

Phishing Email Investigation And IOC Analysis

LOUIS.O



Project Overview



As a cybersecurity consultant assigned to investigate a set of reported phishing emails received by an organization. Your task is to analyze the emails, identify any indicators of compromise (IOCs), and provide recommendations for mitigation and prevention.



This project simulates a real-world incident response scenario commonly encountered by SOC analysts and cybersecurity consultants.

Project Objectives:

- 1 Investigate Suspicious Emails And Extract Useful Metadata.
- 2 Identify IOCs, Including.
 - Malicious URLs or domains
 - Suspicious IP addresses
 - Attachments or payloads
 - Sender anomalies (Return-Path, SPF, DKIM, etc.)
- 3 Phishing Analysis Report: Details Of Your Key Findings With Snapshots And Mitigation Recommendations. (Report Can Be In A Slide Or Document)



Phishing Email Samples:
Download and analyze any 3
sample phishing emails.



Visit: <https://app.phishtool.com/sign-up/community> to Register for Email Analysis Tool

PhishTool

Forensic Email Analysis

Get PhishTool →

Copyright © 2025 PhishTool Limited. All rights reserved.

PhishTool Community

Create a free PhishTool Community account.

Email address*

email@address.com

Password*

Password

Re-enter password*

Password

Legal*

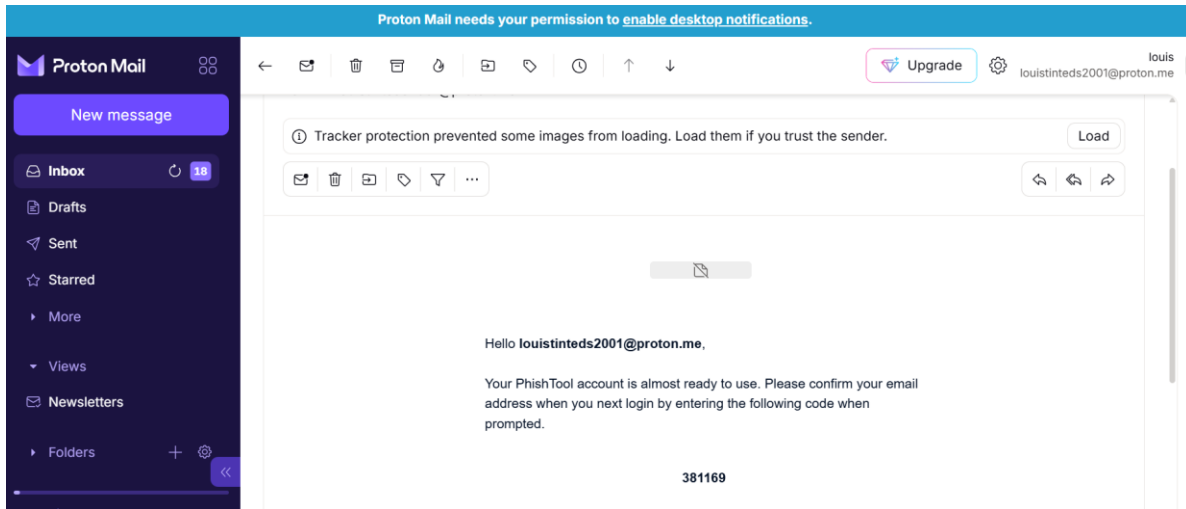
- I agree to Phishtool's [Terms of Service](#)
- I agree to Phishtool's [Privacy Policy](#)
- I agree to Phishtool's [Proof of Value Agreement](#)

Contact preferences

- Occasionally send me feature updates and announcements

Create Account

Copy Verification Code From Email To Complete Registration & sign-in



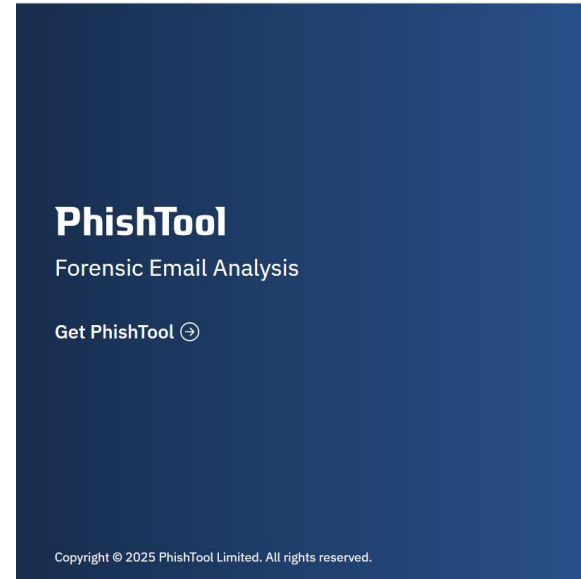
Verify

A verification code has been sent to louistinteds2001@proton.me. Enter your verification code below.

