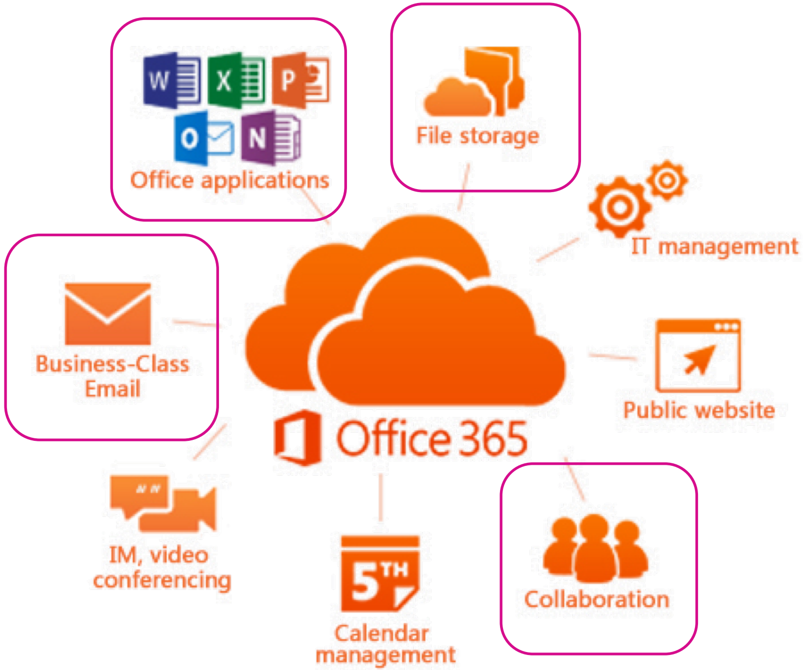
What risks are passing through your Office 365 environment?


Office applications
File storage
IT management
Business-Class Email
Office 365
Public website
IM, video conferencing
Calendar management
Collaboration

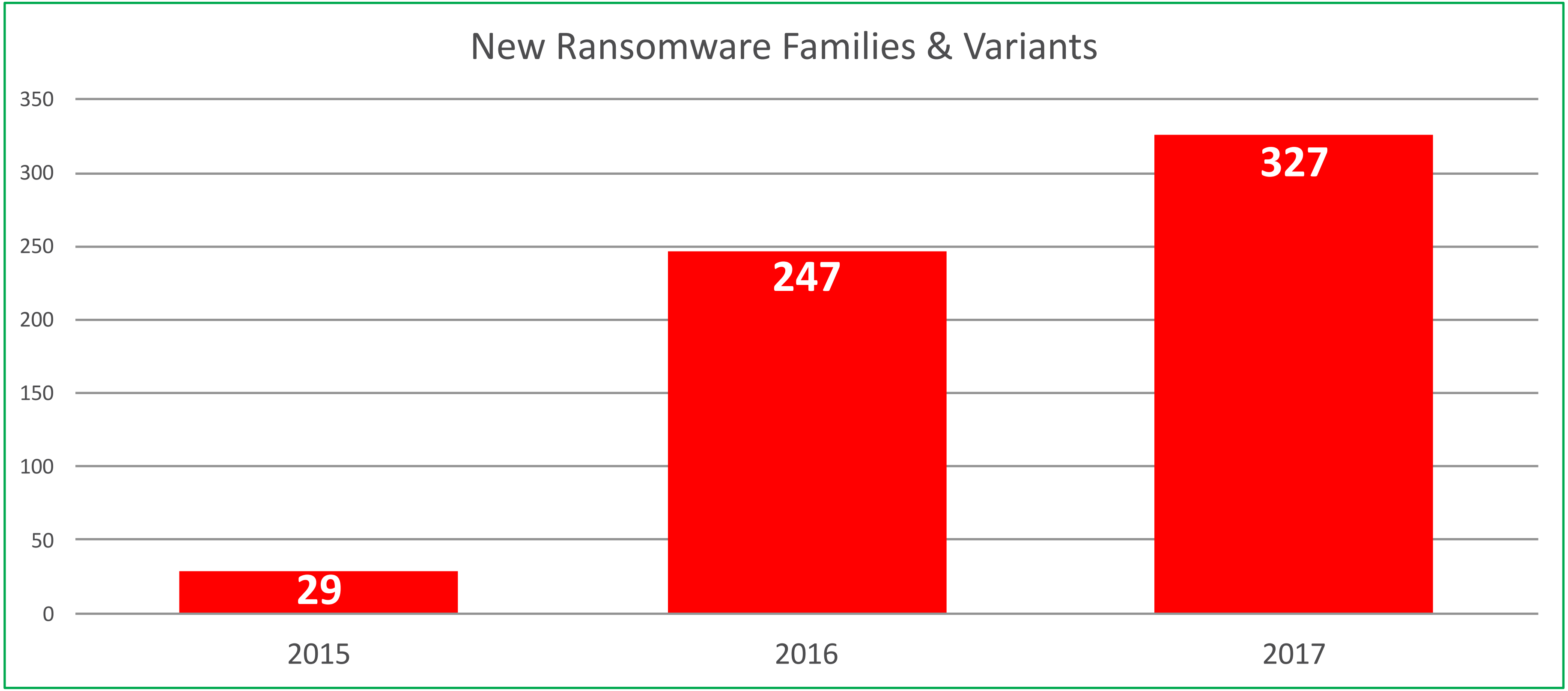
Messaging Threat Landscape

2018 Significant Threats

Ransomware

Business Email Compromise

Ransomware 2017



Ransomware-Related Threats in 2017

94% Email

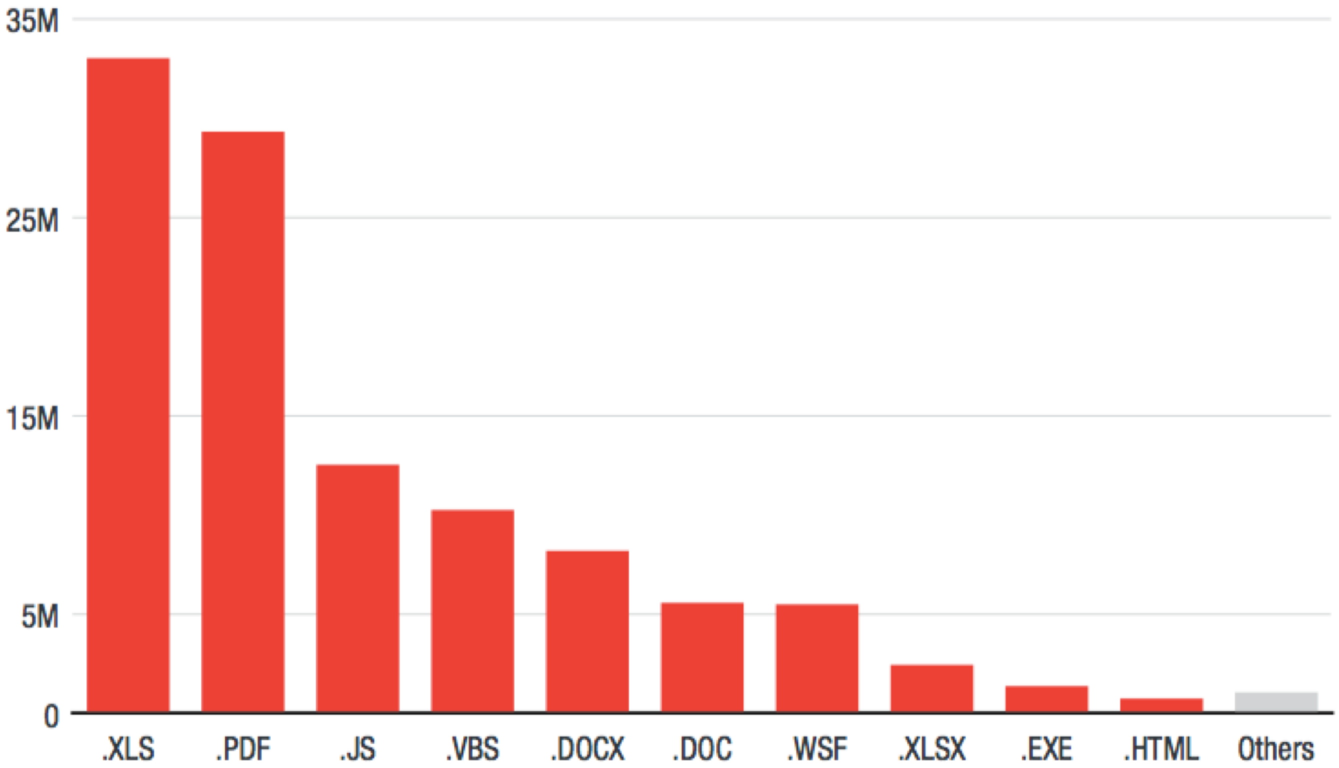
5% URL

1% File

Email Infection Vectors

Malware Hidden in Office Files

Top file types for spam attachments in 2017



Locky Ransomware

Recent Infection Tactics

- HTML attachments posing as invoices
- Archive files masquerading as business missives from multinationals, e.g., audit and budget reports
- Fraudulent emails that involve monetary transactions such as bills, parcel/delivery confirmations, and payment receipts

