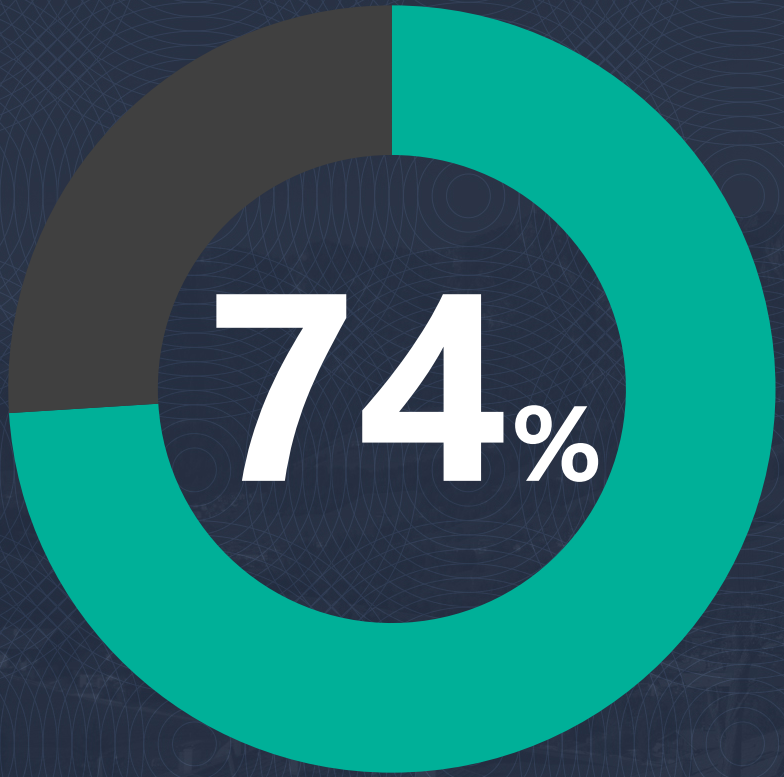

Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT
ETS & Sentinel
Best practice overview

Targeted attacks start with email

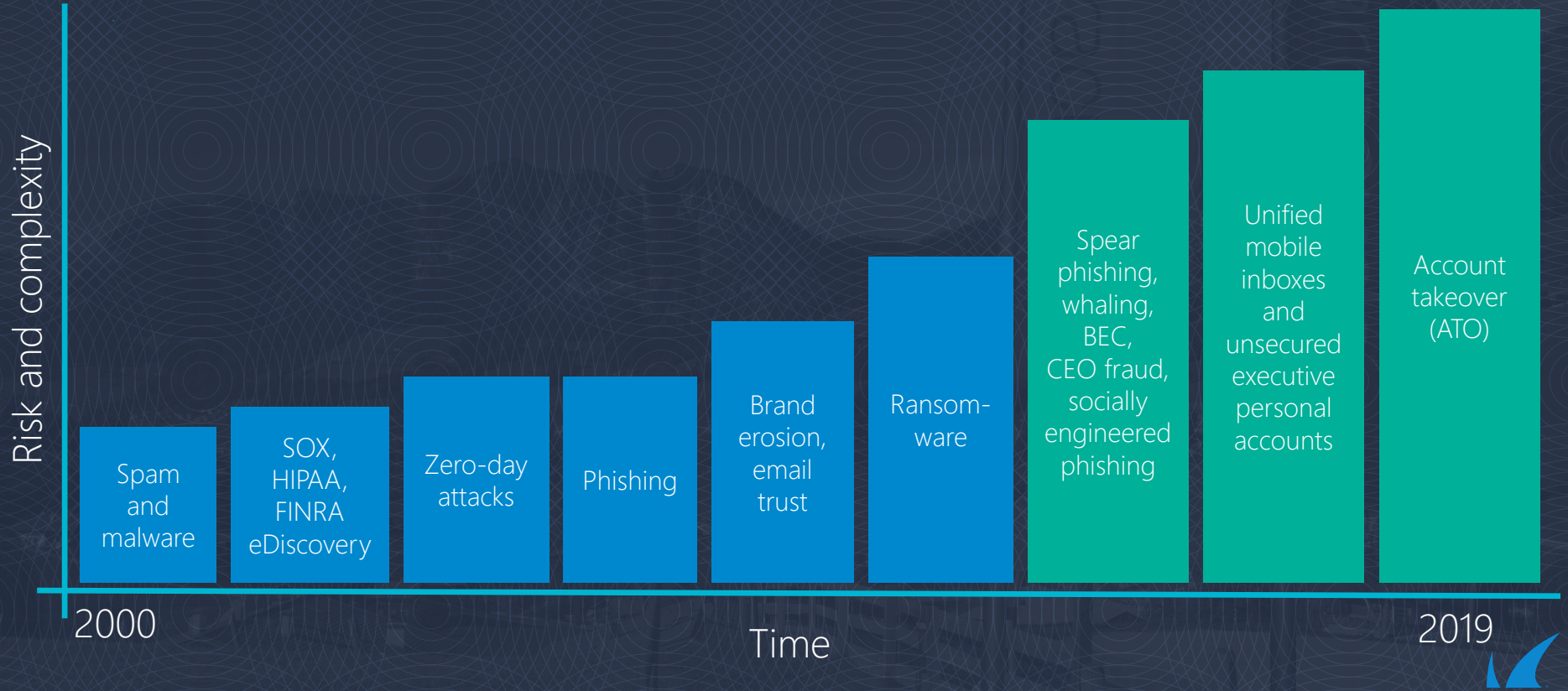


"Almost three quarters of all attacks start with email attachment or a link."

