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:

Incidents	1.				
Home / Phishing Incident Reports					
Phishing Incident Reports	Send Abuse	X Delete	X Delete All	Change Status +	Ownload Plugin •
Filter +					

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:

'n	ishing	Incident Re	ports	6	Send Abuse	X Dele	te 🗙 De	elete All	Settings
	Time 0	Email	Client 0	Campaign 0	Score 0	Status 0		Filter	
	31.05.2019 17:33	pavel@lucysecurity.com	N/A	N/A	0.00	Open	₫0×	Search	
	31.05.2019 16:57	pavel@lucysecurity.com	N/A	N/A	0.00	Open	≊0×	Client	
	30.05.2019 16:10		N/A	N/A	2.50	Open	≊0×	All	
	24.05.2019 18:37	@hotmail.com	Lucy Test	Button testing	0.00	Simulation	≊⊕×	03.06.2018	
	24.05.2019 14:31	@hotmail.com	Lucy Security AG	N/A	0.00	Simulation	⊠⊕ ×	To Date 04.06.2019	
	24.05.2019 14:29	.@hotmail.com	Lucy Security AG	N/A	0.00	Simulation	≊0×	Status	1
	23.05.2019 18:56	nick@lucysecurity.com	Lucy Test	Button testing	0.00	Simulation	₫0×	Al Open In Progress	
	23.05.2019 16:29	i@hotmail.com	Lucy Security AG	N/A	0.00	Simulation	≊0×	Dismissed Simulation Real Phishing	
	23.05.2019 16:28	i@hotmail.com	Lucy Security AG	N/A	0.00	Simulation	≊⊕ ×	Cosed Campaign	
	23.05.2019	pavel@lucysecurity.com	N/A	N/A	0.00	Simulation	≊0×	NA	

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 / P	hishing Incident Reports	/ 03/22/2018 11:1	0:44			
03/22	2/2018 11:	10:44			Send Abuse	C Rescan
Summary	Header Analysis	Domain Analysis	Body Analysis			
	Overall Risk Score:		Email	mailadmin@gaga.com		
			Message	Download		
	10.0 of	10.0	Message Subject	Welcome to your new Ottlice 365 Account!		
)	Thumbnail	• Constraints you want have the Distance want to be the transmission descent you the second and the present of the presence of the second second second second second methy and the second second methy and the second second second second second second second second second second second second second s		
		Highcharts.com		To B consider and possible contraction of both advantages (
			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.
- 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

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 emails can then be manually verified by the

administrator. All emails 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

2024/04/24 14:21

- Domain Analysis
- Body Analysis

Home / Phishing Incident Reports / 15.06.2019 19:19:19	
15.08.2019 19:19:19	🖾 Send Abuse 🛛 📿 Rescan
Summary Mail Server Analysis Domain Analysis Body Analysis	
Overall Risk Score:	A Need More Analysis
5.4 of 10.0	nvyatkin9154@hotmail.com
Message	Download Msg Download Eml
Message From Highchurt.cov	jogshweta5@gmail.com
Message To	
Message Subject	test3
Thumbnail	•
Report Time	15.08.2019 19:19:19
Status	Open *
Notes	
	Save

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:

Summary Header /	Analysis Domain Analysis Body Analysis			
Domain Source	Domain	PhishTank	Google Safebrowsing	Score
From	weltbild.ch	-	-	0.00
То	muenchow.ch	-	-	0.00
Return-path	bounce.mail.weltbild.ch	-	-	0.00
Received	unusunus.lambda.ecm-cluster.com	-	-	0.00
Received	tux367.hoststar.ch	-	-	0.00
Received	app86.muc.ec-messenger.com	-	-	0.00
Received	app86.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_unsubsoribe.jsp	-	-	0.00
List-help	shortest-route.com	-	-	0.00
X-osa-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:

24.04.2	2017 12	:00						C Rescan
Summary	Header Analysis	Domain Analys	is Body Analysis					
From	IP		ву	Lucy Campaigns (Recipients	Whois	Settion - Second - Status Account	Looset
v15708.1blu.de	178.3	254.23.25	tux165.hoststar.ch	Home / Phishing Incide			HIFE Database query service.	
tw124.tattoowida	.com 178.3	254.23.25	v15708.1blu.de	1 new templates available		A The skjects A A The REPE Dat	are in MTML format. abase is subject to Surms and Conditions.	Î
	Lucy Phishing Gmb	н		24.04.2017	12:0	a Mater this o	vw.clpe.net/db/unpport/db-tarms-conditions.pdf urpat has been filtered. mive catput for a database update, use the "	
Il Rights Reserve	id			Summary Header Ar	wysis De		related to '178,258,22.0 - 170,254,23,255'	
				From	р	8 Alexa contae	the "178-204.32.0 - 178-284.23.283" is "also 138.254.22.8 - 178.254.23.255	self lin la , de "
				v15708.1blu.de	178.254.2	notanec descri	100-48-06 1810 170-224.22.0/23	
				tw124.tattoowida.com	178.254.2	ecustry: admix-er Lank-ar	DE DE LEVELE DE LE	
				Copylight © 2017 Lary Phil All Rights Reserved	hing CentrH	statum: mnt-rostes: mnt-by: created:	0.007-0.027-00174 M97-0.0131-0.1270 M97-0.0131-0.1270 2.017-0.05-0.0730-1.0160 2.017-0.05-0.0730-1.0160 2.017-0.05-0.0730-1.0160 E2792	

Detection of real phishing mails vs. Phishing simulations

The plugin automatically handles emails created in a phishing simulation 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 sent as a part of a security awareness program. LUCY generated phishing emails 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 emails 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:

Filter +

Campaigns		+	• New 💆 Đ	sport - Sele	ct All Actions -	⊙ Type-Based +	Add Widget
Statistics Phish Alert	÷ ×						
Users reported a real phishing mail: Users reported a phishing simulation mail: Average response time (days):	24 4 0						
Incident tab:							
Incident tab:	Suggest 4 Sec	1.					
	lugger + - to	1.	_	_	_		ł

Results	Sec	arch						Q
Summary								
Statistics		100%	4	25%	25%	0%	25%	25%
File Downloads		Recipients	Sent	Opened	Clicked	Vulnerable	File Downloaded	Data Submitte
Collected Data								
Recipients	<	Name	OS	UA	Plugins	S	ucc Train	>
Awareness Website		Oliver Muenchow	-	-	1 0 0 Q	- 18	-	SG×
Benchmark		Oliver	-	-	1 0 0 Q	- <u>R</u>	-	26×
Compare		Kaduu	-	-	4000	- 10	-	26×
Reports	-	Login			2000			
Exports		Cliver Muenchow Login	Windows	7 MSIE 11	£ Ø € Q I	N 🔝 🖌	-	36×
Configuration	Nan E-m Pho	ail	Oliver Muenc oliver@kunst	how warenhaus.ch	Plugins Silverlight F	Plug-In 5.1.50907.0		
Base Settings	Lun	e Sent	-		Vulnerable N(A	Applications (0)		
Awareness Settings		sage Sent ning Sent	05/08/2018 1	6:20:22				
Schedule		orted	-					

• 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	Туре	Filter / Details	
Summary	A Export	Recipients	M	×
Statistics	A Export	Recipients	Succeeded to Group	~
Reports	A Export	Recipients	Export recipients within submitted time range to a new group	
Exports	Z Export	Benchmark	Export campaign benchmark results	
Configuration	A Export	Collected Data	Export collected data	
Base Settings				

In LUCY, the incident 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=1559573852



Last update: 2019/07/25 12:52