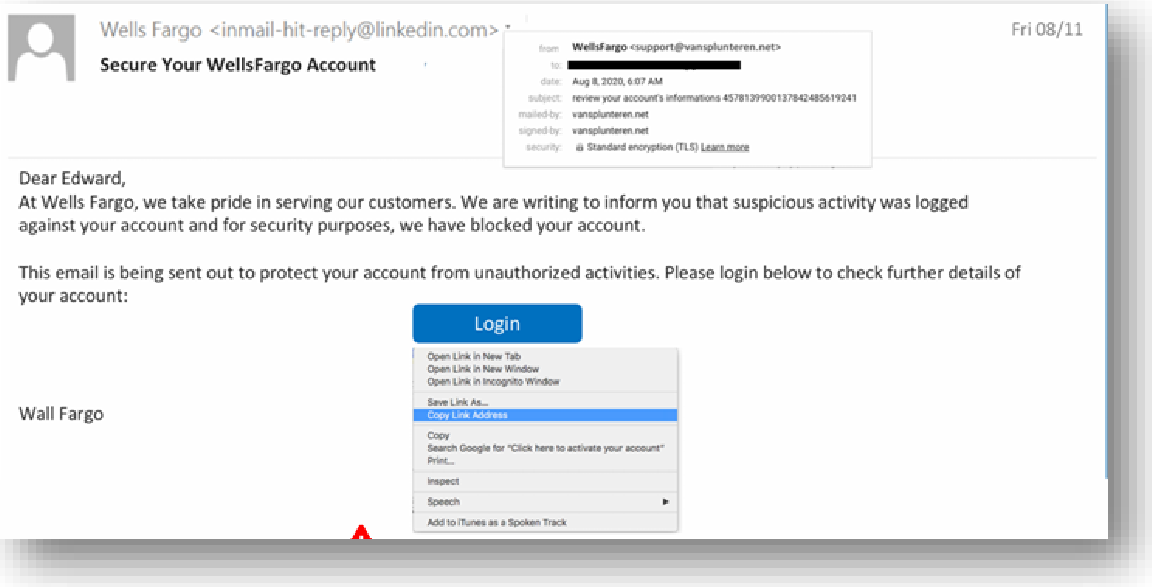
Phishing Email Investigation

Purpose

We are going to investigate a suspected phishing email to determine its legitimacy by performing the following actions:

1. Analyzing embedded URLs for malicious behavior
2. Verifying whether the attached file is malicious
3. Assessing the reputation of the sender's domain

The Phishing Email Screenshot



Wells Fargo <inmail-hit-reply@linkedin.com>

Fri 08/11

Secure Your WellsFargo Account

from: **WellsFargo** <support@vansplunteren.net>
to: [redacted]
date: Aug 8, 2020, 6:07 AM
subject: review your account's informations 4578139900137842485619241
mailed-by: vansplunteren.net
signed-by: vansplunteren.net
security: Standard encryption (TLS) Learn more

Dear Edward,
At Wells Fargo, we take pride in serving our customers. We are writing to inform you that suspicious activity was logged against your account and for security purposes, we have blocked your account.

