Intent-based approach to detect Email Account Compromise

Presented by:
Abhishek Singh & Fahim Abbasi

September 5, 2023

cisco | TALOS

Abhishek Singh

Research and Engineering Leader

Led research and detection engineering at FireEye, Microsoft, Cisco's Security Business Group

Holds 35+ patents on detection algorithms and security technologies, authored books in information security.

2019 Reboot Leadership Award (Innovators Category): SC Media, Nominee for Prestigious Virus Bulletin's 2018 Péter Szőr Award.

Double MS in Computer Science & Info Security from Georgia Tech, B.Tech. in EE from IIT-BHU, Master of Engineering Leadership program from UC Berkley, Post Graduation certification in AI from IIT Guwahati

cisco | TALOS

Fahim Abbasi, Ph.D.

Sr. Research Scientist Engineer

Cybersecurity Researcher and Data Science enthusiast

- 10+ of cybersecurity research experience

- Cisco Email Security technologies like ETD, ESA
- Detection algorithms: BEC, Phishing, Scams
- Based in Auckland, New Zealand

Security Researcher

- Trustwave (Mailmarshal): Email, BEC, Phishing and Scams
- FireEye (NX): Malicious URL, Phishing

Published several industry blogs, patents and academic journals and papers

cisco | TALOS

Email Account Compromise (EAC)

- EAC is a highly sophisticated cyber threat, affecting businesses globally.
- Threat actors gain unauthorized access to legitimate email accounts via
  - Phishing, Malware, Password Cracking etc
- Targets: personal, corporate, partner and customer emails
- Goal
  - Become You – the account owner
  - Financial crime: steal money
  - Data crime: steal data or sensitive information
- BEC/EAC attacks resulted in $2.7 Billion in losses FBI 2022 IC3 report

BEC vs EAC

BEC is a type of EAC, but not all EAC attacks are BEC attacks.

BEC

- A type of EAC that targets businesses
- Impersonate a trusted individual
- Conversational payload targeting businesses – e.g., fraud emails requesting payroll change, W-2 forms, aging reports or gift cards etc; impersonate a C-level executive requesting money transfers;
- Goal is to trick employees into sending money or sensitive information, redirect payments, change bank account information

EAC

- Any unauthorized access to any email account
- Becomes you – the account owner
- Leverage compromised corporate accounts to send phishing, scam, BEC and malware email lures, both internally and externally, to personal, and corporate contacts including partners and customers
- Goal is to steal money, steal personal information, send phishing, spam, malware, pivot and move laterally in an organization

cisco | Talos

EAC Challenges from a SEG

Most SEGs don't scan internal emails

- Defenses deployed at the perimeter for incoming emails makes it challenging.

Emails from compromised accounts

- originate from authenticated employees of the organization
- sent to internal employees (move laterally) or outbound to partners and customers
- Headers are legit, difficult to detect
- Authentication checks pass as mostly coming from Microsoft
  - bypasses controls like SPF, DKIM and DMARC.

Without Analysis of Emails:

- Anomalies in 0365 Login events features such as *UserId, UserAgent, ClientIP and Operation are used* to detect EAC e.g., changes in geolocation and user agent

