ID: 882702
Sample Name: __ EXTERNAL __ .eml
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 17:15:18
Date: 06/06/2023
Version: 37.1.0 Beryl

Table of Contents

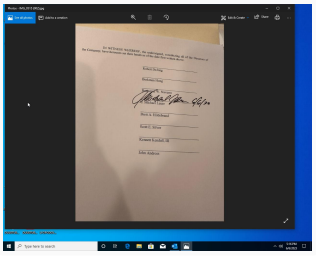
Windows Analysis Report

__ EXTERNAL __ .eml

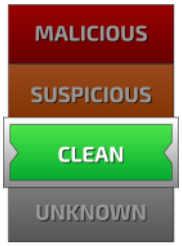
Overview

General Information

Sample Name:	__ EXTERNAL __ .eml
Analysis ID:	882702
MD5:	0e7c2724d4a7…
SHA1:	fd2013b09273f…
SHA256:	0ed963d90609…



Detection

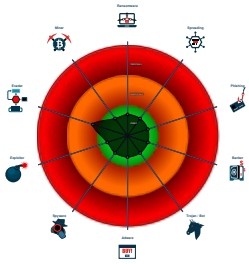


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Stores large binary data to the regis…

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 3604 cmdline: C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /eml "C:\Users\user\Desktop__ EXTERNAL __ .eml MD5: CA3FDE8329DE07C95897DB0D828545CD)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

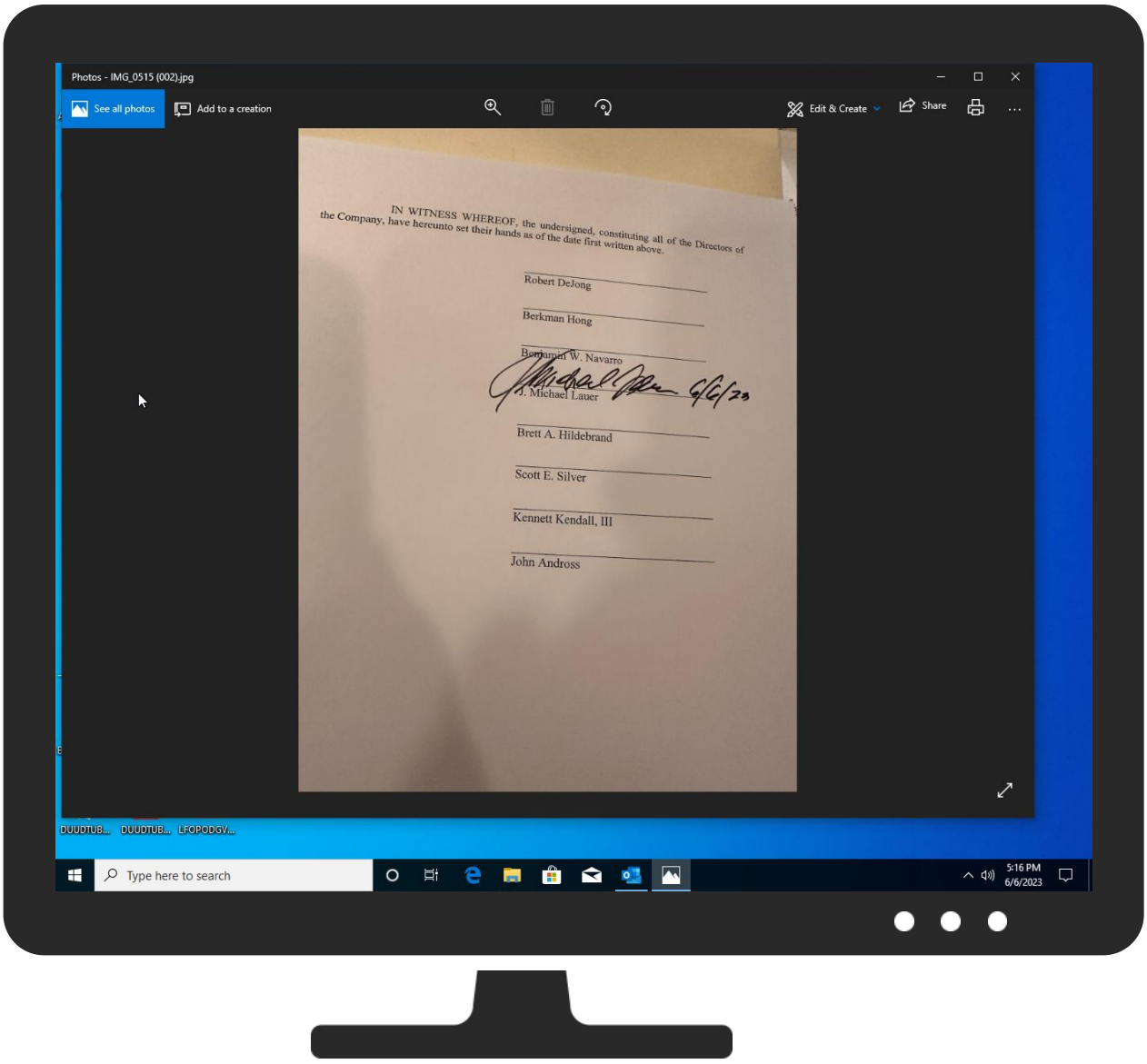
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Modify Registry	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	2 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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

