ID: 756146
Sample Name: Fwd_ Payment_Confirmation.msg
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 17:48:54
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Fwd_ Payment_Confirmation.msg 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Yara Signatures 3
HTML 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Phishing 4
Mitre Att&ck Matrix 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
Private 7
General Information 7
Warnings 7
Created / dropped Files 7
C:\Users\alfredo\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20221129T1749280939-2572.etl 7
C:\Users\alfredo\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20221129T1750110559-2124.etl 8
Static File Info 8
General 8
File Icon 8

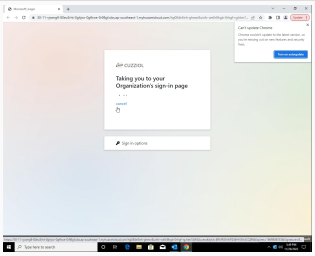
Windows Analysis Report

Fwd_ Payment_Confirmation.msg

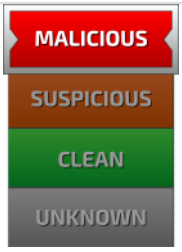
Overview

General Information

Sample Name:	Fwd_ Payment_Confirmation.msg
Analysis ID:	756146
MD5:	4cfb650a9f6716e..
SHA1:	78b9efaf0c5436a..
SHA256:	25a3dbaae7f894..



Detection



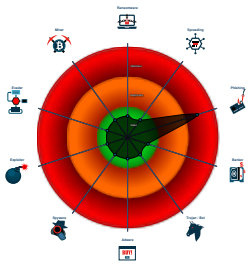
HTMLPhisher

Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Misleading page title found
- Yara detected HtmlPhish10
- HTML body contains low number of …
- Invalid T&C link found
- No HTML title found

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 2572 cmdline: C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" /f "C:\Users\alfredo\Desktop\Fwd_ Payment_Confirmation.msg MD5: CA3FDE8329DE07C95897DB0D828545CD)
- chrome.exe (PID: 6868 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --start-maximized --single-argument C:\Users\alfredo\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\IRQ7T0GH\Payment_Confirmation.hTm MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
  - chrome.exe (PID: 6164 cmdline: "C:\Program Files\Google\Chrome\Application\chrome.exe" --type=utility --utility-sub-type=network.mojom.NetworkService --lang=en-US --service-sandbox-type=none --mojo-platform-channel-handle=2068 --field-trial-handle=1792,i,11491005883064114037,15152354911059901904,131072 --disable-features=OptimizationGuideModelDownloading,OptimizationHints,OptimizationTargetPrediction /prefetch:8 MD5: 7BC7B4AEDC055BB02BCB52710132E9E1)
- OUTLOOK.EXE (PID: 2124 cmdline: "C:\Program Files\Microsoft Office\Root\Office16\OUTLOOK.EXE" -Embedding MD5: CA3FDE8329DE07C95897DB0D828545CD)
- **cleanup**

Yara Signatures

HTML

Source	Rule	Description	Author	Strings
92753.0.pages.csv	JoeSecurity_HtmlPhish_10	Yara detected HtmlPhish_10	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Phishing

