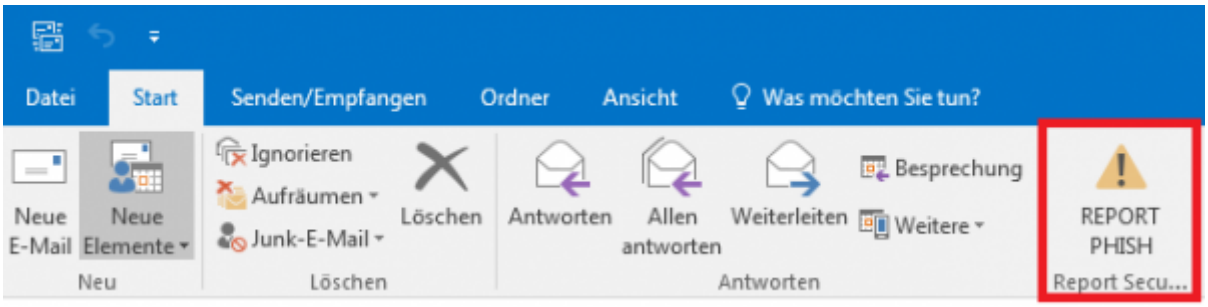
Mail client plugin and threat-analyzer

Introduction

LUCY comes with a "Phish Alert" plugin/addon for mail clients or browsers:

- Outlook 2010,
- Outlook 2013
- Outlook 2016
- Office365
- Office for Mac 2016
- Gmail

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. It has two main features

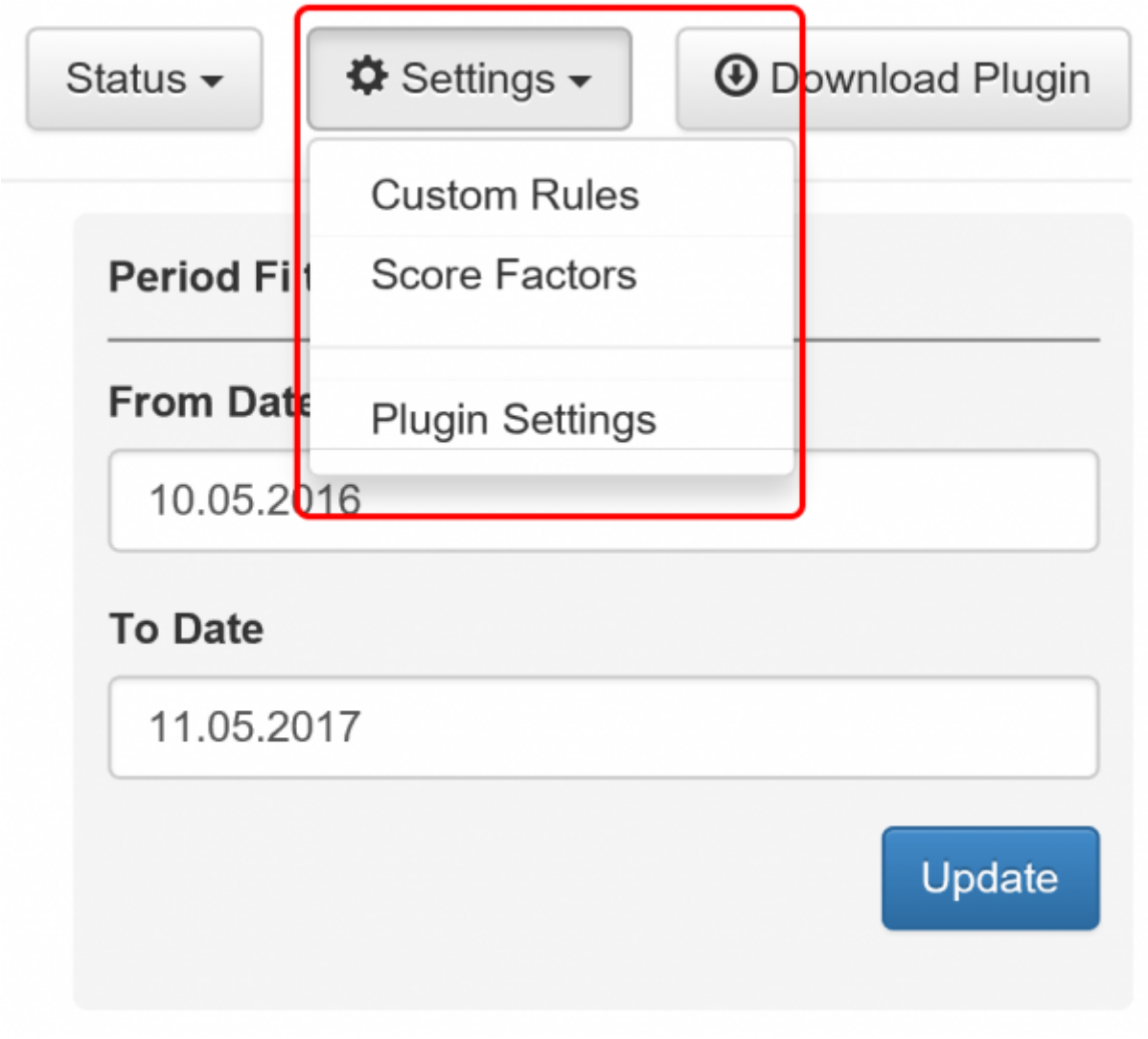


a) Forward the mail (.msg) to a predefined mail address (e.g. your security team). Within the plugin you have the ability to define a custom message that appears to the user after the mail gets reported. Once the message gets forwarded to your team, it will automatically be deleted from the user's inbox to prevent future exposure. b) Report back to LUCY: the plugin may forward suspected phishing emails as well LUCY generated emails back to the LUCY server via HTTPS. If the mail was generated by LUCY, the reports will automatically be processed within the campaign statistics. All other emails can be analyzed in LUCY using our threat analysis engine.

Configuration

The configuration of the plugin and phishing incidents is done within the settings menu (admin/settings/incident-settings) where you can define the settings for:

- MSI Installer
- Custom Rules (create special rules with Regex filters to flag emails)
- Score Factors (adjust the scores for specific incident events)



MSI Installer Settings: The following settings can be configured (this is a small selection; every LUCY release has its own settings. Please contact us for a full configuration tutorial):

Home / Phishing Incident Reports / Settings

Settings

Email	info@kaduu.ch
Thank You Message	Thanks for your help. We will investigate the email anc
Thank You Message For Lucy Emails	Thank you. This was a LUCY phishing simulation. Goc
Button Message	Report Email
Group Label	Group Label
Button Super Tip	Button Super Tip
Report Title	Report Title
Error Title	Error Title
User Request Message	User Request Message
Deeper Analysis Request Message	Deeper Analysis Request Message
No Selection Message	No Selection Message
Eval Error Message	Eval Error Message
Send Error Message	Send Error Message
Unsupported Message	Unsupported Message
Subject	Here is an email reported by LUCY
Ribbon Label	Ribbon Label
ICO	Choose File No file chosen

- [x] Send Reports Over HTTP
- [ ] Send Reports Over SMTP
- [ ] Use SMTP for receiving incident reports on Lucy
- [ ] Never report phishing simulations
- [ ] Use X-Headers in Forwarded Emails
- [ ] Inline Message Forwarding
- [x] Deeper Analysis Request

