



Dragon Advance Tech

# Are there any technologies that can perfectly handle **BEC/Phishing** attacks

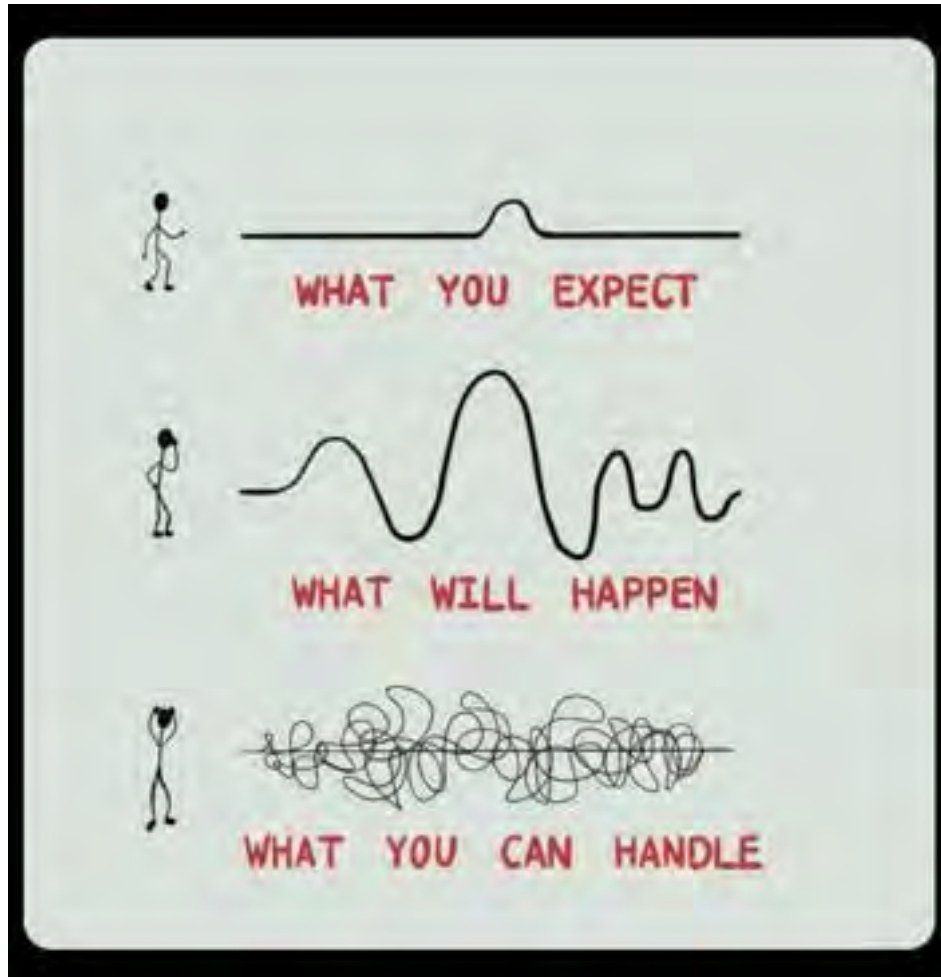
- ISSumit (2022)

# Frankie Li

- Team Lead, Incident Response
- Focus:
  - Incident Response
  - Digital Forensics
  - Malware Analysis
  - MDR
  - SOC Assessment
- Random facts:
  - Speaker in security conferences
  - University lecturer
  - Holder of some IT Security Certifications



# My original plan is to address a non-technical issue, but ...



## Russian APT29 hackers abuse Azure services to hack Microsoft 365 users



By Bill Toulas

August 18, 2022 · 11:52 AM



The state-backed Russian cyberespionage group Cozy Bear has been particularly prolific in 2022, targeting Microsoft 365 accounts in NATO countries and attempting to access foreign policy information.

Microsoft 365 is a cloud-based productivity suite predominately used by business and enterprise entities, facilitating collaboration, communication, data storage, email, office, and more.



Dragon Advance Tech

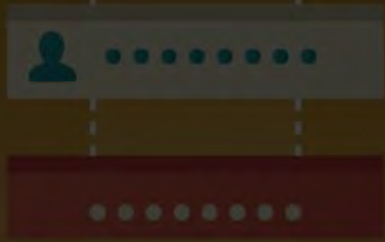
# Agenda

- What is BEC?
- Attack Tactics
  - Spoofing and Look-A-Like domains
  - Phishing with Impersonated Email
  - Account Takeover
  - ATT&CK Office 365 Matrix
- Defence and Mitigation Technologies
  - Domain Authentication: SPF | DKIM | DMARC
  - AI-enabled Anti-Spoofing and Anti-Phishing
  - Multifactor Authentication (MFA)
  - Financial Fraud Kill Chain
- Email Threat Hunting and Response
  - Protect your Identity
  - Get access to advance logs from your email infrastructure, and ...





# WHAT IS BUSINESS EMAIL COMPROMISE?



## ILLEGAL ACCESS

Criminals gain entry to a victim's devices or systems – through hacking, phishing websites, malware – then deceive the victim into transferring money into their bank account.



## SOCIAL ENGINEERING

Criminals can target their victims based on information they share on social media platforms.



## URGENT REQUEST

The criminal impersonates a supplier requesting an urgent payment or change to banking details, or a senior employee in the company with authority to authorize payments.

# What is BEC?

**#BECareful**



INTERPOL

# Why Your Executives Are Targeted

- Your boardroom and executives are the targets
- *Have access* to make a *wire transfer*
- Assigned to have *privileged access* to systems
- They are *wealthy enough* to be targeted individually
- They will *make simple mistakes* with technology easily

From: <name of the CEO> <admin@bzfinc.com>  
Sent: 26 February 2019 10:20  
To: <name of the CFO>  
Subject: Re: <name of the CFO>

Find the client's details below:  
Account name: Hanmore Securities  
Account number: 42334608  
Sort code: 60-13-10  
Bank name: NatWest Bank  
Amount: £19,210

Regards,  
<name of the CEO>  
On February 26, 2019 at 9:37 AM <name of the CFO> <<name of the CFO>@mybusiness.com> wrote:  
I am available now send me the details.

Email impersonation



# The Modern Email Threat

Identify Impersonation

Content Deception



Dragon Advance Tech



# Cybersecurity White Paper on Business Email Compromise

TLP:GREEN

*Business Email Compromise (BEC) is a form of cybercrime threat that has become more prevalent in recent years, prompting the attention and concern of businesses and organizations worldwide. More than US\$195.3 million was defrauded from companies in Hong Kong and overseas in the first 10 months of 2018, and the trend will likely keep growing in 2019.*

*The most common path for the stolen money is through a wire transfer to Hong Kong or China; this makes swift recovery of the money an almost impossible task for foreign victims if no quick intervention by domestic law enforcement.*

*As a quick reference guide to help Hong Kong organizations select their anti-phishing or BEC solutions, Dragon Advance Tech reviewed several common commercial solutions to defend against BEC threats.*





# Use Case for Microsoft 365 Incident Response on Business Email Compromise

A field guide for deploying of Microsoft Sentinel's Analytic Rules, Workbooks, and Logic Apps for BEC investigators

## What is Business Email Compromise (BEC)?

According to the 2021 Internet Crime Report<sup>1</sup> (IC3) from the FBI, BEC/EAC (Email account compromise) has defined **a sophisticated scam targeting both businesses and individuals performing transfers of funds**. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized funds transfers.

The FBI reported<sup>2</sup> on May 4, 2022, that **\$43 billion in scams** continue to grow and evolve, targeting small local businesses to more giant corporations, and found **a 65% increase** in identified global exposed losses during the COVID-19 pandemic. Even though INTERPOL<sup>3</sup> and US DOJ<sup>4</sup> announced the arrest and charging of some prominent fraudsters, phishing scam activities are **expanding in Hong Kong**, especially among the local office of investment funds. On March 22, 2022, the Securities and Future Commission ("SFC") published circular<sup>5</sup> about BEC duping unwary staff of licensed corporations (LCs) into sending money and sensitive information.

Tools: <https://github.com/DATCResearch/Sentinel-UseCase-BEC365-IR>

## 2021 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	123,972	Government Impersonation	11,335
Non-Payment/Non-Delivery	82,478	Advanced Fee	11,034
Personal Data Breach	51,829	Overpayment	6,108
Identity Theft	51,629	Lottery/Sweepstakes/Inheritance	5,991
Extortion	39,360	IPR/Copyright and Counterfeit	4,270
Confidence Fraud/Romance	24,299	Ransomware	3,729
Tech Support	23,903	Crimes Against Children	2,167
Investment	20,561	Corporate Data Breach	1,287
BEC/EAC	19,954	Civil Matter	1,118
Spoofing	18,527	Denial of Service/TDoS	1,104
Credit Card Fraud	16,750	Computer Intrusion	979
Employment	15,253	Malware/Scareware/Virus	810
Other	12,346	Health Care Related	578
Terrorism/Threats of Violence	12,346	Re-shipping	516
Real Estate/Rental	11,578	Gambling	195