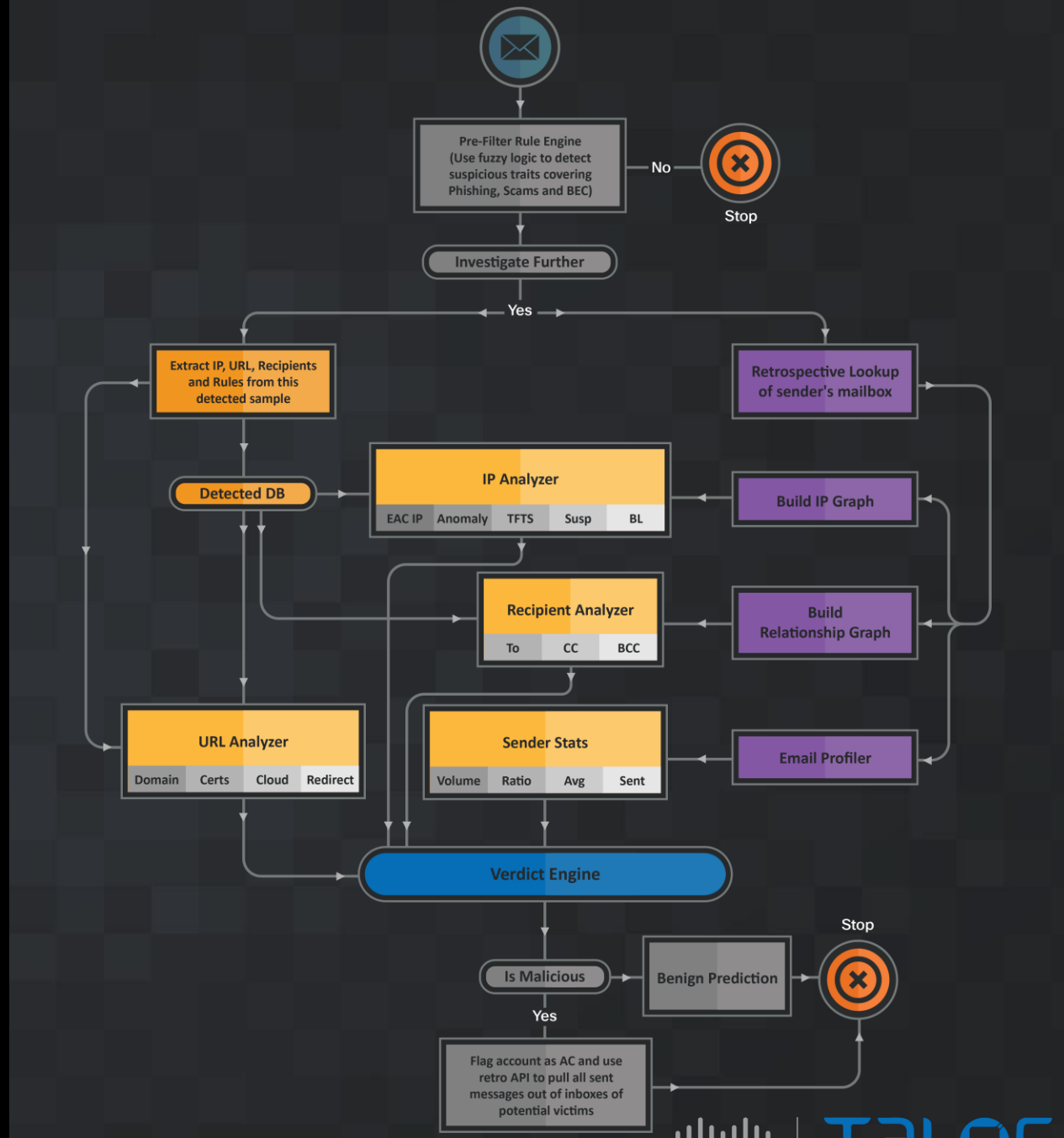
Solution to Detect EAC

With Email Analysis:

- Intent-based approach: detect EAC by isolating suspicious intent (phishing, scam, BEC etc) from internal and outbound emails. Sender's behavior is computed and correlated with features from emails to detect compromised account
- Leveraging XDR: Retrospective verdicts of Phishing URLs in emails can be compared with web gateway logs to detect if a POST request was sent, to determine the account got compromised.

Intent Based Email Account Compromise

Architecture



cisco | TALOS

Prefilter

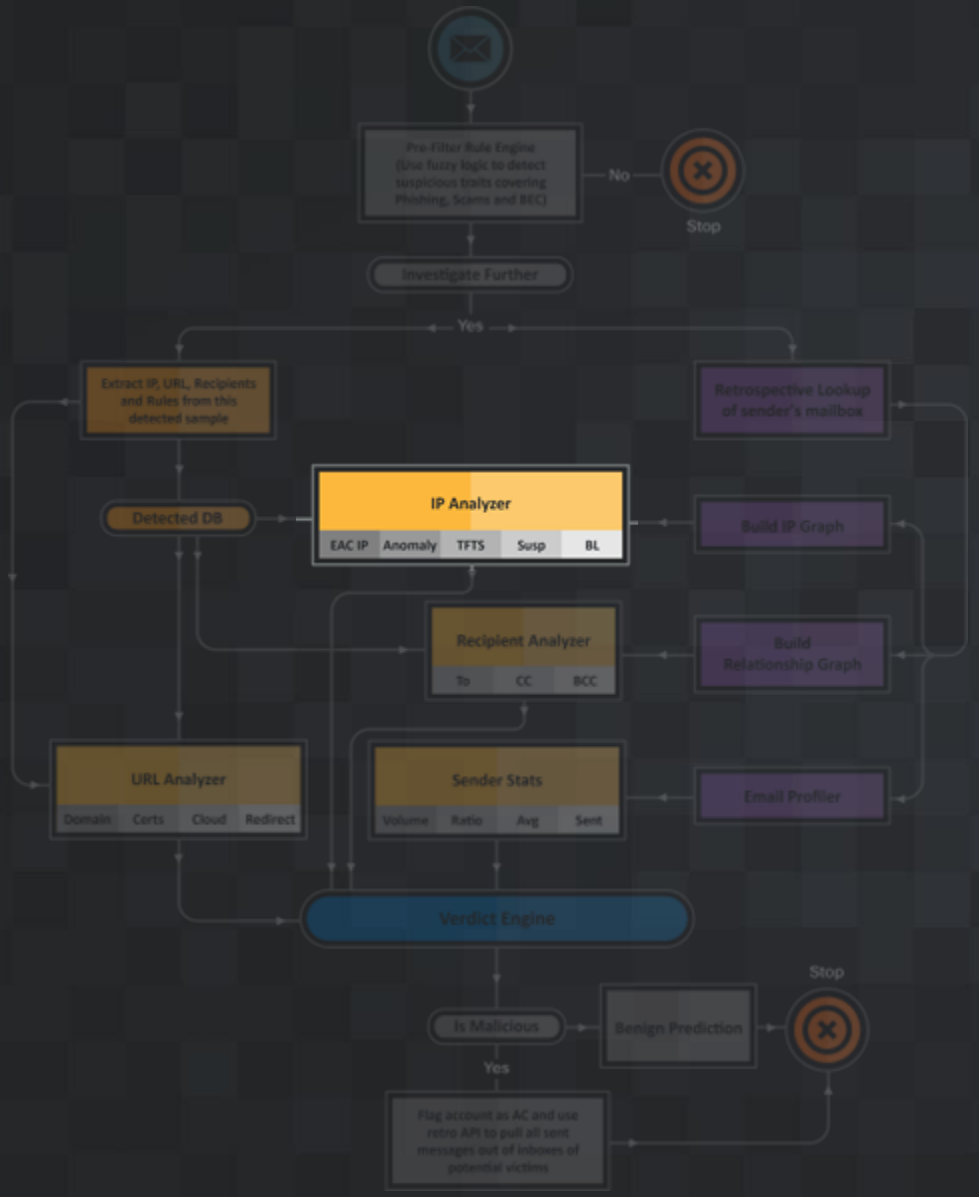
Intent	Examples of the High-Frequency Key Phrases
BEC	(Update change switch|need assist) my (direct deposit banking|paycheck) information, next (payroll salary), (text|send) me your (cell|mobile number), (need|purchase|surprise).*(employee|staff) with (gift|card), are you available, need (favor|assistance), (send|email). *(aging|W2|recievable), wire transfer
SCAM	Mutual benefit, good opportunity, invest. *(million|thousand hundred), reply with your (name|address|email|phone), (recieve|secure) (money|ATM|fund), (loan finance) money, business (venture|partnership), compensation for (scam victim), (late deceased) (husband wife father\mother), unclaimed (inheritence fund package), send payment to my (BTC bitcoin wallet), hacked your (computer laptop webcam), suffer terminal (cancer disease), donate (money|fund), won (jackpot|lottery|lotto), (United Nation|FBI) Fraud Claim, Covid (refund|settlement|fund), next of kin, invest fund, compensate scam victim, work from home, online job opportunity
Phishing	(Update|Change keep) password here, your account will terminate, (outlook 0365|mailbox) (storage reached access outlook account upgrade), password (change|reset|reactivate|account), follow activation link, (update| payment | verify) account