- [ ] Notify of Expired Incidents

Save

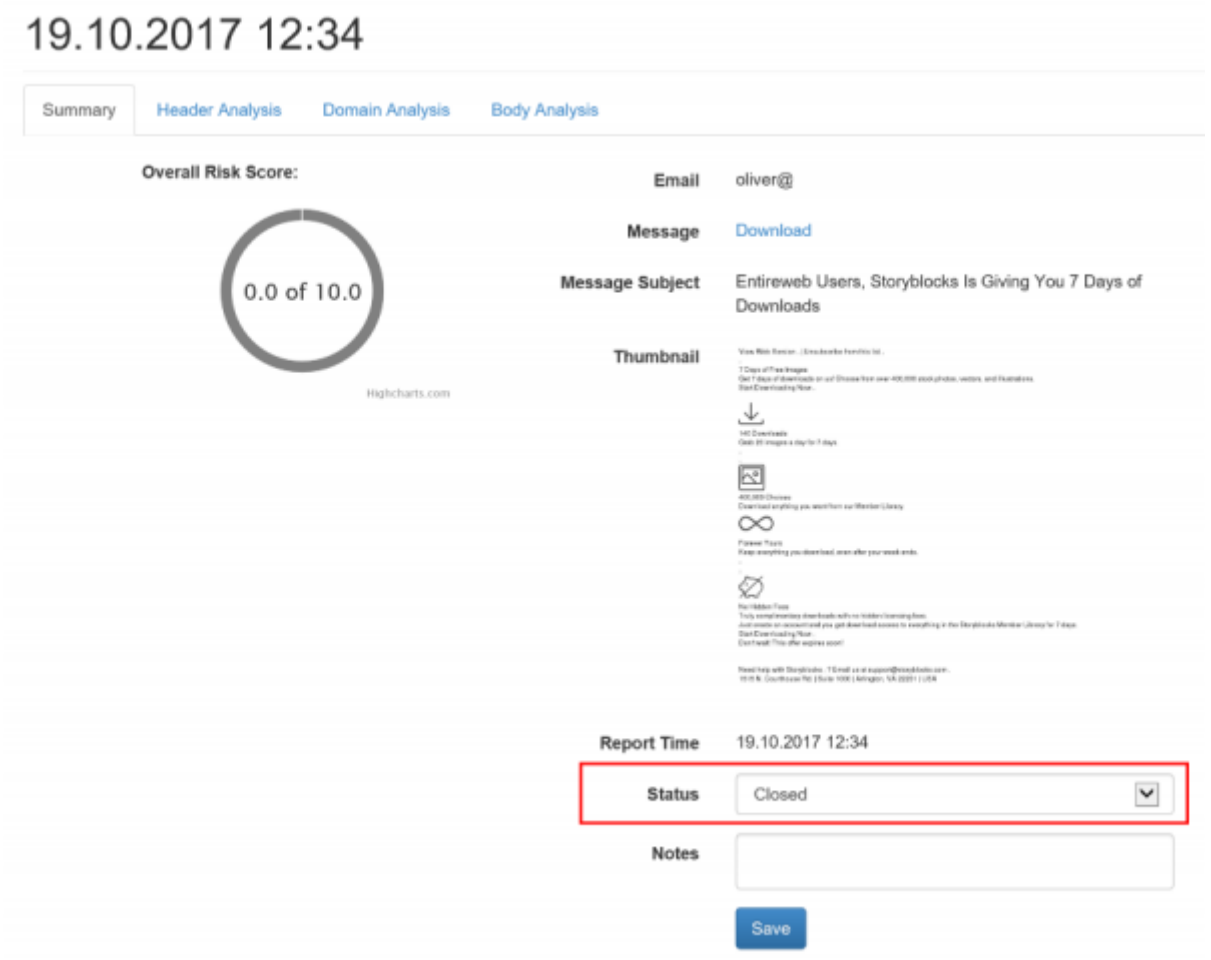
Appearance Settings

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Email	the mail address of your security team. This is the address, where suspected phishing mail gets forwarded. The whole mail will be attached as a .msg and send to a predefined mail address. You may use multiple emails separated by a semicolon symbol (;). Example: john@doe.com;bill@gates.com.	+	+	+
Thank you message	The message that will be displayed after the user marks a suspected phishing email and pushed the plugin button.	+	+	-
Thank you message for LUCY mails	The message that will be displayed for all emails, that are created by LUCY within a simulated phishing campaign.	+	+	-
Button Message	The name of the button in Outlook.	+	+	-
Group Label	Reserved for future release.	-	-	-
Button Super Tip	The help text displayed when the user hovers the mouse over the button.	+	+	-
Report Title	The title of the message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.	+	+	-
Error Title	The title of the message that will be displayed when any error occurs.	+	+	-
User Request Message	The message that will be displayed after the user marks a suspected phishing email and clicks the plugin button.	+	+	-
Deeper Analysis Request Message	Deeper analysis request confirmation text. This message box is shown after user clicks on the report button.	+	+	-
No Selection Message	The title of the message that will be displayed after the user clicks phish button without any selected email.	+	-	-
Eval Error Message	Text displayed when the error of getting the selected item occurs.	+	-	-
Send Error Message	The message that will be displayed when an issue with sending the report occurs.	+	-	-
Unsupported Message	Text displayed when user tries to report an unsupported item (calendar event, etc).	+	-	-
Subject	The subject of the forwarded email message when sending a report over SMTP.	+	+	+
Ribbon Label	The name of the area in which the button is located.	+	-	-

Behavior Settings

Setting Name	Description	Outlook (MSI)	Office365 (XML)	Gmail
Send Reports Over HTTP	Enable this option, if you want the Outlook Plugin to send a copy of the reported phishing mail to LUCY (does not include emails from phishing simulations) and additionally add the statistical info about reported phishing emails to LUCY.	+	+	+
Send Reports via SMTP	Enable this option, if you want to forward the mail to the predefined mail address via SMTP. If enabled, the plugin will send the report to the email you provided on the same page. That is supposed to be your own email or the email of your security team. Do not enable both options (send reports via HTTP and send reports via SMTP at the same time). Only pick one delivery method.	+	+	+
Use SMTP for receiving incident reports on Lucy	if enabled, Lucy will suppose it has to intercept emails that plugin sends over SMTP, so it configures the local postfix accordingly. All emails received will be added to incidents. If you do not enable this, even if the email configured points to Lucy, nothing will happen - Lucy won't wait for reports over SMTP.	+	+	+
Never report phishing simulations	No reports will be sent over SMTP if user reports a simulation email generated by Lucy. So the plugin will send only "real phishing" emails over SMTP. If HTTP is disabled as well, Lucy will not get these reports either, as there is no other delivery method configured for these reports.	+	+	+
Use X-Headers in Forwarded Emails	If true, the plugin will make the following changes in the email forwarded over SMTP: * Add a new header X-CI-Report: True * Add a HTML code X-CI-Report: True after the body tag within the email body.	+	+	-
Inline Message Forwarding	If true, the plugin will clear the body of the forwarded email when sending the report via SMTP.	+	+	-
Deeper Analysis Request	If true, the plugin will ask the user whether to request deeper analysis of the reported phishing mail.	+	+	-
Notify of Expired Incidents	Check this to receive notification if there are reports older than 30 days. This notification will be delivered via email.	+	+	+

