Dragon Advance Tech

InfoSec 2022 Ummit

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

- ISSumit (2022)

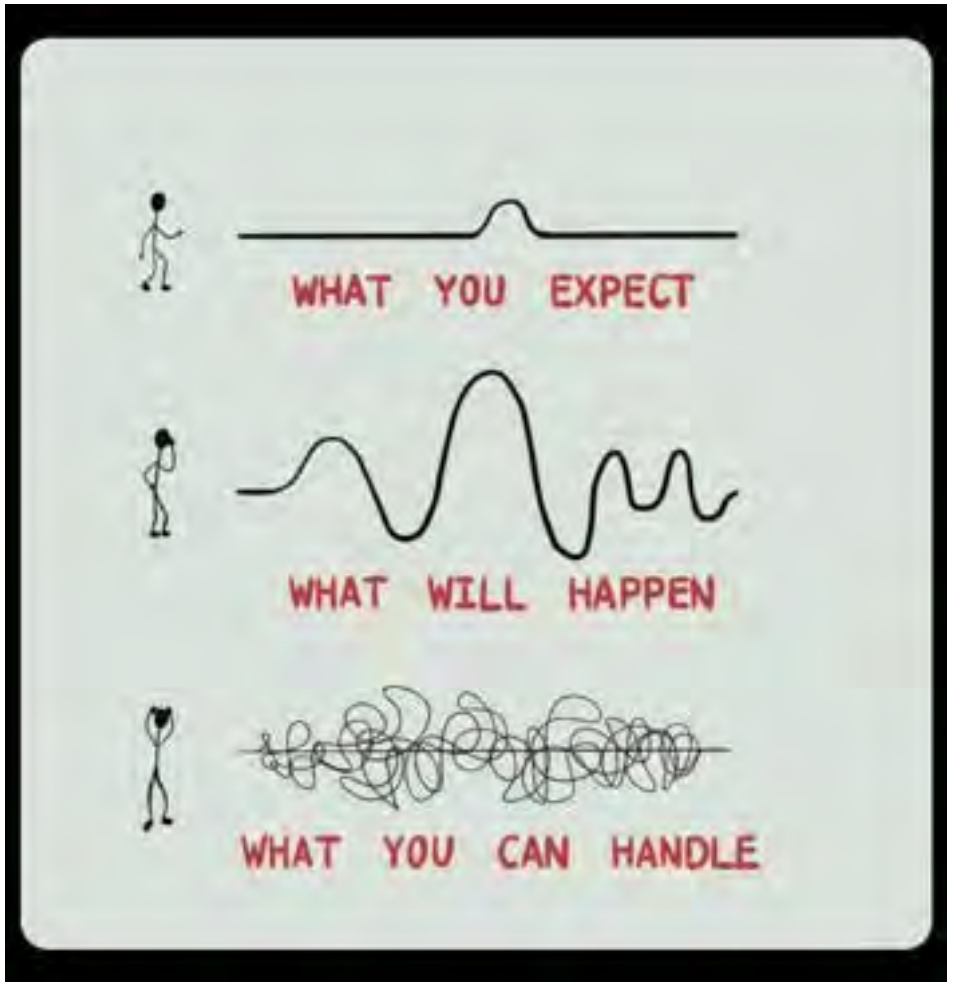
Dragon Advance Tech

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

Dragon Advance Tech

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

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 ...

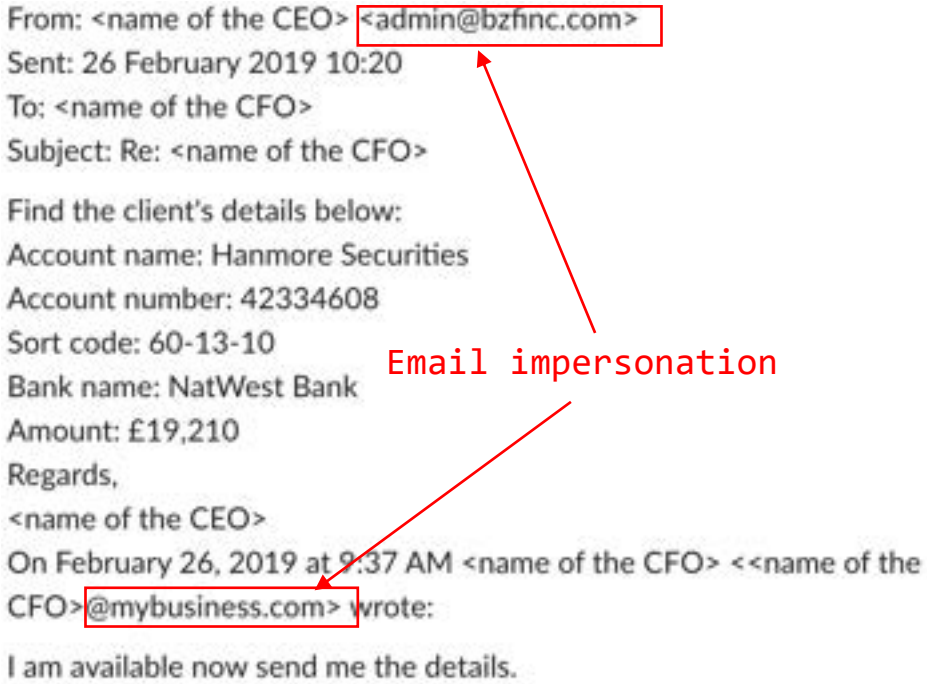
Dragon Advance Tech

What is BEC?


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.
#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



Dragon Advance Tech

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.

Dragon Advance Tech

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[1] (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[2] 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[3] and US DOJ[4] 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[5] 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	323,972	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	18,522	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	395

2021 Crime Types continued

By Victim Loss

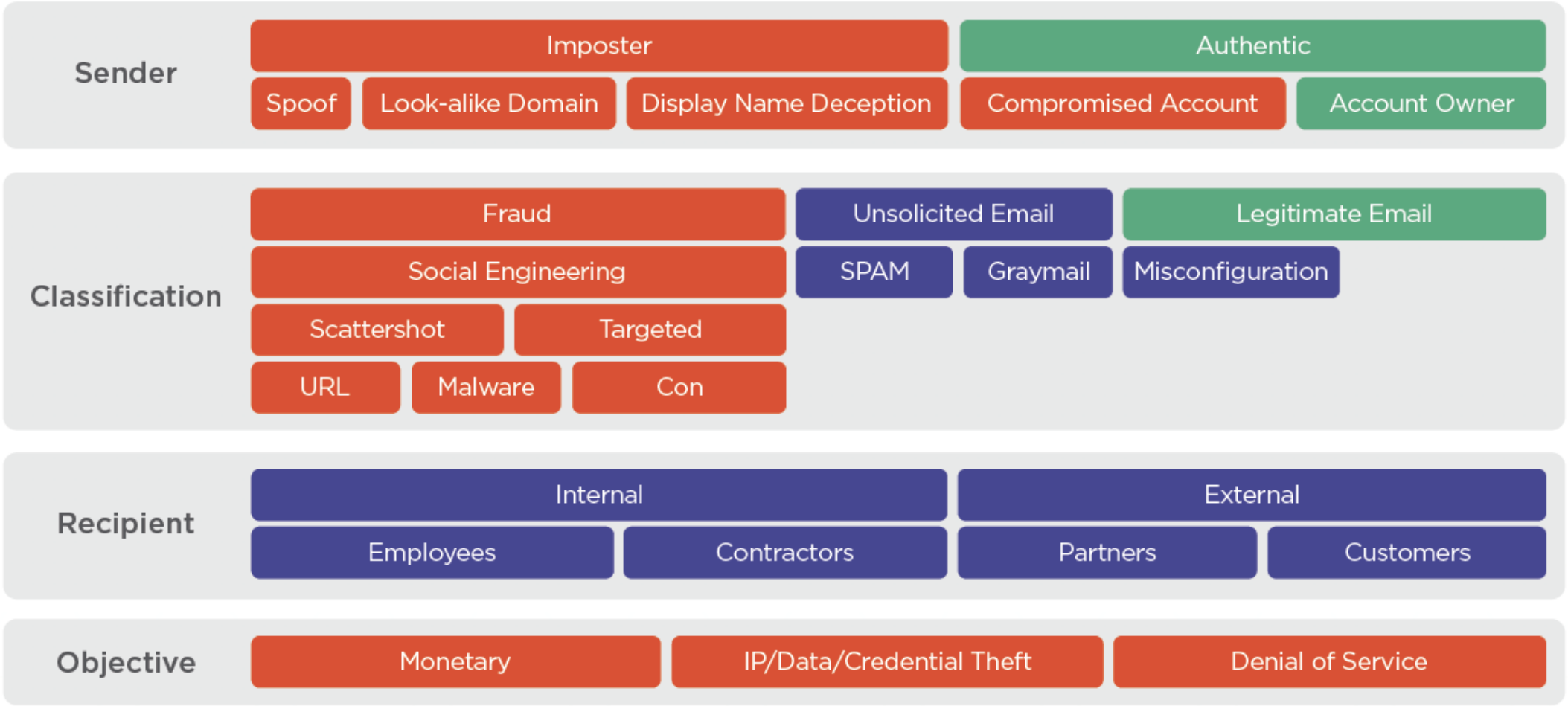
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$44,213,707
Tech Support	$347,657,432	Overpayment	$33,407,671
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	$172,998,385	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	$85,049,939	Re-shipping	$631,466
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950

Attack Tactics

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

Dragon Advance Tech

Identity Deception Diamond Model?



