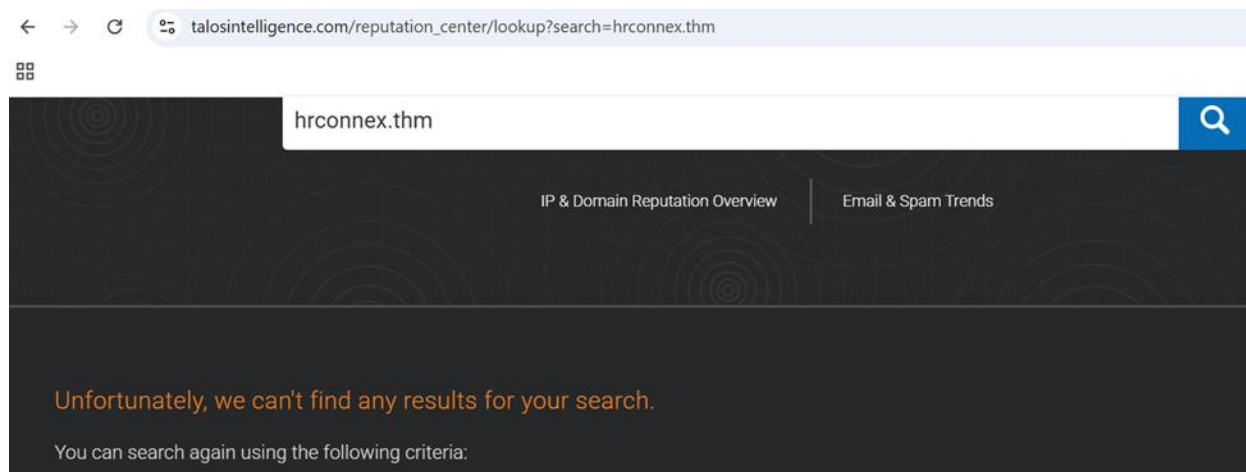


SOC Simulator — Tryhackme — Introduction to Phishing — Write-up

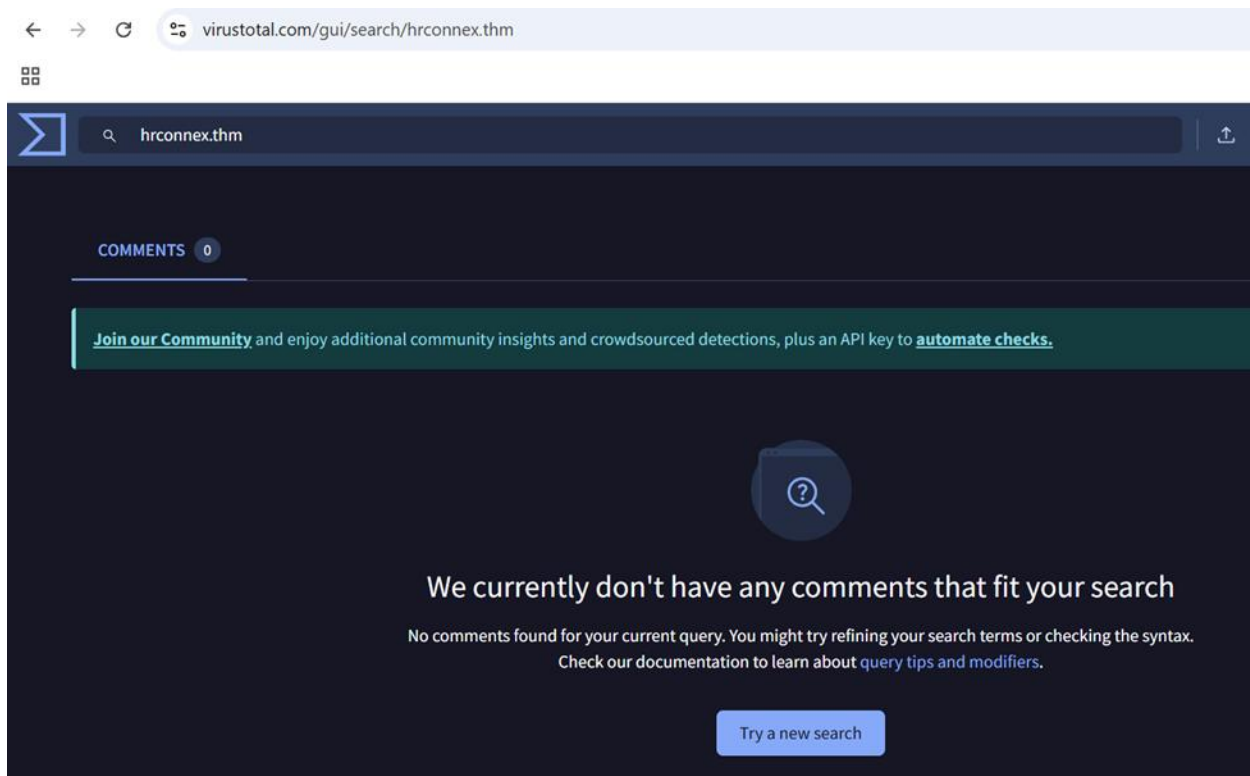
Press enter or click to view image in full size

