Phishing Email Analysis & Incident Response

Title

Phishing Email Analysis using Open-Source Intelligence Tools

Objective

To analyze a suspicious email, extract indicators of compromise (IOCs), validate them using threat intelligence tools, map the attack to the MITRE ATT&CK framework, and create an incident response report.

Tools Used

- Notepad (Email sample creation)
- Virus Total (URL reputation analysis)
- WHOIS Lookup (Domain registration analysis)
- MITRE ATT&CK Framework
- Microsoft Word / Google Docs (Report preparation)

Attack Scenario

A suspicious email was received claiming that the user's account would be suspended unless immediate verification was completed. The email contained a suspicious sender address and a link directing the user to a fake login page.

Email Sample

Sender:

security-update@paypa1.com

Subject:

Urgent: Account Verification Required

Email Content:

Dear Customer,

We detected suspicious activity in your account.

Your account will be permanently suspended unless you verify your details.

Click the link below to verify:

http://paypal-security- check.com/login

Thank you,

PayPal Security Team

Email Analysis

Sender Analysis

- Sender domain: **paypa1.com**
- Uses the number **“1” instead of the letter “l”**
- This is a **typo squatting technique**

Conclusion: Suspicious and likely malicious.

Subject Line Analysis

- Contains urgency: *“Urgent: Account Verification Required”*
- Creates fear and pressure

Conclusion: Social engineering tactic.

Link Analysis

Suspicious link:

paypal-security-check.com

Reasons:

- Not an official PayPal domain
- Uses security-related wording to appear legitimate

Conclusion: Likely phishing URL.

Indicators of Compromise (IOCs)

IOC Type	Value
Sender Email	security-update@paypa1.com
Suspicious Domain	paypa1.com
Phishing URL	paypal-security-check.com

Virus Total Analysis

The suspicious domain was scanned using Virus Total.

Result:

11/94 security vendors flagged this URL as malicious and phishing.

Conclusion:
Multiple security vendors detected the domain as phishing.

WHOIS Analysis

A WHOIS lookup was performed on the domain:

paypal-security-check.com

Observations

- Domain was recently created
- Registrant information was hidden
- Short registration duration

Conclusion

Recently created domains with hidden ownership are commonly associated with phishing campaigns.

Attack Classification

Based on the analysis:

- Fake sender domain
- Urgent social engineering message
- Malicious link
- Suspicious WHOIS details

Attack Type:

Phishing

MITRE ATT&CK Mapping

Tactic:

Initial Access

Technique ID:

T1566

Technique Name:

Phishing

Explanation

The attacker attempted to gain initial access by sending a fraudulent email containing a malicious link designed to steal user credentials.

Severity Assessment

Severity Level: Medium

Reason

- Phishing attempt confirmed
- No evidence of successful compromise
- Potential risk if user had clicked the link

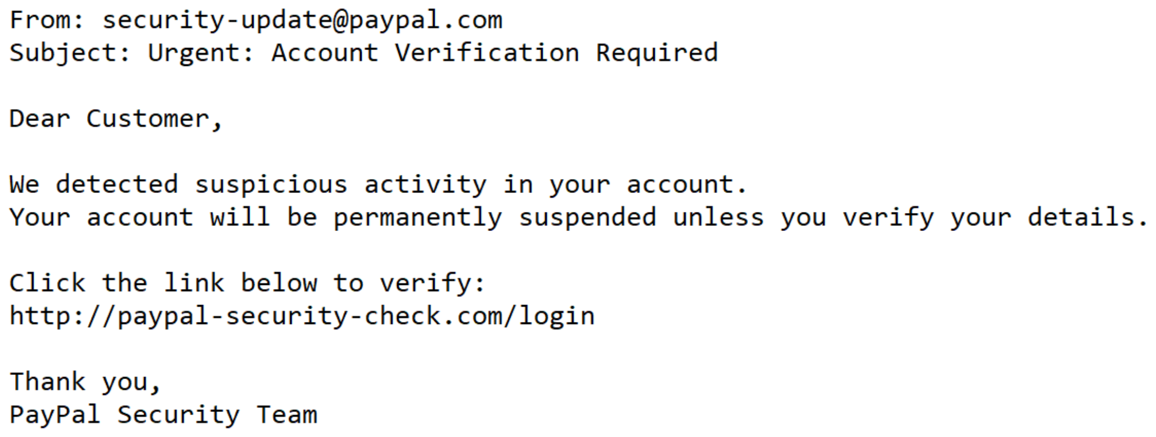
Recommended Response Actions

1. Block the malicious domain at the firewall and email gateway.
2. Remove the phishing email from all user inboxes.
3. Conduct phishing awareness training for users.
4. Enable multi-factor authentication (MFA).
5. Improve email filtering and spam detection policies.

