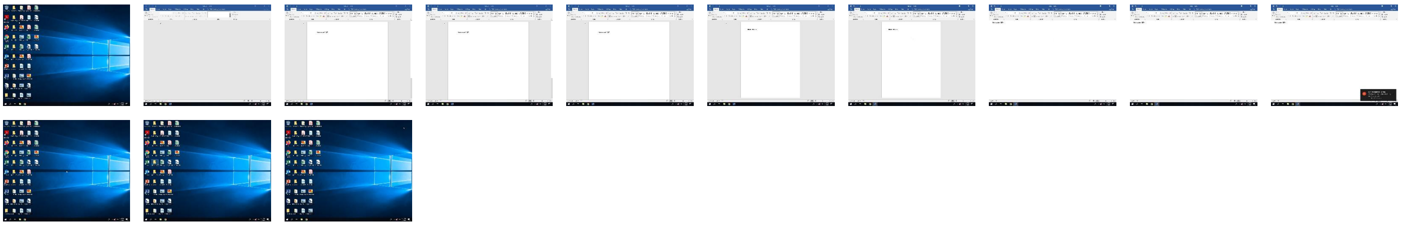
Dropped Files

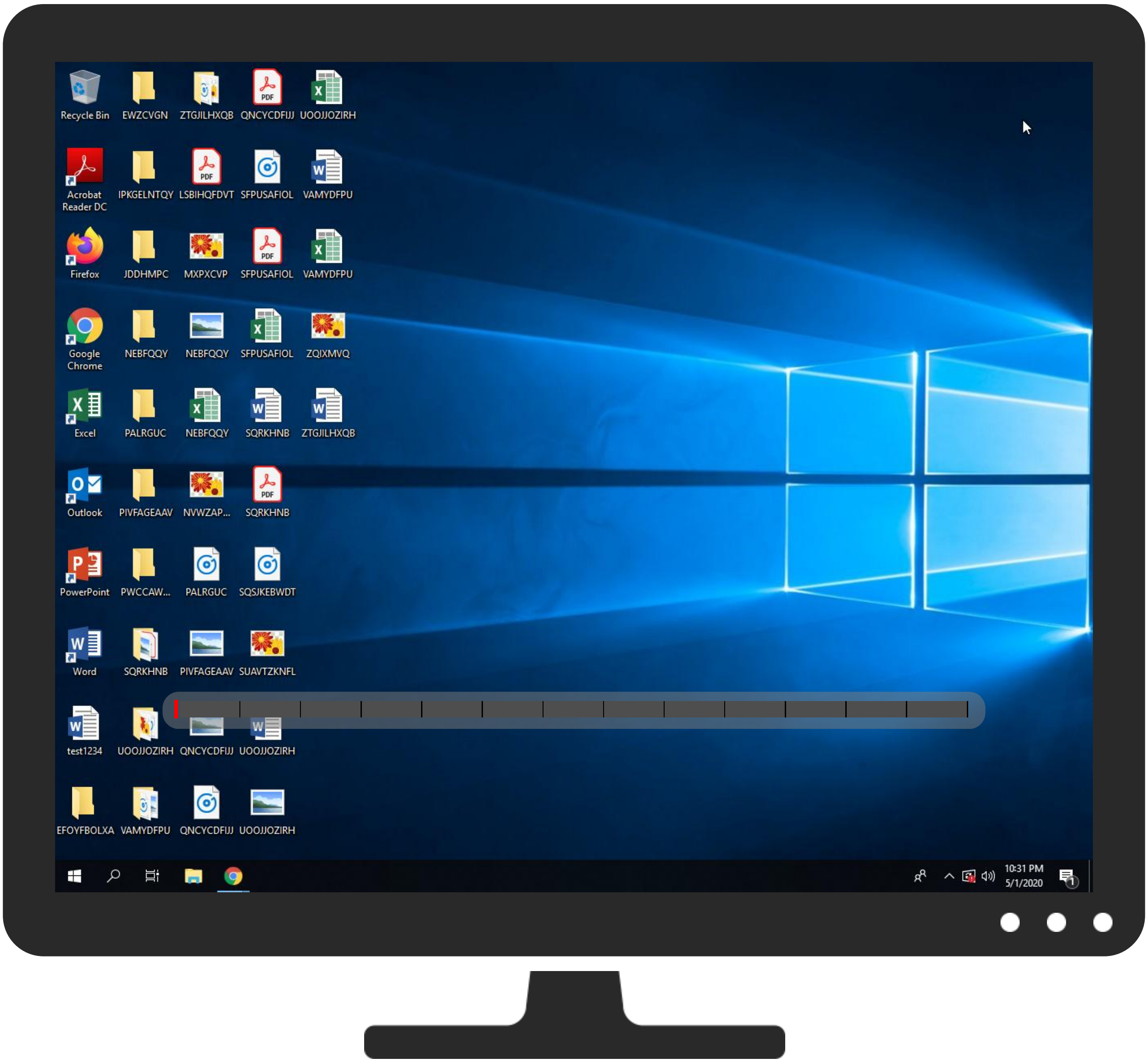
No context

Screenshots

Thumbnails

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





Startup

- **System is w10x64_office**
- WINWORD.EXE (PID: 2308 cmdline: 'C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE' /Automation -Embedding MD5: EFDE23ECDF60D334C31AF2A041439360)
- **cleanup**

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Office\OTele\winword.exe.db-wal	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	SQLite Write-Ahead Log, version 3007000
Size (bytes):	4152
Entropy (8bit):	1.1808060431537526
Encrypted:	false
MD5:	2AF251C385C81334EB7D0CA738521EEC
SHA1:	DDB44AA2ACDA7B7206435CE34056C2B48C131AB0
SHA-256:	0545DF07796A9CE147E37DA8B6A88D3684131F1A15745A4EE3B7D848BCD0D1B1
SHA-512:	082BF2605082888F8C9577CD45789A83541E472941A09F9422B54ED3F77A9B6C439B4E02C19712260C7D15D4B7742701BBD57640224BBDB8FE729859FAA35A17
Malicious:	false
Reputation:	low
Preview:	7....-..........(M..4.5...P;x...........(M..4.5.....fL.JSQLite format 3......@ ....d....d.g..

C:\Users\user\AppData\Local\Microsoft\Office\OTele\winword.exe.db.session	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	SQLite 3.x database, last written using SQLite version 3019003
Size (bytes):	12288
Entropy (8bit):	0.9299388511732635
Encrypted:	false
MD5:	4CE58D336E4862C57152125A89C44F45
SHA1:	14408712451B208B4982F2B5C28566BE9BDC5626
SHA-256:	AFCE2E4762CD1BD55FAFB881FE0058462C76D2990770E9C00D65DC4B73D5035C
SHA-512:	A5C6133605988E910F64E0C64B400A5B6231D6A34F42CE8F27E94B9DCDF421A94110BF8F04206297F6BC31692C6A56DDBDE91C5DAB90F7886EC49E062E369BB
Malicious:	false
Reputation:	low
Preview:	SQLite format 3......@ ....d....d.g...

