Barracuda

TECHSUMMIT19

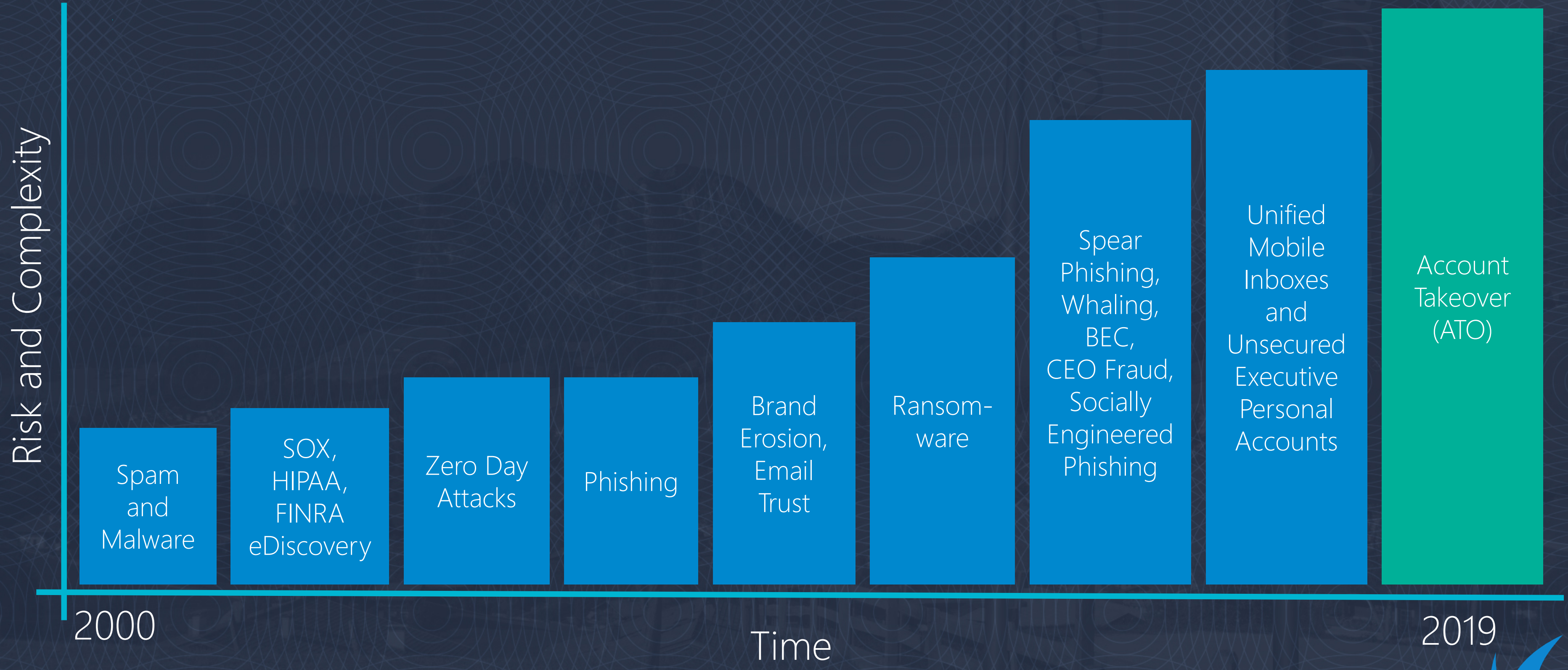
BARRACUDA TECHNICAL SUMMIT

Fighting Account Takeover

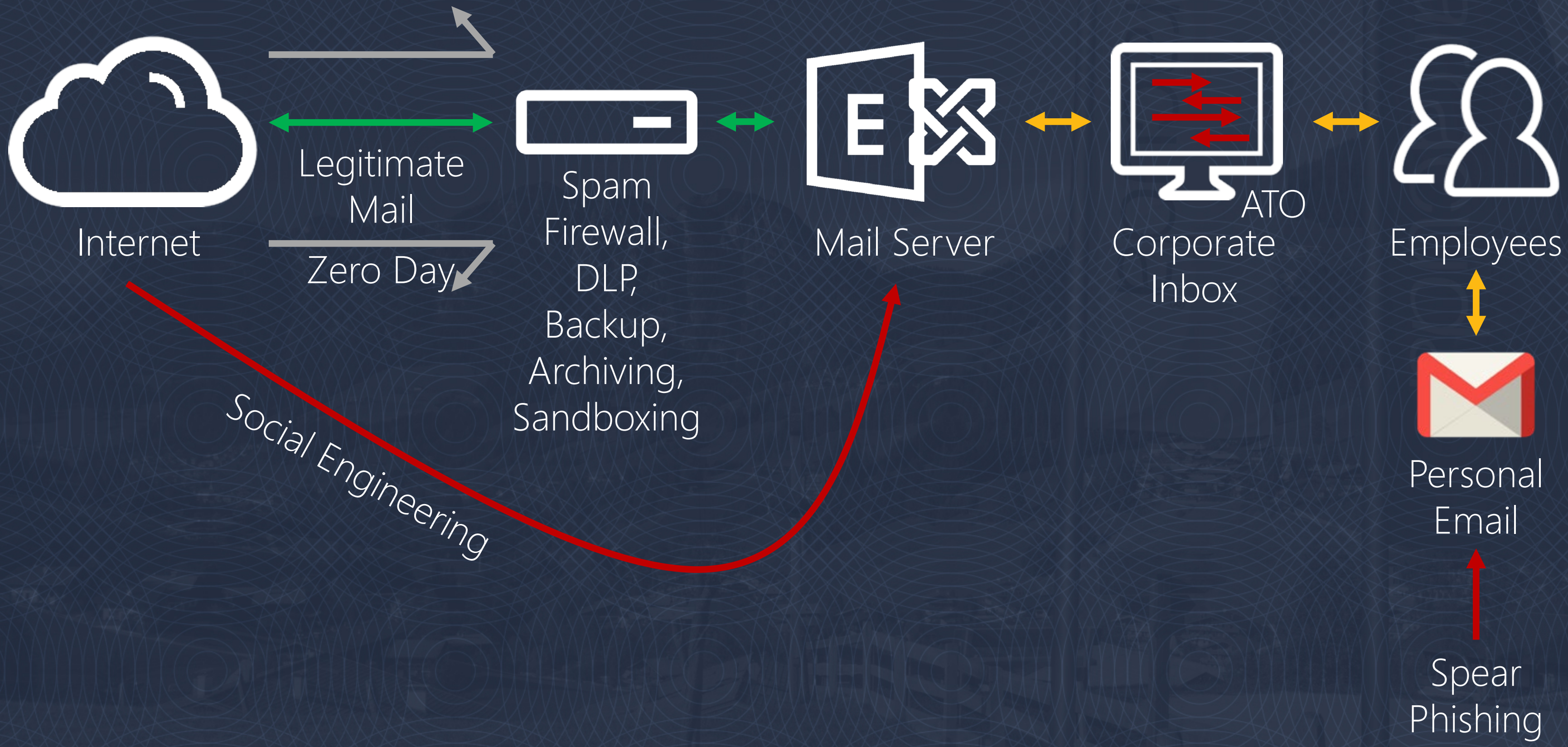
Aseem Asthana

Market context

And it gets more complex every year



Account takeover is the newest threat



Securing the gateway is still necessary, but no longer sufficient

What is ATO?

Account takeover defined

What is account takeover (ATO)?

- Using stolen account credentials to commit fraud by taking over someone's identity

How can email accounts be used when taken over?

- Commit financial fraud
- Steal sensitive information
- Launch phishing campaigns