## 2021 Crime Types continued

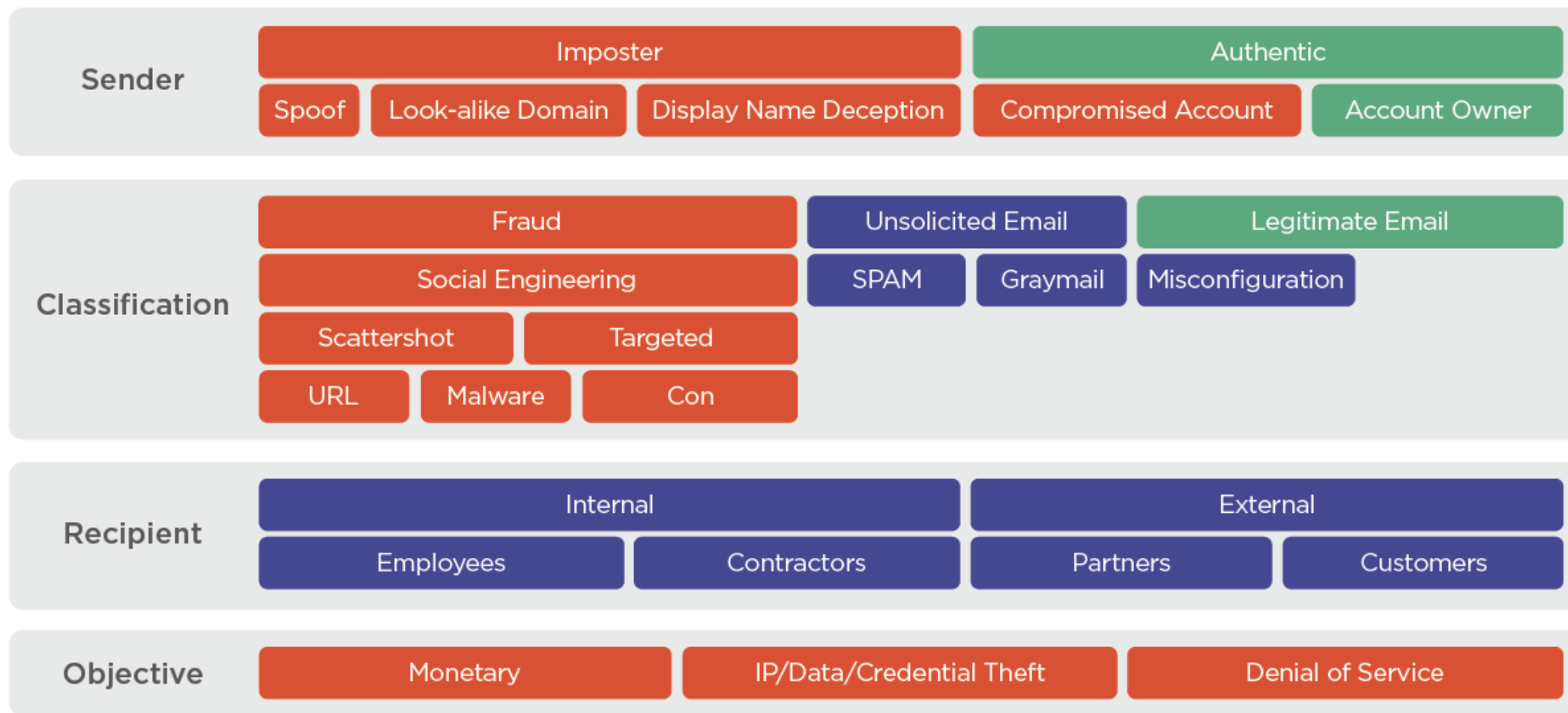
By Victim Loss			
Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$2,395,951,296	Lottery/Sweepstakes/Inheritance	\$71,289,089
Investment	\$1,455,948,191	Extortion	\$60,577,741
Confidence Fraud/Romance	\$956,029,740	Ransomware	*\$49,207,908
Personal Data Breach	\$517,021,288	Employment	\$47,231,023
Real Estate/Rental	\$350,328,166	Phishing/Vishing/Smishing/Pharming	\$44,213,707
Tech Support	\$347,657,432	Overpayment	\$33,807,671
Non-Payment/Non-Delivery	\$337,493,071	Computer Intrusion	\$19,603,037
Identity Theft	\$278,267,918	IPR/Copyright/Counterfeit	\$16,365,011
Credit Card Fraud	\$172,998,185	Health Care Related	\$7,042,942
Corporate Data Breach	\$151,568,225	Malware/Scareware/Virus	\$5,596,889
Government Impersonation	\$142,643,253	Terrorism/Threats of Violence	\$4,390,720
Advanced Fee	\$98,694,137	Gambling	\$1,940,237
Civil Matter	\$85,048,595	Re-shipping	\$811,466
Spoofing	\$82,169,806	Denial of Service/TDoS	\$217,981
Other	\$75,837,524	Crimes Against Children	\$198,350

# Attack Tactics

- Email Impersonation
- Spoofing or Look-A-Like domains
- Account Takeover
- Office 365 Matrix (MITRE ATT&CK)



# Identity Deception Diamond Model?



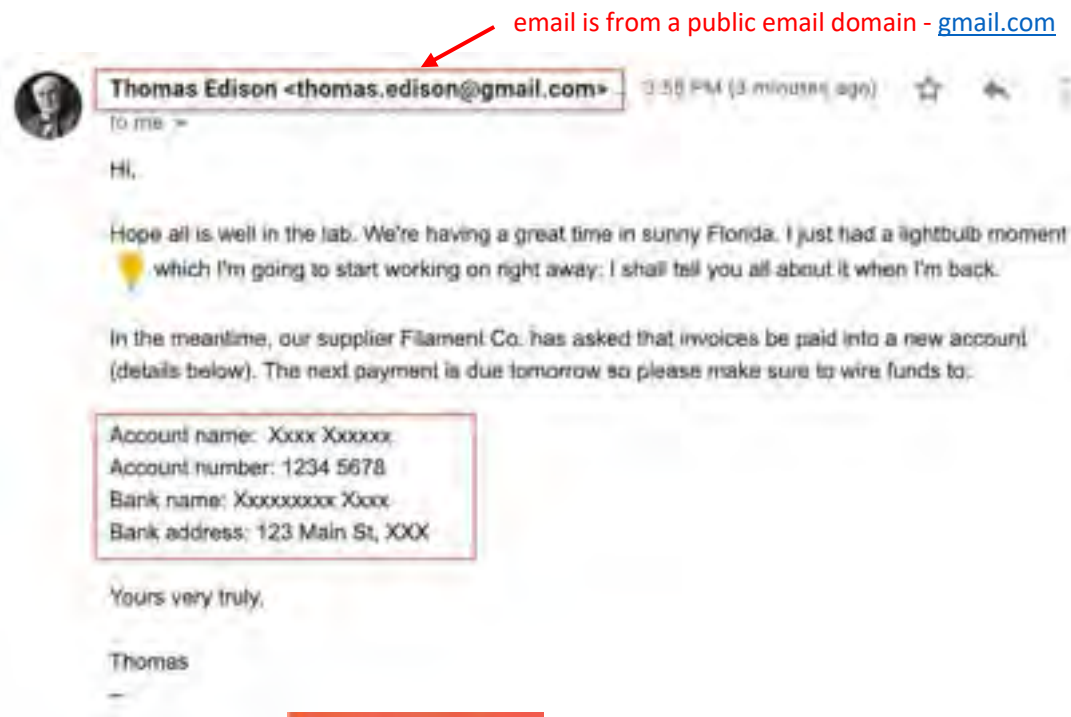
Source: Agrai Identity Graph Whitepaper

# Malicious Links and Attachments





# Email Impersonation



# Spoofing or Look-A-Like Domains

- What is Domain Spoofing?

- A form of phishing with a **fake email domain**
- To fool people into the **trusting** email thread
- The domain appears to be legitimate at **first glance**
- A closer look will reveal that a **W** is actually **two Vs** or a **lowercase L** is actually a **capital I**
- User is lured to interact with the attackers to disclose sensitive information or **send money**

## TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES

<b>TLD swap</b>	phishlabs.tech	<b>Omission</b>	phshlabs.com
<b>Subdomains</b>	phish.labs.com	<b>Transposition</b>	phsihlabs.com
<b>Typosquatting</b>	phishlavs.com	<b>Insertion</b>	phishxlabs.com
<b>Hyphenation</b>	phish-labs.com	<b>Homoglyph</b>	phishlaṽs.com
<b>Repetition</b>	phishllabs.com	<b>Vowel-swap</b>	phishlebs.com
<b>Replacement</b>	ph1shlabs.com	<b>Addition</b>	phishlabss.com

Q http:// adobe.com  
Q http:// adobe.com - Google Search  
G <http://xn--%20adbe-gx4c.com>  
Q adobe.com login - Google Search

“adobe[.]com”,  
serving an executable  
which mimics adobe  
download page.