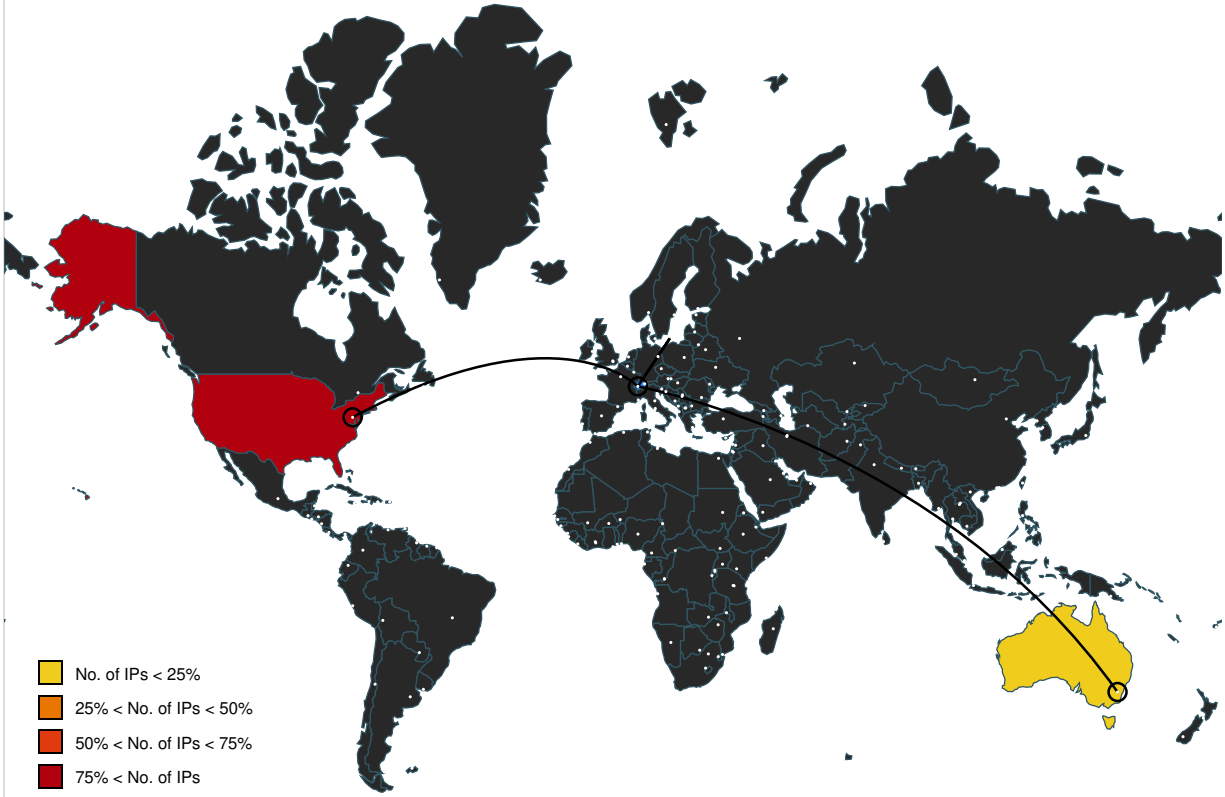
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.113.194.132	unknown	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.13.62	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
1.1.1.1	unknown	Australia		13335	CLOUDFLARENETUS	false
52.109.76.225	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.44.89	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.109.28.62	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	882702
Start date and time:	2023-06-06 17:15:18 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	9

