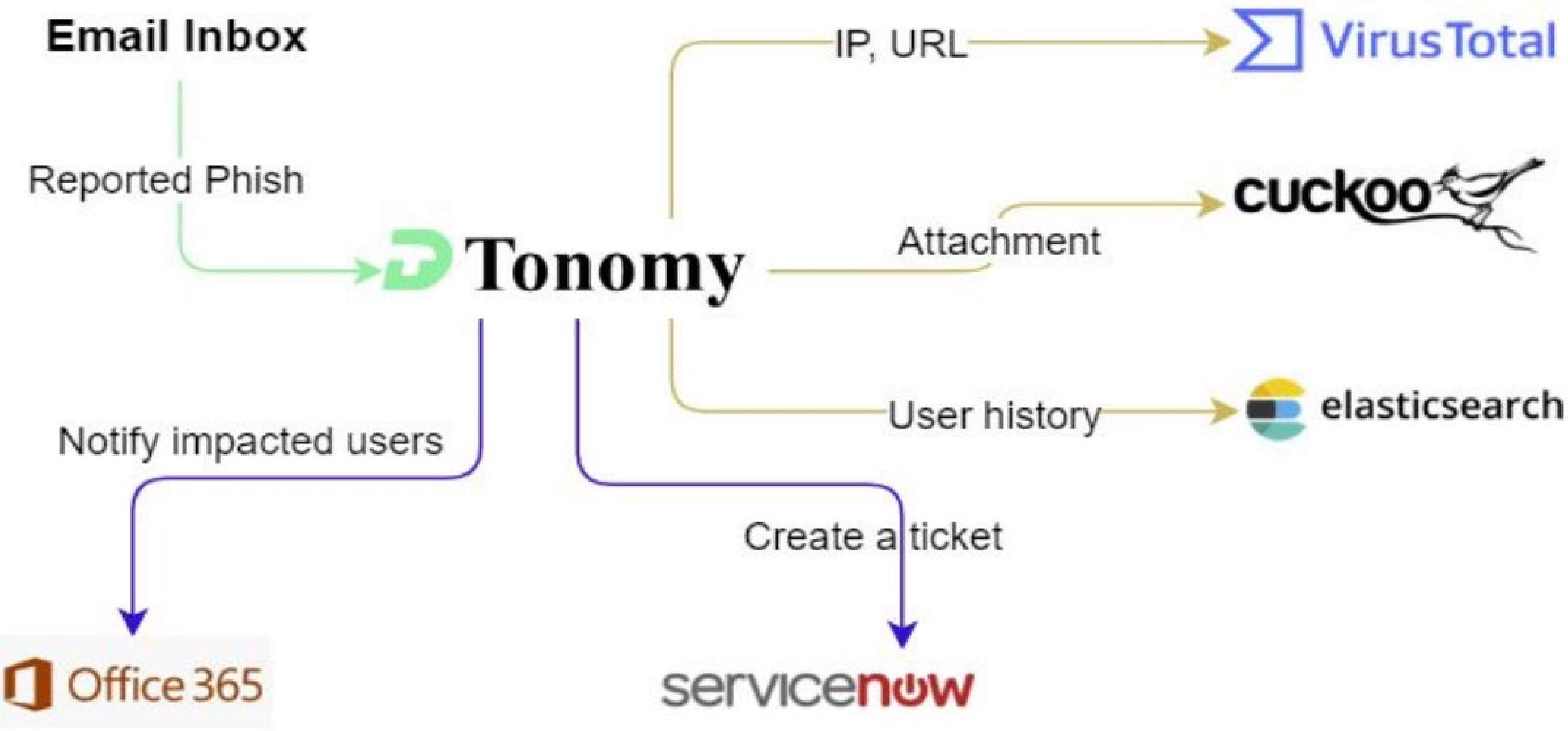
FEATURES OF PHISHING EMAILS

- Too good to be true
- Creates sense of urgency
- Includes suspicious Hyperlinks
- They have malicious attachments.
- You get unexpected emails form unusual senders

PHISHING INVESTIGATION ANATOMY



SPOT THE PHISH GAME

https://training.knowbe4.com/ui/modstore/detail?u=c02fdcb6-b521-11e9-84bf-123d7cbdf51c&back=Suggested%20Content

PHISHING EXECUTIVE SUMMARY

- Date and Time

- Sender

- Receiver

- Subject

- Ips and URLs of sender

  Used Tools: Virus Total, URLScan.io, Mx toolbox, Email Header Analysis Tool And Finally Decide If It Is True Positive Or False Positive, Benign, Or infected

- Should IP or URL be blocked?

