

E-Mail Security Add-on

BEC und O-hour Phishing gezielt verhindern

Context matters:

Introducing a radically different approach to email security

January 2024

About me

- Security nerd and former security researcher
 - Software exploitation and defense
 - Mobile security
 - Cloud side-channels
- Started with offensive security as a teenager
- Co-founded xorlab, an ETH Zurich Spin-off in cybersecurity



Antonio Barresi,
CEO & Co-Founder

xorlab



Email Security 2024



Successful breaches cost \$\$



“Phishing and stolen or compromised credentials were the two most common initial attack vectors.”

IBM Security

Cost of a Data Breach Report 2023

Cost and frequency of a data breach by initial attack vector

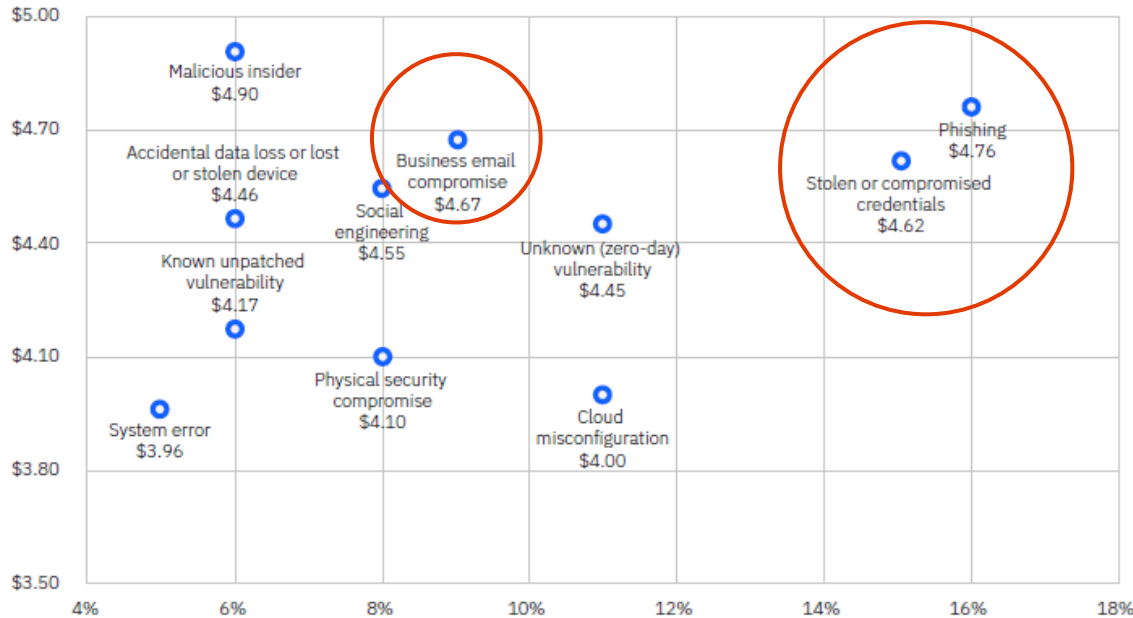


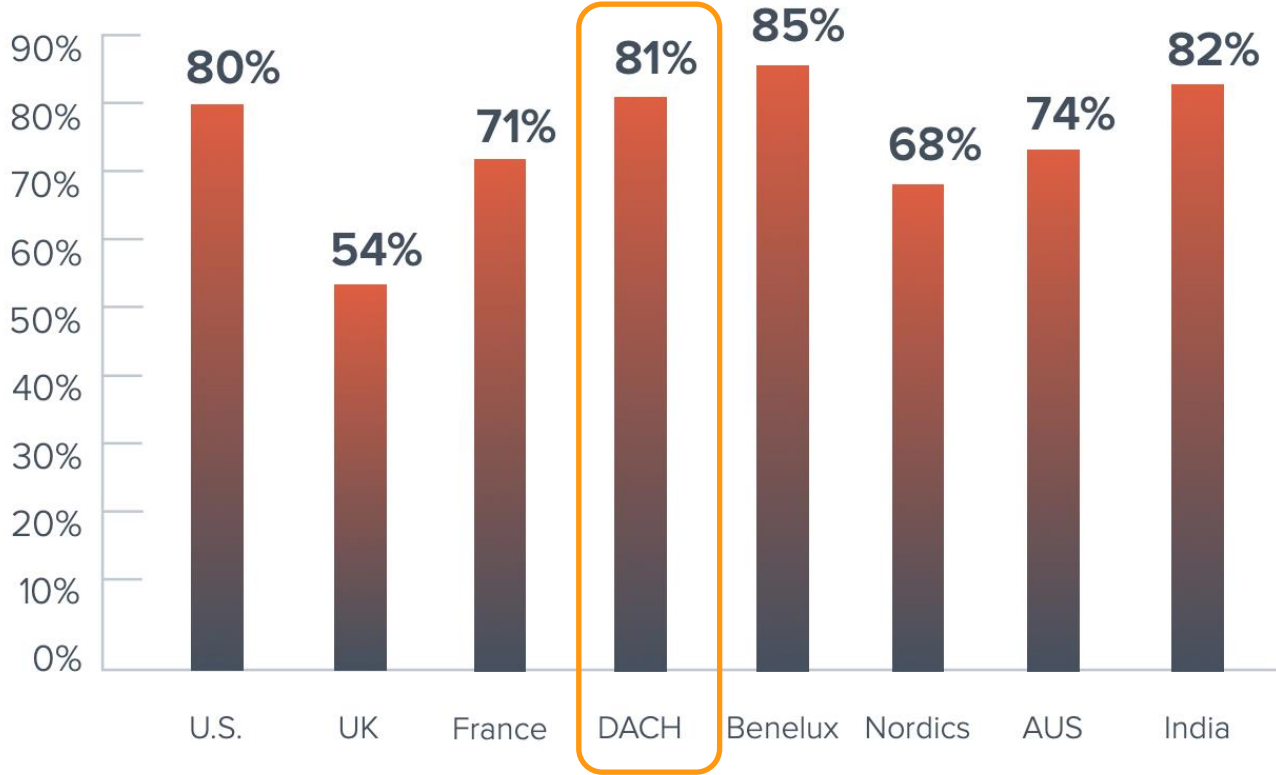
Figure 10. Measured in USD millions



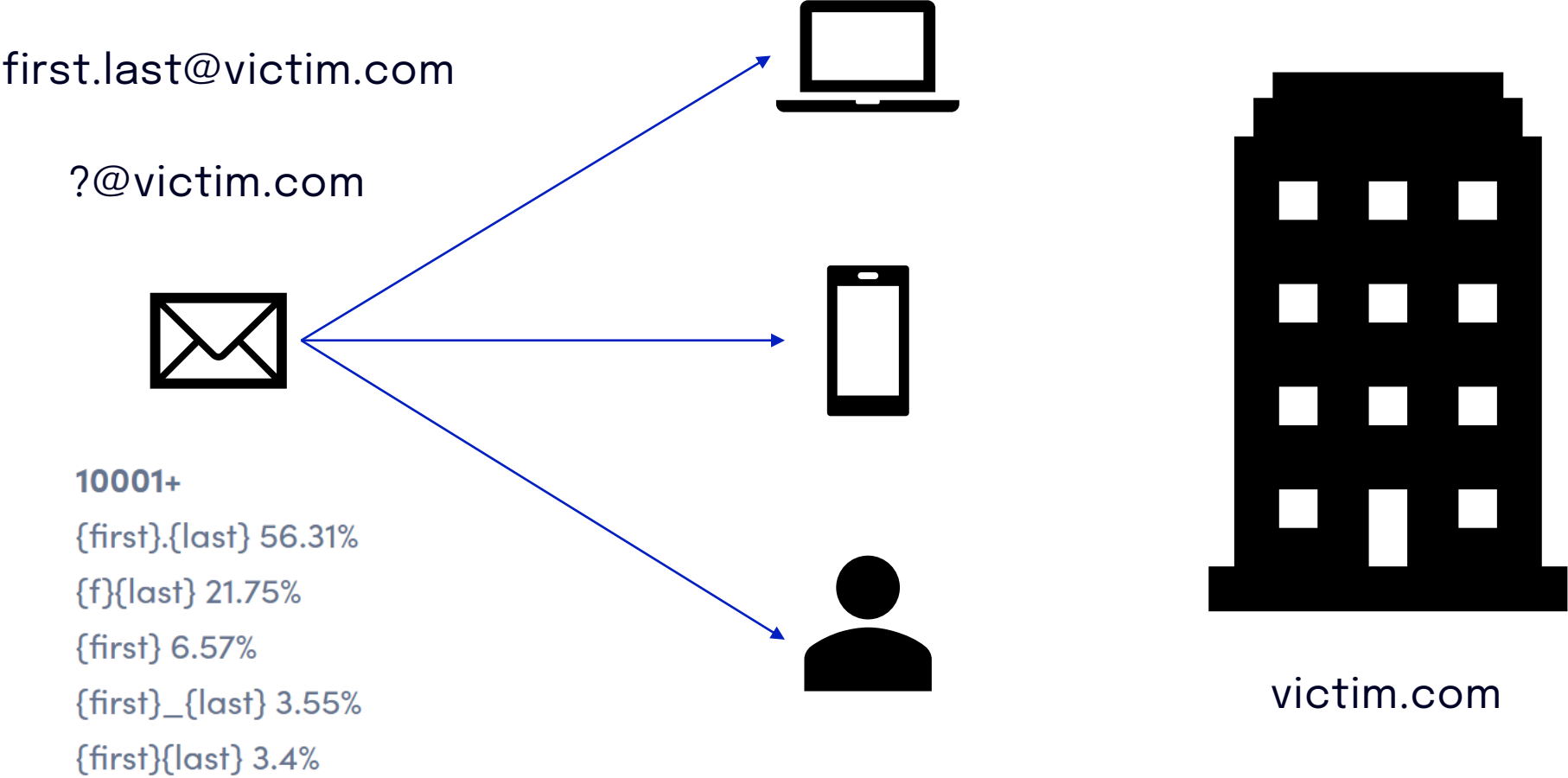
Have you faced one?

Has your organization faced any successful email-based security attacks in the past year?