Source: Agrai Identity Graph Whitepaper

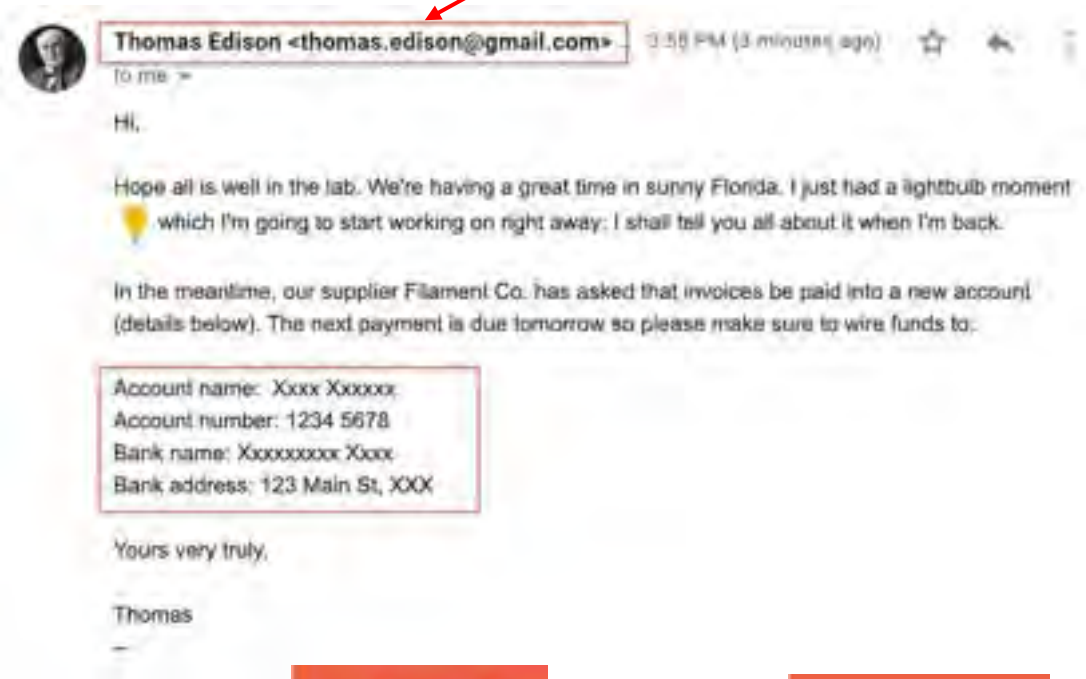
Dragon Advance Tech

Malicious Links and Attachments

Dragon Advance Tech

Email Impersonation

email is from a public email domain - gmail.com



Dragon Advance Tech

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

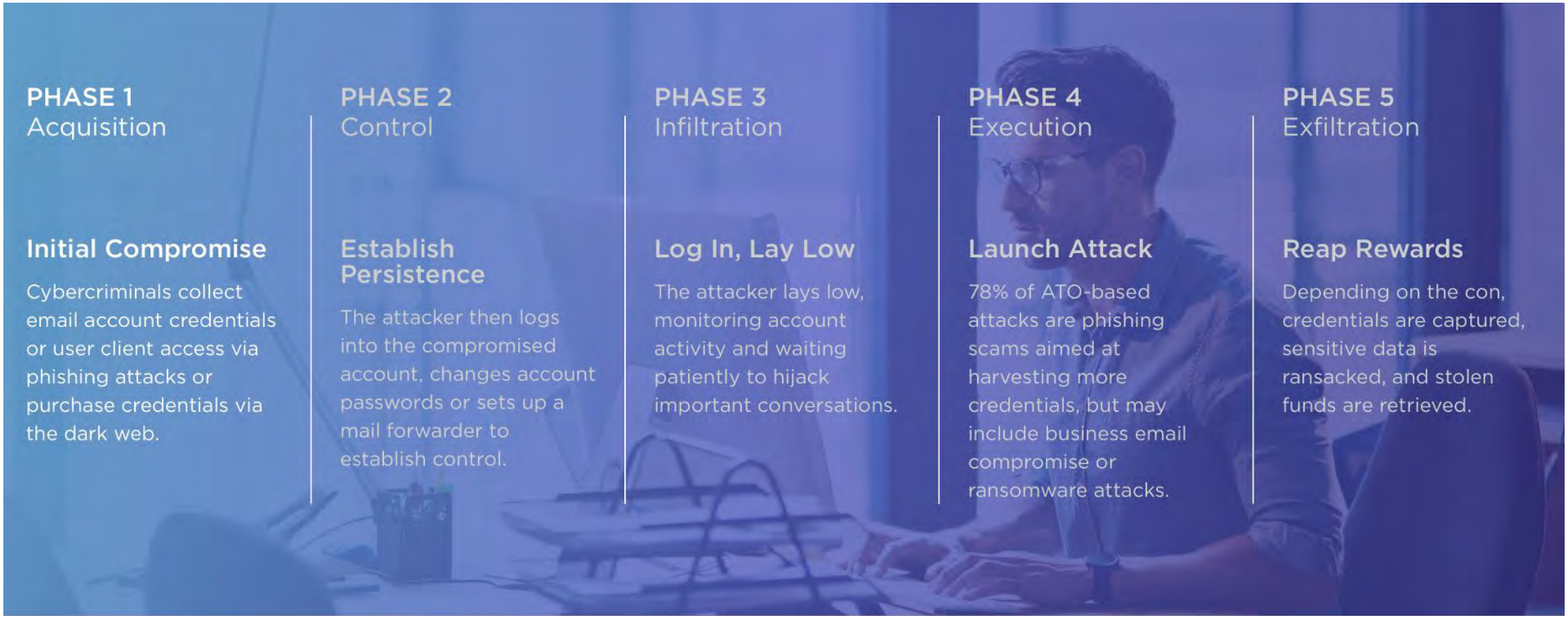
TECHNIQUES TO CREATE LOOK-ALIKE DOMAIN NAMES			
TLD swap	phishlabs.tech	**Omission**	phshlabs.com
Subdomains	phish.labs.com	**Transposition**	phsihlabs.com
Typosquatting	phishlavs.com	**Insertion**	phishxlabs.com
Hyphenation	phish-labs.com	**Homoglyph**	phishlaƄs.com
Repetition	phishllabs.com	**Vowel-swap**	phishlebs.com
Replacement	ph1shlabs.com	**Addition**	phishlabss.com

“adọbe[.]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 | Search

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				

Valid Accounts → Initial Access, Persistence, Privilege Escalation, Defense Evasion