Verification code*

Submit

Cancel



Login

Email address*

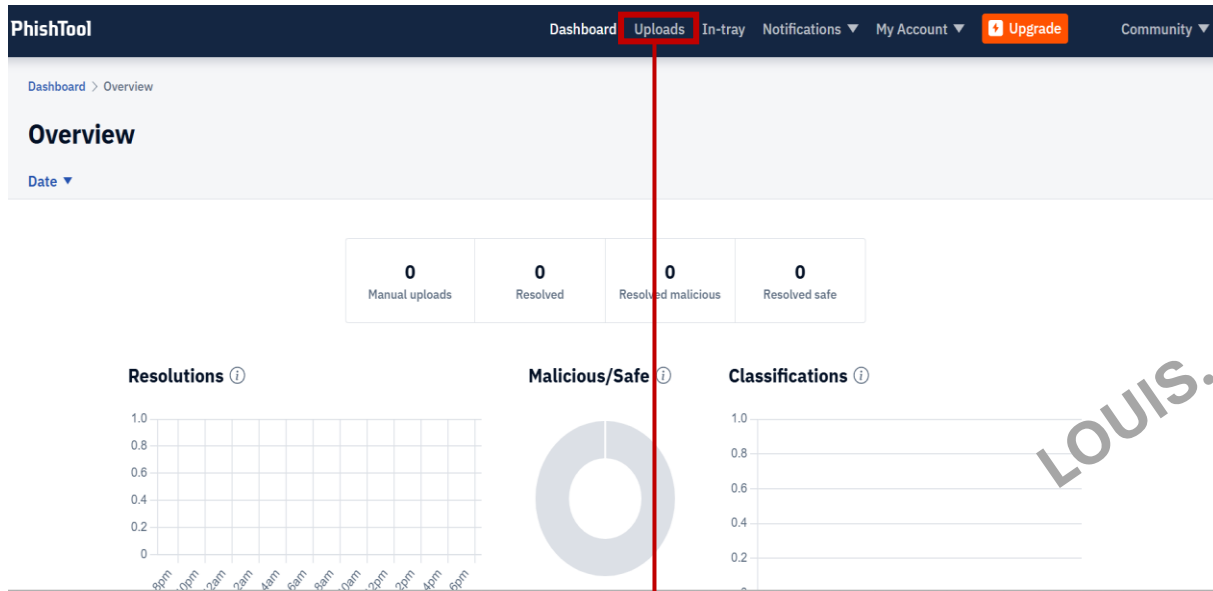
Next

[Create an account](#)

FIRST MALICIOUS EMAIL

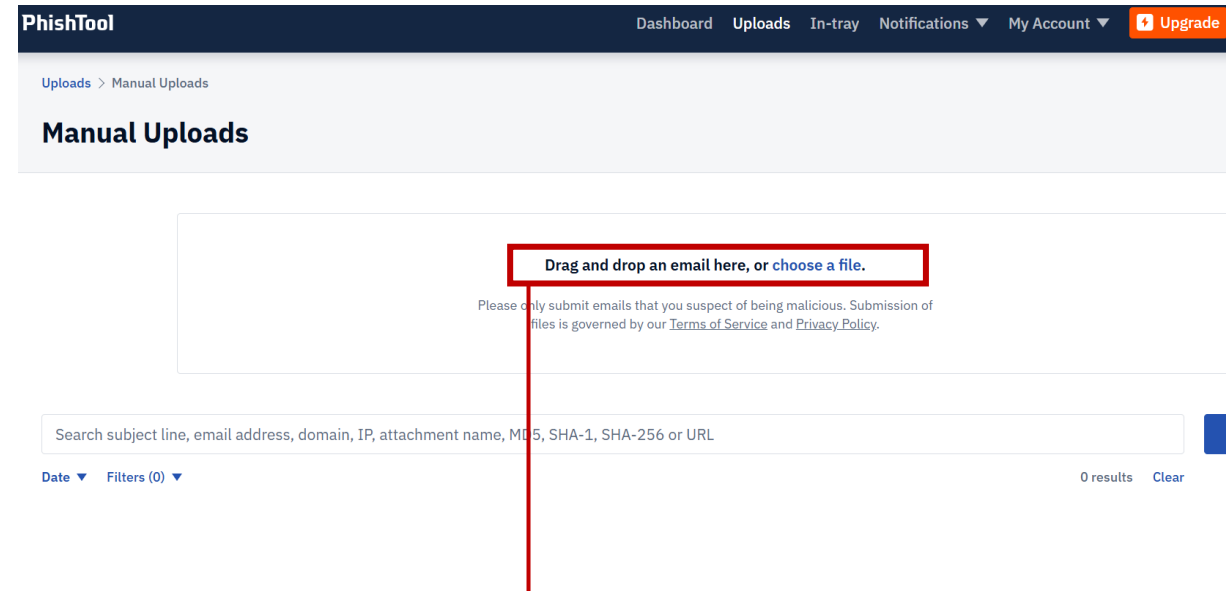
LOUIS.O

Download The Email To Your Host Computer and Upload to PhishTool for Analysis



The screenshot shows the PhishTool Dashboard Overview page. The navigation bar includes 'Dashboard', 'Uploads', 'In-tray', 'Notifications', 'My Account', 'Upgrade', and 'Community'. The 'Uploads' menu item is highlighted with a red box. Below the navigation bar, there are four summary cards: 'Manual uploads' (0), 'Resolved' (0), 'Resolved malicious' (0), and 'Resolved safe' (0). There are also three charts: 'Resolutions' (a line chart), 'Malicious/Safe' (a donut chart), and 'Classifications' (a line chart). A red arrow points from the 'Uploads' menu item to the number '1' below the dashboard.

1



The screenshot shows the PhishTool Manual Uploads page. The navigation bar includes 'Dashboard', 'Uploads', 'In-tray', 'Notifications', 'My Account', 'Upgrade', and 'Community'. The 'Uploads' menu item is highlighted with a red box. Below the navigation bar, there is a large text area with the instruction 'Drag and drop an email here, or choose a file.' This instruction is enclosed in a red box. Below the text area, there is a search bar with the placeholder text 'Search subject line, email address, domain, IP, attachment name, MD5, SHA-1, SHA-256 or URL'. A red arrow points from the red box to the number '2' below the page.

2





Copy the sender's URL & paste on <https://www.virustotal.com/> to confirm if the URL is malicious or not.

Uploads > Delivery Status Notification (Failure)

Delivery Status Notification (Failure)

Details Authentication URLs Attachments Transmission X-headers

Rendered HTML Plaintext Source

From	 mailer-daemon@googlemail.com 
Display name	Mail Delivery Subsystem
Sender	None
To	jeffrealblog@gmail.com
Cc	None
In-Reply-To	64688820326628.5cr7mv0434e31rsw725on25y@email.gmail.com
Timestamp	2025-08-15T20:32:51Z
Reply-To	None
Message-ID	<689f9973.050a0220.174e31.088f.GMR@mx.google.com>
Return-Path	None
Originating IP	 209.85.220.65 (Received-SPF) 
rDNS	mail-sor-f65.google.com



Address not found

Your message wasn't delivered to **jeffrealblog@google.com** because the address couldn't be found, or is unable to receive mail.

