Phishing and Spoofed Email Investigations & Incident Response

by Said Varlioglu

Incident Response Engineer
Trend Micro
Types of Emails

Personal Email → johndoe@gmail.com

Business Email → john.doe@trendmicro.com

Business Group Email → admissions@uc.edu
→ support@trendmicro.com

Disposable Email → 928938@tempemail.co
What is a Phishing Email?

Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an email.

Types of Emails:

→ Deceptive Phishing
→ Spear Phishing
→ Whaling - CEO Fraud
→ Phishing Emails from Compromised Weaponized Accounts
Why Phishing Emails are Dangerous?

Many hacking activities start with a phish email!

- Attackers can steal sensitive or confidential information in emails
- Attackers can copy the address-books to send new phishing emails
- Attackers can re-use the hacked email for a new phishing attack
- Malicious attachments may have some hidden scripts (macros)
- Hidden scripts may download other trojans/malware
- Trojans/Backdoors may provide remote control to the attackers
- Attackers may access, read, modify, steal, publish or encrypt data
- Attackers can move laterally in the network to access the organization's database

Note that new attack trend is Phishing Email + Fileless Malware!
Victim Profiles & Top Targets

Business emails (@company.org)
College students (@college.edu)
College employees (@college.edu)
Government officials (@state.gov)
Journalists (@newspaper.com)
Political organization employees (@party.org)
Employees of companies that works closely with federal agencies (@company.com)
Customers of companies that works closely with federal agencies (@company.com)
Employees of telecommunications and travel companies (@travelcompany.com)
How to **Recognize** a Phishing Email?

How to recognize a phishing email?

- **Strange** names and email addresses
- **Hidden** malicious links under the links (Please, Hover and Look at the actual link)
- **Tricky** words such as “Urgent”, "Executive", "Admin", "Mandatory", "Confidential", "Critical", "Restricted",
- **Spelling** and **grammatical** mistakes
- **Low-resolution** images
- **Generic** greetings, “Dear Sir/Ma’am”
- “Big Deals”; "Big Awards"
- **Fake** full-time/part-time job openings
- **Requests** for personal or financial information
- **Attachments** including fake invoices, fake fax documents, fake voice messages
- **Threatening** or **bossy** words such as "I recorded you", "Read me now", "Confirm it today"
Consequences of a Phishing Attack

Wisconsin Republican Party says hackers stole $2.3 million

The party noticed the suspicious activity on Oct. 22 and contacted the FBI on Friday, said Republican Party Chairman Andrew Hitt.

Hitt stressed that the money stolen was for services already rendered.

“While a large sum of money was stolen, our operation is running at full capacity,” he said.

Hitt said the hackers manipulated invoices from four vendors who were being paid for direct mail for Trump’s reelection efforts as well as for pro-Trump material such as hats to be handed out to supporters. Invoices and other documents were altered so when the party paid them, the money went to the hackers instead of the vendors, Hitt said.

It was discovered after someone noticed that an invoice was generated that should not have been, he said.

Hitt said it appears the attack began as a phishing attempt and no data appears to have been stolen, said party spokesman Alec Zimmerman.
Deceptive Phishing

Attackers impersonate a legitimate company to steal people’s personal data or login credentials.

Those emails frequently use threats and a sense of urgency to scare users into doing what the attackers want.

In this example, a phishing email instructs recipients to click on the link to review pending messages in Office365 account.

However, the link redirects the user to a website designed to impersonate Office365’s login page.
A Malicious Destination of a Deceptive Phishing Link

When users gives their password, the threat actors will receive them!
The attacker sends an email using Dropbox.

The attacker puts a malicious pdf file in a Dropbox account and shares it with the victim.
Inside of the Dropbox account, there is a PDF file.

Inside of the PDF file, there is a link.
The link redirects the user to a website designed to impersonate Microsoft’s login page.
When the attackers know the victim’s name:

**Payroll Account Issue**

From: HR Department <hr_department@company.com>
Subject: [Action Required] Your next payroll cannot be processed

Hi, {{recipient_full_name}}!