- Objective: Filter suspicious emails from internal and outbound traffic for further investigation
- NLP Based Approach: n-gram analysis to extract the top keywords and phrases mapping to the intent of threat actor such as
  - Urgency, Call to Action etc.
  - Money transfer request
  - BEC scams such as direct deposit, initial lure
  - Phishing lures with links
  - SCAM lures
- Volume: Fine-tuned to minimize the volume of prefiltered emails.
  - Isolates around 4000 suspicious emails from 20 M

  (0.000005% of emails are getting isolated)

cisco | TALOS

Retrospective Behavior Engine – IP Analyzer



- EAC-IP
  - Compare 3-tuple IP, Country and Subdivision of detected message with historical messages
  - Calculate a score between 0-mal and 1-benign
- Suspicious Country
  - Sender IP from suspicious countries like RU and IR
- Anomaly Detection
  - Use anomaly detection technique like clustering to detect anomalous IPs from any given user
  - IP, Geography and ASN used as features.
- Too Fast Too Soon
  - Sender IPs are changing too fast too soon.
  - Changing IPs are not from the same ASN
  - Changing IPs from far away geographies
  - Calculate miles per hour required to logon physically from source IP addresses

cisco | TALOS

IP Anomaly Detection -GMM

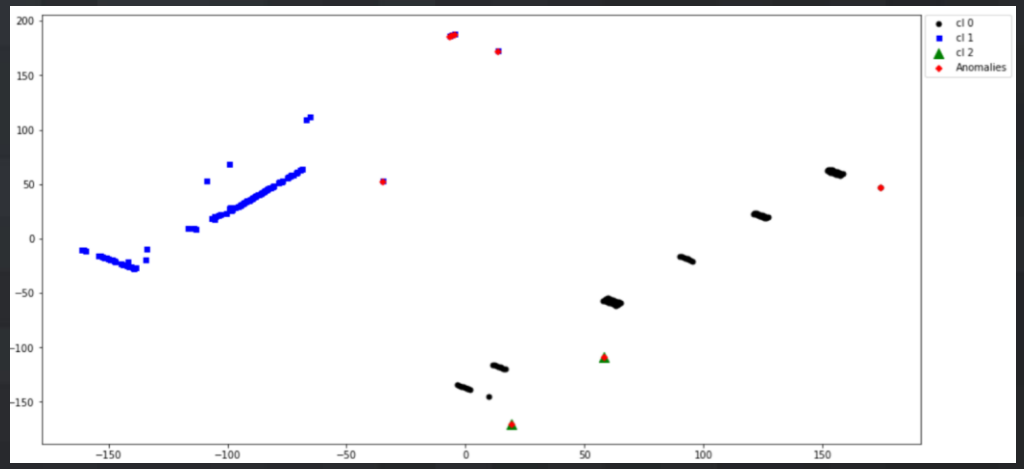
- Detect anomalies in sender's IP
- Build Clusters on retro sender IP's from last 90 days
- Suspicious IP not matching these clusters is considered an anomaly or outlier.
- Unique approach that uses IPs, Country code and ASN as features.
- Uses an unsupervised learning algorithm called Gaussian Mixture Model (GMM) clustering algorithm that is more suited for this IP data

Form clusters on IPs from last 90 days till yesterday

- Cluster 0: 89.212.157.101-118
- Cluster 1: 78.68.172.205-210
- Cluster 2: 5.158.217.169-175