[LEARN MORE](#)

The response was:

The email account that you tried to reach does not exist. Please try double-checking the email address for typos or unnecessary spaces. For more information, go to <https://support.google.com/mail/answer/185833>

Analyzing the sender's Url using <https://www.virustotal.com/>

The screenshot shows the VirusTotal homepage. At the top left is a search bar with the placeholder text "URL, IP address, domain or file hash". The main header features the VirusTotal logo and the text "VIRUSTOTAL". Below this is a descriptive sentence: "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." A navigation bar contains four items: "FILE", "URL", "SEARCH", and a language selector icon. The "URL" tab is highlighted with a red box and labeled "1". Below the navigation bar is a globe icon. A search input field contains the email address "mailer-daemon@googlemail.com" and is highlighted with a red box and labeled "2". A "Search" button is located below the input field and is highlighted with a red box and labeled "3". At the bottom, there is a disclaimer: "By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the sharing of your URL submission with the security community. Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more." A footer link reads: "Want to automate submissions? Check our API, or access your API key."

One of the antivirus platform flagged the sender URL as malicious

The screenshot shows the VirusTotal analysis page for the URL <http://googlemail.com/>. The interface is dark-themed. At the top, a notification states "1/98 security vendor flagged this URL as malicious". A circular gauge on the left shows a "Community Score" of 24 out of 98, with a red "1" indicating the number of vendors that flagged the URL. The URL is listed as "http://googlemail.com/googlemail.com" with a status of 200, content type of text/html, and last analysis date of 2 days ago. Below this, there are tabs for "DETECTION", "DETAILS", and "COMMUNITY" (with a count of 9). A green banner encourages joining the community. The "Crowdsourced context" section shows a "LOW 1" severity level and a warning icon. A specific detection is highlighted: "Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns - The Citizen Lab - according to source ArcSight Threat Intelligence - 2 years ago". The "Security vendors' analysis" section contains a table with the following data:


Vendor	Analysis	Vendor	Analysis
Gridinsoft	Phishing	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean

Uploads > Delivery Status Notification (Failure)

Delivery Status Notification (Failure) [🔗](#)

Details Authentication URLs Attachments Transmission X-headers

Rendered HTML Plaintext Source

Return-Path domain	None
SPF record	None
DKIM	✓ PASS ...
Verification(s)	1 Signature - 1 PASS
Selector	20230601._domainkey.googlemail.com (Signature 1 of 1)
Signing domain	googlemail.com
Algorithm	rsa-sha256
Verification	PASS
DMARC	✓ PASS ...
From domain	 googlemail.com
DMARC record	v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:mailauth-reports@google.com



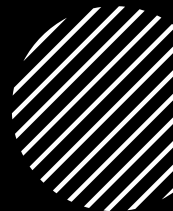
Address not found

Your message wasn't delivered to **jeffrealblog@google.com** because the address couldn't be found, or is unable to receive mail.

[LEARN MORE](#)

The response was:

The email account that you tried to reach does not exist. Please try double-checking the email address for typos or unnecessary spaces. For more information, go to <https://support.google.com/mail/answer/185832>.



The sent email does not contain any **Attachment** , **Return-Path** or **SPF**. But let's investigate the DKIM, if it passes the verification test.



SPF:



An SPF (Sender Policy Framework) check confirms if an originating IP is authorized to send emails for a domain. SPF is designed to detect fraudulently sent emails — although only a combination of SPF, DKIM and DMARC can provide this level of assurance.



DKIM:



DKIM (DomainKeys Identified Mail) is an email security standard that uses cryptographic public and private key pairs to validate the integrity of an email with a given signing domain. The application of DKIM is achieved by a sending SMTP server prepending a digital signature (computed with a private key) linked to a signing domain to each outgoing email

Analyzing the sender's IP address using <https://www.virustotal.com>

Uploads > Delivery Status Notification (Failure)

Delivery Status Notification (Failure) [🔗](#)

Details Authentication URLs Attachments Transmission X-headers

Rendered HTML Plaintext Source

From	✉ mailer-daemon@googlemail.com	⋮
Display name	Mail Delivery Subsystem	
Sender	None	
To	jeffrealblog@gmail.com	
Cc	None	
In-Reply-To	64688820326628.5cr7mv0434e31rsw725on25y@email.gmail.com	
Timestamp	2025-08-15T20:32:51Z	
Reply-To	None	
Message-ID	<689f9973.050a0220.174e31.088f.GMR@mx.google.com>	
Return-Path	None	
Originating IP	✉ 209.85.220.65 (Received-SPF) ⌵	⋮
rDNS	mail-sor-f65.google.com	



Address not found

Your message wasn't delivered to **jeffrealblog@google.com** because the address couldn't be found, or is unable to receive mail.

[LEARN MORE](#)

The response was:

The email account that you tried to reach does not exist. Please try double-checking the email address for typos or unnecessary spaces. For more information, go to <https://support.google.com/mail/answer/28559>

Copy the IP address and open <https://www.virustotal.com/> to confirm if the IP address is malicious.

The image shows the VirusTotal website interface. At the top, there is a search bar with the placeholder text "URL, IP address, domain or file hash". Below the search bar is the VirusTotal logo and the text "Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community." The main navigation bar includes "FILE", "URL", "SEARCH", and a language selector. The "URL" tab is highlighted with a red box and an arrow labeled "1". Below the navigation bar is a globe icon. A search input field contains the IP address "209.85.220.65" and is highlighted with a red box and an arrow labeled "2". Below the input field is a "Search" button, also highlighted with a red box and an arrow labeled "3". At the bottom, there is a footer with the text "© Want to automate submissions? Check our API, or access your API key."