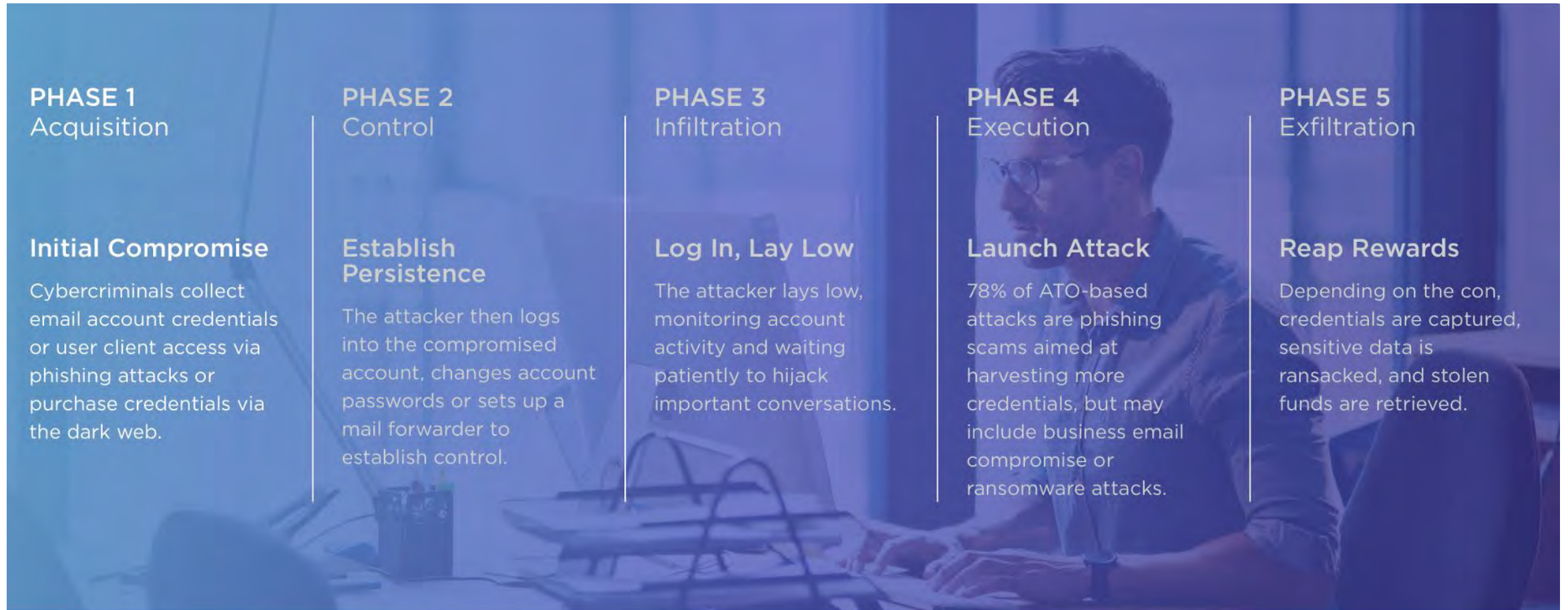


Source: Crowdstrike and Phishlabs



Dragon Advance Tech

# Account Takeover (ATO)



Source: [Hacking the Boardroom](#): Business Email Compromise More than CEO Fraud, coined a threat intelligence term for BEC - “[Financial Fraud Kill Chain](#)” (FFKC)



Dragon Advance Tech



# ATT&CK Office 365 Matrix

[Matrices](#)[Tactics](#)[Techniques](#)[Data Sources](#)[Mitigations](#)[Groups](#)[Software](#)[Resources](#)[Blog](#)[Contribute](#)[Home](#) > [Matrices](#) > Office 365

## Office 365 Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Office 365 platform.

[View on the ATT&CK® Navigator](#)[Version Permalink](#)

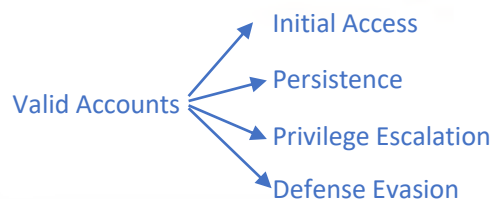
layout: side ▾

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
2 techniques	4 techniques	1 techniques	4 techniques	6 techniques	5 techniques	3 techniques	2 techniques	3 techniques
Phishing (1)	Account Manipulation (2)	Valid Accounts (2)	Hide Artifacts (1)	Brute Force (4)	Account Discovery (2)	Internal Spearphishing	Data from Information Repositories (1)	Account Access Removal
Valid Accounts (2)	Create Account (1)		Impair Defenses	Forge Web Credentials (1)	Cloud Service Dashboard	Taint Shared Content	Email Collection (2)	Endpoint Denial of Service (3)
	Office Application Startup (6)		Use Alternate Authentication Material (2)	Multi-Factor Authentication Request Generation	Cloud Service Discovery	Use Alternate Authentication Material (2)		Network Denial of Service (2)
	Valid Accounts (2)		Valid Accounts (2)	Steal Application Access Token	Permission Groups Discovery (1)			
				Steal Web Session Cookie	Software Discovery (1)			
				Unsecured Credentials				



Last modified: 01 April 2022

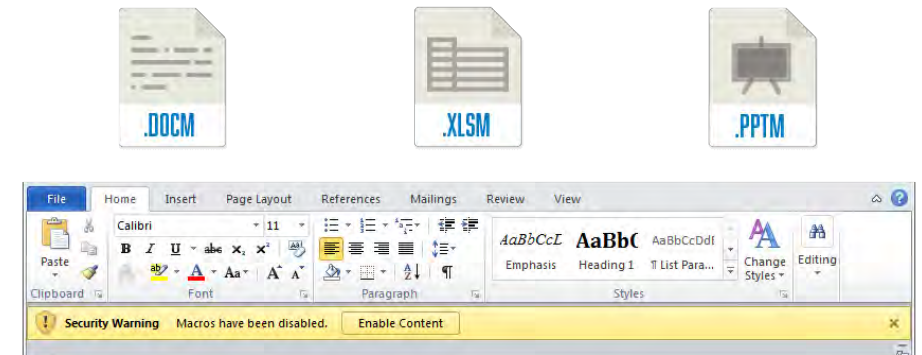
# Defence and Mitigation Technologies

- SPF, DKIM & DMARC
- AI-enabled Anti-Spoofing
- MFA (aka Identify Protection)
- Financial Fraud Kill Chain