- Locky distributed 23

st

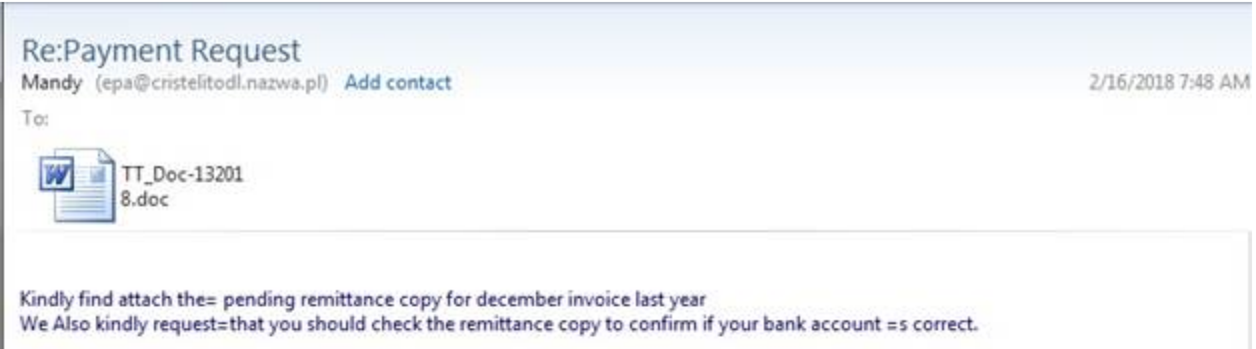
rs

est

in

k from our email-based sensors

Ransomware Email Samples



Re:Payment Request

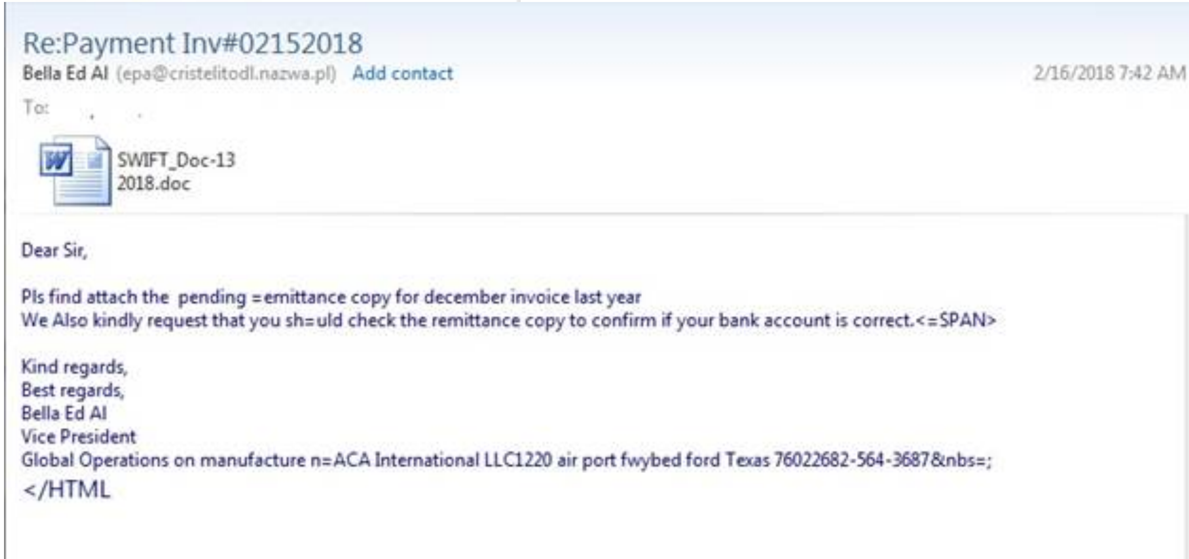
Mandy (epa@cristelitodl.nazwa.pl) Add contact 2/16/2018 7:48 AM

To:

TT_Doc-13201
8.doc

Kindly find attach the= pending remittance copy for december invoice last year
We Also kindly request=that you should check the remittance copy to confirm if your bank account =s correct.

Kind regards,
Best regards,
Mandy
Chief Accountant
Global Operations on m=nufacture n,
ACA International LLC1=20 air port fwybed ford Texas 76022682-564-3687
<=HTML



Re:Payment Inv#02152018

Bella Ed Al (epa@cristelitodl.nazwa.pl) Add contact 2/16/2018 7:42 AM

To:

SWIFT_Doc-13
2018.doc

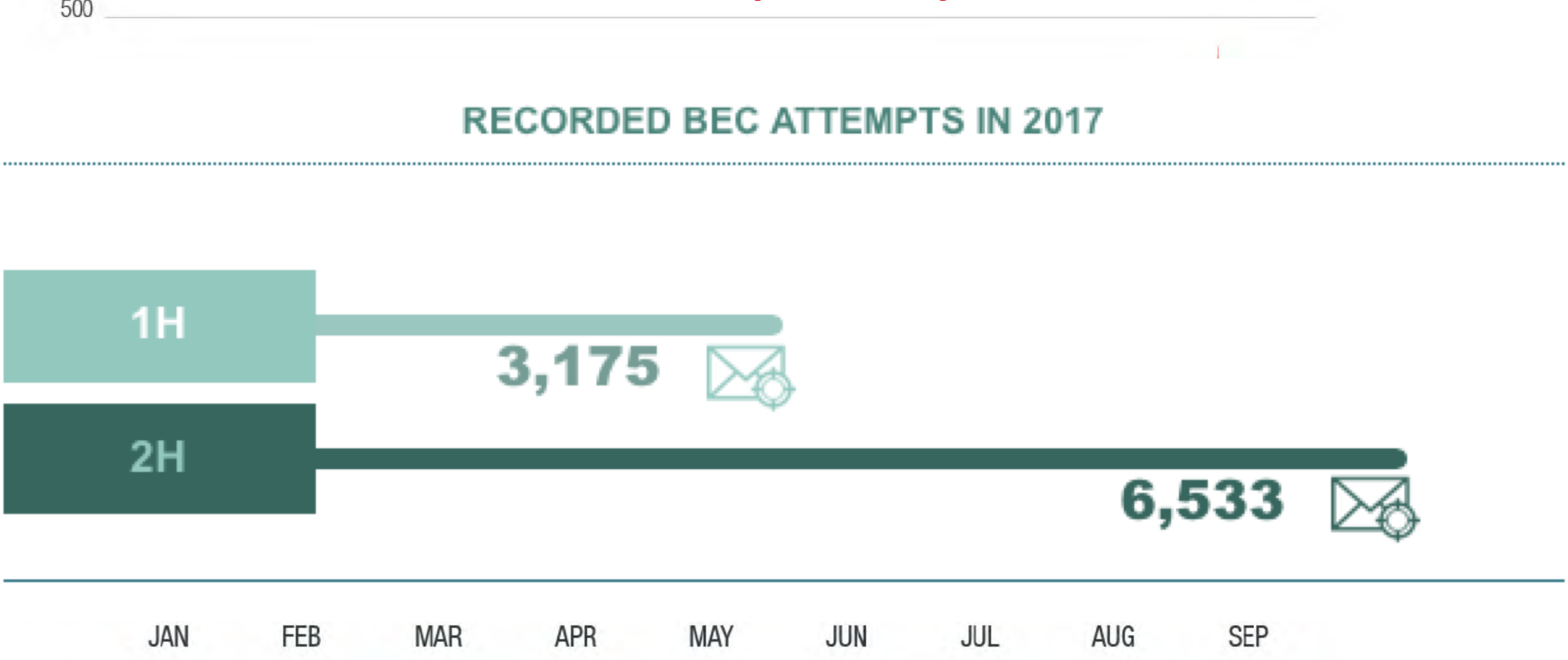
Dear Sir,

Pls find attach the pending =emittance copy for december invoice last year
We Also kindly request that you sh=uld check the remittance copy to confirm if your bank account is correct.<=SPAN>

Kind regards,
Best regards,
Bella Ed Al
Vice President
Global Operations on manufacture n=ACA International LLC1220 air port fwybed ford Texas 76022682-564-3687&nbs=;
</HTML

Business Email Compromise

2017 BEC Attack Frequency

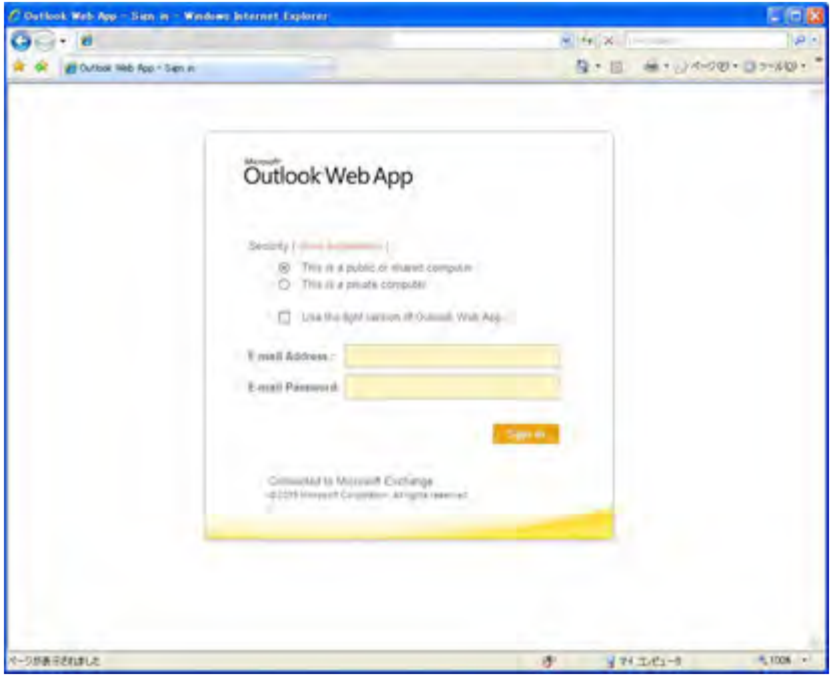


RECORDED BEC ATTEMPTS IN 2017

Timeline showing the frequency of email-only attacks

Two Main Techniques

Email-Only



Outlook Web App - Sign in - Windows Internet Explorer

Microsoft
Outlook Web App

Security ([illegible])