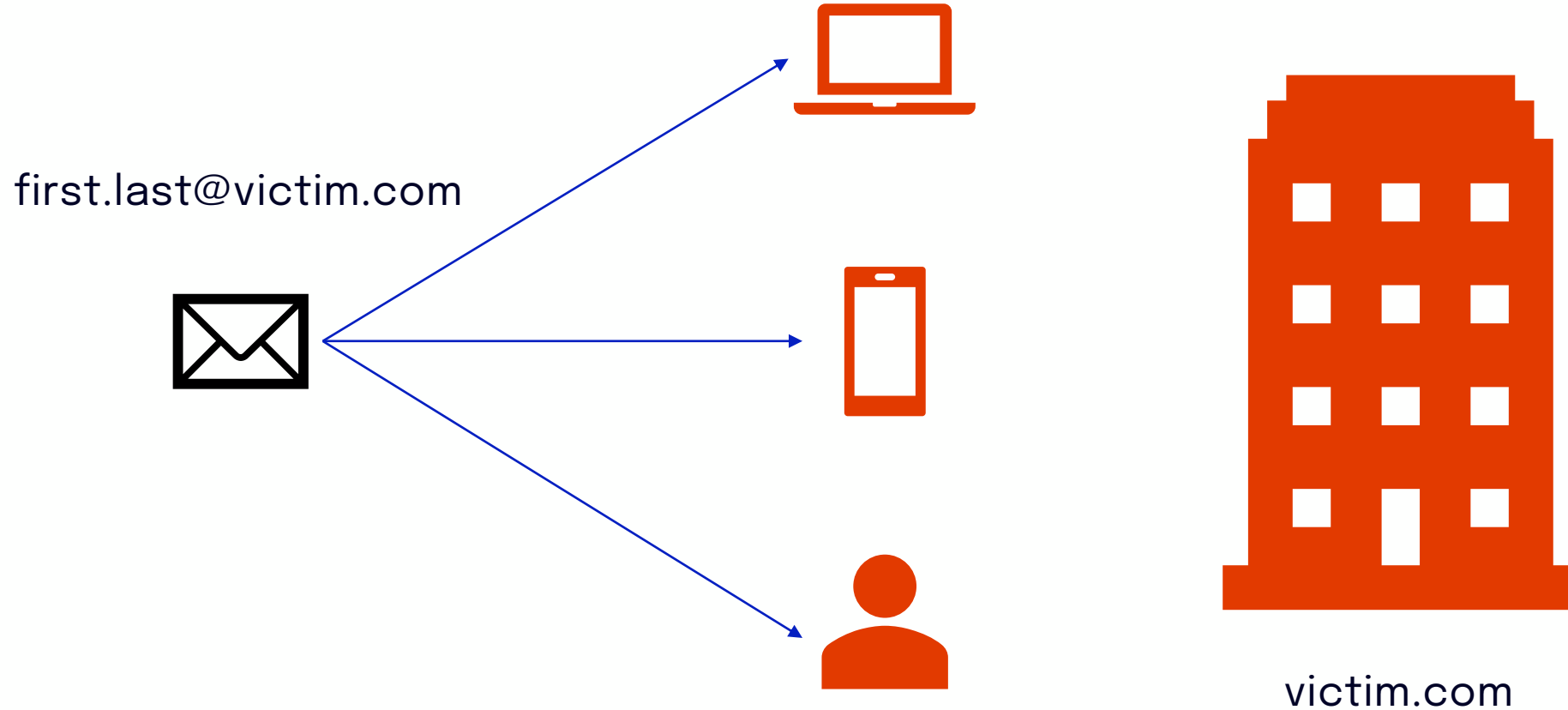
(n=1,350)



Why is email so interesting?



Why is email so interesting?



Modern Threats



BEC/EAC/Thread Hijacking

Business email compromise (or BEC) is a **form of phishing** attack where a criminal attempts to **trick a senior executive (or budget holder) into transferring funds**, or revealing sensitive information.

Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are **crafted to appeal to specific individuals**, and can be even harder to detect.



National Cyber
Security Centre
a part of GCHQ



BEC/EAC/Thread Hijacking

Partner / known organization or person



Unknown organization or person

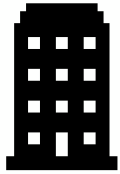


Some other **attacker-controlled** MTA
or service



BEC/EAC/Thread Hijacking

Partner / known organization or person



alice@partner.com



Unknown organization or person



john@unknown.com



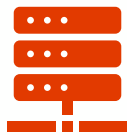
Email Account Compromise

- Brute-force/dictionary attack
- Password spraying
- Phishing
- Malware



bob@victim.com

Some other **attacker-controlled** MTA
or service

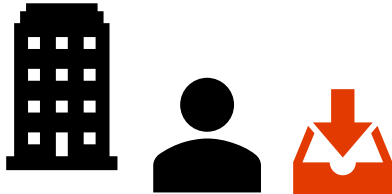


any@thing.com



BEC/EAC/Thread Hijacking

Partner / known organization or person



alice@partner.com

- Phishing/Spear-phishing
- BEC/VIP Fraud
- Thread Hijacking



Unknown organization or person



john@unknown.com

- Phishing/Spear-phishing
- BEC/VIP Fraud
- Thread Hijacking



bob@victim.com

Some other **attacker-controlled** MTA
or service



any@thing.com

- Phishing/Spear-phishing
- BEC/VIP Fraud
- Thread Hijacking



BEC/VIP Fraud

Hello [REDACTED]

I'll be glad to know that you're doing great. I was hoping you could be of assistance to me today. Kindly email back when you have some time.

Kind regards,

Antonio Hüseyin Barresi

Co-founder & CEO
xorlab

The screenshot shows a security tool interface with a dark theme. At the top left, there is a red shield icon with a white 'X' and the text 'VIP Fraud' in white, followed by 'HIGH CONFIDENCE' in a grey box. To the right, a yellow box says 'Incoming message is QUARANTINED' and a grey box says 'and it was CAMPAIGN MATCHED'. Below this, it says 'Received on 04.12.2023 at 09:23:00'. There is a 'Custom Tags' section with a plus icon. A navigation bar contains 'SUMMARY' (underlined), 'ATTACHMENTS', 'DOMAINS & URLS', 'SIMILAR', 'HEADERS', 'MATCHED RULES', and 'CONTEXT VARIABLES'. The 'Message Information' section is visible, showing fields for SUBJECT, FROM, TO, CC, BCC, REPLY TO, and PROCESSED. The 'FROM' field shows 'Antonio Hüseyin Barresi <bing.fane@mail.ru>' with a 'LOW REPUTATION 0' warning in a red box. The 'REPLY TO' field also shows 'Antonio Hüseyin Barresi <bing.fane@mail.ru>'. The 'PROCESSED' field shows '04.12.2023 09:22:56'.

VIP Fraud
HIGH CONFIDENCE

Incoming message is **QUARANTINED**
and it was **CAMPAIGN MATCHED**

Received on 04.12.2023 at 09:23:00

Custom Tags +

SUMMARY ATTACHMENTS DOMAINS & URLS SIMILAR HEADERS MATCHED RULES CONTEXT VARIABLES

Message Information

SUBJECT	[REDACTED]
FROM	Antonio Hüseyin Barresi <bing.fane@mail.ru> LOW REPUTATION 0
TO	[REDACTED]
CC	n/a
BCC	n/a
REPLY TO	Antonio Hüseyin Barresi <bing.fane@mail.ru>
PROCESSED	04.12.2023 09:22:56



BEC/VIP Fraud

Good morning [REDACTED]

Did [REDACTED] attorney at [REDACTED] Law Firm, already contact you on my behalf, by telephone or by email regarding the [REDACTED] file currently managed at the Headquarters ?

If he has not done it yet, contact him immediately on my behalf, **from your private e-mail** at the following address:

[REDACTED]
The file reference [REDACTED] must be specified in your e-mail what we are expecting from you.

I will get back to you once you have spoken to him, to give you m

Freundliche Grüße / Best Regards,

[REDACTED]
CEO | [REDACTED]

von meinem iPhone gesendet

The screenshot shows a security interface with a dark theme. At the top, a red shield icon with a white 'X' is next to the text 'VIP Fraud' and 'HIGH CONFIDENCE'. To the right, it says 'Incoming message is QUARANTINED'. Below this, it indicates the message was received on 21.12.2023 at 10:18:19. There are tabs for 'SUMMARY', 'ATTACHMENTS', 'DOMAINS & URLS', 'SIMILAR', 'HEADERS', 'MATCHED RULES', and 'CONTEXT VARIABLES'. The 'SUMMARY' tab is active, showing 'Message Information' with the following details:

SUBJECT	[REDACTED]
FROM	[REDACTED] <ceo@co-board.cc> LOW REPUTATION 0
TO	[REDACTED]
CC	n/a
BCC	n/a
REPLY TO	n/a
PROCESSED	21.12.2023 10:18:13



BEC/VIP Fraud

Liebe [REDACTED]

Ich schreibe Ihnen mit der Bitte, dass meine Kontodaten vor der nächsten Zahlung aktualisiert werden. Aufgrund kürzlicher Änderungen habe ich ein neues Bankkonto eröffnet und möchte mein Gehalt auf dieses neue Konto überweisen lassen. Kann dies vor dem nächsten Zahltag erfolgen?

Mit freundlichen Grüßen,
[REDACTED]

The screenshot shows a security analysis tool interface. At the top left, there is a red shield icon with a white 'X' and the text 'VIP Fraud' in white, with 'HIGH CONFIDENCE' in a grey box below it. To the right, a yellow box says 'Incoming message is QUARANTINED'. Below this, it says 'Received on 16.01.2024 at 15:25:26'. There is a 'Custom Tags' section with a plus icon. A navigation bar contains 'SUMMARY', 'ATTACHMENTS', 'DOMAINS & URLS' (highlighted in blue), 'SIMILAR', 'HEADERS', 'MATCHED RULES', and 'CONTEXT VARIABLES'. The main content area is titled 'Message Information' and contains a table of message details.

SUBJECT	Anfrage
FROM	[REDACTED] LOW REPUTATION 0
TO	[REDACTED]
CC	n/a
BCC	n/a
REPLY TO	n/a
PROCESSED	16.01.2024 15:25:21

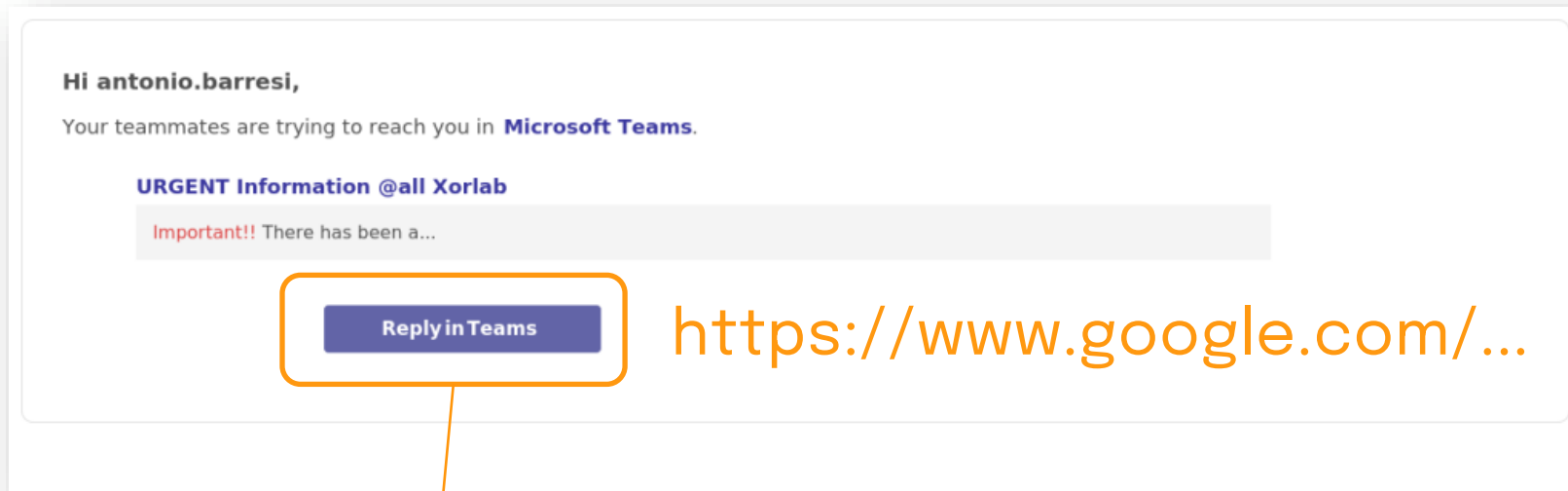


Thread Hijacking

The diagram illustrates thread hijacking. It shows two email messages. The top message, enclosed in an orange box, is a malicious email with the following text: "Hallo, Die Datei für Ihre Überprüfung ist unten angehängt. Sie können mich bei Fragen kontaktieren, lassen Sie es mich wissen. [DOKUMENT DOWNLOAD LINK](#) Danke." An orange arrow points from the word "Malicious" to this message. The bottom message, enclosed in a black box, is an existing thread with the following text: "Sehr geehrte Damen und Herren, [redacted] [redacted] [redacted] Mit freundlichen Grüßen [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]". A black arrow points from the text "Existing thread (obtained from leak or account compromise)" to the redacted content of this message.



Phishing



URL	DISPLAY TEXT	GLOBAL	LOCAL	TYPE
http://rrrtb.ywetxaxzcf.boats	n/a	0	0	Embedded
https://www.google.com/amp/RRrtb.ywetxaxzcf.boats/jTzb6	n/a	96	63	Embedded
https://www.google.com/url?hl=en&q=https://www.google.com/amp/RRrtb.ywetxaxzcf.boats/jTzb6&s...	n/a	96	63	Hyperlink
https://xorlab.com	n/a	90	100	Hyperlink

Phishing

Security vendors' analysis

Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antiy-AVL	Clean
Avira	Clean
Bfore AI PreCrime	Clean
BlockList	Clean
Certego	Clean
CIS Army	Clean
CRDF	Clean
CyRadar	Clean
DNSB	Clean
EmergingThreats	Clean
ESET	Clean
Feodo Tracker	Clean
G-Data	Clean
GreenSnow	Clean
IPsum	Clean
K7AntiVirus	Clean
Malware	Clean
malwares.com URL checker	Clean
Phishing Database	Clean
PREBYTES	Clean
Quttera	Clean
Sangfor	Clean
SCUMWARE.org	Clean
SecureBrain	Clean
SpooT IP sample list	Clean
Heimdal Security	Clean
Juniper Networks	Clean
Lionic	Clean
MalwarePatrol	Clean
OpenPhish	Clean
Phishtank	Clean
Quick Heal	Clean
Rising	Clean
Scantitan	Clean
Seclookup	Clean
securolytics	Clean
Scybe	Clean

0 / 90

No security vendors flagged this URL as malicious

Reanalyze Search Graph API

http://rrrtb.ywetxazcf.boats/

rrrtb.ywetxazcf.boats

text/plain

Status 404 Content type text/plain; charset=utf-8 Last Analysis Date 5 months ago

DETECTION DETAILS COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

History

First Submission	2023-08-15 09:36:22 UTC
Last Submission	2023-08-15 09:36:22 UTC
Last Analysis	2023-08-15 09:36:22 UTC

HTTP Response

Final URL

https://rrrtb.ywetxazcf.boats/

xorlab

Message Detail - Xorlab mentioned you @antonio.barresi on Tuesday, August 15, 2023 #03322295 - [7ebbb714-3d0c-460b-8e68-057972de4f93] - ActiveGuard C2

adrian.kyburz@xorlab.com

Phishing HIGH CONFIDENCE

Received on 15.08.2023 at 10:38:14

0-hour

Tuesday, August 15, 2023 #03322295

Organization 0 Organizational 0

spam 180daysoldsender 90daysoldsender highrisk

domainfirstcontact domainonlyinbound mediumscore

Preview

Hi antonio.barresi,

Your teammates are trying to reach you in Microsoft Teams.

URGENT Information @all Xorlab

Important! There has been a...

Reply in Teams



Zero-hour Phishing

- How many of today's Phishing emails are zero-hour?
- Zero-hour: not seen before and doesn't match any known malicious URLs database
- We did an analysis at one of our customers (almost 6k seats)
 - Over 90 days we saw

Phishing prevented	12'461
- Zero-hour Phishing prevented	10'147
- Known Phishing prevented	2'314

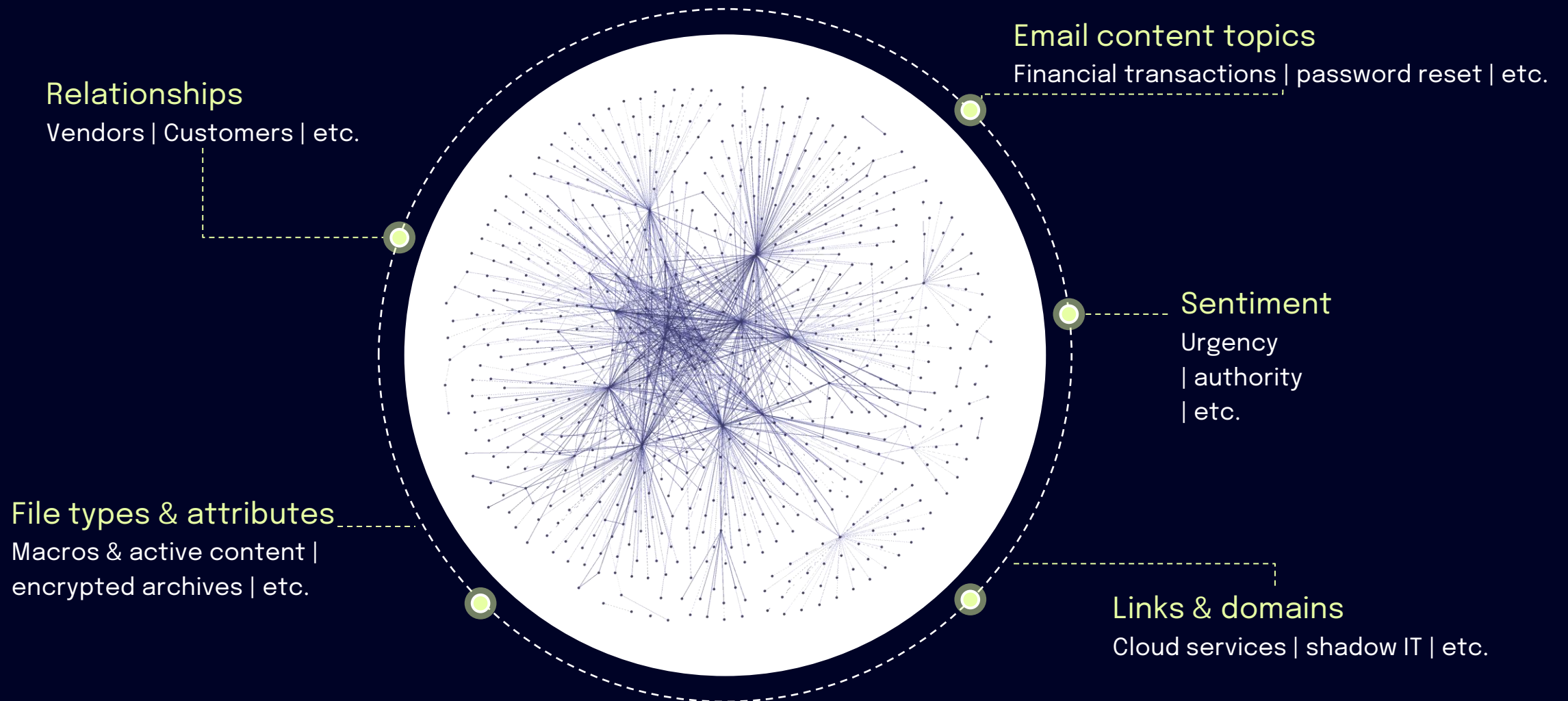
81.43%
were zero-hour



Our approach as
add-on for M365



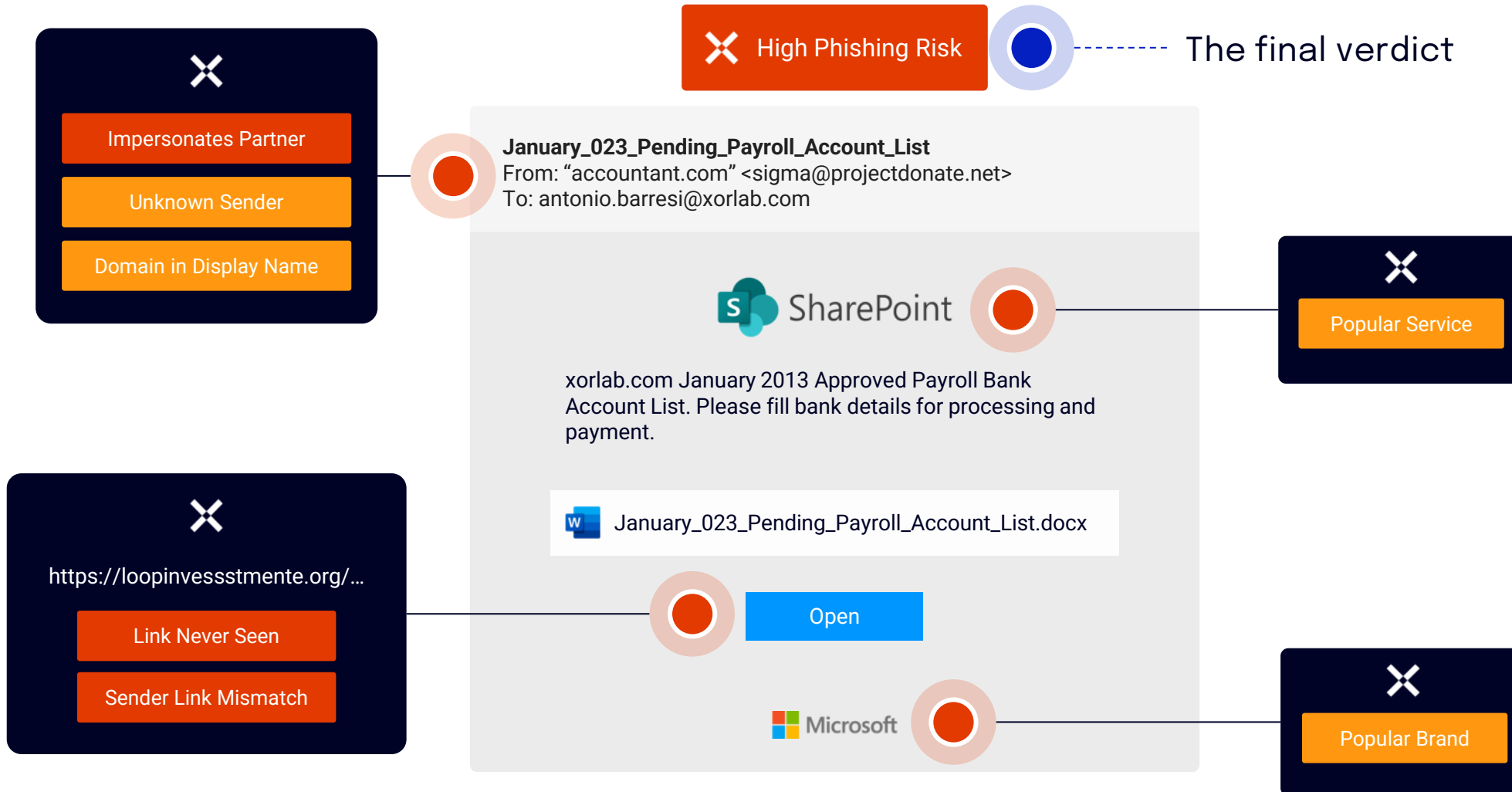
Context-intelligence



Plot: Visualizing the relationships from 3 months worth of xorlab email communication



Stop 0-hour phishing and BEC



xorlab Security Platform | Overview



Solution:

Inbound Email Security

See more, detect more, and stop threats that go otherwise undetected.

- Detect 2-4x more threats than traditional solutions and prevent 0-hour phishing and BEC attacks
- Minimize manual work with adaptive security policies
- Reduce operational efforts with an audited self-service portal

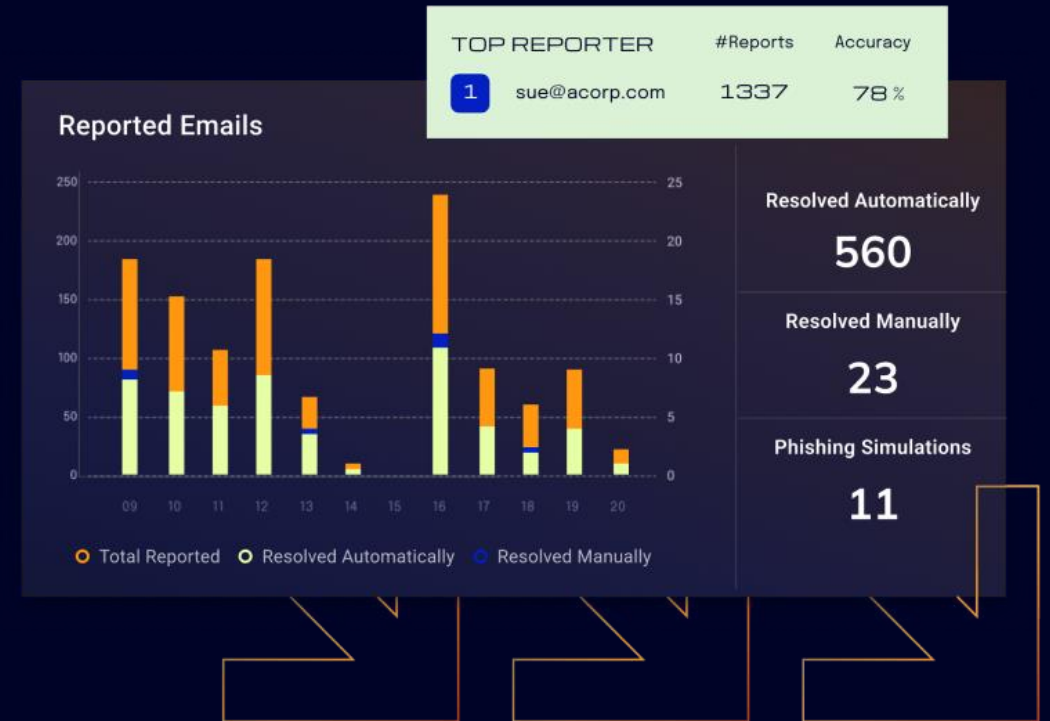


Solution:

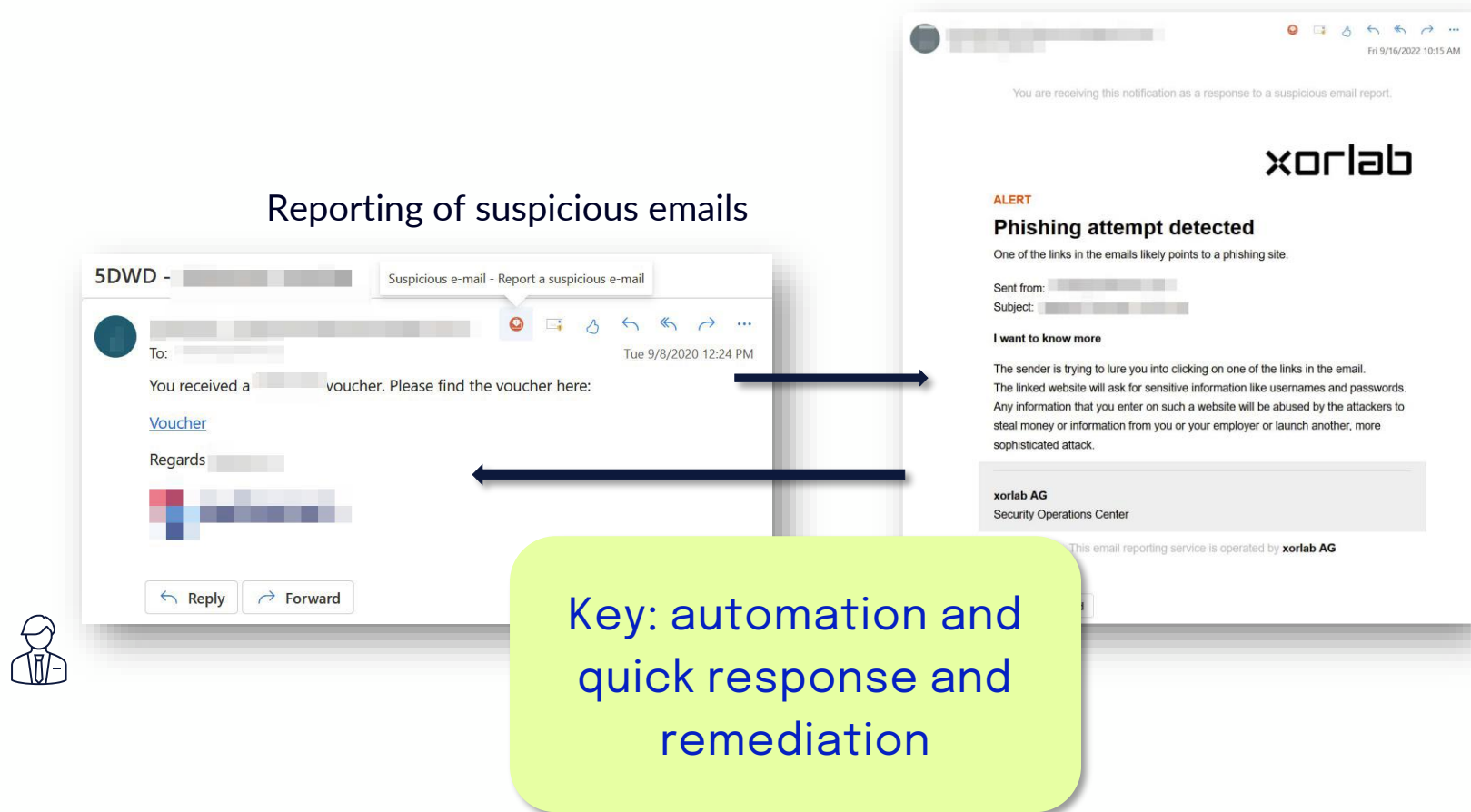
Abuse Mailbox Automation

Automatically handle up to 90% of internally reported suspicious email, ensuring that only critical alerts rise to the surface.

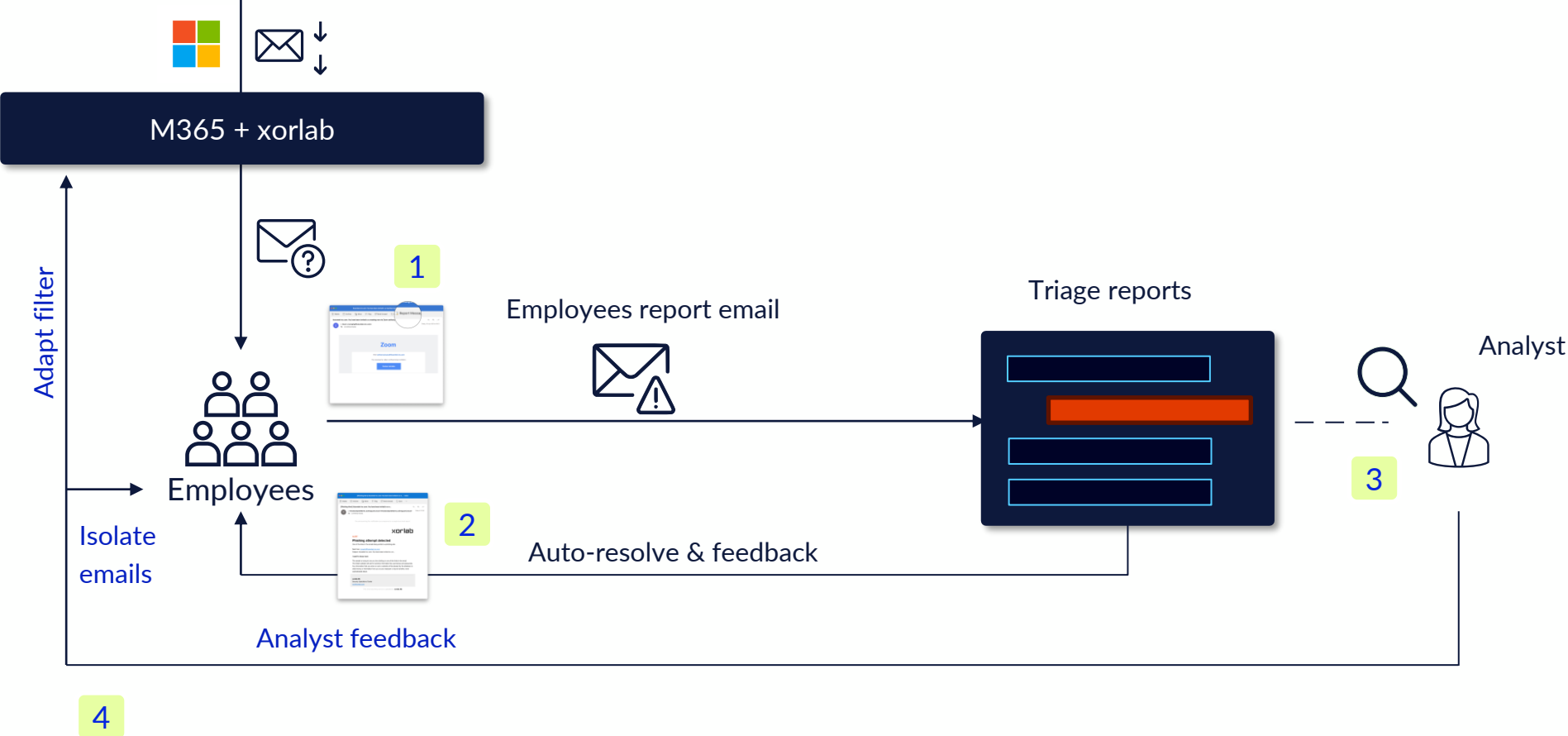
- Collect abuse reports
- Automatically analyze, classify, and triage
- Manage user feedback



Abuse Mailbox Automation



Ideal email security setup



Warn the user: last line of defense

CAUTION: This e-mail originated from outside the organisation. Do not click on links or open attachments unless you recognise the sender and know the content is safe.

Be aware: This is an external email.



Contextual banners

Alert

New external sender and organization

The sender including its organization is not known to us. If you have not expected this message please ignore or report it.



Warning

New external sender

The external sender is not known to us but the organization is. If you have not expected this message please ignore or report it.



Info

Weak relationship with external sender

Be cautious with new relationships in new communication channels. When in doubt, please report the message.



More examples

- Invoice from never seen before organization
- Invoice from known organization
- Graymail
- Potential Phishing, BEC, Spam
- Dangerous file types
- **Additional layer of defense against BEC and Fraud!**

Goal: no banners with most legitimate emails!



Take home messages

- Email-based threats are still the costliest initial attack vectors
 - Zero-hour Phishing and BEC require a new approach
- Users and analysts should also be empowered with contextual banners, a modern self-service quarantine, the possibility to report every email and a platform that allows automation of feedbacks
- M365 is ideally complemented with a specialized add-on that closes these gaps
 - The xorlab Security Platform provides exactly such an add-on