8814	Inbound Email Containing Suspicious External Link	^	Medium	Phishing	Sep 19th 2025 at 08:30	👤-
Description:		This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.				
datasource:		email				
timestamp:		09/19/2025 08:28:01.001				
subject:		Action Required: Finalize Your Onboarding Profile				
sender:		onboarding@hrconnex.thm				
recipient:		j.garcia@thetrydaily.thm				
attachment:		None				
content:		Hi Ms. Garcia,\n\nWelcome to TheTryDaily!\n\nAs part of your onboarding, please complete your final profile setup so we can configure your access.\n\nKindly click the link below:\n\nSet Up My Profile.\n\nIf you have questions, please reach out to the HR Onboarding Team.				
direction:		inbound				

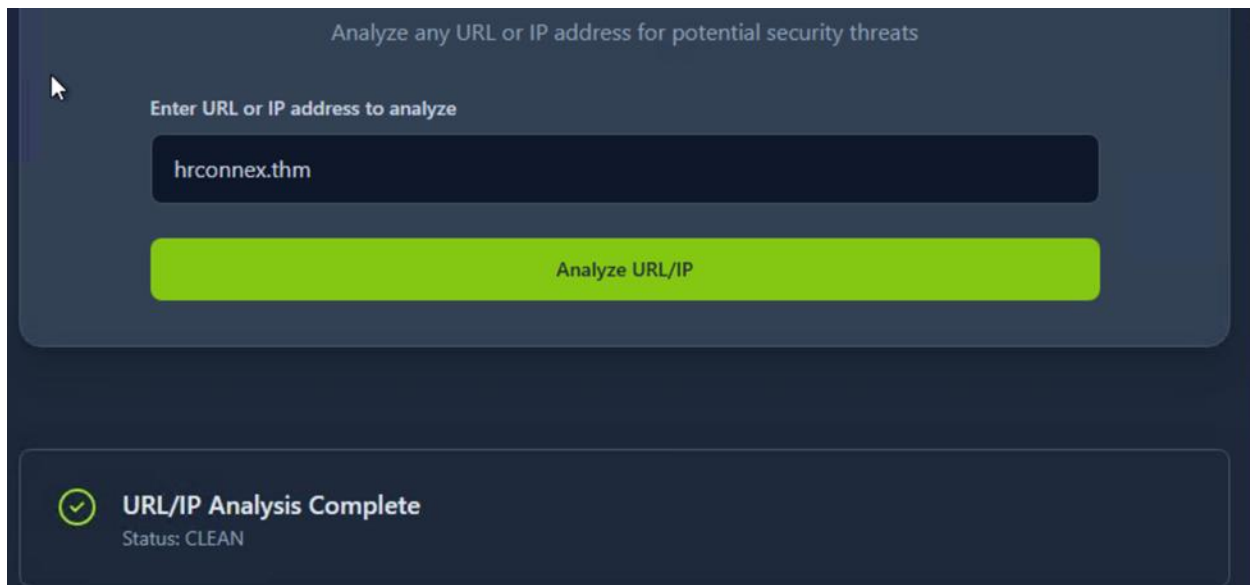
Press enter or click to view image in full size