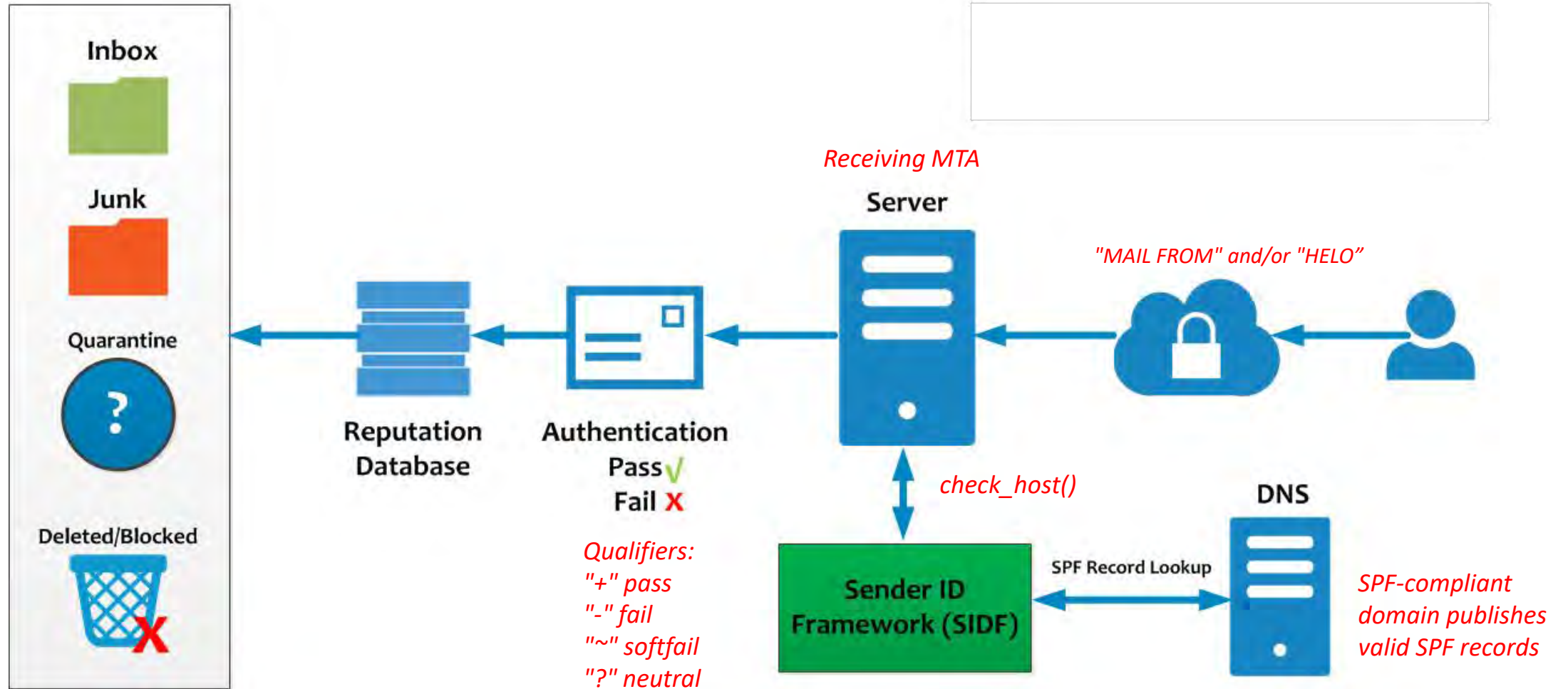




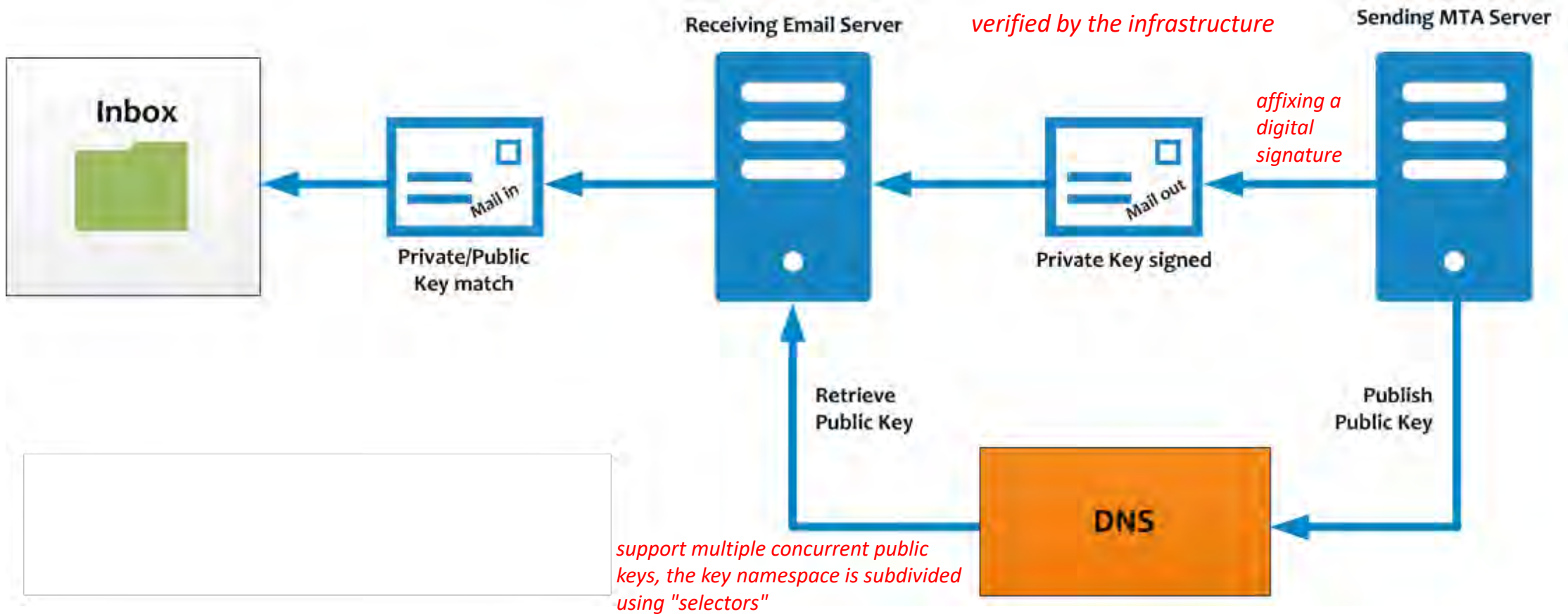
# Traditional Defense for Malicious Links and Attachments



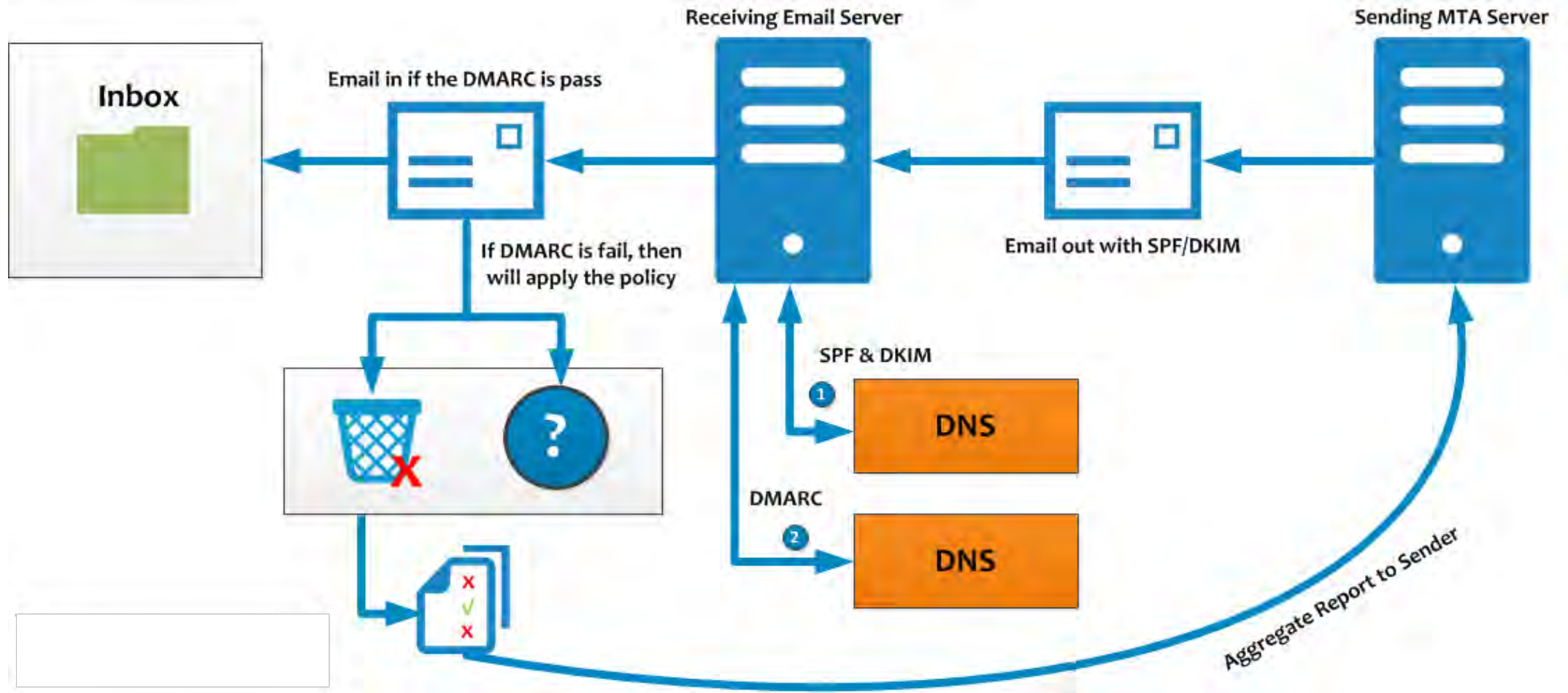
# Sender Policy Framework (SPF)



# Domain Keys Identified Mail (DKIM)



# Domain-based Message Authentication, Reporting & Conformance (DMARC)



*DMARC includes guidance on how to handle the “non-aligned” messages*



# AI-enabled Anti-Spoofing Technologies

[DATC] - Exchange Online

ran2

Done Editing Open

Delivered Phishing or Spam in Junk

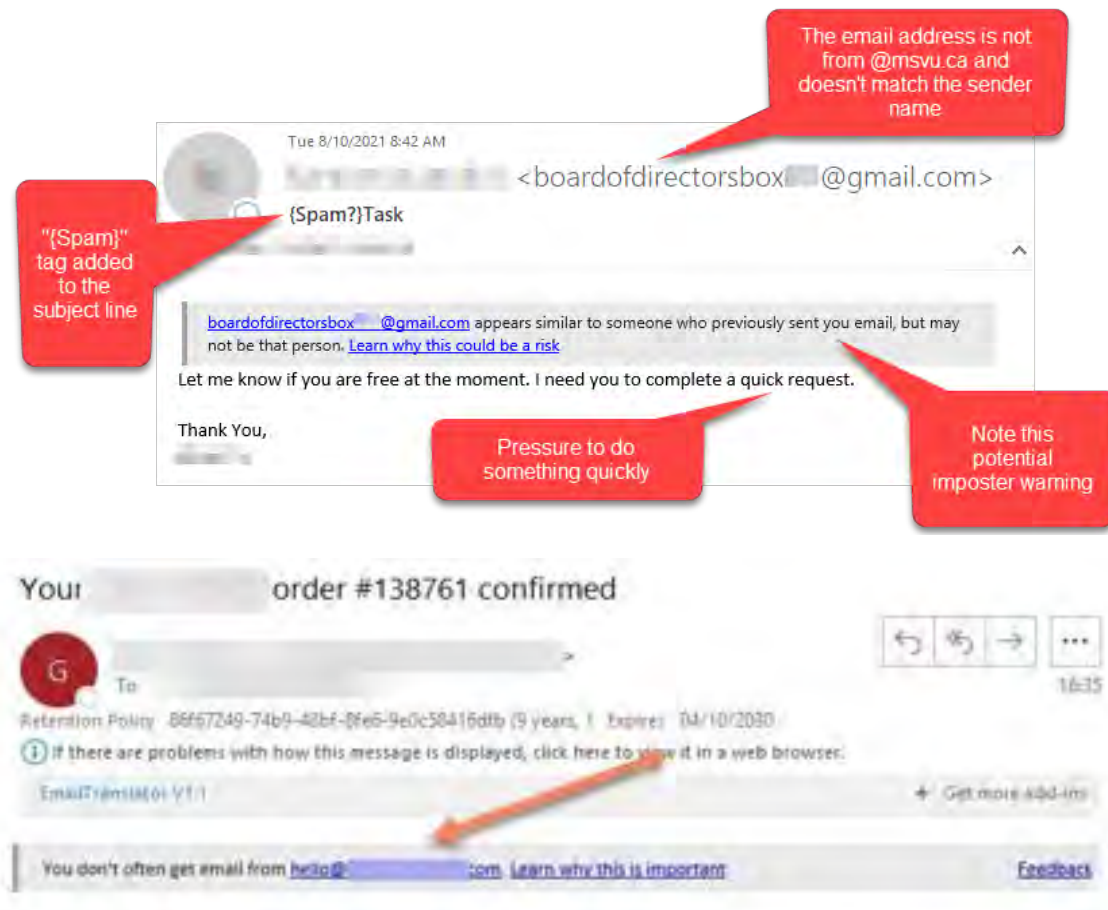
Timestamp	FromDomain	IpAddress	Mailbox	DeliveryA...	DetectedP...	DetectedS...	Auth_SPF	Auth_DKIM	Auth_DMARC	Auth_CompAuth
8/20/2022	gmail.com	209.85.217.47	admin@dragonadva...	Junked		Advanced filter	pass	pass	pass	pass
8/18/2022	ml.etc-meisai.jp	193.233.253.250	frankie@dragonadva...	Blocked	URL detonatio...	General filter	pass	none	none	fail
8/18/2022	virusbulletin.com	77.32.128.80	frankie@dragonadva...	Junked		Advanced filter	pass	pass	bestguesspass	pass
8/19/2022	twitter.com	199.59.150.88	frankie@dragonadva...	Blocked	URL detonatio...		pass	pass	pass	pass
8/19/2022	hitachikoyu.jp	114.179.255.92	ken@dragonadvanc...	Junked		Advanced filter	none	none	none	pass
8/19/2022	revivetech.asia	40.107.117.123	ken@dragonadvanc...	Junked		Advanced filter	pass	none	bestguesspass	pass
8/19/2022	wepro180.com	192.92.97.50	frankie@dragonadva...	Junked	Spoof external...	Advanced filter	pass	pass	none	fail
8/19/2022	hotmail.com	40.92.53.19	admin@dragonadva...	Junked		Advanced filter	pass	pass	pass	pass
8/20/2022	solutionsreview.com	52.128.42.114	frankie@dragonadva...	Junked	Spoof external...	Advanced filter	pass	pass	none	fail
8/20/2022	coffeeroasters.com.hk	77.32.148.253	ken@dragonadvanc...	Junked	Spoof external...	Mixed analysis...	pass	pass	none	fail
8/15/2022	wise.cx	174.129.193.122	frankie@dragonadva...	Junked		Mixed analysis...	pass	pass	none	none