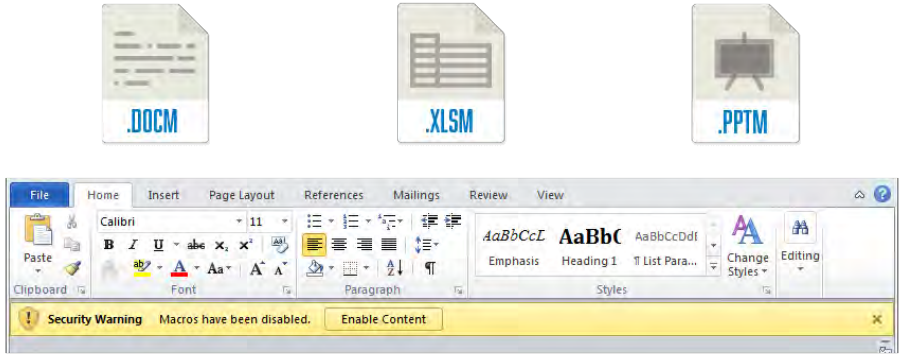
Last modified: 01 April 2022

Defence and Mitigation Technologies

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

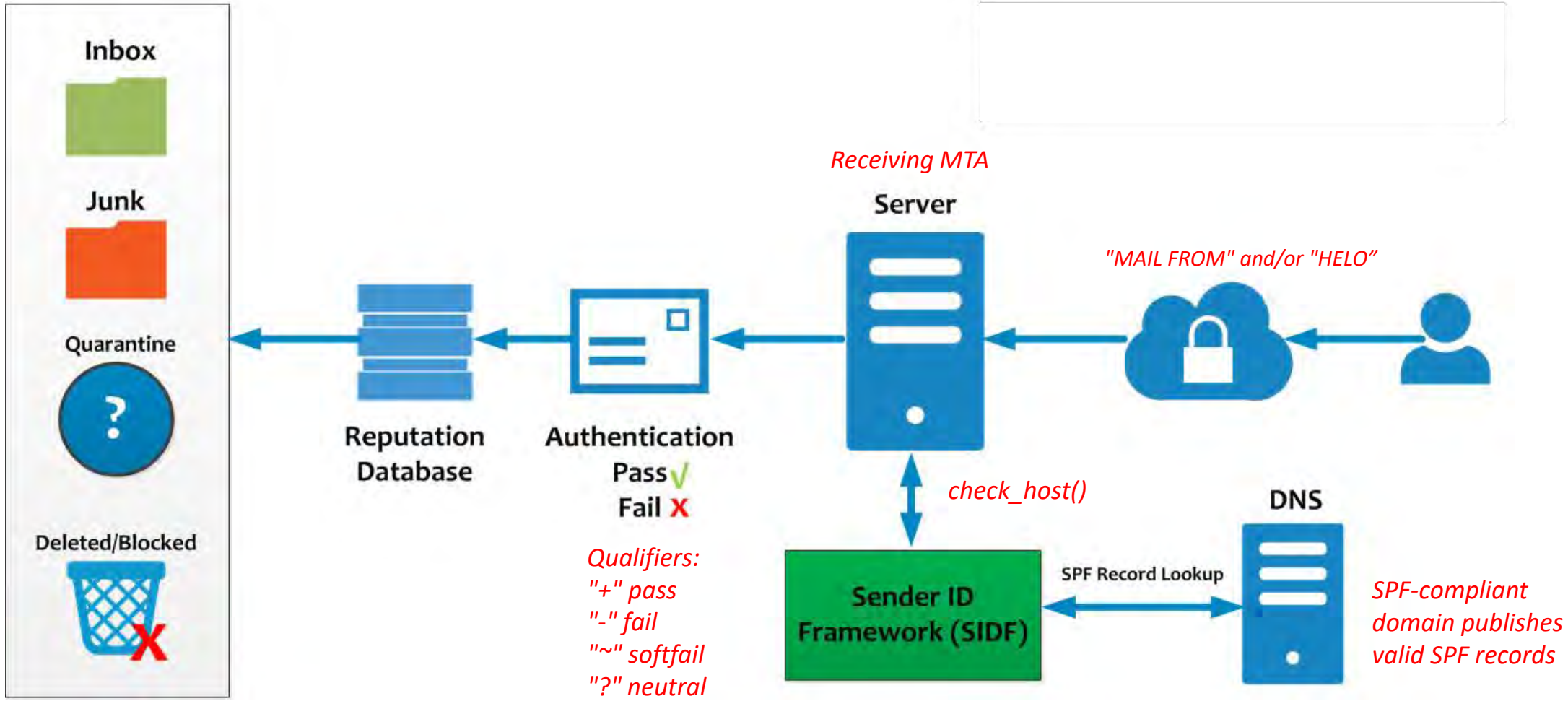
Dragon Advance Tech

Traditional Defense for Malicious Links and Attachments



Dragon Advance Tech

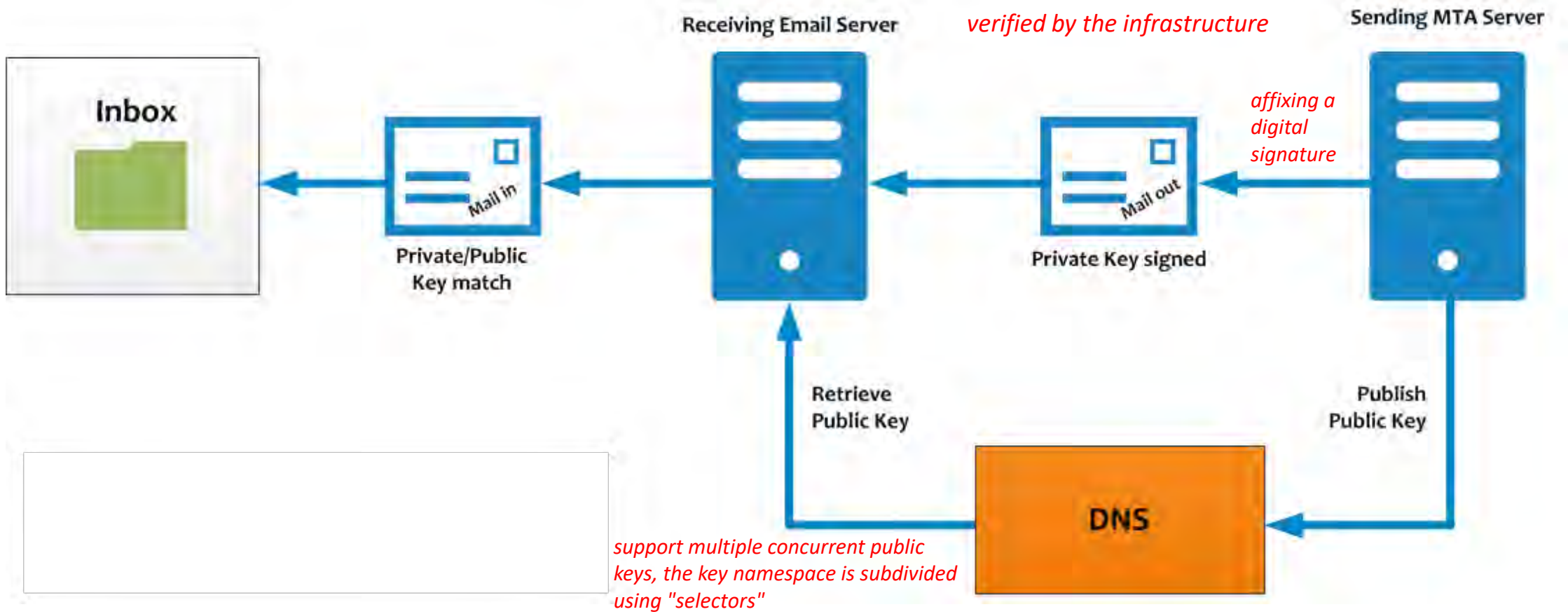
Sender Policy Framework (SPF)