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

E-mail Address :
E-mail Password:

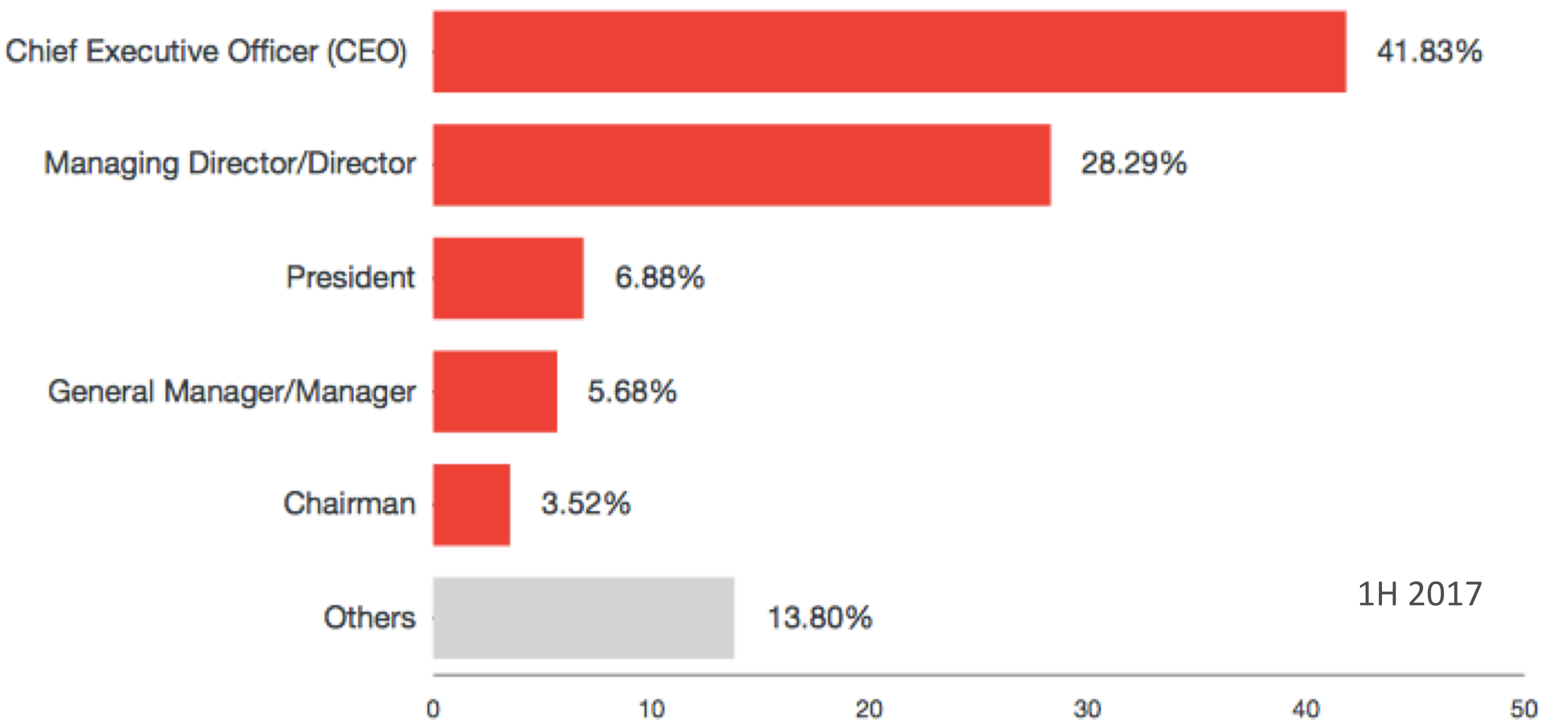
Connected to Microsoft Exchange
©2010 Microsoft Corporation. All rights reserved.

Multi-stage /
Credential-Grabbing

Popular Free Webmail Services

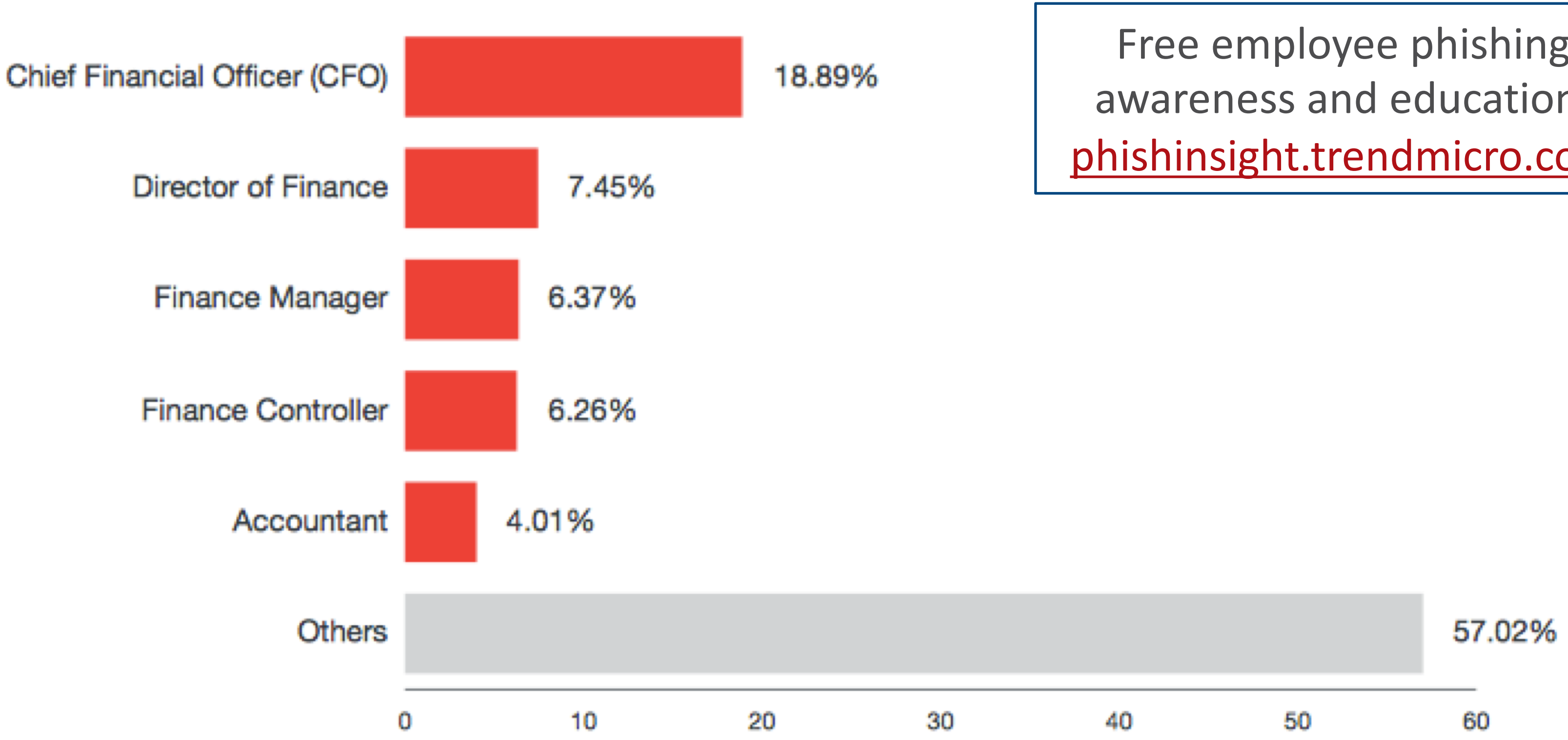
- ❑ accountant[.]com
- ❑ consultant[.]com
- ❑ contractor[.]net
- ❑ execs[.]com
- ❑ groupmail[.]com
- ❑ workmail[.]com
- ❑ writeme[.]com