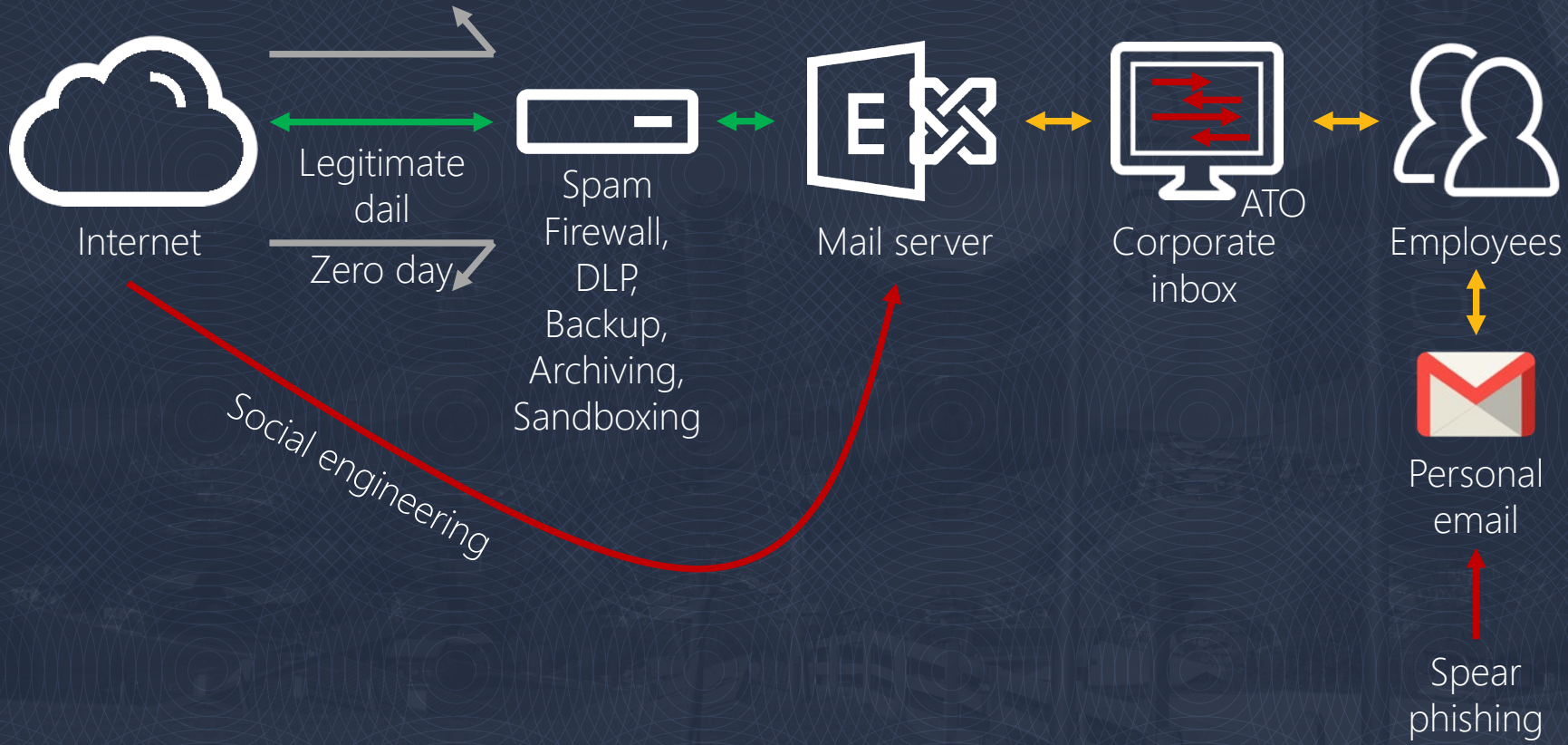
- SANS Analyst Program

2017 Threat Landscape Survey: Users on the Front Line - SANS Analyst Program

Attacks Increased complexity every year



The challenge



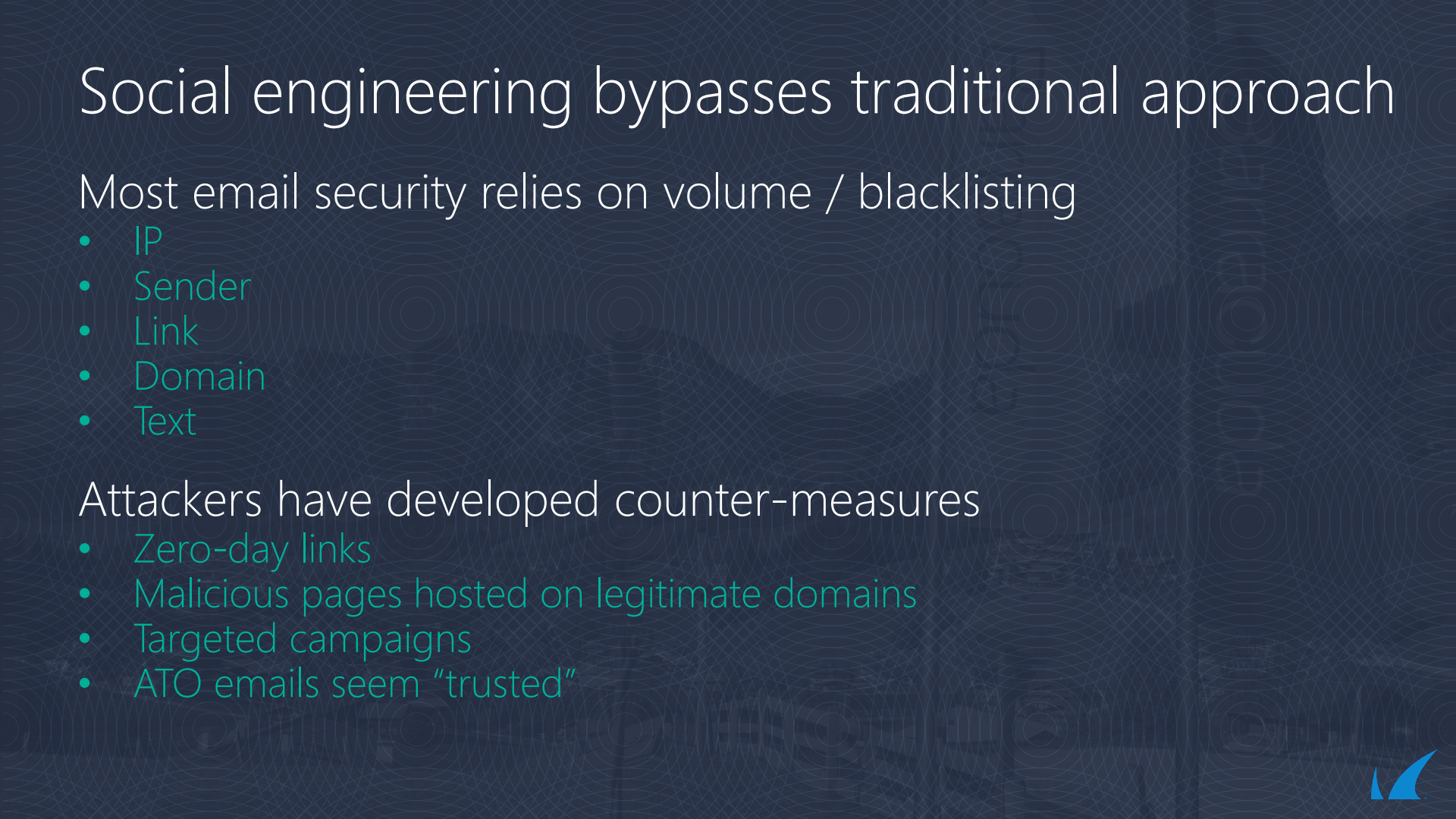
Social engineering bypasses traditional approach

Most email security relies on volume / blacklisting

- IP
- Sender
- Link
- Domain
- Text

Attackers have developed counter-measures

- Zero-day links
- Malicious pages hosted on legitimate domains
- Targeted campaigns
- ATO emails seem “trusted”



Barracuda Total Email Protection

Do you know if your organisation has been exploited?