Press enter or click to view image in full size



Press enter or click to view image in full size



Summary: Incident 1: False Positive Phishing Alert

- **Alert ID:** 8814
- **Initial Classification:** Medium

- **Summary:** An inbound email was flagged as a potential phishing attempt due to a suspicious external link. The email was sent to an employee,
- j.garcia@thetrydaily.thm, from onboarding@hrconnex.thm with the subject "Action Required: Finalize Your Onboarding Profile". The link directed the user to
- <https://hrconnex.thm/onboarding/15400654060/j.garcia.>
- **Investigation:** Using Open-Source Intelligence (OSINT) tools such as Cisco Talos and VirusTotal and Tryhackme's Security Check, I analyzed the domain hrconnex.thm. None of the security checks or threat intelligence feeds flagged the URL as malicious. The email's content and the context of a new hire's onboarding process confirmed it was a legitimate communication.
- **Conclusion:** The alert was classified as a **false positive**. No further action was required, as the email was a routine business communication. This highlights the importance of thorough investigation beyond automated flagging to prevent unnecessary alerts.
- Here is the full case report for this alert:
- **5Ws:**
- **Who:** The email was sent from onboarding@hrconnex.thm to j.garcia@thetrydaily.thm.
- **What:** An inbound email containing a link prompting the recipient to complete their onboarding profile.
- **When:** September 19th, 2025 at 10:18 AM.
- **Where:** Delivered to TheTryDaily's email system.
- **Why:** The email triggered a phishing alert because it contained an external link, which can sometimes indicate suspicious activity.

Details:

The alert initially raised concern due to the presence of an external link in the email. After investigating with OSINT tools (urlscan.io, VirusTotal, Cisco Talos) and running a check through TryHackMe's security scanner, there were no indications of malicious activity. The link is legitimate and part of the recipient's expected onboarding process.

- **Time of Activity:** 09/19/2025 10:18:27
- **Related Entities:** j.garcia@thetrydaily.thm, onboarding@hrconnex.thm, hrconnex.thm
- **Reason for Classifying as False Positive:** The email content is consistent with routine onboarding communications, and none of the security tools flagged it as malicious.

Conclusion:

No further action is required. The alert is considered a false positive.

Press enter or click to view image in full size

8815

Inbound Email Containing Suspicious External Link

Medium

Phishing

Sep 19th 2025 at 08:31

Description:

This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

datasource:

email

timestamp:

09/19/2025 08:29:10.001

subject:

Your Amazon Package Couldn't Be Delivered – Action Required

sender:

urgents@amazon.biz

recipient:

h.harris@thetrydaily.thm

attachment:

None

content:

Dear Customer,\n\nWe were unable to deliver your package due to an incomplete address.\n\nPlease confirm your shipping information by clicking the link below:\n\nhttp://bit.ly/3sHkX3da12340\n\nIf we don't hear from you within 48 hours, your package will be returned to sender.\n\nThank you,\n\nAmazon Delivery

direction:

inbound

Press enter or click to view image in full size

http://bit.ly/3sHkX3da12340

0

/ 98

Community Score

No security vendors flagged this URL as malicious

Reanalyze

Search

http://bit.ly/3sHkX3da12340

bit.ly

Status404

Content typetext/html

Last Analysis Date3 days ago

text/html

trackers

external-resources

DETECTION

DETAILS

COMMUNITY7

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 auto

Abusix

Clean

Acronis

Clean

ADMINUSLabs

Clean

AILabs (MONITORAPP)

Clean

Press enter or click to view image in full size

67.199.248.10 Public Scan Add Verdict Report

Submitted URL: <http://bit.ly/3sHkX3da12340>
Effective URL: <https://bit.ly/3sHkX3da12340>
Submission: On September 19 via manual (September 19th 2025, 8:00:08 am UTC) from — Scanned from

[Summary](#) [HTTP 7](#) [Redirects](#) [Links 3](#) [Behaviour](#) [Indicators](#) [Similar](#) [DOM](#) [Content](#) [API](#) [Verdicts](#)

