Analyse your weird URLs the easy way

and other boring things you'd rather not bother with

Raphaël Vinot

Pass the Salt 2023

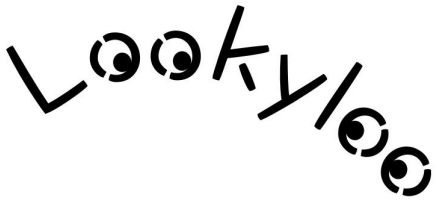
circl.lu
Computer Incident
Response Center
LUXEMBOURG

Few notes about me

- Self employed, based in Bordeaux, France
  - Not in the suburbs of Nashville
  - Full remote \o/
- Building tools to help users make informed decisions
  - Actual intelligence is still our best bet
  - Opensource or GTFO
- Infosec trainings
  - Mostly to at-risk communities, journalists
- The tools are co-developped with (or invented by) Quinn Norton

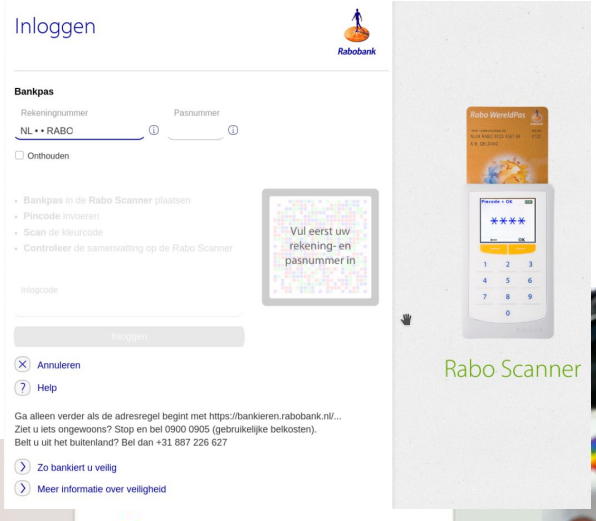
(some of the) Tools maintained by CIRCL

circl.lu
Computer Incident
Response Center
LUXEMBOURG

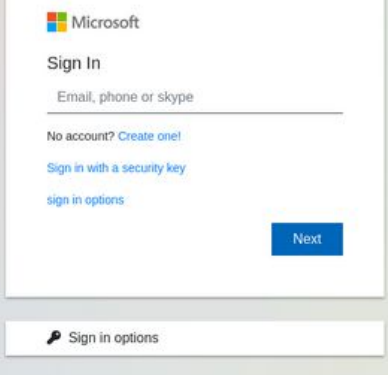


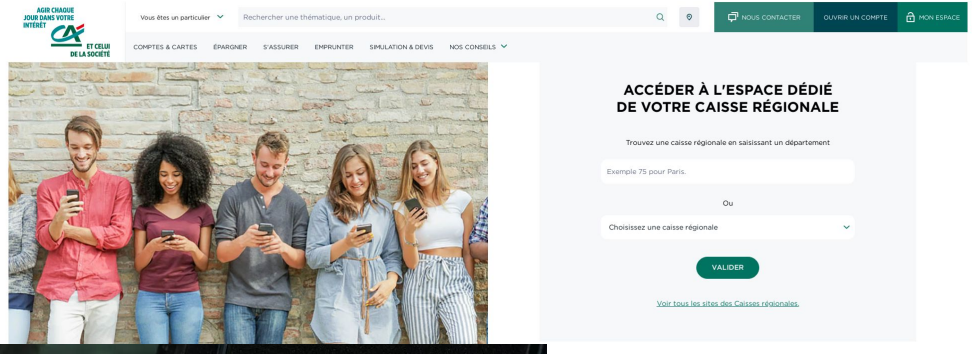
Context

- Everyone receives URLs or stuff they can open in a browser
  - … and y’all are curious
- Hard to know if it is legitimate or not without opening it anyway
  - Special characters, compromised websites, everything is https
- Opening everything in a sandbox isn’t realistic
  - And which sandbox anyway?
- Hard to reproduce and repeat the environment
  - Browser, IP, geolocation, user-agent, locale, timezone, referer, every other HTTP Header
- Can’t do anything with a screenshot only
  - It’s not what you think it means.