Email Threat Scanner

https://www.barracuda.com/email_scan

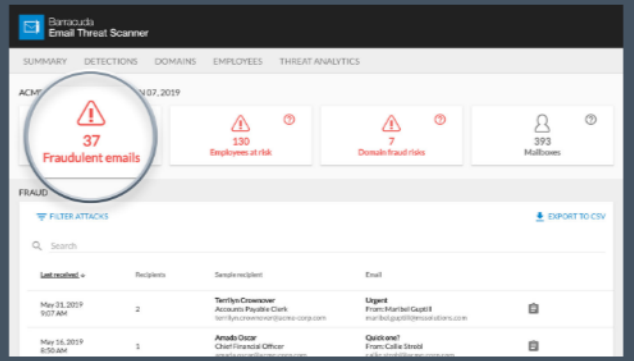
Barracuda Email Threat Scanner

Serious threats may be hiding in your Office 365 mailboxes.

Scan your Office 365 environment. It's fast, free and safe—with no impact on email performance.

SCAN YOUR EMAIL NOW

Detect email threats that got past your email gateway.



Fraud summary

Our artificial intelligence platform understands email sender intent to detect anomalies such as email impersonation and account takeover.

5,000+ organizations

have run this scan and discovered advanced threats in their Office 365 mailboxes.