Dragon Advance Tech

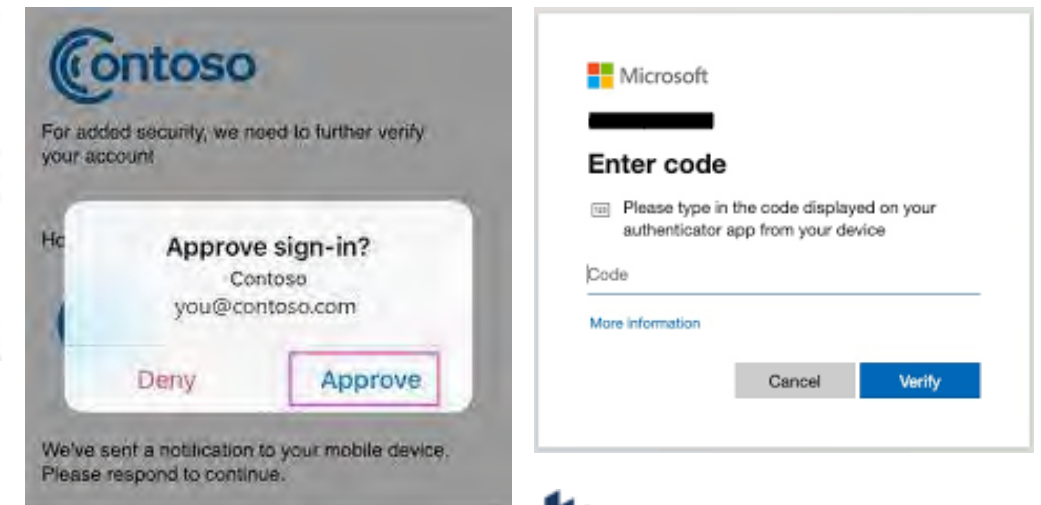
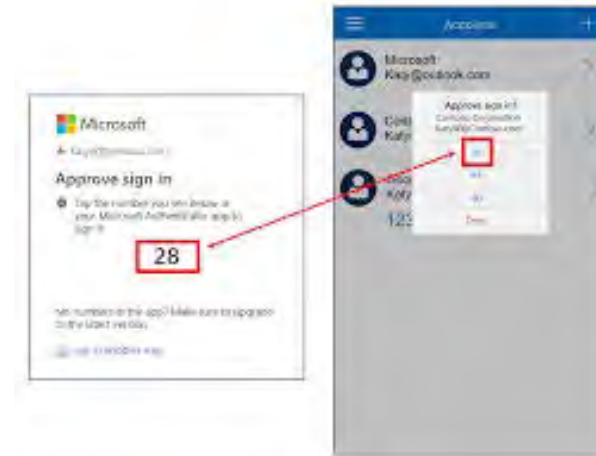
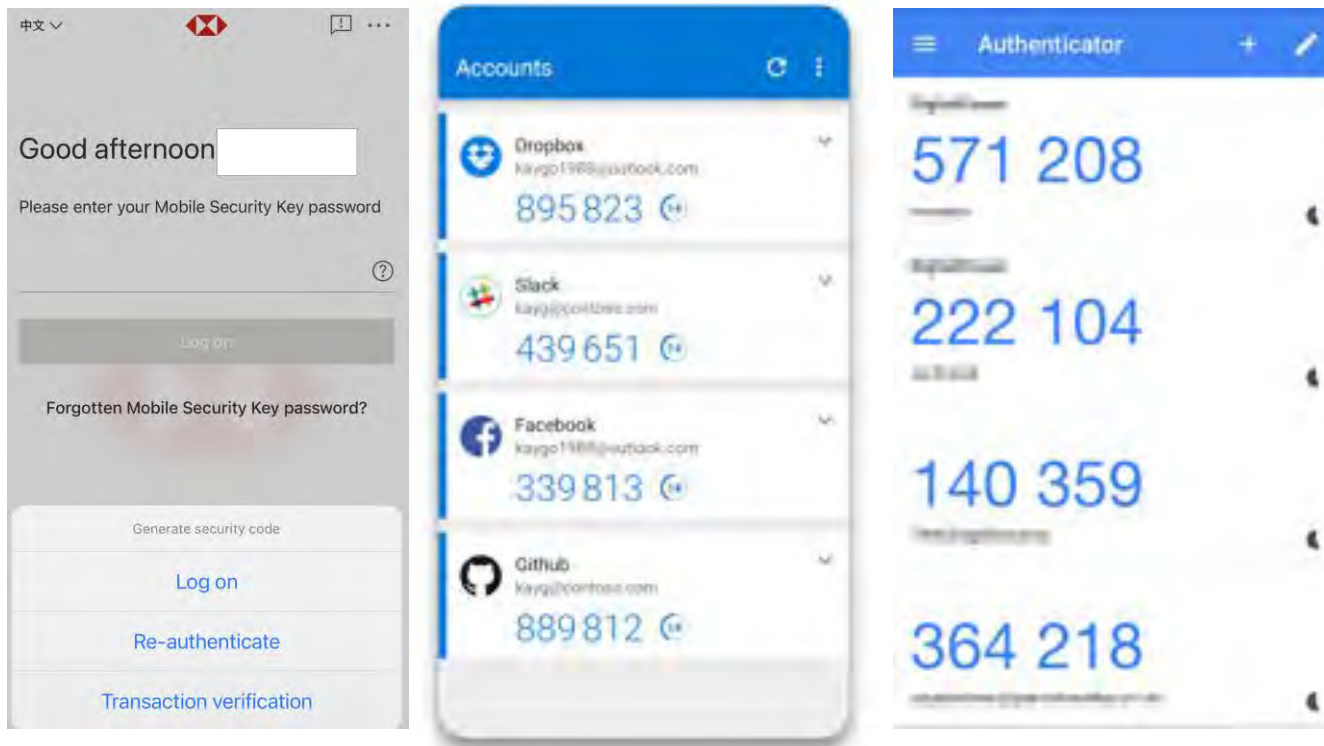


# AI-enabled Anti-Phishing and Impersonation Tips



# Identity Protection with MFA

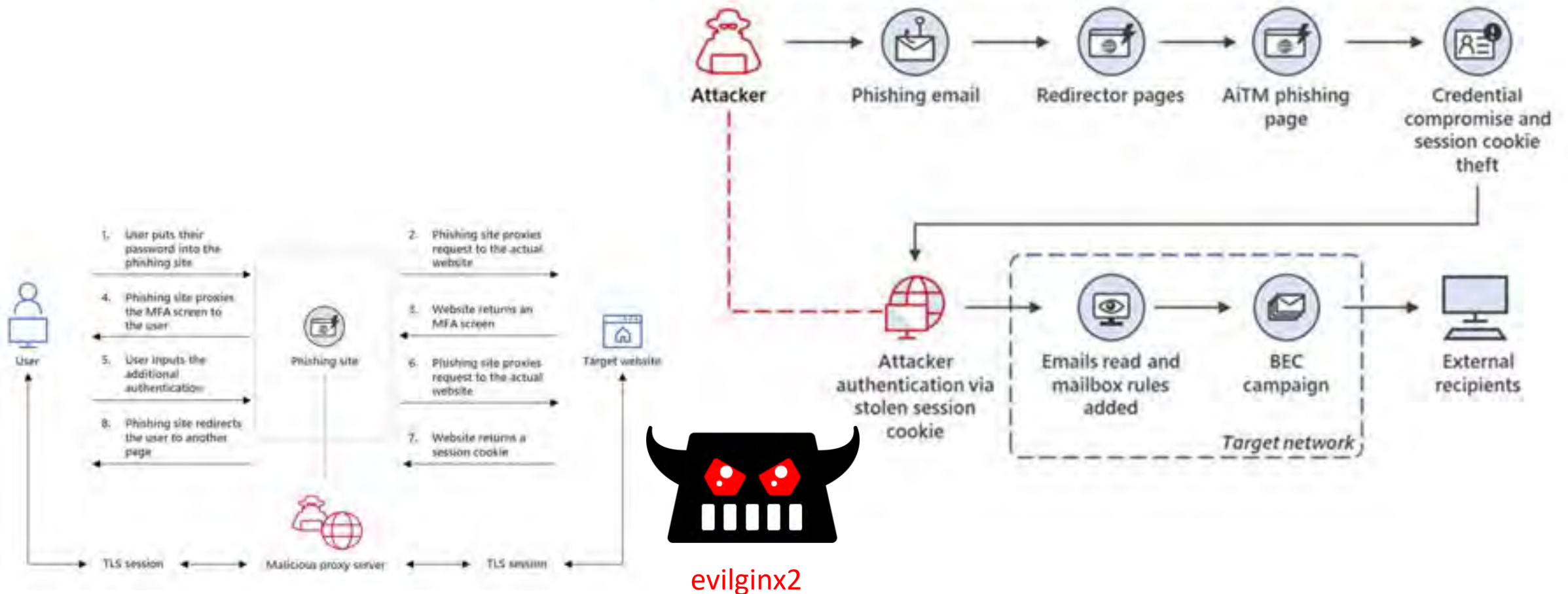
MFA **is not** a magic silver bullet to defense protect your Identity, but it is critical for all cloud/zero-trust access with multiple devices.