Anatomy of ATO

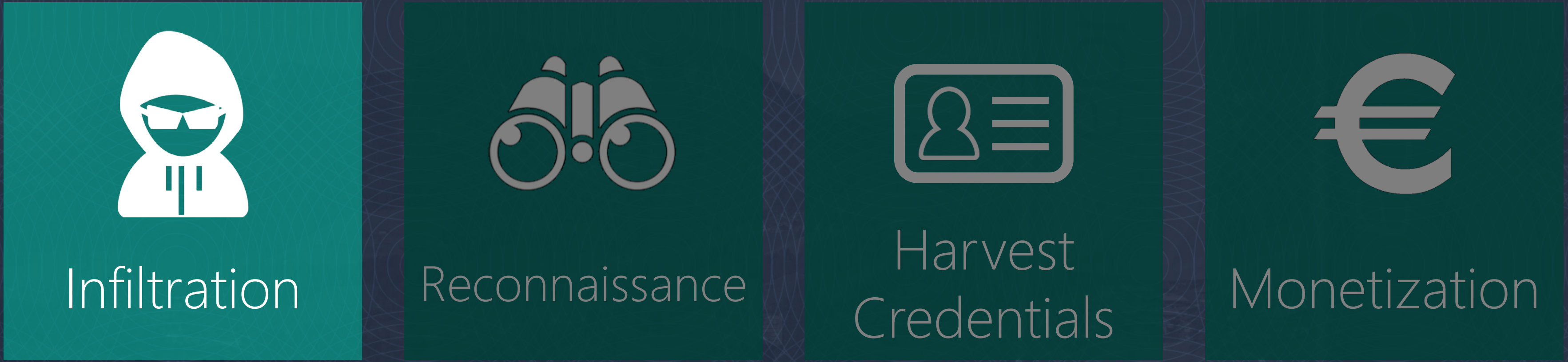
Infiltration

Reconnaissance

Harvest Credentials

Monetization

Step 1: infiltration



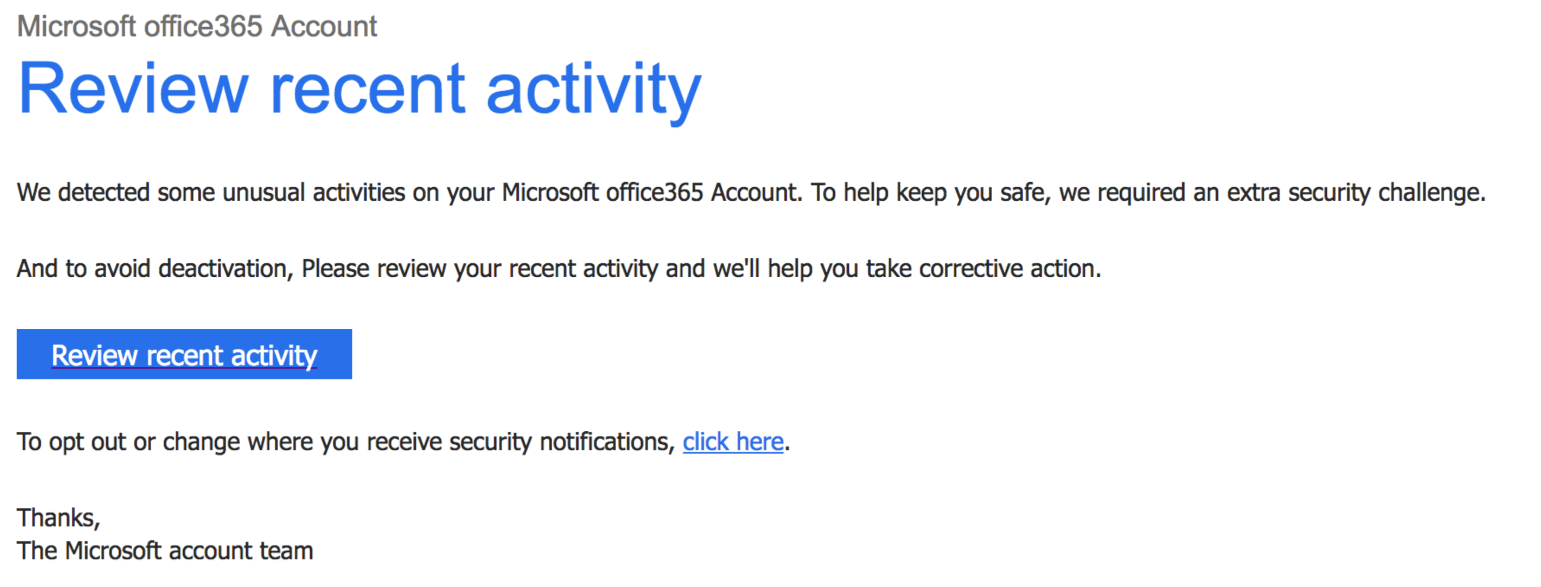
Infiltration

Reconnaissance

Harvest Credentials

Monetization