Conclusion

The suspicious email was identified as a phishing attempt using a fake sender address and a malicious domain. Threat intelligence analysis confirmed the domain’s suspicious nature. The attack was mapped to the MITRE ATT&CK framework under technique T1566 (Phishing). Appropriate response actions were recommended to prevent similar incidents.

Email Sample



```
From: security-update@paypal.com
Subject: Urgent: Account Verification Required

Dear Customer,

We detected suspicious activity in your account.
Your account will be permanently suspended unless you verify your details.

Click the link below to verify:
http://paypal-security-check.com/login

Thank you,
PayPal Security Team
```

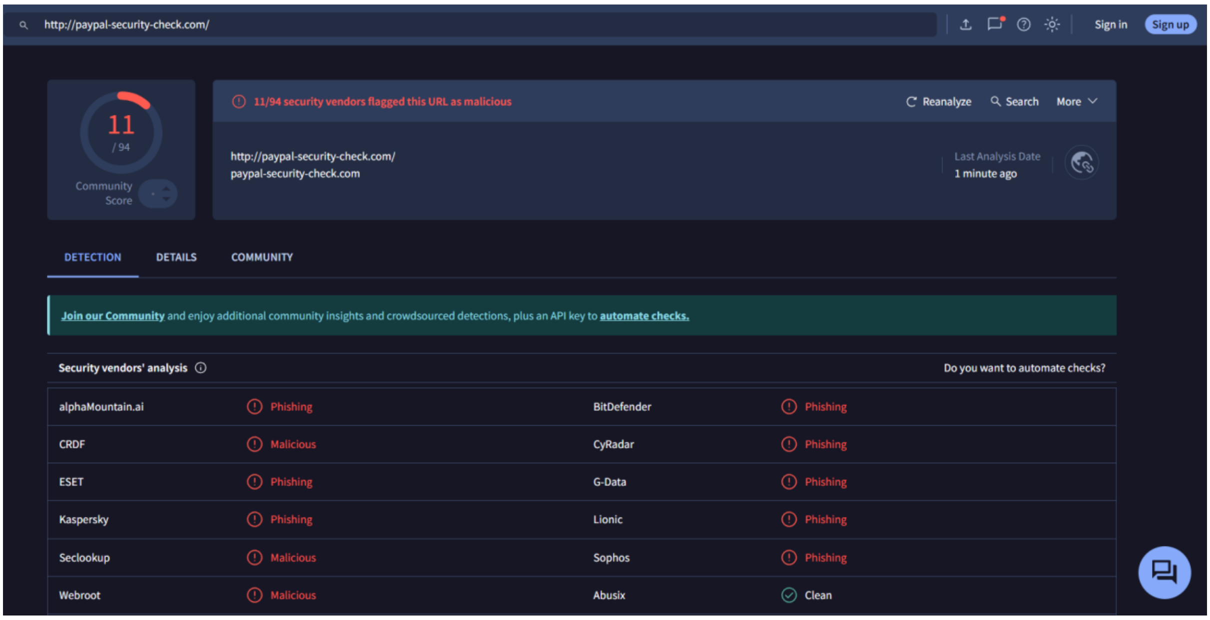
This email shows the suspicious link and email id.

IOC Extraction

IOC Type	Value
Sender email	security-update@paypa1.com
Suspicious domain	paypa1.com
Phishing URL	paypal-security-check.com

The email was analyzed to extract indicators of compromise such as the sender address, suspicious domain, and phishing URL. The sender domain used a typosquatting technique, and the embedded link directed to a non-legitimate website. These indicators confirmed that the email was part of a phishing attempt.

Virustotal Result



11/94 security vendors flagged this URL as malicious

http://paypal-security-check.com/
paypal-security-check.com

Last Analysis Date
1 minute ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