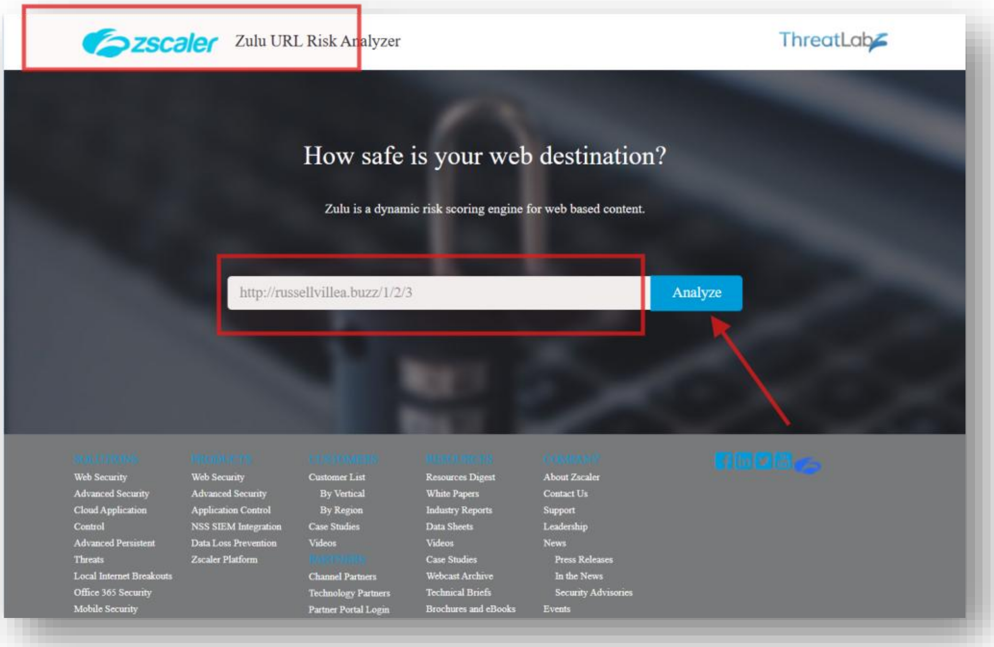
This email is being sent out to protect your account from unauthorized activities. Please login below to check further details of your account:

Wall Fargo

Login
Open Link in New Tab
Open Link in New Window
Open Link in Incognito Window
Save Link As...
Copy Link Address
Copy
Search Google for "Click here to activate your account"
Print...
Inspect
Speech
Add to iTunes as a Spoken Track

Section 1: Check If URLs Are Malicious

To analyze the URLs contained in the email, I used **Zscaler**, a reliable web security tool for URL reputation analysis.



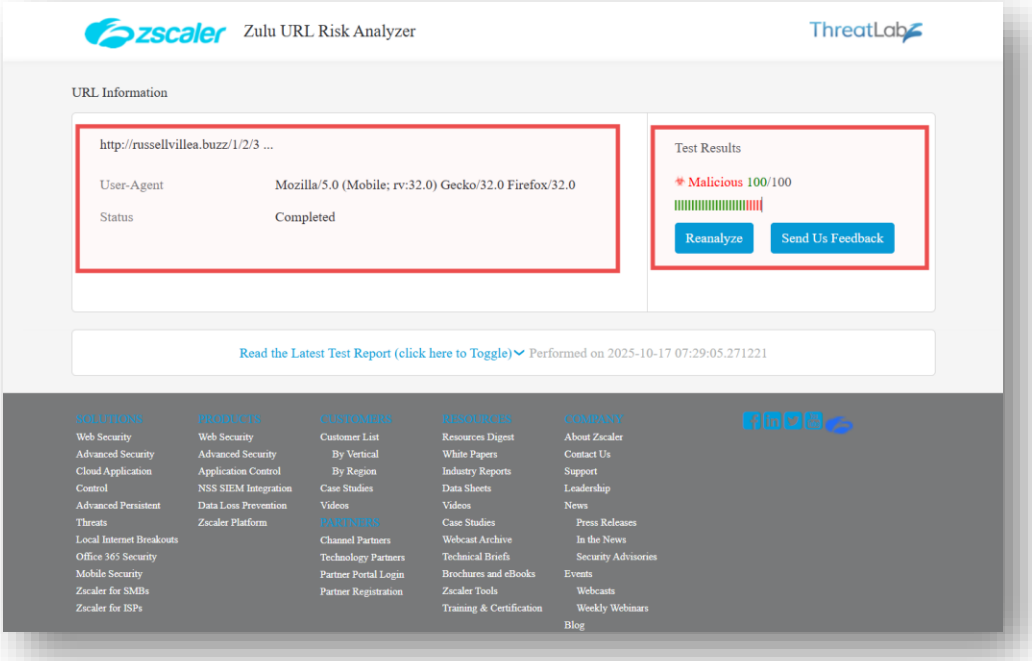
zscaler Zulu URL Risk Analyzer

How safe is your web destination?