Summary

This website contacted 2 IPs in 1 countries across 2 domains to perform 7 HTTP transactions. The main IP is 67.199.248.10, located in United States and belongs to GOOGLE-CLOUD-PLATFORM, US. The main domain is bit.ly. The Cisco Umbrella rank of the primary domain is 7476. TLS certificate: Issued by DigiCert EV RSA CA G2 on March 26th 2025. Valid for: a year.

bit.ly scanned 10000+ times on urlscan.io Show Scans: 10000+

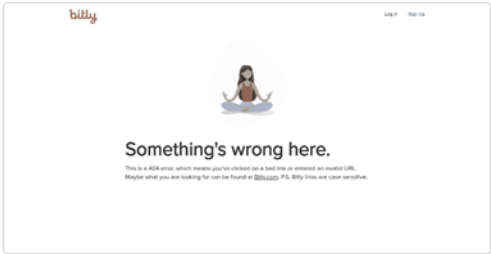
urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for bit.ly
Current DNS A record: 67.199.248.10 (AS396982 - GOOGLE-CLOUD-PLATFORM, US)

Screenshot

Live screenshot Full Image




Page Title
Bitly | Page Not Found | 404

Domain & IP information


Press enter or click to view image in full size

Analyze any URL or IP address for potential security threats

Enter URL or IP address to analyze



Analyze URL/IP

 **URL/IP Analysis Complete**
Status: MALICIOUS

Incident 2: True Positive Phishing Alert & Firewall Block

This incident involved a two-part investigation that confirmed a successful phishing attempt blocked by our security defenses.

Part A: Inbound Phishing Email

- **Alert ID:** 8815
- **Initial Classification:** Medium
- **Summary:** An inbound email was sent to h.harris@thetrydaily.thm from urgents@amazon.biz with the subject "Your Amazon

Package Couldn't Be Delivered - Action Required". The email used urgent language and a threat of a lost package to entice the user to click a suspicious link, which was a URL shortened by Bit.ly:

- <http://bit.ly/3sHkX3da12340>.
- **Investigation:** Analysis of the URL revealed clear phishing tactics, including a deceptive sender and urgent language. While some security vendors did not initially flag the link as malicious, a TryHackMe security check confirmed its malicious nature. The use of a URL shortener and an obfuscated link string confirmed this was a malicious attempt to hide the final destination.
- **Remediation:** The alert was classified as a **true positive**. The recommended remediation actions were to block the URL at the network perimeter, delete the email from the recipient's mailbox, warn the user, and monitor for any related activity.

Here is the full case report:

5Ws:

- **Who:** The email was sent from urgents@amazon.biz to h.harris@thetrydaily.thm.
- **What:** An inbound email attempting to phish the recipient by requesting confirmation of shipping information through a suspicious link.
- **When:** September 19th, 2025 at 10:19 AM.
- **Where:** Delivered to TheTryDaily's email system.
- **Why:** The email uses urgency and a fake shipping notification to trick the recipient into clicking a malicious link.

Details:

The alert was triggered because the email contained an external link that appeared suspicious. Investigation using OSINT sources revealed the following: TryHackMe's Security Check flagged the link as malicious, and the domain uses a URL shortener (bit.ly) which can hide the final destination. CyberChef analysis confirmed that the link string had been obfuscated.

- **Time of Activity:** 09/19/2025 10:19:36
- **List of Affected Entities:** h.harris@thetrydaily.thm, urgents@amazon.biz, <http://bit.ly/3sHkX3da12340>

- **Reason for Classifying as True Positive:** Multiple security sources flagged the link as malicious, and the email content shows clear phishing tactics (urgency, threat of lost package).
- **Reason for Escalating the Alert:** Clicking the link could compromise credentials or allow malware installation on the endpoint. The alert affects internal users and represents a medium-level risk.
- **Recommended Remediation Actions:** Block the URL at the network perimeter, delete the email from the recipient mailbox, warn the user not to click the link, and monitor for any related activity.
- **List of Attack Indicators:** Bit.ly URL (<http://bit.ly/3sHkX3da12340>), sender urgents@amazon.biz, phishing language (urgent action required, package at risk), CyberChef-encoded link string