Misleading page title found

Yara detected HtmlPhish10

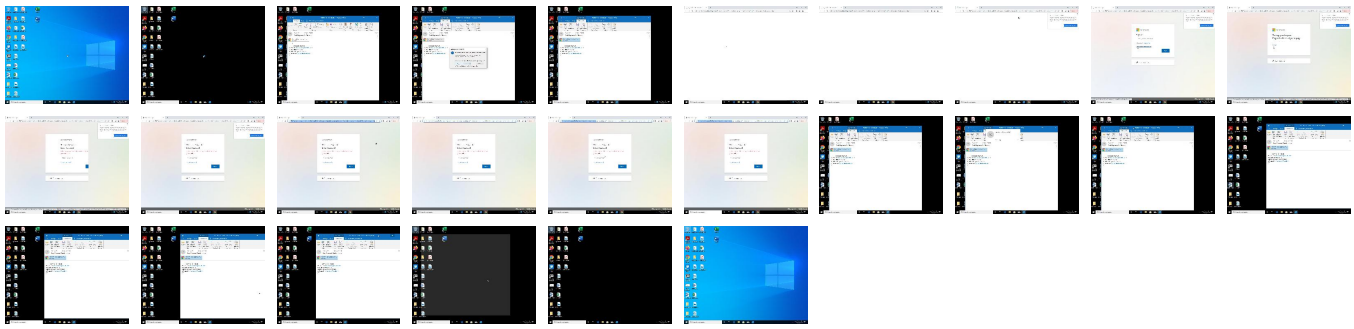
Mitre Att&ck Matrix

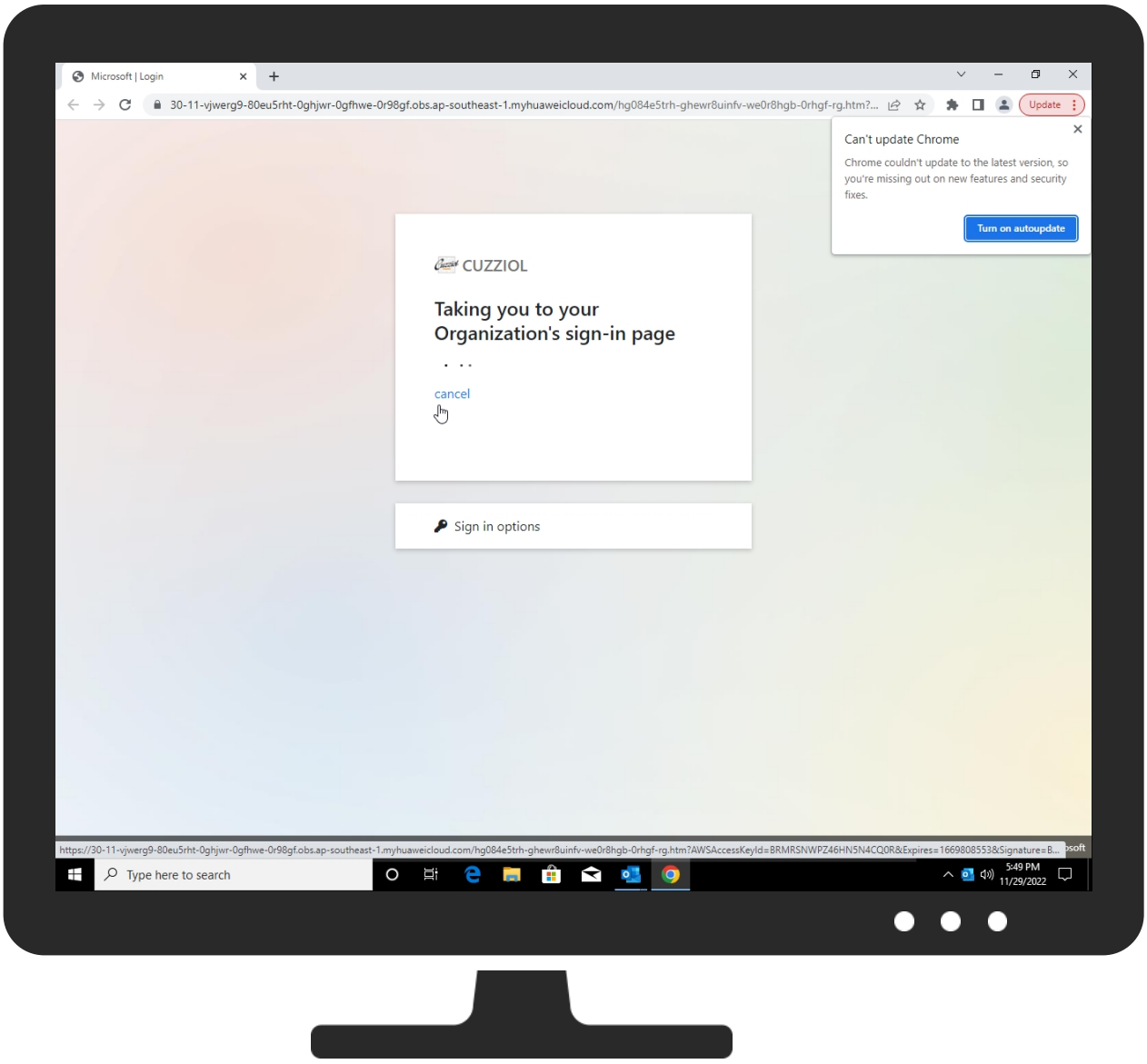
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 Extra Window Memory Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	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	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
part-0017.t-0009.t-msedge.net	0%	Virustotal		Browse
30-11-vjwerg9-80eu5rht-0ghjwr-0gfhwe-0r98gf.obs.ap-southeast-1.myhuaweicloud.com	4%	Virustotal		Browse
part-0017.t-0009.fbs1-t-msedge.net	0%	Virustotal		Browse