Step 1: infiltration



Microsoft office365 Account

Review recent activity

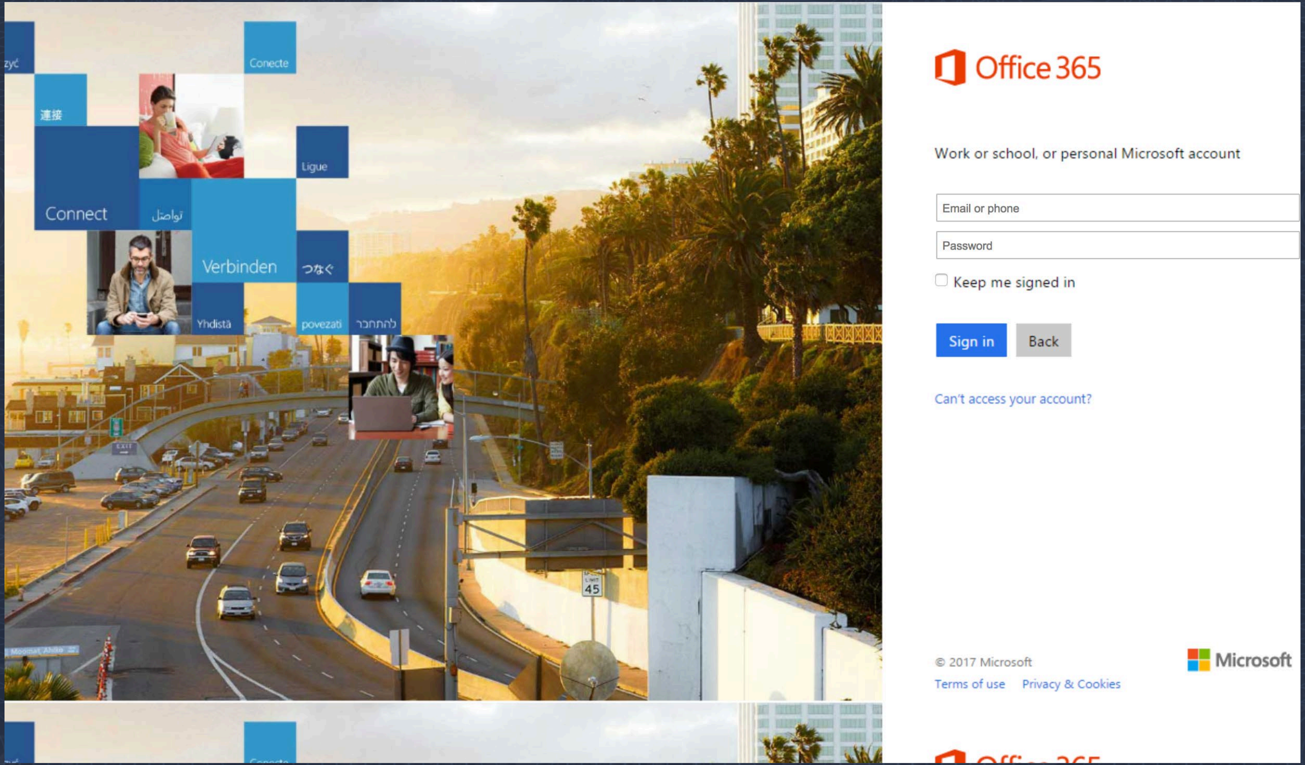
We detected some unusual activities on your Microsoft office365 Account. To help keep you safe, we required an extra security challenge.

