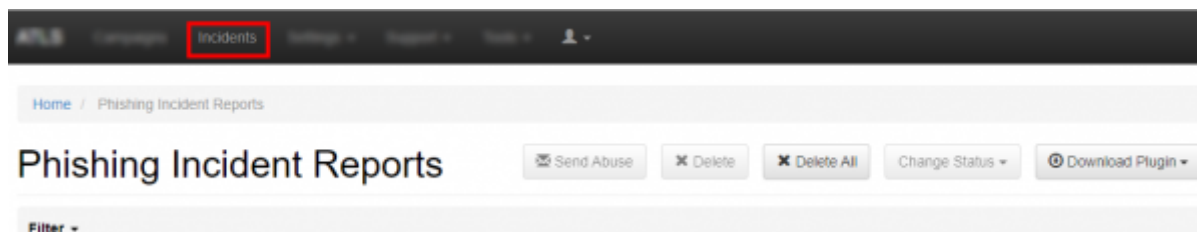


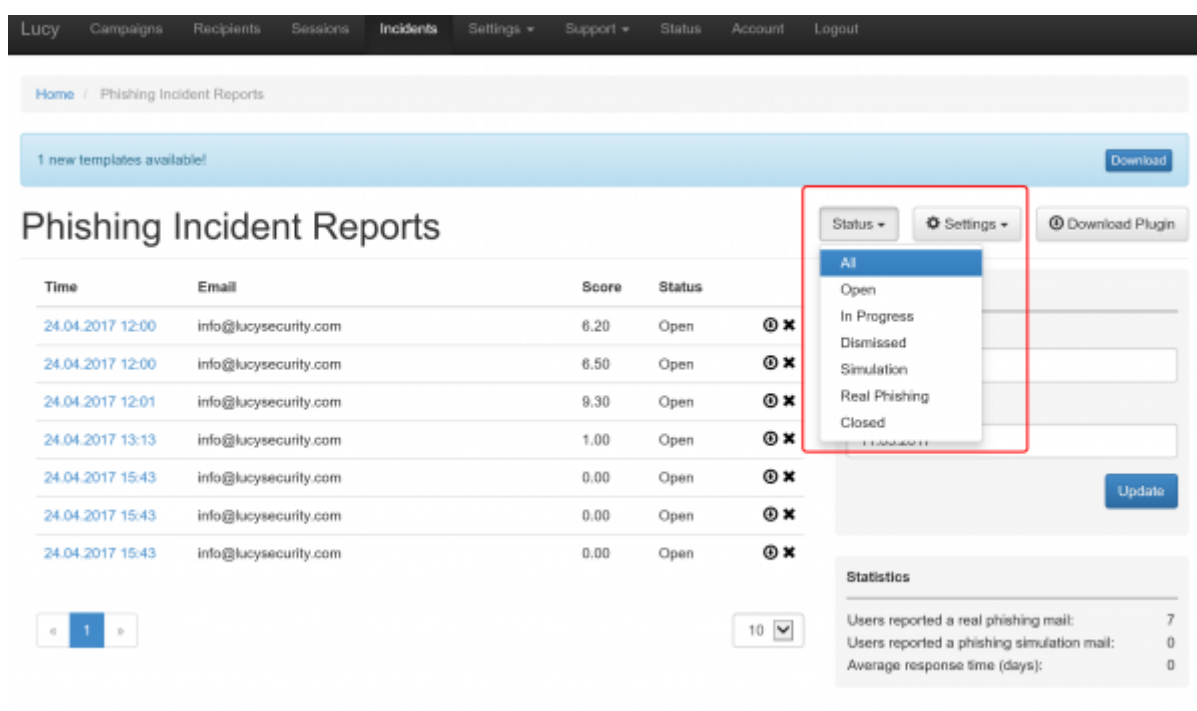
Phishing Incidents (threat analyzer)

LUCY comes with a "Phish Alert" plugin for mail clients. This add-in gives your users a safe way to forward suspected Emails with only one click and have them analyzed automatically by the threat analyzer in LUCY. The tool empowers users to proactively participate in an organization's security program and makes it easy for your employees to report any suspicious email they receive. If you enabled "Send Reports Over HTTP", mail will get forwarded to LUCY. You will find them on the "incident" menu:



Incident Dashboard - Filters & Views

Filter by status: At the top level, LUCY allows you to filter the reported mails by the status of the ticket:



The default status is "open", unless it is a phishing simulation detected by LUCY. The other possible status are:

- 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:

Home / Phishing Incident Reports / 03/22/2018 11:10:44

03/22/2018 11:10:44

Send Abuse Rescan

Summary Header Analysis Domain Analysis Body Analysis

Overall Risk Score:

10.0 of 10.0

Highcharts.com

Email: mailadmin@gaga.com

Message: Download

Message Subject: Welcome to your new Office 365 Account!

Thumbnail:

Report Time: 03/22/2018 11:10:44

Status: Simulation

Notes:

Save

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

Phishing Incident Reports

Status ▾
Delete
Settings ▾
Download Plugin ▾

7	Time	Email	8	Client	Campaign	Score	Status	
<input type="checkbox"/>	02/13/2018 15:19	admin@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	03/22/2018 15:54	mailadmin@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	03/09/2018 12:17	mail-admin@bwg.de	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	03/14/2018 13:29	mail-admin@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	03/22/2018 11:10	mailadmin@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	03/07/2018 17:30	mail-admin@secure-log-in.info	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	02/12/2018 16:38	microsoft@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	02/12/2018 16:21	microsoft@gaga.com	N/A	N/A	10.00	Simulation	📧 📧 📧	
<input type="checkbox"/>	01/23/2018 15:32	noreply@access.phishing.services	N/A	N/A	10.00	Open	📧 📧 📧	
<input checked="" type="checkbox"/>	03/06/2018 10:56	nsa@gaga.com	N/A	N/A	1.80	Simulation	📧 📧 📧	

10 rows per page

Filter

Search

Client

From Date

To Date

From Domain

Min Score

Campaign

Update

1

2

3

Statistics

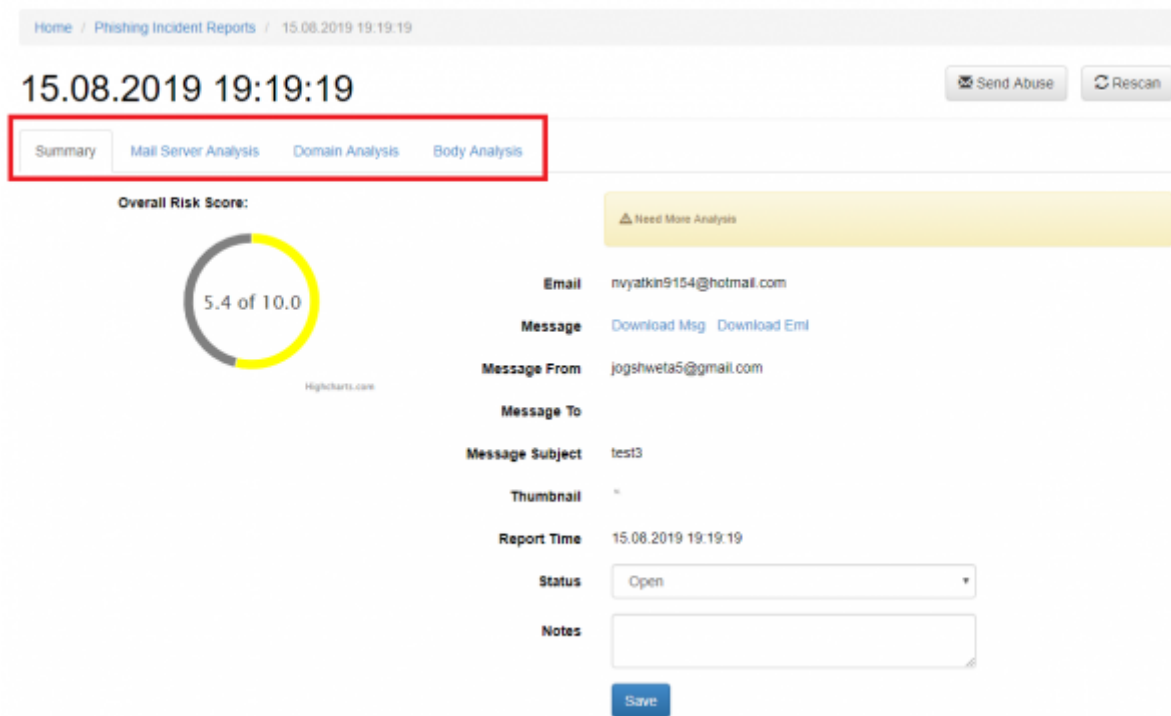
Total:	27
Real Phishing:	0
Simulation:	22
Other (total - real - simulation):	5
Average response time (days):	0

Automatic Incident Analysis (Threat Analyzer)

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.