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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	__ EXTERNAL __ .eml
Detection:	CLEAN
Classification:	clean0.winEML@1/15@0/60
Cookbook Comments:	• Found application associated with file extension: .eml

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, Microsoft.Photos.exe, SIHClient.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 52.109.44.89, 52.109.13.62, 52.113.194.132, 52.109.76.225, 52.109.28.62
- Excluded domains from analysis (whitelisted): ecs.office.com, odc.officeapps.live.com, slscr.update.microsoft.com, europe.odcsm1.live.com.akadns.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, prod.roaming1.live.com.akadns.net, s-0005-office.config.skype.com, eur.roaming1.live.com.akadns.net, prod.nexusrules.live.com.akadns.net, ecs-office.s-0005.s-msedge.net, roaming.officeapps.live.com, login.live.com, s-0005.s-msedge.net, config.officeapps.live.com, officeclient.microsoft.com, ecs.office.trafficmanager.net, nexusrules.officeapps.live.com, prod.odcsm1.live.com.akadns.net
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.
- Report size getting too big, too many NtSetValueKey calls found.

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\FORMS\FRMDATA64.DAT

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	239628
Entropy (8bit):	4.112319133405674
Encrypted:	false
SSDEEP:	
MD5:	3256628B66522C46B5100CFEC3ADC250
SHA1:	58FD59611D2785D2433A953EC2B1A51C5B822037
SHA-256:	FB0A1BF80675713998A148869D59B52EABD59DF4EB49CD0AD86B570A22F3289A
SHA-512:	7813F6900E36AE7C99AE72F1BD20621F56192FF6EB755B3870D45EC95F8C4E53A9F859AFE786B44CB053AE846D0300B2E114989E3FD6CA93CCC7E37F70E8889
Malicious:	false
Reputation:	low
Preview:	TH02..... ....w).....SM01(.....@n.v).....IPM.Activity.....h.....h.....H..h.....h.....H..h.... .....h....0.....h..... .....h.....h....@.....h....H.....0....T.....d.....2h.... .....k.....!h..... h.....#h....8..... ..$h.....<.....''h.....'h.....1h....<.....0h....8...../h....l.....H..h....p.....-h.....+h..... .....F7. .....FIPM.Activity....Form....Standard....Journal Entry...IPM.Microsoft.FolderDesign.FormsDescription.....F.k.....1122110020000000....Microsoft...This form is used to create journal entries.....kf..... .....&.....(.....(...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\FAB46BF9-2267-4C1D-9AD7-3A45B7558D0C

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	157131
Entropy (8bit):	5.350004382562505
Encrypted:	false
SSDEEP:	
MD5:	5A14214763BE836B4092821CD3C52737
SHA1:	DA9C95C8066157026C37C2C9CF7A70DD856828D4
SHA-256:	BEEE54A31CFDA1B2299DD1FE67BCFB9E7234A94C2018C9CA36122FC679B7B428
SHA-512:	7144EBB2F44191188FAE56442BC0A6ECF22AC9EDE146C01ECEE4163C096B564199DF0D3A4370E5BAAE9D6CE4EE87F971C182AC137CB2DD41288FFAE208E6EFF0

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="2023-06-06T15:15:51">.. Build: 16.0.16530.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>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:au thentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:h eaderValue="Passport1.4 from-PP='{}&p=" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAu thorityU

C:\Users\user\AppData\Local\Microsoft\Office\16.0\outlook.exe_Rules.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	272239
Entropy (8bit):	5.128004907390372
Encrypted:	false
SSDEEP:	
MD5:	A1B3E56B290A743CE977C6209FA39C85
SHA1:	839711A2FB9079890925E4E1A4F55A13853BD065
SHA-256:	3E12BC7577C65A23B2ACFB2B309C3C271709C63C3F12D5A7D0D0B1557A805B58
SHA-512:	D7B5086D46CC010FA9CB3ECA1ECCBD698C19012391022F03B557AC36E1EB107AB0C984918787C6574E19357E9DB2B745A813ED942CFAB8AD0A2C78AC277586 C9
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d 448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159 " G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L> <R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N=" ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

