xorlab

AVANTEC
Competence. Security. Trust.

E-Mail Security Add-on

BEC und 0-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."

Cost and frequency of a data breach by initial attack vector

Figure 10. Measured in USD millions

IBM **Security**

Cost of a Data Breach Report 2023

IBM

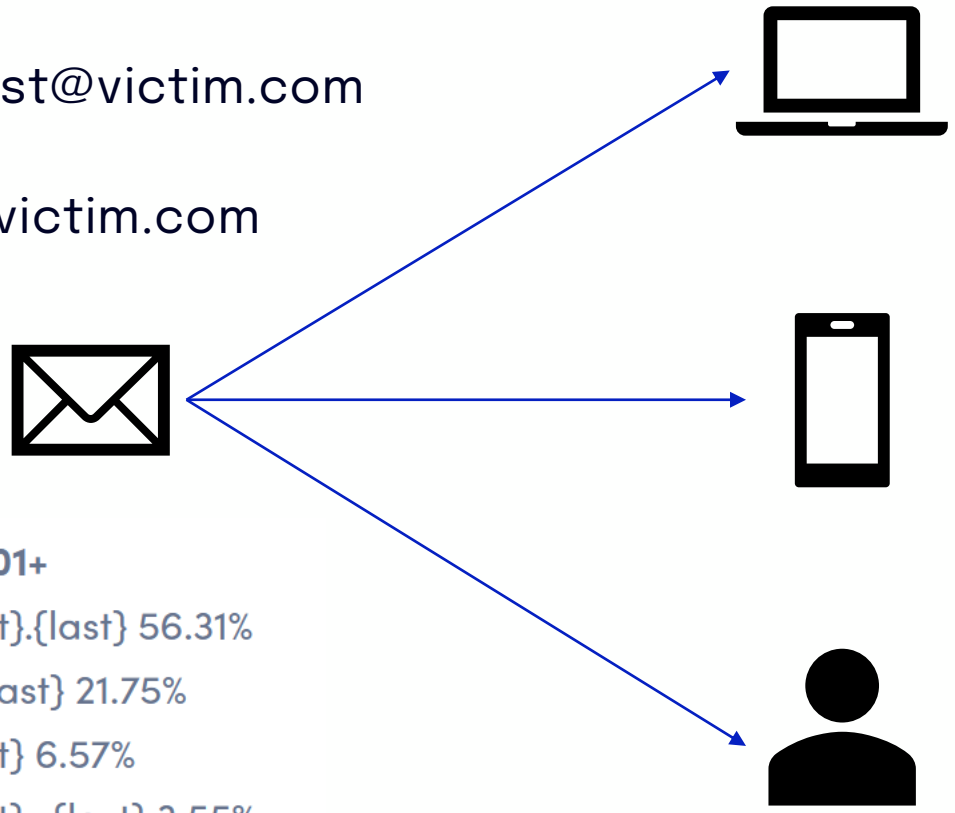
Have you faced one?

Source: Barracuda Email Security Trends 2023

Why is email so interesting?