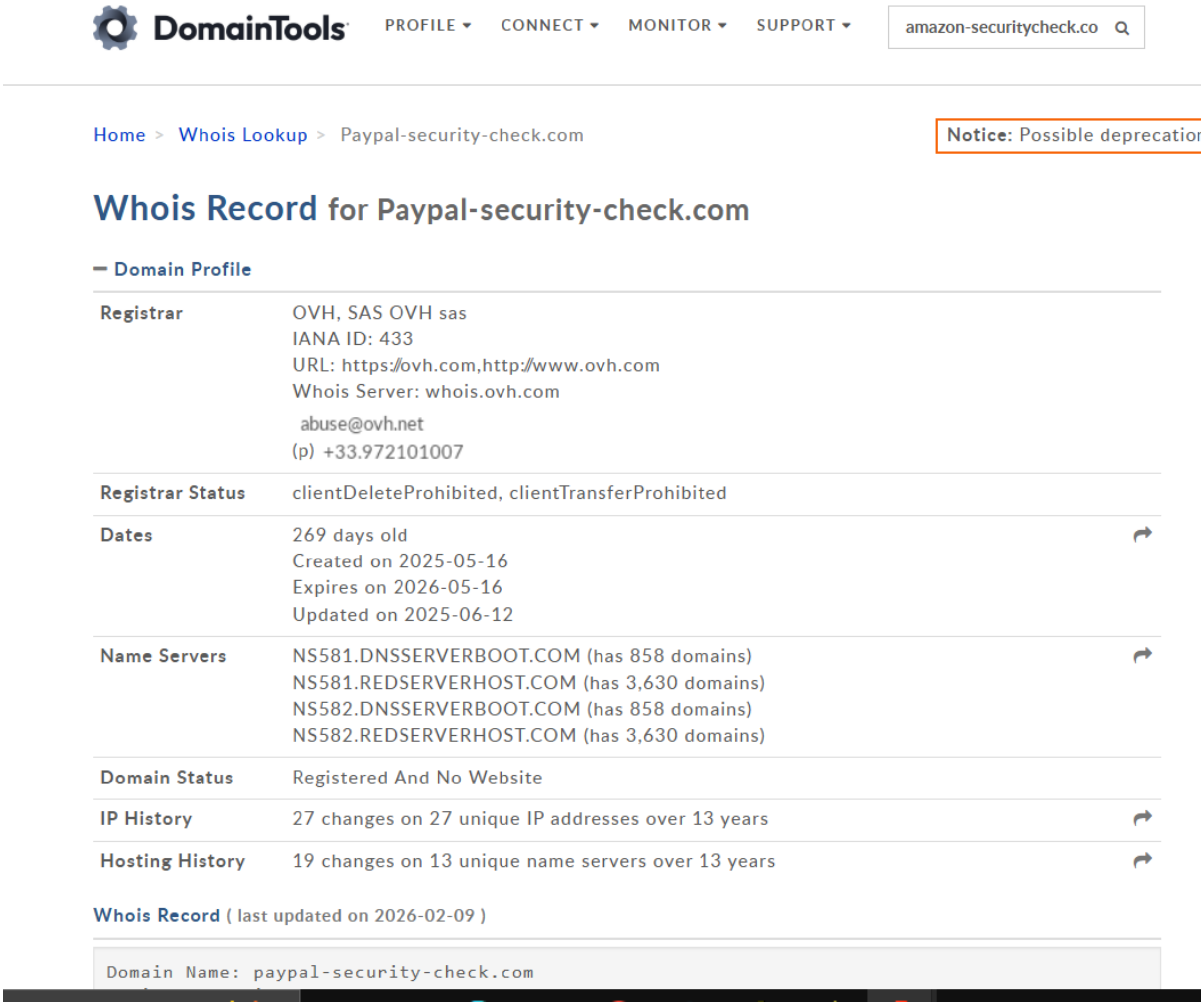
Security vendors' analysis ⓘ

Do you want to automate checks?

alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Phishing
CRDF	ⓘ Malicious	CyRadar	ⓘ Phishing
ESET	ⓘ Phishing	G-Data	ⓘ Phishing
Kaspersky	ⓘ Phishing	Lionic	ⓘ Phishing
Seclookup	ⓘ Malicious	Sophos	ⓘ Phishing
Webroot	ⓘ Malicious	Abusix	✓ Clean

The scanned VirusTotal shows us that the given URL is used for phishing methods.

WHOIS Analysys.



