Author: Jack Fitzgerald

Official Incident Report

Date: Sep, 17, 2024, 12:05 PM

Event ID: 304

Rule Name: SOC326 - Impersonating Domain MX Record Change Detected

Table of Contents

Alert Details

Severity: Medium

Type: ThreatIntel

Source Address: no-reply@cti-report.io

Destination Address: soc@letsdefend.io

Subject: Impersonating Domain MX Record Change Detected

Trigger Reason: The MX record of a suspicious domain was changed, suggesting potential phishing activity.

Domain: letsdefwnd[.]io

Mx_record: mail.mailerhost[.]net

Device Action: Allowed

Based on the information provided in the alert, it appears there has been a detected **Domain MX Record** change of a **suspicious domain**, that could see potential for **targeted phishing activity**. The alert is triggered by rule SOC326 - Impersonating Domain MX Record Change Detected.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

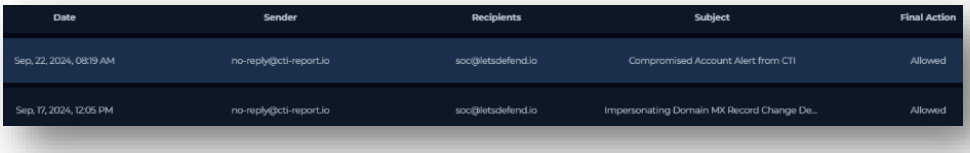
Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

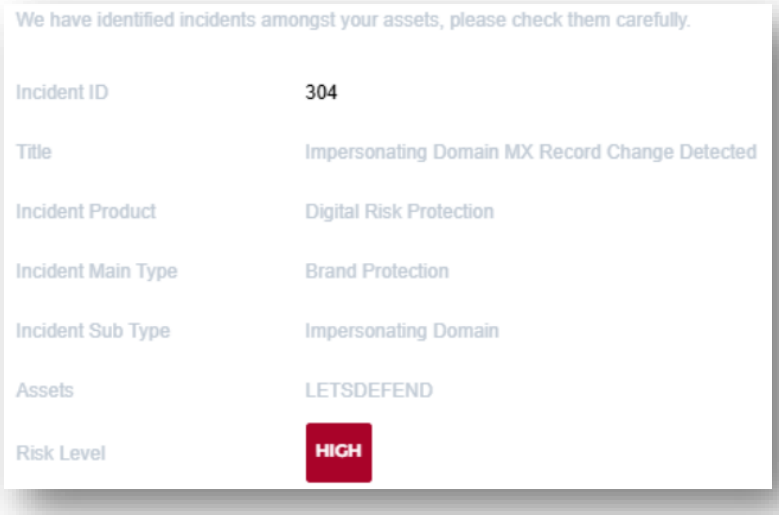
We need to investigate emails for potential security issues and check for any related phishing activity after the alert creation date.

2 emails were found being sent from **no-reply@cti-report.io** to **soc@letsdefend.io**.