C:\Users\user\AppData\Local\Microsoft\Office\OTele\winword.exe.db.session-journal	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Size (bytes):	13360
Entropy (8bit):	0.9062207694841746
Encrypted:	false
MD5:	0689A0725247881D908580B0632E3D21
SHA1:	D63324DFE4522D8A1472FD5C5734663903F2948B
SHA-256:	62F187397339599C4B9426F29BB851741E71D2F8EAD009B6AA24F3C37FA4B6A4
SHA-512:	0E9C31FA000AC079622D530E12697832B435EDAB5C413DF715507651C8CD36F5F038C1EF1A54A5497A20E517965D5AF783FC957BB8A3DC12BDE1FE6853C8028
Malicious:	false
Reputation:	low
Preview:	..............F)..SQLite format 3......@ ....d....d.g..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{364FD987-D4E7-4589-8077-FEDB7D4008CE}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{364FD987-D4E7-4589-8077-FEDB7D4008CE}.tmp	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{9FC62579-4525-4C29-8AA5-DD069F52300F}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Size (bytes):	1536
Entropy (8bit):	0.2492732041907113
Encrypted:	false
MD5:	72032BF006E24C290D51E2B3D9A91662
SHA1:	428EAD7B7BE47EA5D285BB4981ACD9EC0A75D53E
SHA-256:	7A9EBAF645D025B75E453F908B543388F875F1697B4A0963C69DD0DA6701AE01
SHA-512:	6FD6084543721B7C6F0FEA5707ACDEB9DF0545E217E723D283EDA6F1242C5C7EF49FB69E8077451F421961E08A71091E1A15A23DD116F361E3B49768B6F3B67C
Malicious:	false
Reputation:	low
Preview:	..T.h.i.s. .i.s. .a. .t.e.s.t. .1.2.3.4... ....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	64
Entropy (8bit):	4.239961578883821
Encrypted:	false
MD5:	44AC37E6467AAAA42F92014BD11B5A00
SHA1:	F994E8FD3507869B3F50E1370157C008C91A27C5
SHA-256:	4B43C0E89CC1F2C7B7146EEF1229DCCF7BEF82DE293AA94B5E55BE734E75CEFA
SHA-512:	ECD65BBB166EAEFF60D73A6ACB5F0CCA6A737AD38EB526D1A9C77CCB3AB26B50F36B07B808094DDCC1FA090C067BF4BC4960C3BAA6487A46F805D7DFCBA3 25BC
Malicious:	false
Reputation:	low
Preview:	[misc]..test1234.LNK=0..test1234.LNK=0..[misc]..test1234.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\test1234.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Mar 18 14:03:39 2020, mtime=Fri May 1 19:29:48 2020, atime=Fri May 1 19:29:41 2020, length=6096, window=hide
Size (bytes):	1018
Entropy (8bit):	4.587579032859174
Encrypted:	false
MD5:	4DBBDC75AB1CD4247EA6694C04C26B39
SHA1:	D37B6EDC95EA191CFA282CC502B38049DD173A4C
SHA-256:	7B265355D467E73299B5E7AFF8BAF72F41750DF3B83559AE20074FE13DD51C12
SHA-512:	CF04BCD2AE89BC84E9697A98F555903E7DBE15581D1CB93EEC4E361504B9208E60F9E0B8F7DAF478793916531356FB64382C720CB7DFE7518C8144425D2CDAF
Malicious:	false
Reputation:	low
Preview:	L.................F.... ...x..h6....uB......M>..........................j.h.2......P.. .TEST12~1.DOC..L......rPtx.P..........................).2.t.e.s.t.1.2.3.4...d.o.c.x.......R..............-.......Q...........m. .Z.....C:\Users\user\Desktop\test1234.docx..$.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.t.e.s.t.1.2.3.4...d.o.c.x.`.......X.......585948.............x..C..Z.;../.C)i.............x..C..Z.;../.C)i......... E.......9...1SPS..mD..pH.H@..=x.....h....H....X/:......`"...............L.................F.... ...x..h6....uB......M>..........................j.h.2......P.. .TEST12~1.DOC..L......rPtx.P................. ....).2.t.e.s.t.1.2.3.4...d.o.c.x.......R..............-.......Q..........m..Z.....C:\Users\user\Desktop\test1234.docx..$.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.t.e.s.t.1.2.3.4...d.o.c.x.`.......X ....585948.............x..C..Z.;../.C)i.............x..C..Z.;../.C)i..........E.......9...1SPS..mD..pH.H@..=x.....h....H....X/:......