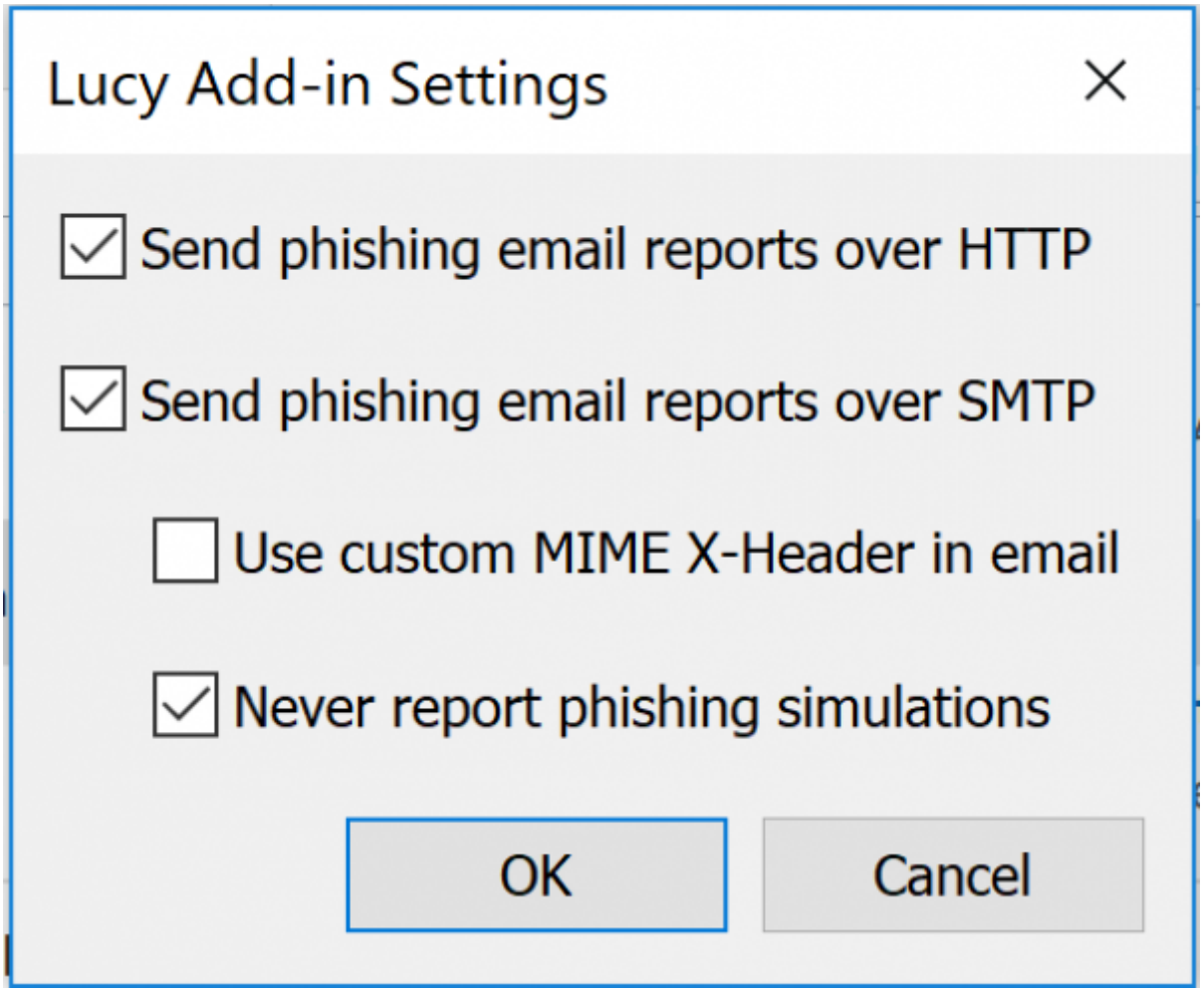
If you don't want any further notification, please set a status of the open tickets or disable the checkbox on LUCY:



The algorithm logic for the different delivery options in the plugin is as follows:

1. Is HTTP enabled? If yes, send a report over HTTP, regardless of its status (simulation or real)
2. Is SMTP enabled? If no, stop, otherwise go to next
3. Is "Never report phishing simulations (Suppress SMTP)" enabled AND this is a simulation email? If BOTH are yes, then stop, otherwise go next
4. Send report over SMTP

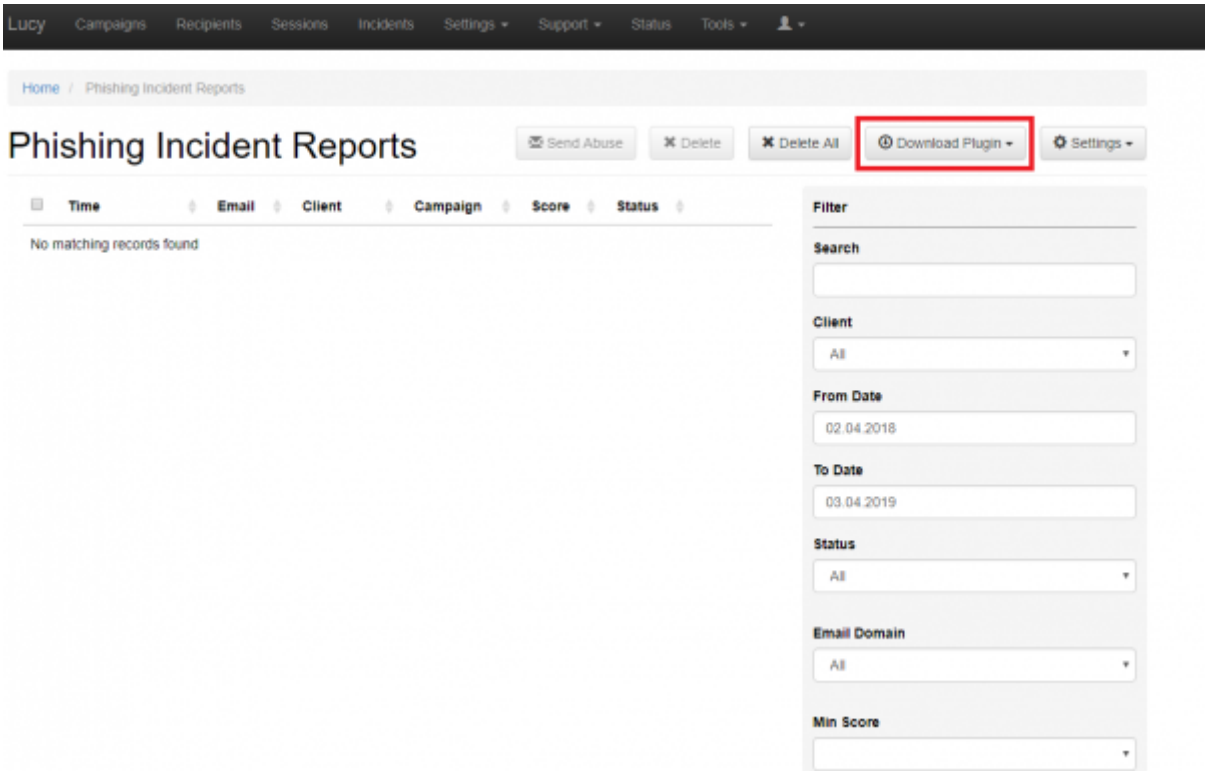
Once you configured the plugin in the LUCY UI and install it, you will notice that the settings can be viewed or changed locally:



Known Issues: if you use SMTP for receiving incident reports on Lucy within the incidents, Lucy will intercept all your emails to the domain specified. If you use example.com as a domain for receiving the incidents in LUCY, the internal Postfix server will be listening for this domain for incoming mails. If you now start at the same time a phishing or awareness campaign and try to send your emails to "@example.com", LUCY will not forward those emails externally.

