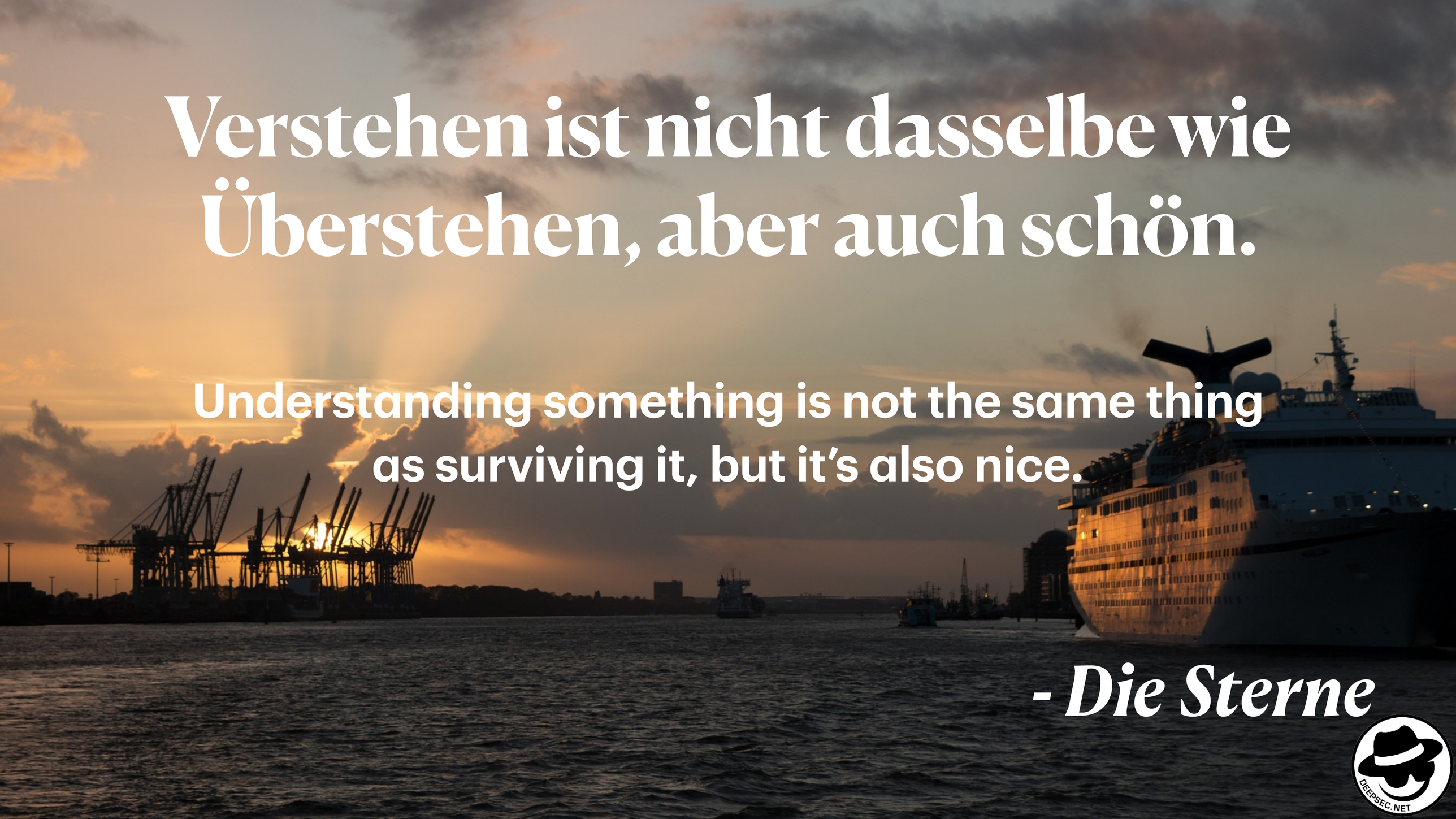
Far Beyond the Perimeter

Exploring External Attack Surfaces

khae 2024

DEEPSEC.NET


Verstehen ist nicht dasselbe wie
Überstehen, aber auch schön.
Understanding something is not the same thing
as surviving it, but it's also nice.
- Die Sterne
DEEPSEC.NET


What this talk
is about
DEEPSEC.NET

About the perimeter...

Ignorance is bliss?


Exposing your private parts by putting your head
in the sand is rarely a viable strategy
DEEPSEC.NET

Digital assets

Leaked Credentials (yawn)

Surprise!