URLs

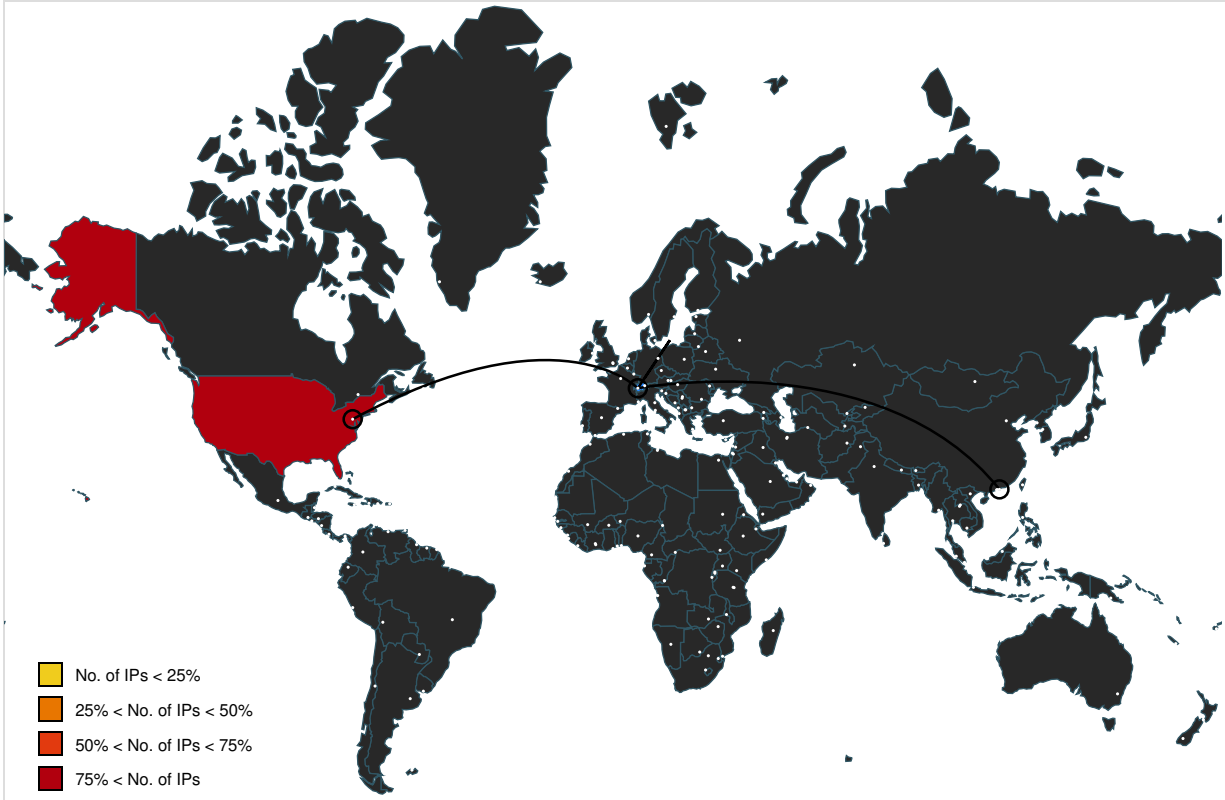
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
d26p066pn2w0s0.cloudfront.net	13.224.189.75	true	false		high
part-0017.t-0009.t-msedge.net	13.107.213.45	true	false	• 0%, Virustotal, Browse	unknown
accounts.google.com	142.250.186.109	true	false		high
f8d5c6ccb462dad.cdd-ap.nexusguard.cloud	27.126.206.60	true	false		unknown
cdnjs.cloudflare.com	104.17.25.14	true	false		high
part-0017.t-0009.fbs1-t-msedge.net	13.107.219.45	true	false	• 0%, Virustotal, Browse	unknown
maxcdn.bootstrapcdn.com	104.18.11.207	true	false		high
www.google.com	142.250.186.100	true	false		high
clients.l.google.com	142.250.185.206	true	false		high
use.fontawesome.com	unknown	unknown	false		high
clients2.google.com	unknown	unknown	false		high
code.jquery.com	unknown	unknown	false		high
30-11-vjwerg9-80eu5rht-0ghjwr-0gfhwe-0r98gf.obs.ap-southeast-1.myhuaweicloud.com	unknown	unknown	false	• 4%, Virustotal, Browse	unknown
logo.clearbit.com	unknown	unknown	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.67	unknown	United States		15169	GOOGLEUS	false
142.250.185.206	clients.l.google.com	United States		15169	GOOGLEUS	false
142.250.185.68	unknown	United States		15169	GOOGLEUS	false
34.104.35.123	unknown	United States		15169	GOOGLEUS	false
172.217.16.202	unknown	United States		15169	GOOGLEUS	false
216.58.212.138	unknown	United States		15169	GOOGLEUS	false
27.126.206.60	f8d5c6ccb462dad.cdd-ap.nexusguard.cloud	Hong Kong		45474	NEXUSGUARD-AS-APNEXUSGUARDLIMITED HK	false
142.250.186.163	unknown	United States		15169	GOOGLEUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