first.last@victim.com

?@victim.com



10001+

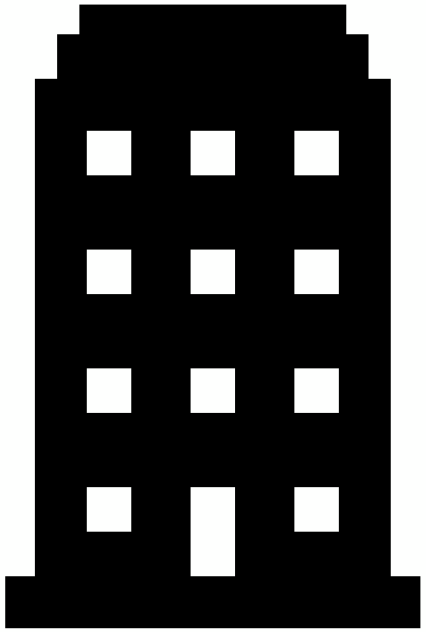
{first}.{last} 56.31%

{f}{last} 21.75%

{first} 6.57%

{first}_{last} 3.55%

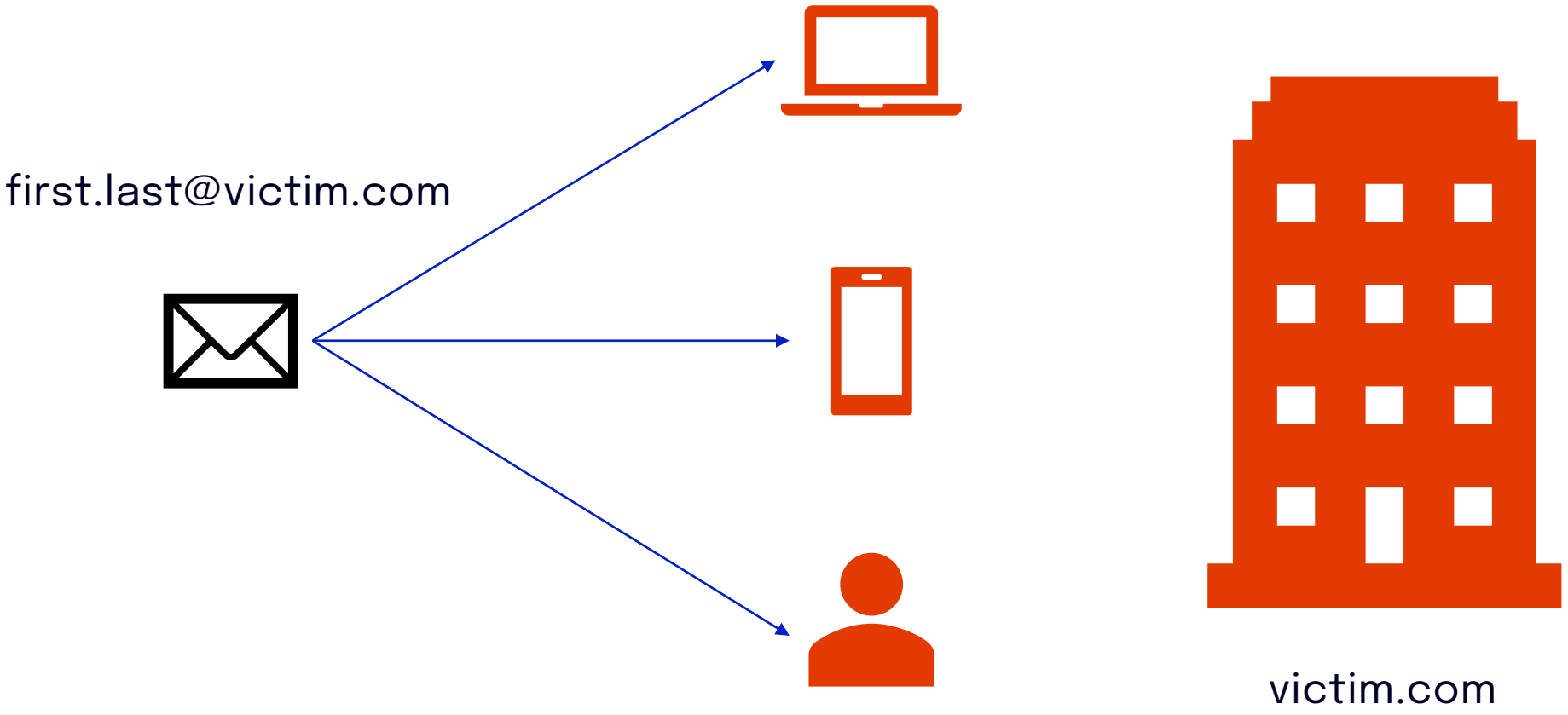
{first}{last} 3.4%



victim.com

https://www.interseller.io/blog/2019/02/04/top-email-address-patterns-by-company-size/

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.

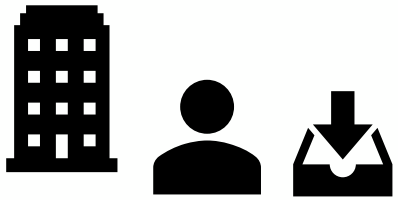
Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC attacks are crafted to appeal to specific individuals, and can be even harder to detect.

National Cyber Security Centre
a part of GCHQ

https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf

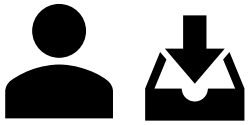
BEC/EAC/Thread Hijacking

Partner / known organization or person



alice@partner.com

Unknown organization or person



john@unknown.com

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

Unknown organization or person

john@unknown.com

Email Account Compromise

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

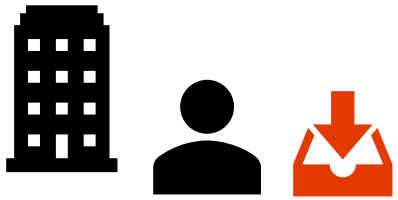
bob@victim.com

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

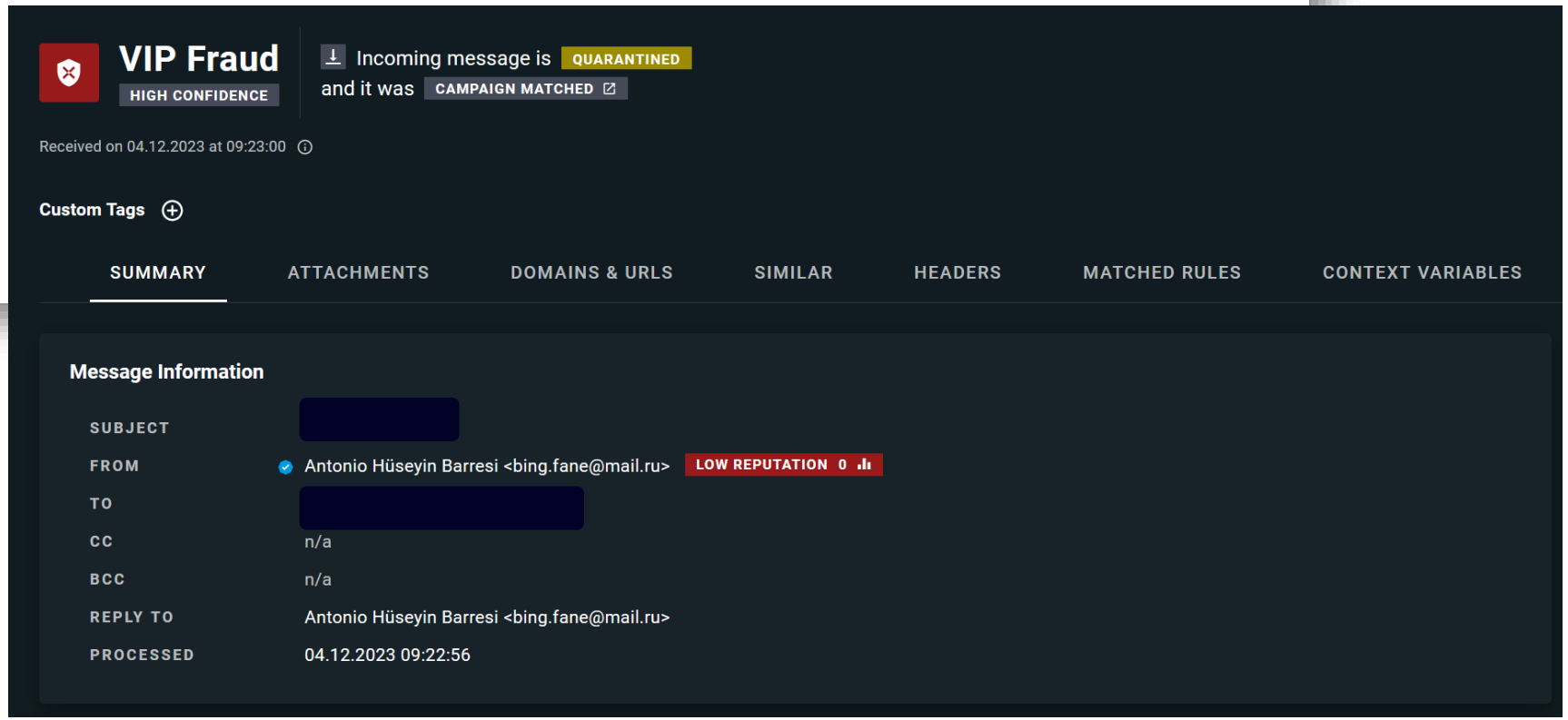
Hello [redacted]

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



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 ?