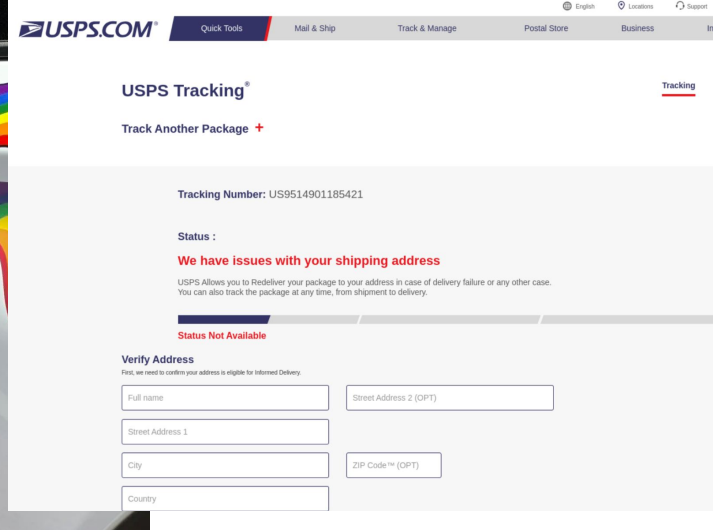

Inloggen
Rabobank
Bankpas
Rekeningnummer
Pasnummer
NL • • RABO
Onthouden
Bankpas in de Rabo Scanner plaatsen
Pincode invoeren
Scan de kleurcode
Controleer de samenvatting op de Rabo Scanner
Inlogcode
Inloggen
Vul eerst uw rekening- en pasnummer in
Annuleren
Help
Ga alleen verder als de adresregel begint met https://bankieren.rabobank.nl/...
Ziet u iets ongewoons? Stop en bel 0900 0905 (gebruikelijke belkosten).
Belt u uit het buitenland? Bel dan +31 887 226 627
Zo bankiert u veilig
Meer informatie over veiligheid

Rabo Scanner


Microsoft
Sign In
Email, phone or skype
No account? Create one!
Sign in with a security key
sign in options
Next
Sign in options

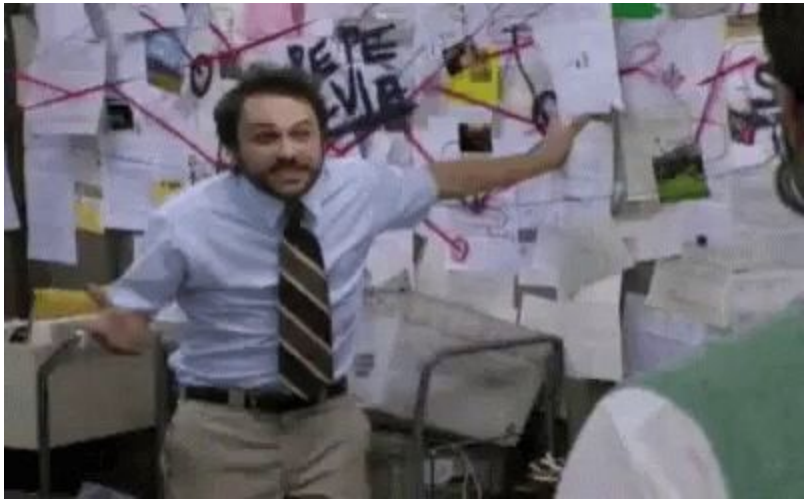

AGIR CHAQUE JOUR DANS VOTRE INTÉRÊT ET CELUI DE LA SOCIÉTÉ
Vous êtes un particulier
Rechercher une thématique, un produit...
NOUS CONTACTER
OUVRIR UN COMPTE
MON ESPACE
COMPTES & CARTES
ÉPARGNER
S'ASSURER
EMPRUNTER
SIMULATION & DEVIS
NOS CONSEILS
ACCÉDER À L'ESPACE DÉDIÉ DE VOTRE CAISSE RÉGIONALE
Trouvez une caisse régionale en saisissant un département
Exemple 75 pour Paris.
Ou
Choisissez une caisse régionale
VALIDER
Voir tous les sites des Caisses régionales.


NYPD
HAPPY PRIDE MONTH
ALL COLORS ARE BEAUTIFUL


USPS.COM
Quick Tools
Mail & Ship
Track & Manage
Postal Store
Business
USPS Tracking®
Tracking
Track Another Package +
Tracking Number: US9514901185421
Status :
We have issues with your shipping address
USPS Allows you to Redeliver your package to your address in case of delivery failure or any other case.
You can also track the package at any time, from shipment to delivery.
Status Not Available
Verify Address
First, we need to confirm your address is eligible for Informed Delivery.
Full name
Street Address 2 (OPT)
Street Address 1
City
ZIP Code™ (OPT)
Country

Context - Where does that URL comes from anyway?

