TESSIAN

SPEAR PHISHING THREAT LANDSCAPE 2021

Why Organizations Need New Methods to Combat New Tricks

Over a 12-month period, Tessian detected nearly 2 million malicious emails that slipped past legacy phishing solutions. Learn more about bad actors' tactics to understand the risk and how to combat it.

TESSIAN

SPEAR PHISHING THREAT LANDSCAPE 2021

JUMP TO PAGE 12 ↗

Microsoft

was the most frequently impersonated brand via Display Name Impersonation

JUMP TO PAGE 5 ↗

2,000,000

emails – which slipped past customers' existing tools (like SEGs) – were flagged as malicious between July 2020 and July 2021

49

malicious emails are received per employee, per year in the retail industry

JUMP TO PAGE 16 ↗

2PM-6PM

is when the most malicious emails land in inboxes.

JUMP TO PAGE 24 ↗

76%

of malicious emails *didn't* contain an attachment

JUMP TO PAGE 21 ↗

14

malicious emails are received per employee, per year

JUMP TO PAGE 16 ↗

JUMP TO PAGE 8 ↗

31%

of the top 30 domains flagged for external account takeover (ATO) came from Legal and Professional Services

JUMP TO PAGE 9 ↗

45%

of employees say they've clicked on a phishing email because they were distracted

JUMP TO PAGE 22 ↗

PDFs

were the #1 file extension seen in malicious emails

Phishing – in its many varieties – is the threat most security leaders are concerned about.

Why?

Because attacks are frequent, hard-to-spot, time-consuming to investigate, and expensive to recover from. And most of the phishing solutions out there today just aren't effective enough.

Native tools do a good job protecting users against bulk phishing attacks and spam, but can't detect never-before-seen attacks or sophisticated spear phishing and social engineering attacks. Phishing awareness programs help, but still leave people as the last line of defense and – as we all know –

`to err is human.`

That's why, despite cybersecurity spending being at an all-time high of $150 billion, threats continue to land in employees' inboxes, and, year-on-year, account takeover (ATO) and social engineering remain top threats.

To help you quantify the risk, we analyzed nearly **two million emails flagged by Tessian Defender as malicious** to identify the **what, how, who, why, and when** of today's spear phishing landscape.

JOSH YAVOR
CISO, Tessian

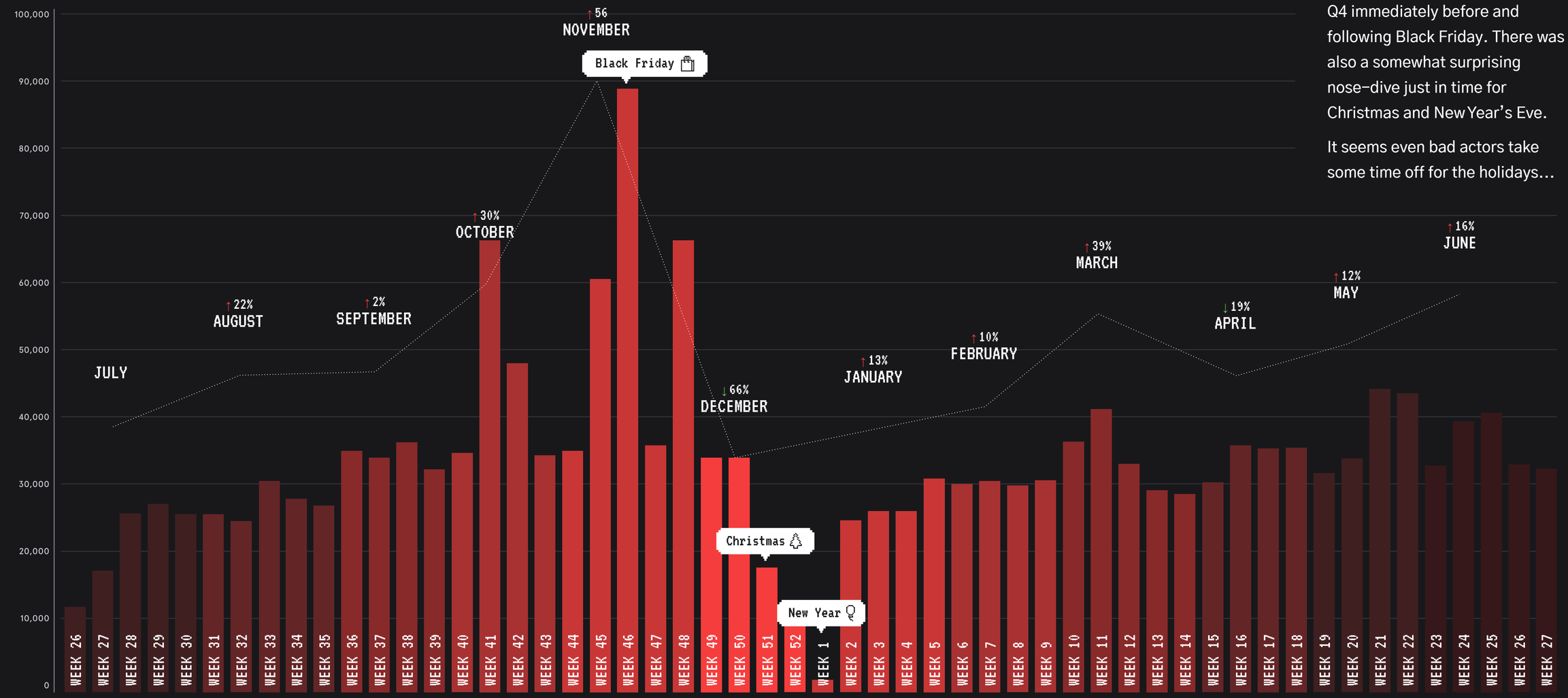
WHAT

Millions of emails are slipping past SEGs and native tools

Between July 2020 and July 2021, Tessian Defender analyzed roughly 4 billion emails, and flagged nearly 2 million as malicious.

In 10 out of 12 months, we saw an increase in the number of attacks, with the biggest spike in Q4 immediately before and following Black Friday. There was also a somewhat surprising nose-dive just in time for Christmas and New Year's Eve.

It seems even bad actors take some time off for the holidays...



But still, 2 million emails **slipped right past customers' SEGs and native tools,** leaving employees as the last line of defense against bad actors who make a sport out of staying a step ahead.

Even with training, it's not fair to expect employees to spot *every* malicious email that lands in their inbox. And what are the consequences of just one honest mistake?

Learn more about the pros and cons of phishing awareness training →

Why can't legacy solutions prevent today's phishing attacks?

We know that security leaders don't expect to be able to reduce the number of malicious emails landing in their employees' mailboxes to zero. But 2 million emails slipping past SEGs and native tools a year? That's a lot.

It begs the question:
Why is this happening so frequently?

Why do threats slip past SEGs?

The backbone of a SEG is traditional email security approaches – static rules, signature based detection, library of known threats, etc. SEGs lack the cutting-edge technology needed to prevent some of today's biggest threats.

Namely, targeted phishing attacks.

They can't detect advanced impersonation, account takeover (ATO), third-party supply chain risk, or wire fraud.

Worse still, SEGs don't address other entry points like Microsoft SharePoint, OneDrive, and ShareFile, which are some of the most hacked cloud tools. It's no wonder Tessian detected so many malicious emails from these sources.

Flip to page 12 to learn more about the most impersonated brands

What about Microsoft O365?

Microsoft O365's native security controls *do* protect users against bulk phishing scams, spam, malware, and domain spoofing. And these tools are great when it comes to stopping broad-based, high-volume, low-effort attacks.

They offer a baseline protection.

But organizations need more than baseline protection as attackers use automation to make small, random modifications to existing malware signatures and use transformation techniques to bypass these native O365 security tools. Unsuspecting – and often untrained – users fall prey to socially engineered attacks that would be hard for even a security expert to spot.

...And training?

Phishing awareness training is an essential part of any cybersecurity strategy. But most security leaders would agree it's expensive, ineffective in the long-term, and that it's difficult to engage with employees.

The bottom line is: People will make mistakes, with or without training.

Want to skip straight to the solution? Jump to page 25 →

HOW

Don’t think you’d be fooled? Think again.

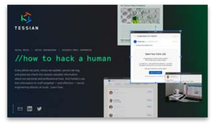
Spear phishing attacks are more sophisticated than traditional “spray-and-pray” phishing attacks and rely on impersonation, a sense of urgency, and trust. It’s all about the art of persuasion. Bad actors will:

- _Research their target using OSINT
- _Use language to pressure the target to act first
- _Pretend to be a trusted person or brand

Let’s take a closer look at each of these.

How do hackers leverage OSINT in phishing attacks?

Between social media, OOO messages, and (free) online tools, it’s impossibly easy for bad actors to research their targets. Armed with information about a person’s company, colleagues, and personal life, they’ll be able to craft personalized, convincing, and effective email campaigns to trick them into handing over sensitive information or transferring funds.



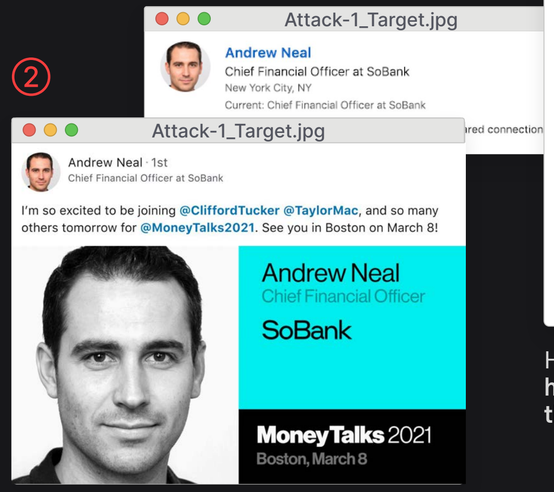
We explore this first step in detail in this report:
How to Hack a Human

TYPE OF ATTACK: CEO/CXO FRAUD
INDUSTRY: FINANCIAL SERVICES
HACKER MOTIVATION: (QUICK) FINANCIAL GAIN

1

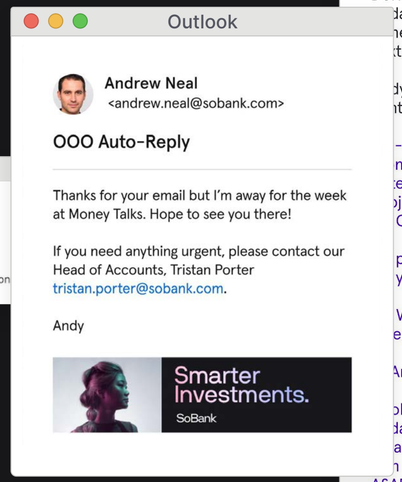
By monitoring news wires, **the hacking group identifies their target:** an asset management firm called SoBank.

2



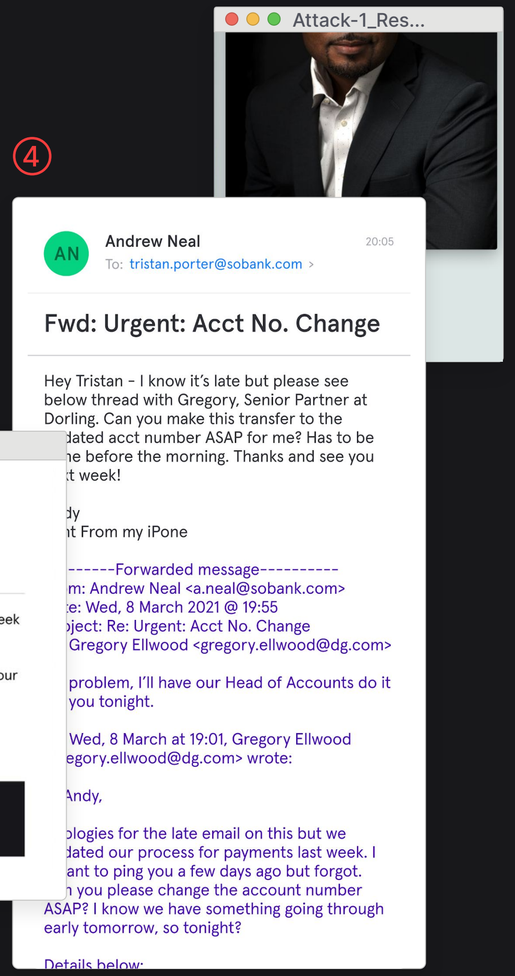
They see that the company’s CFO – Andrew Neal – is **OOO** at a conference.

3



His OOO message offers **helpful information that they use in their attack.**

4



The hacker group sends a **fabricated email chain** that appears to be between Andy and Gregory Ellwood, Senior Partner at Dorling Clayton – SoBank’s advising firm – urging Tristan to make a wire transfer.

Why do hackers like to create a sense of urgency?

The answer to this is simple:

human psychology.

When people are stressed, anxious, or distracted, they're more likely to make mistakes.

Don't believe us?

45%

of employees say they clicked on a phishing email because they were distracted

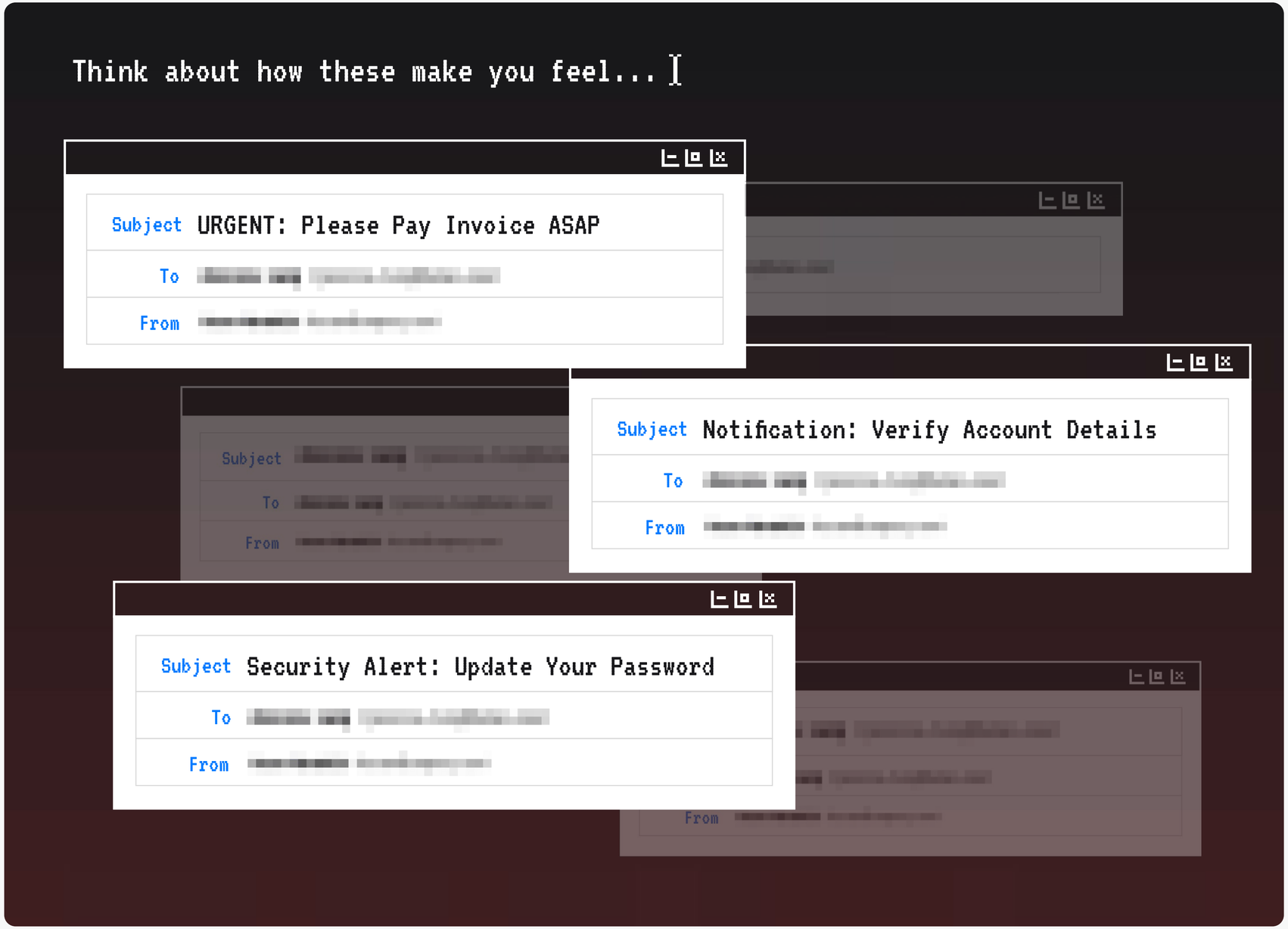
Over half (52%)

say they make more mistakes when they're stressed

1 in 3 (29%)

employees say they clicked a phishing email because they weren't paying attention

Bad actors can create a sense of urgency – and therefore make people stressed, anxious, and distracted – starting in the subject line.



THE KEYWORDS MOST FREQUENTLY USED IN MALICIOUS EMAILS

SUBJECT LINE

invoice
payment data
email new
2021 2020
update contact
security account

BODY COPY

immediately payment
covid-19 today
unsubscribe
$ click here
***confidential
outlook privacy now

Likewise, the body copy of an email will generally motivate the target to act.

Look out for language that suggests there will be a consequence if you don't act quickly.

For example, a hacker may say that if a payment isn't made within 2 hours, you'll lose a customer.

Or, if you don't confirm your email address within 24 hours, your account will be deactivated.

These are both classic examples of social engineering; the stakes appear high, which means the target is more likely to make a hasty decision that could have dire consequences.

How would *you* react?

Check out our research in to the Psychology of Human Error to learn more.

How do hackers impersonate trusted people and brands?

While nearly 60% of the malicious emails seen in Tessian's network relied on "generic" impersonation techniques (freemail impersonation, for example) and Display Name Impersonation, over 30% leveraged more advanced (and difficult to spot) techniques like:

① DOMAIN SPOOF

The attacker sets up an email domain that looks like a legitimate email address, but isn't

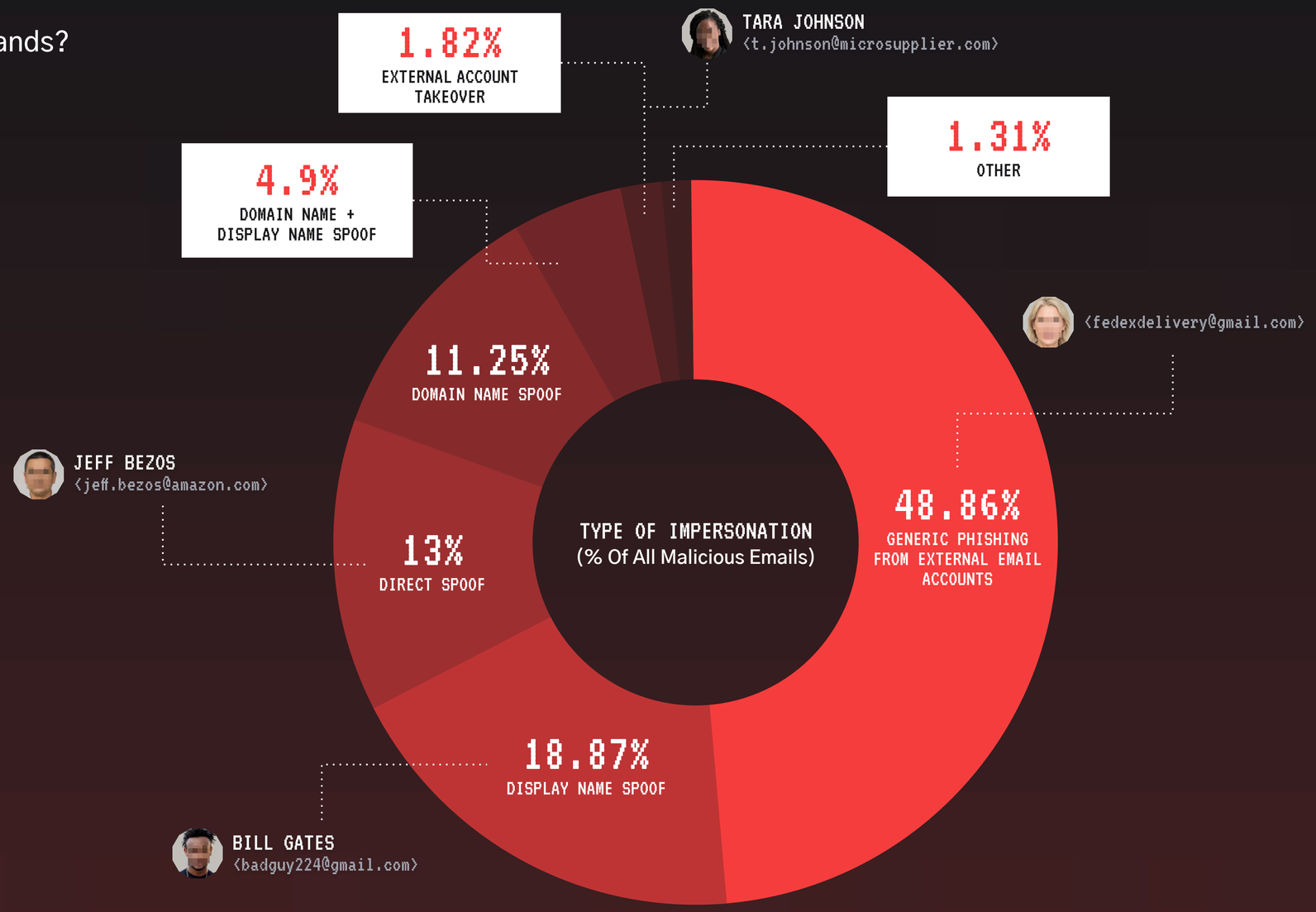
② DIRECT SPOOF

A technical process where the attacker modifies an email's headers so the receiving email client displays a false email address

③ ACCOUNT TAKEOVER

The attacker gains access to another person's account (using hacking or stolen credentials) and uses it to send phishing emails

Email spoofing and account takeover require *some* technical ability, but with display name impersonation and email impersonation, the attacker just needs to secure a domain that looks like it could belong to a legitimate business. Easy-peasy.



TESSIAN

SPEAR PHISHING THREAT LANDSCAPE 2021

MOST IMPERSONATED BRANDS ACROSS ALL INDUSTRIES VIA DISPLAY NAME

1. Microsoft
2. ADP
3. amazon
4. Adobe Sign
5. zoom

Download this list of most impersonated brands in spear phishing attacks to share with employees

EXAMPLES OF DOMAINS FLAGGED FOR IMPERSONATION IN TESSIAN'S NETWORK…

- [redacted]@adp.com.br
- [redacted]@adobesign.com
- [redacted]@account-microsoft365.com
- [redacted]@amazon.online.com
- [redacted]@storage-micro-sharepoint.com

MASTERS OF DISGUISE

MOST IMPERSONATED BRANDS BY INDUSTRY

FINSERV

1. ADP
2. Microsoft
3. Adobe Sign
4. FedEx
5. amazon

LEGAL & PROF. SERVICES

1. Microsoft
2. amazon
3. Virgin media
4. Adobe Sign
5. zoom

TECH

1. codefresh
2. McAfee
3. Microsoft
4. Google
5. DHL

HOW MANY MALICIOUS EMAILS COME FROM FREEMAIL ACCOUNTS?

17% FREEMAIL | 83% OTHER

TOP 5 MOST IMPERSONATED FREEMAIL DOMAINS

1. gmail.com
2. hotmail.com
3. outlook.com
4. icloud.com
5. yahoo.com

SPOTLIGHT

Analysis of an Account Takeover Attack

INDUSTRY: CONSTRUCTION

SIZE: 500 EMPLOYEES

PLATFORM: O365

In March 2021 Tessian Defender flagged an email received by one of our customers from one of their trusted vendors. The vendor had suffered from an account takeover when an attacker used compromised credentials to login to the mailbox of one of their employees and send out malicious emails.

Learn more about vendor email compromise →

TARGETS IDENTIFIED

With access to the vendor, the attacker was able to identify a list of 6 high-ranking employees – including the CEO and their PA – who were part of an organization the employee had regular correspondence with.

ATTACK DEPLOYED

The attacker sent an email containing a malicious link to their targeted list of recipients from the compromised account.

to me

Important: Late Invoice

Hi Ario,

Last month's payment is late. Please click here to download the invoice and make the payment ASAP.

Thank you

THREAT DETECTED

While the targeted firm had another major phishing detection and response platform in place, the account takeover attack was *only* flagged by Defender.

How? Deep content inspection revealed unusual sender characteristics, including the sender's geophysical location.

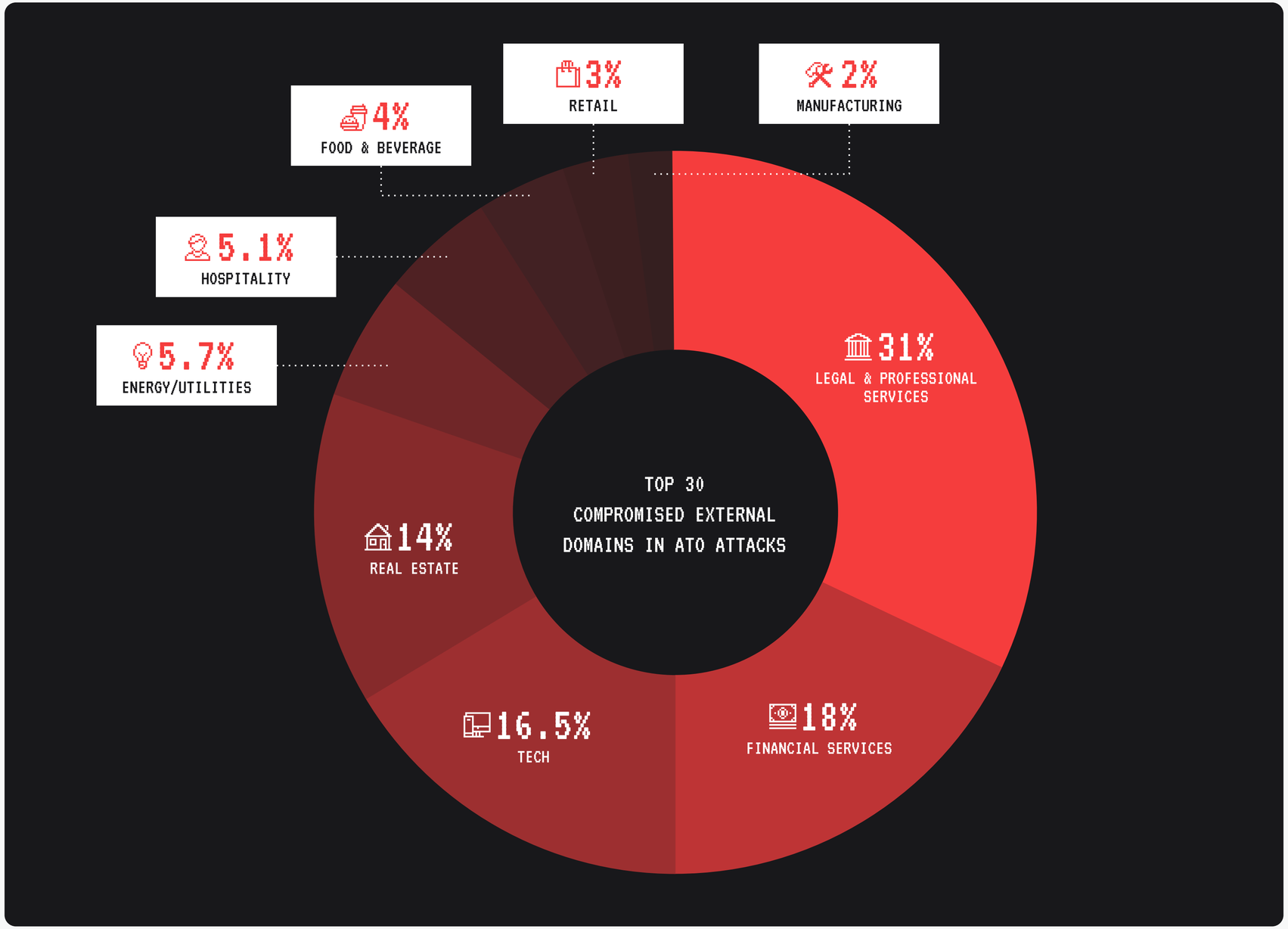
TESSIAN WARNING

Thanks to Tessian Defender's warning message, the recipients of this email marked it as malicious. The firm's security team contacted the real owner of the sending email address by phone to verify the legitimacy of the email and inform them their account had been compromised.

TESSIAN WARNING

Take care, there is something unusual about this email, please take care as it could be malicious.

Report as Malicious and Delete | Mark as Safe | I'm Not Sure



In the example on the previous page, the compromised party was a trade association. But, according to Tessian platform data, email accounts **across several industries** were compromised in ATO attacks between July 2020 and July 2021.

That said, there was a clear winner. We analyzed the top 30 domains compromised in ATO attacks, and over 30% were from companies operating in legal and professional services.

Keep this in mind when thinking about your own security posture, and your supply chain risk.

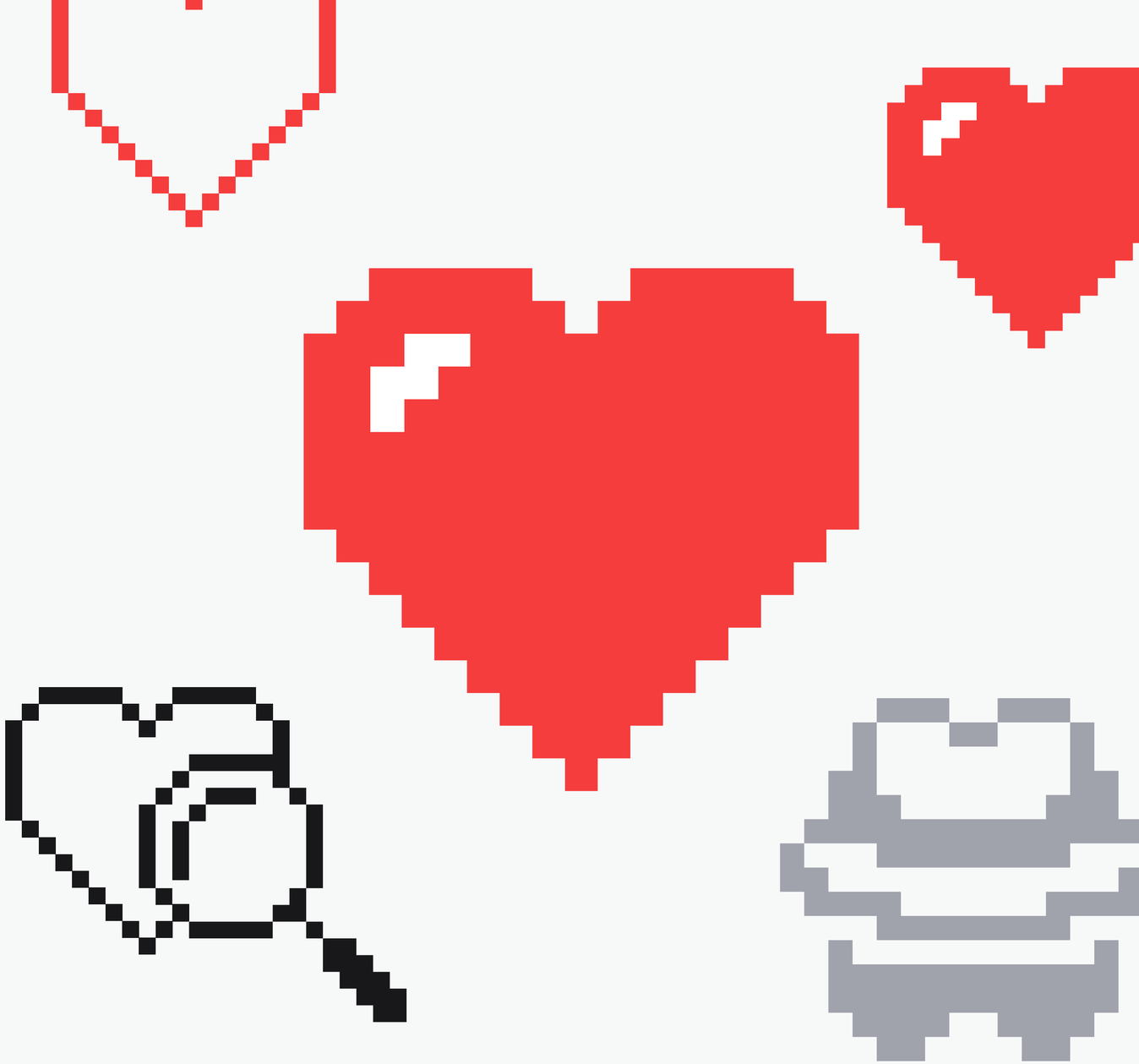
The bottom line:

Whether it's an ATO attack or a domain spoof, today's spear phishing attacks look like the real deal; not like the Nigerian Prince scams of the 1990s. If employees are only on alert for emails from suspicious domains that are riddled with grammatical errors and contain dubious attachments... they'll never spot the phish.

Your SEG won't either.

WHO

Cybercriminals have a type



When it comes to who they target, bad actors cast a wide net, but *do* seem to have an affinity for Retail, Manufacturing, F&B, R&D, and Tech. But still, across all industries, Tessian flagged 14 malicious emails a year, **per employee.**

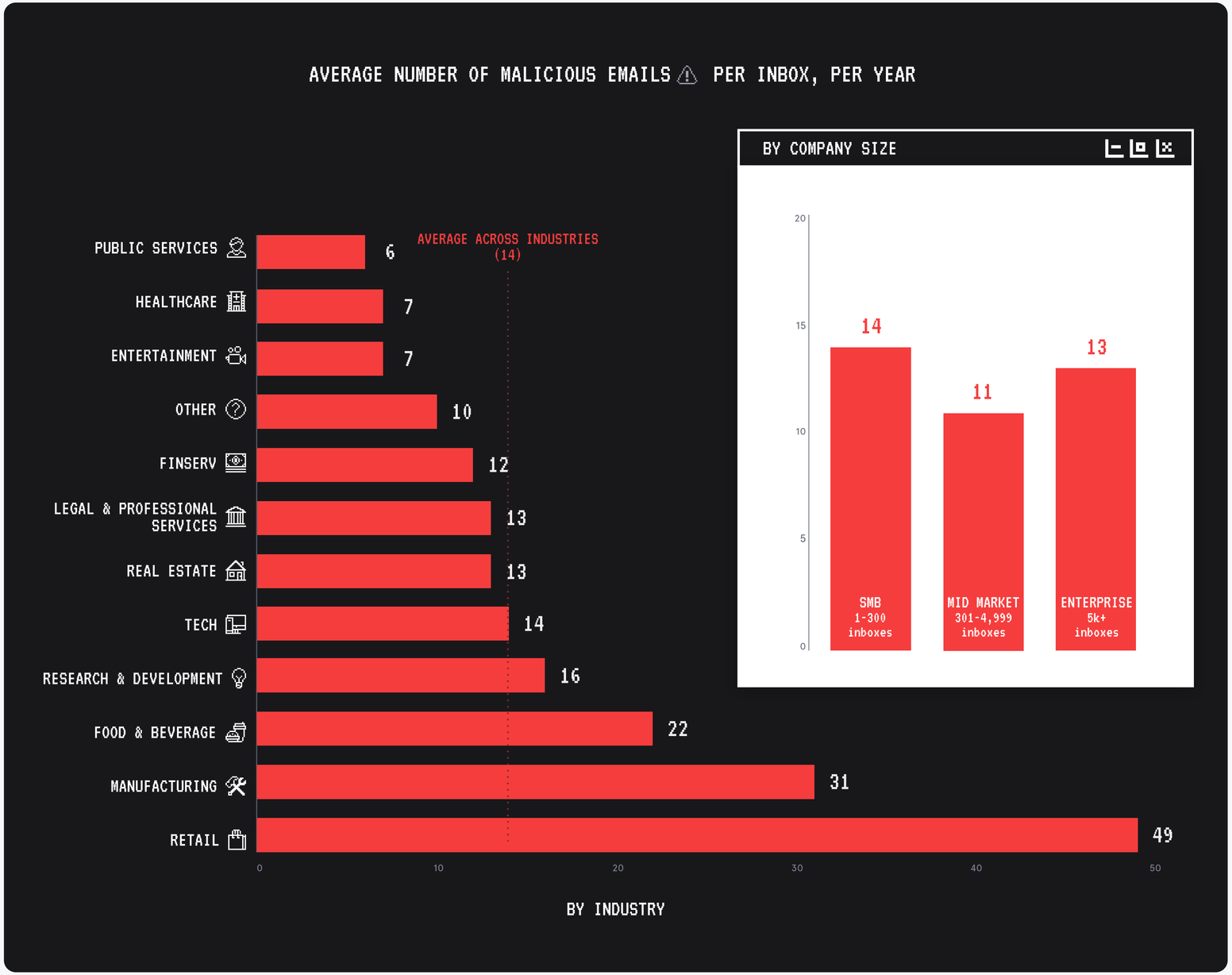
That means that, without Tessian, *each* employee would have to successfully identify 14 carefully crafted emails a year in order to avoid a breach. That's just too much risk.

In terms of company size, bad actors will take whatever they can get.

Wondering why they don't focus exclusively on the "big fish" (i.e. enterprise)? Because smaller companies – who generally have less money to spend on cybersecurity – are often easier to infiltrate. This can be a foothold for lateral movement, especially for companies with large supply chains.

Take the **2020 SolarWinds hack**, for example. After breaching the SolarWinds Orion system (a network management system that helps organizations manage their IT resources), nation-state hacking group **Nobelium** was able to gain access to the networks, systems, and data of thousands of SolarWinds customers, including government departments such as Homeland Security, State, Commerce, and Treasury.

Affected private companies included FireEye, Microsoft, Intel, Cisco, and Deloitte.



Interestingly though, regardless of industry or company size, attacks look just about the same.

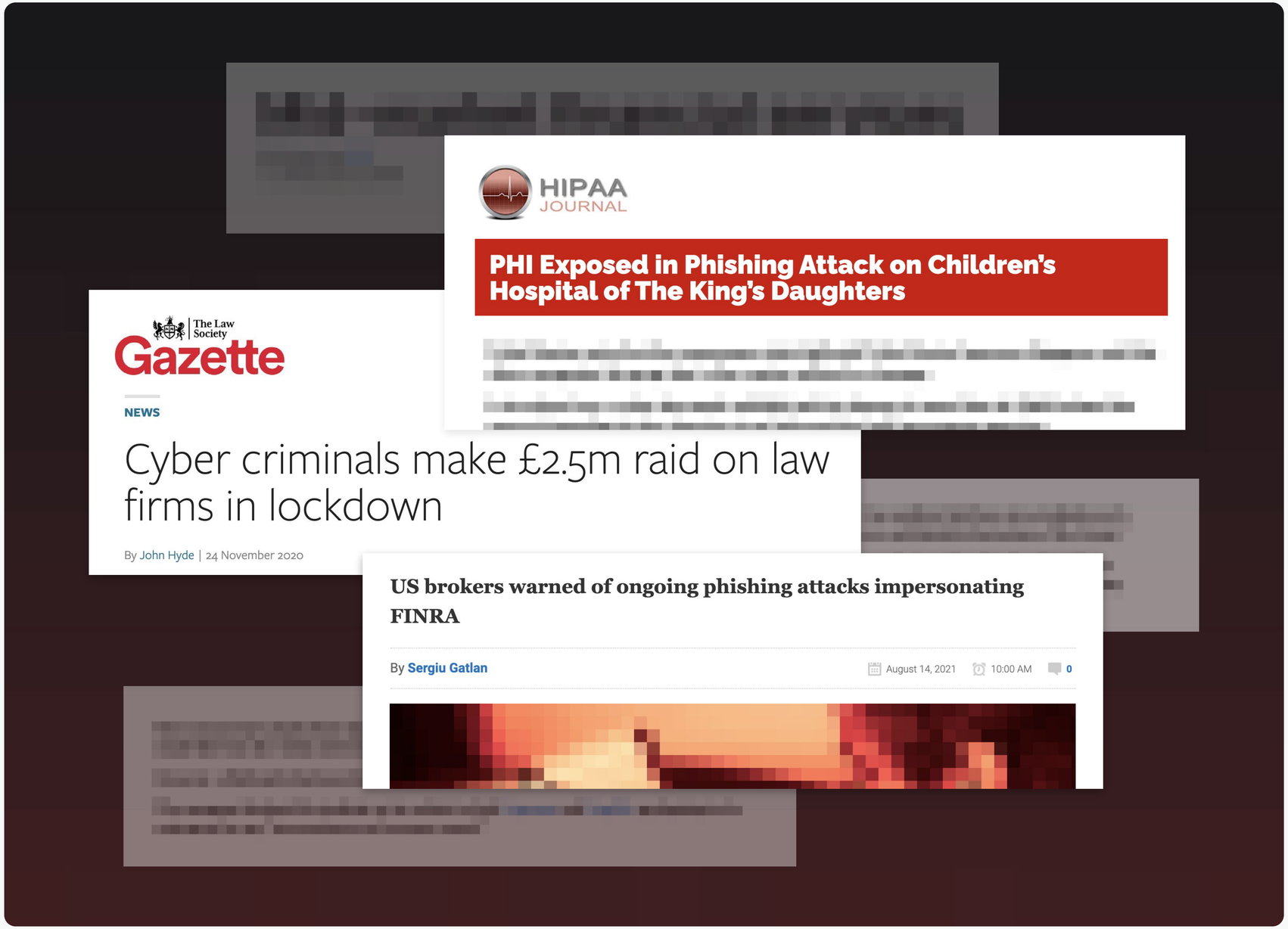
Across the board, display name spoofs are the most commonly used impersonation tactic.

Payloads are more often delivered via URLs than attachments. And keywords related to wire transfers are more frequently seen than keywords related to credentials.

This reinforces just how effective these tactics are, regardless of how much budget an organization has allocated to cybersecurity.

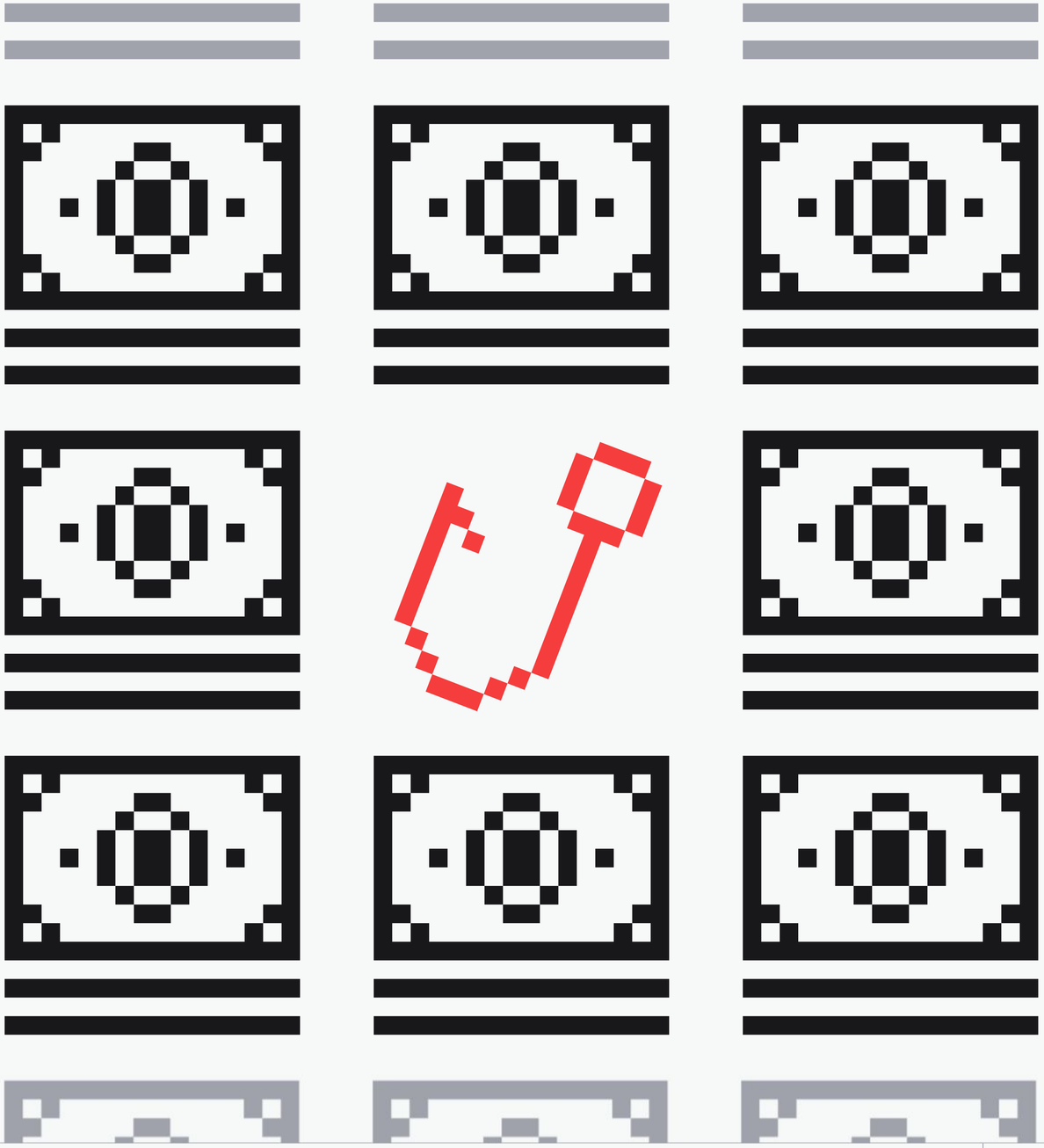
Learn more about how Tessian protects organisations in:

- HEALTHCARE
- FINANCE
- LEGAL



WHY

Phishing is big business for bad guys



It's no secret that bad actors create phishing campaigns with one (or more) of the following end goals in mind:

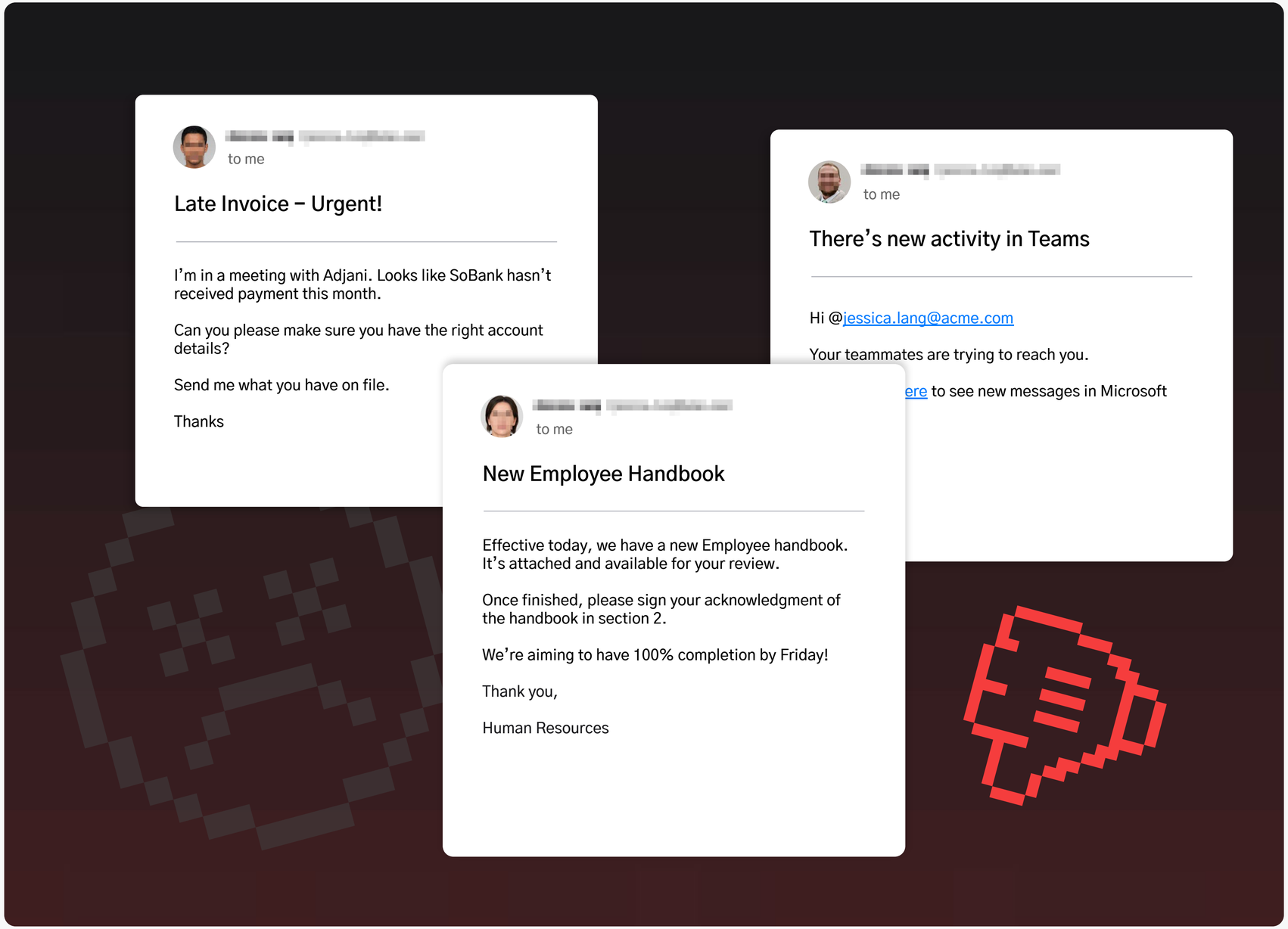
- OBTAINING CREDENTIALS
- INITIATING A WIRE TRANSFER
- INSTALLING MALWARE OR RANSOMWARE

Our payload and keyword analysis corroborate this.

Of course, when we talk about the correlation between payloads and attack goals, there is certainly a gray area, and **we won't claim to know the specific intention of *every* email we've flagged.**

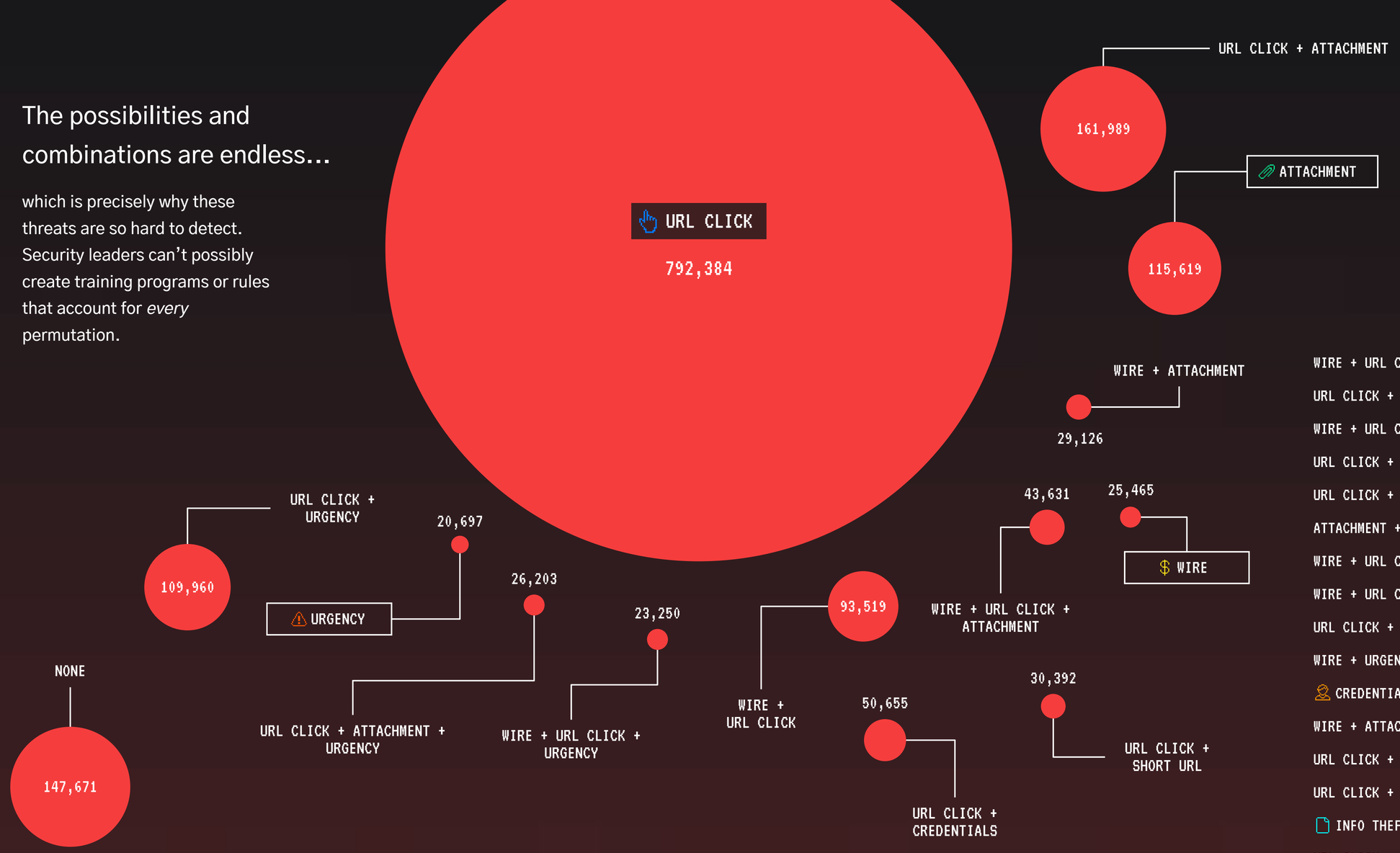
A perfectly safe attachment could instruct you to click on a malicious link, which could automatically deploy malware.

A link could also lead you to a look-a-like site that harvests your credentials, without the word "credentials" ever appearing in the body or subject of the email.



The possibilities and combinations are endless…

which is precisely why these threats are so hard to detect. Security leaders can't possibly create training programs or rules that account for *every* permutation.



WIRE + URL CLICK + INFORMATION THEFT	15155
URL CLICK + CREDENTIALS + URGENCY	14384
WIRE + URL CLICK + ATTACHMENT + URGENCY	9872
URL CLICK + INFORMATION THEFT	9259
URL CLICK + ATTACHMENT + CREDENTIALS	7465
ATTACHMENT + URGENCY	6981
WIRE + URL CLICK + ATTACHMENT + INFO THEFT	6073
WIRE + URL CLICK + INFO THEFT + URGENCY	5006
URL CLICK + ATTACHMENT + SHORT URL	4684
WIRE + URGENCY	4608
CREDENTIALS	4123
WIRE + ATTACHMENT + URGENCY	3770
URL CLICK + SHORT URL + URGENCY	3089
URL CLICK + ATTACHMENT + INFO THEFT	3078
INFO THEFT	2910
URL CLICK + INFO THEFT + URGENCY	2800

NO. OF MALICIOUS EMAILS BY PAYLOAD TYPE AND GOAL

DISCLAIMER:

Most bad emails *don't* contain attachments.

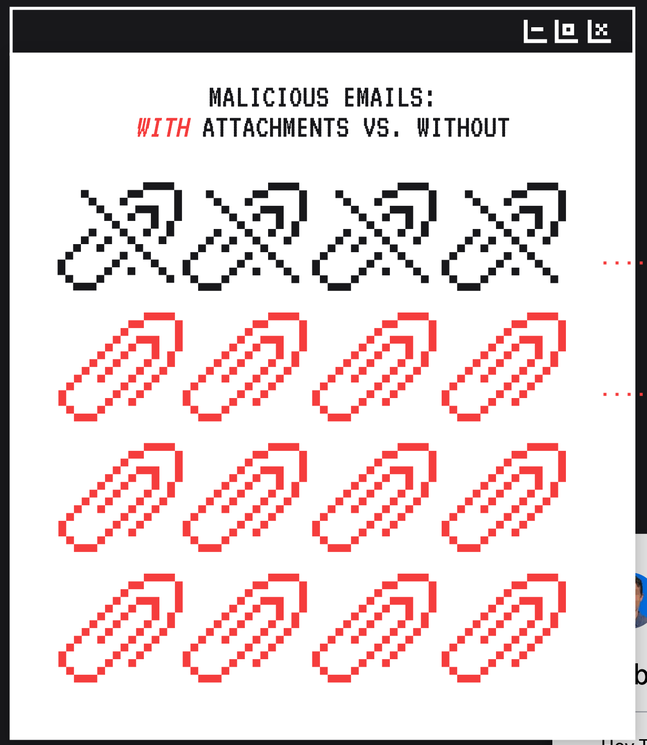
While attachments are listed first in frameworks like MITRE, most bad emails don't actually contain attachments. **That's why it's important to train employees to spot a variety of different malicious payloads, including zero payload attacks.**

Zero payload attacks don't rely on a malicious payloads like attachments or links. The attacker simply persuades the victim to action a request.

Zero payload attacks can be just as devastating as malicious payload attacks, and traditional antivirus and anti-phishing software – which often rely solely on keyword detection and deny/allow lists – struggle to detect them.

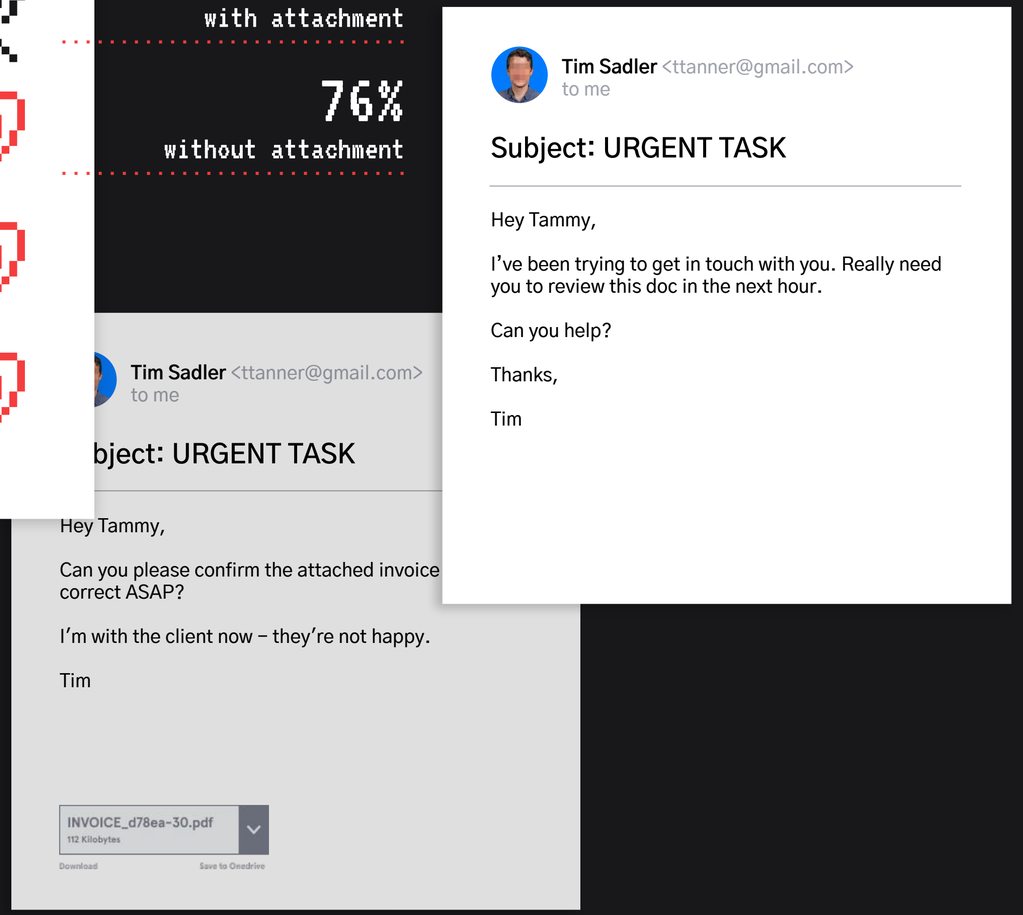
But what about when bad actors *do* leverage attachments?

Flip to the next page to see the most popular attachment extensions



24%
with attachment

76%
without attachment



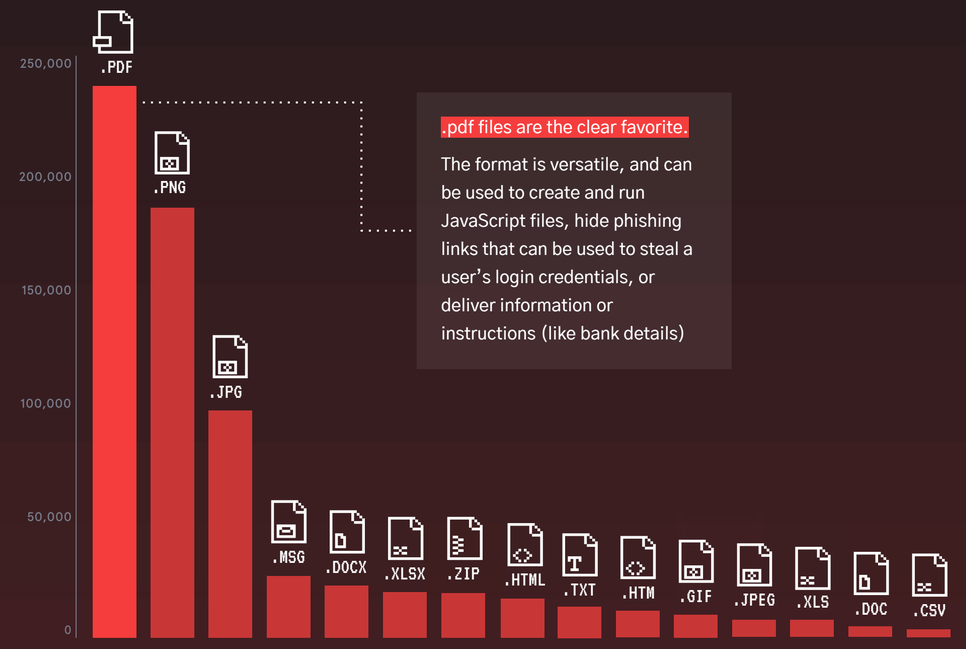
TESSIAN

SPEAR PHISHING THREAT LANDSCAPE 2021

DON'T CLICK THAT!*

While most malicious emails don't actually contain attachments, it's important employees know which file extension types to be most wary of, and how to "test" if an attachment is safe or not.

TOP 15 FILE EXTENSIONS SEEN IN MALICIOUS EMAILS



.pdf files are the clear favorite.

The format is versatile, and can be used to create and run JavaScript files, hide phishing links that can be used to steal a user's login credentials, or deliver information or instructions (like bank details)

* Tessian customers will be alerted when a malicious attachment is detected and can automatically block them

HOW TO IDENTIFY IF AN ATTACHMENT IS SAFE

1. CHECK THE BODY COPY

Even if the sender's email address checks out, you should review the email itself. Is a "customer" addressing by your full name instead of your nickname as he or she normally would? Is a shipping company claiming that you've missed a delivery when you weren't expecting a package? Is your boss acting out of character and urging you to change an account number without following the standard process? Trust your gut!

2. CHECK THE FILE NAME

Filenames composed of random strings of characters should be a red flag. People (especially in professional settings) don't often save documents with a 20-character alphanumeric code as its name. Similarly baiting titles like "freemoney" or "greatopportunity" should set off your internal alarm bells.

3. CHECK THE SENDER

Do you trust this person? Have you confirmed that the email address is legitimate? Have you corresponded with them before?

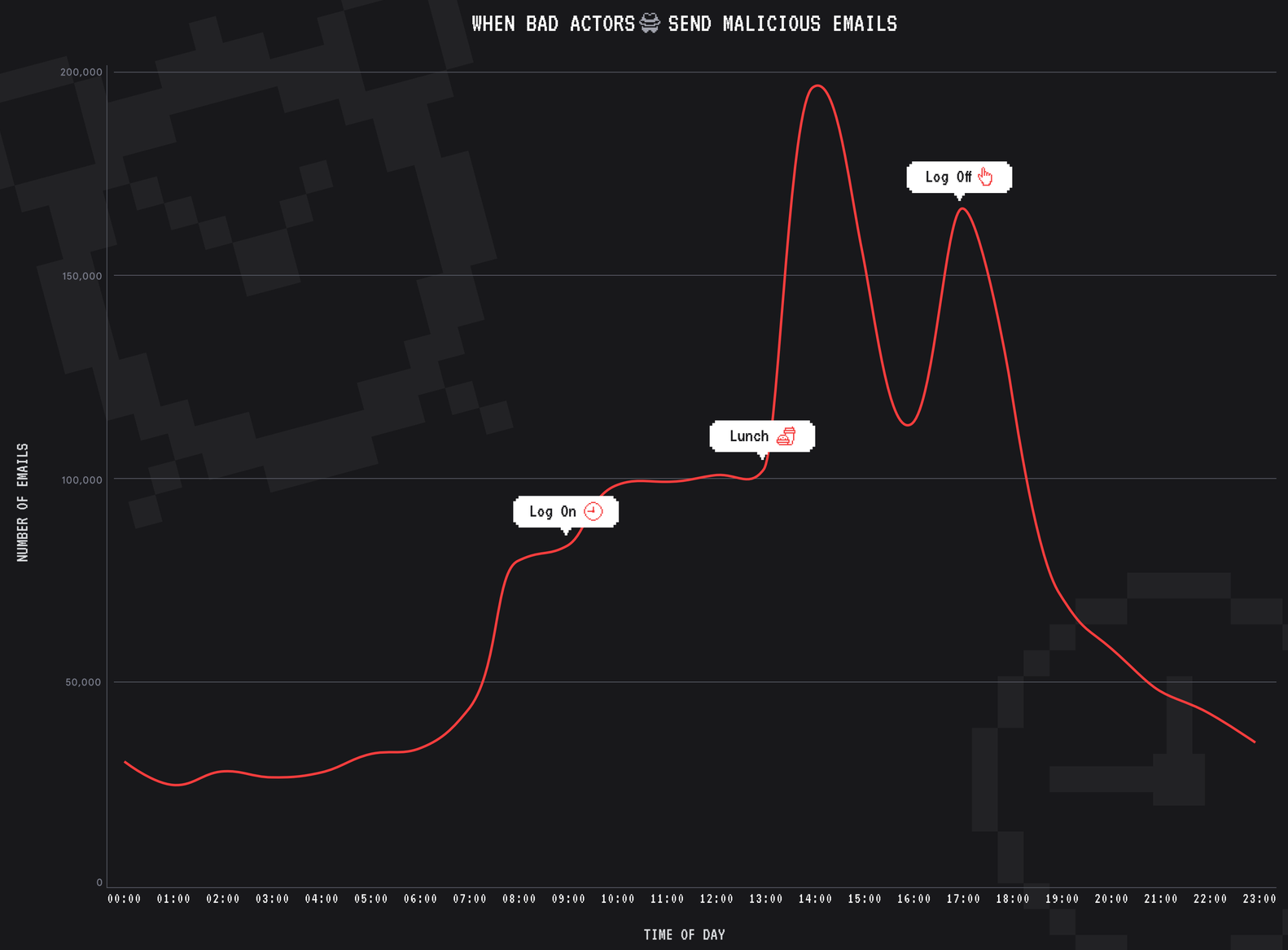
4. CHECK WITH YOUR SECURITY TEAM

If in doubt, don't open the attachment and let your security team know. Better safe than sorry.

Download this list of most common malicious attachments to share with employees

WHEN

Timing is everything



We're often told that bad actors borrow best practice from marketers. If that's the case, most phishing attacks would land in employees' inboxes around 10 AM on Wednesdays.

Our analysis tells a different story.

The most malicious emails are delivered between **2PM** and **6PM**, with very little fluctuation day-to-day (except over the weekend).

This isn't an accident.

Since **employees are more likely to make mistakes when they're stressed, tired, and distracted,** the second half of the work day is a bad actor's best bet.

Help your employees stay alert by letting them know when they're most likely to receive a phishing email, what they look like, and what to do if and when they do spot something suspicious.

Enough about the problem. What's the solution?

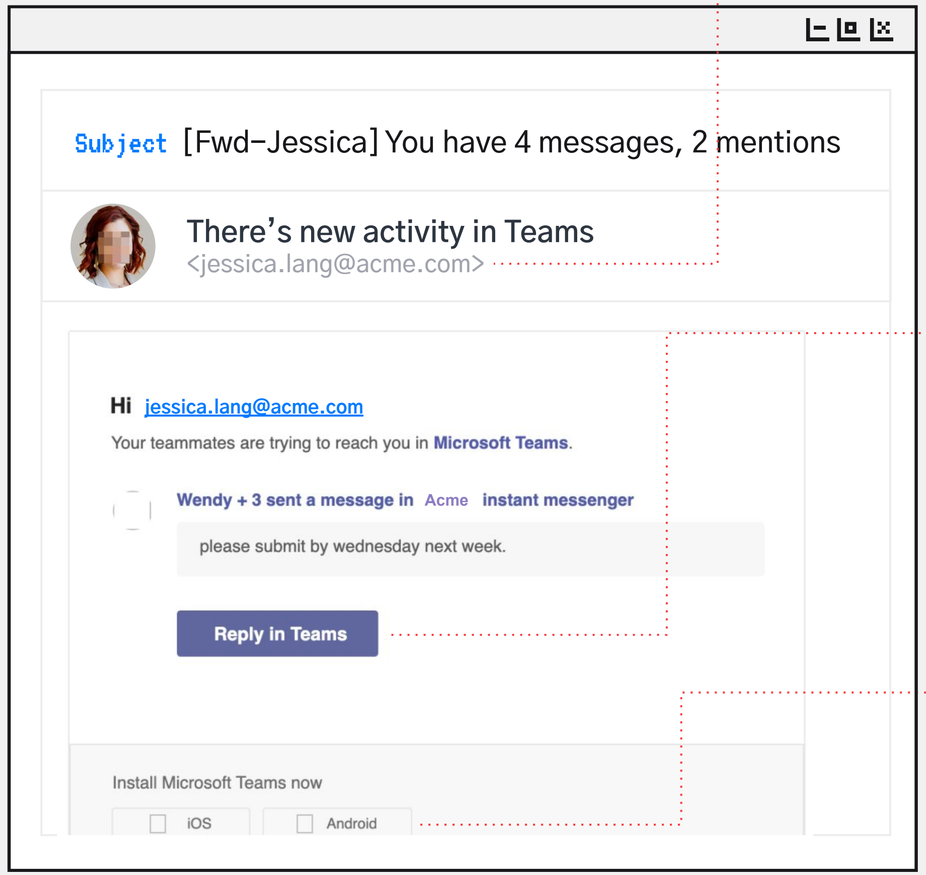
The only question left to answer is: when legacy solutions and training programs aren't enough, how can we prevent employees from interacting with the malicious emails that land in their inbox?

The answer is a layered approach.

SEGs and native tools like O365 provide basic phishing protection, but organizations need an intelligent solution like Tessian to detect and prevent advanced inbound attacks like Business Email Compromise (BEC), ATO, and CEO fraud that make it through inbuilt bulk phishing and spam filters.

Let's look at a real example of an email that slipped past a customers' other phishing defenses, but was flagged by Tessian Defender.

For more examples, download the **Defender Threat Catalogue** →



SENDER'S EMAIL ADDRESS	WHY IT SLIPS PAST OTHER DEFENSES
The sender's email address is spoofing the target's own email address. This is particularly clever; it's not implausible that Microsoft Teams would actually send emails "from" the user's own email address.	The domain itself isn't suspicious and the email didn't fail any authentication check

SUSPICIOUS LINK	WHY IT SLIPS PAST OTHER DEFENSES
The "Reply in Teams" button leads to a fake login page	The malicious page had never been seen in previous attacks, so wasn't denylisted.

FORMATTING	WHY IT SLIPS PAST OTHER DEFENSES
The notification is well-formatted and looks like a genuine email from Microsoft Teams. There aren't any obvious spelling or grammar errors.	After slipping past technological controls, employees are left as the last line of defense. Most won't question the legitimacy of the email because it looks like the real thing.

There is something unusual about this email, please take care as it could be malicious.

Report as Unusual and Delete | Mark as Safe | I'm Not Sure

Tessian has flagged this email because the sender could be pretending to be from "acme.com". Anyone can forge an email to look like it's been sent from another domain, an attack known as Direct Spoof Impersonation.

- The domain "acme.com" does not normally send emails from this server

COVID-19 Update: Phishing attacks are increasing to take advantage of the current situation, please take extra care.

Subject [Fwd-Jessica] You have 4 messages, 2 mentions

There's new activity in Teams
<jessica.lang@acme.com>

Hi jessica.lang@acme.com

Your teammates are trying to reach you in Microsoft Teams.

SUSPICIOUS LINK	HOW TESSIAN DEFENDER CAUGHT IT
The "Reply in Teams" button leads to a fake login page	Tessian understands that the email is a spoof, and doesn't need to rely on detecting malicious payloads.

SENDER'S EMAIL ADDRESS	HOW TESSIAN DEFENDER CAUGHT IT
The sender's email address is spoofing the target's own email address. This is particularly clever; it's not implausible that Microsoft Teams would actually send emails "from" the user's own email address.	Tessian Defender detects anomalies in the sender's server, IP address, and geophysical location to detect spoofed emails.

> We trust Tessian's technology to flag when an email is malicious or anomalous, and we trust our employees to interact with the warnings and do the right thing. And, we can actually see that threats are being prevented. We can see it works. But, without any investigation and no noise.
>
> **MIKE VIEIRA**
> Perimeter and Cloud Security Capability Lead, Schroders

Tessian Defender uses machine learning (ML) to protect your people from even the most advanced inbound threats.

Here's how:

Tessian's machine learning algorithms analyze your company's email data, learn employees' normal communication patterns, and map their trusted email relationships — both inside and outside your organization.

Tessian inspects both the content and metadata of inbound emails for any suspicious or unusual signals pointing to a potential impersonation, ATO, or BEC threat. For example, payloads, anomalous geophysical locations, IP addresses, email clients, and sending patterns.

Once it detects a threat, Tessian alerts employees that an email might be unsafe, explaining the threat in easy-to-understand language via an interactive notification.

TESSIAN

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel, March Capital, and Balderton.

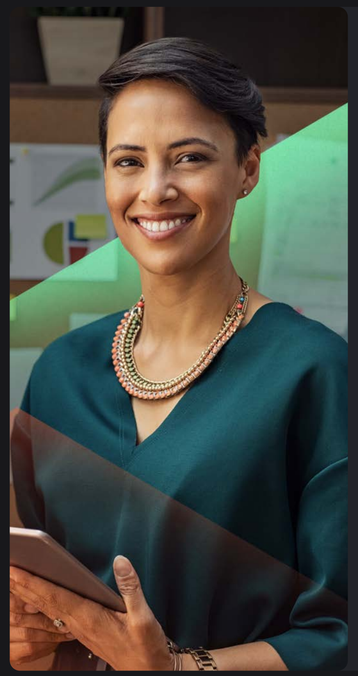
TESSIAN.COM

Methodology

This report is based on analysis of emails flagged as malicious by Tessian Defender between July 2020 and July 2021.

Publically available third-party research was also used, with all sources cited throughout.

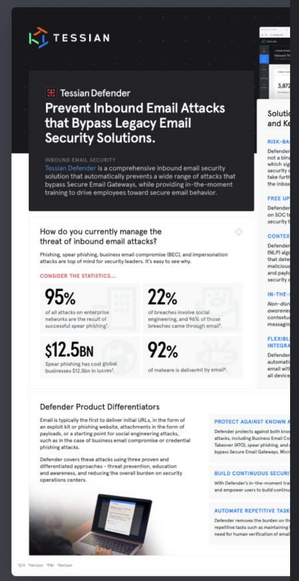
Midpoints and averages were used when calculating some figures and percentages may not always add up to 100% due to rounding.



Learn about Human Layer Security.

Want to learn more about how Tessian prevents spear phishing, business email compromise, account takeover, and other targeted email attacks?

REQUEST A DEMO →



Datasheet: Tessian Defender

Enterprise customers around the world trust Tessian Defender to prevent attacks that bypass SEGs. Learn how you can stop the most advanced threats without admin overhead.

DOWNLOAD NOW →

Share this report

TESSIAN.COM/RESEARCH →