URL, IP address, domain or file hash

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

209.85.220.65

Search

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#).

© Want to automate submissions? [Check our API](#), or [access your API key](#).

One of the antivirus platform flagged the IP address associated with this email as suspicious.

The screenshot shows the VirusShare analysis interface for the URL `http://209.85.220.65/`. The page features a dark theme and includes a search bar, navigation tabs, and a table of security vendor analyses.

Community Score: 0 / 97

Status: No security vendors flagged this URL as malicious

Last Analysis Date: 2 months ago


Navigation: DETECTION, DETAILS, COMMUNITY 1

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

Security vendors' analysis:

Vendor	Result	Vendor	Result
Criminal IP	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
AlphaSOC	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chang Luu Dao	Clean	CINIS Army	Clean

Get more details about the sender's IP address using <https://urlscan.io>



urlscan.io

Home Search Live API Blog Docs Pricing Login





















Sponsored by **SecurityTrail**
A Recorded Future Company

urlscan.io

A sandbox for the web

Public Scan Options

Recent scans  Updates every 10s - Last update: 07:04:36

 URL	Age		Size		IPs	 
 www.activelifeanklesupport.com/	14 seconds		1 MB	104	10	3 
 expireddomains.com/domain/adalynnsattic.com	15 seconds		260 KB	14	2	2
 www.nassaustreetpartners.com/	19 seconds		6 MB	55	17	5 
 138.188.34.4/	21 seconds		72 KB	7	1	1 
 www.aiiis.net/	21 seconds		739 KB	16	3	2
 tcswiss.nl/	22 seconds		2 MB	25	4	2 

SECOND MALICIOUS EMAIL

LOUIS.O

Download the mail to your host computer. Please **DO NOT** open the mail nor any attachment.

The image shows a Gmail interface with a sidebar on the left containing folders like Compose, Inbox (53), Starred, Snoozed, Important, Sent, Drafts (62), Purchases, Social (1,486), Updates (6,176), Forums, Promotions (3,137), and More. The main area displays an email from Google Play with the subject "There's an issue with your Verve-3466". The email content includes the Google Play logo, the heading "Update your payment method for Learn Python - Code Lab by Ocean", and a message to "LOUIS" stating that their subscription is expired. A green "Update" button is at the bottom of the email content. On the right side of the email header, a context menu is open, listing actions such as Reply, Forward, Delete, Mark as unread, Block "Google Play", Report spam, Report phishing, Filter messages like this, Translate, Print, Download message (highlighted with a red box), and Show original. A red arrow labeled "1" points to the menu icon, and another red arrow labeled "2" points to the "Download message" option.

Visit <https://app.phishtool.com/> to Upload the downloaded mail to check the legitimacy of the mail.

The screenshot shows the PhishTool interface with the 'Uploads' tab selected. A Windows File Explorer window is open, showing the 'Downloads' folder. The file 'There's an issue with your Verve-3466.eml' is selected and highlighted. A red box highlights the 'Open' button in the File Explorer. A red arrow points from the 'Uploads' tab to the number '1'. Another red arrow points from a red box containing the text 'Drag and drop an email here, or choose a file.' to the number '2'. A third red arrow points from the selected email file to the number '3'. A fourth red arrow points from the 'Open' button to the number '4'. The PhishTool interface shows a table of uploaded emails with columns for Subject, Resolution, Classification, and Date uploaded.

1

2 Drag and drop an email here, or choose a file.

3

4

Subject	Resolution	Classification	Date uploaded
There's an issue with your Verve-3466	-	-	2025-10-08T13:22:56
phishing@pot Ferreira Peixoto, seu pedido esta retido.	-	-	2025-10-08T12:05:59
wir vergeben deinen NETTO Gutschein an einen anderen ...	-	-	2025-10-08T11:55:26
Delivery Status Notification (Failure)	-	-	2025-10-08T04:38:51

Uploads > There's an issue with your Verve-3466

There's an issue with your Verve-3466 [🔗](#)

[Details](#) [Authentication](#) [URLs](#) [Attachments](#) [Transmission](#) [X-headers](#)[Rendered](#) [HTML](#) [Plaintext](#) [Source](#)

From	📧 googleplay-noreply@google.com	⋮
Display name	Google Play	
Sender	None	
To	louistinteds2001@gmail.com	
Cc	None	
In-Reply-To	None	
Timestamp	2025-10-08T10:01:55Z	
🟢 Reply-To	📧 googleplay-noreply@google.com	⋮
Message-ID	<ed3ada917fc5706528da21021e82d147ac372cb9-20298379-111448487@google.com>	
🔴 Return-Path	📧 3kzbmaBIKAOYOWWOTMXTIg-VWZMXTgOWWOTM.KWU@scoutcamp.bounces.google.com	⋮
Originating IP	📧 209.85.220.69 (Received-SPF) ▼	⋮
rDNS	mail-sor-f69.google.com	

🔴 Auto-analysis

📧 Flag as malicious ▶

DNS lookup

WHOIS lookup

Secure browser

📘 Information

Copy



Update your payment m

- Code Lab by Ocean

Hi LOUIS,

Your Verve-3466 associated with you
Ocean (Yearly Subscription Plan) subTo keep your subscription active and
payment method or use a different o

Upd

Thanks,
The Google Play Team

The Return-Path is flagged as inconsistent, so click on Auto-analysis to see the Return-Path and copy it into VirusTotal to see all malicious embedded files associated with this email.

Copy Inconsistent
Return-Path to
VirusTotal.

Dashboard Uploads In-tray Notifications ▼ My Account ▼ Upgrade Community ▼

Auto-analysis

Return-Path

Filters (0) ▼

! Inconsistent Return-Path domain

The 'Return-Path' domain **scoutcamp.bounces.google.com** is inconsistent with the 'From' domain google.com.