13.224.189.75	d26p066pn2w0s0.cloudfront.net	United States		16509	AMAZON-02US	false
104.18.11.207	maxcdn.bootstrapcdn.com	United States		13335	CLOUDFLARENETUS	false
69.16.175.42	unknown	United States		20446	HIGHWINDS3US	false
13.107.213.45	part-0017.t-0009.t-msedge.net	United States		8068	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
142.250.186.109	accounts.google.com	United States		15169	GOOGLEUS	false
239.255.255.250	unknown	Reserved		unknown	unknown	false
172.64.132.15	unknown	United States		13335	CLOUDFLARENETUS	false
104.17.25.14	cdnjs.cloudflare.com	United States		13335	CLOUDFLARENETUS	false
142.250.184.202	unknown	United States		15169	GOOGLEUS	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756146
Start date and time:	2022-11-29 17:48:54 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fwd_ Payment_Confirmation.msg
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:	12
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
Detection:	MAL
Classification:	mal56.phis.winMSG@24/2@11/218
Cookbook Comments:	• Found application associated with file extension: .msg

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe
- Excluded IPs from analysis (whitelisted): 142.250.185.67, 34.104.35.123, 142.250.184.202, 69.16.175.42, 69.16.175.10, 172.64.132.15, 172.64.133.15, 172.217.16.202, 142.250.186.99, 142.250.186.163
- Excluded domains from analysis (whitelisted): fs.microsoft.com, odc.officeapps.live.com, login.live.com
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