PHISHING EXECUTIVE SUMMARY

- Define phishing and identify various types of phishing scams
- Recognize common baiting tactics used in phishing scams
- Examine real phishing messages
- Understand how to protect yourself from being hooked by a phishing scam

PHARMING

Pharming is a type of cyber attack that redirects website traffic to fraudulent websites, often without the user's knowledge or consent. It is a sophisticated technique used by attackers to deceive individuals and steal sensitive information.

HOW DOES PHARMING WORK

Pharming attacks exploit vulnerabilities in the Domain Name System (DNS) or manipulate hosts files to redirect users to fake websites. This can lead to the theft of login credentials, financial information, and personal data.

THE IMPACT OF PHARMING ATTACKS

Pharming attacks can have severe consequences for individuals and organizations:

Financial Loss: Victims may unknowingly provide their banking details to fake websites, resulting in unauthorized access and financial loss.

Identity Theft: Personal information, such as social security numbers or email credentials, can be stolen and used for identity theft.

Reputation Damage: Organizations targeted by pharming attacks may suffer reputational damage due to compromised customer data and trust.

- Phishing – Cybercriminal attempts to steal personal and financial information or infect computers and other devices with malware and viruses

  - Designed to trick you into clicking a link or providing personal or financial information
  - Often in the form of emails and websites
  - May appear to come from legitimate companies, organizations or known individuals
  - Take advantage of natural disasters, epidemics, health scares, political elections or timely events

PHISHING

- Use of deceptive mass mailing
- Can target specific entities ("spear phishing")
- Prevention:

– Honeypot email addresses

– Education

– Awareness of network and website changes

IMPERSONATION ON HELP DESK CALLS

- Calling the help desk pretending to be someone else
- Usually an employee or someone with authority
- Prevention:
  - Assign pins for calling the help desk
  - Don’t do anything on someone’s order
  - Stick to the scope of the help desk

PHYSICAL ACCESS

- Tailgating
- Ultimately obtains unauthorize

building access

- Prevention

– Require badges

– Employee training

– Security officers

– No exceptions!

COMMON BAITING TACTICS

- Notification from a help desk or system administrator
  Asks you to take action to resolve an issue with your account (e.g., email account has reached its storage limit), which often includes clicking on a link and providing requested information.

- Advertisement for immediate weight loss, hair growth or fitness prowess
  Serves as a ploy to get you to click on a link that will infect your computer or mobile device with malware or viruses.

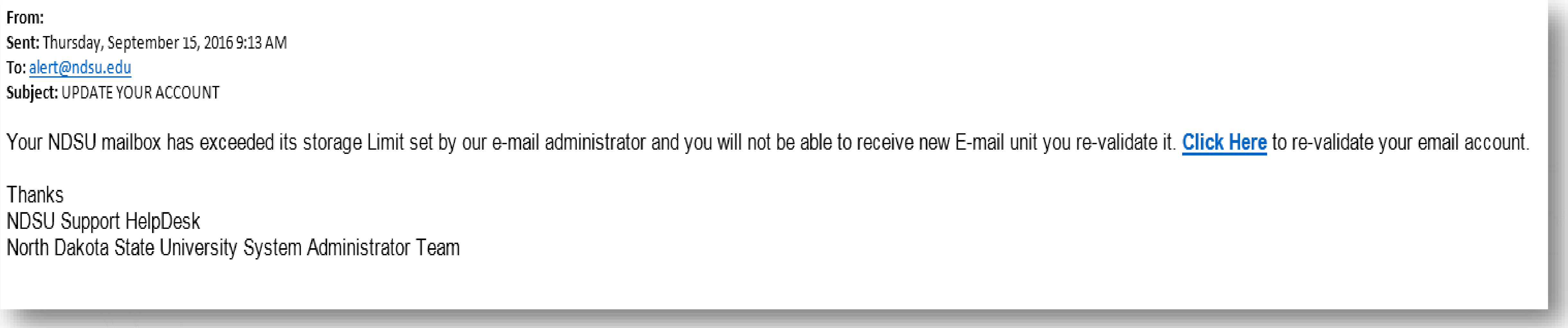
- Attachment labeled “invoice” or “shipping order”
  Contains malware that can infect your computer or mobile device if opened. May contain what is known as “ransomware,” a type of malware that will delete all files unless you pay a specified sum of money.

- Notification from what appears to be a credit card company
  Indicates someone has made an unauthorized transaction on your account. If you click the link to log in to verify the transaction, your username and password are collected by the scammer.

- Fake account on a social media site
  Mimics a legitimate person, business or organization. May also appear in the form of an online game, quiz or survey designed to collect information from your account.

PHISHING LURE

- Claims to come from the NDSU IT Help Desk and system administrators
  - References NDSU and North Dakota State University
  - Calls for immediate action using threatening language
- Includes hyperlink that points to fraudulent site



From:
Sent: Thursday, September 15, 2016 9:13 AM
To: alert@ndsu.edu
Subject: UPDATE YOUR ACCOUNT

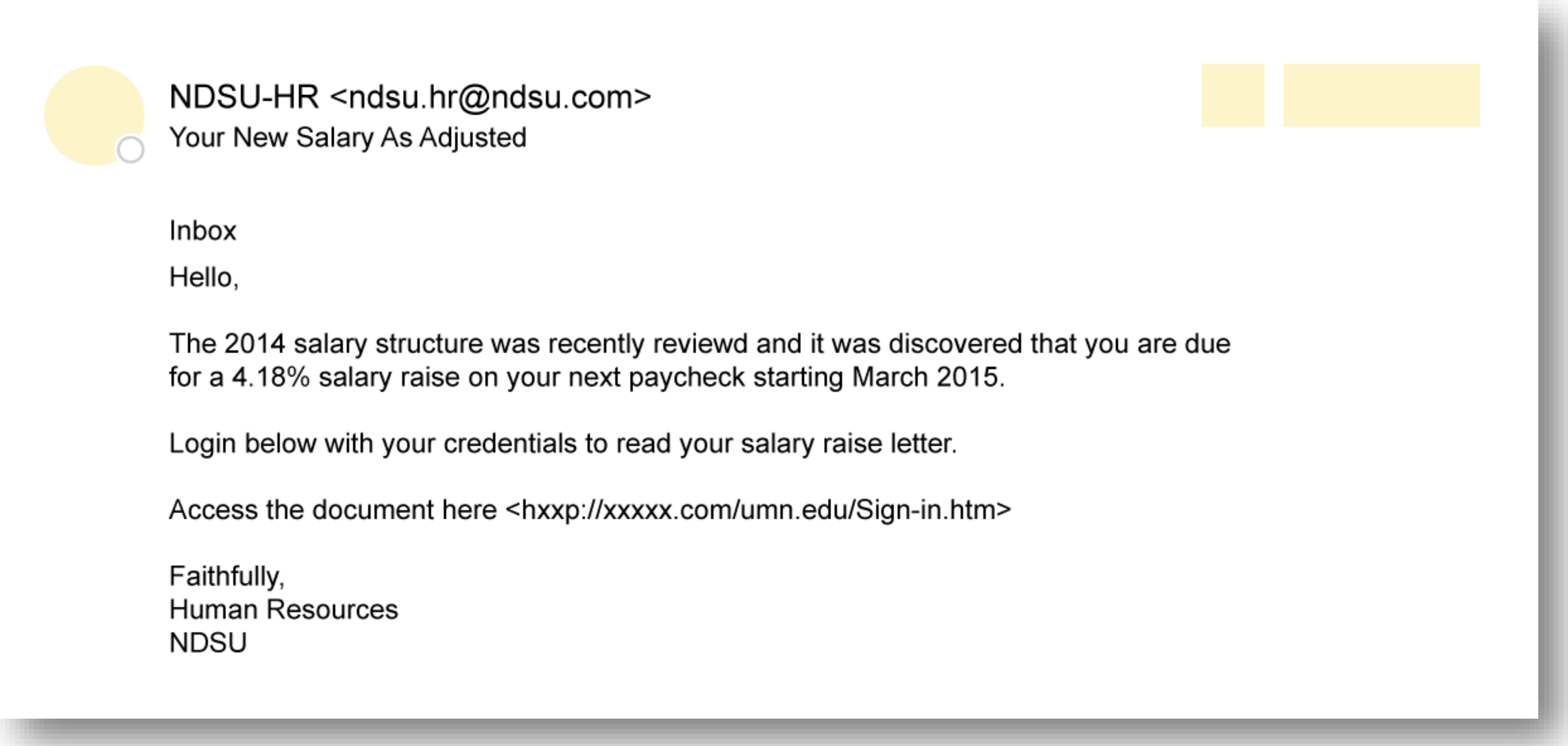
Your NDSU mailbox has exceeded its storage Limit set by our e-mail administrator and you will not be able to receive new E-mail unit you re-validate it. Click Here to re-validate your email account.

Thanks
NDSU Support HelpDesk
North Dakota State University System Administrator Team

Claims to come from the NDSU Human Resources

- Timely call for action during annual review season
- From address includes NDSU, but not .edu address (@ndsu**.com**)

Includes hyperlink that points to fraudulent site



NDSU-HR <ndsu.hr@ndsu.com>
Your New Salary As Adjusted

Inbox

Hello,

The 2014 salary structure was recently reviewd and it was discovered that you are due for a 4.18% salary raise on your next paycheck starting March 2015.

Login below with your credentials to read your salary raise letter.

Access the document here <hxxp://xxxxx.com/umn.edu/Sign-in.htm>

Faithfully,
Human Resources
NDSU

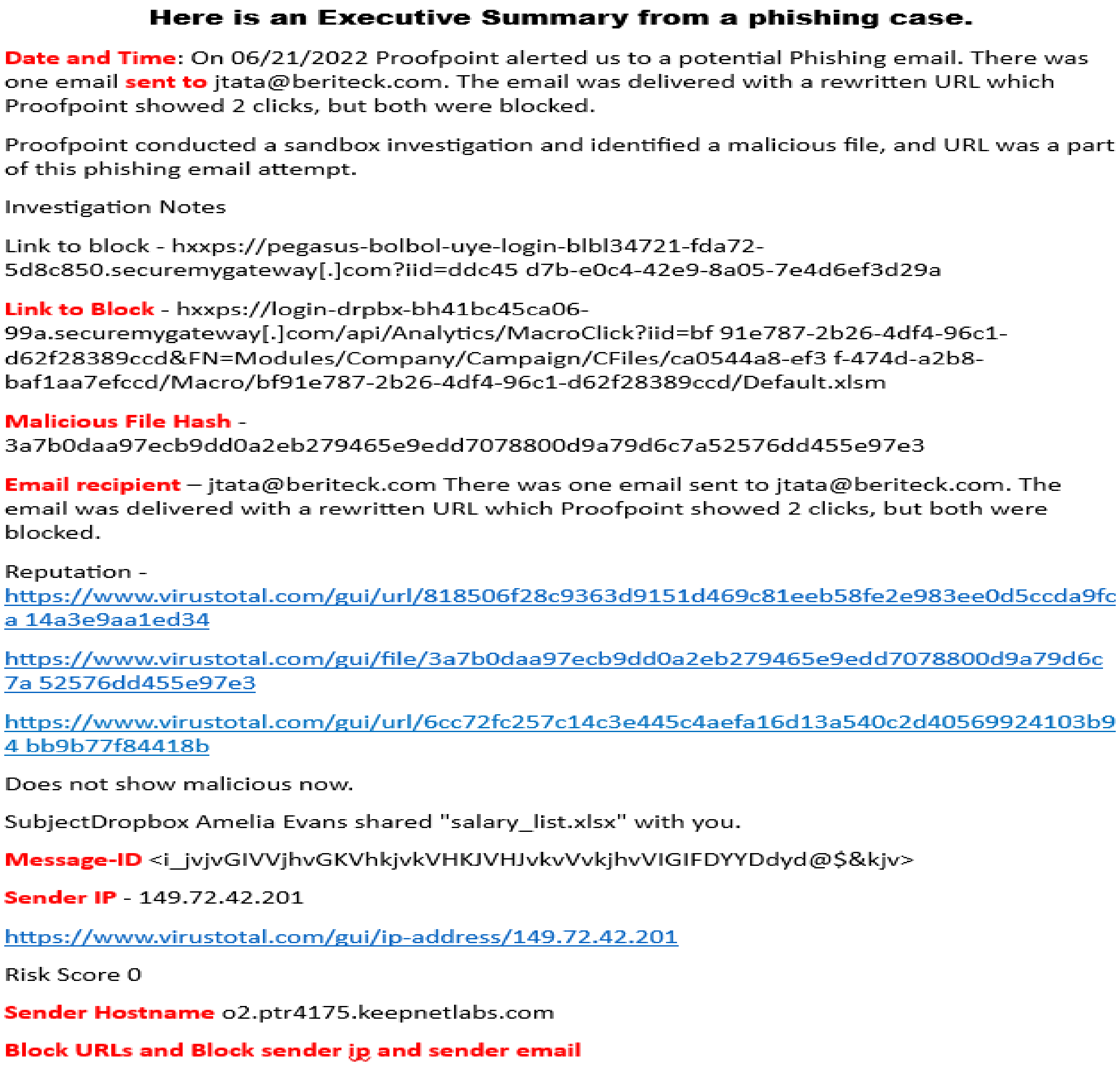
CLONE PYPHISHER AND MOUNT A PHISHING ATTACK

https://github.com/KasRoudra/PyPhisher

  - Clone instagram
  - Clone Gmail
  - Clone Paypal

Mimic an existing email using emkei (<a href ="url">link text</a>)

SAMPLE EXECUTIVE SUMMARY



Here is an Executive Summary from a phishing case.

Date and Time: On 06/21/2022 Proofpoint alerted us to a potential Phishing email. There was one email **sent to** jtata@beriteck.com. The email was delivered with a rewritten URL which Proofpoint showed 2 clicks, but both were blocked.

Proofpoint conducted a sandbox investigation and identified a malicious file, and URL was a part of this phishing email attempt.

Investigation Notes

Link to block - hxxps://pegasus-bolbol-uye-login-blbl34721-fda72-5d8c850.securemygateway[.]com?iid=ddc45 d7b-e0c4-42e9-8a05-7e4d6ef3d29a

Link to Block - hxxps://login-drpbx-bh41bc45ca06-99a.securemygateway[.]com/api/Analytics/MacroClick?iid=bf 91e787-2b26-4df4-96c1-d62f28389ccd&FN=Modules/Company/Campaign/CFiles/ca0544a8-ef3 f-474d-a2b8-baf1aa7efccd/Macro/bf91e787-2b26-4df4-96c1-d62f28389ccd/Default.xlsm

Malicious File Hash - 3a7b0daa97ecb9dd0a2eb279465e9edd7078800d9a79d6c7a52576dd455e97e3

Email recipient – jtata@beriteck.com There was one email sent to jtata@beriteck.com. The email was delivered with a rewritten URL which Proofpoint showed 2 clicks, but both were blocked.

Reputation - https://www.virustotal.com/gui/url/818506f28c9363d9151d469c81eeb58fe2e983ee0d5ccda9fca 14a3e9aa1ed34

https://www.virustotal.com/gui/file/3a7b0daa97ecb9dd0a2eb279465e9edd7078800d9a79d6c7a 52576dd455e97e3

https://www.virustotal.com/gui/url/6cc72fc257c14c3e445c4aefa16d13a540c2d405699241003b94 bb9b77f84418b

Does not show malicious now.

SubjectDropbox Amelia Evans shared "salary_list.xlsx" with you.