We are currently processing the payroll for next month, and found an issue with your account. According to our bank representative, your account was on hold due to suspicious transactions in the past couple of weeks. Please verify your information using this link sent by the bank to reactivate your account.

Kindly complete the verification immediately to avoid any delay in your payroll.

If you have any questions, feel free to send us an email. Thank you.

Regards,
HR Department
Whaling or CEO fraud:

When attackers exploit/weaponize the compromised manager accounts or spoofed manager email accounts:

(high-ranking executives)

---

<table>
<thead>
<tr>
<th>Jim Stapleton (URGENT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jim, I am currently stuck in a meeting, but we need to do a wire transfer as soon as possible for a payment Laura wants us to get done today.</td>
</tr>
<tr>
<td>Can you get that done this morning? Let me know and I will get you the info you need. Thanks.</td>
</tr>
<tr>
<td>David</td>
</tr>
</tbody>
</table>

**David Zimmerman**
CEO
North Group Inc.
Phishing Emails from a Compromised Account

Business email compromise (BEC) is one of the most financially damaging crime.

Attackers can use a victim’s email as a weapon

It is called: “*Weaponized Compromised Business Email Account*”

It usually starts a phishing email.

Attackers send phish emails to executive level employees to hack their account.

After that, attackers try to deceive other employees using the hacked admin/manager accounts to steal sensitive information or money.
Phishing Scams

In common scams (spam) emails, attackers send thousands of phishing emails to a high number of people.

In these emails, usually, there are no attachments or malicious links, but there are deceptive news or demands.

---

**Choi Teng**

doctor@motenghaiplc.com

**To:** me

MOTENGAII BANK (HK) PLC.
FLOOR 19, OLYMPIAN CITY,
11 HOI FAI ROAD,
WEST KOWLOON, HONGKONG.

Greetings, My names are Mr. Choi Teng and I am the CEO and MD of Motenghai Bank (HK) Plc. I have a business proposal, I want to talk to you about a late client of this bank, a VIP customer of this bank who died leaving behind a dormant bank account containing (15 Billion) Fifteen Billion United States dollars. I want share of 30%.

FULL NAME:
ADDRESS:
TELEPHONE:
DATE OF BIRTH:
COUNTRY:
SEX:
OCCUPATION:
IDENTIFICATION:

Contact me on email address for more details: choiteng@motenghaiplc.com

Sincerely,
Mr. Choi
CEO/MD, Motenghai Bank (HK) Plc.
SEND a test phishing email to our Gmail address from an instant disposable email service: https://www.guerrillamail.com

First: Compose an email and send it.

To: dfirway@gmail.com

Subject: Hi

Hi,
I could not see you in the office today,
Can you check this website out and fill out the form asap per HR request.
skyaccountsbill.com

Thanks.
Phishing Email Investigation

Received.

pozmiX+etm2tBlaK64u4
Hi - Hi, I could not see you in ...
11:47 PM
Phishing Email Investigation

Header Analysis:

Let’s look at its header information by clicking this three dots button.
Phishing Email Investigation

Header Analysis:

After clicking this three dots button:

Click "Show original" Button to see email header info:

***Email Header: The raw data of the email which contains IP addresses

10/22/2021 said_varlioglu@trendmicro.com
Phishing Email Investigation

The summary of the email

Original Header

10/22/2021 | said_varloglu@trendmicro.com
Phishing Email Investigation

If the **Return-Path** is the same with the sender, this is not a spoofed email.

**X-Originating-IP** is the IP address of the real sender.
Phishing Email Investigation

Investigate the IP address

Find the real sender location

AbuseIPDB » 74.132.226.2

74.132.226.2 was not found in our database

- ISP: Charter Communications Inc
- Usage Type: Fixed Line ISP
- Hostname(s): cpe-74-132-226-2.kya.res.rr.com
- Domain Name: spectrum.com
- Country: United States of America
- City: Edgewood, Kentucky
Phishing Email Investigation

Received: by ➔ The email server IP address
Phishing Email Investigation

AbuseIPDB » 168.119.142.36

The email server is in Germany
Phishing Email Investigation

Investigate the suspicious link?

skyaccountsbilli.art
Phishing Email Investigation

Virustotal

It has been reported as a phishing source

The creation date:
4 days ago
Very suspicious!