Zulu is a dynamic risk scoring engine for web based content.

http://russellvillea.buzz/1/2/3

The results clearly indicated that the URL was **100% malicious**.



zscaler Zulu URL Risk Analyzer

URL Information

http://russellvillea.buzz/1/2/3 ...

User-Agent Mozilla/5.0 (Mobile; rv:32.0) Gecko/32.0 Firefox/32.0

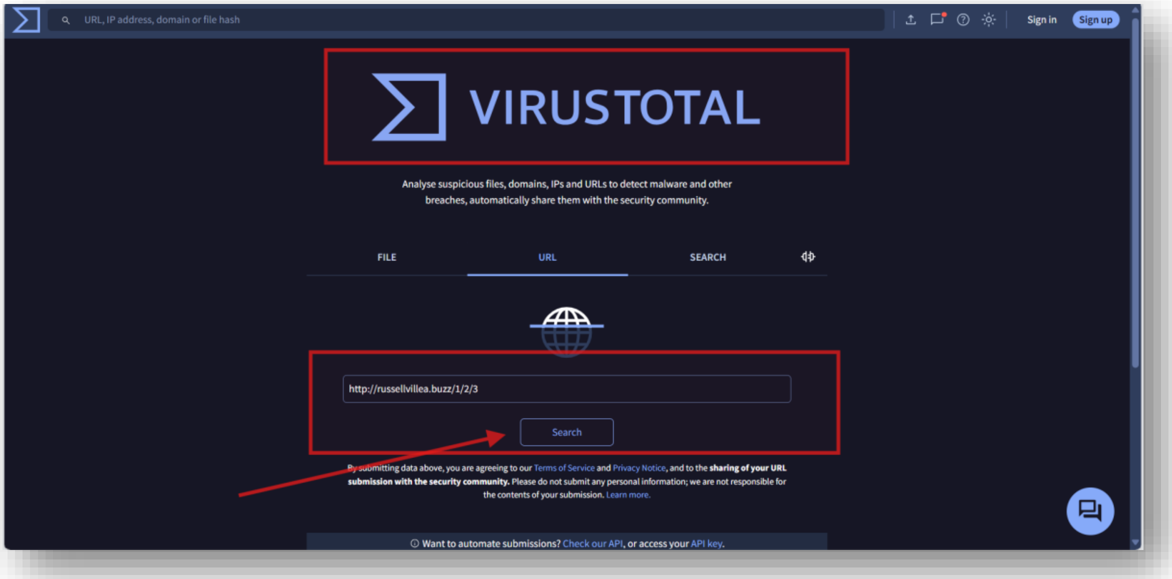
Status Completed

Test Results

Malicious 100/100

Read the Latest Test Report (click here to Toggle) Performed on 2025-10-17 07:29:05.271221

I also verified the same URL using **VirusTotal**, which provides detailed multi-engine reports on suspicious links and files.