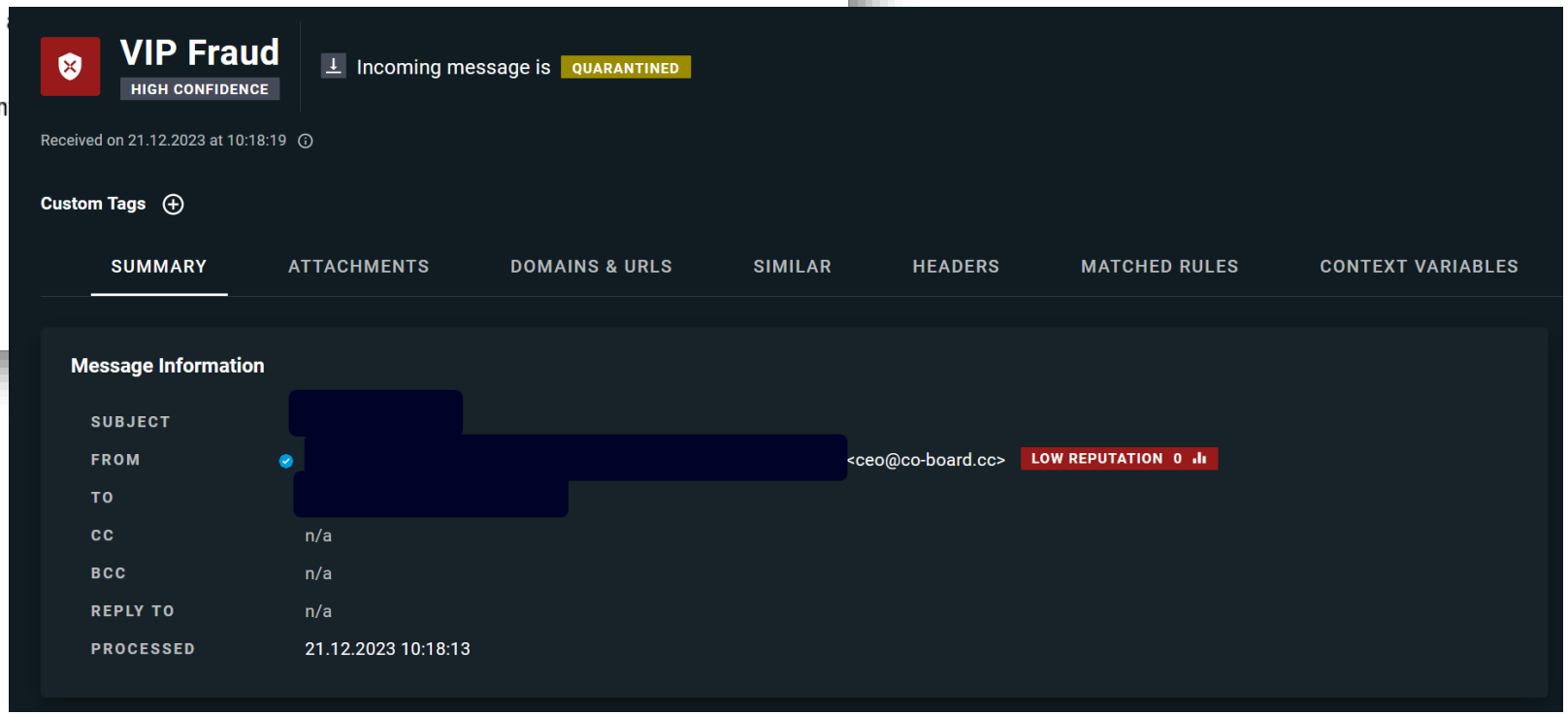
If he has not done it yet, contact him immediately on my behalf, **from your private e-mail** at the following address:
[redacted]
The file reference [redacted] must be specified in your e-mail
what we are expecting from you.