- E-mails
  - HTML body
  - Attachment (PDF, Office doc, HTML page, archive with all the above)
- Logs files (firewall, proxy)
- MISP, Phishtank
- Some random webform used by your customers to send you things
- Some random vendor feeding you cyber cyber intel
  - Yes, half the URLs are down, but you still need to check
  - And they may come back up
- Your nephew, from a discord channel
- Your attorney, from their fax machine
- Emmanuel Macron, from a telegram channel



Lookyloo

- Web UI to precisely configure the settings of the browser used to capture
- Uses a HTTP Archive (HAR) to build the tree of redirects and ressources loaded by a URL
- Lets you extract artefacts from the capture
  - Screenshot of the landing page
  - Ressources, see their types (HTML, CSS, JS, images)
  - HTTP requests/responses
- Connector to 3rd party services
  - MISP, Hashlookup, URLScan, Phishtank
  - Monitoring for changes
  - Ticketing system

Lookyloo - Examples

- Capture interface
  - https://lookyloo.circl.lu/capture
- Captures
  - Pass The Salt: https://lookyloo.circl.lu/tree/87c842bb-f9b5-4224-a96e-7706628bb6c3
  - Valeurs Actuelles: https://lookyloo.circl.lu/tree/79aebd93-7e7c-499f-88db-43651b69a339
  - CNEWS: https://lookyloo.circl.lu/tree/336ee635-c76d-46a9-91fc-2cc00ee7321a
- Many redirects: https://lookyloo.circl.lu/tree/c0ffc64f-c4a3-49ec-bc4f-e10060376635
- Phishing: https://lookyloo.circl.lu/tree/a7f3e4c4-d74f-419d-8d32-12f8a13bddf4

Lacus

- Standalone capturing service (API only, no long term storage)
  - Can be used without Lookyloo (ex. AIL Framework, talk at 11am)
- Uses actual browsers instrumended with Playwright
  - Bypasses most simple bot detections
- High throughput
- Returns complete capture
  - HTTP Archive (HAR)
  - Screenshot of the full page
  - Cookie Jar
  - Rendered HTML

Pandora - How about that URL downloads a file?

- Static analysis of a file
- Attempt to generate a preview for supported files
- Search for active content
  - Office docs, PDFs
- Check against your own Yara Rules
- Send hashes to 3rd parties services
  - VirusTotal, Hybrid Analysis, ClamAV, Hashlookup, MalwareBazaar
  - Not the actual file!
- Extracts observables (URLs, hashes, email addresses)
- Connector so MISP, Lookyloo, manual notification to ticketing system

- Uploaded files are limited to a browser session
  - can generate a sharable URL
- No user account (except for admin)