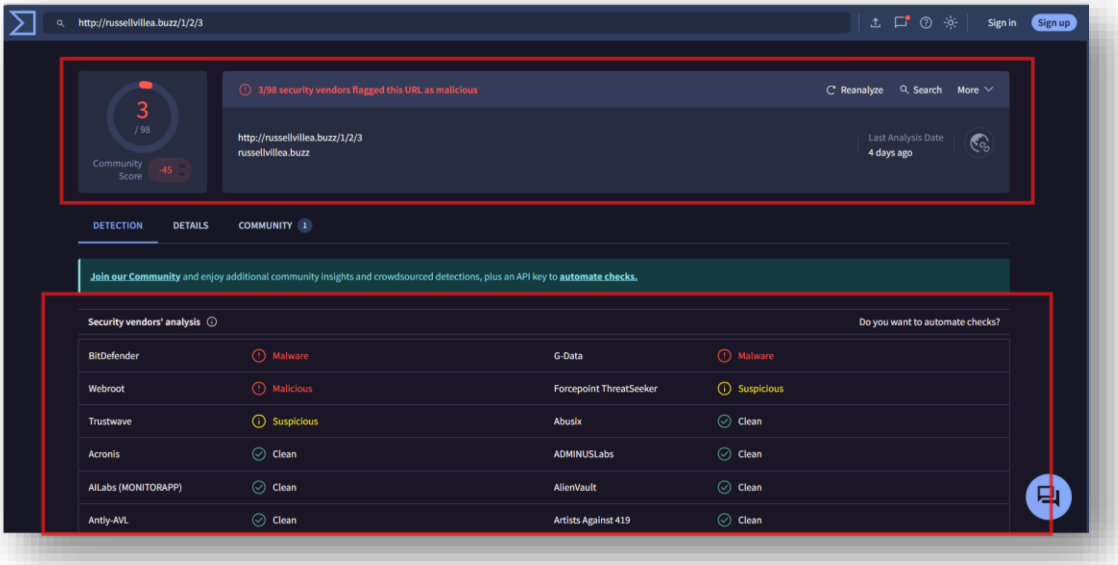
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

http://russellvillea.buzz/1/2/3

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.

The analysis confirmed that the URL was associated with **malicious activity**.



http://russellvillea.buzz/1/2/3

ⓘ 3/98 security vendors flagged this URL as malicious

http://russellvillea.buzz/1/2/3
russellvillea.buzz

Last Analysis Date
4 days ago

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

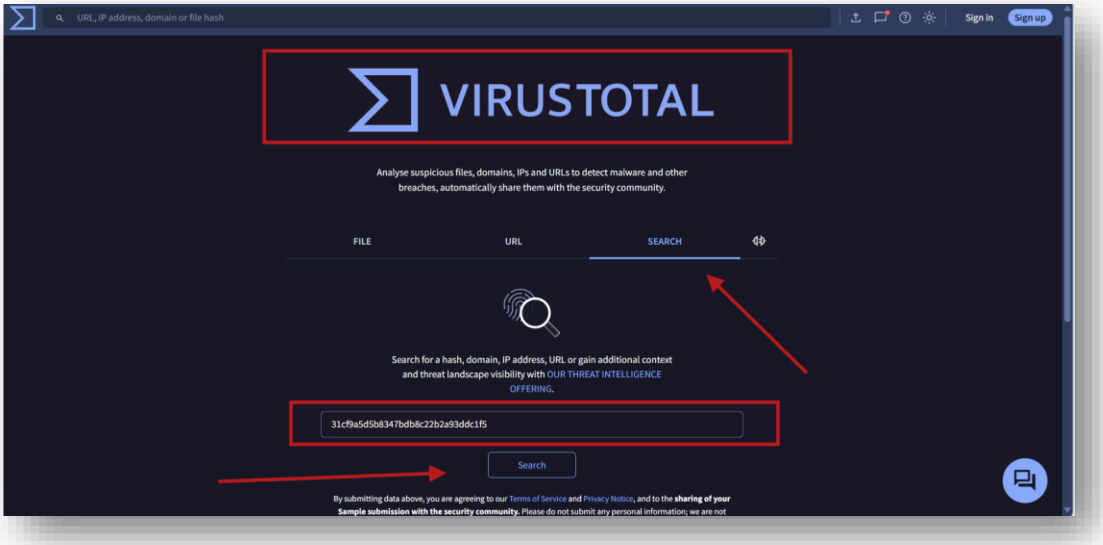
Security vendors' analysis ⓘ

Do you want to automate checks?

BitDefender	ⓘ Malware	G-Data	ⓘ Malware
Webroot	ⓘ Malicious	Forcepoint ThreatSeeker	ⓘ Suspicious
Trustwave	ⓘ Suspicious	Abusix	✓ Clean
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AILabs (MONITORAPP)	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean

Section 2: Is the file malicious (based on the given hash)?