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Size (bytes):	162
Entropy (8bit):	3.3753041861136164

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Encrypted:	false
MD5:	9C6831A6819631FDE8892AAEEAC72C09
SHA1:	E653C08E23BA1A831F68921222D106CDFAC335BD
SHA-256:	4648DE07C8A2E7C1392EBB2F1A900B66323C94EA9E2F8847D682CAF6CF324435
SHA-512:	EC64D77943F88E42E3D8BEDFD53C935085A424CAAA6A3D47F04907635FEC5DC7BFA9903271F035B843133606098F21E2787367C3C49B2B505EDE0C0AD8B055D
Malicious:	false
Reputation:	low
Preview:	.user..L.y.n.n.......`(..<....d.k...k.................I......s._6......R6........5....................X.k........

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Size (bytes):	16
Entropy (8bit):	2.6556390622295662
Encrypted:	false
MD5:	7C2BCD8D62C7D1E49DDD33CE20876267
SHA1:	B09141445851302075E4A46F9F48998FF8695857
SHA-256:	940436D80A7A518EC2740082FFBBA23DCC0F3A5F6D25F4C9A912949DBBDC9606
SHA-512:	C67FC36383FC25401169CDFA75B9872A207C8AB8DFC0BE1A0DA4DA5E7D62B7F0720A9E09588A570780232B1176D9C547251CA26B4759D391CBF3CCBEEA1DF3 3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	....L.y.n.n.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

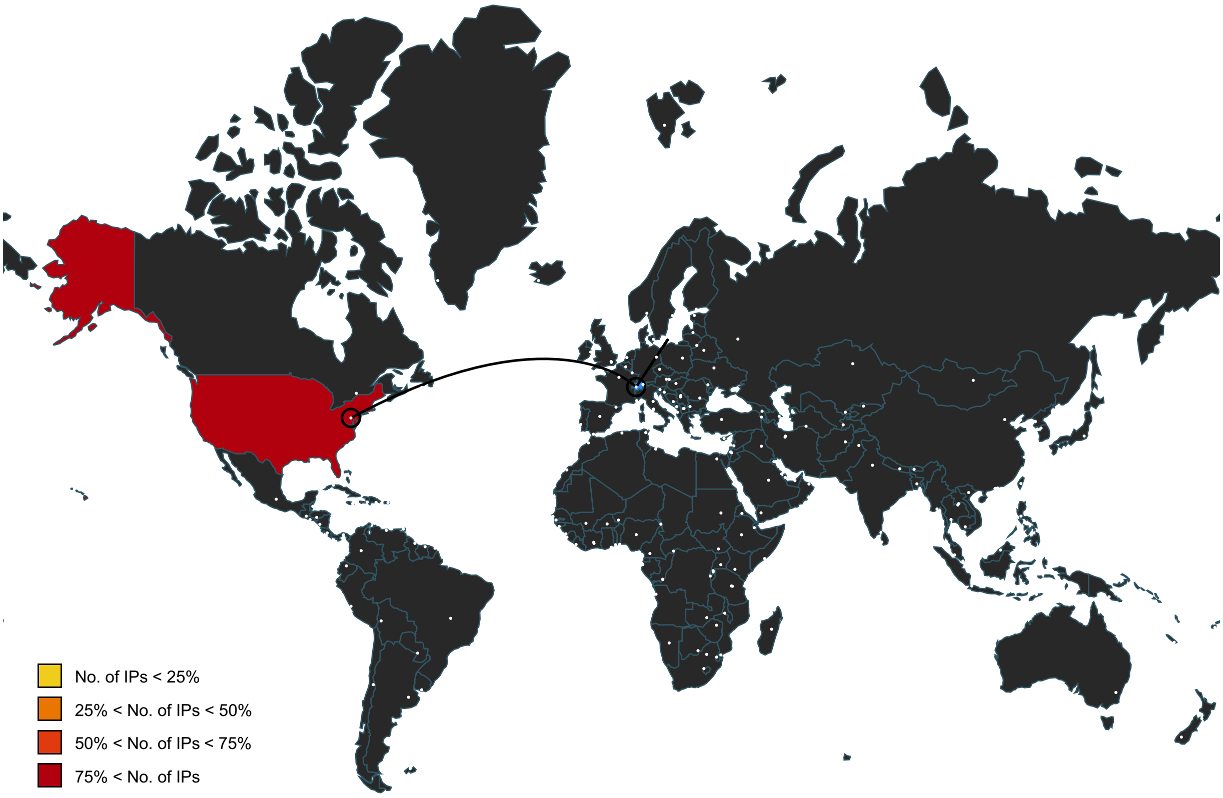
C:\Users\user\Desktop\~$st1234.docx	
Process:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
File Type:	data
Size (bytes):	162
Entropy (8bit):	3.0790996033581397
Encrypted:	false
MD5:	29F44180B27C0F65931458CB579C9F69
SHA1:	3547F1BB2D37C4F49905DC117FC4544AD11EDDD6
SHA-256:	C42CEF6252DD2D611FC8A07ECAFF6908DB9BFBADED408242D628786185ED9CE4
SHA-512:	95503F0371914E65766E8C6A575A83B60310697B701C6A32AB57355F11DB74AC7312241D28DE396F07D07FC9D6D108E289251A9B87F84042692720C8A421E5E4
Malicious:	false
Reputation:	low
Preview:	.user..L.y.n.n.......P....D...d.k.............................M>....x..h6...5.#?.........c...........X.kHa......