Test all IP's seen today against known clusters, if not then its an anomaly

Anomaly: 195.178.120.219



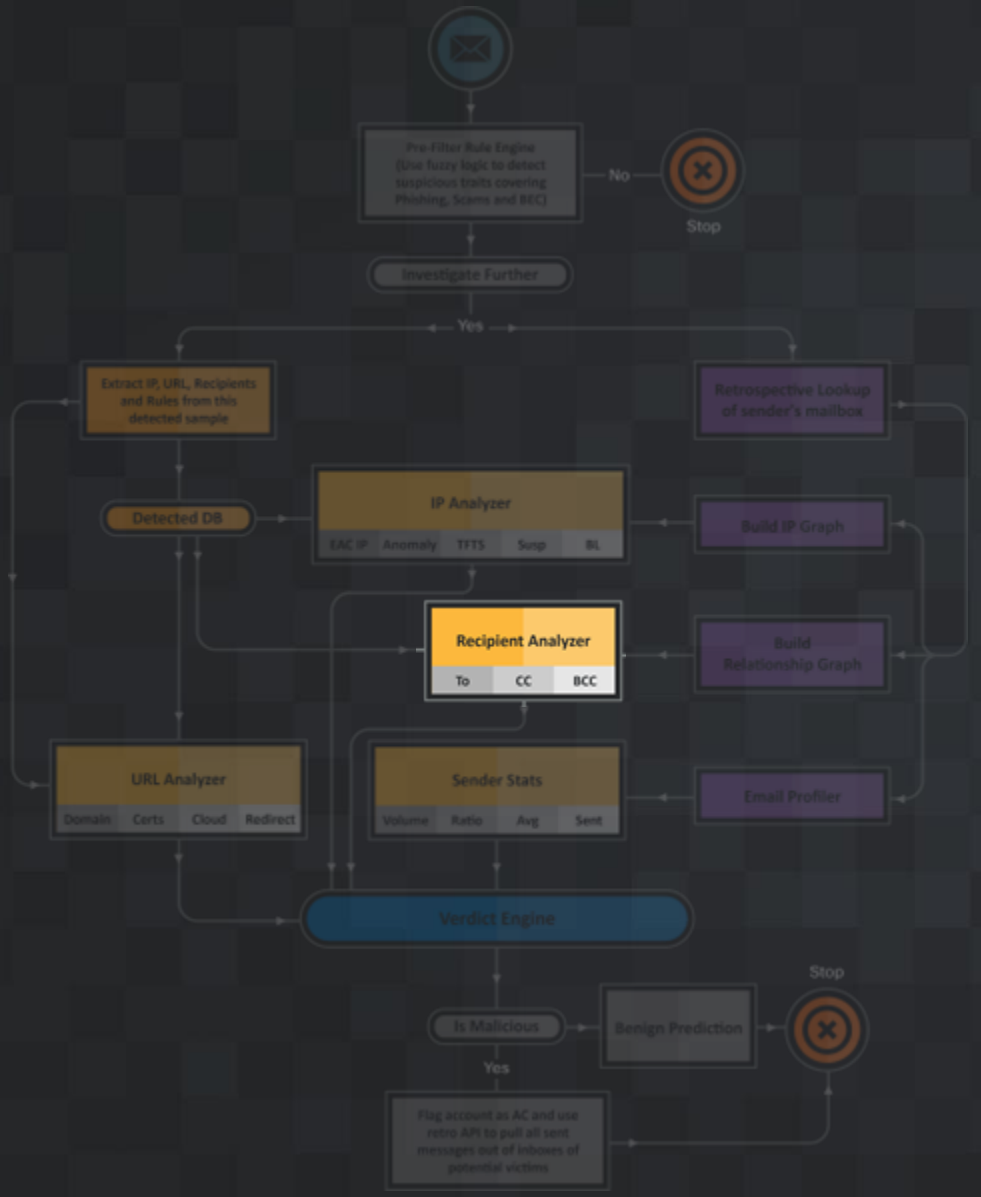
cisco | Talos

Too Fast Too Soon

Detect if email sender's IP changes too fast too soon between subsequent emails.

- FAST: Sender IPs are changing too fast too soon
  - Calculate time between changed sender source IP and distance in miles per hour
  - Calculate miles per hour required to logon physically from source IP addresses to determine if two logons are "geoinfeasible" based on distance and time
- ASN: Flag if ASN change detected
- DISTANCE: Changing IPs from far away geographies > 1000 miles
- Criteria: FAST + ASN + DISTANCE

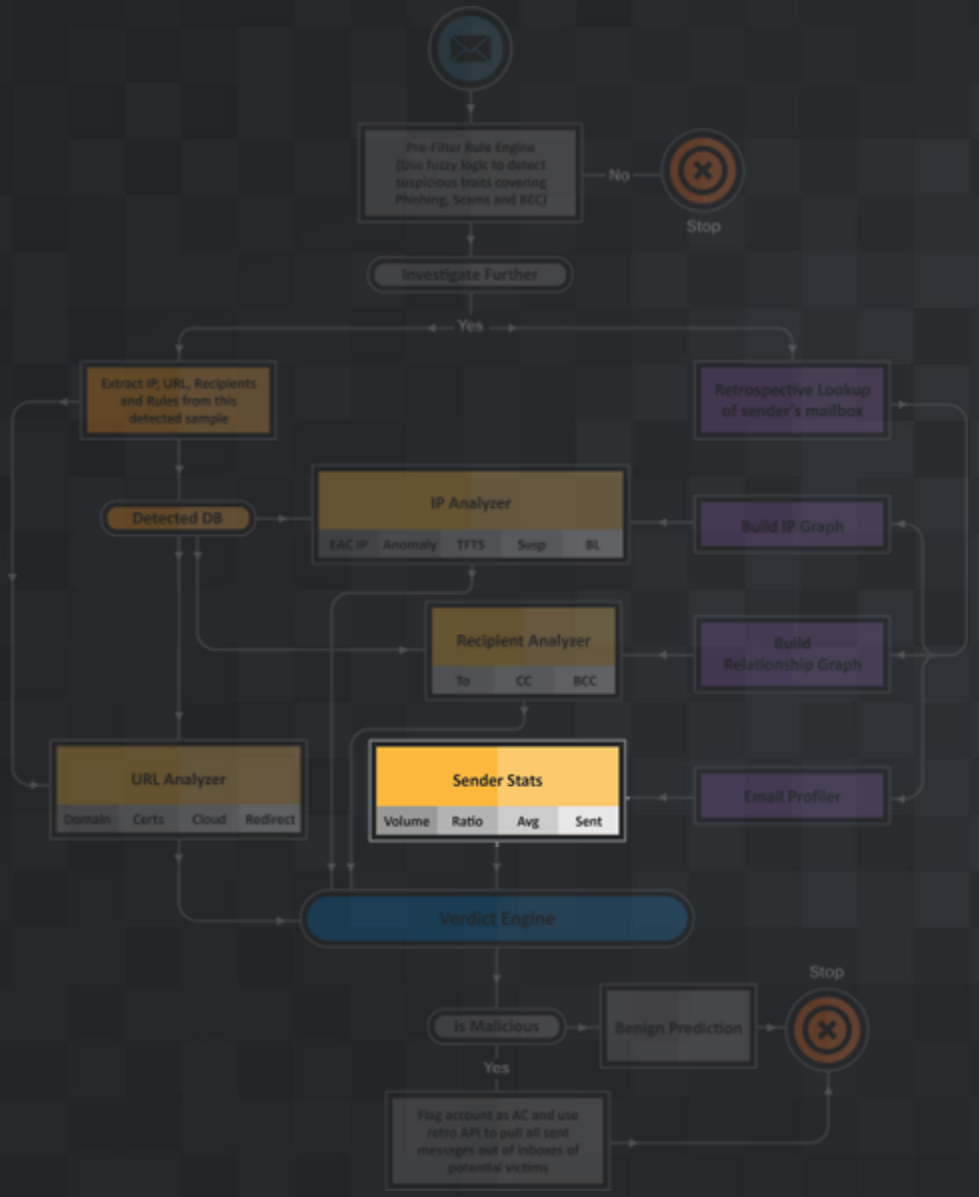
Retrospective Behavior Engine – Recipient Analyzer