And to avoid deactivation, Please review your recent activity and we'll help you take corrective action.

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Step 1: infiltration



Office 365

Work or school, or personal Microsoft account

Email or phone

Password

□ Keep me signed in

Sign in Back

Can't access your account?

© 2017 Microsoft

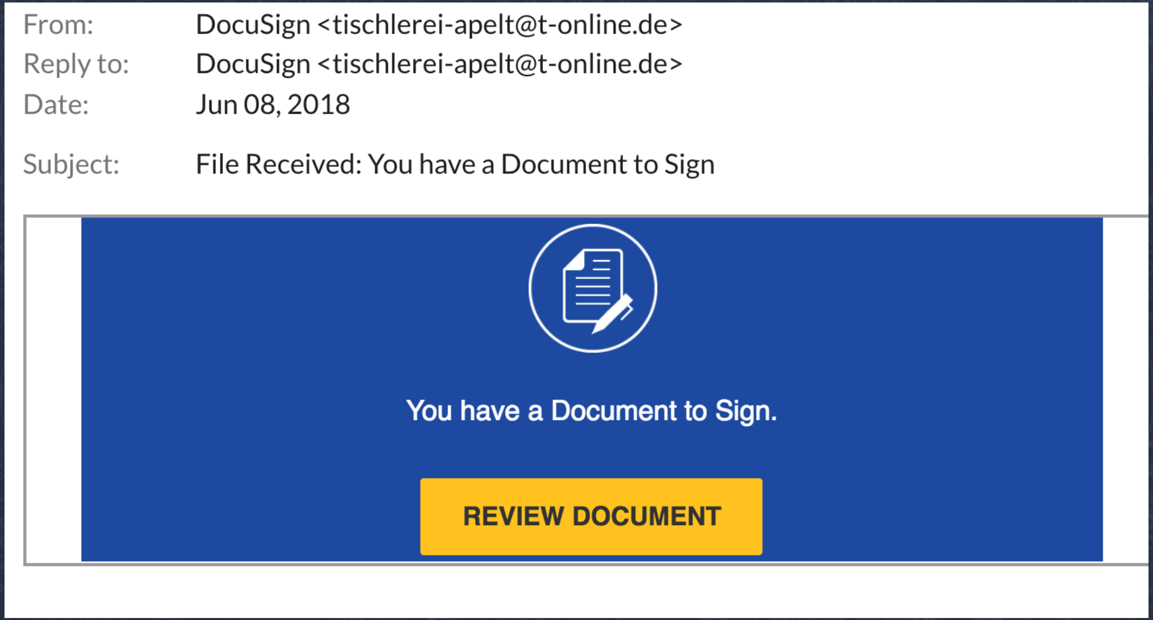
Terms of use Privacy & Cookies

Microsoft

Why does it work?

LinkProtect cannot prevent these attacks since the links are ***low volume*** *and* ***highly personalized***

Signatures, packages, and other excuses

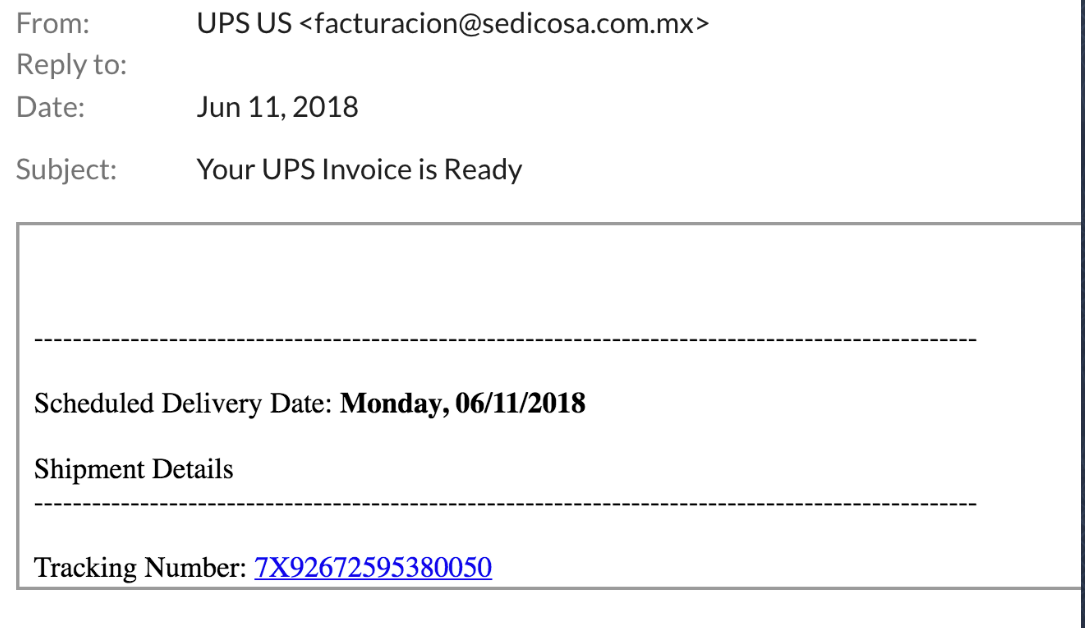


From: DocuSign <tischlerei-apelt@t-online.de>
Reply to: DocuSign <tischlerei-apelt@t-online.de>
Date: Jun 08, 2018

Subject: File Received: You have a Document to Sign

You have a Document to Sign.

Signatures, packages, and other excuses



From: UPS US <facturacion@sedicosa.com.mx>

Reply to:

Date: Jun 11, 2018

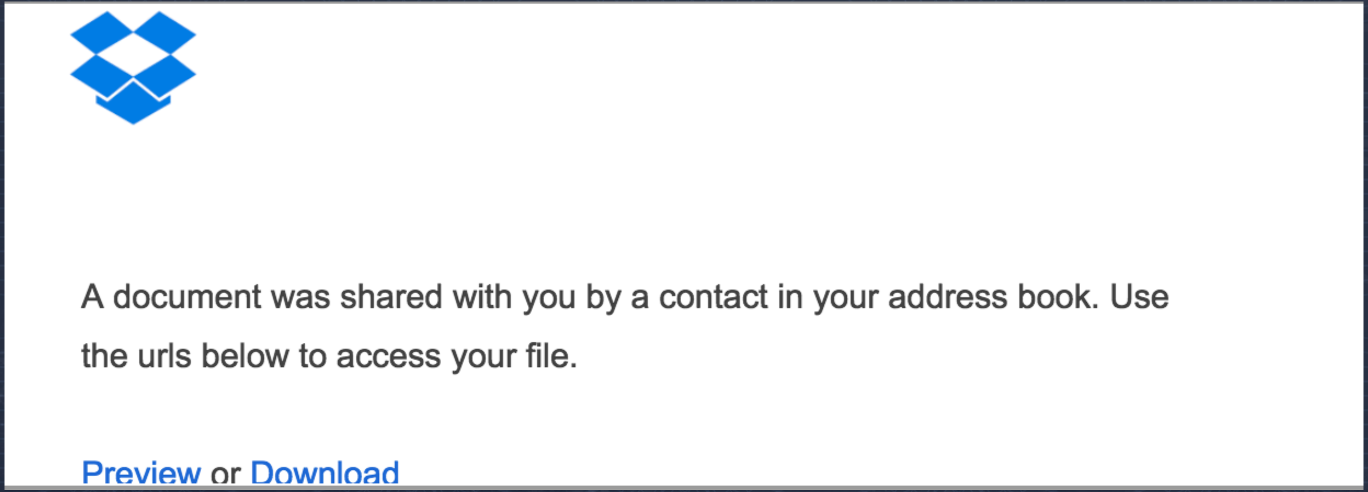
Subject: Your UPS Invoice is Ready

Scheduled Delivery Date: **Monday, 06/11/2018**

Shipment Details

Tracking Number: 7X92672595380050

Signatures, packages, and other excuses



A document was shared with you by a contact in your address book. Use the urls below to access your file.

Preview or Download

Commonly impersonated web services

Enterprise

Google

Dropbox

Microsoft

DocuSign®

Consumer

facebook

NETFLIX

Infiltration has many forms

Weakness	Method
Password reuse across services	Password repository breach *(Yahoo, Slack, LinkedIn, etc.)*
Weak passwords	Brute force attack
Endpoint exposure to malware	Browser credential theft
Social trust	Emails, text and voice impersonations

Step 2: reconnaissance

Infiltration

Reconnaissance

Harvest Credentials

Monetization

Step 2: Reconnaissance

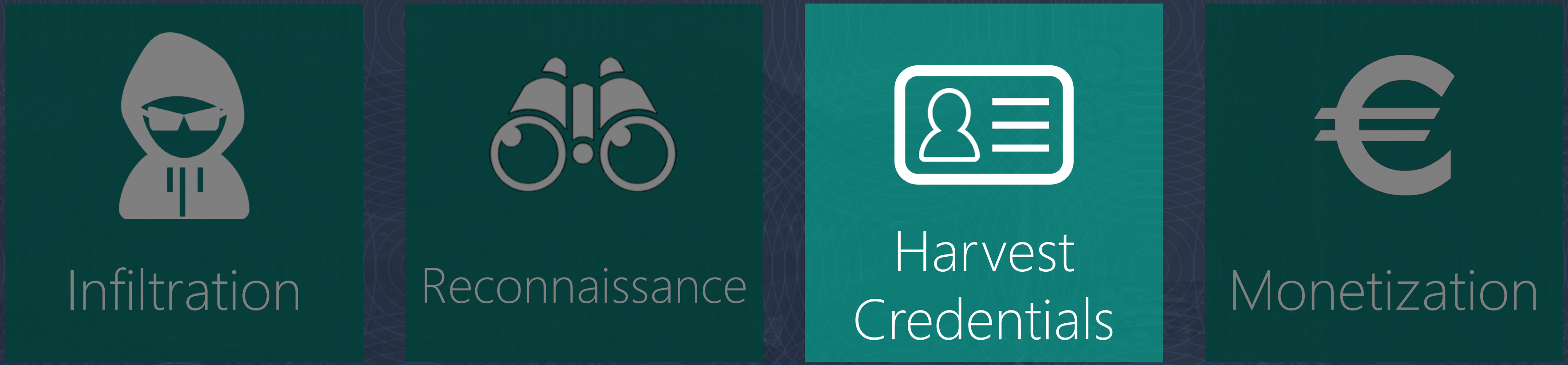
Method

- Sign in (oftentimes via VPN)
- Forwarding rules to external account
- Cleanup of traces

Common objectives

- Study org hierarchy, identify who has access to systems
- Learn signatures, email style
- Real-time transaction data

Step 3: harvest credentials



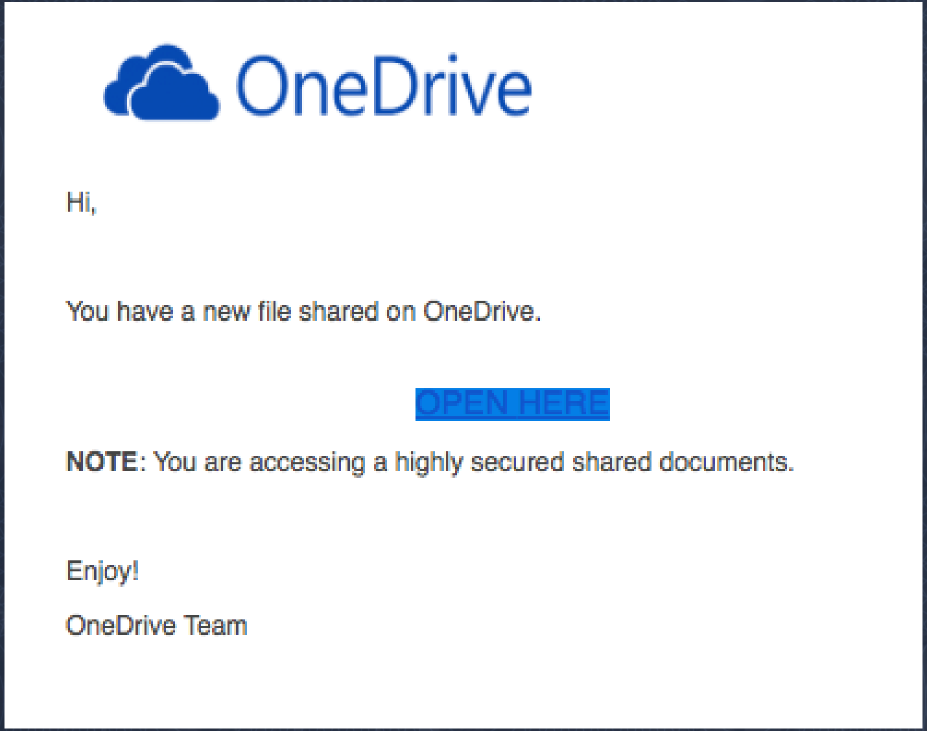
Infiltration

Reconnaissance

Harvest Credentials

Monetization

Step 3: Harvest credentials



OneDrive

Hi,

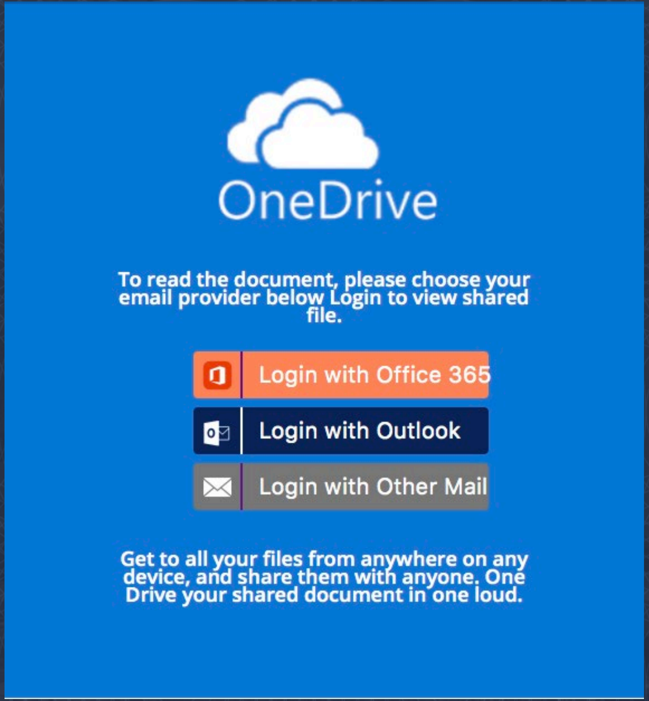
You have a new file shared on OneDrive.

OPEN HERE

NOTE: You are accessing a highly secured shared documents.

Enjoy!

OneDrive Team



OneDrive

To read the document, please choose your email provider below Login to view shared file.

Get to all your files from anywhere on any device, and share them with anyone. One Drive your shared document in one loud.

Step 4: monetization

Infiltration

Reconnaissance

Harvest Credentials

Monetization

Step 4: Monetization

Common: sell credentials downstream

- Carried out on dark web
- Sold to attackers that specialize in advanced techniques
- High value orgs/executives command higher price
  - More access
  - More authority to execute transactions