Press enter or click to view image in full size

8816	Access to Blacklisted External URL Blocked by Firewall	^	High	Firewall	Sep 19th 2025 at 08:32	
Description:		This alert was triggered when a user attempted to access an external URL that is listed in the organization's blacklist or threat intelligence feeds. The firewall or proxy successfully blocked the outbound request, preventing the connection. Note: The blacklist only covers known threats. It does not guarantee protection against new or unknown malicious domains.				
datasource:		firewall				
timestamp:		09/19/2025 08:30:24.001				
Action:		blocked				
SourceIP:		10.20.2.17				
SourcePort:		34257				
DestinationIP:		67.199.248.11				
DestinationPort:		80				
URL:		http://bit.ly/3sHkX3da12340				
Application:		web-browsing				
Protocol:		TCP				
Rule:		Blocked Websites				
Playbook link						

Part B: Firewall Block

- **Alert ID:** 8816
- **Initial Classification:** High

- **Summary:** Shortly after the phishing email was received, an internal user at IP address 10.20.2.17 attempted to access the same malicious URL from the email. The firewall successfully blocked the outbound request to the destination IP 67.199.248.11.
- **Investigation:** This alert provided crucial confirmation of the malicious nature of the URL identified in Alert 8815. The successful block demonstrates that our perimeter defenses are actively protecting users from known threats.
- **Conclusion:** This alert was also classified as a **true positive**. The user was protected, but further monitoring was recommended to ensure no follow-up attempts.

Here is the full case report:

5Ws:

- **Who:** User on IP 10.20.2.17 attempted to access a known malicious URL.
- **What:** Outbound web request blocked by the firewall because the URL is listed in the organization's blacklist.
- **When:** September 19th, 2025 at 10:20:50 AM.
- **Where:** Attempt originated from internal network (10.20.2.17) to the external IP 67.199.248.11 over HTTP.
- **Why:** The URL is associated with phishing activity and was flagged by threat intelligence feeds. Accessing it could compromise user credentials or deliver malware.

Details:

The firewall successfully blocked the request, preventing any connection to the malicious URL. This URL matches the same Bit.ly link reported in the previous phishing email alert, confirming its malicious nature. The block demonstrates that the organization's perimeter defenses are actively protecting users.

- **Time of Activity:** 09/19/2025 10:20:50
- **List of Affected Entities:** 10.20.2.17, 67.199.248.11, <http://bit.ly/3sHkX3da12340>
- **Reason for Classifying as True Positive:** The URL is confirmed malicious by threat intelligence sources, including TryHackMe Security Check, and matches an active phishing attempt.
- **Reason for Escalating the Alert:** Users attempting to access the link could expose credentials or devices to compromise. Monitoring is required to ensure no follow-up attempts or lateral movement.

- **Recommended Remediation Actions:** Ensure the user is aware not to attempt accessing the URL again, continue monitoring for repeated attempts, and verify that endpoint protections are up to date.
- **List of Attack Indicators:** Bit.ly URL (<http://bit.ly/3sHkX3da12340>), destination IP 67.199.248.11, web-browsing over TCP port 80, firewall rule “Blocked Websites”

Press enter or click to view image in full size

8817

Inbound Email Containing Suspicious External Link

^

Medium

Phishing

Sep 19th 2025 at 10:23

Description:

This alert was triggered by an inbound email contains one or more external links due to potentially suspicious characteristics. As part of the investigation, check firewall or proxy logs to determine whether any endpoints have attempted to access the URLs in the email and whether those connections were allowed or blocked.

datasource:

email

timestamp:

09/19/2025 10:21:54.717

subject:

Unusual Sign-In Activity on Your Microsoft Account

sender:

no-reply@microsoftsupport.co

recipient:

c.allen@thetrydaily.thm

attachment:

None

content:

Hi C.Allen,\n\nWe detected an unusual sign-in attempt on your Microsoft account.\n\nLocation: Lagos, Nigeria\nIP Address: 102.89.222.143\nDate: 2025-01-24 06:42\nIf this was not you, please secure your account immediately to avoid unauthorized access.\n\n<https://microsoftsupport.co/login>>Review Activity\n\nThank you,\n\nMicrosoft Account Security Team

direction:

inbound

[Playback link](#)