Rogue websites

Code repositories

Partners and 3rd parties

Archives


ngur
App Store

Pastebins

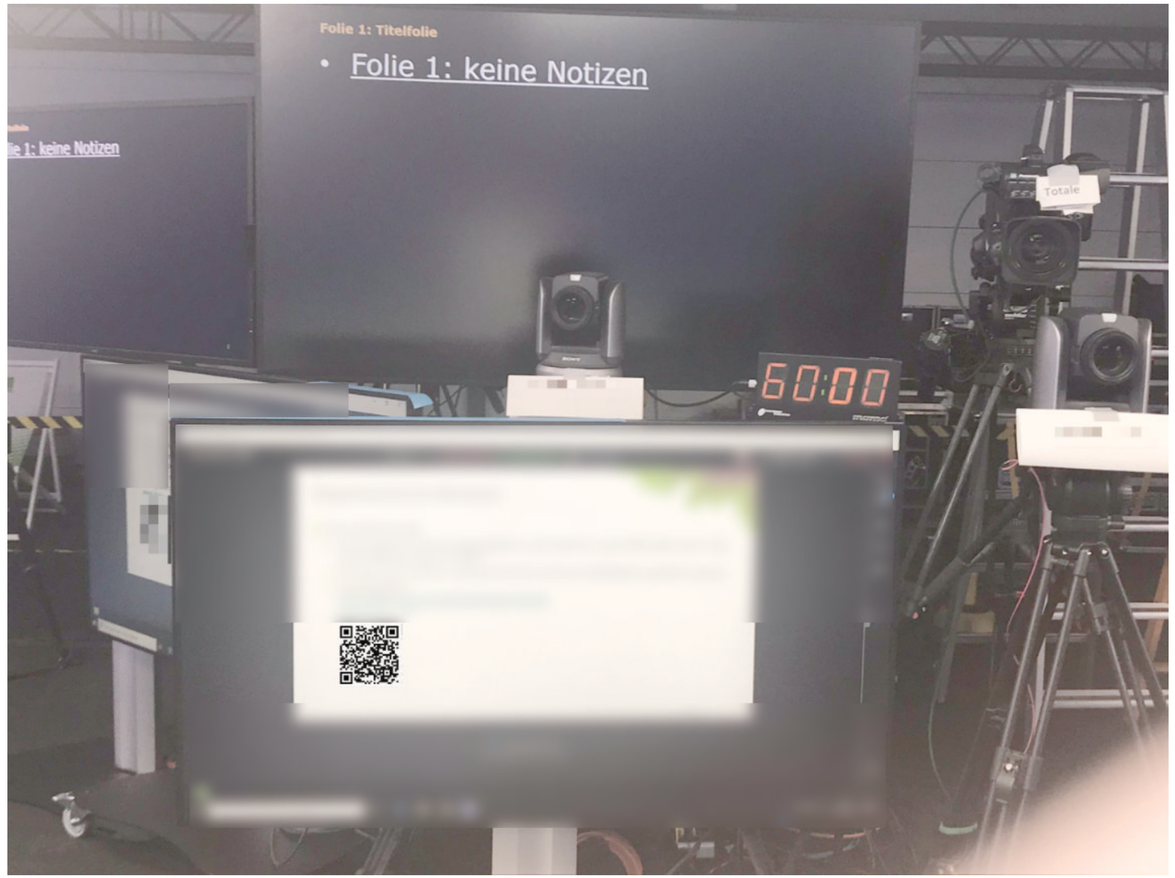

RACCOLTA
CARTA
RACCOLTA
VETRO
RACCOLTA
PLASTICA