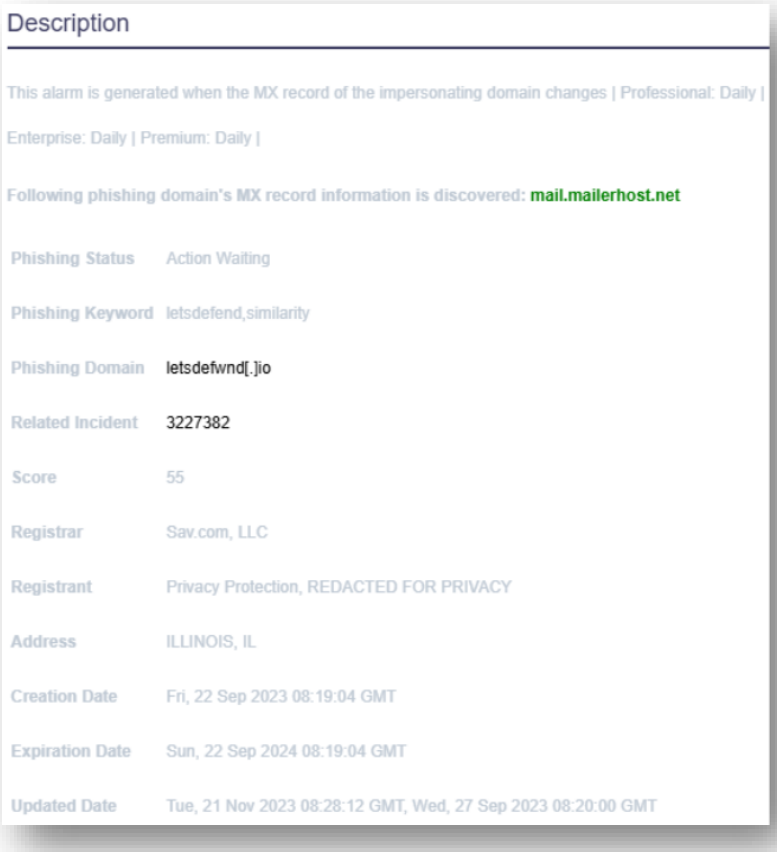
Date	Sender	Recipients	Subject	Final Action
Sep, 22, 2024, 08:19 AM	no-reply@cti-report.io	soc@letsdefend.io	Compromised Account Alert from CTI	Allowed
Sep, 17, 2024, 12:05 PM	no-reply@cti-report.io	soc@letsdefend.io	Impersonating Domain MX Record Change De...	Allowed

The first email was on Sep 17, 2024, 12:05 PM.



We have identified incidents amongst your assets, please check them carefully.

Incident ID	304
Title	Impersonating Domain MX Record Change Detected
Incident Product	Digital Risk Protection
Incident Main Type	Brand Protection
Incident Sub Type	Impersonating Domain
Assets	LETSDEFEND
Risk Level	HIGH



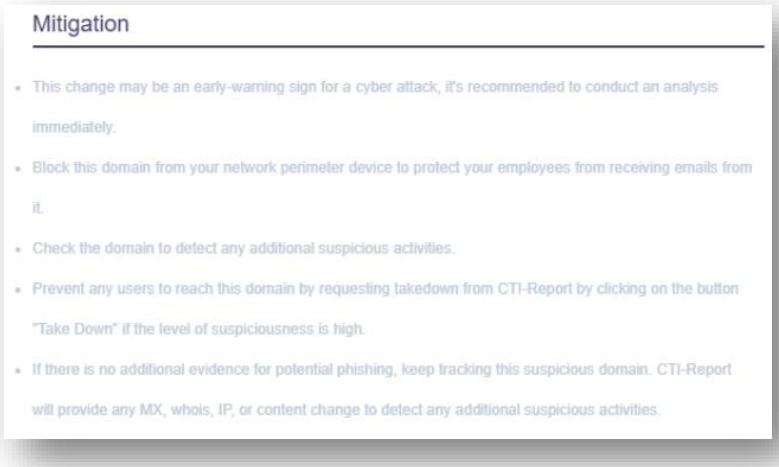
Description

This alarm is generated when the MX record of the impersonating domain changes | Professional: Daily | Enterprise: Daily | Premium: Daily |

Following phishing domain's MX record information is discovered: **mail.mailerhost.net**