Sender: BEC Spoofed Title Distribution



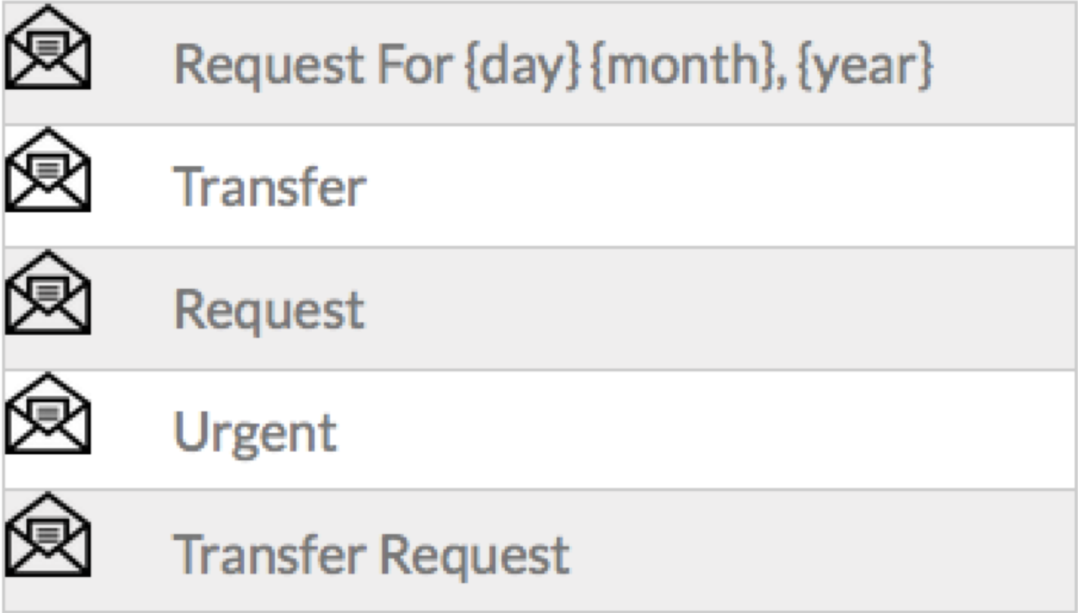
*Others includes founder, owner, practitioner, pastor, admin, consultant, secretary, controller, coordinator, sales

Recipient: Most Common Targets



Free employee phishing awareness and education: phishinsight.trendmicro.com

Common E-Mail subjects

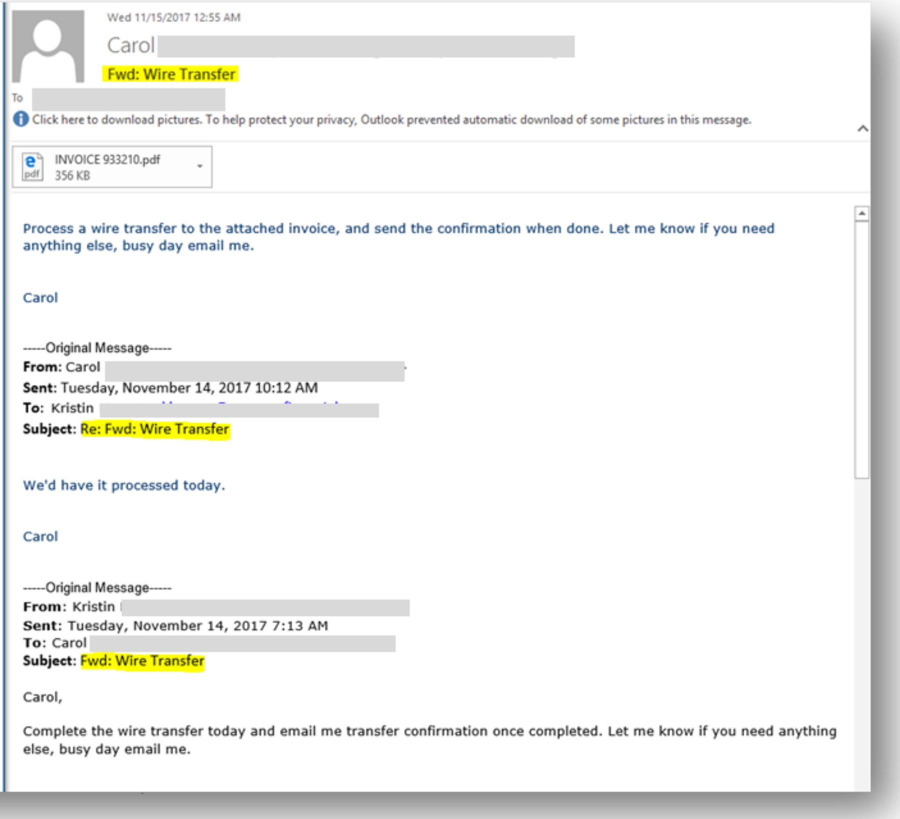


- Request For {day} {month}, {year}
- Transfer
- Request
- Urgent
- Transfer Request

Email subjects used

Long Conversation History

- Convince the receiver of legitimacy



Wed 11/15/2017 12:55 AM

Carol [redacted]

Fwd: Wire Transfer

To [redacted]

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

INVOICE 933210.pdf
356 KB

Process a wire transfer to the attached invoice, and send the confirmation when done. Let me know if you need anything else, busy day email me.

Carol

-----Original Message-----
From: Carol [redacted]
Sent: Tuesday, November 14, 2017 10:12 AM
To: Kristin [redacted]
Subject: Re: Fwd: Wire Transfer

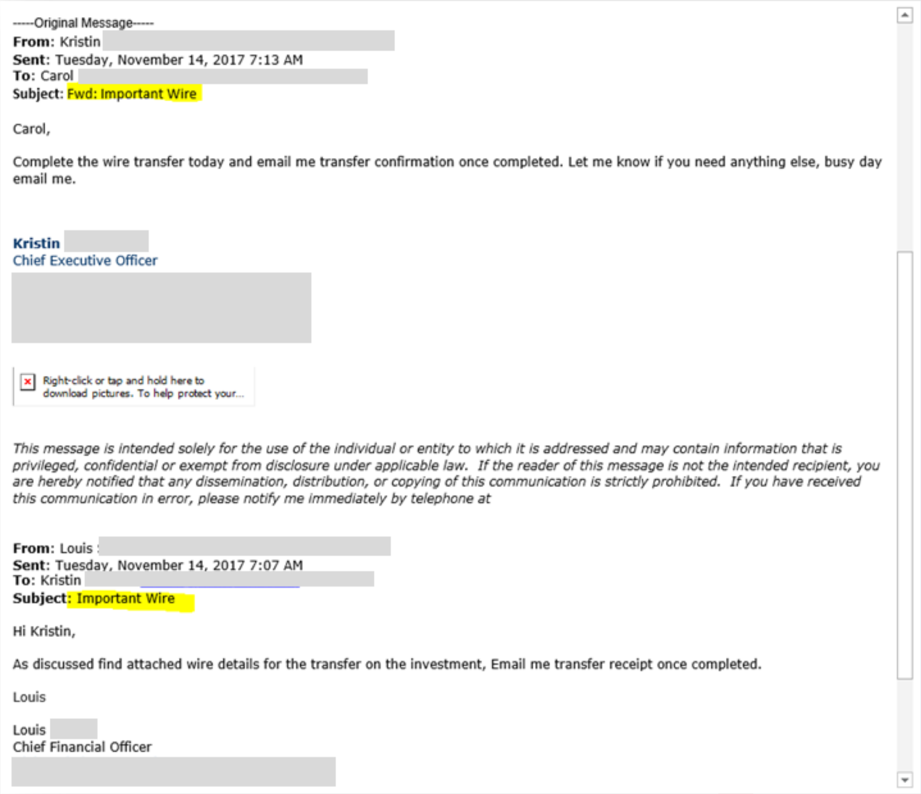
We'd have it processed today.

Carol

-----Original Message-----
From: Kristin [redacted]
Sent: Tuesday, November 14, 2017 7:13 AM
To: Carol [redacted]
Subject: Fwd: Wire Transfer

Carol,

Complete the wire transfer today and email me transfer confirmation once completed. Let me know if you need anything else, busy day email me.



-----Original Message-----
From: Kristin [redacted]
Sent: Tuesday, November 14, 2017 7:13 AM
To: Carol [redacted]
Subject: Fwd: Important Wire

Carol,

Complete the wire transfer today and email me transfer confirmation once completed. Let me know if you need anything else, busy day email me.

Kristin [redacted]
Chief Executive Officer

[redacted]

Right-click or tap and hold here to download pictures. To help protect your...

This message is intended solely for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential or exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by telephone at

From: Louis [redacted]
Sent: Tuesday, November 14, 2017 7:07 AM
To: Kristin [redacted]
Subject: Important Wire

Hi Kristin,

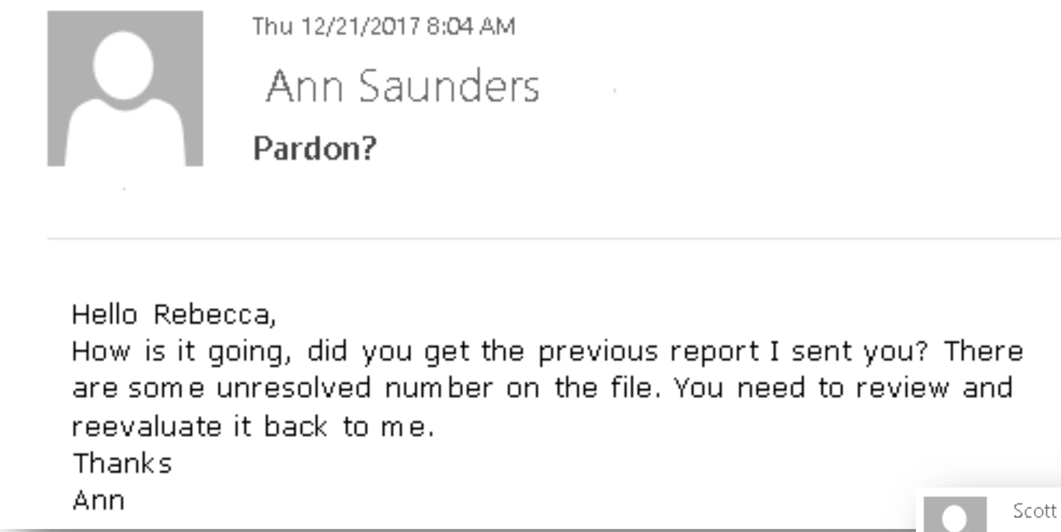
As discussed find attached wire details for the transfer on the investment, Email me transfer receipt once completed.

Louis

Louis [redacted]
Chief Financial Officer

[redacted]

Induce Recipient to Reply

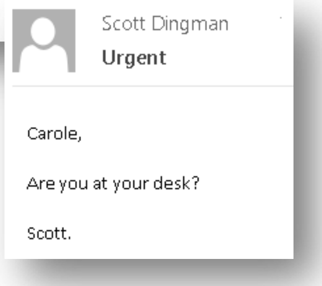


Thu 12/21/2017 8:04 AM

Ann Saunders

Pardon?

Hello Rebecca,
How is it going, did you get the previous report I sent you? There are some unresolved number on the file. You need to review and reevaluate it back to me.
Thanks
Ann



Scott Dingman

Urgent

Carole,

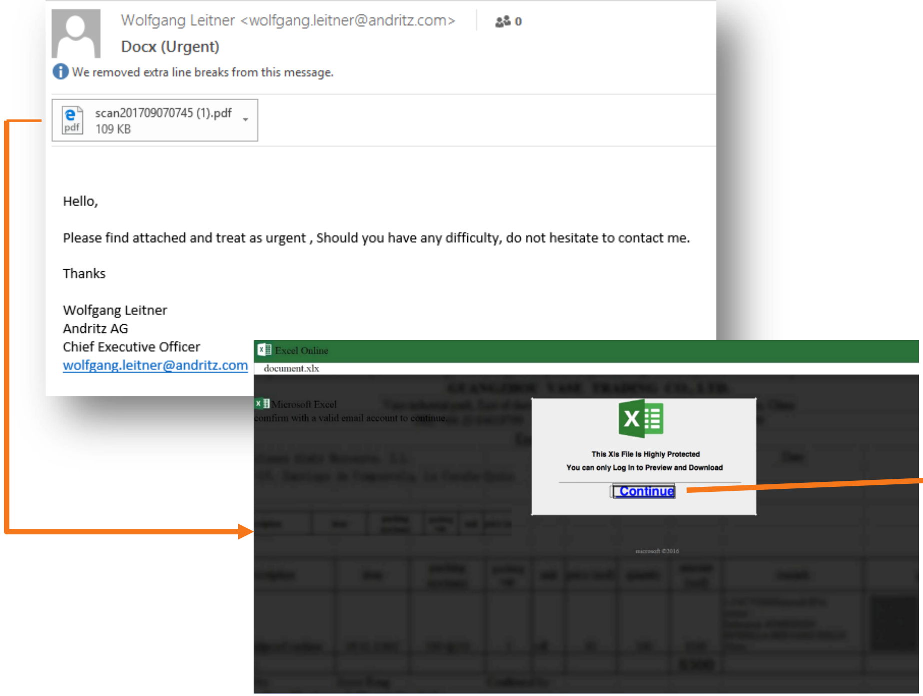
Are you at your desk?

Scott.

- Once the recipient replies, attacker might send back a fake report (might be a malicious file) and the recipient will be infected.
- Just like the common BEC scenario, “Are you at your desk?”, the attacker only send out the instructions after recipient replies.

Multi Stage: Credential Stealing

- Email sender claim as CEO
  - Email with pdf attachment (looks like excel) and try to phish enterprise employees



Wolfgang Leitner <wolfgang.leitner@andritz.com>

Docx (Urgent)

We removed extra line breaks from this message.

scan201709070745 (1).pdf
109 KB

Hello,

Please find attached and treat as urgent , Should you have any difficulty, do not hesitate to contact me.

Thanks

Wolfgang Leitner
Andritz AG
Chief Executive Officer
wolfgang.leitner@andritz.com

Excel Online

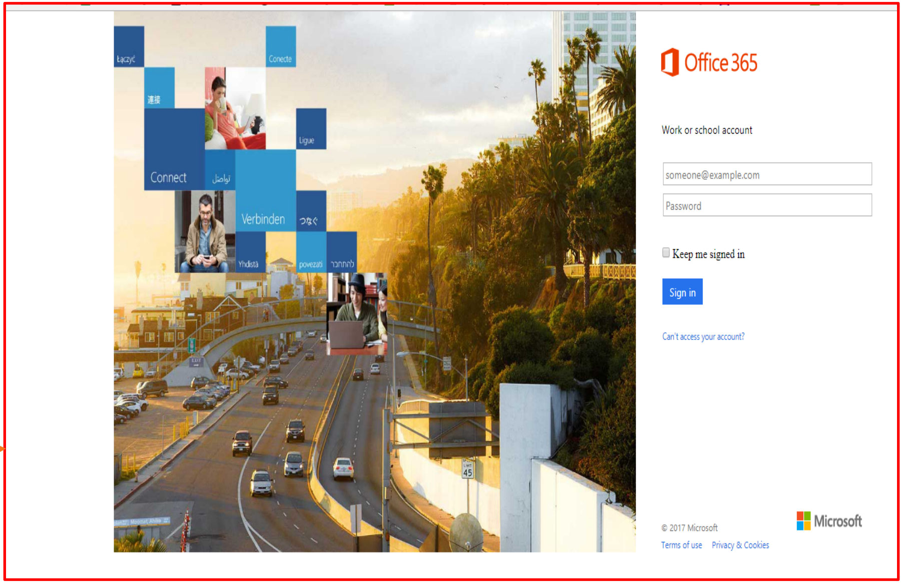
document.xlx

Microsoft Excel
confirm with a valid email account to continue

This Xls File Is Highly Protected
You can only Log In to Preview and Download

Continue

microsoft ©2016



Office 365

Work or school account

someone@example.com

Password

□ Keep me signed in

Sign in

Can't access your account?

© 2017 Microsoft

Terms of use Privacy & Cookies

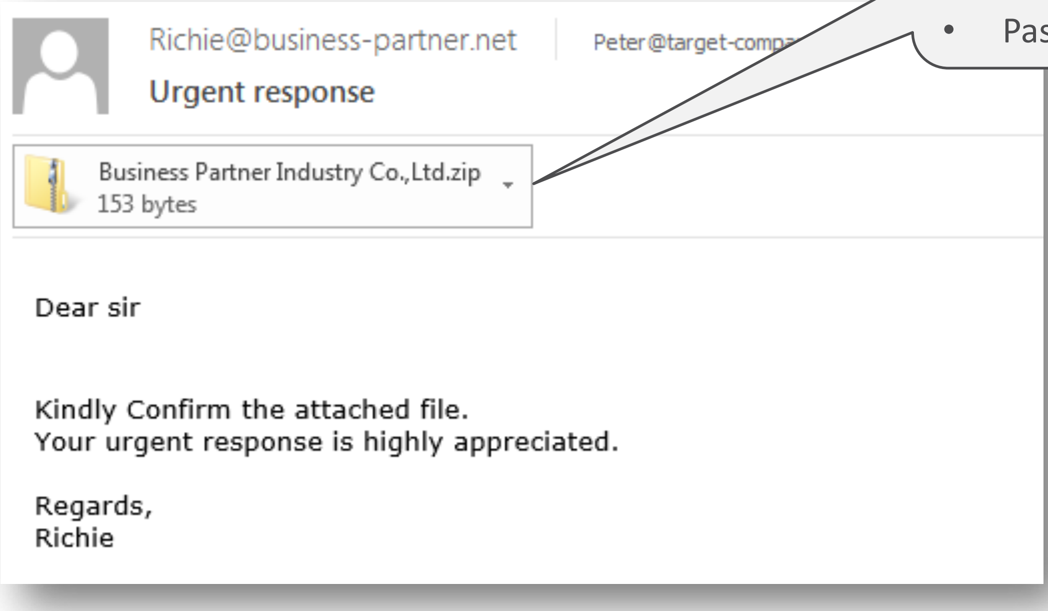
Microsoft

Multi Stage Attacks: *Reconnaissance*

$9
incl 24x7
support

‘Agent Tesla’ malware:

- Keystroke logger
- Screenshot
- Password recovery



Richie@business-partner.net | Peter@target-compa

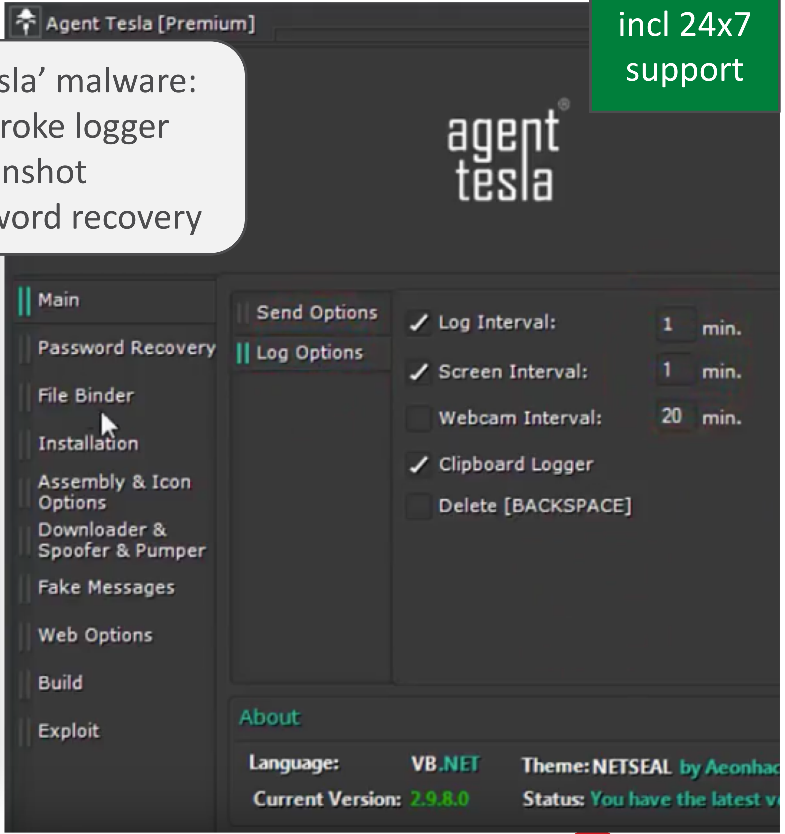
Urgent response

Business Partner Industry Co.,Ltd.zip
153 bytes

Dear sir

Kindly Confirm the attached file.
Your urgent response is highly appreciated.

Regards,
Richie



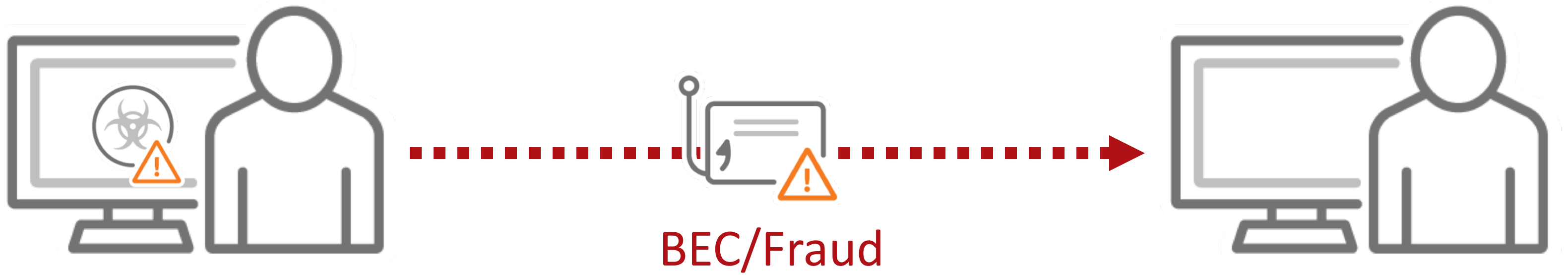
Agent Tesla [Premium]

✓ Log Interval: 1 min.
✓ Screen Interval: 1 min.
□ Webcam Interval: 20 min.
✓ Clipboard Logger
□ Delete [BACKSPACE]

About

Language: VB.NET
Current Version: 2.9.8.0
Theme: NETSEAL by Aeonhac
Status: You have the latest v

Multi Stage Attacks:
Internal Phishing Emails from Trusted Users

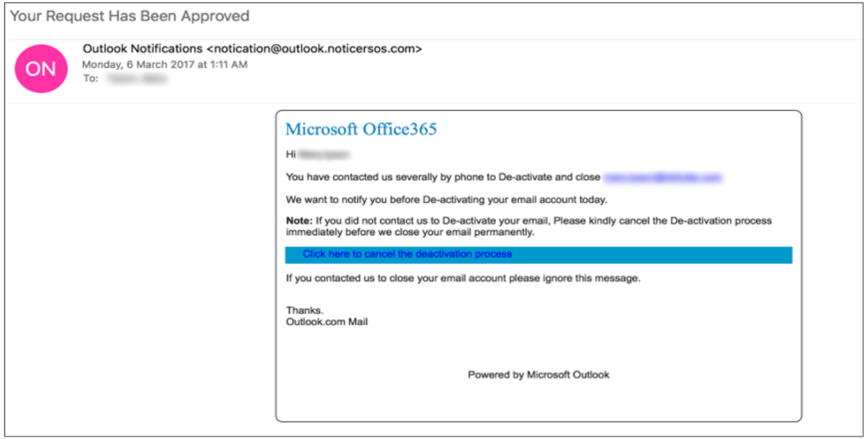


BEC/Fraud

Employee A
compromised device or email credentials

Employee B

Multi-stage attack example:
Credential Phishing → Internal BEC Attack



Your Request Has Been Approved

ON Outlook Notifications <notication@outlook.noticersos.com>
Monday, 6 March 2017 at 1:11 AM
To: [redacted]

Microsoft Office365

Hi [redacted]

You have contacted us severally by phone to De-activate and close [redacted]

We want to notify you before De-activating your email account today.

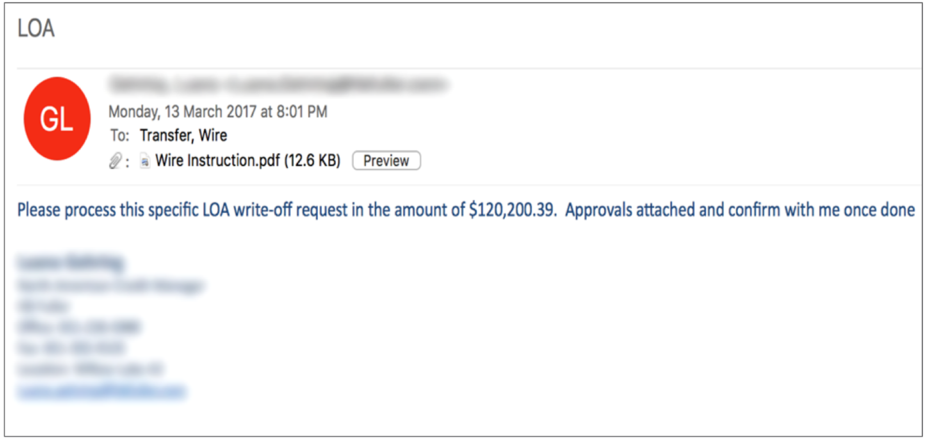
Note: If you did not contact us to De-activate your email, Please kindly cancel the De-activation process immediately before we close your email permanently.

Click here to cancel the deactivation process

If you contacted us to close your email account please ignore this message.

Thanks.
Outlook.com Mail

Powered by Microsoft Outlook

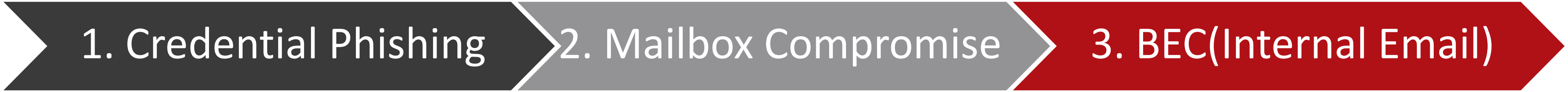


LOA

GL [redacted]
Monday, 13 March 2017 at 8:01 PM
To: Transfer, Wire
Wire Instruction.pdf (12.6 KB) Preview

Please process this specific LOA write-off request in the amount of $120,200.39. Approvals attached and confirm with me once done

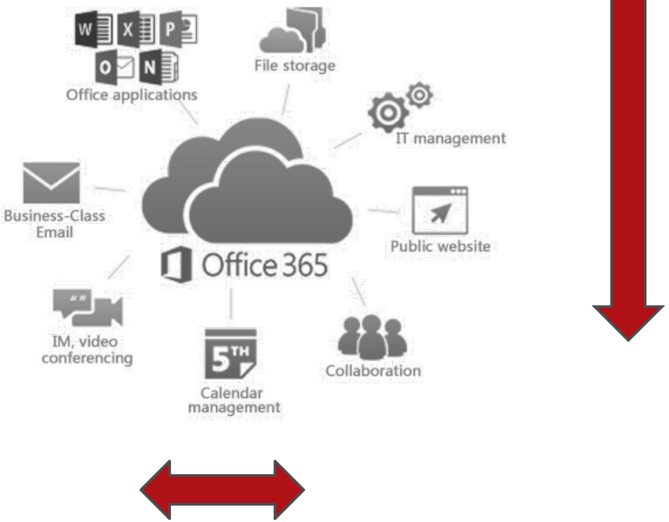
[redacted]



1. Credential Phishing
2. Mailbox Compromise
3. BEC(Internal Email)

Office 365 Risks

Office 365 Content Security Risks



Inbound Email Threats:

- Phishing
- Business Email Compromise (i.e. fake CEO emails, wire transfer scams)
- Malware
  - Known malware
  - Unknown malware
  - Malicious macros, scripts
- Malicious URLs

Internal Email/File Sharing Threats:

- *Internal* phishing emails from compromised accounts/devices
- Malware shared via OneDrive, SharePoint

Why add 3rd Party Security to Office 365?