- Retrospective Relationship Graph
  - Build relationship graph of suspected user by harvesting historical email data mainly To, CC, BCC fields from the last 90 days.
- Relationship Graph of suspected email
  - Compute list of recipients from the suspicious email's To, CC, BCC fields
- Compare suspected email recipients with relationship graph recipients to flag any new relation/conversation

cisco | TALOS

Retrospective Behavior Engine – Sender Stats



Volumetric Analysis

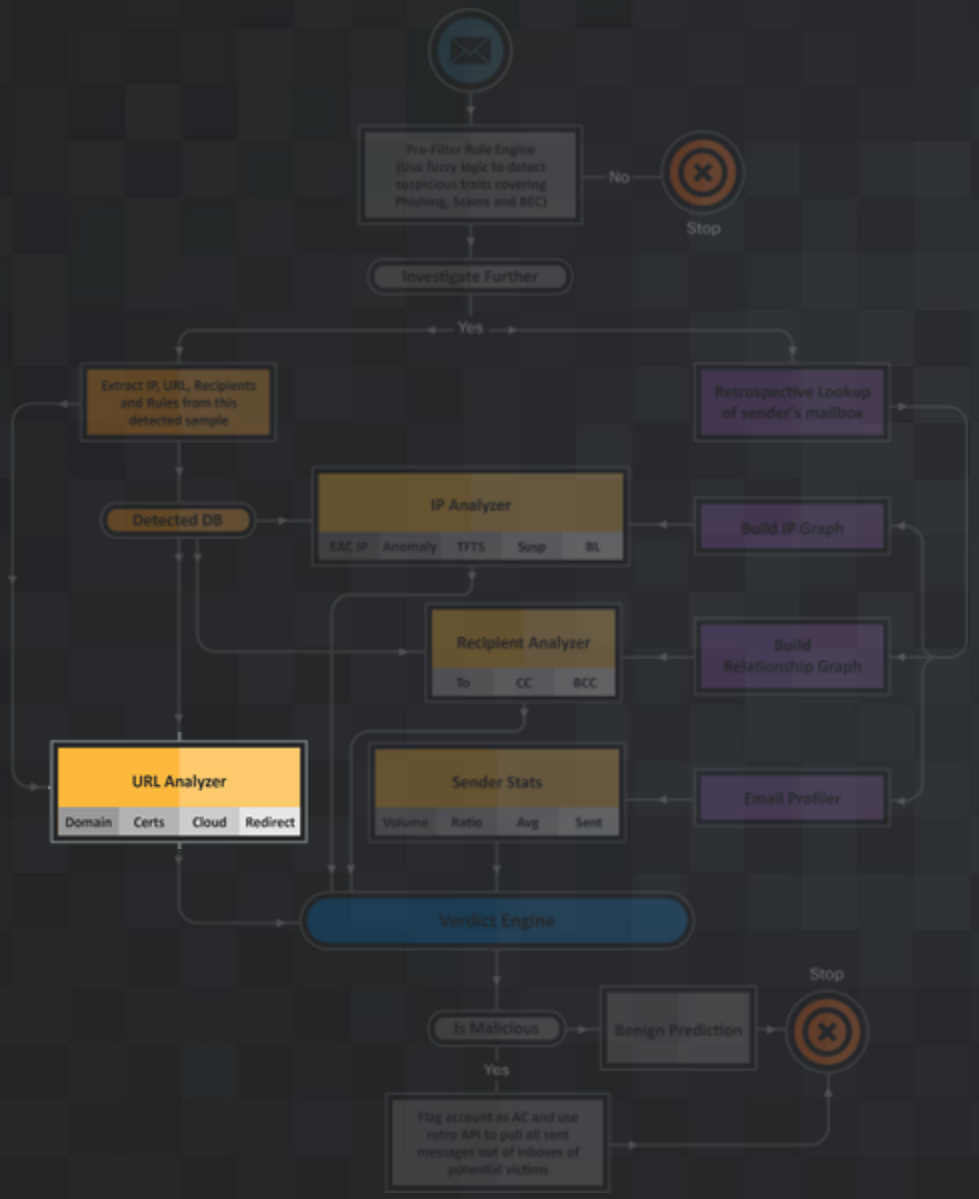
- Profile user's past email sending behavior and compare with today's behavior.
- Number of email sent today
- Avg number of email sent in the last 90 days
- Ratio of emails sent today compared to the past

$$\textit{Average number of emails sent} = \frac{\textit{Total number of emails sent in the past X days}}{X}$$

$$\textit{Vratio} = \frac{\textit{Total number of emails sent on the day suspicious email was detected}}{\textit{Average number of emails sent}}$$

cisco | TALOS

URL Analyzer



- Extracts all URLs from suspicious emails
- Detects Suspicious URLs using domain and URL algorithms
- Suspicious Domain detection
  - Exclude domains matching top 1 Million Umbrella list
  - *Domain Whois information checks*
    - *recently created < 6 months*
    - *expiring soon < 6 months*
    - *valid registrant org*
  - *SSL Certificate* checks
    - Stolen or Expired Certificate
    - Certificate issuing authority (cPanel,Let's Encrypt etc)
    - Expiry time of certificate < 6 months
- Suspicious URL Detection
  - URL contains an email as plain or base64 encoded
  - URL on file-sharing services like google forms, draw, drive, DocuSign, JotForm etc., or on cloud hosting
  - URL shorteners like Bitly, TinyURL, goo. Gl
  - Evasive feature in URL, such as google redirect

cisco | TALOS

EAC : Verdict Consolidation

- Consolidate output from multiple modules like volumetric analysis, recipient analysis, IP analysis, and URL analysis are correlated to give the verdict as malicious or benign
- Can be implemented as an expert system (human) or an AI/ML system
- 3 Verdicts: Benign, Suspicious and Malicious
- Multiple conditions to give Malicious and Suspicious verdicts after statistical analysis and manual fine-tuning
- Scalable solution to handle millions of internal emails per day