However, I see a lots of entities are **not deploying** such defense because of ignorance or not obtaining buying in from management.

# Large-scale AiTM phishing campaign targeted +10,000 orgs since 2021

July 13, 2022 By Pierluigi Paganini



Source: <https://securityaffairs.co/wordpress/133154/hacking/aitm-phishing-campaigns.html>



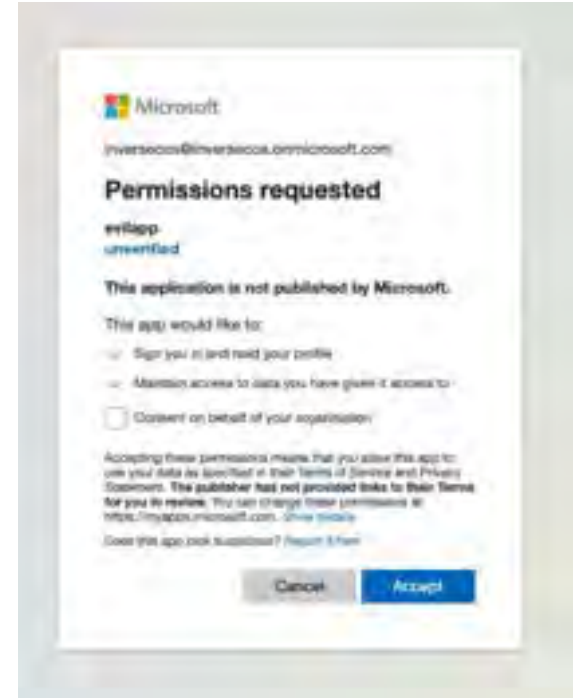
# Financial Fraud Kill Chain

- Identity protection
  - Brute force attacks or password guessing [APT29 – through unknown means]
  - Suspicious logins [using unusual devices or apps in foreign regions]
  - Disable MFA to unsecure credentials [ATT&CK (T1552) or enroll MFA for a dormant account [APT29]
- Steal session or authentication token
  - OAuth2 [ATT&CK (T1528)– steal access token]
  - MFA session token [APT29 - evilginx2]
  - Explicitly deny multi-factor authentication (MFA) [MFA Fatigue]
- After ATO
  - Create and modify forwarding rules [ATT&CK (T1562) – impair defenses]
  - Moving selected compromised account messages to the RSS folder [BEC]
  - Make changes to log configuration – [APT29 - You can't audit me]
- Gain the trust of internal users
  - To get email collection [ATT&CK (T1114) - email collection]
  - to arrange remittance or transfer of fund [BEC]

Source:

<https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft>

<https://attack.mitre.org/matrices/enterprise/cloud/office365/>





# Email Threat Hunting and Response



# FINDING BEC ATTACK INDICATORS FROM EMAIL HEADER OR BODY?

- An inbound compromised email account
- URL to download payment instruction
- Invoice or altered payment instruction as an attachment
- Bad spelling or grammar
- Immediate calls to action
- Funny text or images
- Unfamiliar message tone
- Request personal details
- Too good to be true
- The subject line contains keywords:
  - *Wire, Invoice, Payment, Cash, Remittance ...*



# Identity: Sign-ins Assessment

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks

[DATC] - Azure AD

ran2

Edit Open Refresh Help Auto refresh: Off

## Sign-ins by Location

All Sign-ins

24.6k

Success

23.1k

	Na...	Sign-in Co...	Trend	Failure
<input type="checkbox"/>	HK	1.197K		59
<input type="checkbox"/>	US	1.8K		0
<input type="checkbox"/>	HK	1.197K		59
<input type="checkbox"/>	JP	58		13
<input type="checkbox"/>	KR	21		21

## Changes in Security Info or MFA Status

TimeGenerated	OperationName	targetUser	initL
8/16/2022, 9:11:09 AM	User cancelled security info regis...	xendless@cisp.com.hk	xen...
8/12/2022, 9:10:01 AM	Reset user password	rafaelkwok@cisp.com.hk	ken...
8/12/2022, 9:15:06 AM	User started security info registra...	rafaelkwok@cisp.com.hk	rafa...
8/12/2022, 9:15:17 AM	User registered security info	rafaelkwok@cisp.com.hk	rafa...
8/12/2022, 9:15:30 AM	User registered all required secur...	rafaelkwok@cisp.com.hk	rafa...
8/12/2022, 9:17:04 AM	Change password (self-service)	rafaelkwok@cisp.com.hk	rafa...

Multiple success login from sam...

IPAddress	Country	Unique
119.236.68.252	HK	
112.118.116.229	HK	
202.83.241.126	HK	

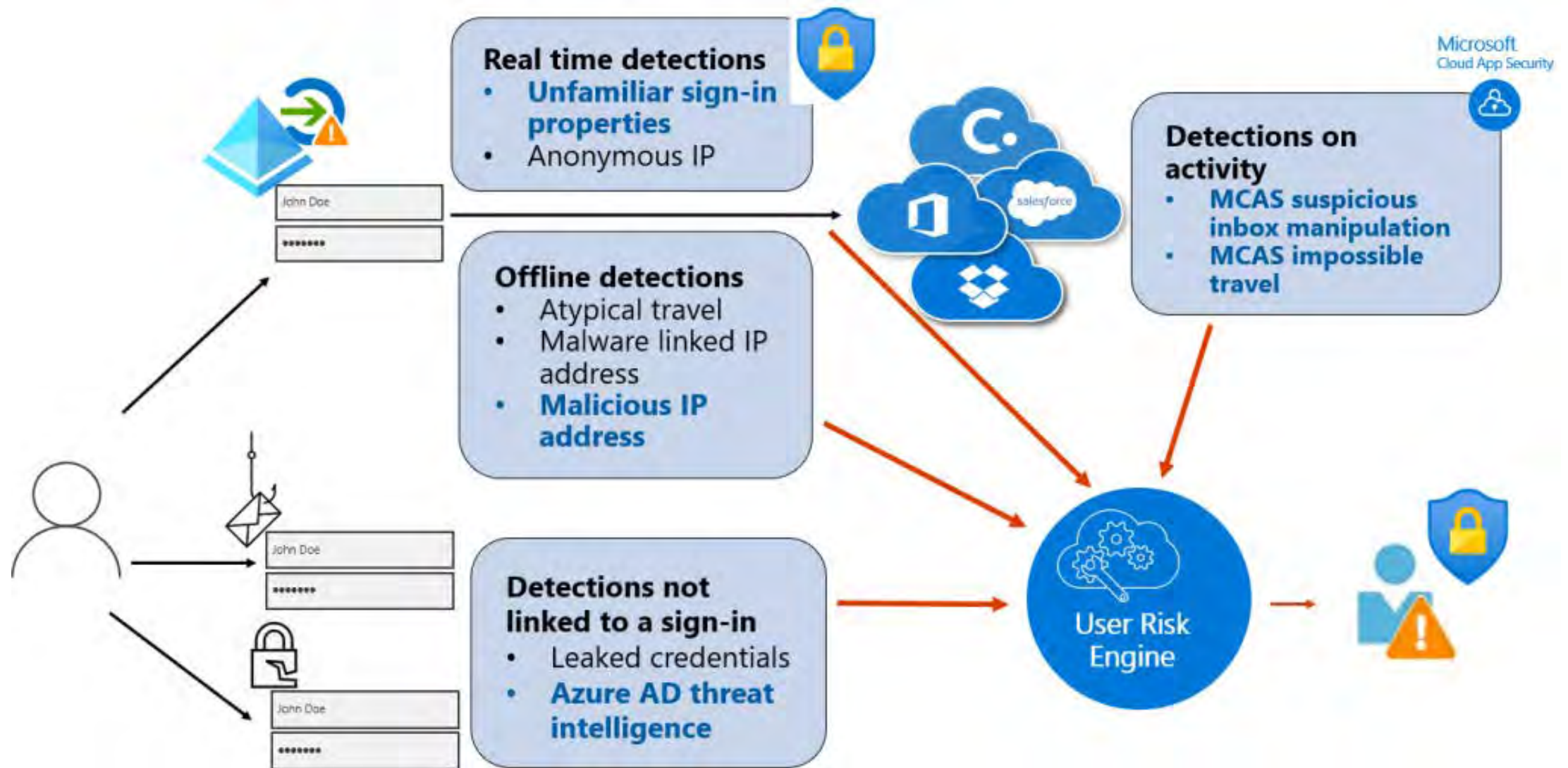
## Success login out of HK

UserPrincipalName	Country	Count
admin@dragonadvancetech.com	US	623
lr@dragonadvancetech.com	US	589
ken@dragonadvancetech.com	US	588
hey@cisp.com.hk	JP	46
ken@dragonadvancetech.hk	KR	12
ken@dragonadvancetech.hk	SG	10

## Login Failure out of HK

UserPrincipalName	Country	Count
ken@dragonadvancetech.hk	US	10
ken@dragonadvancetech.hk	JP	7
frankie@cisp.com.hk	KR	6
nimitzyau@cisp.com.hk	SG	4
xendless@cisp.com.hk	JP	3
frankie@dragonadvancetech.com	GB	3

# Identity: Impossible Travel Sign-ins





# Identity: Suspicious MFA Sign-ins

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

## [DATC] - Azure AD

ren?