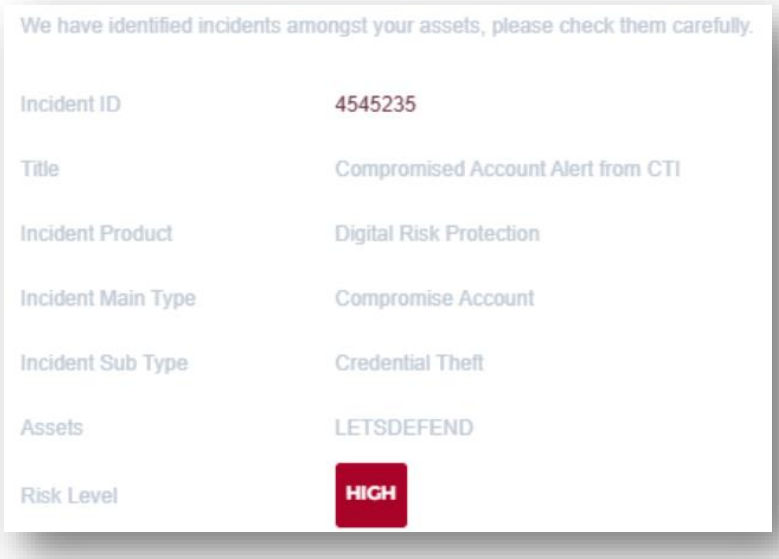
Phishing Status	Action Waiting
Phishing Keyword	letsdefend,similarity
Phishing Domain	letsdefwnd[.]io
Related Incident	3227382
Score	55
Registrar	Sav.com, LLC
Registrant	Privacy Protection, REDACTED FOR PRIVACY
Address	ILLINOIS, IL
Creation Date	Fri, 22 Sep 2023 08:19:04 GMT
Expiration Date	Sun, 22 Sep 2024 08:19:04 GMT
Updated Date	Tue, 21 Nov 2023 08:28:12 GMT, Wed, 27 Sep 2023 08:20:00 GMT

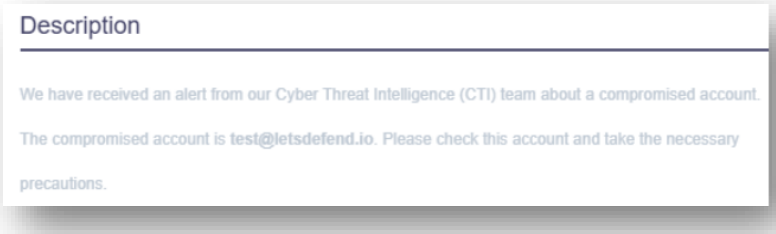
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
DNS Records	ns2.giantpanda.com, ns1.giantpanda.com
State	NOT PARKED
IP Addresses	72.14.178.174,45.33.30.197,72.14.185.43,173.255.194.134,45.79.19.196,45.56.79.23,96.126.123.244,45.33.20.235,45.33.18.44,45.33.2.79,198.58.118.167,45.33.23.183
MX Records	mail.mailerhost.net