https://tools.ietf.org/html/rfc7208

Dragon Advance Tech

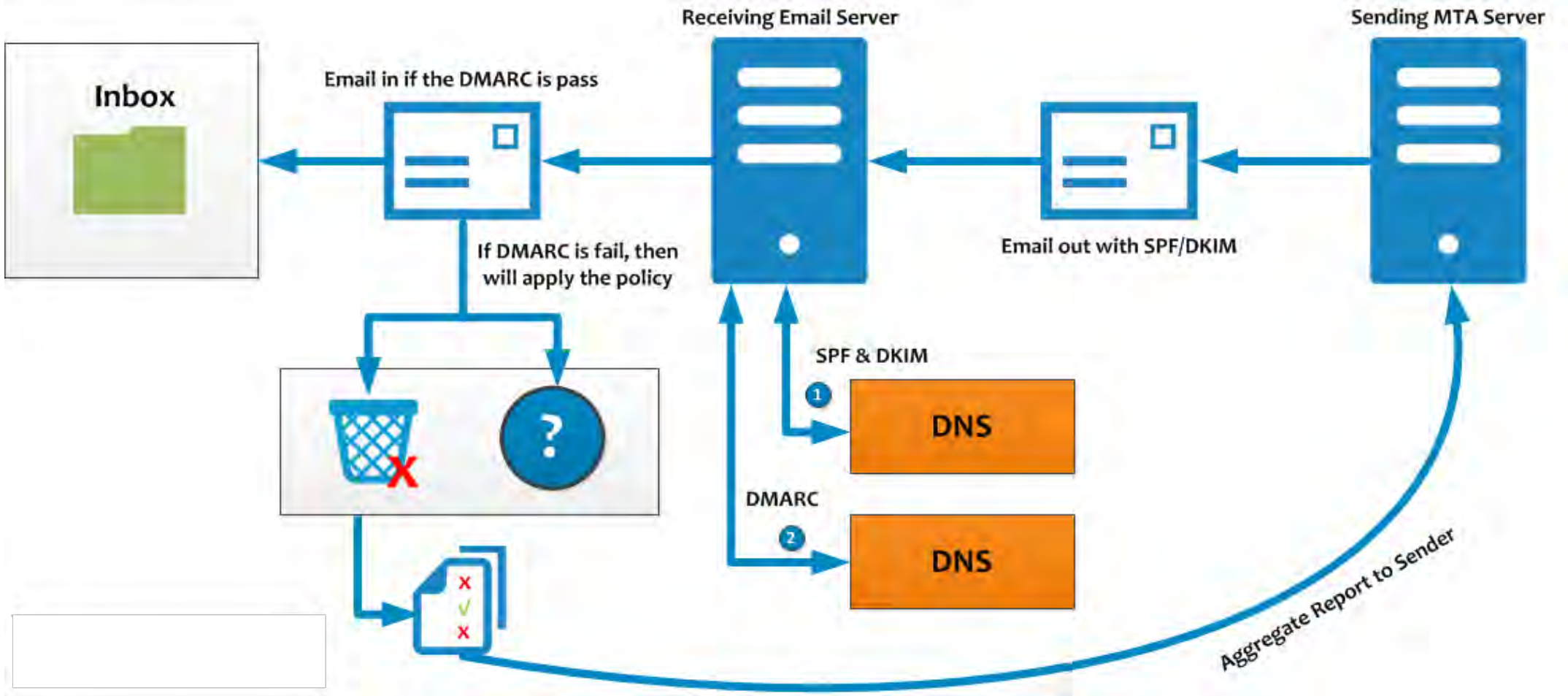
Domain Keys Identified Mail (DKIM)



https://tools.ietf.org/html/rfc4871

Dragon Advance Tech

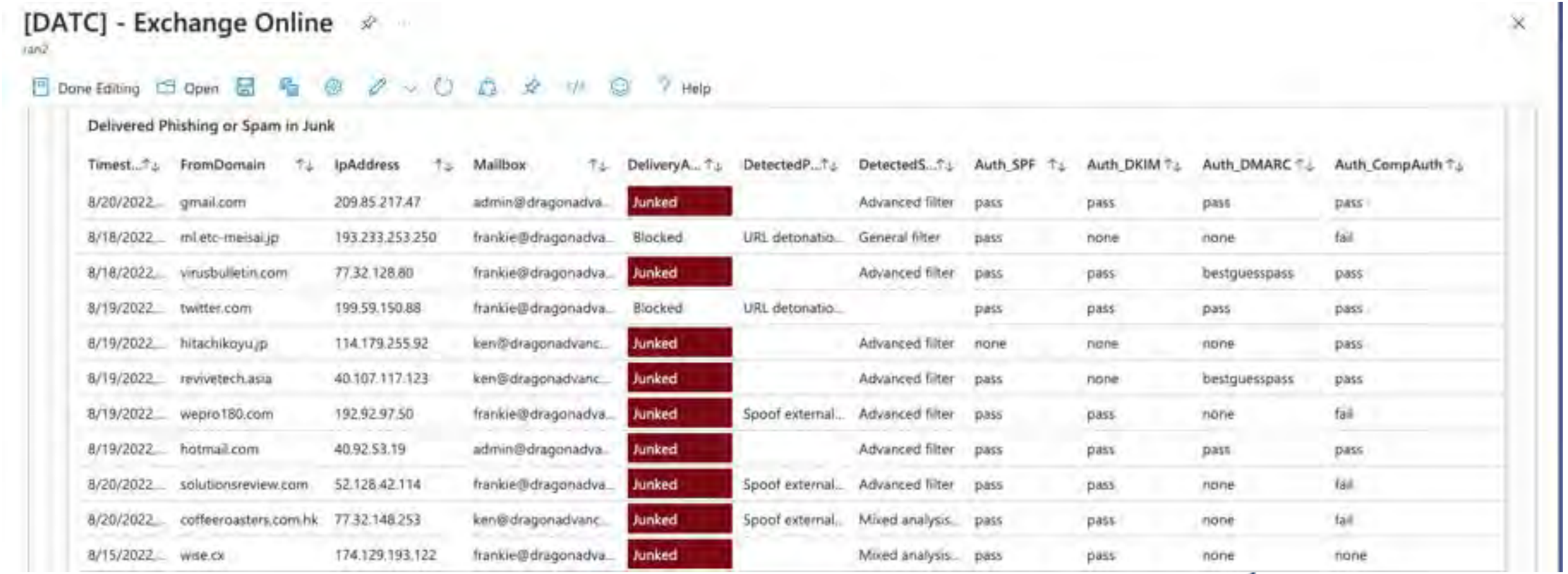
Domain-based Message Authentication, Reporting & Conformance (DMARC)



DMARC includes guidance on how to handle the "non-aligned" messages

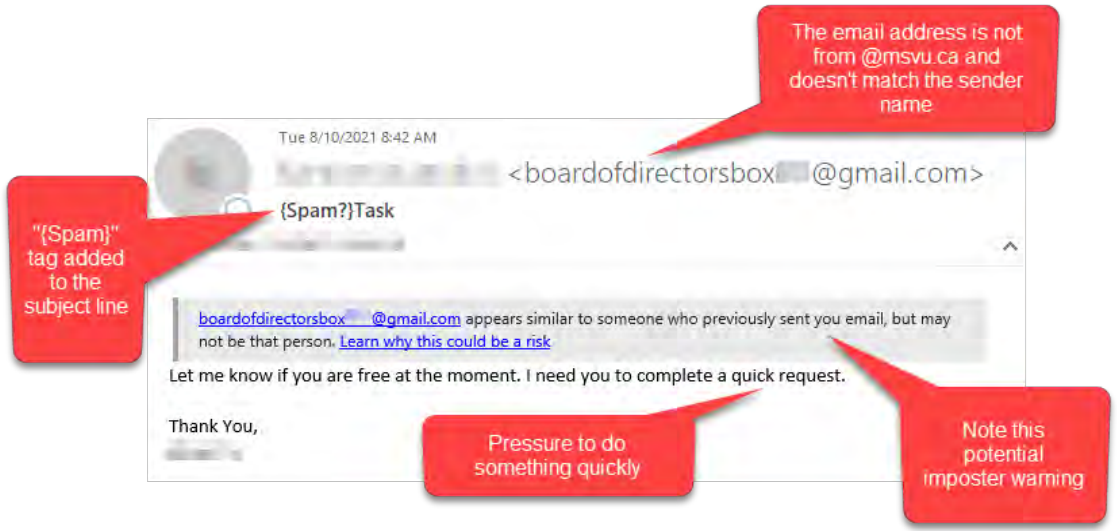
Dragon Advance Tech

AI-enabled Anti-Spoofing Technologies



Timest...	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...	wse.cx	174.129.193.122	frankie@dragonadva...	Junked		Mixed analysis...	pass	pass	none	none

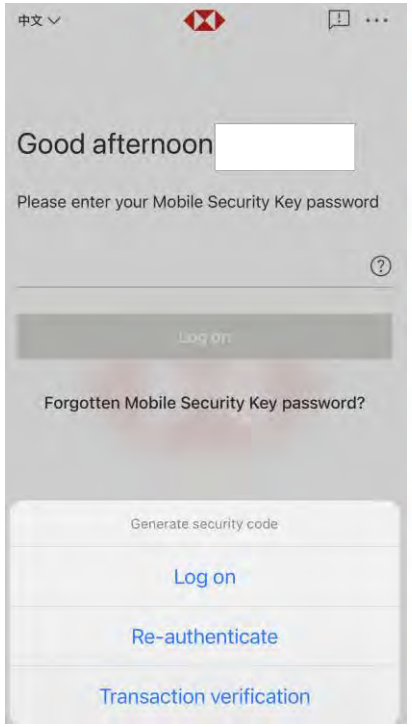
AI-enabled Anti-Phishing and Impersonation Tips