Edit Open Help Auto refresh: Off

TimeRange: Last 30 days Apps: All UserNamePrefix: All Username: All Category: All Country: All About: Hide

### Summary of top errors

Error Code	Reason
50173	Fresh auth token is needed. Have the user re-sign using fresh cre...
700084	Other
700082	Other
500131	Other
50126	Invalid username or password or Invalid on-premise username or...
50055	Invalid password, entered expired password.

### Login Failure (including: Invalid passwords)

Time generated	User	IPAddress	Country	Error	Result description
8/21/2022, 4:00:05 PM	eric@dragonadvancetech.com	202.83.241.126	HK	50173	Fresh auth token is need...
8/21/2022, 4:00:05 PM	eric@dragonadvancetech.com	202.83.241.126	HK	50173	Fresh auth token is need...
8/21/2022, 4:00:04 PM	eric@dragonadvancetech.com	202.83.241.126	HK	50173	Fresh auth token is need...
8/21/2022, 4:00:04 PM	eric@dragonadvancetech.com	202.83.241.126	HK	50173	Fresh auth token is need...
8/21/2022, 4:00:04 PM	eric@dragonadvancetech.com	202.83.241.126	HK	50173	Fresh auth token is need...
8/21/2022, 12:00:02 PM	frankie@dragonadvancetech.hk	20.189.106.246	HK	700082	Other

### Login failure because of MFA failure or Token Expired

Time generated	User	Operating system	IPAddress	Region	City	Error Code	ResultDescription
8/21/2022, 4:16:49 PM	frankie@cisp.com.hk	MacOs	112.118.116.229	HK	Aberdeen	50074	User did not pass the MFA challenge
8/21/2022, 4:16:49 PM	frankie@cisp.com.hk	MacOs	112.118.116.229	HK	Aberdeen	50074	User did not pass the MFA challenge
8/18/2022, 9:58:34 PM	hey@cisp.com.hk	iOS 15	61.92.102.36	HK	Aberdeen	50057	User account is disabled: The account has been disabled by a...
8/18/2022, 9:58:33 PM	hey@cisp.com.hk	iOS 15	61.92.102.36	HK	Aberdeen	50057	User account is disabled: The account has been disabled by a...
8/18/2022, 9:58:31 PM	hey@cisp.com.hk	iOS 15	61.92.102.36	HK	Aberdeen	50057	User account is disabled: The account has been disabled by a...
8/18/2022, 9:58:30 PM	hey@cisp.com.hk	iOS 15	61.92.102.36	HK	Aberdeen	50057	User account is disabled: The account has been disabled by a...

### Sign-ins by Location

All Sign-ins: 24.6k

Search

Na... Sign-in Co... Trend

### Changes in Security Info or MFA Status

Search

Failure TimeGenerated OperationName targetUser

# Identity: Suspicious MFA Sign-ins

Edit Open Help Auto refresh: Off

Security Settings & MFA

TimeRange: Last 7 days Apps: All UserNamePrefix: All UserName: All Category: SignInLogs Country: All AuthProc: singleFactorAuthentication About: Hide

### Successfully Sign-Ins

timestamp	Name	IPAddress	Country	ClientUsed	ResourceDisp
8/21/2022, 4:17:...	frankie@cisp.com.hk	112.118.116.229	HK	Browser	Windows Azu
8/21/2022, 4:17:...	frankie@cisp.com.hk	112.118.116.229	HK	Browser	Windows Azu
8/21/2022, 4:17:...	frankie@cisp.com.hk	112.118.116.229	HK	Browser	Windows Azu
8/19/2022, 2:57:...	frankie@dragonadvancete...	220.241.155.25	HK	Mobile Apps a...	Windows Azu
8/19/2022, 3:07:...	frankie@dragonadvancete...	220.241.155.25	HK	Mobile Apps a...	OfficeServices
8/18/2022, 11:2:...	ken@dragonadvancetech.hk	119.236.68.252	HK	Browser	Windows Azu

Results were limited to the first 200 rows.

### Changes in Security Info or MFA Status

TimeG...	targetUser	OperationName	Result	SetupBy	Re
8/15/2022...	xendless@cisp.com.hk	User cancelled security inf...	success	xendless@cisp...	U-
8/15/2022...	lcw.alfred.lai@cisp.com.hk	Change user password	failure	lcw.alfred.lai@...	M
8/15/2022...	lcw.alfred.lai@cisp.com.hk	Change password (self-ser...	failure	lcw.alfred.lai@...	U-
8/15/2022...	xendless@cisp.com.hk	User cancelled security inf...	success	xendless@cisp...	U-
8/16/2022...	xendless@cisp.com.hk	User cancelled security inf...	success	xendless@cisp...	U-

### MFA not pass, need 2nd factor or failed

timestamp	Name	IPAddress	Country	ResultType	ResultDescri
8/21/2022, 4:16:...	frankie@cisp.com.hk	112.118.116.229	HK	50074	User did not
8/21/2022, 4:16:...	frankie@cisp.com.hk	112.118.116.229	HK	50074	User did not
8/17/2022, 11:2:...	ken@dragonadvancetech.hk	220.246.201.197	HK	50074	User did not
8/17/2022, 11:2:...	ken@dragonadvancetech.hk	220.246.201.197	HK	50074	User did not
8/15/2022, 11:0:...	ken@dragonadvancetech.hk	210.3.87.68	HK	50074	User did not
8/15/2022, 11:0:...	ken@dragonadvancetech.hk	210.3.87.68	HK	50074	User did not



Login Failed (Token-related)

MFA failure: Token expired

Set rules operations - in detail

TimeGenerated	UserId	UserType	Key	Value
8/13/2022,...	[Redacted]	Admin	Identity	[Redacted]001.prod.outlook
8/13/2022,...	[Redacted]	Admin	Type	Shared
8/13/2022,...	[Redacted]	Admin	Confirm	False
8/13/2022,...	[Redacted]	Admin	Force	True
8/5/2022, ...	[Redacted]	Admin	Identity	4bb7c3e9-[Redacted]
8/5/2022, ...	[Redacted]	Admin	Type	Shared
8/5/2022, ...	[Redacted]	Admin	Confirm	False
8/5/2022, ...	[Redacted]	Admin	Force	True
8/5/2022, ...	[Redacted]	Admin	Identity	4bb7c3e9-[Redacted]
8/5/2022, ...	[Redacted]	Admin	Type	Regular
8/5/2022, ...	[Redacted]	Admin	Confirm	False

Inbox rules operations by UserId

TimeGenerated	UserId	UserType	IP	Key	Value
8/22/2022,...	Steven [Redacted]	Regular	160.72. [Redacted]		
8/22/2022,...	Andrew [Redacted]	Regular	73.226. [Redacted]		
8/22/2022,...	Andrew [Redacted]	Regular	73.226. [Redacted]		
8/22/2022,...	Andrew [Redacted]	Regular	73.226. [Redacted]		
8/22/2022,...	Andrew [Redacted]	Regular	73.226. [Redacted]		
8/22/2022,...	Andrew [Redacted]	Regular	73.226. [Redacted]		

# Impair Defenses: Forwarding Rules

Transport rules operations - in details

TimeGenerated	UserId	UserType	Key	Value
7/28/2022, [Redacted]	[Redacted]	Admin	FromAddressContainsWords	[Redacted]
7/28/2022, [Redacted]	[Redacted]	Admin	Name	block *. [Redacted] com *. [Redacted] .net
7/28/2022, [Redacted]	[Redacted]	Admin	StopRuleProcessing	False
7/28/2022, [Redacted]	[Redacted]	Admin	SetAuditSeverity	



# Phishing Incident Response

## Cybersecurity Incident & Vulnerability Response Playbooks

### Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

## INCIDENT RESPONSE PLAYBOOK

This playbook provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2,<sup>5</sup> including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities. This playbook describes the process FCEB agencies should follow for confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

- Incident response can be initiated by several types of events, including but not limited to:
- Automated detection systems or sensor alerts
- Agency user report
- Contractor or third-party ICT service provider report
- Internal or external organizational component incident report or situational awareness update
- Third-party reporting of network activity to known compromised infrastructure, detection of malicious code, loss of services, etc.
- Analytics or hunt teams that identify potentially malicious or otherwise unauthorized activity

### When to use this playbook

Use this playbook for incidents that involve confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out.