Malicious

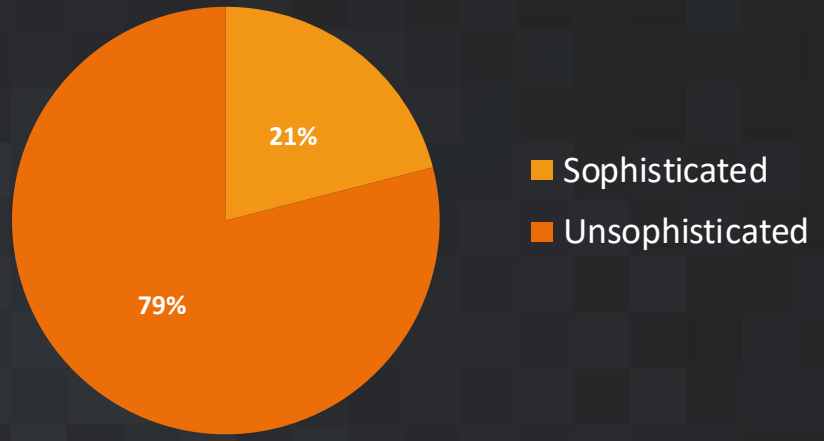
- ratio > 2 and eac < 0.5 and (anom > 0 or tfts == 'Suspicious') and (phish == 1 or cloud ==1 or redirect ==1) and (ip_rep == 1 or susp ==1)
- Ratio > 2: user has sent twice as many emails as in the past.
- eac < 0.5: sender's geo-location and IP address changed
- Anom: IP is anomalous not seen before
- TFTS: Too fast too soon triggered
- phish == 1: phishing URL present
- IP belongs to suspicious country with bad reputation

Preview inside EAC Cases

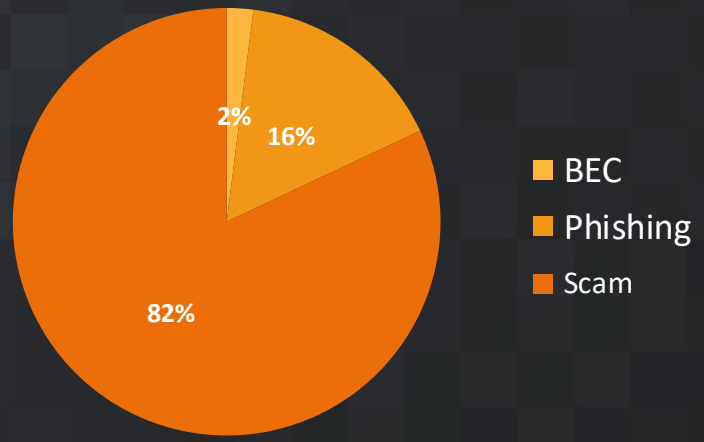
Threat Actors Intent

- Sophisticated vs Unsophisticated
  - Targeted vs spray-and-pray
  - ~80% spray-and-pray
  - Sophisticated Phishing URLs.
- Intent by Attack Type
  - Scam email: 82%
  - Phishing: 16%
  - BEC: 2%
  - Main Intent to collect credentials and personal information

Complexity of EAC Email

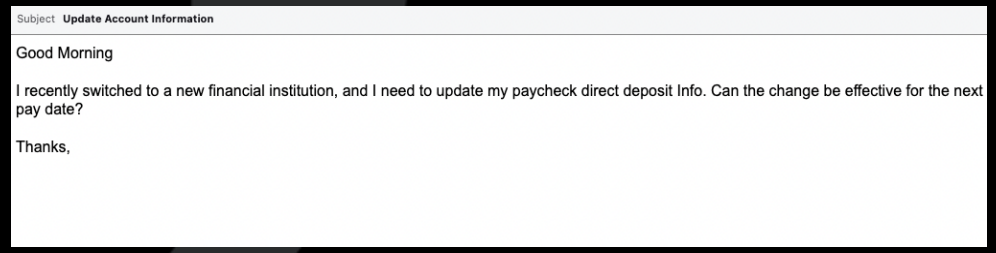


Types of EAC Emails Detected



cisco | Talos

Sophisticated EAC Attack - BEC Example


Subject **Update Account Information**

Good Morning

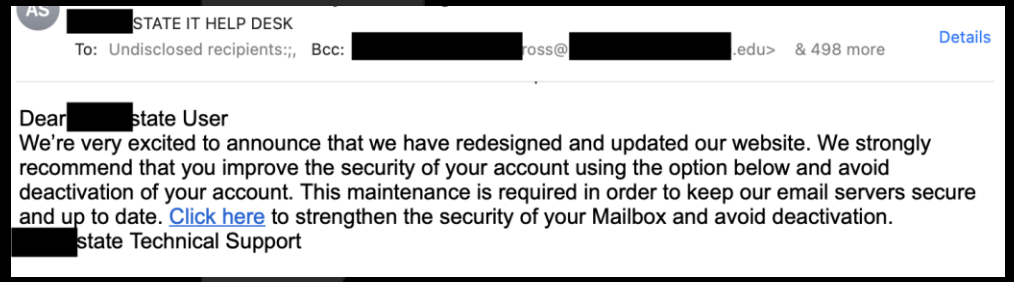
I recently switched to a new financial institution, and I need to update my paycheck direct deposit Info. Can the change be effective for the next pay date?