8,000+
scans completed
since 2018

8.5 million
mailboxes
have been scanned for threats

4 million
spear phishing attacks
identified to date

Email Threat Scanner benefits

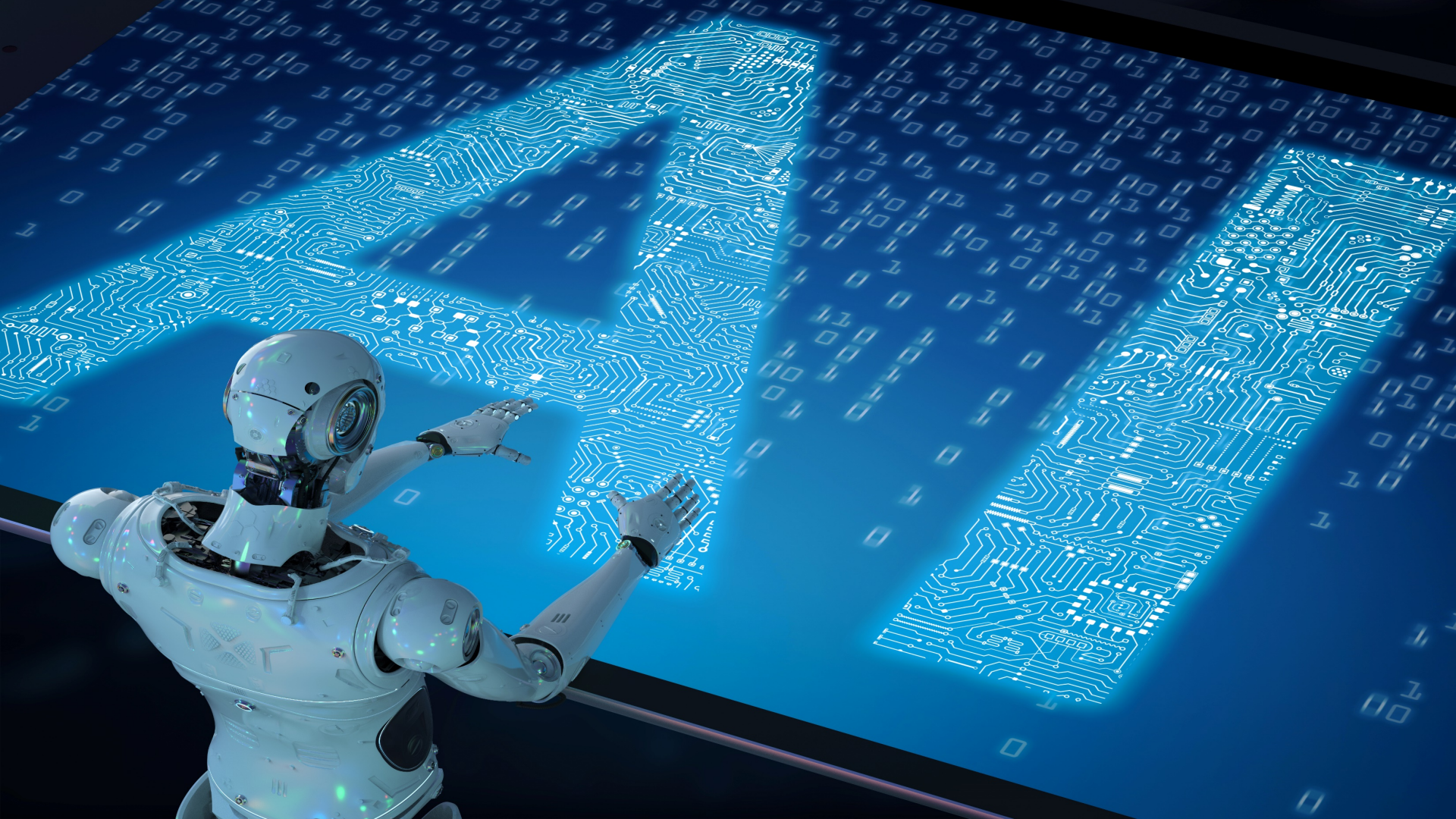
One time pass of your O365 instance

Identifies current threats already within the employee inbox

Produce a report to visualise the business risk

Support build of business case & further discussions

Why is Barracuda Sentinel different?



Attack from Mar 08, 2019
Quarantined

ANALYSIS
× The from address is not Lior Gavish's typical address
× This email makes an unusual request to the recipient

To: Lior Gavish <lior@sookasa.onmicrosoft.com>
From: Lior Gavish <lior.632039@cudapost.com>
Reply to:
Date: Mar 08, 2019 10:11 PM
Subject: Action Required

EMAIL HEADERS

Are you available? Kindly email me immediately you receive this.

Lior

Attack from Jul 11, 2018
Quarantined

ANALYSIS
× Apple does not typically use this email address to send messages
× This email contains a suspicious URL that Apple does not typically use

To: Itay Bleier <itay@sookasa.onmicrosoft.com>
From: Apple <671689@cudapost.com>
Reply to:
Date: Jul 11, 2018 8:07 PM
Subject: Verify Your ID

EMAIL HEADERS

Your Apple account has been locked due to unusual login attempt.

Please follow instructions below to restore fullaccess.

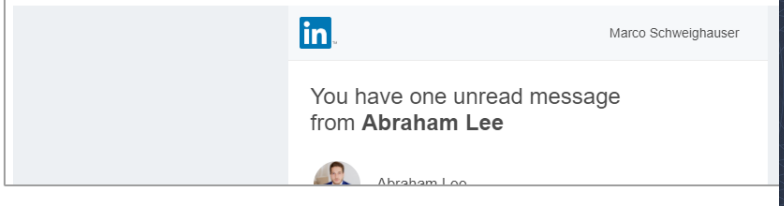
Restore Access

Attack from Jan 18, 2019
Quarantined

ANALYSIS
× LinkedIn does not typically use this email address to send messages
× This email contains a suspicious URL that LinkedIn does not typically use

To: Lior Gavish <lior@sookasa.onmicrosoft.com>
From: LinkedIn <994366@cudapost.com>
Reply to:
Date: Jan 18, 2019 9:38 PM
Subject: Your name was mentioned within my network. In a positive sense :)

