

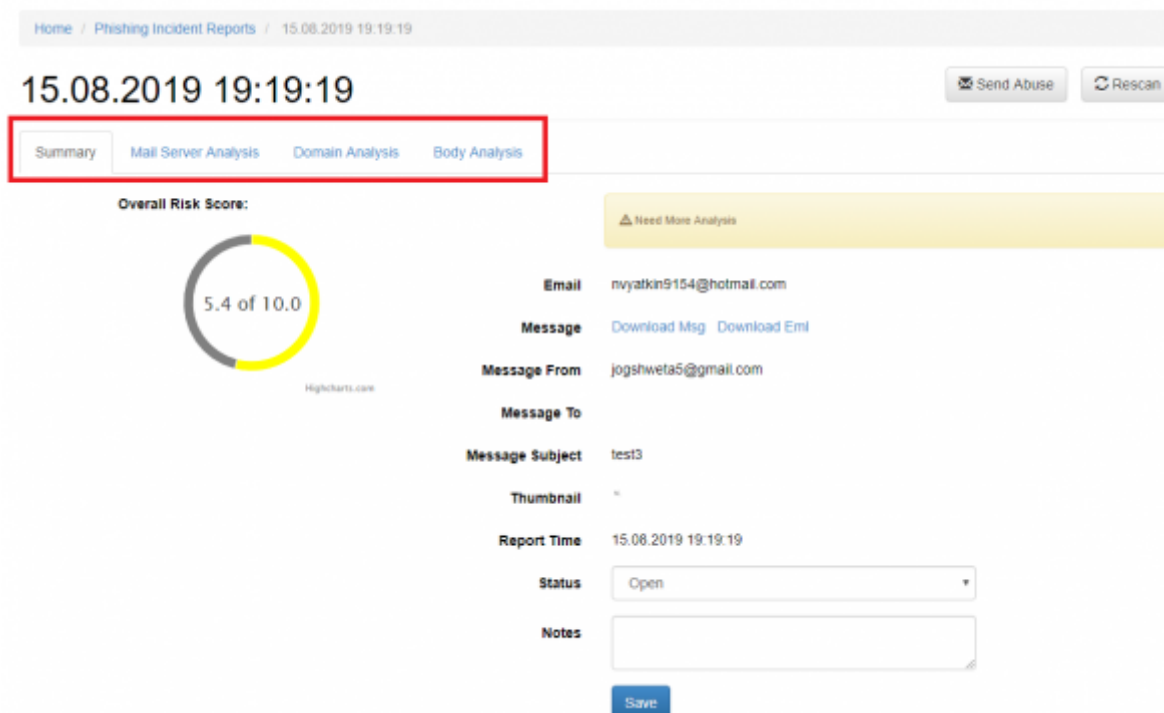
Centralized Analysis

Automatic Incident Analysis (Threat Analyzer)

Once the mail has been reported by the user it will popup as an incident in LUCY in case you have enabled the HTTP option in LUCY. There are a few automatic analysis routines build into LUCY (e.g. check an IP in Google's Safe Browsing Database or Phishtank Database). More checks will follow in the upcoming versions.

When you click on a reported mail you will first see the overall risk score. The overall risk score is a weighted average of the following score from different scans:

- Header Analysis
- Domain Analysis
- Body Analysis




LUCY will automatically flag mail simulations. All other mails can then be manually verified by the administrator. All mails can be downloaded as .msg or .eml file and/or add an incident report.

[Home](#) / [Phishing Incident Reports](#) / 15.08.2019 19:19:19

15.08.2019 19:19:19

[Send Abuse](#) [Rescan](#)

[Summary](#) [Mail Server Analysis](#) [Domain Analysis](#) [Body Analysis](#)

Overall Risk Score:

5.4 of 10.0
Highcharts.com

[Need More Analysis](#)


Email nvyatkin9154@hotmail.com

Message [Download Msg](#) [Download Emi](#)

Message From jogshweta5@gmail.com

Message To

Message Subject test3

Thumbnail 

Report Time 15.08.2019 19:19:19

Status

Notes

[Save](#)

[Home](#) / [Phishing Incident Reports](#)

Phishing Incident Reports

[Send Abuse](#) [Delete](#) [Delete All](#) [Change Status](#) [Download Plugin](#)

Filter

Statistics

<input type="checkbox"/>	Time	Email	Client	Campaign	Score	Status	
<input type="checkbox"/>	08/17/2020 15:17	test@gmail.com	A	5522 (1)	0.00	Simulation	
<input type="checkbox"/>	08/17/2020 14:08	test@gmail.com	N/A	N/A	10.00	Open	
<input type="checkbox"/>	08/17/2020 14:08	test@gmail.com	N/A	N/A	10.00	Open	
<input type="checkbox"/>	08/17/2020 14:07	test@gmail.com	N/A	N/A	10.00	Open	

When a user forwards an email to LUCY all the domains and IP's from the mail header & body are extracted. For each IP and domain LUCY will then lookup public databases like google's safe browsing or phishtank, if any threat was reported:

24.04.2017 13:13

Rescan

Summary

Header Analysis

Domain Analysis

Body Analysis

Domain Source	Domain	PhishTank	Google Safebrowsing	Score
From	weltbild.ch	—	—	0.00
To	muenchow.ch	—	—	0.00
Return-path	bounce.mail.weltbild.ch	—	—	0.00
Received	unusunus.lambda.ecm-cluster.com	—	—	0.00
Received	tux357.hoststar.ch	—	—	0.00
Received	app66.muc.ec-messenger.com	—	—	0.00
Received	app66.muc.domeus.com	—	—	0.00
Received	hp13mta041.muc.domeus.com	—	—	0.00
Dkim-signature	mail.weltbild.ch	—	—	0.00
List-id	700002643.mail.weltbild.ch	—	—	0.00
List-unsubscribe	list_unsubscribe.jsp	—	—	0.00
List-help	shortest-route.com	—	—	0.00
X-csa-complaints	eco.de	✓	—	1.00

The current sources are:

- <https://safebrowsing.googleapis.com/v4/threatMatches:find> (port 443)
- <http://data.phishtank.com/data/online-valid.csv> (port 80)
- DNS BL queries to bl.spamcop.net and zen.spamhaus.org
- CI Army (list) (<http://cinsscore.com/>) - Network security Block Lists.
- Cybercrime tracker (<http://cybercrime-tracker.net/>) -

More sources will be added with each new major release. Lucy will query those sources directly from the location where the software is installed. No data is transmitted back to our infrastructure.

The LUCY admin can also quickly just manually investigate the WHOIS records from the IP's by clicking on the help symbol:

24.04.2017 12:00

Rescan

Summary	Header Analysis	Domain Analysis	Body Analysis
From	IP	By	
v15708.1blu.de	178.254.23.25	tux165.hoststar.ch	
tw124.tattooidea.com	178.254.23.25	v15708.1blu.de	

Copyright © 2017 Lucy Phishing GmbH
All Rights Reserved

Lucy Campaigns Reports

24.04.2017 12:00

Summary Header Analysis

From IP

v15708.1blu.de 178.254.23.25

tw124.tattooidea.com 178.254.23.25

Copyright © 2017 Lucy Phishing GmbH
All Rights Reserved

Whois

This is the RDP Database query session.
The objects are in RDP format.
The RDP Database is subject to Terms and Conditions.
See <http://www.rdp.net/08/support/08-terms-conditions.pdf>
Note: this output has been filtered.
To receive output for a database update, use the "-u" flag.
Information related to '178.254.23.0 - 178.254.23.255'
Block content for '178.254.23.0 - 178.254.23.255' is 'abuse@tux.ch'

```

netname: 178.254.23.0 - 178.254.23.255
status: RDP-08-04
descr: RDP 178.254.23.0/23
country: DE
admin-c: RDP02-RDP
tech-c: RDP02-RDP
org: ORG-RDP02-RDP
status: ASSIGNED PA
mnt-routes: RDP-RDP02-RDP
mnt-by: RDP-RDP02-RDP
created: 2017-03-04T13:18:00
last-modified: 2017-03-04T13:18:00
source: RDP02

```

Filter View Incidents

Home / Phishing Incident Reports

[Send Abuse](#) [Delete](#) [Delete All](#) [Change Status](#) [Download Plugin](#)

Phishing Incident Reports

Filter ▾

Search

From Date To Date

Client Status Email Domain Campaign Score type Min value

[Update](#)

Lucy offers more filter and view options:

1. Search: You can search for any text from the mail subject or body. All emails that contain that exact search string will get displayed. This allows you to quickly identify similar attacks, even if the mail sender and recipients are different.
2. Client: Every campaign is associated with a client. This feature is helpful for MSSP's or companies with multiple legal entities to quickly identify submitted reports from different sources.
3. Date: You can use a date or date range to narrow down your search criteria
4. Domain: This field relates to the sender domain used in the reported email (not the user who reports the Email)
5. Minimum Score: The automatic risk score calculated in the system
6. Campaign: If the Email is associated with a specific campaign from LUCY
7. Select all View
8. All fields are sortable
9. Threat Details can be viewed by clicking on the date

Reported Emails Categories

The reported emails can be categorized by status:

- Open
- In Progress
- Dismissed
- Simulation
- Real Phishing
- Closed

14.08.2020 10:19:30

Summary | Mail Server Analysis | Domain Analysis | Body Analysis

Overall Risk Score:

A donut chart representing the overall risk score. The chart is mostly grey, indicating a low risk level. A small green segment at the top indicates the current score. The text "0.1 of 10.0" is displayed in the center of the chart.

Highcharts.com

Email

Message Download Msg Download Emi

Message From

Message To

Message Subject Fwd: Please join our new corporate WhatsApp group

Thumbnail

The thumbnail shows the beginning of an email body. It starts with a header line containing several underscores followed by the date and time "14.08.2020 10:19:30". Below this is a salutation "Dear Sir," followed by a paragraph of text about creating a WhatsApp group for employees. The text ends with "Kind regards," followed by placeholders for name and company.


Report Time 14.08.2020 10:19:30

Status

Notes

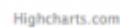
Open
Please select...
Open
In Progress
Dismissed
Simulation
Real Phishing
Closed

The status can be set by the LUCY administrator after clicking on the detail of a reported Email. If you don't want any further notification, please set a status of the open tickets or disable the checkbox on LUCY:

 Rescan

Body Analysis

 Need More Analysis



Task 4a)

To make a more cost-effective business use employees the management board decided to create a 50/50 split between the two countries. The board will give its child units, separately

To perform their job participants should have the opportunity to exchange group members.

Find a group:
Team name:
Team strategy:

..... different results in practice, did not have activities designed and carried out

Save