For example:

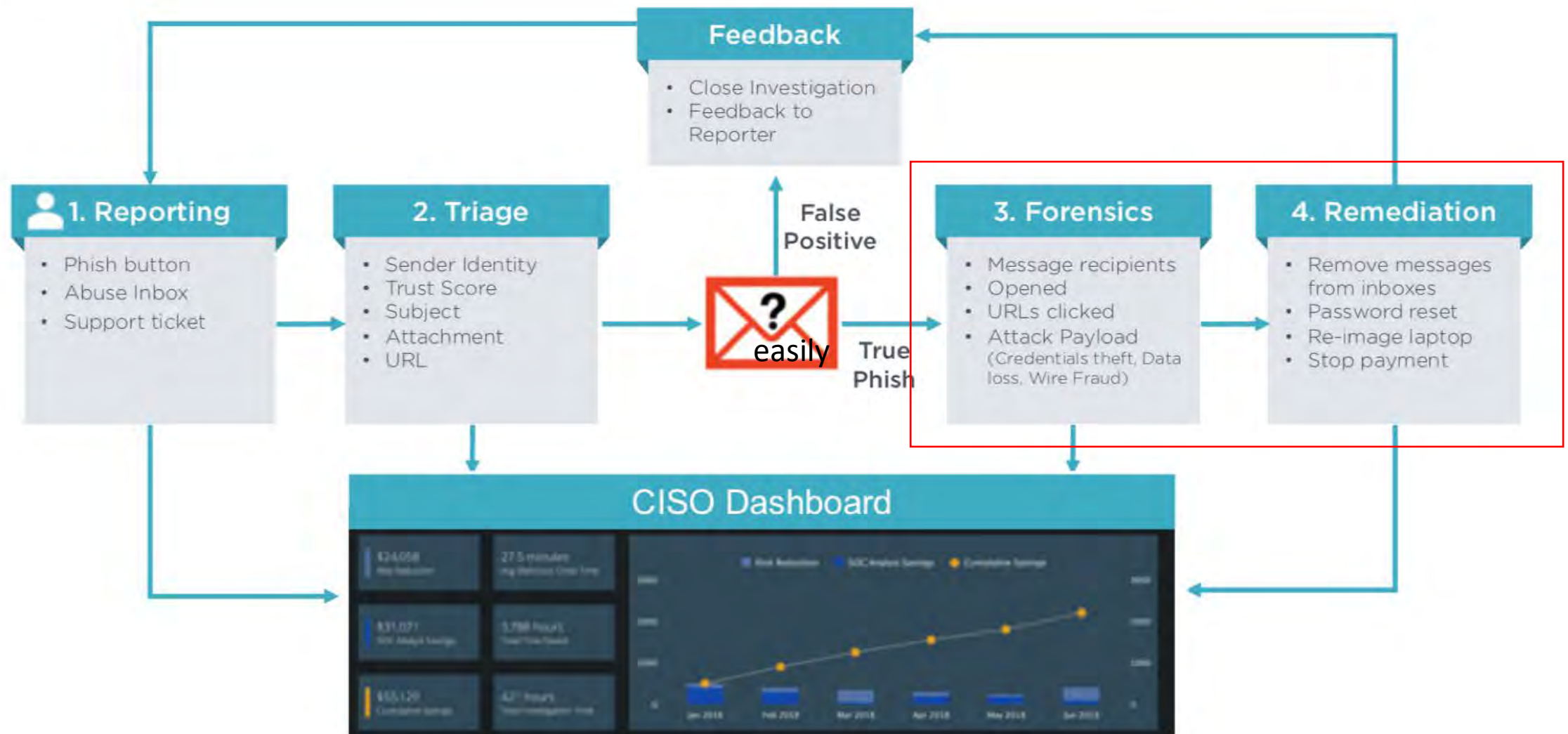
- Incidents involving lateral movement, credential access, exfiltration of data
- Network intrusions involving more than one user or system
- Compromised administrator accounts

This playbook does not apply to activity that does not appear to have such major incident potential, such as:

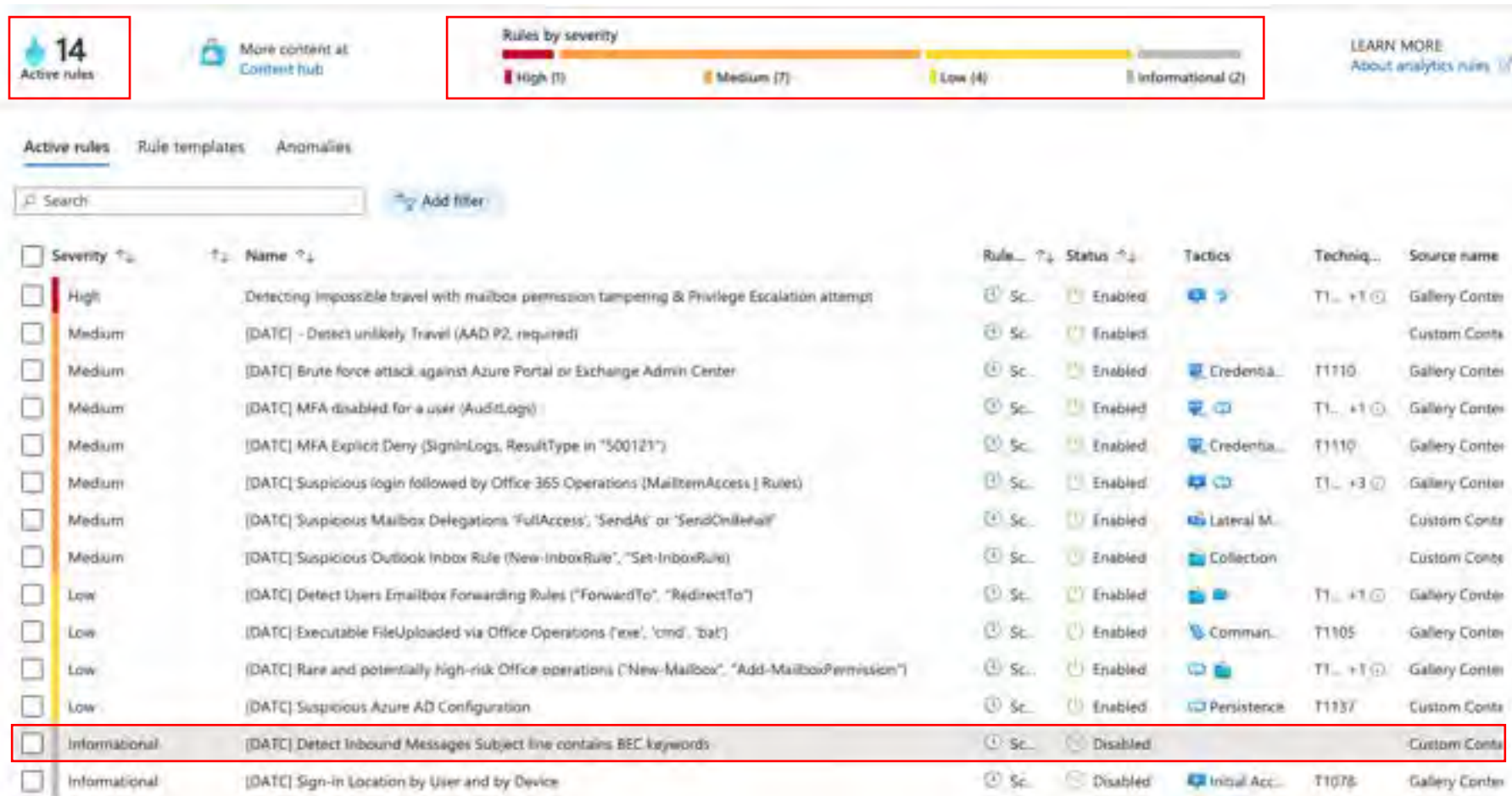
- "Spills" of classified information or other incidents that are believed to result from unintentional behavior only
- Users clicking on phishing emails when no compromise results
- Commodity malware on a single machine or lost hardware that, in either case, is not likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.



# Incident Response Automated Phishing Playbook



# BEC Threat Hunting and Response



The screenshot shows the configuration page for the rule '[DATC] Detect Inbound Messages Subject line contains BEC keywords'. The rule is currently disabled. The configuration includes a description, a rule query, rule frequency, rule period, rule threshold, and event grouping.

**Id:** 2f4b599f-d7d0-472a-9c64-db1152d4f35c

**Description:** [DATC] - Detect Deduplicated Inbound Messages Subject line contains BEC keywords

**Rule query:**

```
MailEvents  
| where TimeGenerated > ago(starttime)  
| where DeliveryAction == "Delivered" and  
DeliveryLocation == "Inbox/folder" and  
EmailDirection == "Inbound"  
| where Subject contains "wire" or Subject  
contains "invoice" or Subject contains
```

**Rule frequency:** Run query every 1 day

**Rule period:** Last 1 day data

**Rule threshold:** Trigger alert if query returns more than 0 results

**Event grouping:** Group all events into a single alert

# Take Away

- The identity of your boardroom are the targets
- Interpol: BEC criminals gain entry to a victim's devices or systems – through hacking, phishing, malware
- From 2018-2019, based on the IC3 reports, banks in Thailand and Hong Kong were the primary international destination of fraudulent funds
- Technologies + Policies can handle well traditional anti-spoofing and anti-phishing attacks (deploy SPF | DKIM | DMARC | AI-enabled)
- Have the right approach to configure your secure email solutions properly
- Implement MFA to protect our executives' online identity
- Understand the Financial Fraud Kill Chain and actors TTP
- Hunt evil mailbox activities for BEC actors' lateral movements



Q & A