Message-ID <i_jvjvGIVVjhvGKVhkjvkVHKJVHJvkvVvkjhvVIGIFDYYDdyd@$&kjv>

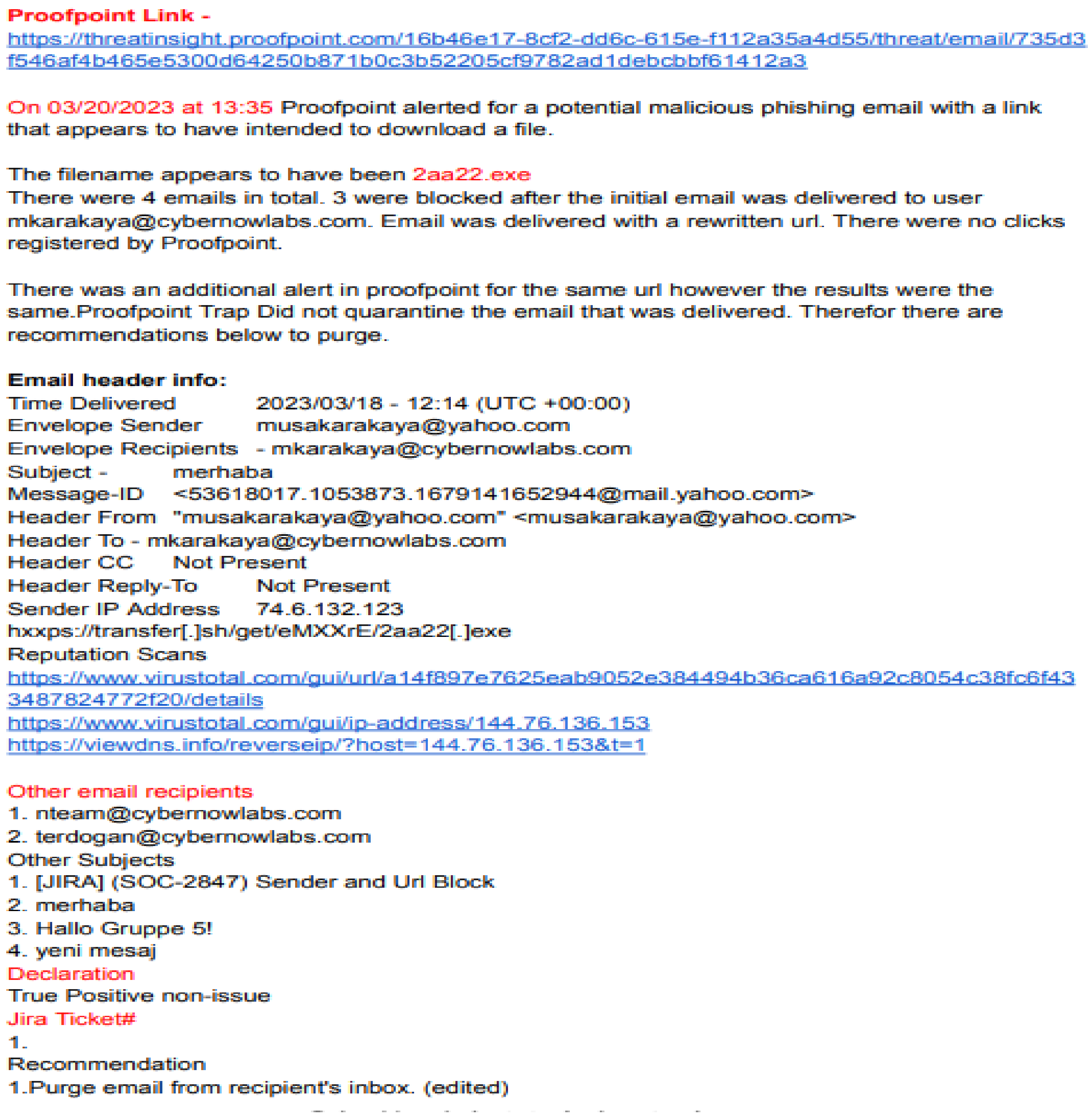
Sender IP - 149.72.42.201

https://www.virustotal.com/gui/ip-address/149.72.42.201

Risk Score 0

Sender Hostname o2.ptr4175.keepnetlabs.com

Block URLs and Block sender ip and sender email



Proofpoint Link -
https://threatinsight.proofpoint.com/16b46e17-8cf2-dd6c-615e-f112a35a4d55/threat/email/735d3f546af4b465e5300d64250b871b0c3b52205cf9782ad1debcbbf61412a3

On 03/20/2023 at 13:35 Proofpoint alerted for a potential malicious phishing email with a link that appears to have intended to download a file.

The filename appears to have been 2aa22.exe
There were 4 emails in total. 3 were blocked after the initial email was delivered to user mkarakaya@cybernowlabs.com. Email was delivered with a rewritten url. There were no clicks registered by Proofpoint.

There was an additional alert in proofpoint for the same url however the results were the same.Proofpoint Trap Did not quarantine the email that was delivered. Therefor there are recommendations below to purge.

Email header info:
Time Delivered 2023/03/18 - 12:14 (UTC +00:00)
Envelope Sender musakarakaya@yahoo.com
Envelope Recipients - mkarakaya@cybernowlabs.com
Subject - merhaba
Message-ID <53618017.1053873.1679141652944@mail.yahoo.com>
Header From "musakarakaya@yahoo.com" <musakarakaya@yahoo.com>
Header To - mkarakaya@cybernowlabs.com
Header CC Not Present
Header Reply-To Not Present
Sender IP Address 74.6.132.123
hxxps://transfer[.]sh/get/eMXXrE/2aa22[.]exe
Reputation Scans
https://www.virustotal.com/gui/url/a14f897e7625eab9052e384494b36ca616a92c8054c38fc6f433487824772f20/details
https://www.virustotal.com/gui/ip-address/144.76.136.153
https://viewdns.info/reverseip/?host=144.76.136.153&t=1

Other email recipients
1. nteam@cybernowlabs.com
2. terdogan@cybernowlabs.com
Other Subjects
1. [JIRA] (SOC-2847) Sender and Url Block
2. merhaba
3. Hallo Gruppe 5!
4. yeni mesaj
Declaration
True Positive non-issue
Jira Ticket#
1.
Recommendation
1.Purge email from recipient's inbox. (edited)