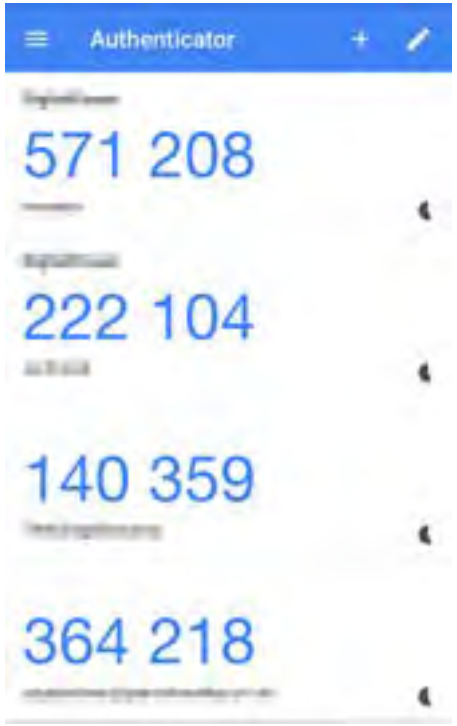


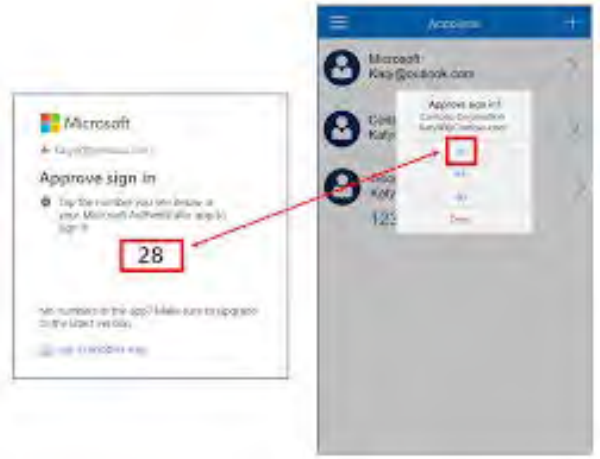
Dragon Advance Tech

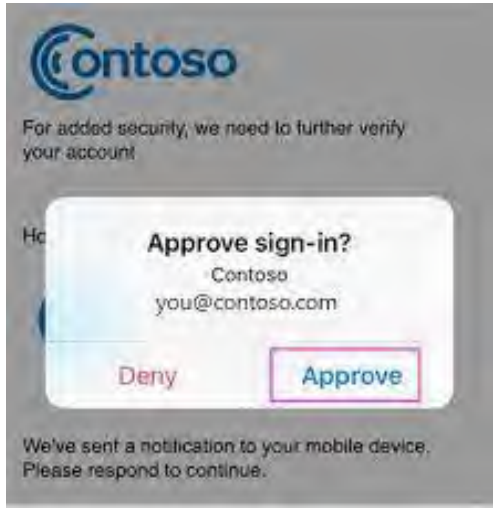
Identity Protection with MFA

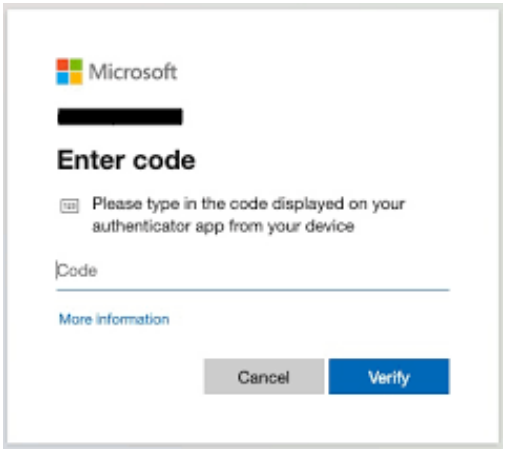
MFA is not a magic silver bullet to defense protect your Identity, but it is critical for all cloud/zero-trust access with multiple devices.









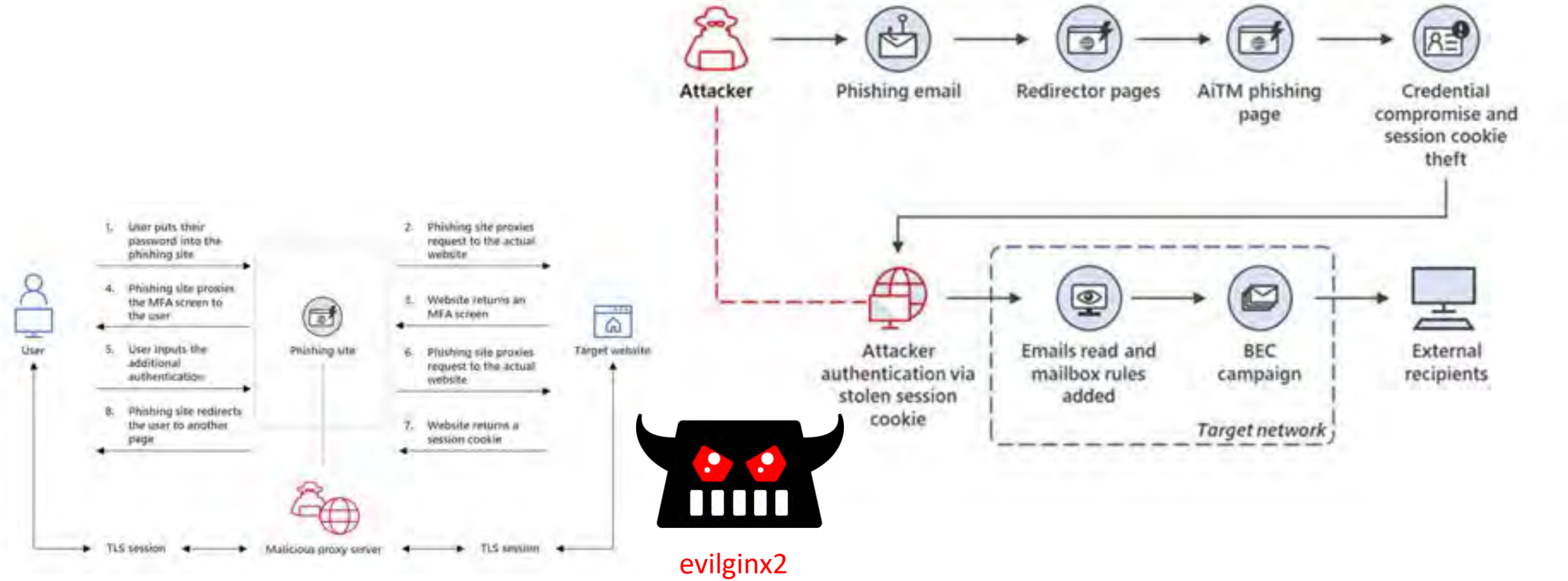


However, I see a lots of entities are not deploying such defense because of ignorance or not obtaining buying in from management.