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

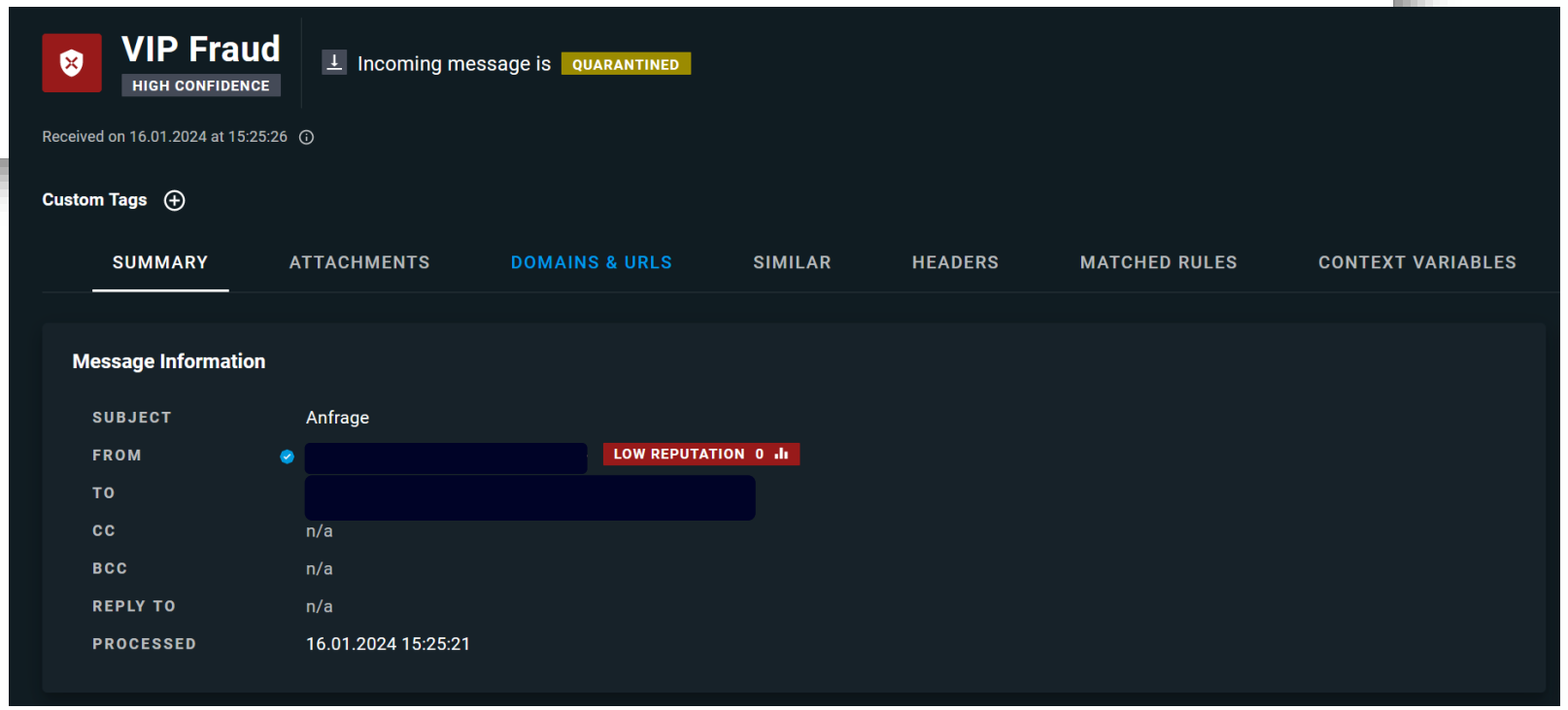


BEC/VIP Fraud

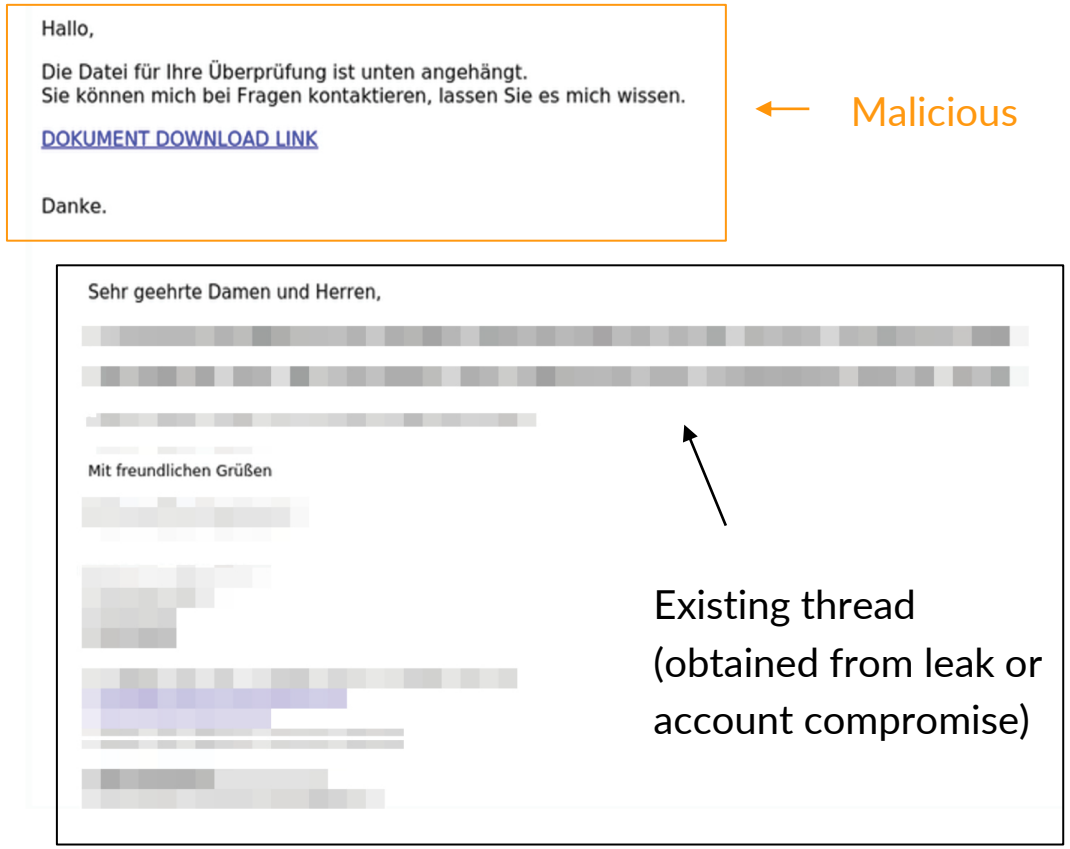
Liebe [redacted]

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?

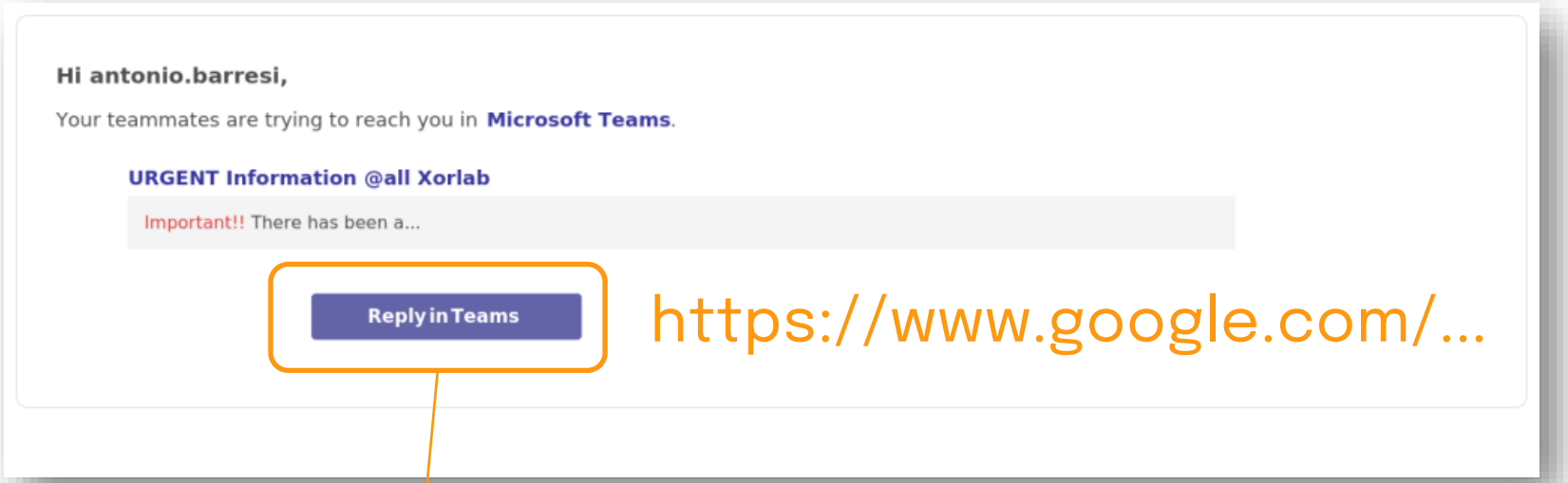
Mit freundlichen Grüße,
[redacted]