However, the old websites can be used as phish sources!
Phishing Email Investigation

Verdict: Dangerous

Why?

Let's check more

sitesafety.trendmicro.com
Phishing Email Investigation

VirusTotal

Phishing

Its IP Address: 64.98.145[.]30
Phishing Email Investigation

abuseipdb.com

Phishing

Its IP Address: 64.98.145[.]30

10/22/2021 | said_varloglu@trendmicro.com
VirusTotal

delivers trojans

delivers trojans

skyaccountsbilli[.]art

Click to select

Click to select

... and 62 items more

... and 68 items more

1 / 88 skyaccountsbilli.art
Name: skyaccountsbilli.art
Creation date: 2021-10-17 00:00:00
Last update: 2021-10-17 00:00:00

Detections
G-Data: phishing
Netcraft: malicious
Kaspersky: phishing
Avira: phishing
Webroot: malicious
... and 63 items more

1 / 67 7f6106d564b428289d4d09c31124b3c1d15dd...
Type: Win32 EXE
Size: 246.94 KB
First Seen: 2021-10-20 06:36:32
Last Seen: 2021-10-20 06:36:32
Submissions: 1
File Name: payment
advice_109690121.exe

Detections
Cybereason: malicious.aib36c
BitDefenderTheta: Gen NN.ZeriaF.34218.cq4@aOjwSGl
Fortinet: W32/Injector_AGen AW/tr
SentinelOne: Static AI - Malicious PE
Malwarebytes: Trojan Injector
... and 68 items more
More threat intel:

Twitter threat intel

Fake forums
Email spoofing is the creation of email messages with a forged sender address.

It is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source.

This is very common in cases of CEO/CFO fraud.

Attackers can use the exact email address to send an email by

– e.g. from “info@amazon.com” (it is actually not from this address)

or they can change the well-known email domains by erasing a letter:

– e.g. “info@amzn.com” instead of “info@amazon.com”. 
Spoofed Email Investigation

Let’s send a test spoofed email to our Gmail address from a free spoofed email service:

http://www.sendanonymousemail.net/
Spoofed Email Investigation

Fake sender
Spoofed Email Investigation

Email Server IP

- Message ID: <20211022013851.0EE87180FED@emkei.cz>
- Created at: Thu, Oct 21, 2021 at 9:38 PM (Delivered after 0 seconds)
- From: Christiana Ronaldo <Christiana.Ronaldo@manchestercity.com>
- To: dfirway@gmail.com
- Subject: Do you want to play in MCity
- SPF: NEUTRAL with IP 101.99.94.116 Learn more
Spooofed Email Investigation

Spoof email service

101.99.94.116 was found in our database!
This IP was reported 1 times. Confidence of Abuse is 5%:

ISP: Shinjiru Technology Sdn Bhd
Usage Type: Data Center/Web Hosting/Transit
Hostname(s): emkei.cz
Domain Name: shinjiru.com.my
Country: Malaysia
City: Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur
How to Know If Your Email Has been Hacked? **GMAIL**

**Investigate:**

**Gmail Last Sign Ins**

In Gmail, you can see the last sign-in activities using “Details” button that is in the bottom of the page.
Investigate:

Gmail Last Sign Ins

Visit Security Checkup for more details
How to Know If Your Email Has been Hacked? OUTLOOK

Investigate:

In Outlook, to see your recent activity, follow the steps below:

1- My Account

2- My Sign-ins – Review Recent Activity
How to Know If Your Email Has been Hacked?

Investigate:

Outlook

1. **Location:**
   - Kentucky, US
   - Operating System: Windows 10
   - Browser: Google Chrome
   - IP Address: 24.166.238.99
   - Account: varioms@mail.uc.edu
   - Last sign-in: Today at 2:59:38 AM CST

2. **Location:**
   - Texas, US
   - Operating System: Windows 10
   - Browser: Google Chrome
   - IP Address: 64.198.32.41
   - Account: varioms@mail.uc.edu
   - Last sign-in: Last Thursday at 11:01:05 PM CST
How to Know If Your Email Has been Hacked? **OUTLOOK**

**Investigate:**

**Outlook Email Inbox Rule Investigation**

1). Set up a search rule.