EMAIL HEADERS



Commonly impersonated web services

Enterprise

Google

Dropbox

Microsoft

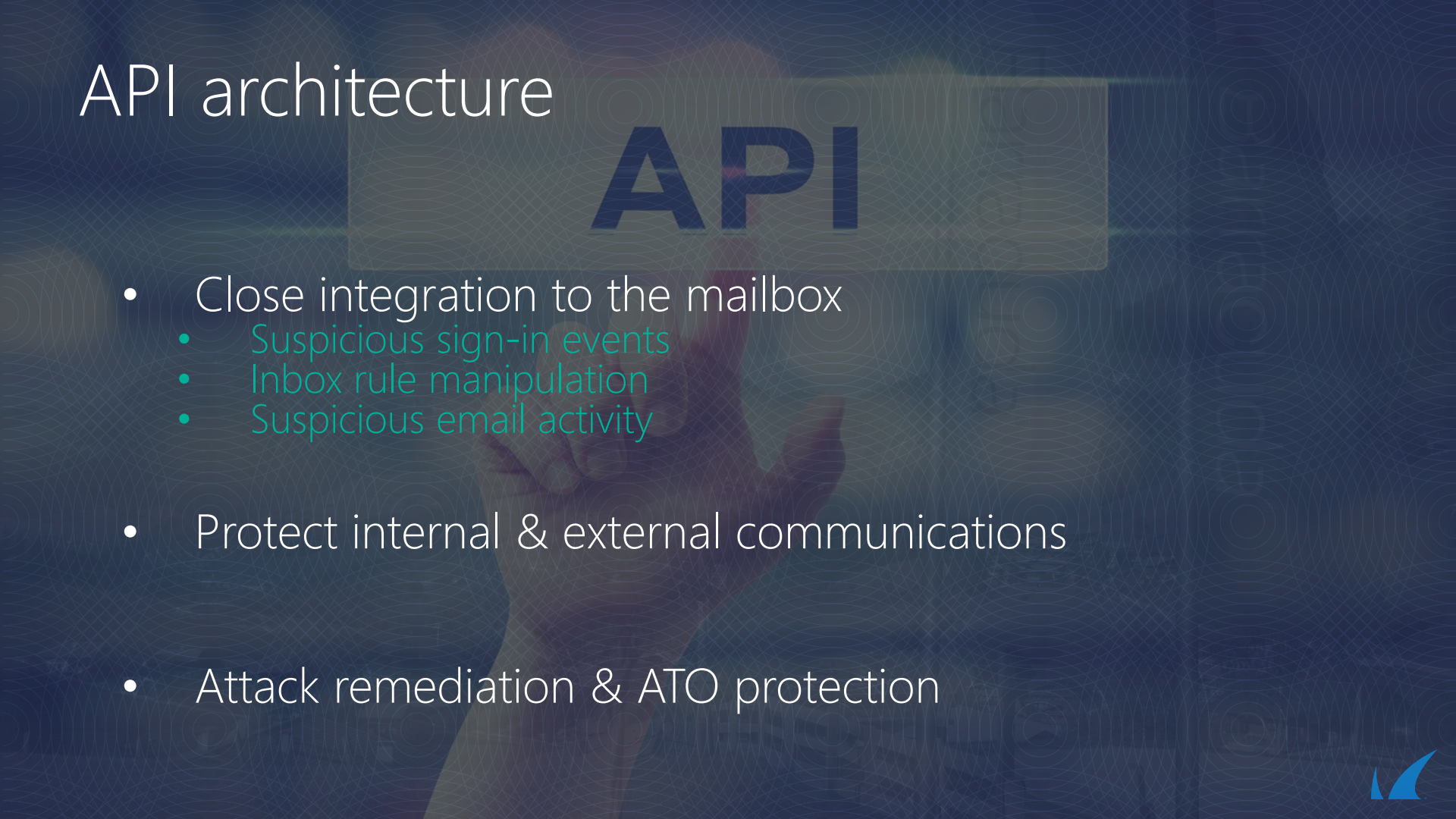
DocuSign

Consumer

facebook

NETFLIX

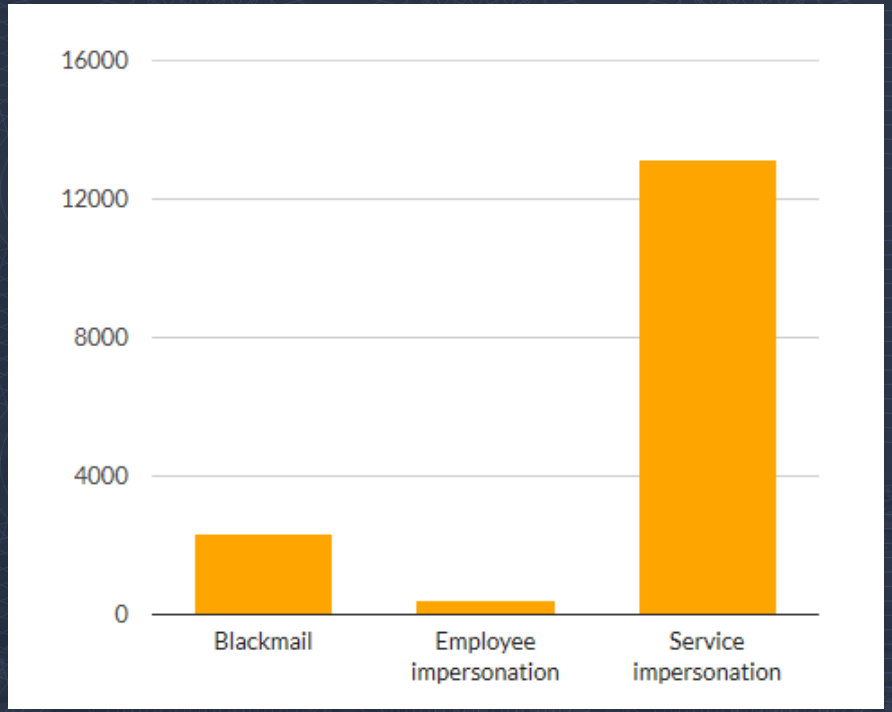
API architecture



- Close integration to the mailbox
  - Suspicious sign-in events
  - Inbox rule manipulation
  - Suspicious email activity
- Protect internal & external communications
- Attack remediation & ATO protection

How do we know the approach works?

Detected types of fraud



Bank account change request from (CEO) to (HR/Payroll)

Jun 04, 2019 11:08 AM	2	**Elaine** Regional HR/Payroll Administrator .com	**Direct Deposit Change Request** From: Pat ceo13@wi.rr.com

Attack from Jun 04, 2019

ANALYSIS
× The from address is not Pat typical address
× This email makes an unusual request to the recipient

To: Elaine <e.com>
From: Pat <ceo13@wi.rr.com>
Reply to:
Date: Jun 04, 2019 11:08 AM
Subject: Direct Deposit Change Request

EMAIL HEADERS

I need to update my paycheck direct deposit information because my account on file is temporarily closed due to an ongoing audit by my bank.. Please can you handle it now ?

Thanks

…is actually an attempt to fraudulently change direct deposits

- Use of publicly available information
- The scammer did his/her homework and it was addressed to the person in charge of payroll in HR.