Dragon Advance Tech

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

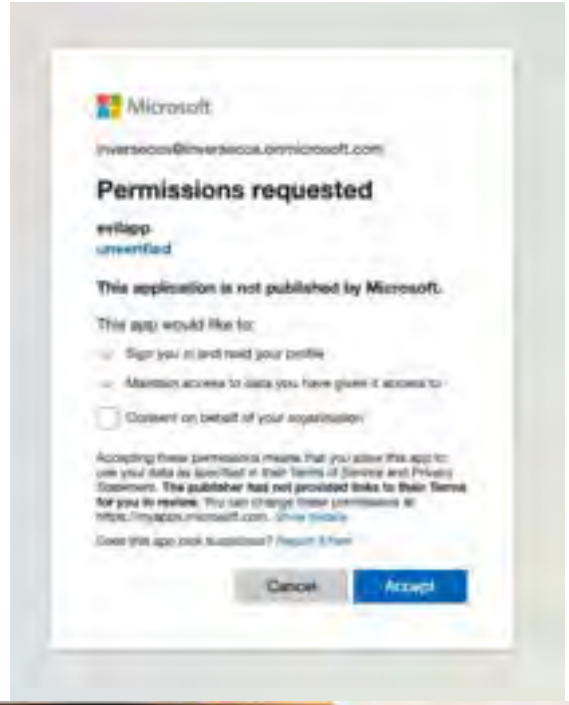
July 13, 2022 By Pierluigi Pagarini



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/

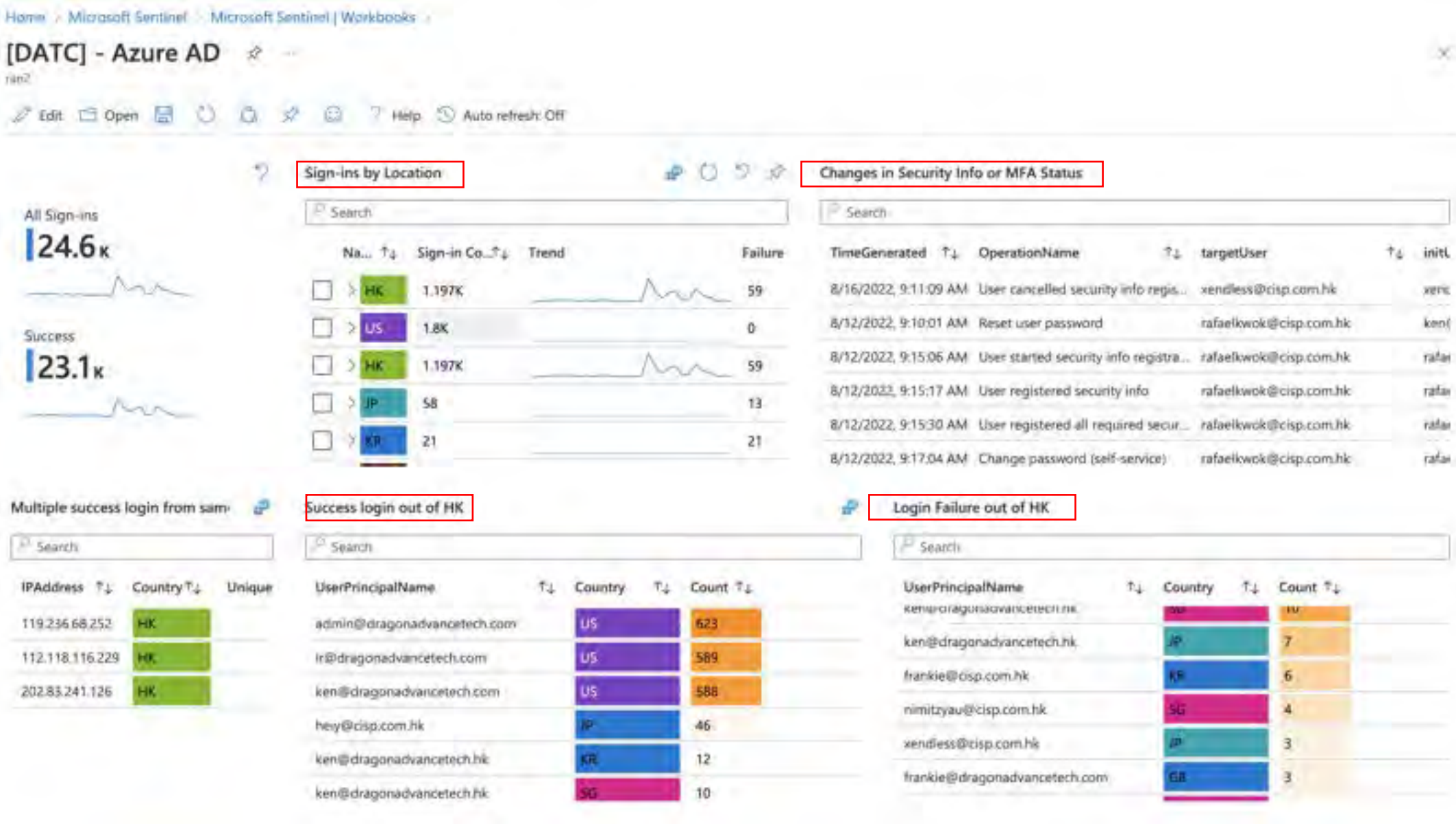
Email Threat Hunting and Response

Dragon Advance Tech

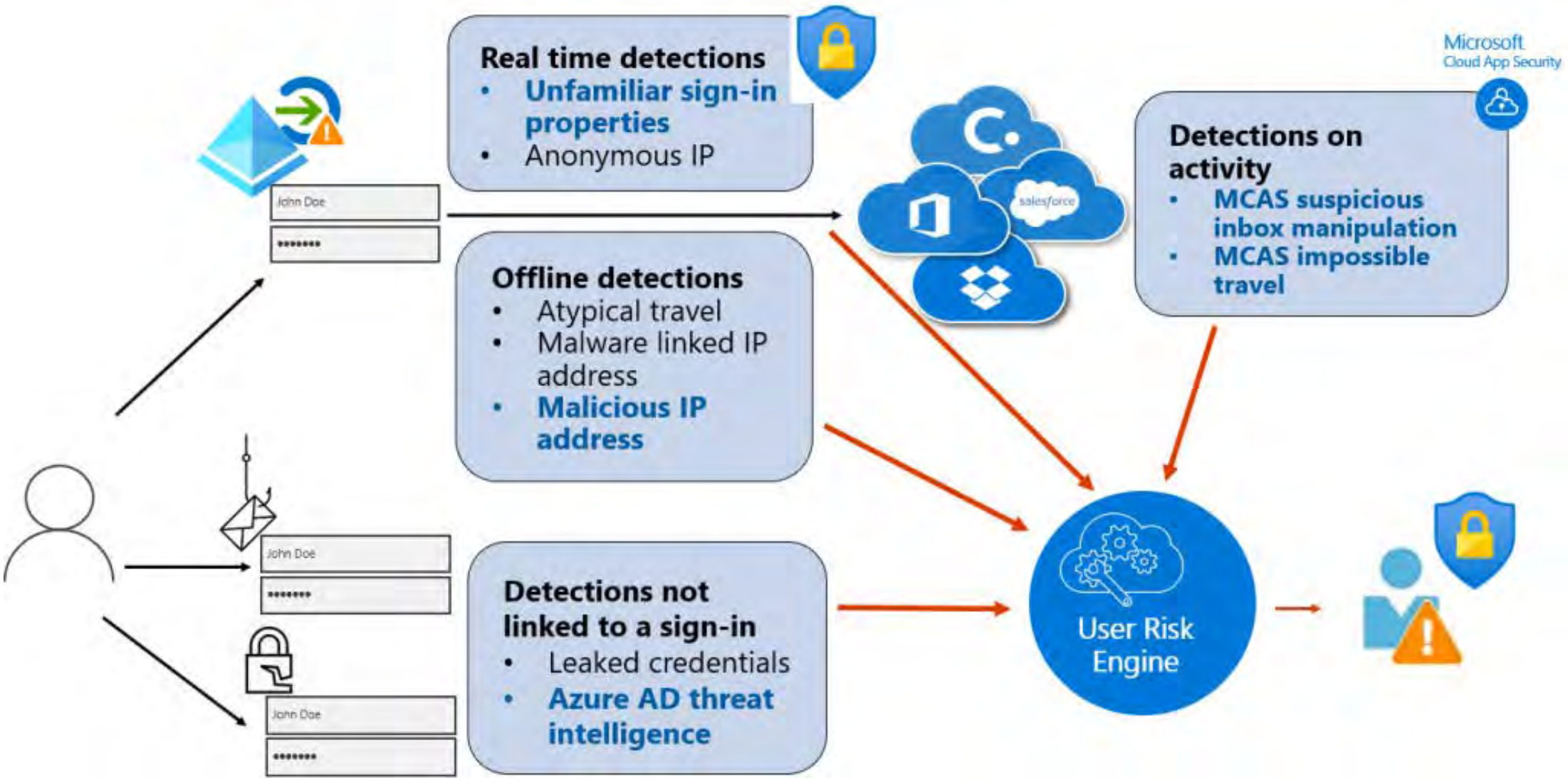
FINDING BEC ATTACK INDICATORS FROM EMAIL HEADER OR BODY?