Monetizing credentials has many forms

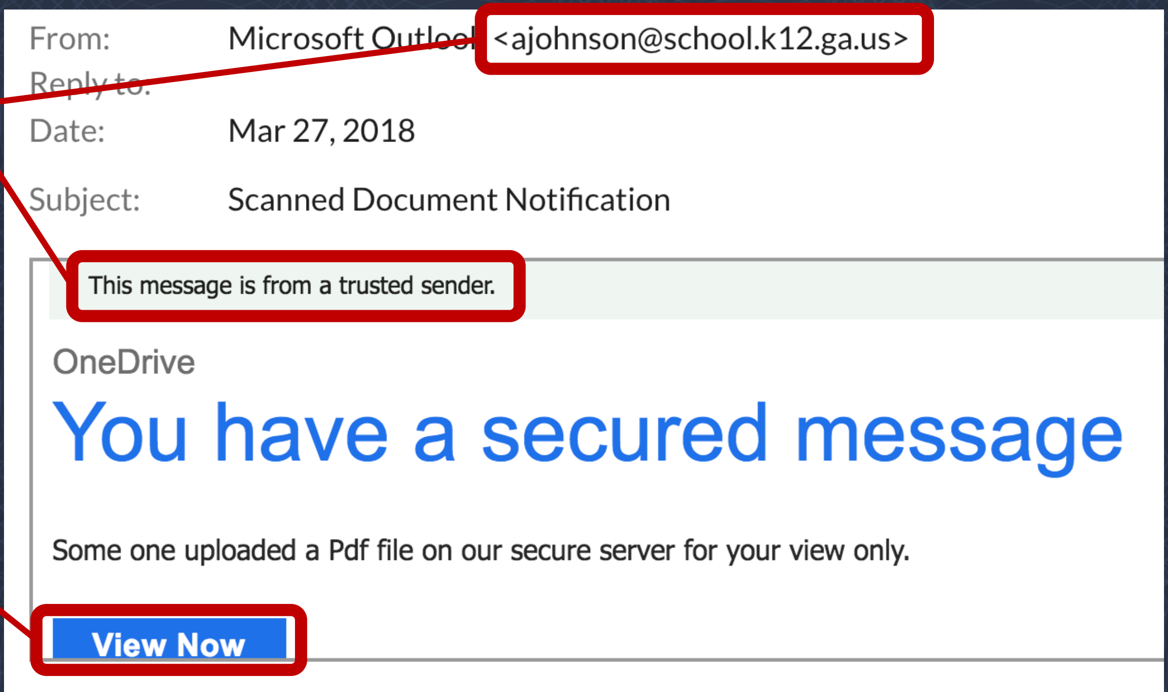
Techniques employed by sophisticated hacker groups

- Phishing campaigns targeting other orgs
- CEO fraud
- Spam campaigns
- Leverage information for fraud against customers/partners
    - e.g. real-estate wire fraud

External phishing campaigns

“Trusted” sender from a compromised account

Link does not point to Microsoft



From: Microsoft Outlook <ajohnson@school.k12.ga.us>

Reply to:

Date: Mar 27, 2018

Subject: Scanned Document Notification

This message is from a trusted sender.

OneDrive

You have a secured message

Some one uploaded a Pdf file on our secure server for your view only.

CEO fraud

From: Jane Johnson <jjohnson@corp.com>

Real email address of CEO

To: Michael Blake <michael.blake@corp.com>

Subject: Request

Body: Hey Michael,

Are you in the office, I need to process a bank transfer for me. Give me a quick reply when you can get it done.

Regards,

Jane Johnson

CEO, Corp Corporation

Cell: 408-292-2020

Why traditional email security can’t protect you

Traditional email security fails at every step

Infiltration

Reconnaissance

Harvest Credentials

Monetization

Infiltration 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”

Failing against recon/harvesting/monetization

Only inspects emails from external sources

Cannot track signals that indicate a compromised account

- Internal emails
- Anomalous Forwarding rules
- Unusual cleanup and side effects

Cannot pull back emails after delivery

So how do we fix this?