Context

An SPF check compares the sending SMTP server IP address with the IP address(es) published in the SPF policy within the 'Return-Path' domain's SPF record. As a result, an attacker might insert a malicious 'Return-Path' email address with a domain that they control to successfully PASS an SPF check, whilst also spoofing the 'From' email address.

It is common for marketing emails to insert an inconsistent 'Return-Path' for legitimate purposes. Typically this takes the form of a 'bounce address', used for mailing list management.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with [OUR THREAT INTELLIGENCE OFFERING](#).

scoutcamp.bounces.google.com

Search

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your** information with the **security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more](#)

VirusTotal has detected "At least 10 files embedding this domain"

scoutcamp.bounces.google.com

Community Score: 0 / 95

At least 10 detected files embedding this domain

Reanalyze Similar More

scoutcamp.bounces.google.com
google.com
top-1M

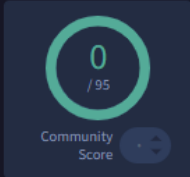
Registrar: MarkMonitor Inc. | Creation Date: 28 years ago | Last Analysis Date: 9 hours ago

DETECTION DETAILS **RELATIONS** COMMUNITY 1

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?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	Antiy-AVL	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean
ChainPatrol	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean



At least 10 detected files embedding this domain

Reanalyze Similar More

scoutcamp.bounces.google.com
google.com
top-1M

Registrar
MarkMonitor Inc.

Creation Date
28 years ago

Last Analysis Date
9 hours ago



DETECTION DETAILS RELATIONS COMMUNITY 1

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

Siblings (6.6 K)

0support.google.com	0 / 95			
1.google.com	0 / 95	74.125.202.100	74.125.202.113	74.125.202.139 ...
1ers.google.com	0 / 95			
2.google.com	0 / 95			
216-239-33-25.google.com	0 / 95	216.239.33.25		
216-239-45-10.google.com	0 / 95	216.239.45.10		
216-239-45-36.google.com	0 / 95	216.239.45.36		
216-239-45-4.google.com	0 / 95			
216-239-45-45.google.com	0 / 95	216.239.45.45		
216-239-45-5.google.com	0 / 95	216.239.45.5		

Files Referring (35)

Scanned	Detections	Type	Name
2018-09-23	1 / 58	Email	45822c0ccfe24b29c25fa690f1af127391076fac27f444219b2ed8f428741725
2021-01-18	15 / 60	Email	Inbox
2018-09-04	1 / 59	Email	INBOX.001
2018-08-07	2 / 59	unknown	55CF5AC3-0A54-4721-80F2-892A94406047.olk15MsgSource
2018-07-17	12 / 57	Email	privat-1
2018-07-15	2 / 58	Email	4234.emlx
2018-06-17	1 / 58	Email	2016-10
2020-02-16	12 / 58	Email	Trash
2018-05-09	1 / 60	Email	a559b5138e7cc591007b97684260ec15862086b7bee19a3e853d7837fcd9acb6
2019-09-19	1 / 55	Email	Hugo Kollion



11686cf509da9c9049f9661a642d704324132cb16432474cb044416a9aa82137



15/60 security vendors flagged this file as malicious

Reanalyze Similar More

11686cf509da9c9049f9661a642d704324132cb16432474cb044416a9aa82137

Size
3.35 MB

Last Analysis Date
4 years ago



Inbox

email

DETECTION DETAILS COMMUNITY 5

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?

Ad-Aware	VB:Trojan.VBA.Downloader.NE	ALYac	VB:Trojan.VBA.Downloader.NE
Antiy-AVL	Trojan[Downloader]/MSOffice.Agent.fmg	Avira (no cloud)	HEUR/Macro.Downloader.FAE.Gen
BitDefender	VB:Trojan.VBA.Downloader.NE	ClamAV	Xls.Downloader.Sload-6774021-0
Cynet	Malicious (score: 85)	DrWeb	Exploit.Siggen.10386
Fortinet	VBA/Agent.49DF!tr.dldr	GData	VB:Trojan.VBA.Downloader.NE
Ikarus	Trojan-Downloader.VBA.Agent	Kaspersky	HEUR:Trojan-Downloader.MSOffice.SLoa...
MAX	Malware (ai Score=86)	Trellix (ENS)	RDN/Generic Downloader.x
ZoneAlarm by Check Point	HEUR:Trojan-Downloader.MSOffice.SLoa...	AegisLab	Undetected

An alternative technique to detect malicious emails.

The screenshot shows a Gmail inbox with a selected email from Google Play. The email subject is "There's an issue with your Verve-3466" and the sender is "Google Play <googleplay-noreply@google.com>". The email content includes a warning about an expired subscription for "Learn Python - Code Lab by Ocean" and a green "Update" button. A context menu is open over the email, listing actions such as Reply, Forward, Delete, Mark as unread, Block "Google Play", Report spam, Report phishing, Filter messages like this, Translate, Print, Download message, and Show original. The "Show original" option is highlighted with a red box. Two red arrows point from the highlighted options to numbers 1 and 2 below the interface.

2

1

Copy the IP address into VirusTotal platform to check the legitimacy of the IP address

Original Message

Message ID <ed3ada917fc5706528da21021e82d147ac372cb9-20298379-111448487@google.com>

Created at: Wed, Oct 8, 2025 at 11:01 AM (Delivered)

From: Google Play <googleplay-noreply@google.com>

To: louistinteds2001@gmail.com

Subject: There's an issue with your Verve-3466

SPF: PASS with IP **209.85.220.69** [Learn more](#)

DKIM: 'PASS' with domain google.com [Learn more](#)

DMARC: 'PASS' [Learn more](#)

[Download Original](#)