Thread Hijacking

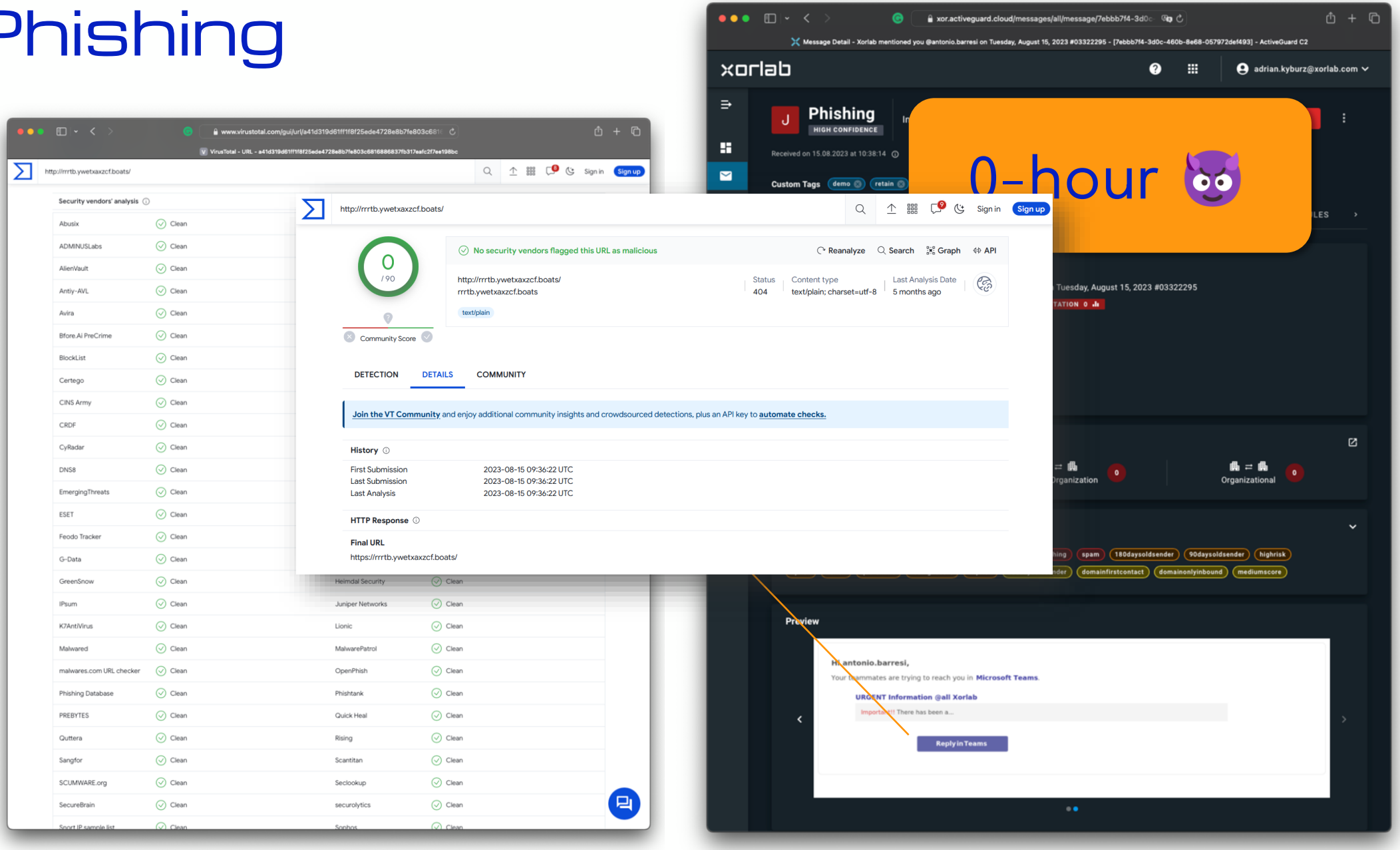


Phishing



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


0-hour
xorlab
Phishing
HIGH CONFIDENCE
Custom Tags
demo
retain
adrian.kyburz@xorlab.com
http://rrrtb.ywetxaxzcf.boats/
Sign in
Sign up
Security vendors' analysis
No security vendors flagged this URL as malicious
Reanalyze
Search
Graph
API
0
/ 90
Community Score
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.ywetxaxzcf.boats/
Preview
Hi antonio.barresi,
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