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



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

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.lambdas.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 (LUCY 3.7) are:

- <https://developers.google.com/safe-browsing/v4/lookup-api>
- <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:

The screenshot shows the LUCY interface with a date/time stamp of 24.04.2017 12:00 and a Rescan button. The main report is titled 'Summary' and shows a table of email data:

From	IP	By
v15708.1bku.de	178.254.23.25	tux165.hoststar.ch
tw124.tattooidea.com	178.254.23.25	v15708.1bku.de

A red box highlights the IP address 178.254.23.25 in the second row. A red arrow points from this box to a 'Whois' window that is open. The 'Whois' window displays the following information:

```

This is the RIPE Database query service.
The objects are in RRD format.
The RIPE Database is subject to Terms and Conditions.
See http://www.ripe.net/db/support/db-terms-conditions.pdf

Note: this output has been filtered.
To receive output for a database update, use the "-a" flag.

Information related to '178.254.23.25':

 abuse-contact for '178.254.23.25 - 178.254.23.255' in 'abuse@tux165.ch'
 last-modified: 178.254.23.25 - 178.254.23.255
 netname: 178-254-23-25
 descr: 178-254.23.25
 country: DE
 admin-c: RIPE-RIPE
 tech-c: RIPE-RIPE
 status: ASSIGNED PA
 net-without: 178-254-23-25
 created: 2017-03-08T13:18:00
 last-modified: 2017-03-08T13:18:00
 source: RIPE
  
```

Detection of real phishing mails vs. Phishing simulations

The plugin automatically handles emails created in a phishing simulations from LUCY: it will ensure that only reports of potentially malicious emails are delivered to appropriate security staff. All emails created by LUCY itself will create a custom message to inform the user, that the mail has been send as a part of a security awareness program. LUCY generated phishing mails won't be forwarded to the security team. But they will be reported back to LUCY in order to process the information within the campaign statistics. The reported mails will then be purged from the successful attack listings in LUCY.

Where are incidents (LUCY generated emails) from the plugin reported?

If a user spots the phishing simulation and reports the email, you can see this information in various places:

- Incident widget on the dashboard:

The screenshot shows the LUCY dashboard with a 'Campaigns' section. A red box highlights a widget titled 'Statistics Phish Alert' which displays the following data:

Statistics Phish Alert	
Users reported a real phishing mail:	24
Users reported a phishing simulation mail:	4
Average response time (days):	0

- Incident tab:

Phishing Incident Reports

Time	Email	Score	Status
04/02/2018 11:14	oliver@muenchow.ch	10.00	Simulation
03/23/2018 00:02	test.igor@hotmail.com	10.00	Simulation
03/22/2018 23:52	test.igor@hotmail.com	10.00	Simulation
03/22/2018 23:51	test.igor@hotmail.com	10.00	Simulation
03/22/2018 15:57	oliver@muenchow.ch	10.00	Simulation
03/22/2018 15:54	mailadmin@gaga.com	10.00	Simulation
03/22/2018 11:10	mailadmin@gaga.com	10.00	Simulation
03/15/2018 13:55	oliver@muenchow.ch	0.00	Open
03/14/2018 13:35	oliver@muenchow.ch	10.00	Open
03/14/2018 13:34	oliver@muenchow.ch	10.00	Simulation

- Under the campaign statistics (recipients) under the "reported" item:

Results

Summary

Statistics

File Downloads

Collected Data

Recipients

Awareness Website

Benchmark

Compare

Reports

Exports

Configuration

Base Settings

Awareness Settings

Schedule

Name	OS	UA	Plugins	Succ	Train
Oliver Muenchow Login	-	-	-	-	-
Oliver Login	-	-	-	-	-
Kaduu Login	-	-	-	-	-
Oliver Muenchow Login	Windows 7	MSIE 11	-	✓	-

Name: Oliver Muenchow

E-mail: oliver@kunstwarenhaus.ch

Phone: -

Lure Sent: -

Message Sent: 05/08/2018 16:20:22






Training Sent: -

Reported: -

Plugins: Silverlight Plug-In 5.1.50907.0

Vulnerable Applications (0): N/A

- If you want a comparison of all reported emails, you can export the whole campaign data via CSV. Within the CSV there is a reported column:

Results	Action	Type	Filter / Details
Summary	 Export	Recipients	All
Statistics	 Export	Recipients	Succeeded to Group
Reports	 Export	Recipients	Export recipients within submitted time range to a new group
Exports	 Export	Benchmark	Export campaign benchmark results
Configuration	 Export	Collected Data	Export collected data
Base Settings			

In LUCY 4.4, the incidents reports will also be integrated on the dashboard under the general statistics.

From:

<https://wiki.lucysecurity.com/> - LUCY

Permanent link:

https://wiki.lucysecurity.com/doku.php?id=threat_analyzer_-_mail_plugin&rev=1559571302

Last update:

2019/07/25 12:51