Download Outlook Plugin & Deployment

The deployment can be done via MSI file which can be downloaded after the initial configuration under the "incidents" menu (/admin/incidents). The plugin installer needs user to have read and write access at least to keys under HKCU (current user).



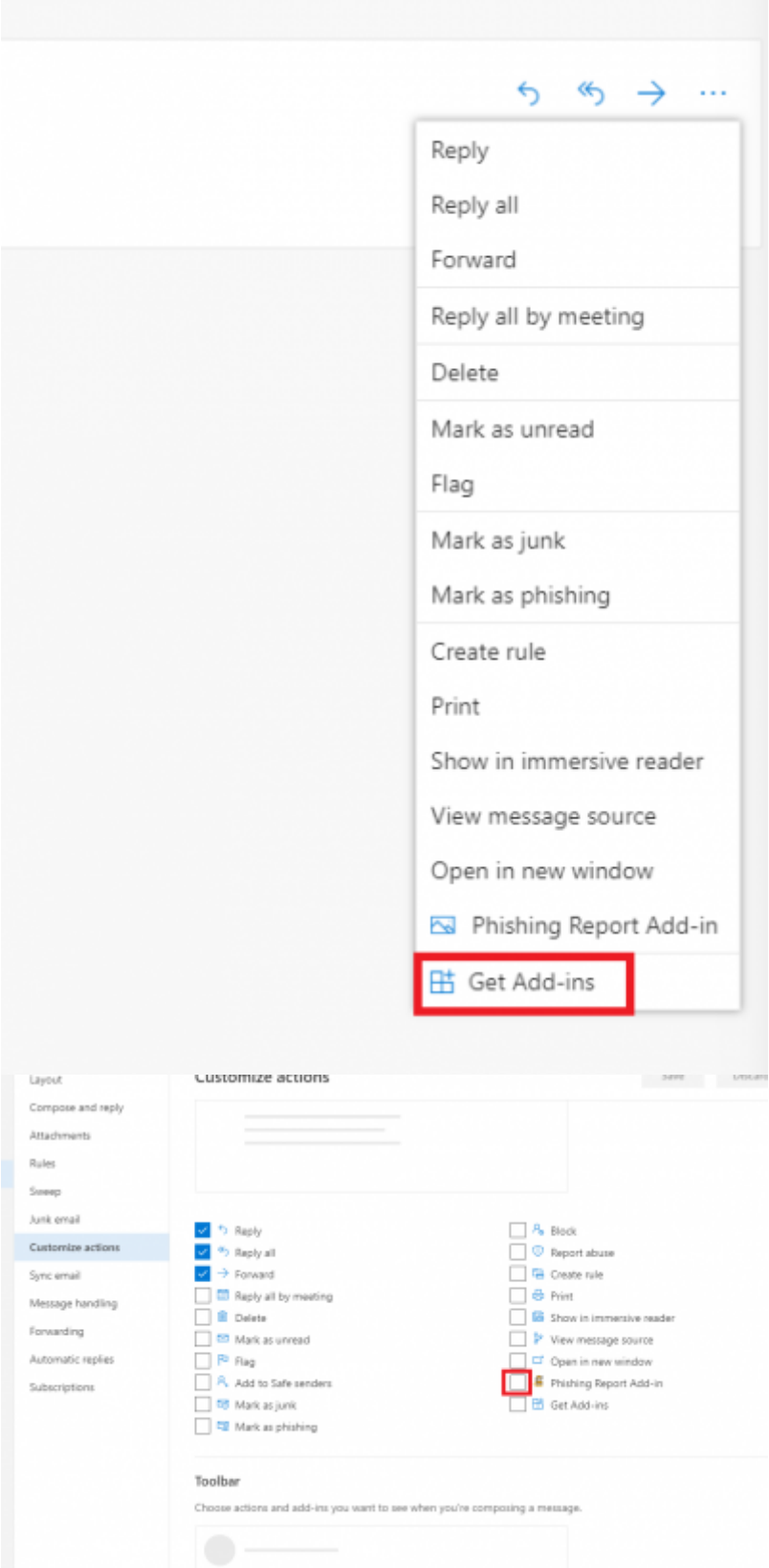
Upon installation, a temporary config.dat file is created. But all settings are written in the registry and can therefore be controlled via GPO. The plugin may be installed in the user context HKCU or in machine context (to HKLM.

Download Office365 Plugin & Deployment

The Outlook 365 button works the same as the Outlook client – just for the web based Outlook access 365. The XML is the file that needs to be installed for O365:

Outlook 365 sequence:

1. go to incidents, press "Download Plugin" → "Microsoft Outlook 365", your browser will download an XML file
2. go to MS Outlook - https://outlook.live.com/owa/
3. open any email and press "Get Add-ins" as it described on the screenshot below
4. go to "My add-ins" and upload the XML file from the step 1
5. go to Settings → Customize actions, select the LUCY Add-In, press "Save" button
6. Now in email panel, you will see a monkey icon, which is the add-in
7. press the monkey and hit "Send Report" on the right
8. on Macs the monkey will be visible on the ribbon menu

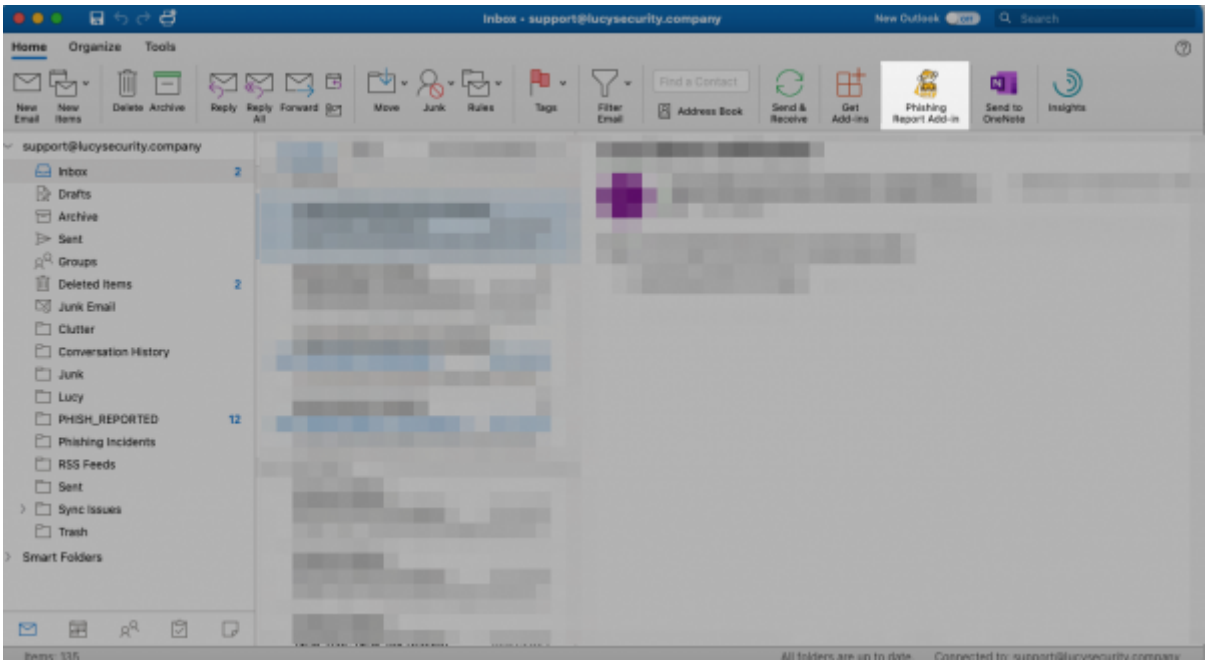


Deployment on Apple Computer

Microsoft has "Office for Mac 2016" product, which requires the O365 account to run. When you open Outlook application on Mac, it fetches all plugins from the corresponding O365 account and shows them in the interface, so the plugin is available both in the web interface and on Mac. Therefore, you first need to install the plugin in O365 before you set it up on a MAC.