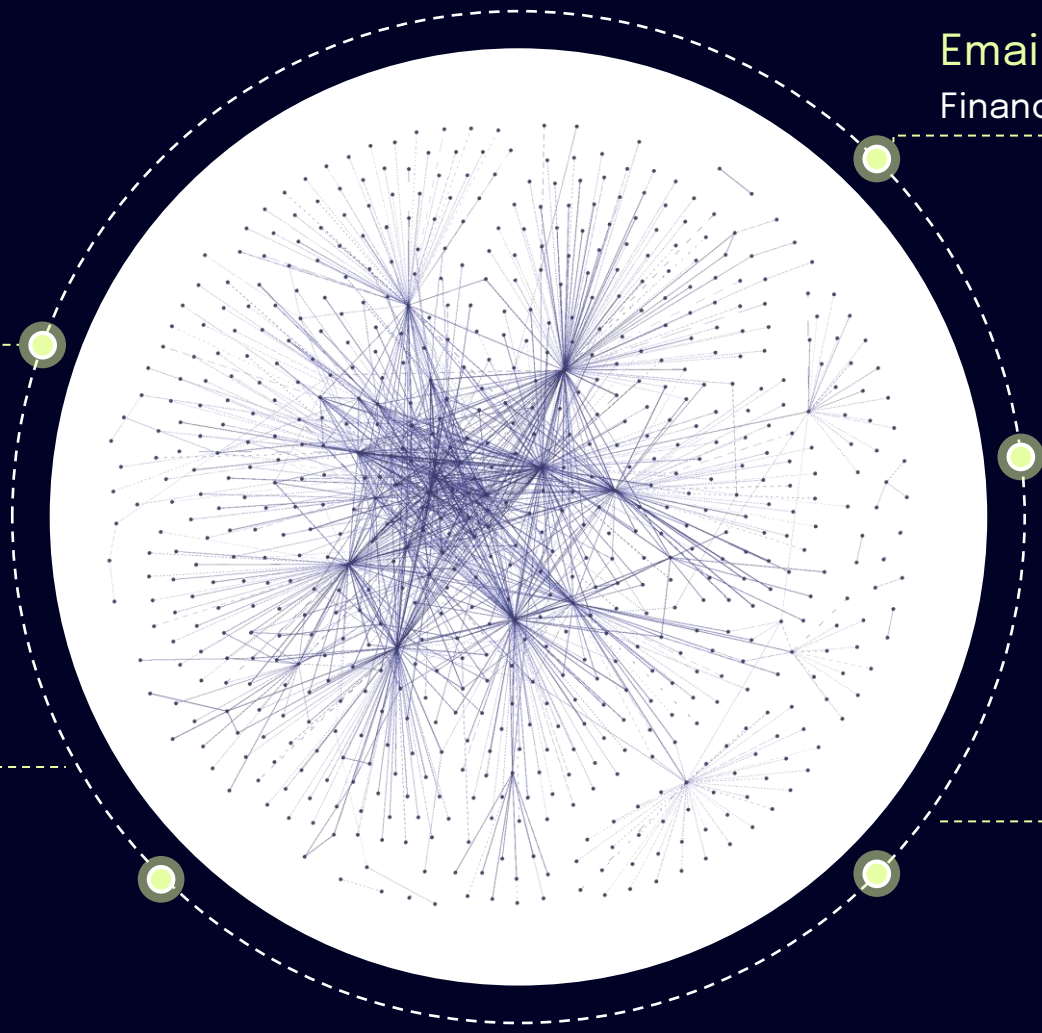
Phishing prevented	12'461
- Zero-hour Phishing prevented	10'147
- Known Phishing prevented	2'314

81.43%

were zero-hour

Our approach as add-on for M365

Context-intelligence



Email content topics
Financial transactions | password reset | etc.

Relationships
Vendors | Customers | etc.

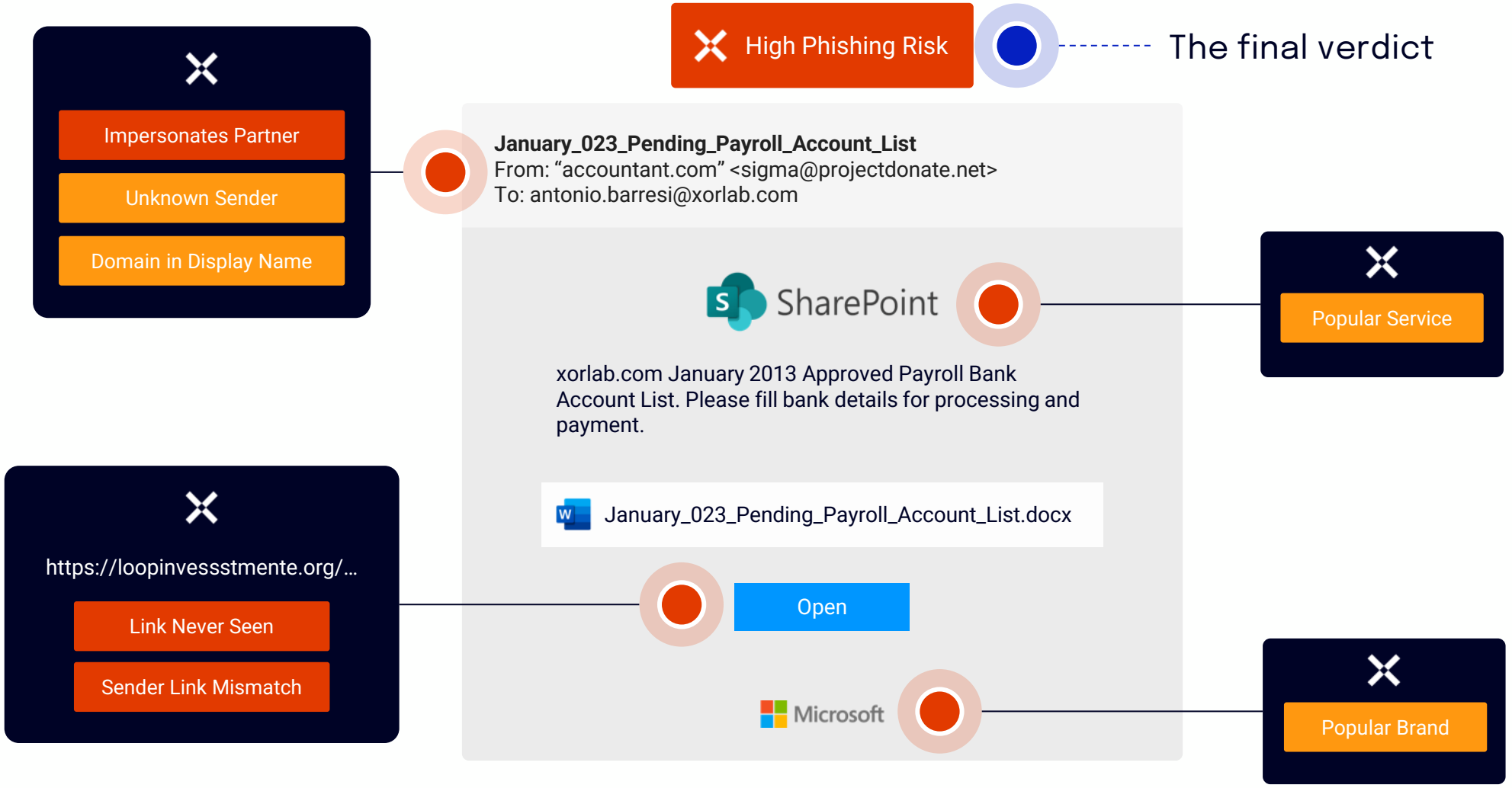
Sentiment
Urgency
| authority
| etc.

File types & attributes
Macros & active content |
encrypted archives | etc.

Links & domains
Cloud services | shadow IT | etc.