Delivered-To: louistinteds2001@gmail.com
Received: by 2002:a05:651c:897:b0:366:7d43:87e8 with SMTP id d23csp5984611jq;
Wed, 8 Oct 2025 03:01:55 -0700 (PDT)
X-Received: by 2002:a05:690c:5506:10b0:748:a6a0:9ff with SMTP id 00721157ae682-780d222e60cmr68715597b3.14.17599177153;
Wed, 08 Oct 2025 03:01:55 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1759917715; cv=none;
d=google.com; s=arc-20240605;
b=FMTZH7ch1i2NKGvYxoGtrE6N4hZ9jknioi+6HCPorQ7p+8JFGXIN4LgMt7KEVLQ5X/
zhmYjRYpOHSwB6PnA95cDGZMLSyEFIfeidWgoLB/Sd3FLzCn6m6pnJQBWhG3mhsedkr1
FHNVLHSIL+A0te9tc+TPmRRVPu4Z6SQsxCcPfalSrvIA0tqixIL8/UpiMPN/46HoUtA
6jgFXdF9s6gwuy+344FNcDjhGwPXKzaSwlVKQGTw0hVMJygz39Ro2DHqDxmZL/bbsCDZ
jPPFzbe9XDNIWn17RD1Y+ew/07sgwAtL8vQX7e9rhVA8F78ZggJ34dp3VwSCpdpjYyh
juhc
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
h=to:from:subject:message-id:feedback-id:reply-to:date:mime-version
:dkim-signature;
bh=GcAjwg17tpLW+yN04CI8bViiHVj410wbJF7Nn4hfuKA=;
fh=ii+/9x6pbGt2qi2vZId0cZ6tTjPb/d+qM4E+ogNuMok=;
b=C+XqV+LmxPWQWOHbDjEKYnUq0tvAX7P/o1tqIoq0ihHnWh9u33yoIDRLgw8byQqvc0
VZJ8xMJ3AUBv9zZqwaSH22p8nx5AA2dxMKtovSNadTL2Ff/VelKi1wsPUfz1Viu6EmTJ
CbPzbNigulskM/0n/40jLYUwKaCd7fHOa7/010RZAQ17ry1yBSX9sF8BuuFEAoZ4/7Y5
ySDKNhpA8KuDFfj0Gk4AY6M7TfBDtQrKsbIkjkbqBx6x1S46PGvHis5QnBn2vAqP6dBY
cXaN/Uw92Fq5TMy8wKukOdXdTN2LX7aACrZmDoK0b9J2W06qztgNIaBeQ+A6jBZX4Wtq
7D+g==;
dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@google.com header.s=20230601 header.b="h8/KG70M";
spf=pass (google.com: domain of 3kzmbaBIKAOYOWWOTMXTig-VWZMXTgOwWOTM.KWU@scoutcamp.bounces.google.com designated
smtp.mailfrom=3kzmbaBIKAOYOWWOTMXTig-VWZMXTgOwWOTM.KWU@scoutcamp.bounces.google.com);
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=google.com;
dara=pass header.i=@gmail.com
[Return-Path: <3kzmbaBIKAOYOWWOTMXTig-VWZMXTgOwWOTM.KWU@scoutcamp.bounces.google.com>](mailto:3kzmbaBIKAOYOWWOTMXTig-VWZMXTgOwWOTM.KWU@scoutcamp.bounces.google.com)
Received: from mail-sor-f69.google.com (mail-sor-f69.google.com. [209.85.220.69])
by mx.google.com with SMTPS id 00721157ae682-780e1d214basor13409367b3.0.2025.10.08.03.01.55
for <louistinteds2001@gmail.com>
(Google Transport Security);
Wed, 08 Oct 2025 03:01:55 -0700 (PDT)



VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

1

FILE

URL

SEARCH



2

209.85.220.69

3

Search

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Notice](#), and to the **sharing of your URL submission with the security community**. Please do not submit any personal information; we are not responsible for the contents of your submission. [Learn more.](#)

Want to automate submissions? [Check our API](#), or [access your API key](#).

http://209.85.220.69/

Community Score

No security vendors flagged this URL as malicious

http://209.85.220.69/
209.85.220.69

ip

Reanalyze Search More

Last Analysis Date
24 days ago

DETECTION DETAILS COMMUNITY 8

[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?

Criminal IP	⚠ Suspicious	Abusix	✔ Clean
Acronis	✔ Clean	ADMINUSLabs	✔ Clean
ALabs (MONITORAPP)	✔ Clean	AlienVault	✔ Clean
AlphaSOC	✔ Clean	Antiy-AVL	✔ Clean
Artists Against 419	✔ Clean	benkow.cc	✔ Clean
BitDefender	✔ Clean	BlockList	✔ Clean
Blueliv	✔ Clean	Certego	✔ Clean
Chong Lua Dao	✔ Clean	CINS Army	✔ Clean
CMC Threat Intelligence	✔ Clean	CRDF	✔ Clean
Cyble	✔ Clean	CyRadar	✔ Clean
desenmascara.me	✔ Clean	DNS8	✔ Clean
Dr.Web	✔ Clean	EmergingThreats	✔ Clean
Emsisoft	✔ Clean	ESET	✔ Clean

THIRD MALICIOUS EMAIL

LOUIS.O

The IP address is malicious and such mail should not be open.

The screenshot shows the VirusShare analysis interface for the URL `http://209.85.220.69/`. The top navigation bar includes a search icon, the URL, and options for 'Reanalyze', 'Search', and 'More'. A status bar indicates 'No security vendors flagged this URL as malicious'. A 'Community Score' widget shows a score of 0 out of 98. The 'DETECTION' tab is active, displaying a table of security vendors' analyses. A large watermark 'LOUIS.O' is overlaid on the page.

Community Score: 0 / 98

No security vendors flagged this URL as malicious

Reanalyze Search More

http://209.85.220.69/
209.85.220.69

Last Analysis Date: 22 days ago

ip

DETECTION DETAILS COMMUNITY 8

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?