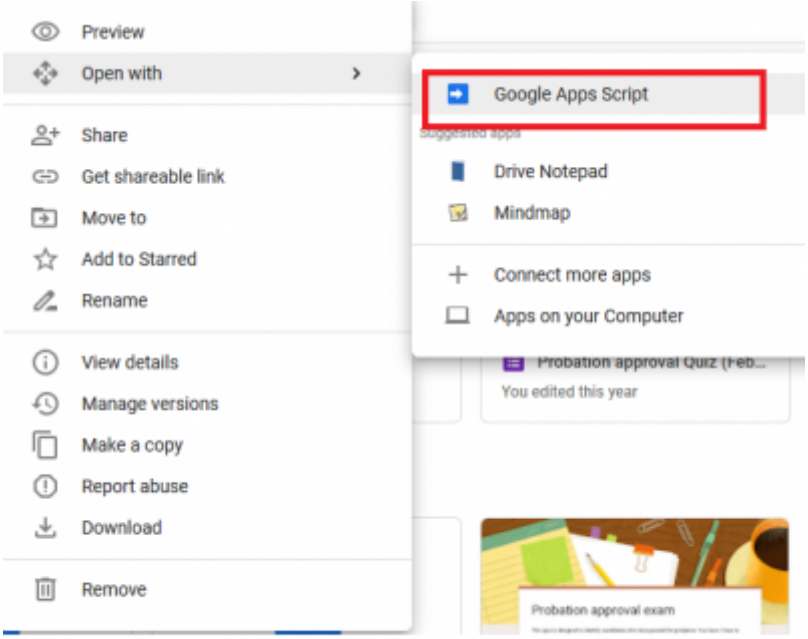
Outlook 365 sequence:

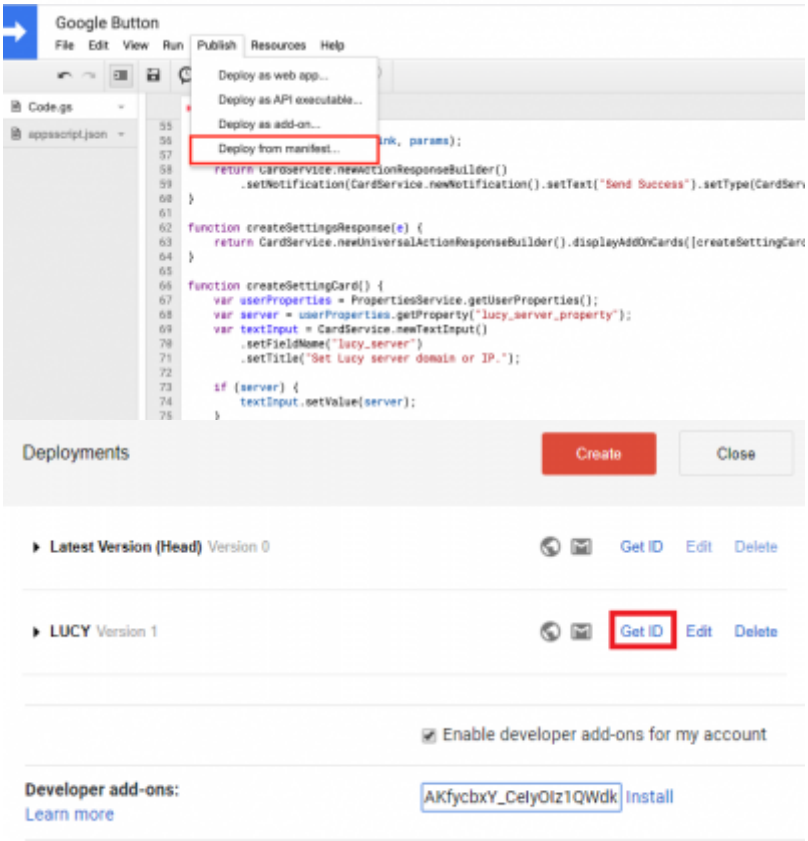
1. Go to incidents, press "Download Plugin" → "Microsoft Outlook 365", your browser will download an XML file
2. Go to MS Outlook - https://outlook.live.com/owa/
3. Press "cog" icon and then "Manage Add-ins"
4. Click "Click here to add a custom add-in" text right below the page title
5. Upload the XML you downloaded on step 1
6. Go to any email in your inbox, you will see a little monkey on the top right in email header
7. Press the monkey and hit "Send Report" on the right
8. On Macs the "LUCY" symbol will be visible on the ribbon menu



Gmail Plugin & Deployment

1. Download Gmail plugin file from Lucy
2. Open Google Drive in a web browser, select the uploaded file, click on it with the right mouse button and choose "Open with" → Connect more apps → Search for "Google Apps Script" → Connect
3. Right click on the file again, "Open with" → Google Apps script
4. A new tab will open, there In main menu click "Publish" → "Deploy from manifest"
5. The modal window will open, click "Get ID" in there
6. Copy the "Deployment ID" from the window
7. Go to Gmail web application, go to "Settings" → "Add-ons" (https://mail.google.com/mail/u/0/#settings/addons)
8. Enable "Allow add-ons for developers in this account" checkbox
9. Paste add-on's Deployment ID into the "Install developer add-on" textbox and click "Install"
10. In the "Install developer add-on" dialog that appears, click the checkbox to indicate that you trust this developer, then click Install

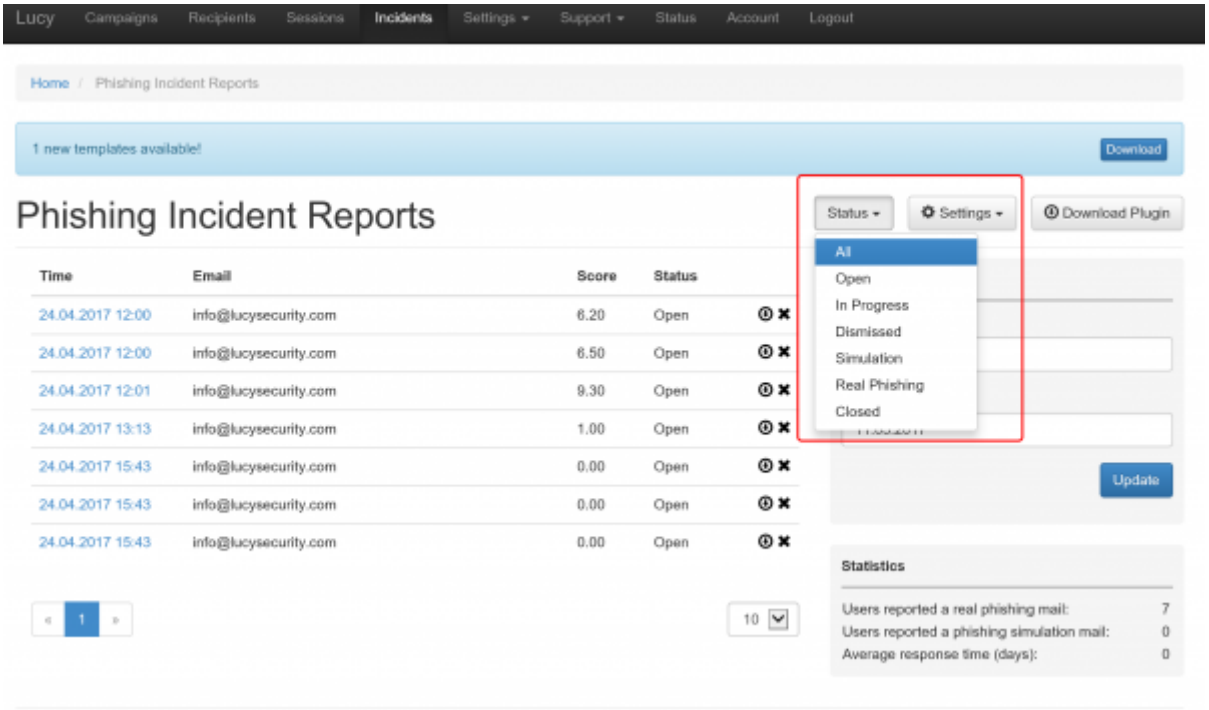




Where do you see the incidents reported by the users?

Phishing Incident Center Features (threat analyzer)

- **Dashboard Filter:** LUCY allows you to filter the incoming mails on the dashboard:



- **Centralized Analysis:** This feature allows you to analyse the incoming mails manually or automatically (see next chapter)
- **Centralized Campaign Reporting:** Any reported mail which is part of a phishing simulation will be processed within the campaign statistics
- **Threat Mitigation**: The Threat Mitigation (LUCY 3.5) allows you to take actions against legitimate phishing attacks
- **Custom Regex & Score**: LUCY allows you to define custom rules to scan mails for specific keywords and flag them with a individual threat score.

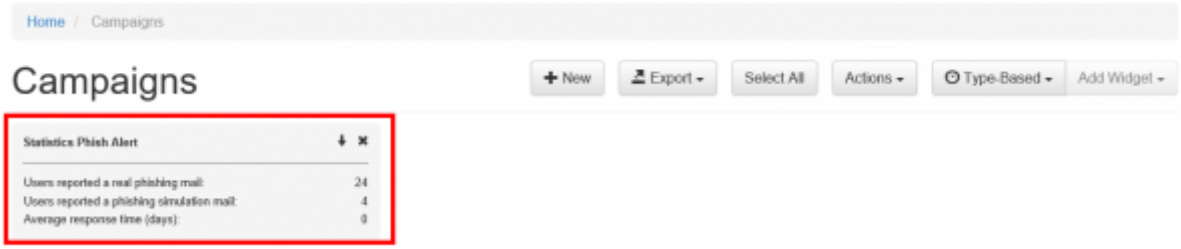
Detection of real phishing mails vs. Phishing simulations

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.

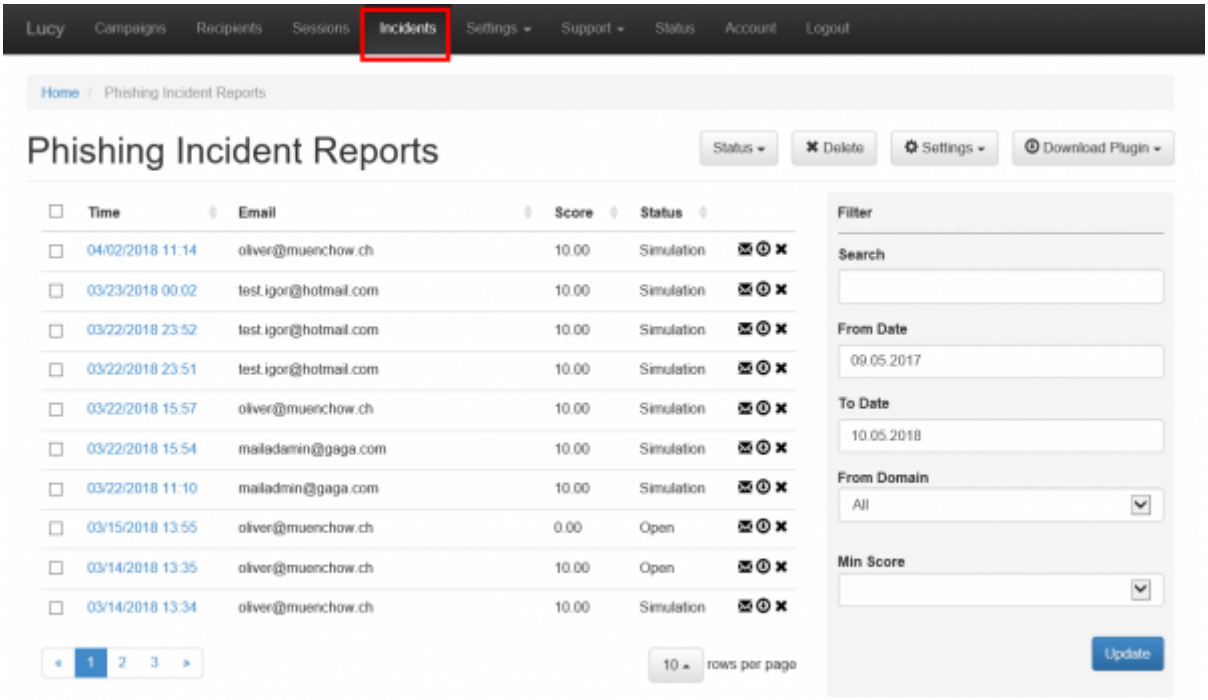
Where are incidents (LUCY generated emails) from the plugin reported?

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

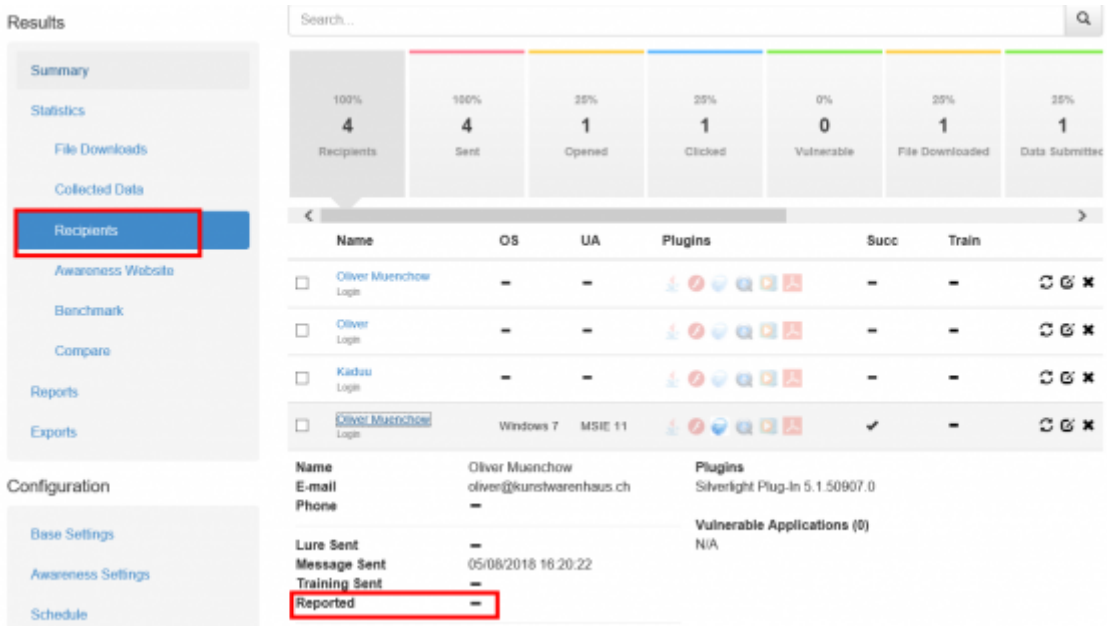
- Incident widget on the dashboard:



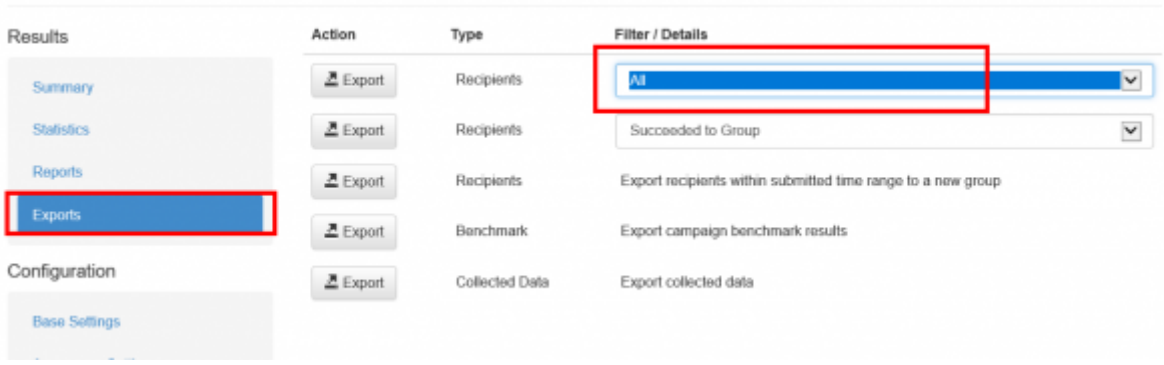
- Incident tab:



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



- 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:



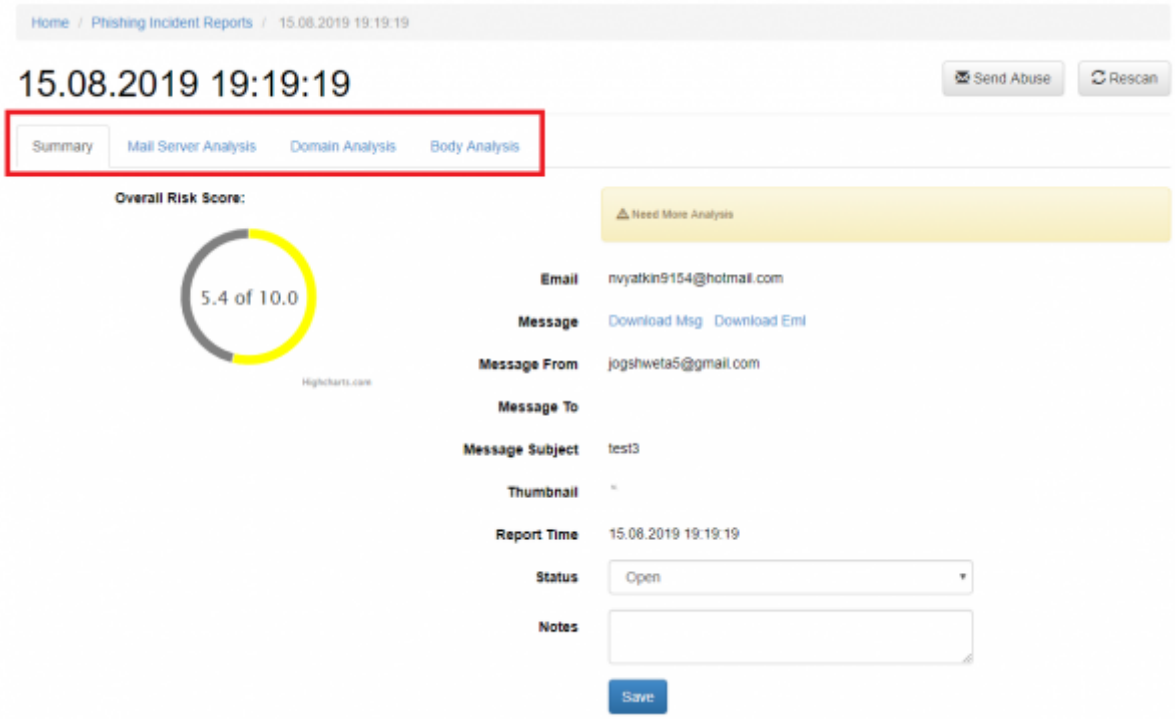
In LUCY 4.4, the incidents reports will also be integrated on the dashboard under the general statistics.

Centralized analysis

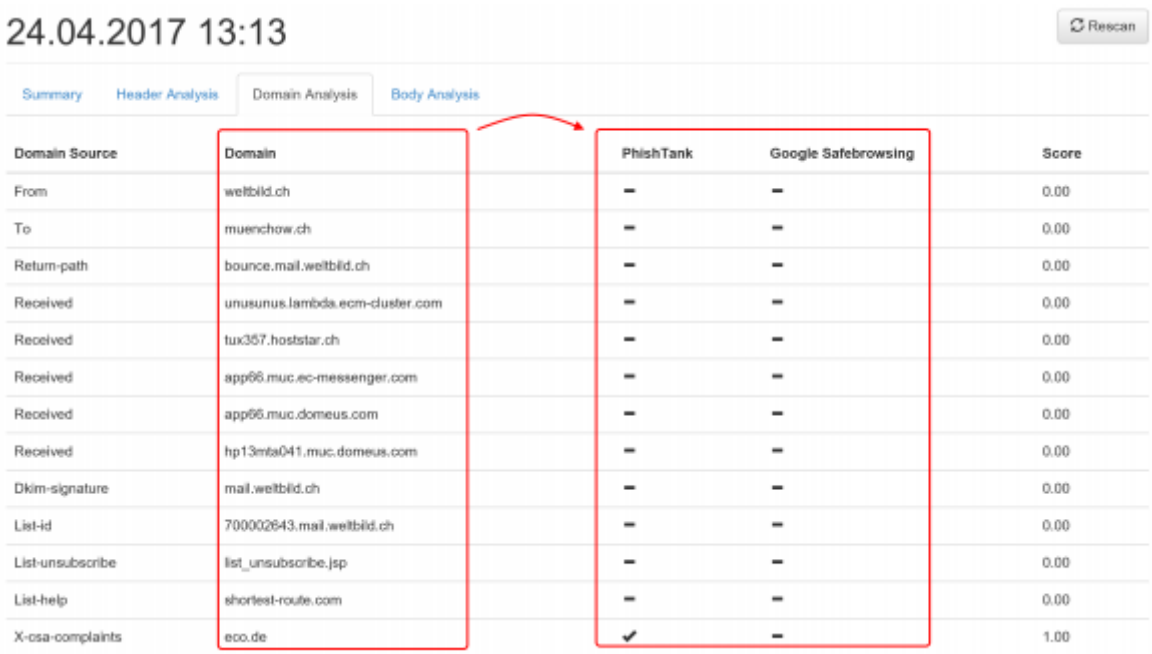
Once the mail has been reported by the user it will popup as an incident in LUCY in case you have enabled the HTTP option in LUCY. There are a few automatic analysis routines build into LUCY (e.g. check an IP in Google's Safe Browsing Database or Phishtank Database). More checks will follow in the upcoming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