Thanks,

- Client: ABC SCHOOL DISTRICT
- Compromised account: john.doe@schooldistrict.org
- Sending IP belongs to suspicious country
- IP Reputation: Suspicious
- Sending IP Anomalies detected: Yes, 10 anomalies found corresponding to 10 emails sent one of which was BEC
- Historic IPs changing Too Fast Too Soon: False, only 1 IP used to send out all these emails
- Avg. Emails sent per day by this user in last 90 days: 0.7emails/day
- Emails Sent Today: 10
- Email Sent Ratio: 14 (email_count/avg_email)
- Uniq historical IPs seen prior to today: 17
- Prefilter: EAC_Prefilter_BEC

cisco | TALOS

EAC Phishing ITHelpdesk Example



[redacted] STATE IT HELP DESK
To: Undisclosed recipients:;, Bcc: [redacted]ross@[redacted].edu> & 498 more Details

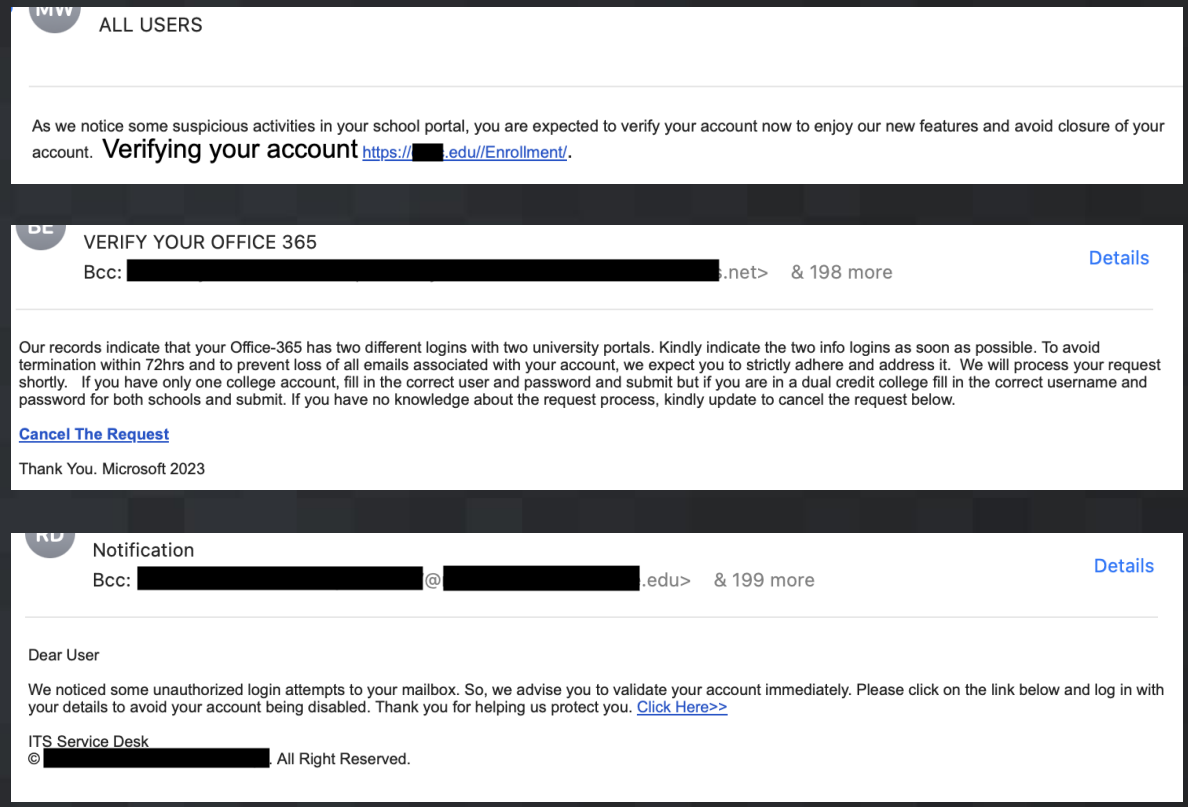
Dear [redacted]state User
We're very excited to announce that we have redesigned and updated our website. We strongly recommend that you improve the security of your account using the option below and avoid deactivation of your account. This maintenance is required in order to keep our email servers secure and up to date. Click here to strengthen the security of your Mailbox and avoid deactivation.
[redacted]state Technical Support

- Client: ABC STATE UNIVERSITY
- Compromised account: john.doe@stateuni.edu
- Avg. Emails sent/day by this user in last 90 days: 0.9emails/day
- Emails Sent Today: 78
- Email Sent Ratio: 86 (email_count/avg_email)
- Sending IP belongs to suspicious country
- Sending IP Anomalies detected: Yes, 78 anomalies found
- Historic IPs changing Too Fast Too Soon: True
- IP Reputation: Suspicious
- Prefilter: EAC_Prefilter_Phishing
- Final Verdict: Malicious

cisco | TALOS

EAC Attack Trends - Phishing

- Majority phishing lures were sent out to large org groups in a spray-and-pray strategy.
- Most lures were Office 365 account termination or upgrade/renewal lures.
- Other lures include Fake Docusign, fake Sharepoint etc
- Phishing URLs mostly pointed to data collection services like Google Forms, Jotform, Office forms etc
- Some campaigns targeting academia asked the victims to supply credentials of their current and prior school/university



ALL USERS

As we notice some suspicious activities in your school portal, you are expected to verify your account now to enjoy our new features and avoid closure of your account. Verifying your account https://[redacted].edu//Enrollment/.

VERIFY YOUR OFFICE 365

Bcc: [redacted].net> & 198 more Details

Our records indicate that your Office-365 has two different logins with two university portals. Kindly indicate the two info logins as soon as possible. To avoid termination within 72hrs and to prevent loss of all emails associated with your account, we expect you to strictly adhere and address it. We will process your request shortly. If you have only one college account, fill in the correct user and password and submit but if you are in a dual credit college fill in the correct username and password for both schools and submit. If you have no knowledge about the request process, kindly update to cancel the request below.