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

Stop 0-hour phishing and BEC



Note: This is a simplified illustration. In reality, xorlab collects hundreds of signals per email and matches them against the context of the organization.

xorlab Security Platform | Overview

2 Security modules

Adaptive policies

“Make sense” of data

Context intelligence

Integration options

Solution:

Inbound Email Security

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

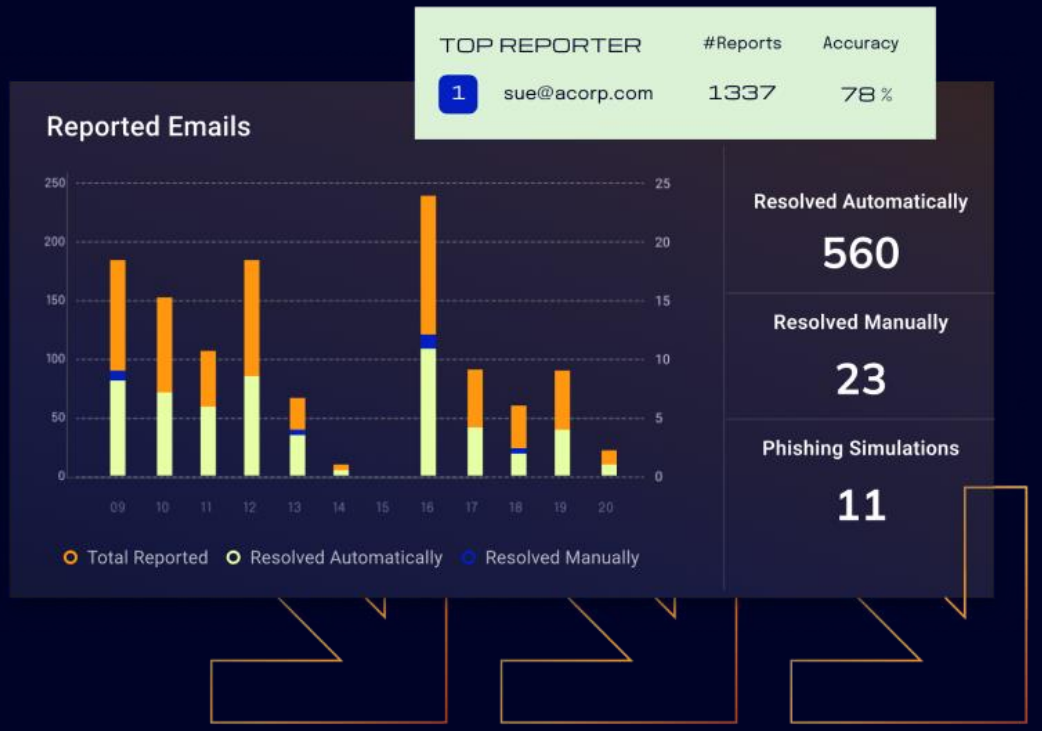
- Detect 2-4x more threats than traditional solutions and prevent 0-hour phishing and BEC attacks
- Minimize manual work with adaptive security policies
- Reduce operational efforts with an audited self-service portal

Solution:

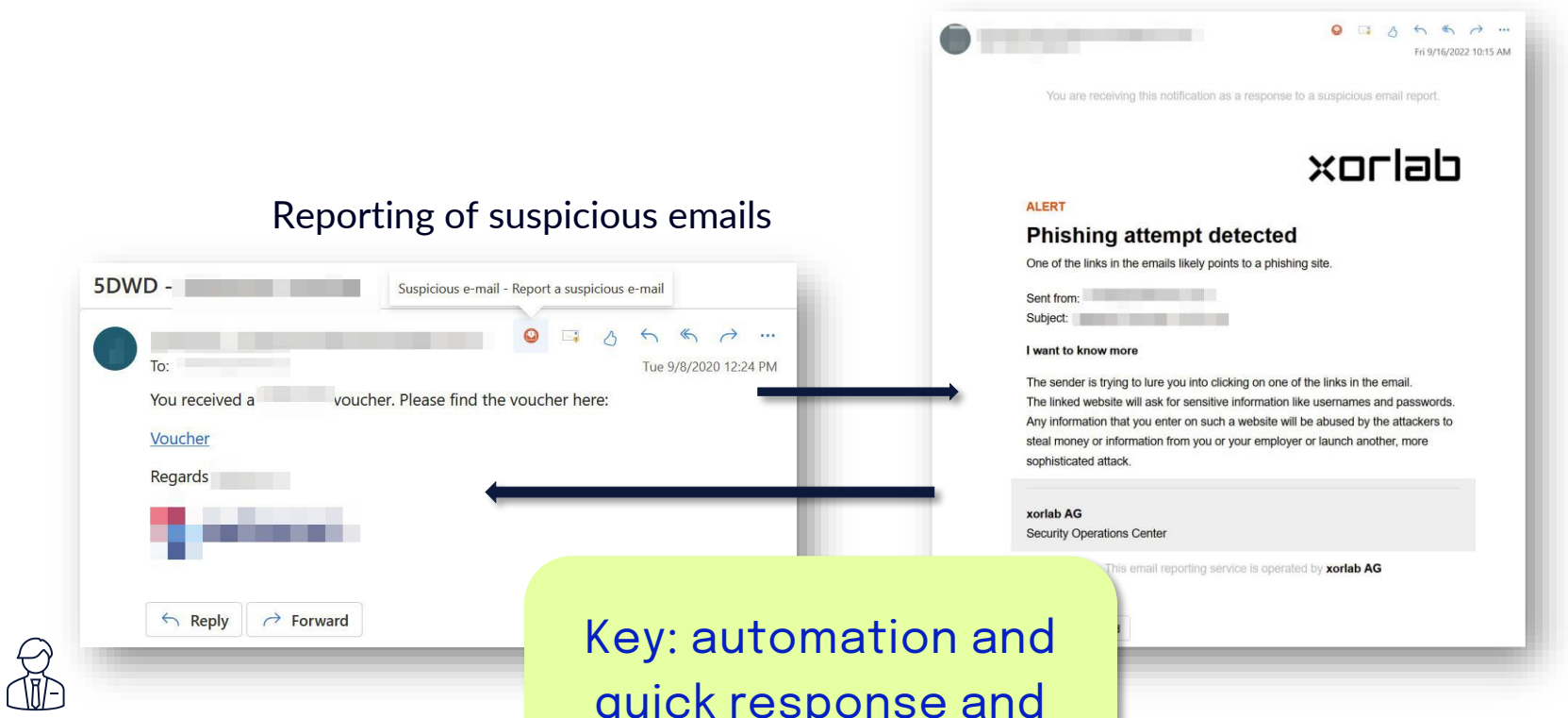
Abuse Mailbox Automation

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

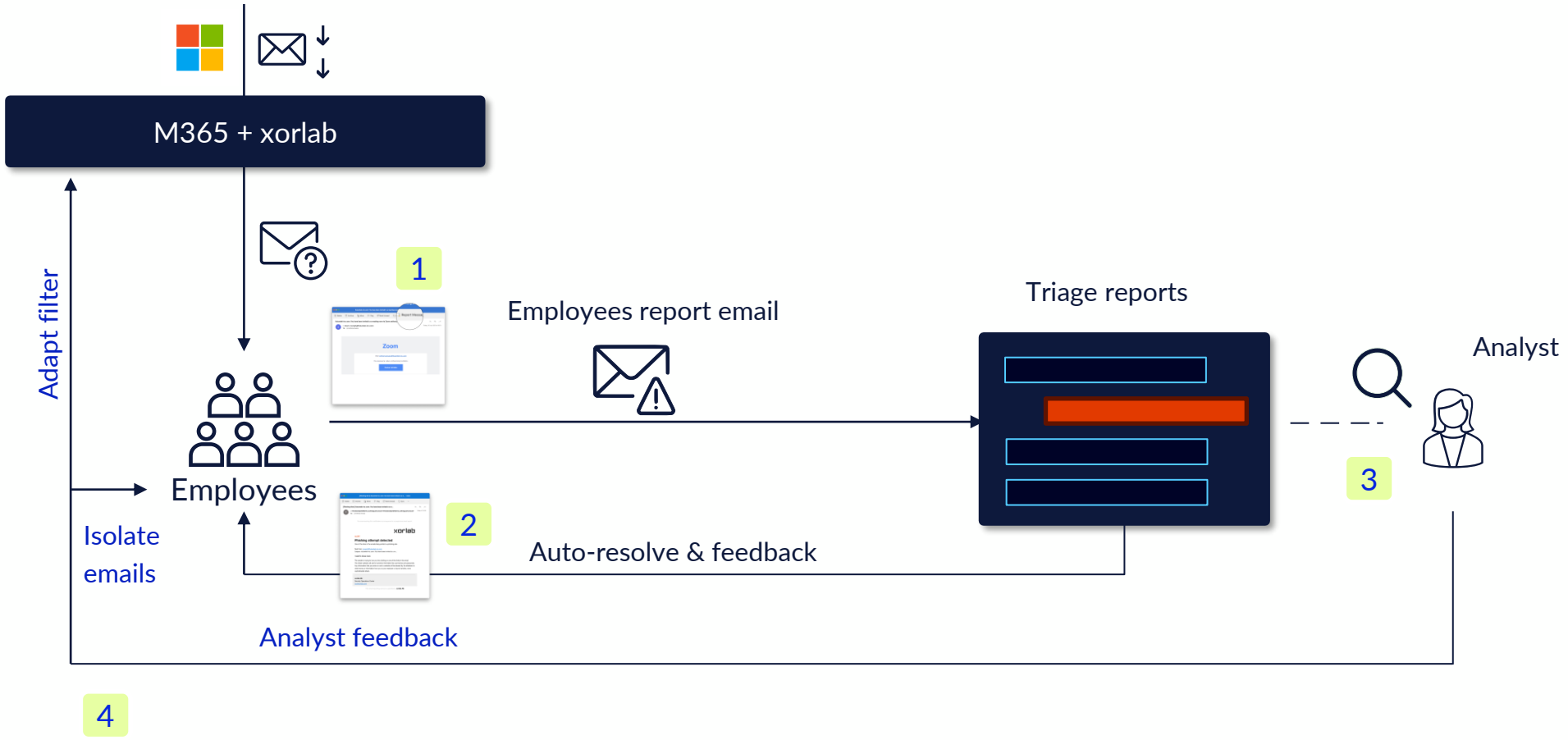
- Collect abuse reports
- Automatically analyze, classify, and triage
- Manage user feedback



Abuse Mailbox Automation



Ideal email security setup



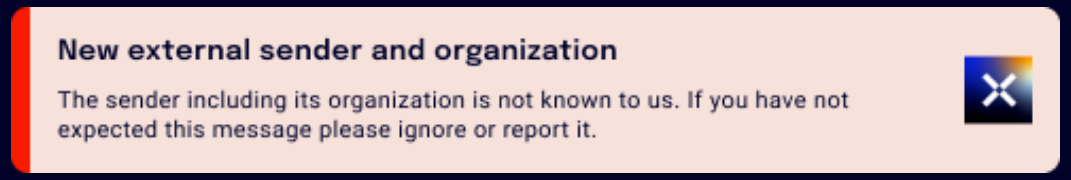
Warn the user: last line of defense

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.

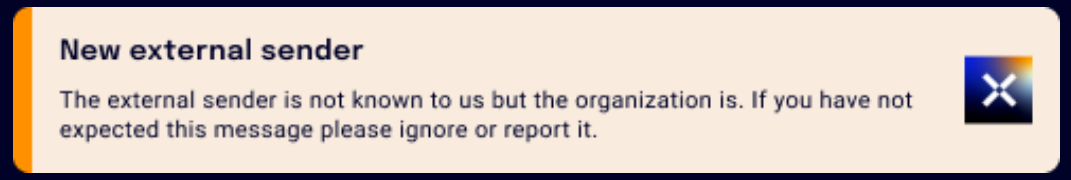
Be aware: This is an external email.

Contextual banners

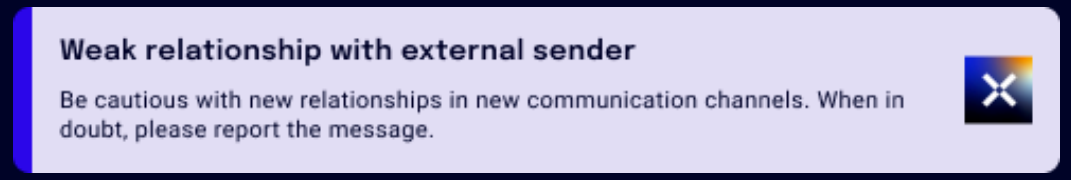
Alert



Warning



Info



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