RACCOLTA
LATTINE

Social Media for Managers

Part I

Social Media for Managers

Part II

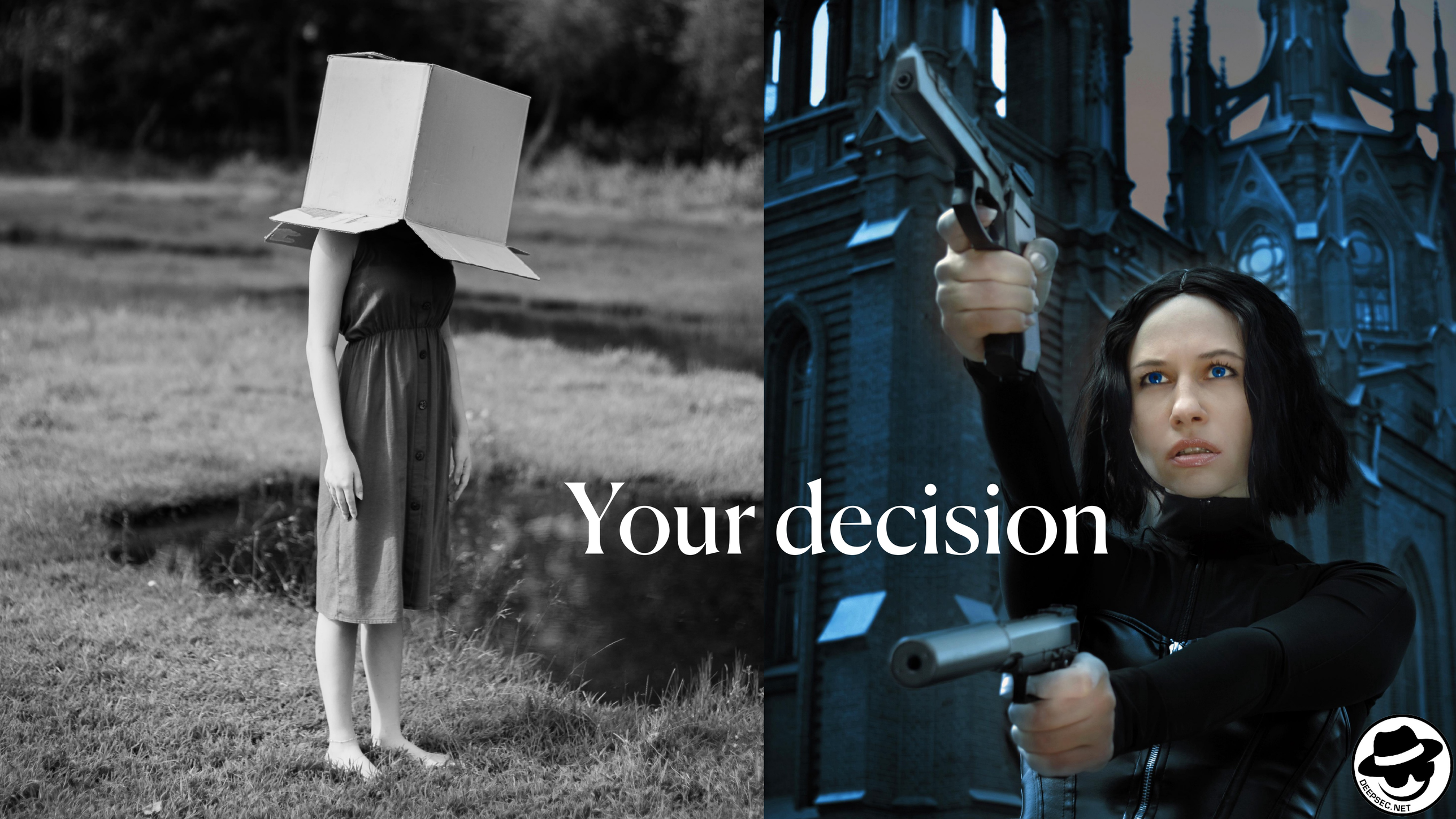



Patching
2024
DEEPSEC.NET

Wait, there's more!