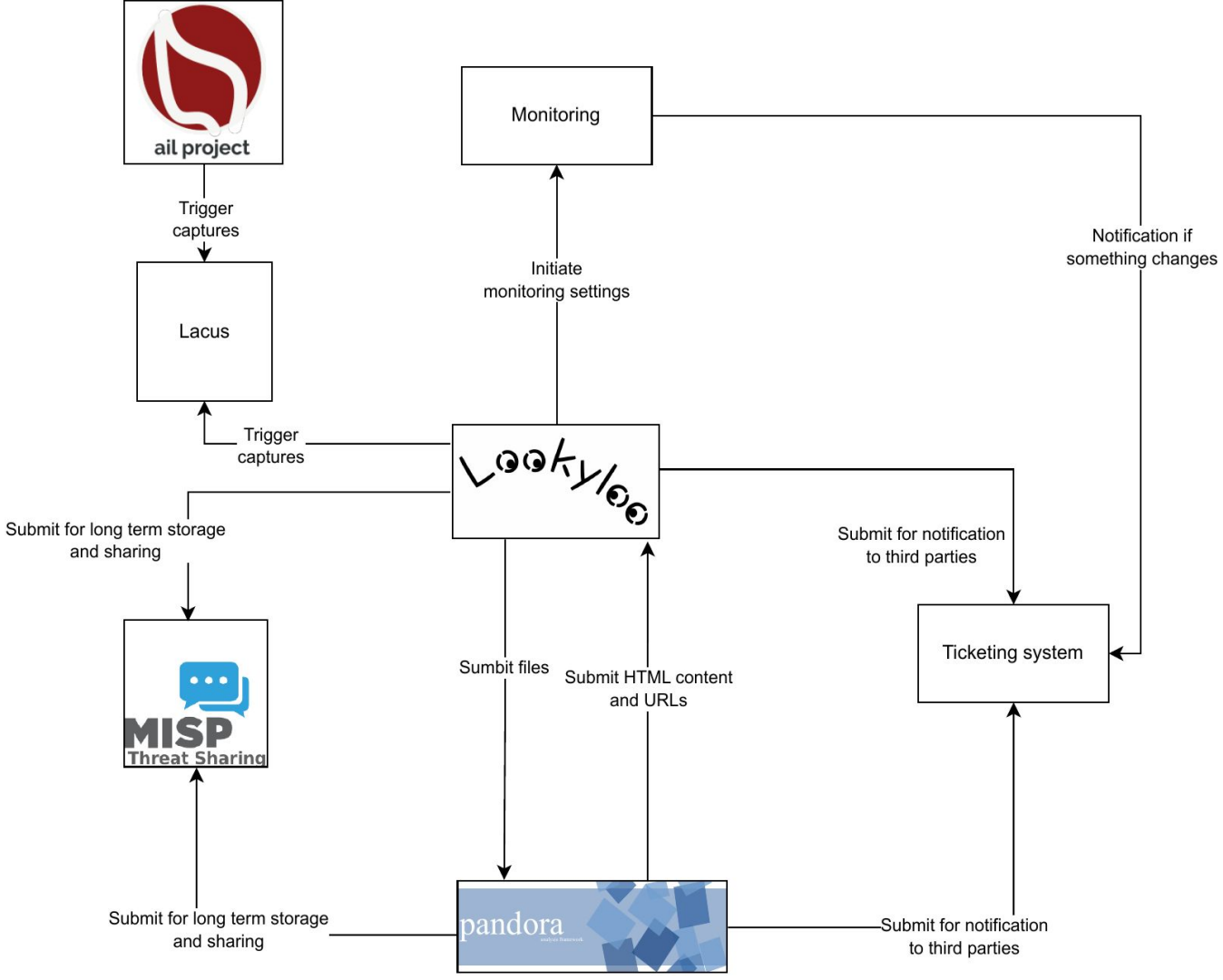
Pandora - Examples

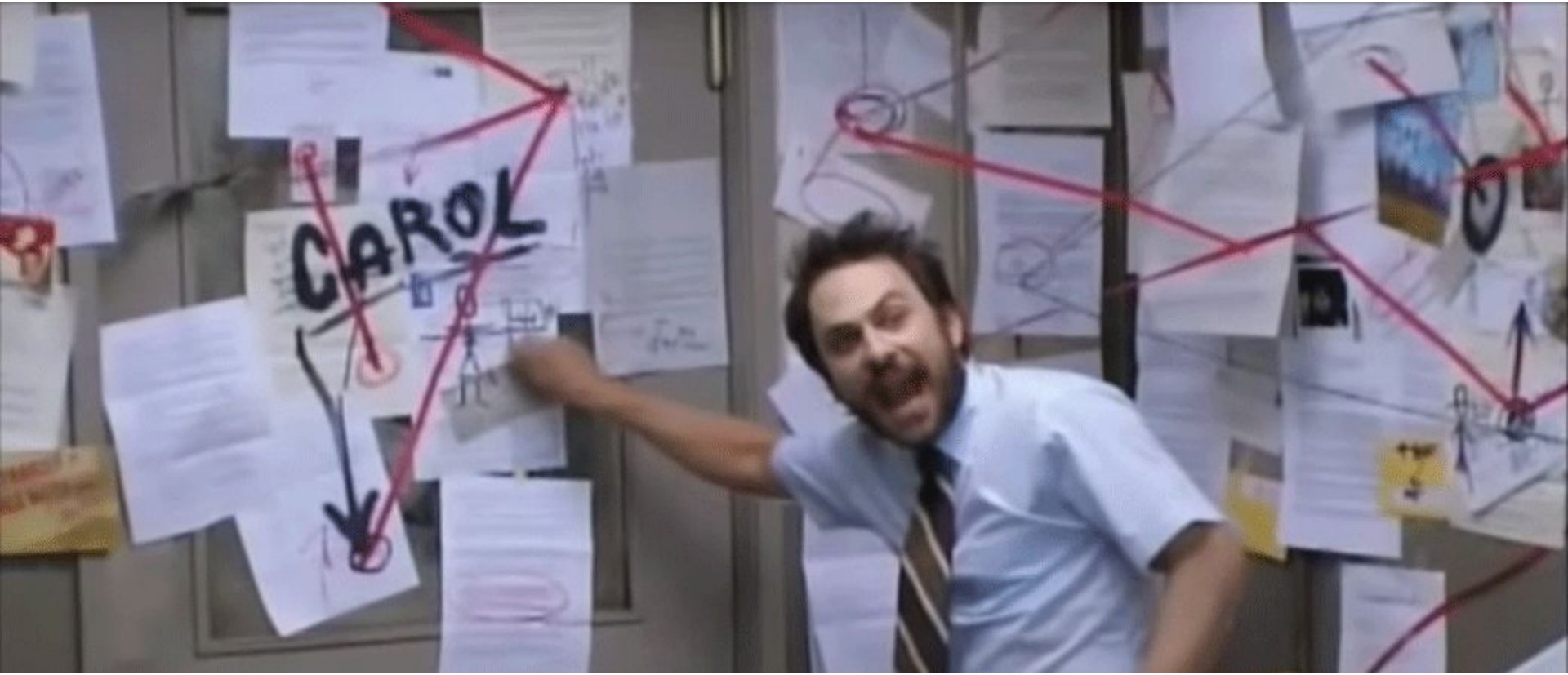
- ODT file: https://pandora.circl.lu/analysis/1f1ee83c-5482-4991-914c-a91986a84618/seed-1dFFfMfzvYLgV1fC_r52Iaiq5YLqI-qqbngH4HXb9pk
- Office doc: https://pandora.circl.lu/analysis/622b4635-c085-4296-8487-12febfa0661b/seed-QzRSTeXhTuxfajPeRDceoY4xjc49uuPH3U-gRtpz0cw
- Email: https://pandora.circl.lu/analysis/28789137-82c5-4203-9731-4a852a1dc345/seed-Vir3qBuvaC7zcoW14LXZxdyfLZCe5nG9VnBTP9F7CUs
- HTML & Lookyloo: https://pandora.circl.lu/analysis/20d38a73-d51b-45f7-9896-d5ea792d80fb/seed-uRWmo9fAYZT5t60sQr6OiqNO_MeNq8JXAGqkcV4_pmo