Home > Whois Lookup > Paypal-security-check.com

Notice: Possible deprecatior

Whois Record for Paypal-security-check.com

− Domain Profile

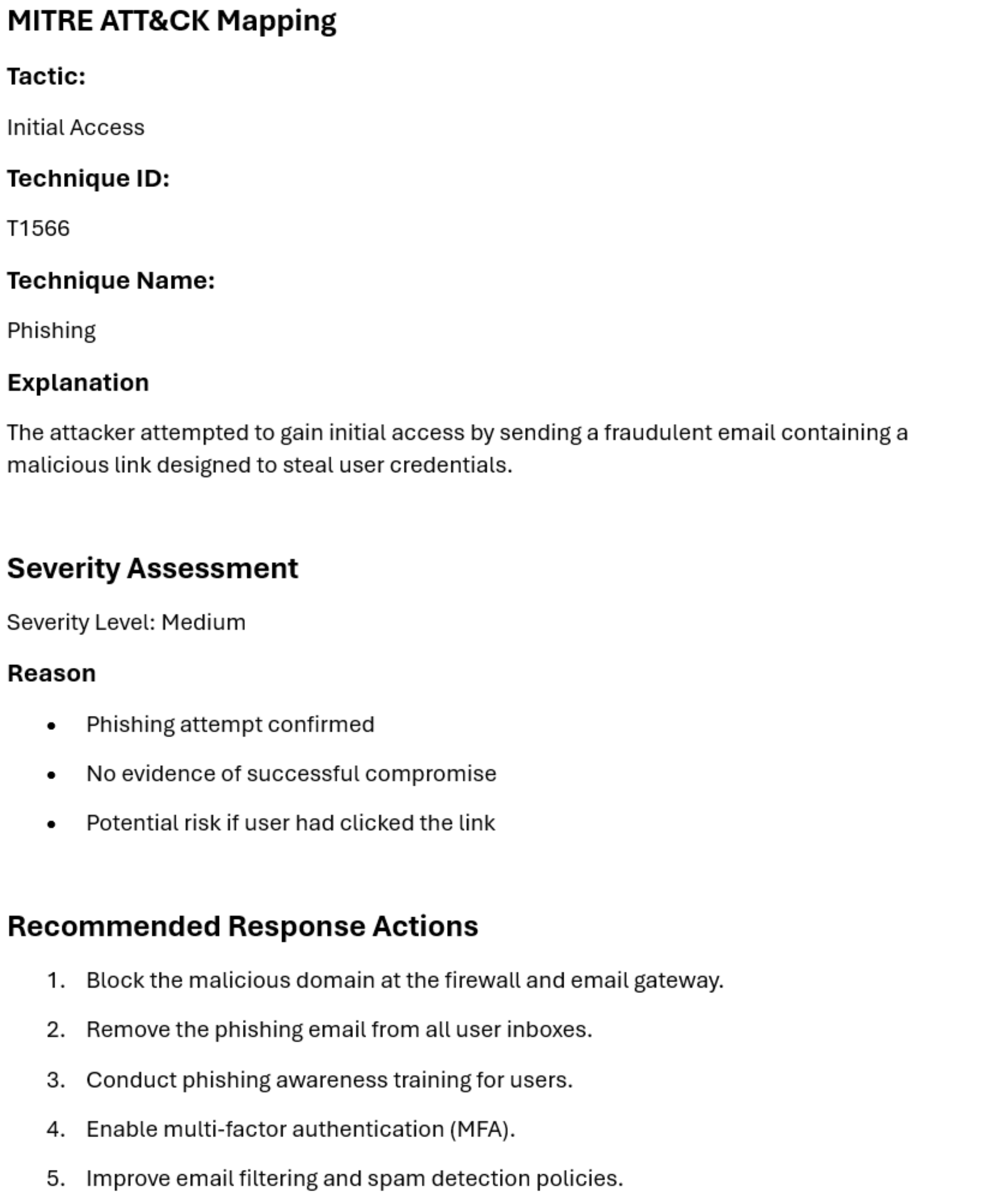
Registrar	OVH, SAS OVH sas IANA ID: 433 URL: https://ovh.com,http://www.ovh.com Whois Server: whois.ovh.com abuse@ovh.net (p) +33.972101007
Registrar Status	clientDeleteProhibited, clientTransferProhibited
Dates	269 days old Created on 2025-05-16 Expires on 2026-05-16 Updated on 2025-06-12
Name Servers	NS581.DNSSERVERBOOT.COM (has 858 domains) NS581.REDSERVERHOST.COM (has 3,630 domains) NS582.DNSSERVERBOOT.COM (has 858 domains) NS582.REDSERVERHOST.COM (has 3,630 domains)
Domain Status	Registered And No Website
IP History	27 changes on 27 unique IP addresses over 13 years
Hosting History	19 changes on 13 unique name servers over 13 years

Whois Record (last updated on 2026-02-09)

```
Domain Name: paypal-security-check.com
```

This clearly describes the date created, server names and IP history and the registrar names as well for the domain.

Final Report



MITRE ATT&CK Mapping

Tactic:

Initial Access

Technique ID:

T1566

Technique Name:

Phishing

Explanation

The attacker attempted to gain initial access by sending a fraudulent email containing a malicious link designed to steal user credentials.

Severity Assessment

Severity Level: Medium

Reason

- Phishing attempt confirmed
- No evidence of successful compromise
- Potential risk if user had clicked the link

Recommended Response Actions

1. Block the malicious domain at the firewall and email gateway.
2. Remove the phishing email from all user inboxes.
3. Conduct phishing awareness training for users.
4. Enable multi-factor authentication (MFA).
5. Improve email filtering and spam detection policies.

The email was analyzed to extract indicators of compromise such as the sender address, suspicious domain, and phishing URL. The sender domain used a typosquatting technique, and the embedded link directed to a non-legitimate website. These indicators confirmed that the email was part of a phishing attempt.