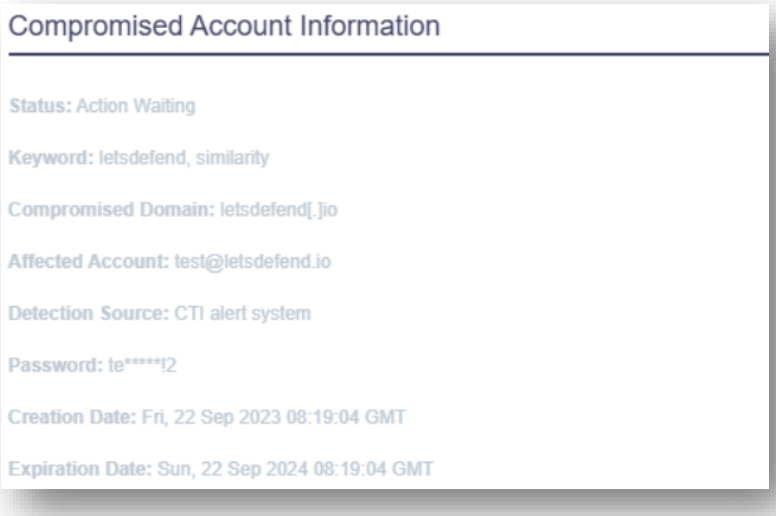


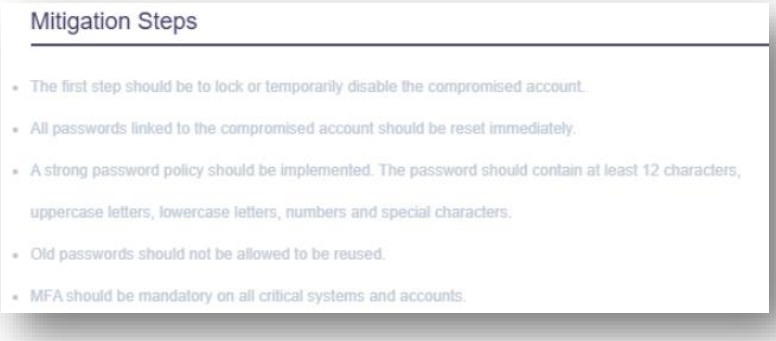
This is the original email informing **letsdefend** of the **MX Record change** for **mail.mailerhost.net**, and to be on the lookout for any **potential phishing activities**.

The second email on Sep 22, 2024, 08:19 AM.



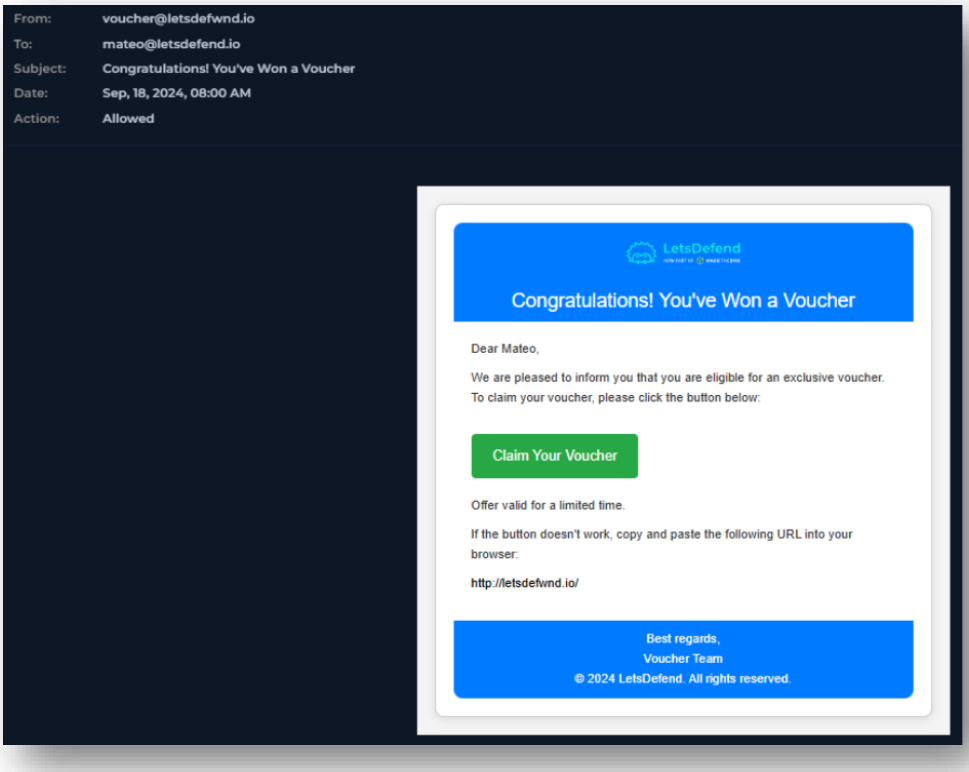






This is a follow-up email from **CTI** informing **letsdefend** that their **test@letsdefend.io** account has been **compromised**, resulting in **credential theft**, presumably following **suspicious phishing activity** coming from **mail.mailerhost.ne**t.