- 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 …*

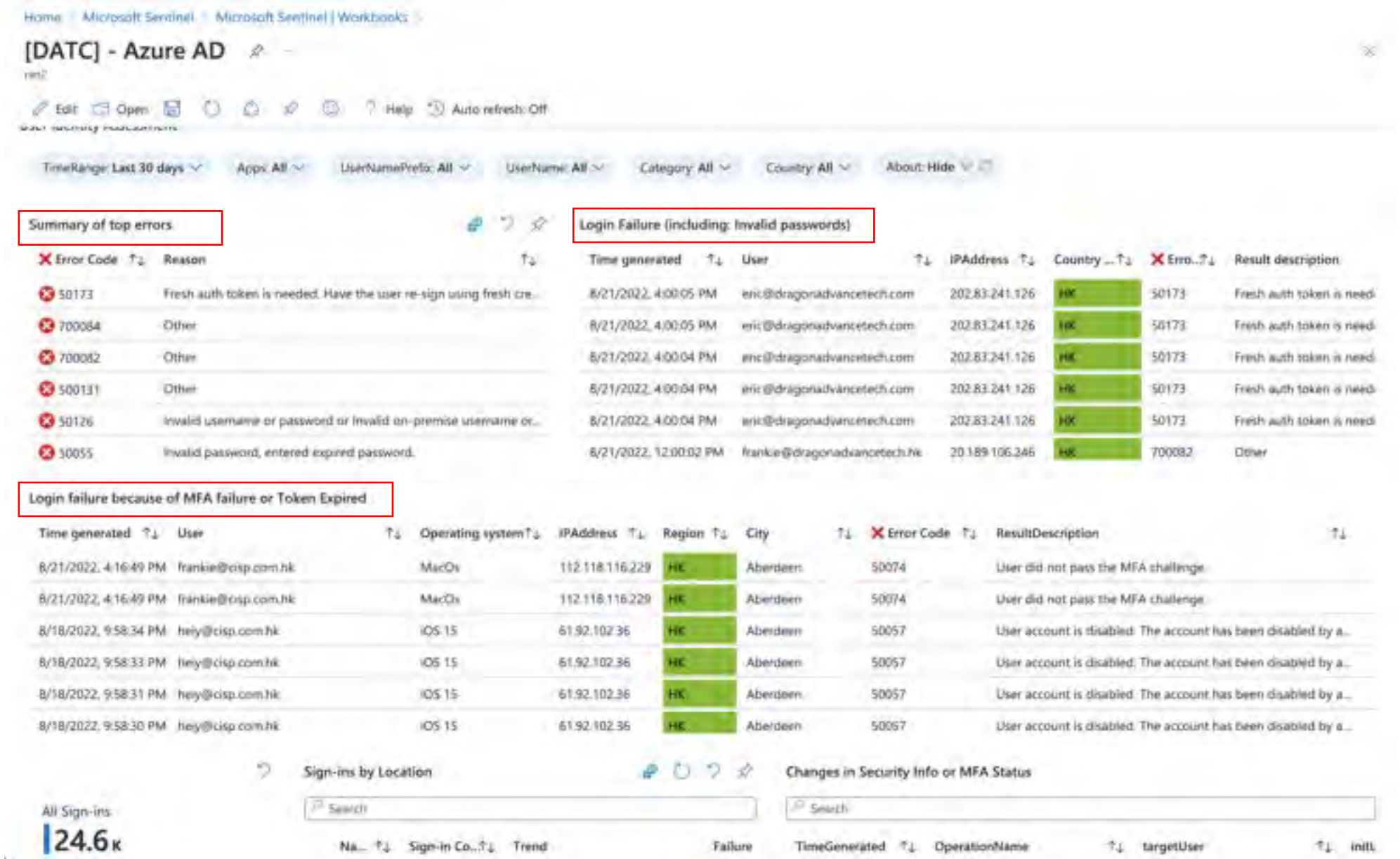
Identity: Sign-ins Assessment



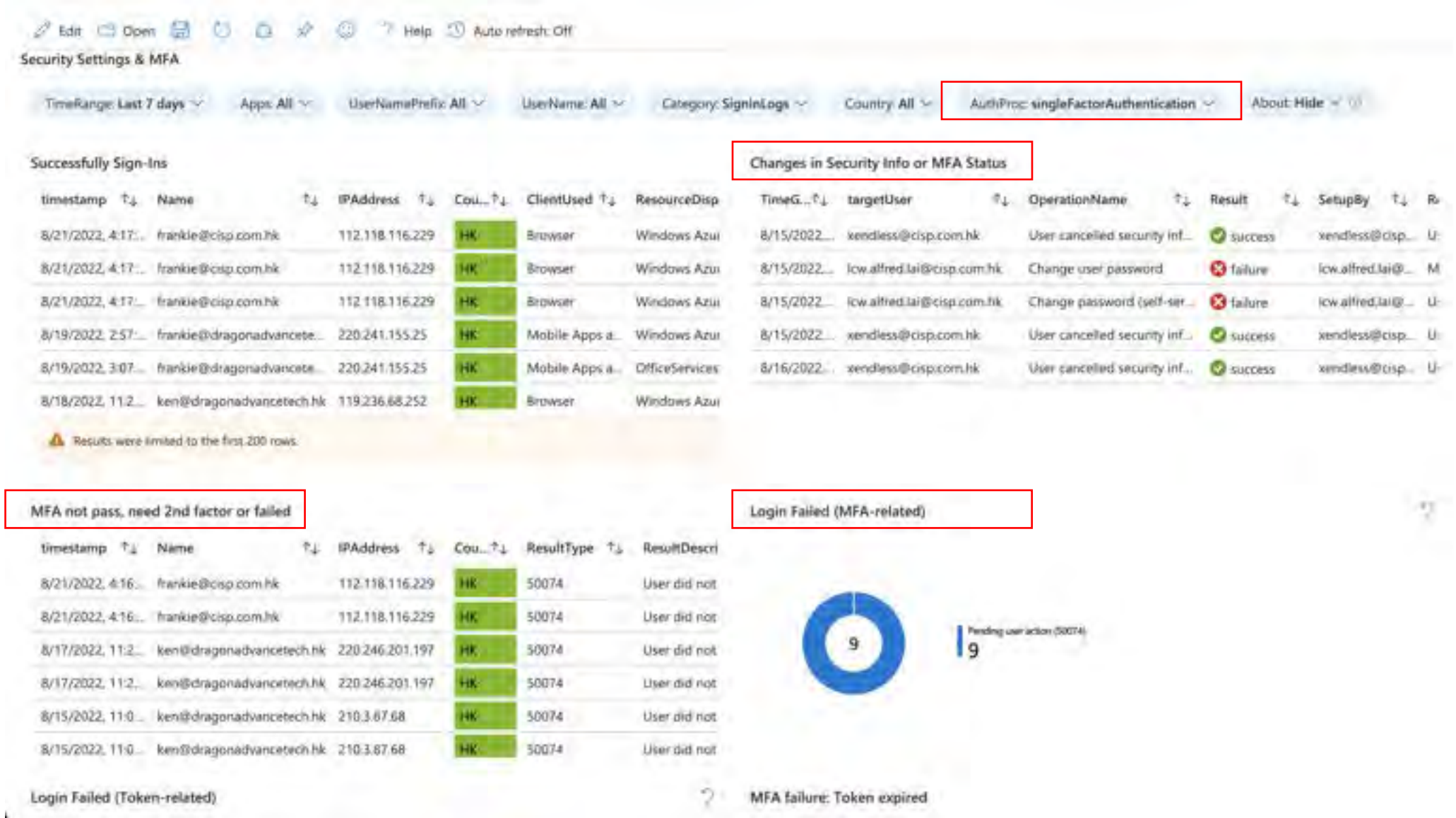
Identity: Impossible Travel Sign-ins



Identity: Suspicious MFA Sign-ins



Identity: Suspicious MFA Sign-ins




[DATC] - Exchange Online
Edit
Open
Help
Auto refresh: Off
Set rules operations - in detail
Search
TimeG...
UserId
User...
Key
Value
8/13/2022,...
Admin
Identity
Type
Shared
Confirm
Force
True
8/5/2022, ...
Admin
Identity
Type
Shared
Confirm
False
Force
True
Identity
Type
Regular
Confirm
False
Inbox rules operations by UserId
TimeG...
UserId
UserType
IP
Key
Value
8/22/2022,...
Steven
Andrew
Regular
160.72.
73.226.
Impair Defenses: Forwarding Rules
Transport rules operations - in details
TimeGenerated
UserId
UserType
Key
Value
7/28/2022,
Admin
FromAddressContainsWords
Name
block *.
com *.
.net
StopRuleProcessing
False

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,[5] 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.