Criminal IP	ⓘ Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
AlphaSOC	✓ Clean	Antiy-AVL	✓ Clean
Artists Against 419	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	BlockList	✓ Clean
Blueliv	✓ Clean	Certego	✓ Clean

Secure Your Nano Now [🔗](#)

[Details](#) [Authentication](#) [URLs](#) [Attachments](#) [Transmission](#) [X-headers](#) [Rendered](#) [HTML](#)

From	security@reposepoint.com	...
Display name	Security Team	3 ←
Sender	None	
To	phishing@pot	
Cc	None	2 ←
In-Reply-To	None	
Timestamp	2023-12-12T20:23:43Z	
Reply-To	None	
Message-ID	<ZtwBFuOfR-e84ius7Hf8VA@geopod-ismtpd-10>	
Return-Path	bounces+15134169-c574-phishing@pot=hotmail.com@send.ksd2.klaviyomail.com	1 ←
Originating IP	167.89.100.80 (Received-SPF) ▼	...
rDNS	o1314.shared.klaviyomail.com	

LOUIS.O

- ! Auto-analysis
- Flag as malicious ▶
- DNS lookup
- WHOIS lookup
- Secure browser
- Information
- Copy

Auto-analysis

Return-Path

Filters (0) ▼

! Inconsistent Return-Path domain

The 'Return-Path' domain pot=hotmail.com is inconsistent with the 'From' domain **reposepoint.com**.

Context

An SPF check compares the sending SMTP server IP address with the IP address(es) published in the SPF policy within the 'Return-Path' domain's SPF record. As a result, an attacker might insert a malicious 'Return-Path' email address with a domain that they control to successfully PASS an SPF check, whilst also spoofing the 'From' email address.

It is common for marketing emails to insert an inconsistent 'Return-Path' for legitimate purposes. Typically this takes the form of a 'bounce address', used for mailing list management.



0
/ 95
Community Score

1 detected file embedding this domain

Reanalyze Similar More

reposepoint.com

Registrar
NAMECHEAP INC

Creation Date
6 years ago

Last Analysis Date
8 days ago



top-1M

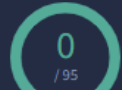
DETECTION DETAILS RELATIONS COMMUNITY

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?

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	benkow.cc	✓ Clean
BitDefender	✓ Clean	Blueliv	✓ Clean
Certego	✓ Clean	Chong Lua Dao	✓ Clean
CINS Army	✓ Clean	CMC Threat Intelligence	✓ Clean
CRDF	✓ Clean	Criminal IP	✓ Clean
Cyble	✓ Clean	CyRadar	✓ Clean
desenmascara.me	✓ Clean	DNS8	✓ Clean
Dr.Web	✓ Clean	EmergingThreats	✓ Clean
Emsisoft	✓ Clean	ESET	✓ Clean
ESTsecurity	✓ Clean	Forcepoint ThreatSeeker	✓ Clean
Fortinet	✓ Clean	G-Data	✓ Clean



Community Score

1 detected file embedding this domain

Reanalyze Similar More

reposepoint.com

top-1M

Registrar
NAMECHEAP INC

Creation Date
6 years ago

Last Analysis Date
8 days ago

DETECTION DETAILS RELATIONS COMMUNITY

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

Passive DNS Replication (11)

Date resolved	Detections	Resolver	IP
2022-12-03	0 / 95	VirusTotal	104.19.154.92
2022-10-31	0 / 95	Georgia Institute of Technology	104.19.155.92
2022-10-01	0 / 95	VirusTotal	34.86.59.15
2022-08-25	0 / 95	Georgia Institute of Technology	34.121.194.18
2022-08-02	0 / 95	VirusTotal	104.196.162.239
2020-06-16	0 / 95	VirusTotal	35.208.103.169
2020-06-13	1 / 95	VirusTotal	151.139.128.11
2020-06-05	0 / 95	VirusTotal	63.250.43.4
2020-06-05	0 / 95	VirusTotal	63.250.43.3
2019-12-09	0 / 95	VirusTotal	23.227.38.32

Subdomains (14)

staging29.reposepoint.com	0 / 95	35.208.103.169
staging26.reposepoint.com	0 / 95	35.208.103.169
staging27.reposepoint.com	0 / 95	35.208.103.169
authsmtp.reposepoint.com	0 / 95	35.208.103.169
staging20.reposepoint.com	0 / 95	35.208.103.169
mailserver.reposepoint.com	0 / 95	35.208.103.169
mvideo.reposepoint.com	0 / 95	35.208.103.169
www.reposepoint.com	0 / 95	35.208.103.169
www.reposepoint.com	0 / 95	35.208.103.169
www.reposepoint.com	0 / 95	35.208.103.169



151.139.128.11



1/95 security vendor flagged this IP address as malicious

Reanalyze Similar More

151.139.128.11

US Last Analysis Date 18 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 291

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?

Xcitiem Verdict Cloud	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AILabs (MONITORAPP)	Clean	AlienVault	Clean
Antiy-AVL	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean
Certego	Clean	Chong Lua Dao	Clean
CINS Army	Clean	CMC Threat Intelligence	Clean
CRDF	Clean	Criminal IP	Clean
Cyble	Clean	CyRadar	Clean
desenmascara.me	Clean	DNS8	Clean
Dr.Web	Clean	EmergingThreats	Clean
Emsisoft	Clean	ESET	Clean
ESTsecurity	Clean	Fortinet	Clean
G-Data	Clean	Google Safebrowsing	Clean

1
/ 95Community
Score -21

1/95 security vendor flagged this IP address as malicious

Reanalyze Similar More

151.139.128.11

US

Last Analysis Date



15 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 291

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Passive DNS Replication (200)