Security is *your* responsibility

<E3: basic security for *known* malware
→ 90% malware is *unknown*

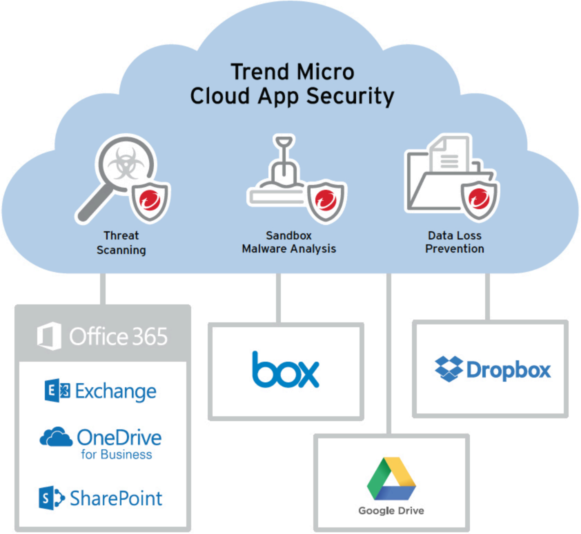
E5/ATP: has sandbox but not as mature. No fraud technology.

Popularity creates vulnerability

90% organization use at least 1 Office 365 service

Protect Against Malicious Emails

Trend Micro Cloud App Security



Advanced Threat Detection

- 2nd layer of protection to Office 365
- Finds zero-day and hidden threats
- AI and sandbox malware detection
- BEC and advanced phishing protection

Simple API Integration

- No impact to user/admin functionality

2017: Protected customers from 3.4M high-risk threats not detected by Office 365 security

Detecting Unknown Malware

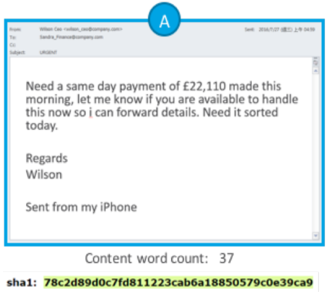
Pre-execution machine learning – Predicts file malicious using thousands of file features and a machine learning model. Improves email delivery efficiency by finding unknown malware before sandbox.

Document Exploit Detection – Parses files to look for known and potential exploits to the intended office application. Key technology in discovering new zero-day exploits in the wild.

Sandbox analysis – Behavioral analysis with multiple OS in parallel. Uses top-rated Deep Discovery technology. Pre-filters screen out 98% files and average analysis time is only 3 minutes.

New A.I. based Email Fraud (BEC) Detection: mimics the decision making of a security expert

Real



From: Wilson Ceo <wilson_ceo@company.com>
To: Sandra_Finance@company.com
Cc:
Subject: URGENT
Sent: 2016/7/27 (週三) 上午 04:59

Need a same day payment of £22,110 made this morning, let me know if you are available to handle this now so i can forward details. Need it sorted today.

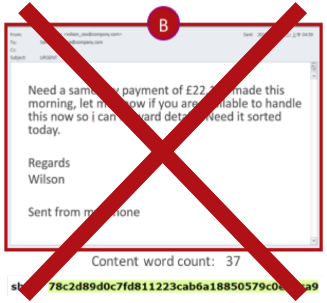
Regards
Wilson

Sent from my iPhone

Content word count: 37

sha1: 78c2d89d0c7fd811223cab6a18850579c0e39ca9

Fraud



From: <wilson_ceo@company.com>
To: Sa e@company.com
Cc:
Subject: URGENT
Sent: 20 上午 04:59

Need a sam y payment of £22. made this morning, let m ow if you are ilable to handle this now so i can ward deta Need it sorted today.

Regards
Wilson

Sent from m hone

Content word count: 37

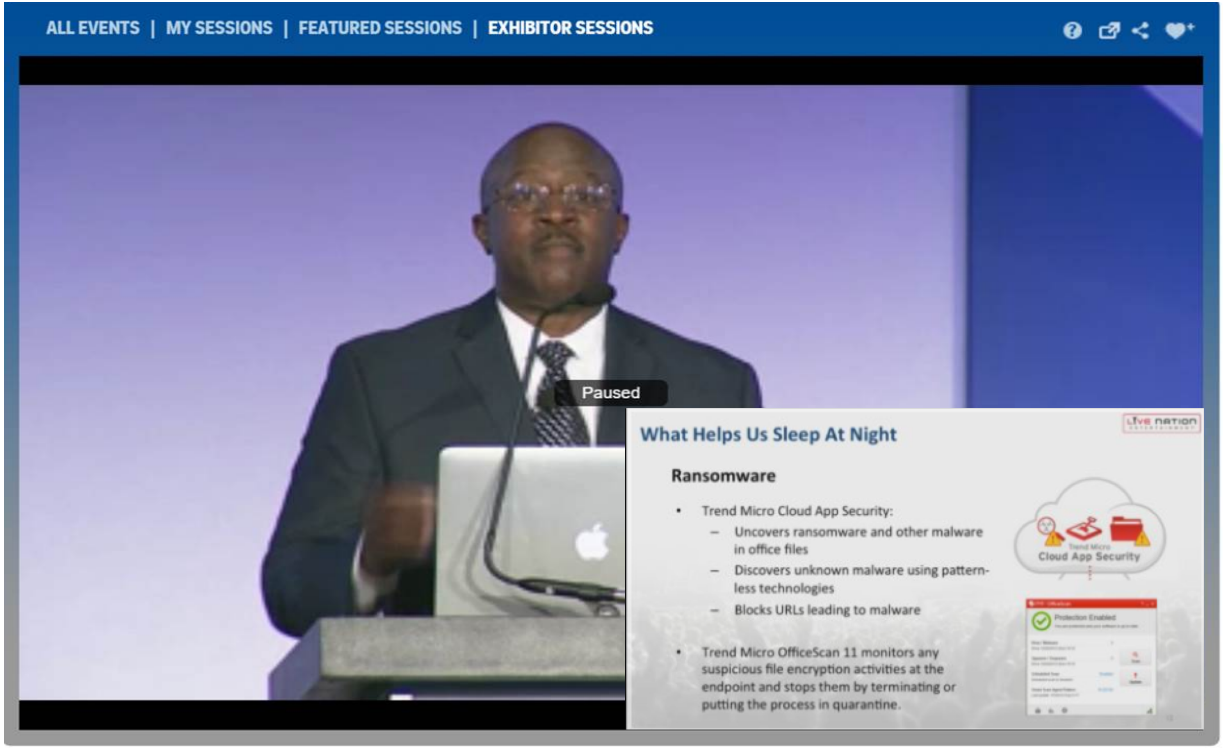
sh 78c2d89d0c7fd811223cab6a18850579c0e a9

Behavior	Routing behavior
	Cousin domain
	High-profile user similarity
	…
Intention	Payment, PII
	Urgency
	…

Rule weighting and correlation

More precise identification

Customer: Live Nation


ALL EVENTS | MY SESSIONS | FEATURED SESSIONS | EXHIBITOR SESSIONS
Paused
Trend Micro
Cloud App Security
Protection Enabled

What Helps Us Sleep At Night

Ransomware

- Trend Micro Cloud App Security:
  - Uncovers ransomware and other malware in office files
  - Discovers unknown malware using pattern-less technologies
  - Blocks URLs leading to malware
- Trend Micro OfficeScan 11 monitors any suspicious file encryption activities at the endpoint and stops them by terminating or putting the process in quarantine.

"Deploying Trend Micro Cloud App Security [for Office 365] reduced the malware infections that the Incident Response Team needed to respond to by 90%"

James Patterson Wicks, CISSP (Sr. Director at Live Nation), June 2016. (video starting at 00:11:55)