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
skypedataprdcolwus01.cloudapp.net	52.114.159.112	true	false		unknown

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
52.114.159.112	United States	🇺🇸	8075	unknown	false

Static File Info

General

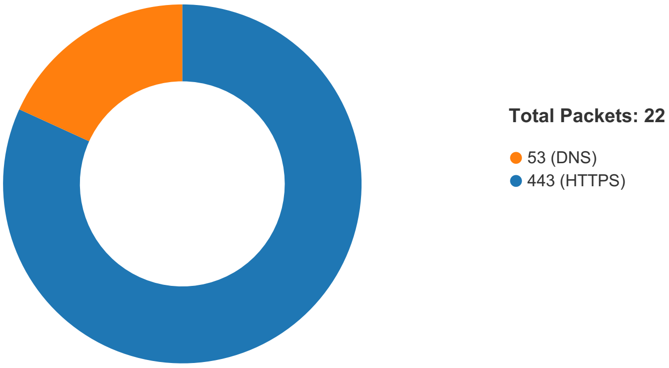
File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.716505933103133
TrID:	• Word Microsoft Office Open XML Format document (43504/1) 84.47% • ZIP compressed archive (8000/1) 15.53%
File name:	test1234.docx
File size:	6096
MD5:	b9f29aa3a1255d5441ce08c0865df188
SHA1:	7937056709c88668c9a57c8dde63eea938254b3a
SHA256:	21e1cb930823886b506b770664d831b1ef9dd124d84a43 06d7a2cab5b92ee7eb
SHA512:	a2fa213582a6605ce23e7ea34bcab991c65c93af6c03d0c 8a0d26e88aea0c489eb583445cddc9458f71e347971d7b 83373901b9377c012042746543b1848add5
SSDEEP:	96:yxMzwP5dZj6/kcLy1bBJ6TLSQoj8RNbaQPWnIwa0 G5Zc7+3yRn+eRTd:QsIZjtcu1+LnYg8xFc67+3yRHz
File Content Preview:	PK.........g.P................word/numbering.xml..MN.0..O..".. $. .5...6......X.=..I..q..R$..U.........K...h.......\3...R....x".uTg T..)9rK...u..J.9.}.Gh.(...9...e%W...p..9.../....Ce....N.........t. HI.:...%.....$...`.......Jv.*..;;......-..=M...b.C...Q+..k.

File Icon

Icon Hash:	74fcd0d2d6d6d0cc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2020 22:29:51.384249926 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.384336948 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.545876026 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.546088934 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.546132088 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.546397924 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.553158998 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.570435047 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.716314077 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.716357946 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.716382980 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.716406107 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.716689110 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.734467983 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.734509945 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.734534025 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.734556913 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.734822035 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.743287086 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.750194073 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.905172110 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.905536890 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.907572031 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.907740116 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.912475109 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:51.912844896 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.914340019 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:51.914751053 CEST	49691	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:52.068968058 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:52.070427895 CEST	443	49692	52.114.159.112	192.168.1.102
May 1, 2020 22:29:52.070624113 CEST	49692	443	192.168.1.102	52.114.159.112
May 1, 2020 22:29:52.076404095 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:52.219837904 CEST	443	49691	52.114.159.112	192.168.1.102
May 1, 2020 22:29:52.220128059 CEST	49691	443	192.168.1.102	52.114.159.112

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2020 22:29:46.111237049 CEST	56942	53	192.168.1.102	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 1, 2020 22:29:46.134962082 CEST	53	56942	8.8.8.8	192.168.1.102
May 1, 2020 22:29:51.338521957 CEST	56097	53	192.168.1.102	8.8.8.8
May 1, 2020 22:29:51.370568037 CEST	53	56097	8.8.8.8	192.168.1.102
May 1, 2020 22:30:27.289087057 CEST	65008	53	192.168.1.102	8.8.8.8
May 1, 2020 22:30:27.312757015 CEST	53	65008	8.8.8.8	192.168.1.102
May 1, 2020 22:30:32.316766977 CEST	51342	53	192.168.1.102	8.8.8.8
May 1, 2020 22:30:32.359975100 CEST	53	51342	8.8.8.8	192.168.1.102

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 1, 2020 22:29:51.370568037 CEST	8.8.8.8	192.168.1.102	0xc7b4	No error (0)	skypedataprdcolwus01.cloudapp.net		52.114.159.112	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: WINWORD.EXE PID: 2308 Parent PID: 788

General

Start time:	22:29:41
Start date:	01/05/2020
Path:	C:\Program Files (x86)\Microsoft Office\root\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Root\Office16\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x950000
File size:	1966368 bytes
MD5 hash:	EFDE23ECDF60D334C31AF2A041439360
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	64C270E2	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$st1234.docx	success or wait	1	64B64024	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\test1234.docx	2993	241	success or wait	1	64B64024	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	64B64F25	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	64B64F25	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\389E3	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	success or wait	1	64B64024	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Shared Tools\Panose	Cambria Math	binary	02 04 05 03 05 04 06 03 02 04	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\389E3	389E3	binary	04 00 00 00 04 09 00 00 29 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 4C 00 79 00 6E 00 6E 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 16 36 2E 55 F7 1F D6 01 E3 89 03 00 E3 89 03 00 00 00 00 00 1F 05 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	64B64024	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	File Path	unicode	C:\Users\user\AppData\Local\Temp\imgs.htm	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Datetime	unicode	2020-05-01T22:30	success or wait	1	64B64024	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Reading Locations\Document 0	Position	unicode	1 0	success or wait	1	64B64024	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Resiliency\DocumentRecovery\31138	31138	binary	04 00 00 00 04 09 00 00 23 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 4C 00 79 00 6E 00 6E 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 74 00 65 00 73 00 74 00 31 00 32 00 33 00 34 00 2E 00 64 00 6F 00 63 00 78 00 08 00 00 00 74 00 65 00 73 00 74 00 31 00 32 00 33 00 34 00 00 00 00 00 01 00 00 00 00 00 00 00 D7 DC 4D 3E F7 1F D6 01 38 11 03 00 38 11 03 00 00 00 00 00 1F 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00	04 00 00 00 04 09 00 00 23 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 4C 00 79 00 6E 00 6E 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 74 00 65 00 73 00 74 00 31 00 32 00 33 00 34 00 2E 00 64 00 6F 00 63 00 78 00 08 00 00 00 74 00 65 00 73 00 74 00 31 00 32 00 33 00 34 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 38 11 03 00 38 11 03 00 00 00 00 00 1F 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00	success or wait	1	64B64024	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00				

Disassembly