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:

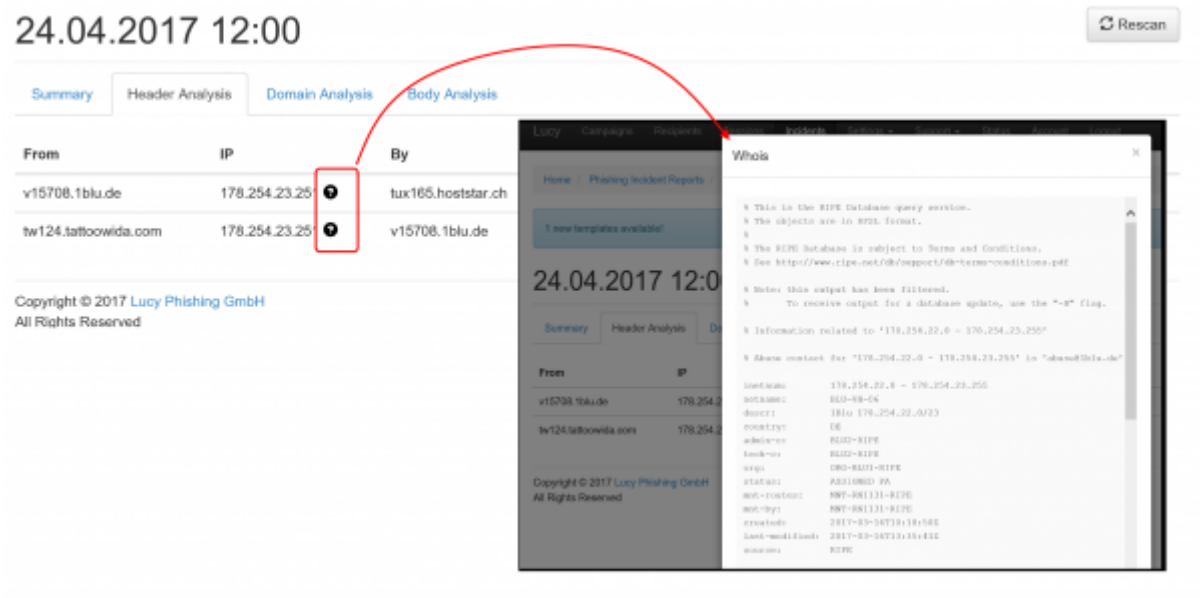


The current sources (LUCY 3.7) are:

- 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.
- Palevo Blocklists (https://palevotracker.abuse.ch/blocklists.php) - Botnet C&C blocklists.
- 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:



Threat mitigation

The threat mitigation allows a LUCY admin to report reported phishing mails to according abuse contact of the provider's originating IP address taken from the message header. You can click on the mail symbol within the incident center to initiate the sending of the report. More info here.

API Integration

The e-mails reported to LUCY via plugin can be automatically forwarded to external systems (e.g. Splunk) via LUCY's REST API. This ensures a seamless connectivity to a SOC.

Technical Details

The plugin is a non signed MSI file and programmed as a C++/COM object. It is bundled with Microsoft Visual C++ 2015 Redistributable (x86) Package (14.0.23026). The loading time of the plugin is around 10 MS. It has been tested in Outlook 2010, 2013 & 2016. An Office365 Plugin is available with LUCY > 3.7.

A phishing mail generated in LUCY will have a "X-Lucy-VictimUrl" value in the mail Header. This allows LUCY to identify the phishing mail and Report it back to the app using a HTTPS call. Example:

X-Lucy-VictimUrl: https://microsoft.secure-log-in365.info/f56/phishing-report Message-Id:

20170414072426.390935E2095F@demo.phishing-test.services

If the user click the phish button where the HTTP delievery is configured in the Settings, a new click Event is generated. The variables could look like this:

```
url: https://demo.phishing-test.services/phishing-report
email: test@lucysecurity.com
message: Thanks. Your help is appreciated!
lucyMessage: This was a phishing simulation. Thank you for your help!
buttonText: Phish Reporter
submitHttp: yes
submitSmtp: yes
something is selected
user clicked yes
property accessor is ok
submitting over smtp...
successfully submitted over smtp
submitting over http...
    url: https://microsoft.secure-log-in365.info/f56/phishing-report
```

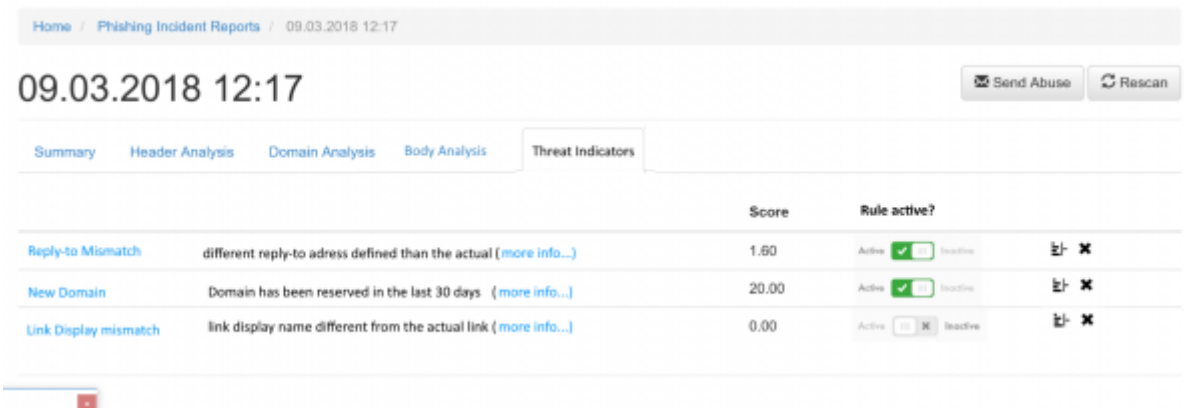
HTTPS communication - plugin to LUCY: The XML always uses web browser to send data to Lucy. In case of running as a web-plugin in MS Outlook it uses the build-in web browser (for Windows it is Internet Explorer) to communicate with Lucy. Both, MSI and XML, use the proxy system settings (Windows > Control Panel > Network and Internet > Internet Options). If Windows-based authentication is required for the proxy, it will work transparently as well as for MSI and XML.

Source Code

In case you want to customize the Features we can provide the source code to the plugin upon request by giving access to our private GIT repository.

Upcoming Features

- Advanced Threat Analysis in LUCY



- Client Based Threat Analysis

Potential Issues

If you enable "send reports via SMTP" you cannot send emails to the same domain (e.g. "example.com") anymore: this setting will cause Lucy to intercept all your emails to "example.com" domain. If you remove the checkbox, then Lucy won't try to intercept emails for that domain and the feature will work as expected. Using "Send Reports Over SMTP" along with "Use SMTP for receiving incident reports on Lucy" is the other way to deliver phishing reports to Lucy. You can specify, for example, some custom email like lucy-phishing-reports@separatedomain.com as a primary email in Incidents settings, check both those checkboxes and point separatedomain.com MX records to Lucy. So all emails being sent to lucy-phishing-reports@separatedomain.com will be intercepted by Lucy, as well as emails sent from Outlook plugin - they will be added to "Incidents" page. If you just want to receive a copy of incident report to your own email (yourname@example.com), that is not tied to Lucy, then you should keep "Use SMTP for receiving incident reports on Lucy" checkbox clear - in that case Lucy won't attempt to intercept anything and the plugin will just forward all reports to yourname@example.com.