C:\Users\user\AppData\Local\Microsoft\Office\OTele\outlook.exe.db-shm

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.05925320230744877
Encrypted:	false
SSDEEP:	
MD5:	8FCF381F01131A1137D57E7B0589459B
SHA1:	05378FD171165BA66D791B21D7EF82885655BC9D
SHA-256:	C79AC558C6C5123D90B74E7A3CDE6FDE3966A39EBCA089AA72D5EBDE94FB1271
SHA-512:	0DE5914CF847067F2247A593B9E6D0558ED9D246489385210C7839FA1ED5A51AFA4BD975D6935B74E9C9B68B2949C8F43B99422896B2C722BC27941998AC9BB8
Malicious:	false
Reputation:	low
Preview:	..-.....&H[.0..$.{.W..?..".Ze..-.....&H[.0..$.{.W..?..".Ze..... ....

C:\Users\user\AppData\Local\Microsoft\Office\OTele\outlook.exe.db-wal

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	SQLite Write-Ahead Log, version 3007000
Category:	dropped
Size (bytes):	111272
Entropy (8bit):	2.738287838721946
Encrypted:	false
SSDEEP:	
MD5:	F84C88A27AA1EB11ECA61397DE267F4B
SHA1:	7E490CB2878082B36B05AF54E7710862243BD90F
SHA-256:	55A452E9721DDB6BDF3BFD102DE0CBD3D8539E9DE046004C9769AF0991914416

SHA-512:	22DADE4A9FBD93E8F271E7463CE3D05F2EA20C760690CD975F0F331C4E03AB987D8733CCFCB9039F1C2882AD1592F4DB7A3822C05484BA0B51A266E02AB6896
Malicious:	false
Reputation:	low
Preview:	7....-.....$.{.W..?.b.7.y.3.....$.{.W..?./.....SQLite format 3.....@ ....#.....g..... ....

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.844173720473874
Encrypted:	false
SSDEEP:	
MD5:	9828D7FC7F3A08F45830E748CA1152E9
SHA1:	7B812D2FDBCD6C3642BBBDF0760150A368F36011
SHA-256:	466E156C255544074444C1C31500066E6FBB385DAA0F835C890B81FC031756B7
SHA-512:	44837F668A21486C28C288751DCEC9853931F678E6508C64D735ED3B08135D00A2753394E11FDA578D8966736BA2B9810CDCCC262CF570699B850F0187062D2E
Malicious:	false
Reputation:	low
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".C.J.1.m.u.g.S.o.z.s.S.9.x.S.Z./.Q.v.O.c.+.E.J.4.u.2.c.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".g.M.K.C.K.p.K.Y.2.Q.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.E.p.7./.F.I.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	5938
Entropy (8bit):	4.00994939360995
Encrypted:	false
SSDEEP:	
MD5:	725266AA0C084D4FA82800B3DF6D3DA3
SHA1:	9F20918BD136FF852F0813F4CB87139ACAB885EE
SHA-256:	5D1423232A8BDC5771EABABF03F6073C2686B3A6CACB66E645C748868DA879BB
SHA-512:	D5D040DC3CDABC995DEFF66437EBB8B0EF03A47DB184DFFAC955B0C38A5284C73F44B5FE79D0A0F14043207177323B11FEE914ED6B8CD43211418B7C2420D2F3
Malicious:	false
Reputation:	low
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".V.H.X.L.G.R.5.H.j.D.k.3.C.i.F.b.L.a.m.K.N.+.n.c.g.T.0.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".I.g.w.F.Q.I.u.3.2.g.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.E.p.7./.F.I.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\9aad439831564ef9f88438a70a63c87e26ef3852.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	3902
Entropy (8bit):	3.9887251261836334
Encrypted:	false
SSDEEP:	
MD5:	C60EF5AD056E507E2AC0135BCAA97F72
SHA1:	C4B3EC254D5B9BF6E241A91AF9449575C7713A58
SHA-256:	2A1F4DB4486741AD8568750838DE690950FA446D62751F098C88B519806E3432

SHA-512:	297502565A036C3BCAA62BAF7F8EFF2388C3E4739AB618E93EACA3E1BACADBADCFE4EA6F6358C97975CECE89C91BCABC754D119D8F88A153B840E9417CFE0CB0
Malicious:	false
Reputation:	low
Preview:	{."T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:{."H.e.a.d.e.r.".:{."O.b.j.e.c.t.T.y.p.e.".:".T.o.k.e.n.R.e.s.p.o.n.s.e.".,".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:2.,".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:1.},.,".O.b.j.e.c.t.D.a.t.a.".:{."S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:{."R.e.q.u.e.s.t.I.n.d.e.x.".:{."T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".m.q.1.D.m.D.F.W.T.v.n.4.h.D.i.n.C.m.P.I.f.i.b.v.O.F.I.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:{."T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".Z.p.x.k.E.I.q.Y.2.Q.E.=.".},.,".S.t.a.t.u.s.".:{."T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:f.a.l.s.e.,".V.a.l.u.e.":.".A.w.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:{."T.y.p.e.".:".I.n.l.i.n.e.B.y.t.e.s.".,".I.s.P.r.o.t.e.c.t.e.d.".:t.r.u.e.,".V.a.l.u.e.":.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.E.p.7./.F.I.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\PSFUO2BE\IMG_0515 (002).jpg:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E98
Malicious:	false
Reputation:	low
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\PSFUO2BE\IMG_0515.jpg

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 20, Exif Standard: [TIFF image data, big-endian, direntries=5, xresolution=74, yresolution=82, resolutionunit=2], baseline, precision 8, 1536x2048, components 3
Category:	dropped
Size (bytes):	453765
Entropy (8bit):	7.9297759229662415
Encrypted:	false
SSDEEP:	
MD5:	C99BA0F556028AF24A4D4C20C7B408F2
SHA1:	D77AC06E1A0955D940D1643DF36A9FC1EDFA37F7
SHA-256:	742869086D3ADCB7578EBE7FCCC58AF392FA0A5858784752E5DC4C35C53DDFD5
SHA-512:	11B6D8EB43E13030724AE8B8DAA1FD01535CC3EFF4D88AD3632E276F9CB47E3BB06EAB37D19C7A4DCEA199E28CFB4B99D7F08A9E83AA9FB1DE7C3BE5CEA3418F
Malicious:	false
Reputation:	low
Preview:	......JFIF.....,..AMPF....Exif..MM.*.....J.....R.(.....i.....Z.....H.....H.....0221.....0100.....XMPF.MM.*.....0100..... ...2.....AROT.....k.....(...5...@..cL...X...c...n..&z.....O.....T.....$...>...U..Ek...|..].....!.....8...&.....=$...+...2...:...F...Y..Jm...{.....l.....7...z...h...'&...-...4...>..oO...b...l...r..6y.....c.....a.....u.....4...Q...C...4"..k)...1..'?...P...^...e..Xm...t..d|.....Z.....{.....t...l.....m...g.....#...-...6...?...H...R..`[...d...m..,w.....x.....`....."....

C:\Users\user\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20230606T1715490538-3604.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	DIY-Thermocam raw data (Lepton 2.x), scale 0-0, spot sensor temperature 0.000000, unit celsius, color scheme 0, calibration: offset 0.000000, slope 134217728.000000
Category:	modified
Size (bytes):	241664
Entropy (8bit):	4.85520777764295
Encrypted:	false
SSDEEP:	
MD5:	7682DFD6A7956FAEDAA8EEEAB591659B
SHA1:	1BA13BAAB2A660BAF8F89D5F2FC75774266AE6DB
SHA-256:	CA29C3FF93D3FF7044EBCB11FE8F2672C542AC187B66E0AE21D10931E8D69013
SHA-512:	9D13C07503906922D4D9686BA330F9FB0F58D95DAB15461EBFC9F370AFAFA9DD6DC2EE53800FD7619ED5C711792FFBCDDA89BF1E709666543314C7B8C781D25