Cancel The Request

Thank You. Microsoft 2023

Notification

Bcc: [redacted]@[redacted].edu> & 199 more Details

Dear User

We noticed some unauthorized login attempts to your mailbox. So, we advise you to validate your account immediately. Please click on the link below and log in with your details to avoid your account being disabled. Thank you for helping us protect you. Click Here>>

ITS Service Desk
© [redacted]. All Right Reserved.

cisco | TALOS

Complexity of Phishing Links

Data collection forms

- hxxps[:]//docs.google[.]com/forms/d/e/1FAIpQLSeVJ38UInmc7lX6_sSSIlVyahq2b0k2jkRNKUgkIv-LMNWMWQ/viewform?usp=pp_url
- hxxps[:]//forms[.]gle/73KLav2zFGX9r4kS7
- hxxps[:]//docs.google[.]com/drawings/d/1gqRAYNczzxrmn9rN5-0e3xLNeUyXJFDoloocuZihgFQ/preview
- hxxps[:]//forms.office[.]com/r/kVXQU27PLV

Redirects

- hxxps[:]//www.google[.]com/url?q=https%3A%2F%2Fnaughtymilfl5vj.com%2F%3Futm_source%3DRgVunY3DTnByC7%26utm_campaign%3Dren&sa=D&sntz=1&usg=AOvVaw0Tty-URzTvXXWirDtwHI3o
- https[:]//www.bing.com/ck/a?!&&p=6e9a1f3929ba4ff2JmltdHM9MTY4NTkyMzIwMCZpZ3VpZD0xNGQyOGJiMS0wNDI5LTYzZTEtMTQ1Yy05ODk3MDU5YTYyZWUmaW5zaWQ9NTE3Nw&ptn=3&hsh=3&fclid=14d28bb1-0429-63e1-145c-9897059a62ee&u=a1aHR0cHM6Ly93d3cuZm9yZXN0YmF0aGluZ3N1ZmZvbGsuY29tL21vdmluZ3NwYWNlLW1vdmVtZW50LWNsYXNzZXM#amphbmRyYWluQGJ1dHRlcmJhbGwuY29t

Free hosting providers

- hxxps[:]//outlookfacepage.weebly[.]com

URL Shorteners

- hxxp[:]//bit[.]ly/SOMEUNI_EDU

EAC Attack Trends -Scam

Majority scams were Job scams luring students and financially vulnerable victims to provide their personal data and use them as money mules.

Romance Scams make up the other big category, followed by smaller advance fee scams

Job, Romance and advance fee scams are sent with a spray-and-pray strategy with the goal to maximize reach.

BEC Payroll Scam attacks were targeted.

cisco | TALOS

EAC - Scams

Hello!
I understand that we do not know each other, but I decided to take a chance and write you a letter.
I hope my letter reached you and you don't mind receiving the message.
I am writing to you with the hope of meeting an interesting person or finding a new friend.
I noticed that we have a lot in common in our interests, and I would like to get to know you better.
Let me share with you a few words about myself:
My name is Simona, I am 30 years old, I work as a photographer and love to travel.
I like to spend time in nature and cook delicious meals
In addition, I really appreciate smart and
polite people, and I think that you can be one of them.I
I hope that my letter will not cause you any unpleasant feelings.
I'm not used to making the first move,
but I couldn't pass up the opportunity to write to you.
I have been living here for about four months.
All my friends are related to work, and when we meet, we talk only about it.
And I need to find not just a friend, but a person with whom we can spend our free time
That is why I decided to try to find new friends on the Internet,
where I think you can find people with similar interests and hobbies.
And I believe that you are a decent and kind man who I liked :)
If you don't mind, I suggest starting an acquaintance
on the site in order to avoid unpleasant situations.
For me, and for you, safety is very important, I think you will agree with me
It's very easy to find me. Here is all the information about me Snowflake_lady
I am waiting for your response on the site
and I hope we will have more than just friendship

NL

UNICEF Part-time Job opportunity

To: [redacted]@unicef-jobs.org> Bcc: & 91 more Details

Good morning and Happy New Year.

I am sharing a winter job opportunity with anyone who might be interested in a paid temporary job over the break and in the new year with a weekly pay of $500.00 (USD).

Attached is further information about the employment details. Kindly follow the steps in the attached document and send a message with your alternate/non-school email address (i.e., Gmail, Yahoo, Hotmail, etc.). For more details on the job,

Take note: this is strictly a work-from-home position.

Hello!

This is to notify you about an available part-time vacancy. Mr. Mike Kem needs a part-time Personal Assistant Position in your area.

He offers to pay five hundred dollars ($500) weekly. Please send your Full Name and Phone Number to (mikekemfortross@hotmail.com) for more information. Remember to email Him with your private email or your school email when applying.

Thanks

AD

THIS EXTRA OFFER IS FOR YOU!!

[redacted].edu> [redacted].edu>

Good Day !!!

During this time that we are in, working from home would be great. Therefore, you have been offered a campus employment office Job Opportunity which serves as a gateway to pay all expenses incurred on campus.

This opportunity should be done at leisure taking at most 7 Hours Weekly and earn $500 Weekly. It is a Flexible Opportunity where you will determine your working time.

All the tasks are work from home/on campus job, you do not need to travel, you do not need to have a car to get started. You can be in any location and work from your home/school.

If you are interested in working with her Kindly email her (olsonmary899@gmail.com).

Kindly include your private email and cellphone number when applying for direct contact.

Please Note: This position is available on a first come, first served basis.

Sincerely,

cisco | TALOS

Take Aways

- Intent based approach identifies both set of victims, person whose account has been compromised and person who receives emails from compromised accounts.

- With each detected attempt of exploitation, intent of the threat actor (Phishing, SPAM, BEC etc.) also gets captured which aids in additional remediation
  - Such as blocking Phishing Links
  - Correlating Phishing links with Web gateway logs to detect additional compromised accounts.

Acknowledgements

We would like to acknowledge Eric Peterson, Sachin Shukla and Ankit Tater for their support during the project

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity

Thank you!

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM