Targeted Phishing Attacks and their Signals

https://campus.barracuda.com/doc/88114342/

Barracuda uses techniques such as natural language processing, account statistics, and domain assessment to detect signals to protect you from potential targeted attacks. For example, Barracuda can analyze language patterns and detect language often used in attack emails. It can then send suspicious emails to your **Junk Email** folder, protecting you from potential attacks.

This article provides a general sense of the signals used by Barracuda for Impersonation Protection. Note that it would be irresponsible to disclose the inner workings of Barracuda Networks' Impersonation Protection.

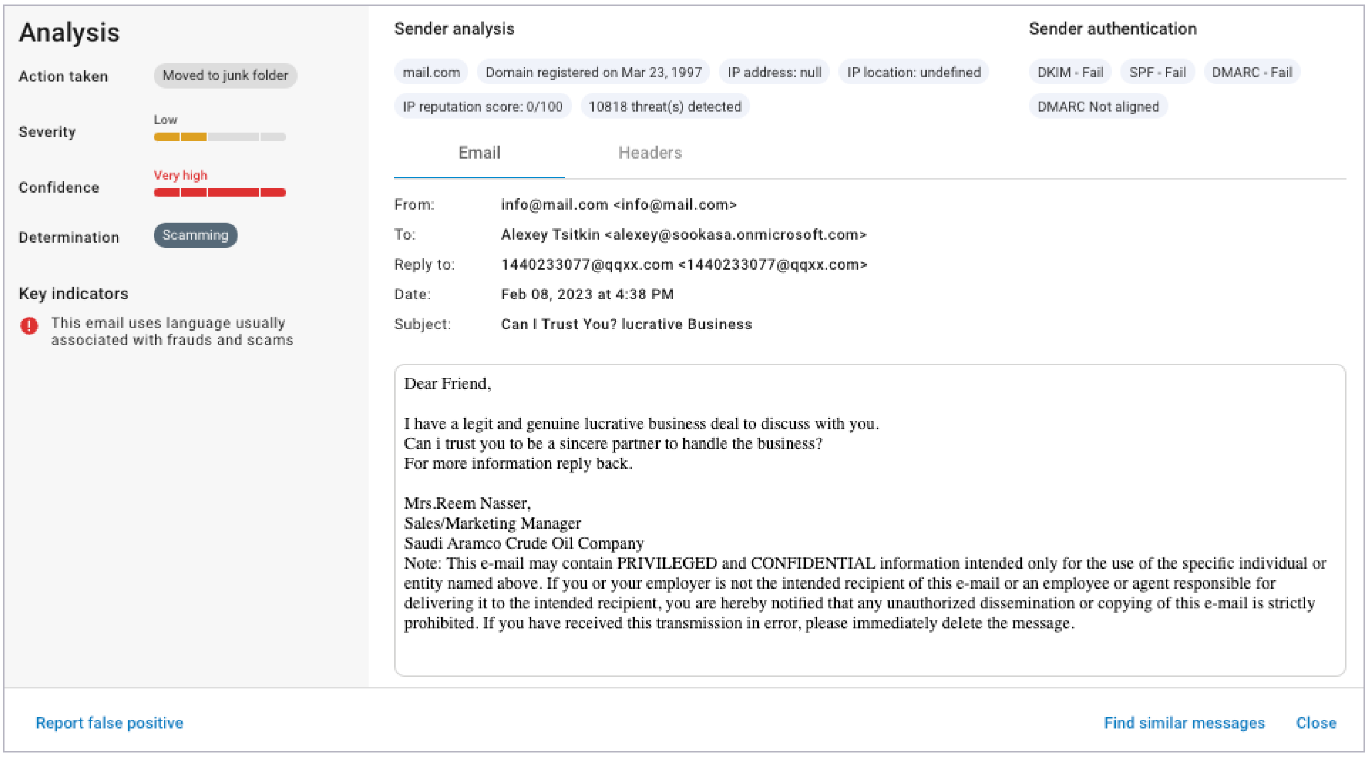
Barracuda Networks also detects signals to protect you from account takeover (ATO) attacks. See Account Takeover Attacks and their Signals for details.

Types of Phishing Attacks

Barracuda protects against the targeted types of phishing attacks described here.

Scamming

In a scam, an unusual request is made of the recipient – like a request from a stranger, asking the target to send a large amount of money in return for a share in some other large sum of money. The **Severity** score for Scamming attacks is Low.



From: info@mail.com <info@mail.com>
To: Alexey Tsitkin <alexey@sookasa.onmicrosoft.com>
Reply to: 1440233077@qqxx.com <1440233077@qqxx.com>
Date: Feb 08, 2023 at 4:38 PM
Subject: Can I Trust You? lucrative Business

Dear Friend,

I have a legit and genuine lucrative business deal to discuss with you.
Can i trust you to be a sincere partner to handle the business?
For more information reply back.

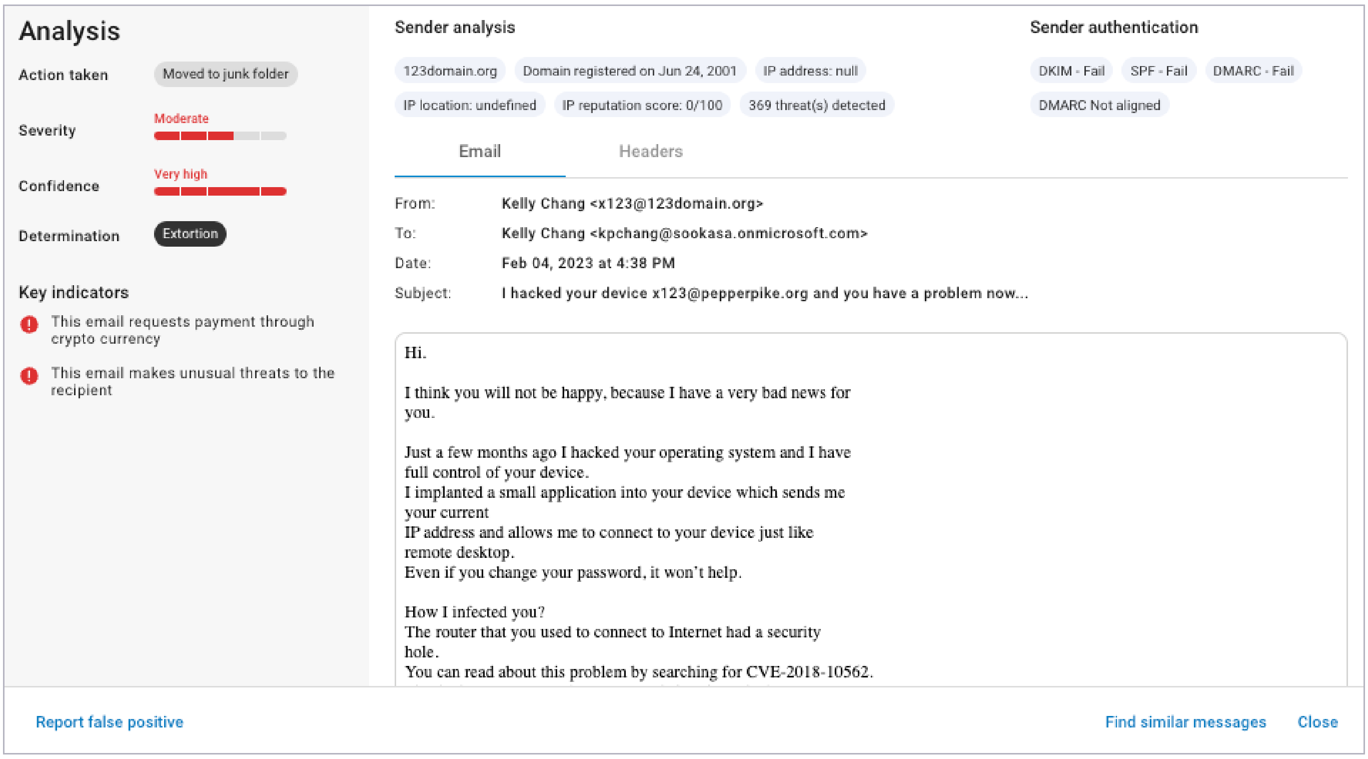
Mrs.Reem Nasser,
Sales/Marketing Manager
Saudi Aramco Crude Oil Company
Note: This e-mail may contain PRIVILEGED and CONFIDENTIAL information intended only for the use of the specific individual or entity named above. If you or your employer is not the intended recipient of this e-mail or an employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any unauthorized dissemination or copying of this e-mail is strictly prohibited. If you have received this transmission in error, please immediately delete the message.

For more information, see Getting Started.

Extortion

Similar to standard extortion, online extortion involves demands for large payments to a stranger in exchange for their not revealing some embarrassing information about the target.

The **Severity** score for Extortion attacks is Moderate.



Analysis

Action taken: Moved to junk folder

Severity: Moderate

Confidence: Very high

Determination: Extortion

Key indicators

- This email requests payment through crypto currency
- This email makes unusual threats to the recipient

Sender analysis

123domain.org · Domain registered on Jun 24, 2001 · IP address: null · IP location: undefined · IP reputation score: 0/100 · 369 threat(s) detected

Sender authentication

DKIM - Fail · SPF - Fail · DMARC - Fail · DMARC Not aligned

From: Kelly Chang <x123@123domain.org>
To: Kelly Chang <kpchang@sookasa.onmicrosoft.com>
Date: Feb 04, 2023 at 4:38 PM
Subject: I hacked your device x123@pepperpike.org and you have a problem now...

Hi.

I think you will not be happy, because I have a very bad news for you.

Just a few months ago I hacked your operating system and I have full control of your device.
I implanted a small application into your device which sends me your current
IP address and allows me to connect to your device just like remote desktop.
Even if you change your password, it won't help.

How I infected you?
The router that you used to connect to Internet had a security hole.
You can read about this problem by searching for CVE-2018-10562.

For more information, see Getting Started.

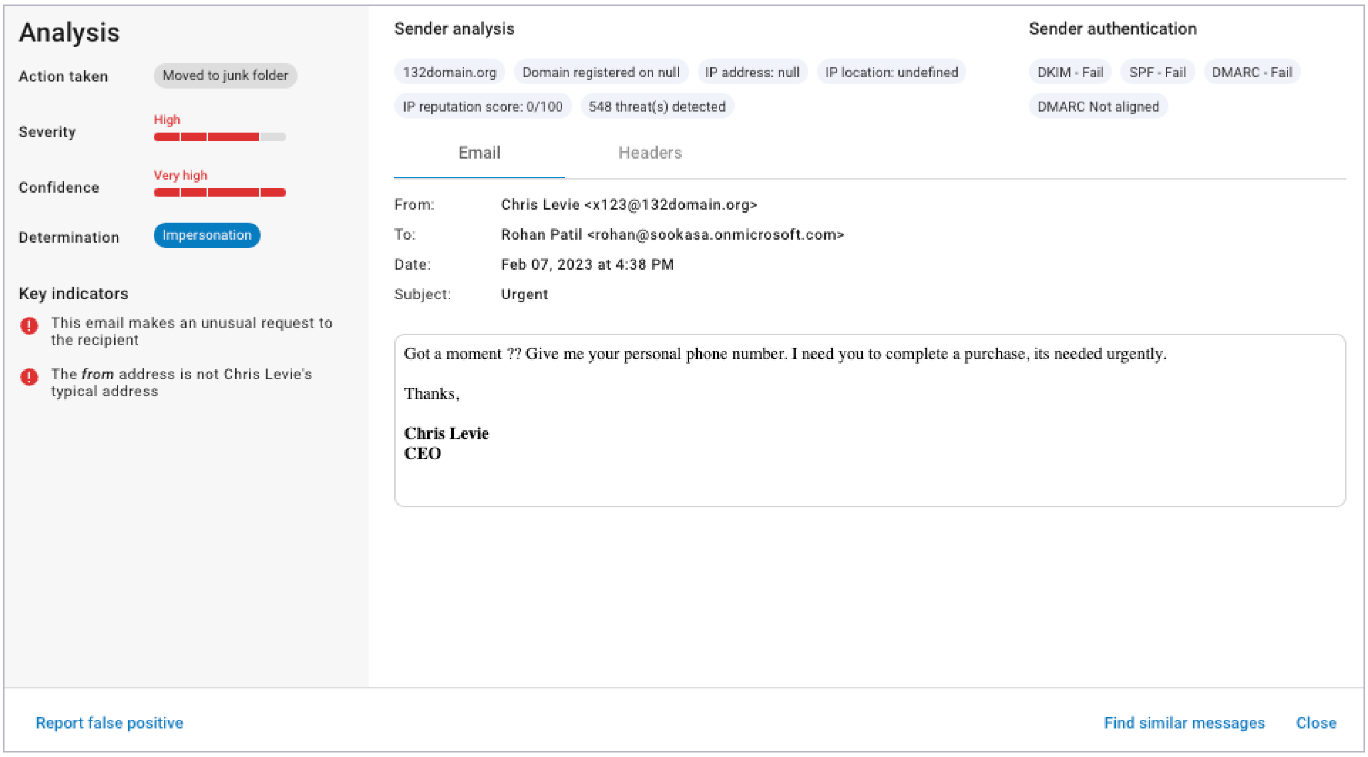
Impersonation

Impersonation attacks might impersonate a domain, an employee, or both.

The sender might purposely misspell the *From* address, altering it slightly, so the change is barely perceptible. The target might respond to a nefarious request, thinking the request is coming someone they know and trust.

The attacker might also assume the identity of an employee, assuming a position of trust with other employees. With this trust, the attacker can gain access to important corporate information or convince another employee to perform a task, like a bank transfer to a nefarious account.

The **Severity** score of Impersonation attacks is High.



Analysis

Action taken: Moved to junk folder

Severity: High

Confidence: Very high

Determination: Impersonation

Key indicators

- This email makes an unusual request to the recipient
- The *from* address is not Chris Levie's typical address

Sender analysis

132domain.org | Domain registered on null | IP address: null | IP location: undefined | IP reputation score: 0/100 | 548 threat(s) detected

Sender authentication

DKIM - Fail | SPF - Fail | DMARC - Fail | DMARC Not aligned

From: Chris Levie <x123@132domain.org>
To: Rohan Patil <rohan@sookasa.onmicrosoft.com>
Date: Feb 07, 2023 at 4:38 PM
Subject: Urgent

Got a moment ?? Give me your personal phone number. I need you to complete a purchase, its needed urgently.

Thanks,

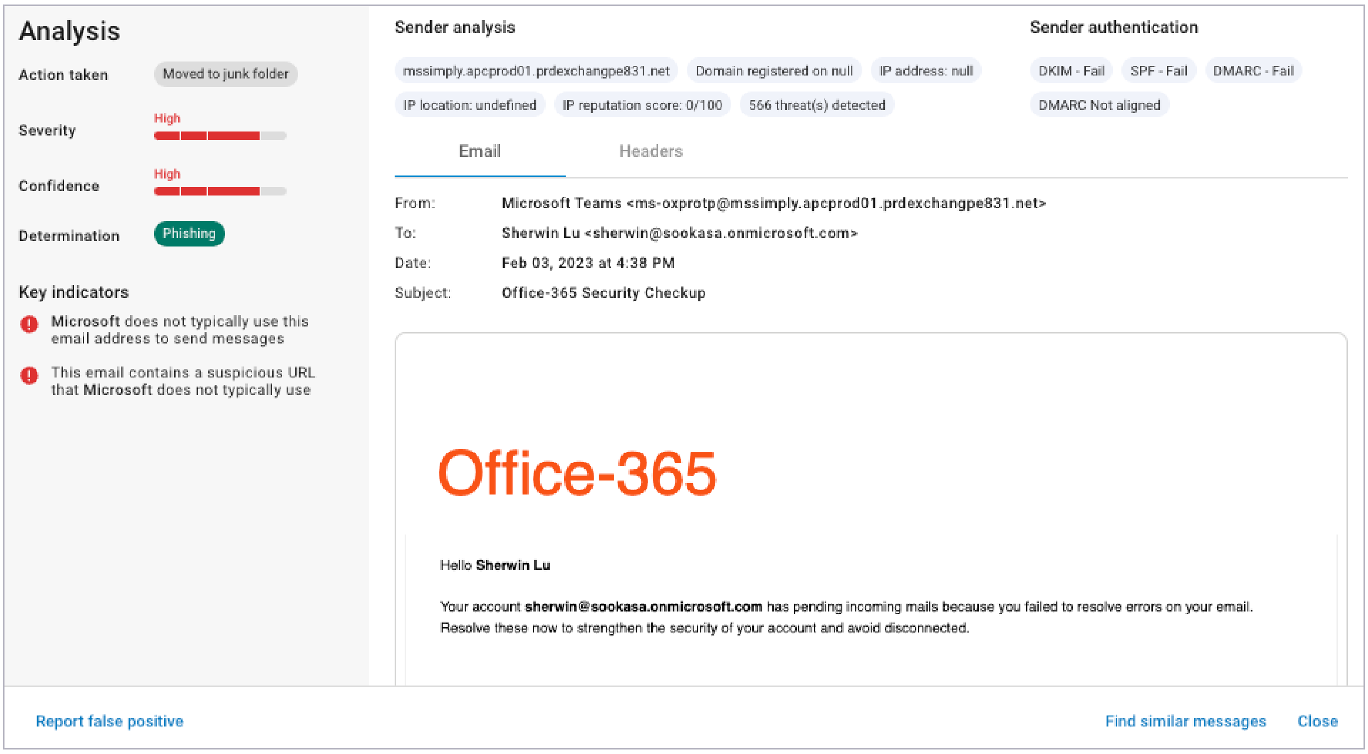
Chris Levie
CEO

For more information, see Getting Started.

Phishing

The attacker impersonates a well-known service, like a bank or an Internet service provider, and asks the user to click a link and log into their account. The attacker can then steal the user's login credentials.

The **Severity** score for Phishing attacks is High.



Analysis

Action taken: Moved to junk folder

Severity: High

Confidence: High

Determination: Phishing

Key indicators

- Microsoft does not typically use this email address to send messages
- This email contains a suspicious URL that Microsoft does not typically use

Sender analysis

mssimply.apcprod01.prdexchangpe831.net · Domain registered on null · IP address: null · IP location: undefined · IP reputation score: 0/100 · 566 threat(s) detected

Sender authentication

DKIM - Fail · SPF - Fail · DMARC - Fail · DMARC Not aligned

From: Microsoft Teams <ms-oxprotp@mssimply.apcprod01.prdexchangpe831.net>
To: Sherwin Lu <sherwin@sookasa.onmicrosoft.com>
Date: Feb 03, 2023 at 4:38 PM
Subject: Office-365 Security Checkup

Office-365

Hello **Sherwin Lu**

Your account **sherwin@sookasa.onmicrosoft.com** has pending incoming mails because you failed to resolve errors on your email. Resolve these now to strengthen the security of your account and avoid disconnected.

For more information, see Getting Started.

Signals

Here is a *sampling* of the signals Barracuda uses to detect potential attacks:

- The email:
  - uses language usually associated with frauds and scams.
  - makes an unusual or urgent request of the recipient.
  - requests payment through cryptocurrency.
  - makes unusual threats to the recipient.
  - contains a link to a URL not usually used by the sender.
- The *From* address is not the sender’s typical address.
- The *Reply To* or *Sender* domain appears to be impersonating another domain.

Figures