Malicious:	false
Reputation:	low
Preview:	.....f.....+.....G.....Zb..2.....@.t.z.r.e.s...d.l.l.,.-.3.2.2..... .....@.t.z.r.e.s...d.l.l.,.-.3.2.1.....+.....v.2._.O.U.T.L.O.O.K.:.e.1.4.:.d.d.d.3.7.b.9.4.f.7.7.7.4.1.c.9.9.7.5.2.f.4.c.d.9 .0.3.f.e.f.8.8...C.:\.U.s.e.r.s.\.e.y.u.p.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.O.u.t.l.o.o.k. .L.o.g.g.i.n.g.\.O.U.T.L.O.O.K._.1.6._.0._.1.3.9.2.9._.2.0.3.8.6.-.2.0.2.3.0.6.0.6 .T.1.7.1.5.4.9.0.5.3.8.-.3.6.0.4...e.t.l.....P.P.....+..... .....

C:\Users\user\AppData\Local\Temp\olk7A73.tmp

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	322693
Entropy (8bit):	7.918998207445186
Encrypted:	false
SSDEEP:	
MD5:	544FD9D2F1A77DDB016E57265BB511F1
SHA1:	3994CDD70F87E932A59C91355CD4C0C199B4074B
SHA-256:	790D3AD63EDC00B7B4F38E5A489EE6460BBF2DB93200FD43433C2EC3920280CB
SHA-512:	5947B4A077698CC265599EF7089E635C72E941612E93A5D47685610315C060950319F5360D7314D1FD975D04C588541DBA18395AC460030810B3E38D44C924FE
Malicious:	false
Reputation:	low
Preview:	..A....."....zTa.x.51.....W.z.....AR8.oc..P....g.GJ....OJ..T.../.?*~.P63..+..O.j...gaM...x.r..."..y.s..n?...H.A^.....J@{).O L..q..O4.....0.P.Q.c$qL,C..UD...r....`.....=8.}T..... .Ln.....T..8.t..`zu.OjB...N:{W.[ad?&...N.0;T,..I.Z.|.';}(.+mBX.U}..t...pMD....4.....1.{.....R.../OC@.7.H.....`.....*..>.Zt../.8. D.....>~.{...q...3.8..Ae..#...]....:.,x..^\".q.t...)....rW.. dB..wP..>..&.d..-.....*...*.i.i.b..N....E....6c.H...d|.I5H.=*n....#.O.B..(.s.|..=EM.W...<..C.]LD.[.+..8X.`.p.*x.8#.*.BUX..b..9.~.%.....zqB)..5.o....{T....h.=:b.3.qQu...R.s...t...#.Jy>..." ...4.z....b....@..&....2.c.p\.<.`Lv..i...v.....!*...2.....=i.\s.P.&.G.MBy..L..j|D.....i:...I..... dSY.~..p.=(...q....q.1.i....aO|~.....q..SN...0$-.v..sM.N.h....4.~z..TI..<...R(x<.....n. =)..a.....8.....v..P.z...)..N.....s.....P@..'..4..Z.a...)..0.....E._.(.d.F*#.8...i.`..@.m.).1F..@.=3@....G#.JNN1.=.=0(..g.N....Jb.Q.T....9.v.I

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	14
Entropy (8bit):	2.699513850319966
Encrypted:	false
SSDEEP:	
MD5:	09B7FD4F63059FB967C6CF0D36AF99A4
SHA1:	BDFABECF4B7BB2A0A08C69150C770C45C5A81303
SHA-256:	AF2F74E5947D19590946BA404ED7FBEBF59A85BBF83354E24015FA9729A2808C
SHA-512:	AEAC2A4520FD462248176C30E094269F6A285E1ADF731912E62E24B88EA792E2E42E92498FA944F677AC84758C41DFEA044216A96F6FD204E8CEC82E42351B4E
Malicious:	false
Reputation:	low
Preview:	..e.y.u.p.....

C:\Users\user\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	Microsoft Outlook email folder (>=2003)
Category:	dropped
Size (bytes):	2302976
Entropy (8bit):	2.5394033450954647
Encrypted:	false
SSDEEP:	
MD5:	4A206EE14819FAC2EE32E7E41B7CDE81
SHA1:	7FEBB31113B43309CC232D7AEC203ADCEBE95628
SHA-256:	737114B4A913151D19FB7D65DBDF0F7FD5DAE468F446DD58CD40A83FB90EB36E
SHA-512:	BD989D5E93CA613F305D972CA78A7213E1FF8F65B30FBED3747B458E2733D7D37C4AB56FE52187B3CB436A21D2AA3EB868509A76189EFA5E5B44747B0EC8FAF2
Malicious:	false
Reputation:	low

Preview:	!BDN....SM.....x....y.....|.....@.....@...@.....@.....$#.....D.....w.....{..... ....O..... .....

C:\Users\user\Documents\Outlook Files\~Outlook Data File - NoEmail.pst.tmp	
Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	524288
Entropy (8bit):	7.573989967506226
Encrypted:	false
SSDEEP:	
MD5:	CFBB388E98E1D7B3423EA9BC25A3F49F
SHA1:	BBA6CE23DB1C705CCF03233C097B8117D9649C07
SHA-256:	7ABCC49CF24AE7D0B4EAFFF3BCCB31BEF9D33A6803C865ACCCC499189BAA8ECF
SHA-512:	02B906A045B0AB2ACC9D3D64939408051FEC4AFF505F111C52E93E9FE1F29CDC9956A2138CD99B881A31367693A01999FAC44B032DC9B3903CB9EDDBB404AE1
Malicious:	false
Reputation:	low
Preview:	Q..!C.....i.#.....#.!BDN....SM.....x....y.....|.....@.....@...@.....@.....$#..... D.....w.....{..... .....O.....i.#.....B.....#.....`*..`..... .....

Static File Info

General

File type:	RFC 822 mail, ASCII text, with CRLF line terminators
Entropy (8bit):	6.024272233233932
TrID:	• E-Mail message (Var. 5) (54515/1) 100.00%
File name:	__ EXTERNAL __ .eml
File size:	625619
MD5:	0e7c2724d4a7fd642a09152fb8bdf975
SHA1:	fd2013b09273fa3a55c0a956840e135cbb2448b2
SHA256:	0ed963d906095c42fabc5b2ced49f3354fa273ef564b9be8b6aeb23edcfcb032
SHA512:	736ea6438275c79086209f15aef8ea3fd0f7ce5381fa161c04b906aa4c5e750cf824d0d4f78f6caa91fdd98f6bc2930e1d0935c7396d55d8f92607fc29e88dbc
SSDEEP:	12288:56KdzfEMJyijvwLO1RMXrFuqWmshpPDF3x73MXXKv2:564DD8LOjirFuHNprFhoXXKu
TLSH:	C8D41274CEEBAFED4B0189E7251DB876548F09C319C642EF4388C17A34E0735CA6A5A7
File Content Preview:	Received: from BN9PR03CA0750.namprd03.prod.outlook.com.. (2603:10b6:408:110::35) by PH0PR17MB5836.namprd17.prod.outlook.com.. (2603:10b6:510:123::12) with Microsoft SMTP Server (version=TLS1_2,.. cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6455

Static Mail

General

Subject:	** EXTERNAL **
From:	2623478468@mms.att.net
To:	Alison Prince <Alison.Prince@creditone.com>
Cc:	
BCC:	
Date:	Tue, 06 Jun 2023 14:33:16 +0000
Communications:	
Attachments:	• IMG_0515.jpg

Headers

Key	Value
Received	from zbot2ammsc01nfe002.wnsnet.bot2a.tci.att.com ([107.79.70.28]) by bizsmtp with ESMTP id 6XdTqA4x6TM7N6XkKqL04P; Tue, 06 Jun 2023 09:33:17 -0500
Authentication-Results	spf=pass (sender IP is 44.202.169.45) smtp.mailfrom=mms.att.net; dkim=pass (signature was verified) header.d=mms.att.net;dmarc=bestguesspass action=none header.from=mms.att.net;

Key	Value
Received-Spf	Pass (protection.outlook.com: domain of mms.att.net designates 44.202.169.45 as permitted sender) receiver=protection.outlook.com; client-ip=44.202.169.45; helo=omta046.useast.a.cloudfilter.net; pr=C
Dkim-Signature	v=1; a=rsa-sha256; c=relaxed/simple; d=mms.att.net; s=EMG20171113; t=1686061997; bh=dG9Rrr5vX82CZzZILGpBT5BAGhFgg7/gJmzx7szLEvk=; h=In-Reply-To:To:From:Date; b=eV1VcTEYiNRLy5+TbqZxnSFIe2ql2NO37P8x4RhaYuQbQdGfw+ZKO3QXf4YjqDuyp VDRdMAyVoDFUvRt4JSOyCbxfVTTaOdctCzcGBwFjO7cWJg/yTZSfDF/uGeq7CQt0y9 DmLVeoEfL6O8h/qNhpNjnGmrqpy+ab2rNpJu9hVE2dtXMBJOlgsYEnz7G97e79Ju5l hOXMnDmbltaXc7IYph13OFRwdMWUINmcpz4sBO6MbB2Zm3+bovDNwP0+Ug8XQA63pj z7R4e3cn9zy8OlL67lQbxst4rHnqSkwDql74QkcRrj/xipdkWezB3TlCUipU3FvWkO tMr833q1PjVmg==
X-Authority-Analysis	v=2.4 cv=D7xUl9dj c=1 sm=1 tr=0 ts=647f43ad a=4KXCUzhBzoMCTCvOBLK/Fg==:117 a=Bx2Cwp6ym4y6W6eL0VYUQA==:17 a=s5jvgZ67dGcA:10 a=of4jigFt-DYA:10 a=ywgSPo00G5OZj1TEPAwA:9 a=KQqxNPgzF0kA:10
Message-Id	<6XdTqA4x6TM7N6XkKqL04P@txt.att.net>
In-Reply-To	<583726506.215142278.1686061996565.JavaMail.nems@zbot2ammsc01nfe002>
X-Mms-Message-Type	m-send-req
X-Mms-Transaction-Id	1686061983-0
X-Mms-Mms-Version	1.2
To	Alison Prince <Alison.Prince@creditone.com>
From	2623478468@mms.att.net
Date	Tue, 06 Jun 2023 14:33:16 +0000
X-Mms-Sender-Visibility	Show
Content-Type	multipart/mixed; boundary="----sinikael-?=_1-16860621853150.2634394059019074"
MIME-Version	1.0
X-Cmae-Envelope	MS4xfDogK+8NYLH+ONzHxOLPaisfGmCeDy/cLMY50PAx7lyzrdNydEc7LqCH9FtWb64aFyULC1WnMYZcJu/u8sph5B/n1E8C6NL8stHTUEqoDAmVOIQecMuP nH0BTU9kZkKCmiepUCjCxSQBo1om33tjryLxeBM/IzbBBHDMThcQHNPiRnvxcouOmeJTCk7y20/9Dlfh5xL/leEDl9lR+K5OMfSMLP+Ern908izEicYf/Spl
Return-Path	2623478468@mms.att.net
X-Ms-Exchange-Organization-Expirationstarttime	06 Jun 2023 14:33:18.0495 (UTC)
X-Ms-Exchange-Organization-Expirationstarttimereason	OriginalSubmit
X-Ms-Exchange-Organization-Expirationinterval	1:00:00:00.0000000
X-Ms-Exchange-Organization-Expirationintervalreason	OriginalSubmit
X-Ms-Exchange-Organization-Network-Message-Id	7ef91565-5fcc-4bc7-dafd-08db669af856
X-Eopattributedmessage	0
X-Eoptenantattributedmessage	d48cfd66-1099-47e8-898f-6de8401f42b8:0
X-Ms-Exchange-Organization-Messagedirectionality	Incoming
X-Ms-Publictraffictype	Email
X-Ms-Traffictypediagnostic	BN7NAM10FT105:EE_|PH0PR17MB5836:EE_
X-Ms-Exchange-Organization-Authsource	BN7NAM10FT105.eop-nam10.prod.protection.outlook.com
X-Ms-Exchange-Organization-Authas	Anonymous
X-Ms-Office365-Filtering-Correlation-Id	7ef91565-5fcc-4bc7-dafd-08db669af856
X-Ms-Exchange-Atpmessageproperties	SA|SL
Subject	** EXTERNAL **
Content-Transfer-Encoding	7bit

File Icon

Icon Hash:	46070c0a8e0c67d6