Multi-factor authentication

Password manager

Resilient process

AI to prevent, detect and remediate ATO

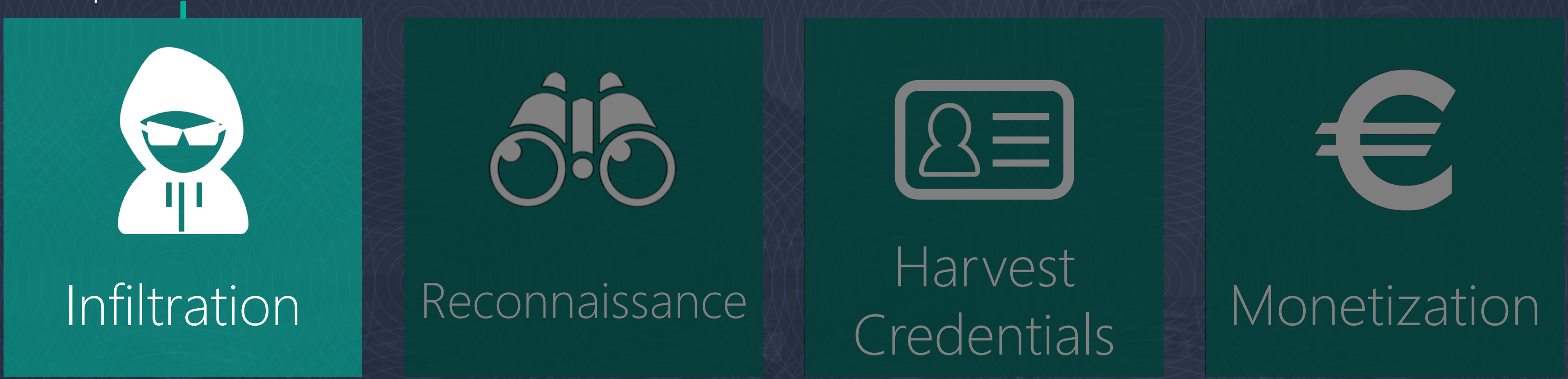
Security awareness training

API architecture enables ATO protection

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

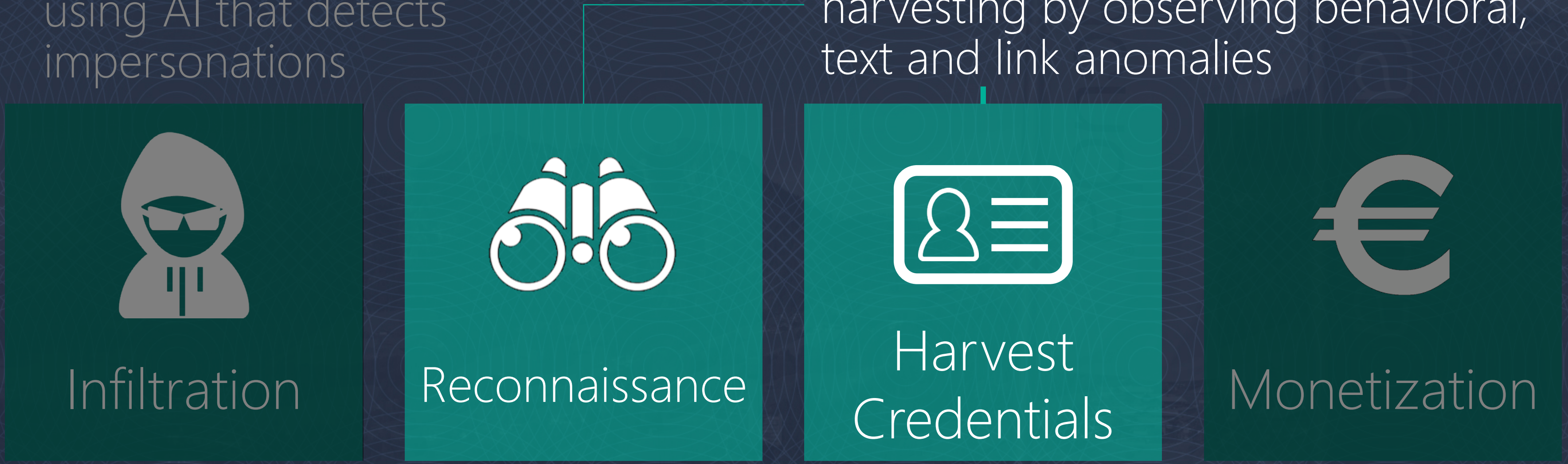
Monetization

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



Infiltration

Reconnaissance

Harvest Credentials

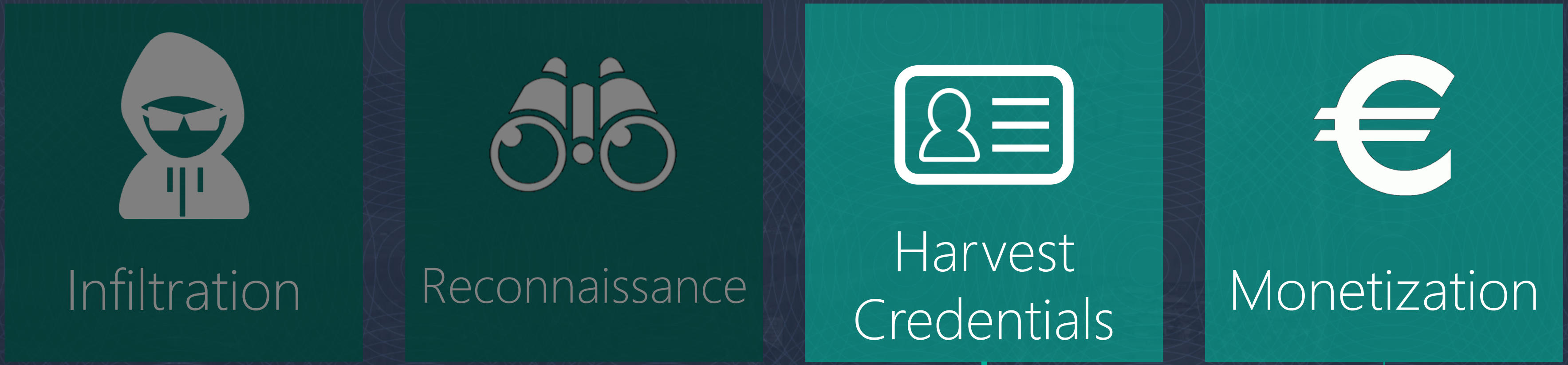
Monetization

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

Atlantic Bay
Mortgage Group

ATO remediation checklist

Change password

Disconnect all active sessions

Remove rules from Outlook

Delete all internal phishing emails

Submit phishing email

Scan computer using AV

Notify internal employees

Notify external recipients

Lock down account

**Prevent future attacks
and clean up collateral damage**

Communication

Atlantic Bay Mortgage Group

Where Sentinel fits in

Change password

Disconnect all active sessions

Remove rules from Outlook

Delete all internal phishing emails

Automation via AI and APIs

Submit phishing email

Scan computer using AV

Notify internal employees

Notify external recipients

Reporting and visibility

Moving forward

Next Steps

Evaluate the types of risks your organization is exposed

Think about where you are in your journey

Run a free Email Threat Scan to test your defenses

- scan.barracudanetworks.com

Don't let Account Takeover derail your organization!

Thank you

Barracuda

TECHSUMMIT19

BARRACUDA TECHNICAL SUMMIT