To verify whether the attached file was malicious, I used VirusTotal again. Instead of uploading the file directly, I calculated its hash value **(MD5: 31cf9a5d5b8347bdb8c22b2a93ddc1f5)** using a hash calculation tool and submitted the hash to VirusTotal.So I just pasted the value on the VIRUSTOTAL



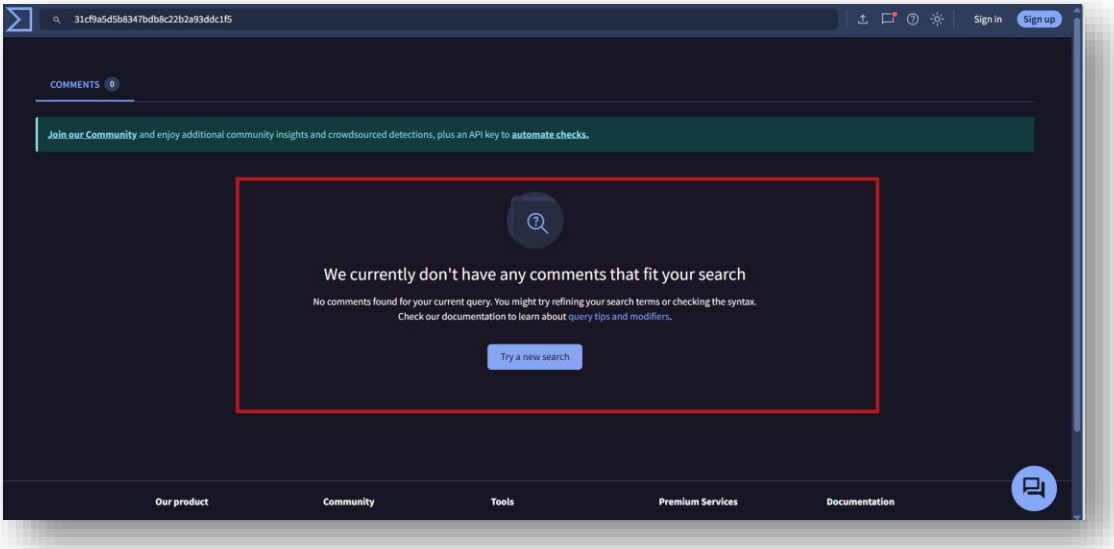
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

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

31cf9a5d5b8347bdb8c22b2a93ddc1f5

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not

The search returned no prior reports for this hash, indicating that the file had not yet been analyzed or flagged by the platform.



31cf9a5d5b8347bdb8c22b2a93ddc1f5

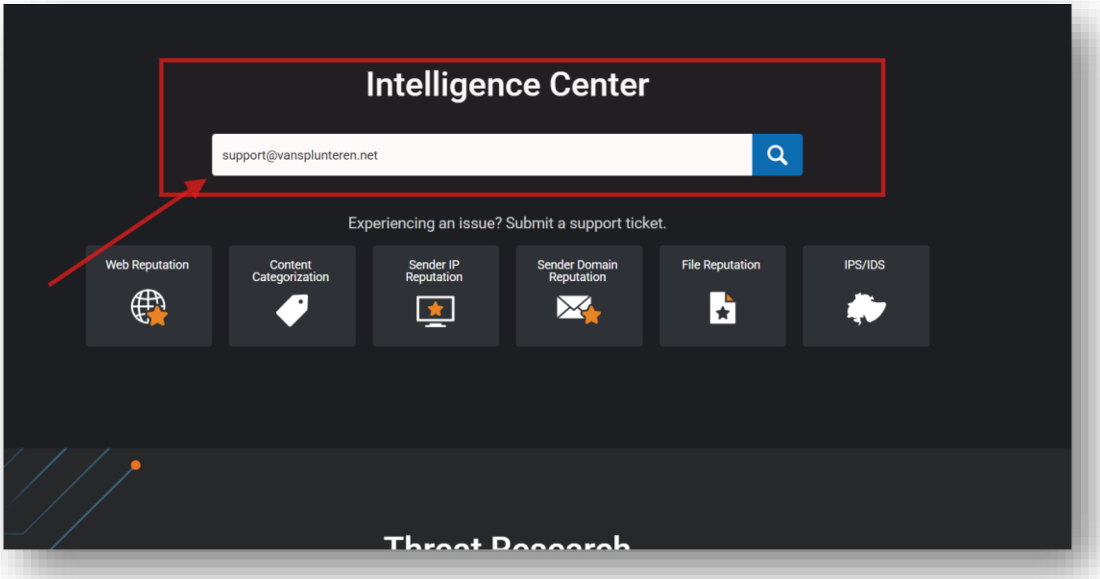
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

We currently don't have any comments that fit your search

No comments found for your current query. You might try refining your search terms or checking the syntax. Check our documentation to learn about query tips and modifiers.

Section 3: Check reputation of the sender domain

To assess the sender's credibility, I examined the domain reputation of vansplunteren.net using Cisco Talos Intelligence.

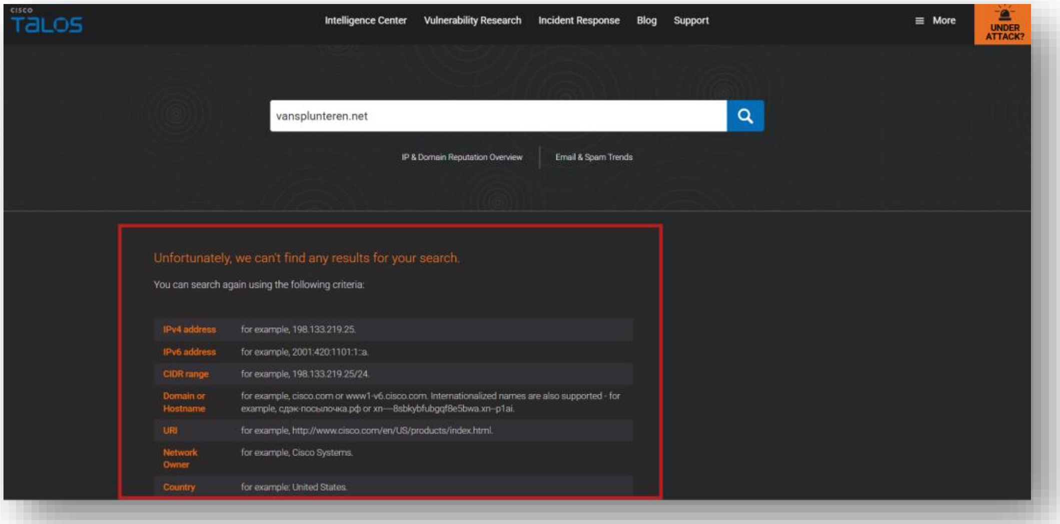


Intelligence Center

support@vansplunteren.net

Experiencing an issue? Submit a support ticket.

The query returned no specific results for this domain, which may indicate that it is neither recognized as reputable nor previously associated with malicious activity.
However, the absence of data for a single email address does not necessarily represent the entire domain's reputation.



vansplunteren.net

Unfortunately, we can't find any results for your search.

You can search again using the following criteria:

IPv4 address	for example, 198.133.219.25.
IPv6 address	for example, 2001:420:1101:1::a.
CIDR range	for example, 198.133.219.25/24.
Domain or Hostname	for example, cisco.com or www1-v6.cisco.com. Internationalized names are also supported - for example, сдэк-посылочка.рф or xn----8sbkybfubgqf8e5bwa.xn--p1ai.
URI	for example, http://www.cisco.com/en/US/products/index.html.
Network Owner	for example, Cisco Systems.
Country	for example: United States.

Conclusion:

The investigation confirmed that the URL included in the email was malicious, while the attached file hash was not previously flagged. The sender domain showed no known reputation data. Based on the malicious URL result and phishing indicators, this email can be classified as a phishing attempt.