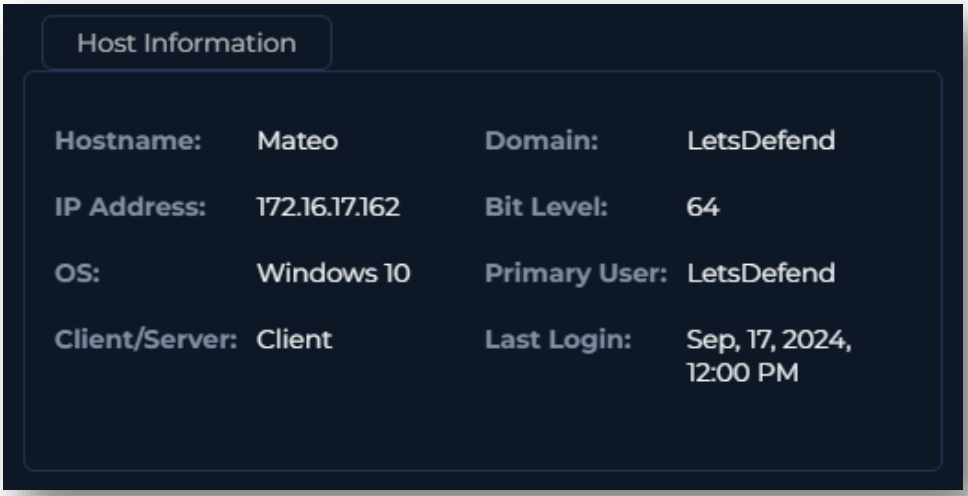
We found the phishing email from **voucher@letsdefwnd.io** to **mateo@letsdefend.io**, offering a **free letsdefend voucher**.



The email contains a link directing the user to **http://letsdefwnd.io/**, **impersonating the letsdefend.io domain**.

Analysis

Now that we have detected that attack, we can begin the analysis by investigating Endpoint Security.



After investigating Browser History, we found that Mateo **accessed** the **phishing email link**, directing the user to **http://www.letsdefwnd.io/**.

Next, we investigate Network Action, where we find 2 IP addresses of interest, and analyse them using **VirusTotal**, the third address being a **link-local** address.

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Sep 18 2024 01:32:09	23.44.17.219
Sep 18 2024 01:32:13	45.33.23.183
Sep 18 2024 01:32:39	169.254.169.254

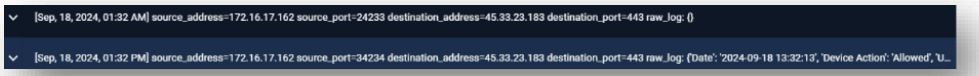
https://www.virustotal.com/gui/ip-address/45.33.23.183

3/95 security vendors flagged this IP address as malicious

https://www.virustotal.com/gui/ip-address/23.44.17.219

8 detected files communicating with this IP address

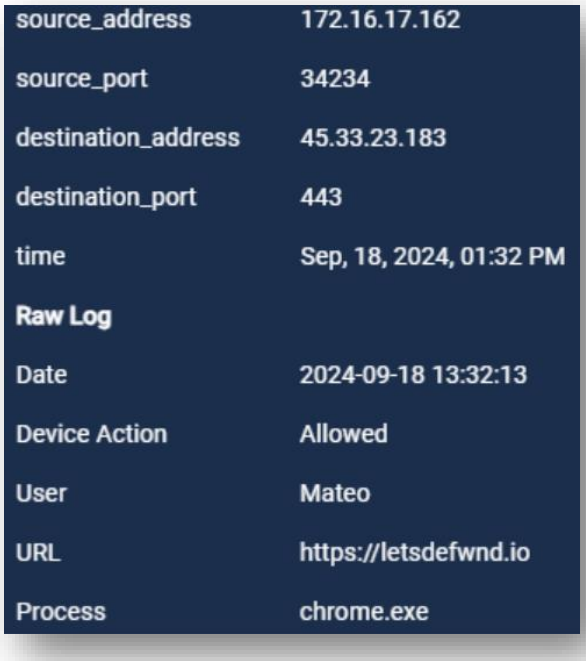
Next, we investigate Log Management, where 2 events were found to originate from the **Mateo** host machine **172.16.17.162**.