DEEPSEC.NET


Now what?
DEEPSEC.NET

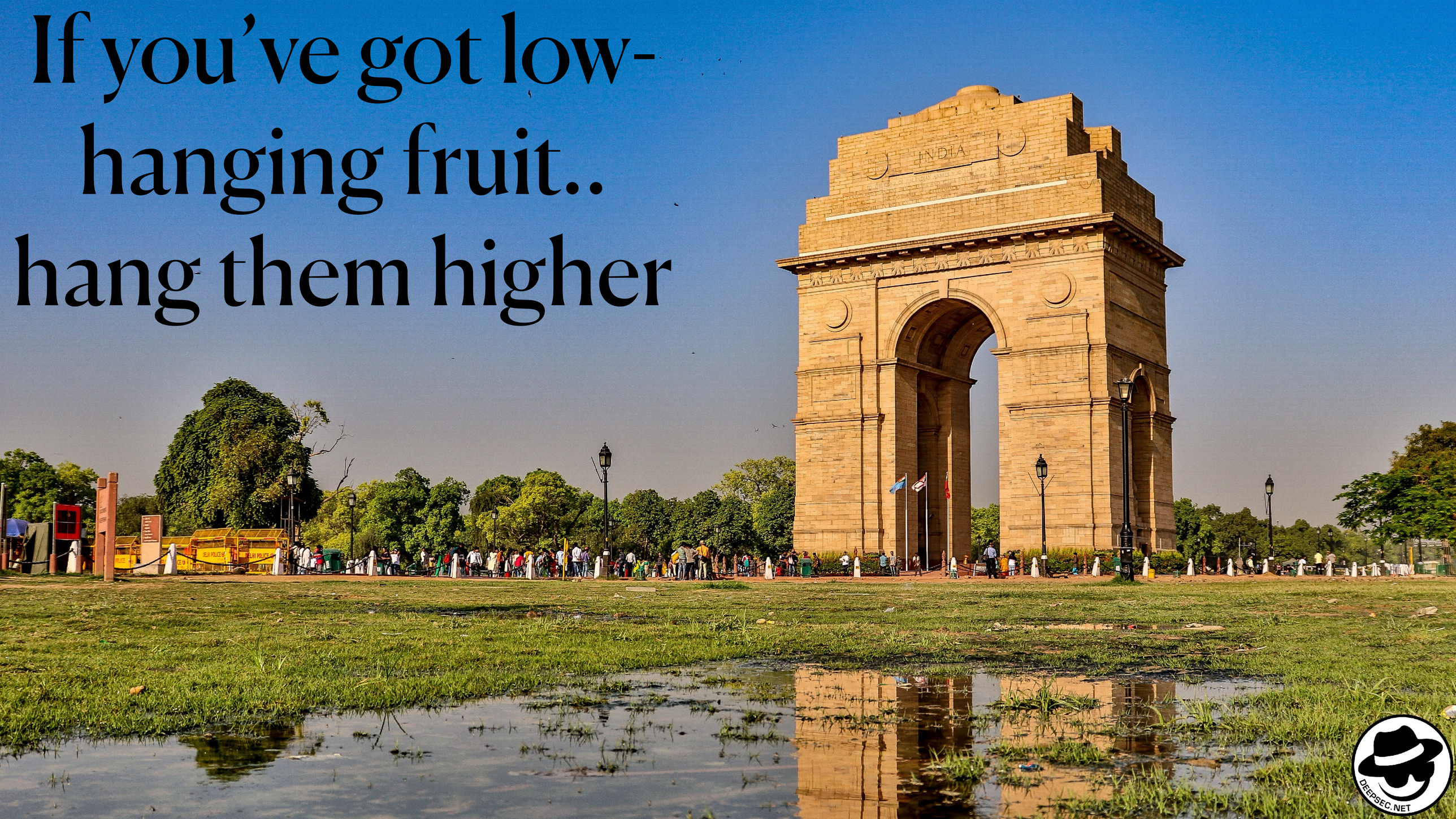

Your decision
DEEPSEC.NET

If you aim for 100% - 99.999% is better than 99.99%

surely?

10% is better than 0%

If you've got low-hanging fruit.. hang them higher




Sinkholes


Keeping an eye
on the Deep and
Dark
DEEPSEC.NET

Trust Issues

(Sub-)domain reconnaissance

Using LLMs to test for side-channel attacks

DEEPSEC.NET

Getting help

Pitfalls & Problems

Are the “good” people really good people?

Legal stuff I

Should you buy info from the darknet?

Legal stuff II

Should you buy info from someone who buys info from the darknet?

Compliant doesn't mean secure

Cosmetics: why looking good is important


Attribution
DEEPSEC.NET


Internal struggles
DEEPSEC.NET

Time


900
Litronic
RÜTHER
34630 Gilserberg / 0 66 96 - 911 05 92
LIEBHERR
02
20
02

Conclusion

Links

Checking for leaked credentials:

haveibeenpwned.com

leakchecker.uni-bonn.de/de/index (German)

Rogue websites / newly registered domains:

letsencrypt.org/docs/ct-logs/

developers.facebook.com/tools/ct/ (needs facebook account)

dnslytics.com/domain-search/

Links

TLS version checker:

testssl.sh (it's a website)

Website hygiene:

www.immuniweb.com/cloud/

www.bitsight.com/

Sinkholes

www.shadowserver.org/

Links

Code repositories:

github.com

gitlab.com

bitbucket.org

Archives

archive.org

archive.io

Subdomain reconnaissance

github.com/aboul3la/Sublist3r

Canary Tokens:

www.canarytokens.org/nest/

Pastebins

pastebin.com

kleber.io

Links

Some unofficial app stores

pkpure.net

apkpure.com

aptoide.com

gratuitpourpc.com

apkgk.com

apkdownload.com

apk.support

luckymodapk.com

napkforpc.com

moddescargar.com

uptodown.com

aapks.com

steprimo.com

apkcombo.com

apkmonk.com

apkdll.com

apkfab.com

daroid.com

modapkdown.com

apkaio.com

softonic.com

9apps.com

appfurpc.com

apkonline.net

apksos.com

apkfun.com

apkfollow.com

...


Thank you for
listening!
DEEPSEC.NET

Questions?

You have questions, I have gifts...

I also am shameless.