Sextortion/Blackmail attempt

Attack from Oct 18, 2018

ANALYSIS
× This email requests payment through crypto currency
× This email makes unusual threats to the recipient

To: Susana <s[redacted].com>
From: s[redacted].com
Reply to:
Date: Oct 18, 2018 9:26 PM

Subject: UNVERIFIED SENDER: s[redacted].com is hacked

EMAIL HEADERS

Hello!

My nickname in darknet is riordan11.
I hacked this mailbox more than six months ago,
through it I infected your operating system with a virus (trojan) created by me and have been monitoring you for a long time.

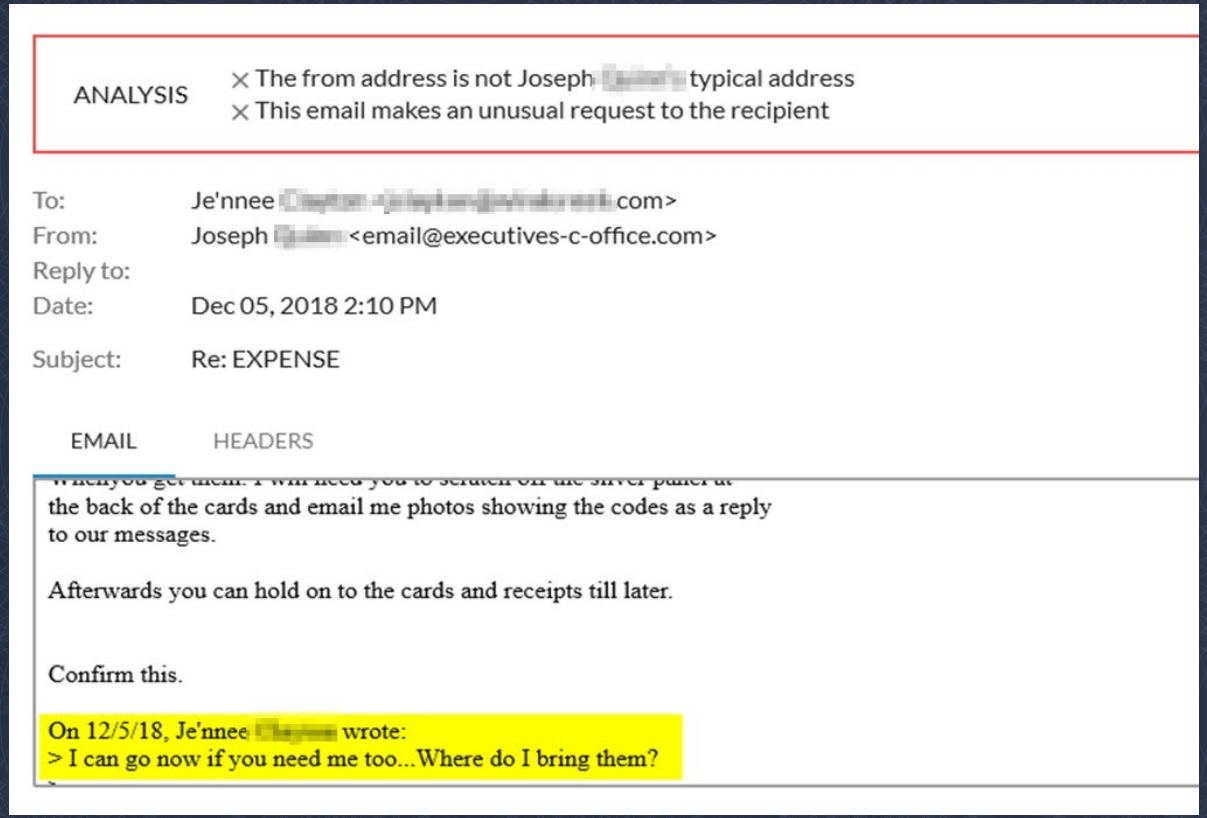
So, your password from s[redacted].com is [redacted]

Even if you changed the password after that - it does not matter, my virus intercepted all the caching data on your computer
and automatically saved access for me.

…is blackmail

- Attacker claims to have hacked the account, ‘proving’ so by spoofing the recipients address as sender.
- An old password is provided as additional ‘proof’ that the attacker has access. These credentials are typically sourced from the large data breaches that are available on the Internet.
- The fact that a legitimate password is shown is enough scare tactics.
- Ransom is requested in Bitcoin / Cryptocurrency
- Threats of ruining the victim’s reputation

Giftcard conversation between (Exec. assistant) and (CFO)



ANALYSIS

× The from address is not Joseph [redacted] typical address
× This email makes an unusual request to the recipient

To: Je'nnee [redacted] com>
From: Joseph [redacted] <email@executives-c-office.com>
Reply to:
Date: Dec 05, 2018 2:10 PM
Subject: Re: EXPENSE

EMAIL HEADERS

[redacted] the back of the cards and email me photos showing the codes as a reply to our messages.

Afterwards you can hold on to the cards and receipts till later.

Confirm this.

On 12/5/18, Je'nnee [redacted] wrote:
> I can go now if you need me too...Where do I bring them?

… is actually a successful attempt of the scammer to establish rapport

- Attacker fakes urgency and authority to get victim to buy giftcards and send the barcodes to the scammer

- Victim responded not once but multiple times in this thread

E-Mail account upgrade scam

Attack from Jun 24, 2019

ANALYSIS
× This email has a suspicious call-to-action
× This email contains a suspicious URL (sankang-germany.de, warezpage.ga)

To: Jennifer <j[redacted].com>
From: Mail Server [redacted].com <noreply@[redacted].com>
Reply to:
Date: Jun 23, 2019 10:58 PM

Subject: Mail Suspension Notice For j[redacted].com

EMAIL HEADERS

j[redacted]
Do please re-confirm your email j[redacted] to upgrade mail quota and enjoy your MailBox with the new upgrade.