Monitoring

- Is my domain that should be up really up?
  - Technical problem, takedown, stolen domain name, DNS snafu
- I know the ressources it should be loading, do they change?
  - Buggy update, defacement
- Typosquatting
  - Tracking a takedown request
  - Initiate a takedown request on a newly used domain
  - Stay in the room for the next talk!

- Comparing a capture is non-trivial


ail project
Monitoring
Trigger captures
Initiate monitoring settings
Notification if something changes
Lacus
Trigger captures
Lookyloo
Submit for long term storage and sharing
Submit for notification to third parties
MISP Threat Sharing
Sumbit files
Submit HTML content and URLs
Ticketing system
Submit for long term storage and sharing
pandora
Submit for notification to third parties


CAROL

Other integrations

- Mail to pandora
  - Forward a mail to a mailbox monitored by pandora
- Phishtank
  - Is the URL known on phishtank? And you hate the official UI?
- Hashlookup - Talk at 15:10!
  - Is this hash of the file/webresource known?
- MISP
  - Sharing is caring
- Ticketing system
  - Let’s not implement a mail client in everything please

- No STIX export
  - Use MISP for that, and come to Christian’s talk tomorrow at 11:45!

Projects

- Lookyloo: https://github.com/Lookyloo
- Pandora: https://github.com/pandora-analysis/
- Lacus: https://github.com/ail-project/Lacus
- Monitoring: https://github.com/Lookyloo/monitoring
- Phishtank Lookup: https://github.com/Lookyloo/phishtank-lookup
- MISP: https://github.com/MISP - Stix Talk at 11:45 tomorrow
- Hashlookup: https://github.com/hashlookup - Talk at 15:10 Today
- AIL: https://github.com/ail-project - Talk at 11:00 Today
- TypoSquatting: https://github.com/typosquatter/ail-typo-website - Talk now!
- Evetything has a python module / REST API, duh.

Demo interfaces

- https://lookyloo.circl.lu
- https://pandora.circl.lu/
- https://typosquatting-finder.circl.lu/
- https://hashlookup.circl.lu/
- https://phishtankapi.circl.lu/
- https://monitor.circl.lu/

Contact

- Raphael@vinot.info
- info@circl.lu
- Twitter: @rafi0t
- Mastodon: @rafi0t@social.yoyodyne-it.eu
- Github: https://github.com/rafiot