Customer: Transportation and Logistic Company in EU
Users: over 25,000

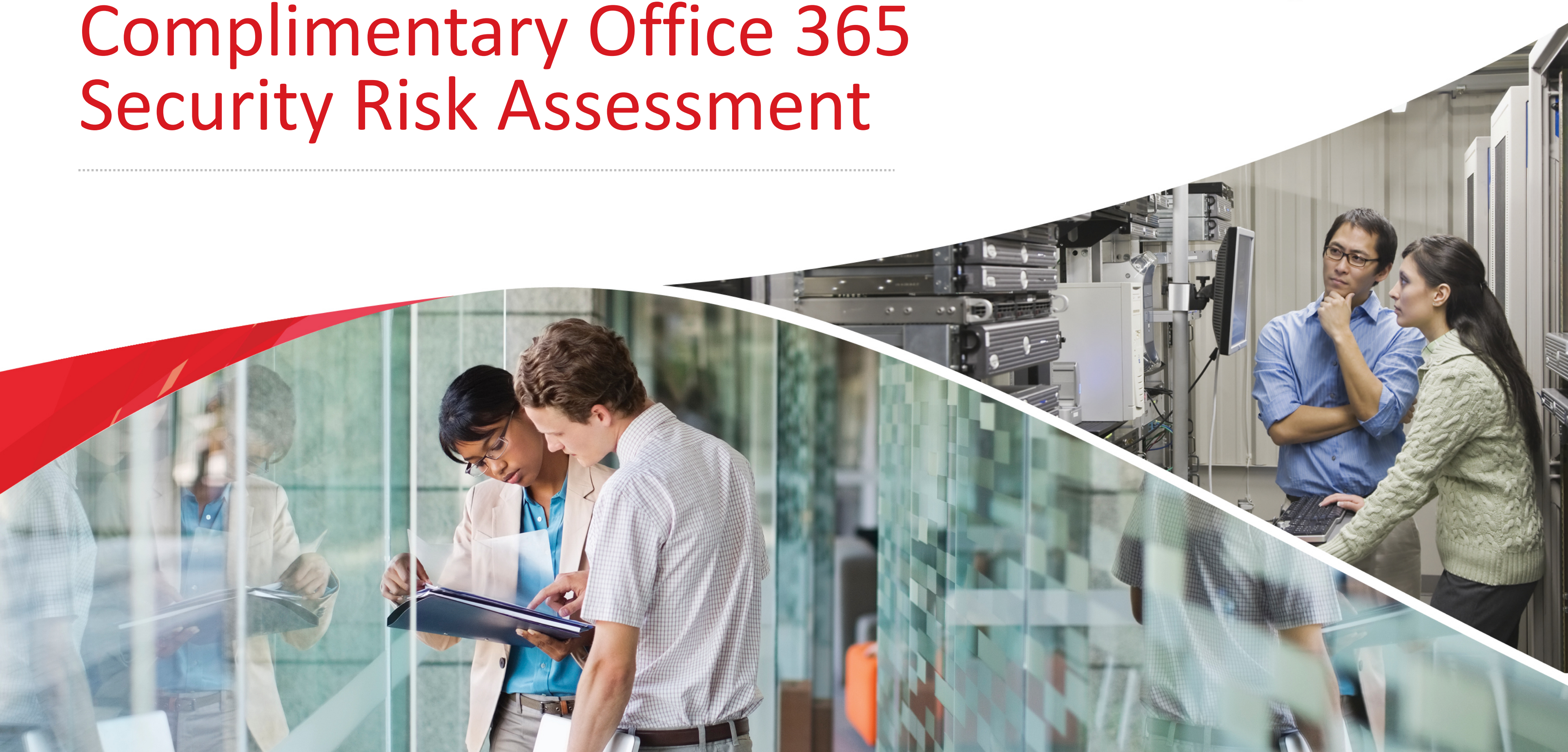
CHALLENGE

- Ransomware attacks result in reputation damage & revenue loss
- Currently using Microsoft **Office 365 E5 with ATP service**
- Need to identify security gap in a short period

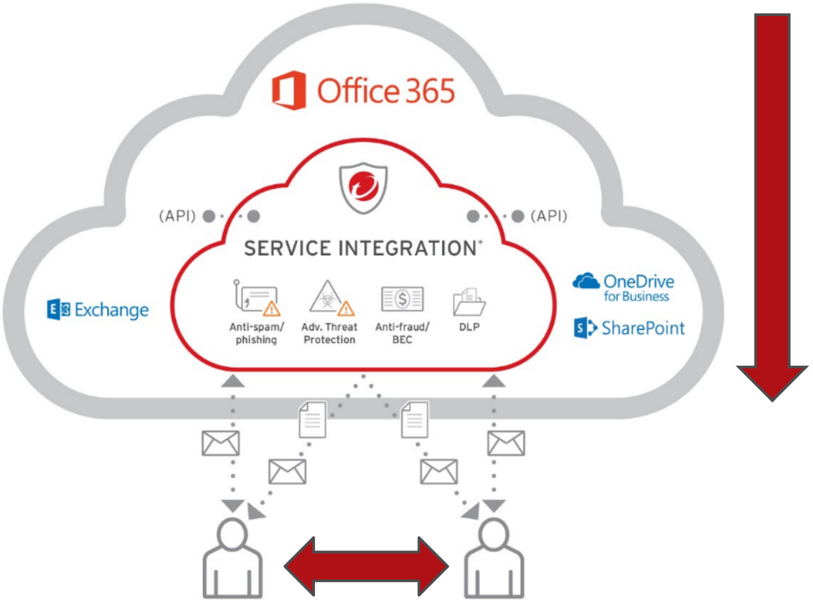
RESULTS (before XGen and without sandbox)

- Manual scan 3 days email and OneDrive Data
- Identified 3,000 adv. phishing, 28 ransomware in email
- Identified 4 ransomware files in OneDrive

Complimentary Office 365 Security Risk Assessment



Risks to Office 365 Covered by Assessment



Inbound Email Threats:

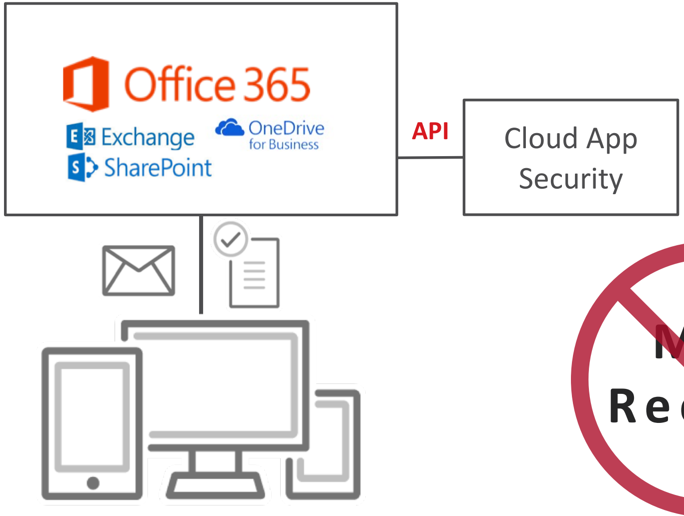
- Phishing
- Business Email Compromise
- Malware
  - Known malware
  - Unknown malware
  - Malicious macros, scripts
- Malicious URLs

Internal Email & File Sharing Threats:

- *Internal* phishing emails from compromised accounts/devices
- Malware shared via OneDrive, SharePoint

Simple Integration with Office 365

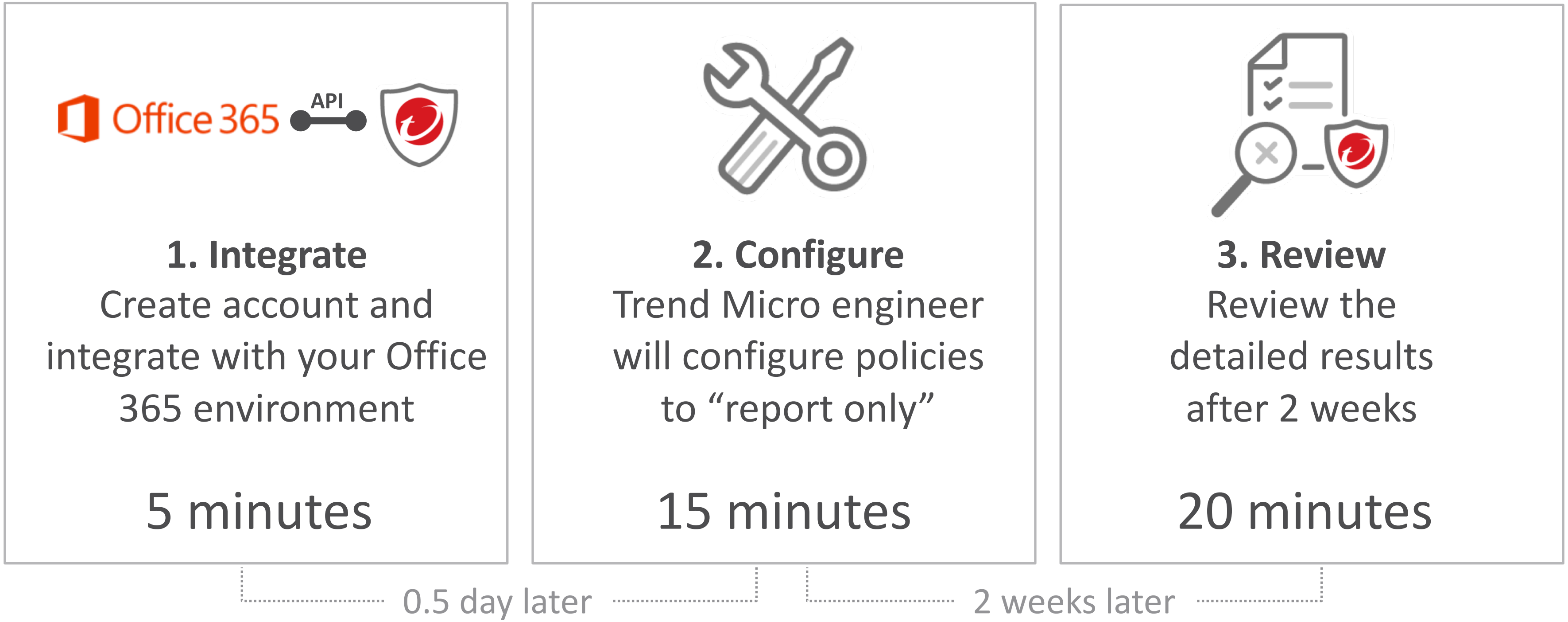
- Direct cloud-to-cloud integration using Microsoft API's
- Assessment will monitor only and will not delay/block email
- No impact to user/admin functionality.



Office 365
Exchange
OneDrive for Business
SharePoint
API
Cloud App Security

MX Record
Software
User settings

3 Steps for the Office 365 Risk Assessment



1. Integrate
Create account and integrate with your Office 365 environment

5 minutes

2. Configure
Trend Micro engineer will configure policies to “report only”

15 minutes

3. Review
Review the detailed results after 2 weeks

20 minutes

0.5 day later

2 weeks later

Sign Up for Complimentary O365 Risk Assessment:

Email: enterprise_marketing_sg@trendmicro.com

For more information visit: www.trendmicro.com/office365