2). Open the Rules section to create new rules.
How to Know If Your Email Has been Hacked? OUTLOOK

Outlook Email Inbox Rule

The attackers exploit this feature frequently in phishing campaigns.

In this example rule,

- It deletes all the coming messages.
- It also marks all the coming messages as read.
- The attacker may use only “.” (a dot) or “inbox rule” for the rule name to hide the rule.
- Some attackers forward the emails to themselves before delete function.
- The victim never receive emails.
Scenario

- Received more than **50 Phish Alerts** from the users
- The phishing emails come from an **employee account**
- An employee account have been **compromised and weaponized**

**What will we do?**

Let’s **respond** this incident on Office365
“Incidents can’t always be prevented but must always be detected.”
Incident Response on Office365

**Identification**

- ✓ Detect the compromised account
- ✓ Identify the incident start time
- ✓ Find the malicious IP of the attacker
- ✓ Check the inbox and forwarding rules
Incident Response on Office365

Image from https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins
Incident Response on Office365

Image from https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins
Incident Response on Office365

Containment & Eradication & Recovery

✓ Reset the password
✓ Signed out all sessions
✓ Blocked the malicious IP of the attacker
✓ Blocked the malicious URL
✓ Delete malicious inbox and forwarding rules
✓ Search and Destroy all malicious emails
✓ Detect who clicked the malicious links
✓ Notify all recipients about the phishing campaign
✓ Identify whether there is another account was touched by the malicious IP
Incident Response on Office365

Containment & Eradication & Recovery

✓ Set a new password for compromised account

```powershell
PS C:\> Set-ADAccountPassword -Identity <USERNAME> -server <DOMAINNAME> -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "<NEWPASSWORD>") -Force -credential <ADMINUSERNAME>
```
Incident Response on Office365

Containment & Eradication & Recovery

✓ Signed out all sessions

```powershell
PS C:\> Connect-AzureAD
PS C:\> Get-AzureADUser -SearchString <EMAILADDRESS> | Revoke-AzureADUserAllRefreshToken
PS C:\>
```
Containment & Eradication & Recovery

Search and Destroy all malicious phishing emails

1- Go to Office 365 Security & Compliance - https://protection.office.com/contentsearchbeta?ContentOnly=1

2- Open Search → Search button

3- Search Phishing Emails with a query
   - Sender address
   - If the sender address is spoofed or multiple phishers exist, use keywords from the body text

4. Run the Windows PowerShell as the Administrator and Connect to Office 365 PowerShell via

   $SccSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
   https://ps.compliance.protection.outlook.com/powershell-liveid/ -Credential $credential -Authentication "Basic" -AllowRedirection
   Import-PSSession $SccSession -Prefix cc

6. Connect to Security & Compliance Center via

   $UserCredential = Get-Credential
   $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
   Import-PSSession $Session

7. Delete Emails that have been found on the Content Search with Search Name

   New-ComplianceSearchAction -SearchName "THE_SEARCH_NAME" -Purge -PurgeType SoftDelete

8. Confirm Delete
   Y
INCIDENT RESPONSE CHECKLIST

Phishing Emails from Internal Compromised/Weaponized Account

- Detect the compromised account and the incident time
- Reset the password of the compromised account
- Sign out all sessions of the compromised account
- Search and destroy the phishing emails from the weaponized account
- Block the malicious links
- Check and delete the malicious inbox rules
- Check the sign-in logs of the compromised account to detect the malicious IP addresses
- Check other activities with the malicious IP addresses
- Detect and notify the users who took the link
- Keep monitoring the compromised account
- Keep monitoring the users who took the link
- Keep monitoring attacker IPs and locations
- Keep monitoring the similar IPs and locations
- Observe the patterns of the attacks
- Checked the similar attack vectors
Increase Phishing Awareness

Free Phishing Simulation Platform

Increase Phishing Awareness

Thank You!

said_varlioglu@trendmicro.com