C:\Users\alfredo\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20221129T1749280939-2572.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data

Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.678242832905412
Encrypted:	false
SSDEEP:	
MD5:	AF0AEF305F3E769721F3770A7E3B2DF9
SHA1:	DBEAA70EAD35B41946DE72D24254810423598189
SHA-256:	E8A40504CE173543748F2A9E8FAFBAD7370804AB79C5389D48C85CA55F122A34
SHA-512:	AFF188D39263D2F0D9CDB661D4CD101F4A8F5D92B7BF03CAAC9D97C007D78910230270298DA784F8F2006496B09DC68BF4B2A9419F581E36E2E1BAD43095FC9C
Malicious:	false
Reputation:	low
Preview:	.....I.. .....-.....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.....`9N.m.....-.....v.2._.O.U.T.L.O.O.K.:.a.0.c.:.6.6.7.7.7.b.9.a.e.6.5.e.4.2.4.5.a.d.a.6.1.9.f.f.2.9.f.6.c.3.0.1...C.:.\.U.s.e.r.s.\.a.l.f.r.e.d.o.\.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.-.2.0.2.2.1.1.2.9.T.1.7.4.9.2.8.0.9.3.9.-.2.5.7.2...e.t.l.....P.P. .....9.....

C:\Users\alfredo\AppData\Local\Temp\Outlook Logging\OUTLOOK_16_0_13929_20386-20221129T1750110559-2124.etl

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	3.6716367200007447
Encrypted:	false
SSDEEP:	
MD5:	1742896B44D33D382C7895EB52F158A6
SHA1:	90C0895B8025F17ADE7D59C179D5EDAAF4B9A675
SHA-256:	2F1F3DA5ADC7F382A06899874ABDF8BFFD37D7503A64AA974B1CCB49C8D0202E
SHA-512:	7079226CEBB6C170CDFC8C15CFE2F5C95C514813A8147A7AC1311B3ACC98147AA22A33EDE2A08D0F304692BFF31EED4D5A97D63FB126A219349706C35686CB2
Malicious:	false
Reputation:	low
Preview:	.....l.....L...|5o.....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.....`9N.m.....|5o.....v.2._.O.U.T.L.O.O.K.:.8.4.c.:.7.e.4.3.7.0.b.d.d.8.6.b.4.9.5.d.b.d.4.f.d.1.6.2.2.5.9.4.9.3.9.3...C.:.\.U.s.e.r.s.\.a.l.f.r.e.d.o.\.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.-.2.0.2.2.1.1.2.9.T.1.7.5.0.1.1.0.5.5.9.-.2.1.2.4...e.t.l.....P.P.....L...|5o.....

Static File Info

General

File type:	CDFV2 Microsoft Outlook Message
Entropy (8bit):	3.30316637471596
TrID:	• Outlook Message (71009/1) 58.92% • Outlook Form Template (41509/1) 34.44% • Generic OLE2 / Multistream Compound File (8008/1) 6.64%
File name:	Fwd_ Payment_Confirmation.msg
File size:	39424
MD5:	4cfb650a9f6716e65b12578ad7357869
SHA1:	78b9efaf0c5436a04ab38b456ad935507359c7f8
SHA256:	25a3dbaae7f8949703add1c993037243f3b149c7a220eb4e5878e860976b87e0
SHA512:	c240f73d537fd7e795c3bfba37bde7b8c2795a342ecff29cb2e2ac338dd0593479578ef4e91f64c8e47cd4f6b46aedda4f8fded00a5a22cc0898a2996acdd972
SSDEEP:	768:kr2JwM4mknonBHqHBoZxAi1ZIA6gXPRb3vLfyAflj+DqPG:kS/HqHBo91Hh9lG
TLSH:	AB034A2536E58B09F27FDF3649E680C78522BCD1ED11D78F3296730F1972981A861B2B
File Content Preview:	.....>.....

File Icon

Icon Hash:	00ecb28ec8d28200