Press enter or click to view image in full size

https://microsoftsupport.co/login

IP & Domain Reputation Overview

Email & Spam Trends

OWNER DETAILS

URI

microsoftsupport.co/login

HOSTNAME

microsoftsupport.co

DOMAIN

microsoftsupport.co

CONTENT DETAILS

CONTENT CATEGORY

No established content categories

REPUTATION DETAILS

WEB REPUTATION

Unknown

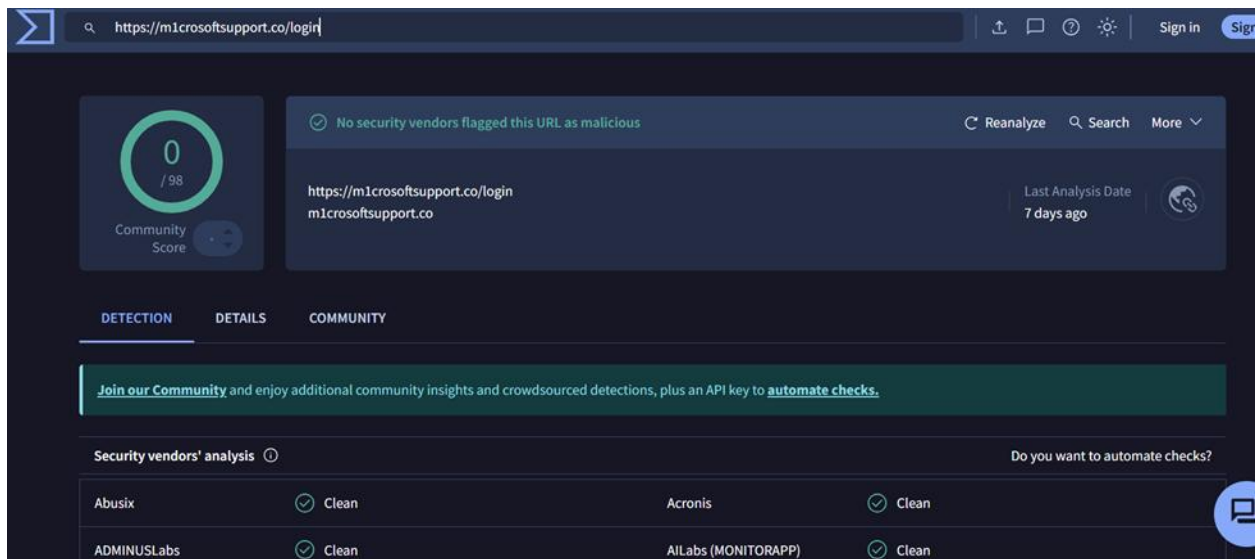
BLOCK LISTS

TALOS SECURITY INTELLIGENCE BLOCK LIST

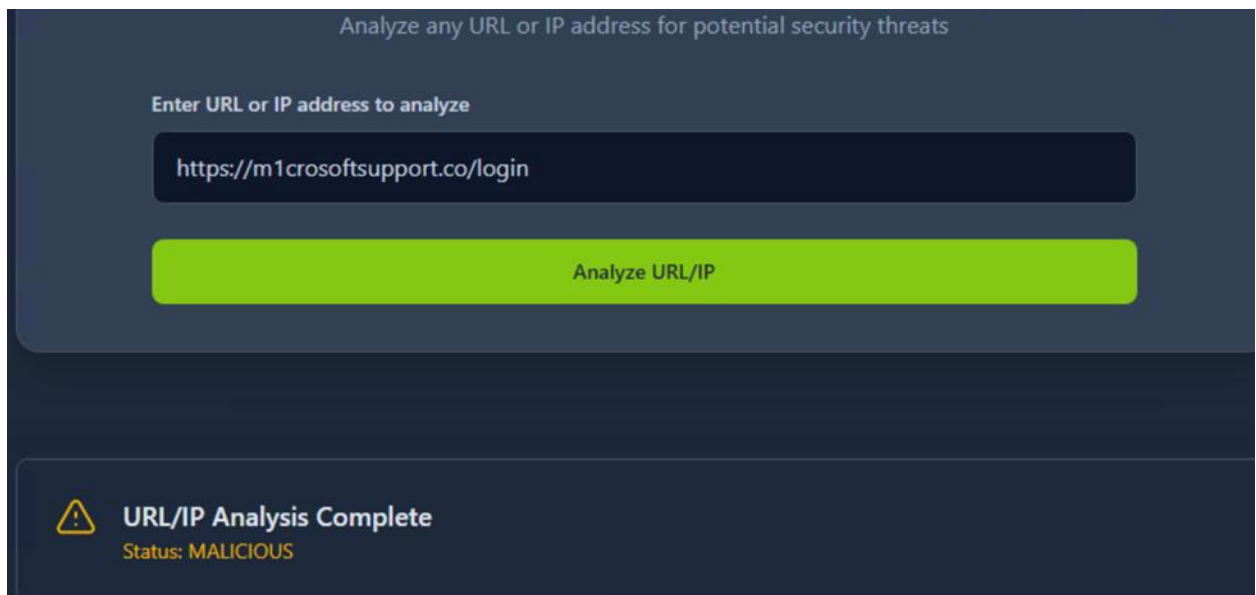
ADDED TO BLOCK LIST

No

Press enter or click to view image in full size



Press enter or click to view image in full size



Incident 3: True Positive Phishing Alert

- **Alert ID:** 8817
- **Initial Classification:** Medium
- **Summary:** An inbound email was flagged as a phishing attempt. The email, sent to c.allen@thetrydaily.thm from no-reply@m1crosoftsupport.co, used impersonation tactics to mimic a Microsoft security alert. The email warned of "unusual sign-in activity" and urged the user to click a link to "Review Activity". The link directed to

- <https://m1crosoftsupport.co/login>.
- **Investigation:** The domain m1crosoftsupport.co is a clear example of **typosquatting** designed to trick users into believing they are on a legitimate Microsoft site. The sender's email address was also fraudulent. A TryHackMe security check and other tools confirmed the link was malicious. The email's content, including the use of urgency and fear, confirmed it was a credential-harvesting attempt.
- **Conclusion:** This alert was classified as a **true positive**. Recommended remediation actions included blocking the domain at the network perimeter, removing the email from the user's mailbox, and warning the user about the attack.

Here is the full case report:

5Ws:

- **Who:** The email was sent from no-reply@m1crosoftsupport.co to c.allen@thetrydaily.thm.
- **What:** An inbound email attempting to phish the recipient by warning of unusual Microsoft account activity and requesting login via a malicious link.
- **When:** September 19th, 2025 at 10:21 AM.
- **Where:** Delivered to TheTryDaily's email system.
- **Why:** The email uses impersonation and urgency to trick the recipient into revealing credentials.

Details:

The phishing alert was triggered due to the external link pointing to a suspicious domain. To fully understand the email, CyberChef was used to decode the original email content and remove obfuscations, revealing the true malicious URL. TryHackMe Security Check confirmed the link is malicious. The domain (m1crosoftsupport.co) mimics Microsoft but is fraudulent.

- **Time of Activity:** 09/19/2025 10:21:54
- **List of Affected Entities:** c.allen@thetrydaily.thm, no-reply@m1crosoftsupport.co, <https://m1crosoftsupport.co/login>
- **Reason for Classifying as True Positive:** The decoded link was confirmed malicious by TryHackMe Security Check, and the email uses phishing tactics such as urgency, impersonation, and account fear.

- **Reason for Escalating the Alert:** Clicking the link could compromise user credentials or deliver malware, potentially affecting internal systems.
- **Recommended Remediation Actions:** Block the domain at the network perimeter, remove the email from the recipient's mailbox, warn the user not to click the link, and monitor the account for any suspicious activity.
- **List of Attack Indicators:** Malicious domain <https://m1crosoftsupport.co/login>, sender no-reply@m1crosoftsupport.co, phishing content (unusual sign-in alert, urgent account action).