Mateo's host machine is found to be accessing the malicious IP address **45.33.23.183** on Sep 18, 2024, 01:32 AM.

Field	Value
type	Firewall
source_address	172.16.17.162
source_port	24233
destination_address	45.33.23.183
destination_port	443
time	Sep, 18, 2024, 01:32 AM

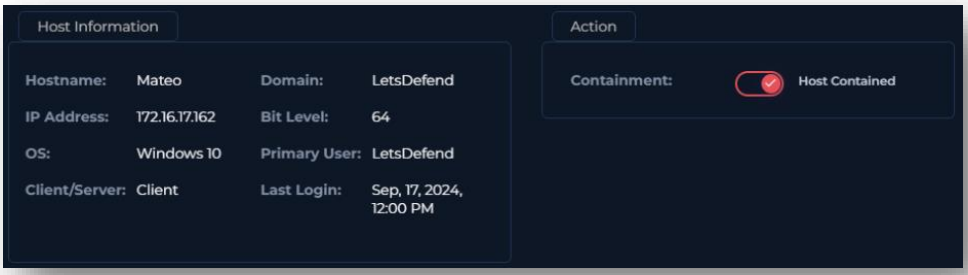
Mateo's host machine is found to have accessed **https://letsdefwnd.io** via chrome.exe at the same time.



source_address	172.16.17.162
source_port	34234
destination_address	45.33.23.183
destination_port	443
time	Sep, 18, 2024, 01:32 PM
Raw Log	
Date	2024-09-18 13:32:13
Device Action	Allowed
User	Mateo
URL	https://letsdefwnd.io
Process	chrome.exe

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.



Summary

The incident involves a compromised system named **Mateo** with an IP address of **172.16.17.162**. The alert was triggered by the identification of a suspicious hash on the host, based on the rule SOC326 - Impersonating Domain MX Record Change Detected.

Upon further analysis, it was discovered that **CTI** sent a **warming email** to letsdefend informing of an **MX record change** to **letsdefwnd.io** at Sep, 17, 2024, 12:05 PM.

At Sep, 18, 2024, 08:00 AM, **voucher@letsdefwnd.io** sent a **spearphishing** email to **mateo@letsdefend.io** directing the user to **http://letsdefwnd.io** to **claim a free voucher**.

At Sep, 18, 2024, 01:32 PM, Mateo **accessed** the link, directing the user to **45.33.23.183**, where **credentials were stolen**, using a **fake login page impersonating letsdefend.io**.

Based on the findings of the incident, immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Attackers shift from forging your exact domain to using deceptive look-alikes (typosquatting, homoglyphs, extra characters) and exploiting DNS flaws once DMARC blocks direct spoofing

- Users clicking malicious links or interacting with deceptive emails are often the entry point, highlighting training needs

Remediation Actions

- Use tools to scan for look-alike domains (typosquatting, different TLDs, Internationalized Domain Names - IDNs) that mimic yours

- Regularly review all DNS records (MX, SPF, TXT, wildcards) for your primary and dormant domains

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1598.003 - Spearphishing Link
Initial Access	T1566 - Phishing
Defense Evasion	T1656 - Impersonation

Artifacts

Value	Comment	Type
http://letsdefwnd.io	URL contained in the phishing email	URL Address
voucher@letsdefwnd.io		E-mail Sender
letsdefwnd.io	Impersonating letsdefend.io domain	E-mail Domain
45.33.23.183	C2 Traffic accessed	IP Address

LetsDefend Playbook

LetsDefend Event ID: 304