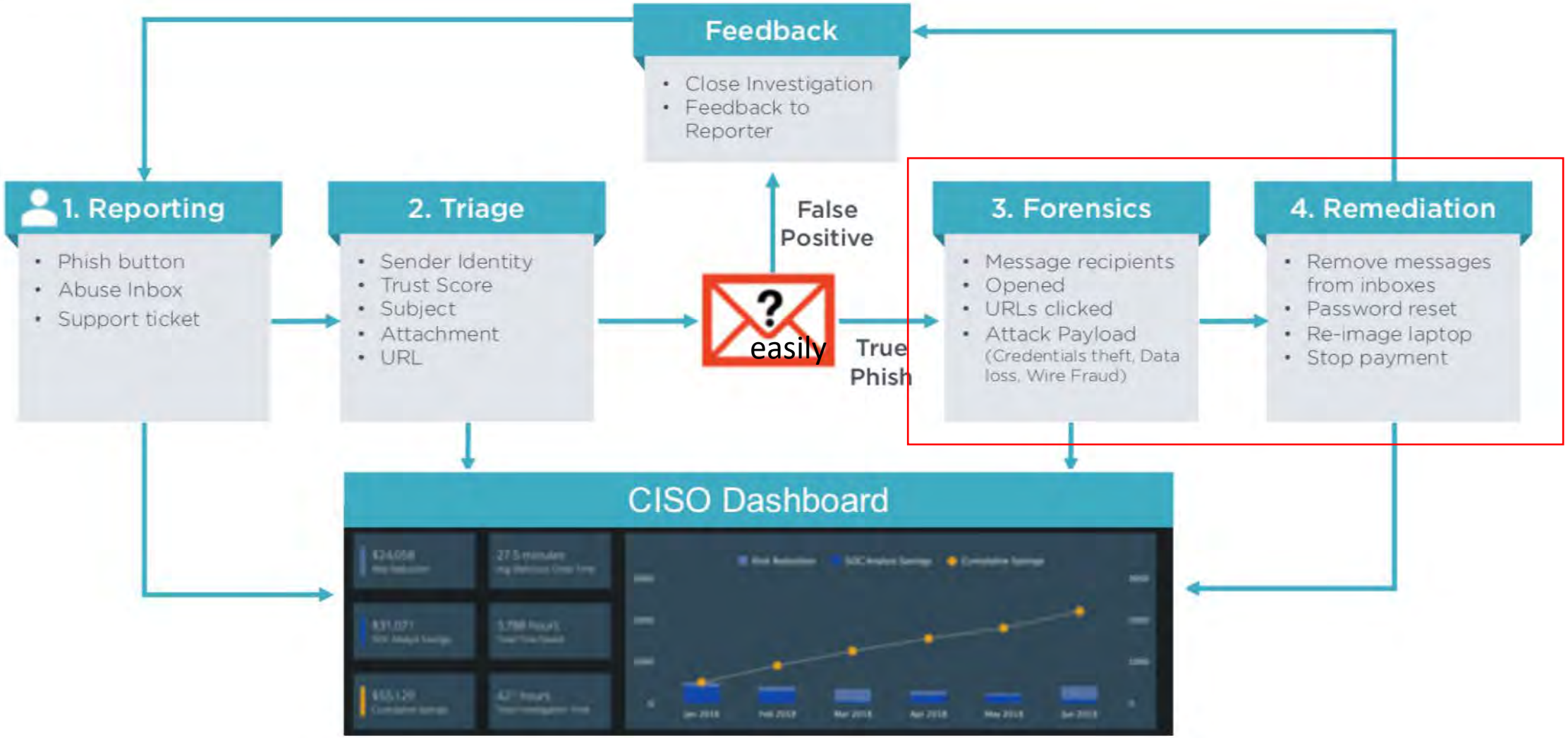
For example:

- 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:

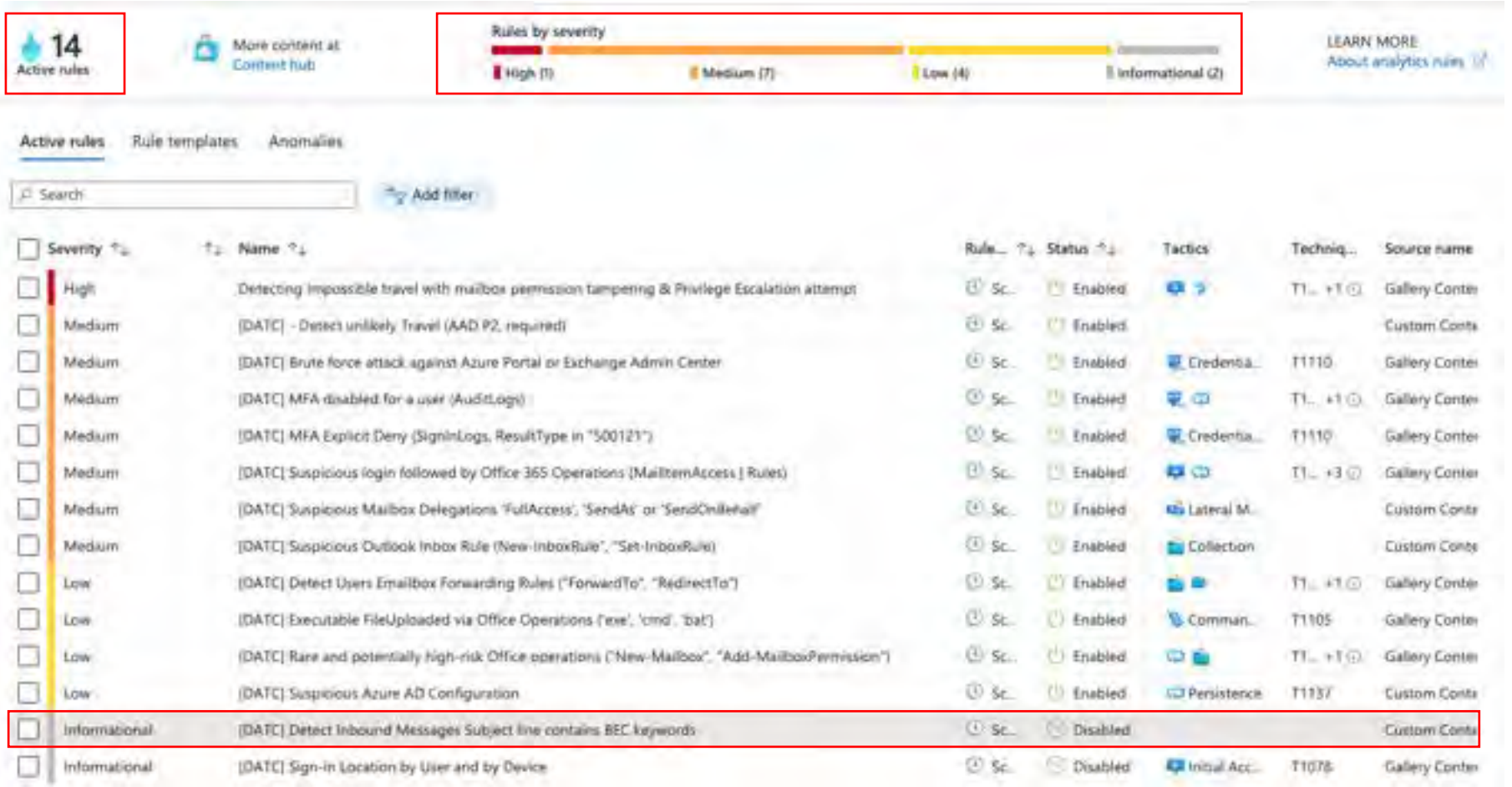
- "Spills" of classified information or other incidents that are believed to result from unintentional behavior only
- Users clicking on phishing emails when no compromise results
- Commodity malware on a single machine or lost hardware that, in either case, is not likely to result in demonstrable harm 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



Dragon Advance Tech

BEC Threat Hunting and Response



Dragon Advance Tech

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

Dragon Advance Tech