Please sign in to re-confirm [redacted] ownership.

CLICK HERE To Confirm ownership and Upgrade.

Web Site Has Been Blocked!

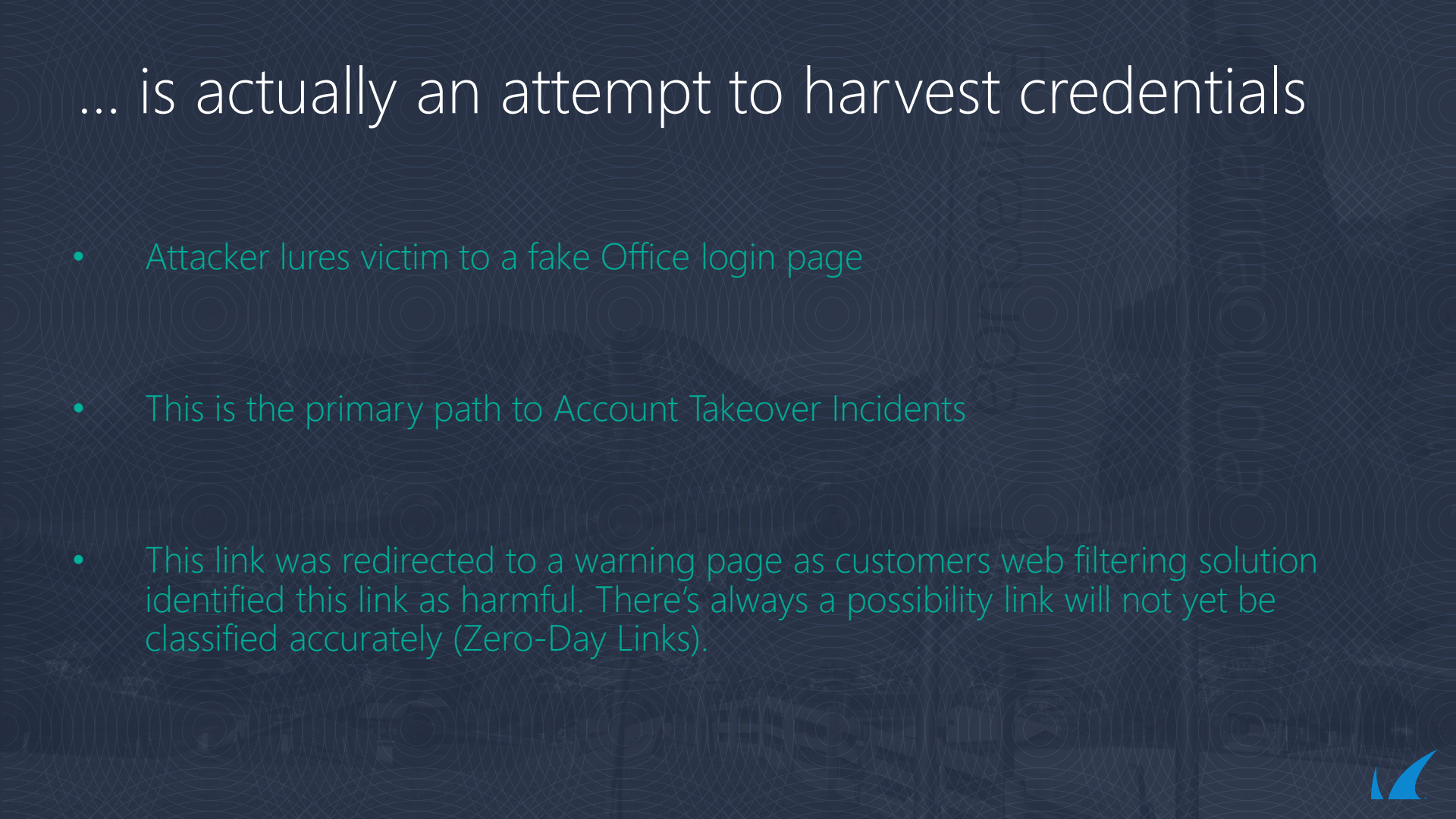
The web page you are attempting to access has been classified as malicious. This classification is determined by direct analysis of the web page. Although an entire web site may be blocked as malicious, it is very common for a single page on a valid web site to be blocked.

Your organization has enabled this technology to protect you, your system, and the organization from harm. Blocked pages contain material such as:

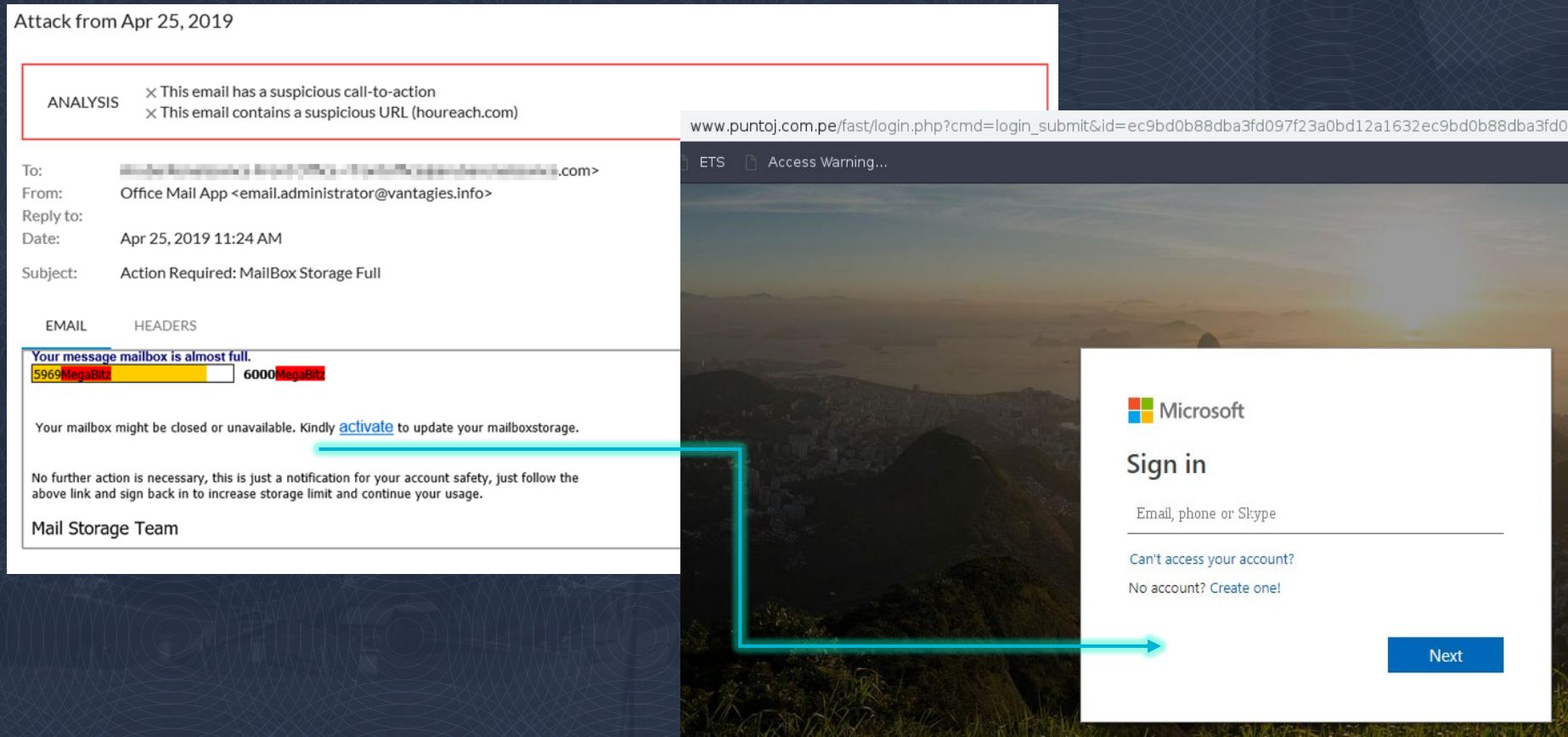
- Credential Theft: A page may be designed to look like a valid financial institution, a well-known organization, or an otherwise trusted source. The page is requesting a login and/or password for malicious purposes.
- Malware: A page may contain files or other malicious material which are intended to harm your system or organization. The malicious material may contain a virus, an installation program, or it may expose a vulnerability in a program which exists on your system.

… is actually an attempt to harvest credentials

- Attacker lures victim to a fake Office login page
- This is the primary path to Account Takeover Incidents
- This link was redirected to a warning page as customers web filtering solution identified this link as harmful. There's always a possibility link will not yet be classified accurately (Zero-Day Links).

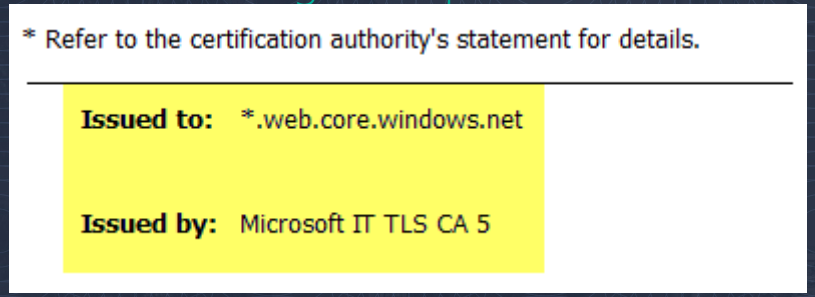


E-Mail account upgrade scam

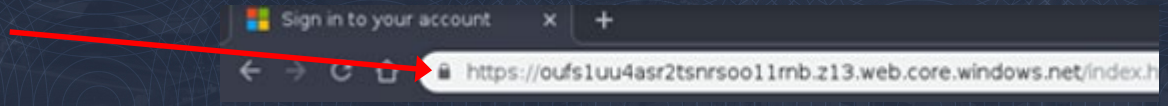


… is another attempt to harvest credentials

- This link was not redirected to a warning page.
  The gateway security solution that successfully identified the malicious link in the previous example failed to protect here. The malicious link points to an MS Azure hosted site, so it's a link that has a good reputation and even has an MS signed SSL certificate:



This SSL certificate results in the browsers trusting this as a legitimate website:



ATO – the benefit of Barracuda Sentinel

Sentinel offers a complete solution

Prevent infiltration using AI that detects impersonations

Detect reconnaissance and harvesting by observing behavioral, text and link anomalies

Infiltration

Reconnaissance

Harvest Credentials

Monetization

Remediate using APIs to discover and delete harvesting/monetization and prevent "viral" ATO / brand abuse

Sentinel offers a complete solution

Prevent infiltration using AI that detects impersonations

Detect reconnaissance and harvesting by observing behavioral, text and link anomalies

Remediate using APIs to discover and delete harvesting/monetization and prevent "viral" ATO / brand abuse

Sentinel offers a complete solution

Prevent infiltration using AI that detects impersonations

Detect reconnaissance and harvesting by observing behavioral, text and link anomalies

Infiltration

Reconnaissance

Harvest Credentials

Monetization

Remediate using APIs to discover and delete harvesting/monetization and prevent “viral” ATO / brand abuse

ATO remediation demo

Securing the gateway is still necessary,
but no longer sufficient


Thank you
Barracuda
TECHSUMMIT19
BARRACUDA TECHNICAL SUMMIT