Date resolved	Detections	Resolver	Domain
2025-08-07	0 / 95	VirusTotal	cpcontacts.southenddogtraining.co.uk
2025-06-04	0 / 95	VirusTotal	power4d.net
2025-06-03	0 / 95	Georgia Institute of Technol ogy	hiu4d1.com
2025-02-21	0 / 95	VirusTotal	doinitinthedark.com
2025-02-15	0 / 95	Georgia Institute of Technol ogy	suksestoto.com
2025-02-01	0 / 95	VirusTotal	guacharecords.cl
2025-01-30	0 / 95	Georgia Institute of Technol ogy	coachhire.london
2025-01-20	0 / 95	VirusTotal	www.operajp.co
2024-12-19	0 / 95	Georgia Institute of Technol ogy	slotgacorhelo4d.com
2024-12-18	0 / 95	Georgia Institute of Technol ogy	spin707.asia

Communicating Files (24.6 K)

Scanned	Detections	Type	Name
2025-09-16	67 / 72	Win32 EXE	TXTRESSE
2025-09-08	70 / 72	Win32 EXE	Macromedia Flash Player 6.0
2025-08-01	64 / 71	Win32 EXE	interneter.exe
2024-02-13	65 / 71	Win32 EXE	UPDATEVISUCONF_109_2
2025-08-16	67 / 72	Win32 EXE	Adobe Help Viewer
2025-08-16	69 / 72	Win32 EXE	Adobe Help Viewer
2025-08-16	67 / 72	Win32 EXE	Adobe Help Viewer



Community Score -60

67/72 security vendors flagged this file as malicious

Reanalyze Similar More

00001dd58b69582cc30a16b000bce3d96d369487444385489084719676afba4d

Size
89.00 KB

Last Analysis Date
22 days ago



TXTRASSE

peexe checks-user-input checks-usb-bus runtime-modules malware direct-cpu-clock-access spreader long-sleeps checks-network-adapters detect-debug-environment

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16+

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label virus.ramnit/nimnul

Threat categories virus

Family labels ramnit nimnul rmndrp

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	! Win32/Ramnit.B	Alibaba	! Virus:Win32/Ramnit.gen2
AliCloud	! Virus:Win/Ramnit	ALYac	! Win32.Ramnit
Antiy-AVL	! Virus/Win32.Nimnul.a	Arcabit	! Win32.Ramnit
Arctic Wolf	! Unsafe	Avast	! Win32:RmnDrp [Inf]
AVG	! Win32:RmnDrp [Inf]	Avira (no cloud)	! W32/Ramnit.CD
Baidu	! Win32.Virus.Nimnul.a	BitDefender	! Win32.Ramnit
Bkav Pro	! W32.RamnitNNA.PE	ClamAV	! Win.Trojan.Ramnit-1847
CrowdStrike Falcon	! Win/malicious_confidence_100% (W)	CTX	! Exe.virus.ramnit
Cynet	! Malicious (score: 100)	DeepInstinct	! MALICIOUS
DrWeb	! Win32.Rmnet	Elastic	! Malicious (high Confidence)
Emsisoft	! Win32.Ramnit (B)	eScan	! Win32.Ramnit
ESET-NOD32	! Win32/Ramnit.A	Fortinet	! W32/Ramnit.A
GData	! Win32.Virus.Ramnit.C	Google	! Detected

Mitigation & Recommendations



- Block all malicious IPs, URLs, and domains on email gateways and firewalls.



- Quarantine and delete identified phishing emails from user inboxes.



- Keep antivirus, EDR, and spam filters up to date with latest signatures.



- Enforce SPF, DKIM, and DMARC to prevent email spoofing.

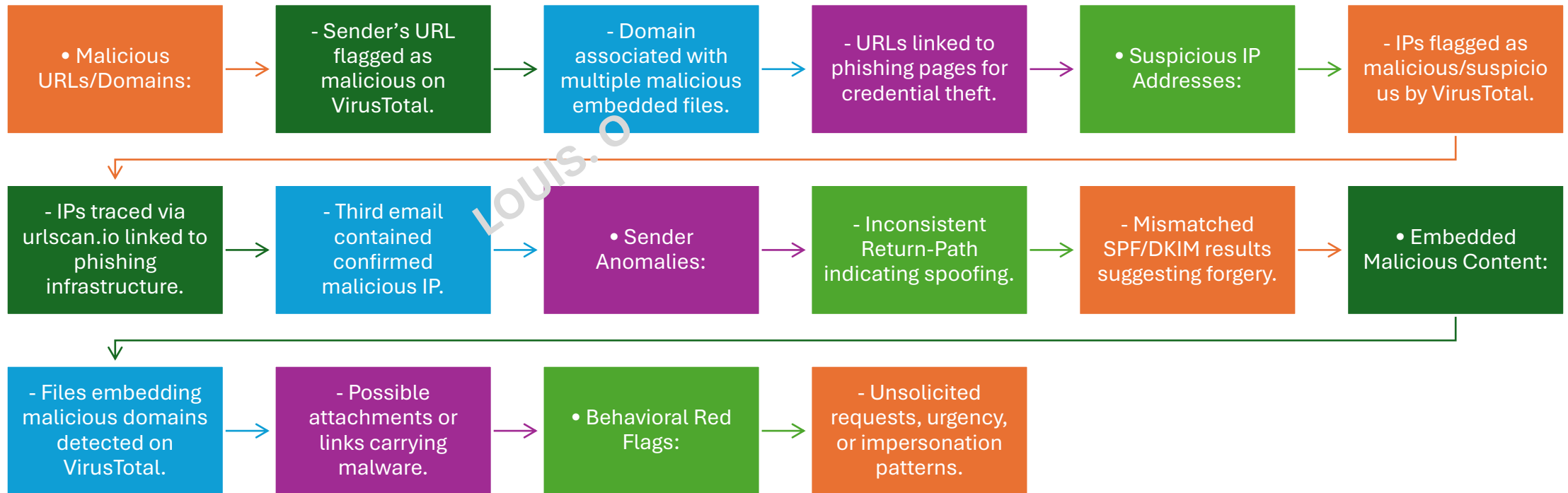


- Conduct regular phishing awareness training for employees.



- Monitor IOCs in SIEM tools and review access logs for suspicious activity.

Indicators of Compromise (IOCs)



Thank
you

LOUIS.O

