

Malware und Social Engineering

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-SE8>

Autor:

Tom Gries <TT-SE8@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.3.0 vom 22.07.2025



Arten von Malware



Arten von Malware

Malware lässt sich je nach ihrem Verhalten, Verbreitungsweg und Ziel in verschiedene Kategorien einteilen. Viren hängen sich an bestehende Dateien an und verbreiten sich durch deren Ausführung weiter. Würmer hingegen benötigen keine Wirtsdatei und können sich selbstständig über Netzwerke ausbreiten.

Trojaner tarnen sich als nützliche Programme, führen aber im Hintergrund schädliche Aktionen aus. Ransomware verschlüsselt Daten und fordert ein Lösegeld zur Freigabe, während Spyware heimlich Informationen sammelt und an Angreifer überträgt.

Ein weiteres Beispiel sind Rootkits, die sich tief ins Betriebssystem einnisten, um ihre Existenz und andere Malware zu verbergen.



1. Viren:

Definition:

Schadprogramme, die sich an legitime Dateien anhängen und beim Öffnen dieser Dateien aktiv werden.

Verbreitung:

Manuell durch den Nutzer (z.B. infizierte E-Mail-Anhänge, USB-Sticks).

Ziel:

Daten zerstören, Systeme stören oder weitere Malware nachladen.

Beispiel:

Sasser.



2. Würmer:

Definition:

Selbstreplizierende Malware, die sich ohne Benutzerinteraktion über Netzwerke verbreitet.

Verbreitung:

Über E-Mail, Netzwerklücken, USB-Geräte.

Ziel:

Daten zerstören, Systeme stören oder weitere Malware nachladen.

Beispiel:

Conficker, Stuxnet.



3. Trojaner (Trojanische Pferde):

Definition:

Malware, die sich als legitime Software tarnt, um unbemerkt Schaden anzurichten.

Verbreitung:

Über gefälschte Software, E-Mail-Anhänge, manipulierte Websites.

Ziel:

Backdoors öffnen, Daten stehlen, Systeme kontrollieren.

Beispiel:

Zeus-Trojaner.



4. Banking-Trojaner:

Definition:

Spezialisierte Trojaner, die es auf Online-Banking-Daten abgesehen haben.

Verbreitung:

E-Mail-Anhänge, manipulierte Websites.

Ziel:

Finanzinformationen stehlen, Transaktionen manipulieren.

Beispiel:

Emotet, Dridex.



5. Ransomware:

Definition:

Malware, die Daten verschlüsselt und ein Lösegeld verlangt, um den Zugriff wiederherzustellen.

Verbreitung:

Phishing-Mails, Drive-by-Downloads, Exploit-Kits.

Ziel:

Erpressung von Geld.

Beispiel:

WannaCry, Locky.



6. Spyware:

Definition:

Überwachungssoftware, die heimlich Informationen über den Nutzer sammelt.

Verbreitung:

Freeware/Shareware, infizierte Webseiten, Phishing.

Ziel:

Passwörter, Tastatureingaben, Screenshots erfassen.

Beispiel:

DarkHotel.



7. Botnetze:

Definition:

Infizierte Geräte, die ferngesteuert in einem Botnetz agieren.

Verbreitung:

Trojaner, Würmer, Drive-by-Downloads.

Ziel:

DDoS-Angriffe, Spam-Verbreitung, Krypto-Mining.

Beispiel:

Mirai-Botnet.



8. Keylogger:

Definition:

Programme, die Tastatureingaben aufzeichnen, um Passwörter und andere sensible Daten zu stehlen.

Verbreitung:

Trojaner, Phishing, Drive-by-Downloads.

Ziel:

Diebstahl von Zugangsdaten.

Beispiel:

HawkEye.



9. Rootkits:

Definition:

Software, die sich tief im System verankert, um die Kontrolle zu übernehmen und andere Malware zu verbergen.

Verbreitung:

xploits, Social Engineering, infizierte Software.

Ziel:

Persistenz, Privilegien-Eskalation, Verschleierung anderer Malware.

Beispiel:

Sony BMG Rootkit.



Beispiele bekannter Malware

Jahr	Name	Wirkung	Schadenshöhe
2017	Wannacry	Ransomware	
2010	Stuxnet	Vermutlich zur Spionage (genauer Zweck bis heute unbekannt). Es waren überwiegend iranische Industrieanlagen betroffen.	
2004	Sasser	Nutzte Sicherheitslücke in XP aus. Befallene Rechner schalteten sich in unregelmäßigen Abständen aus. Ein 17-jähriger aus Niedersachsen.	
2003	SQL_Slammer	Verbreitete sich innerhalb von 10 Minuten auf mehr als 70.000 Rechner. Nutzte eine Sicherheitslücke des MS SQL Servers.	
2001	Nimda	Weltweite Verbreitung innerhalb von 22 Minuten. Versendete sich selbst an alle Outlook Kontakte.	590 Mio. USD
2001	Code Red	Kaperte Computer und missbrauchte diese für Angriffe.	2,6 Mrd. USD
2000	I love you (Lovebug)	Email-Wurm. Überlastete Mailserver. Anhang sah aus wie eine Textdatei.	10 Mrd. USD
1999	Melissa	Versendete sich selbst an Outlook Kontakte.	1,1 Mrd. USD

Social Engineering



Was bedeutet Social Engineering?

Social Engineering ist eine Methodik, die es einem Angreifer erlaubt, technische Sicherungsmaßnahmen zu umgehen, indem der Mensch angegriffen wird.

Allgemeinen versteht man darunter psychologische Manipulation, also die zwischenmenschliche Beeinflussung mit dem Ziel, bestimmte Verhaltensweisen hervorzurufen oder Ergebnisse zu erzielen, zum Beispiel:

- Preisgabe von vertraulichen Informationen
- Kauf eines Produktes
- Vorteilsgewährung
- Freigabe von Finanzmitteln
- Zutrittsbewilligung
- Politische und gesellschaftliche Beeinflussung
- Schaden bei einer Person/Firma erzeugen



Schäden durch Social Engineering



Pressebereich > Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro

Juli 2017

Spionage, Sabotage, Datendiebstahl: Deutscher Wirtschaft entsteht jährlich ein Schaden von 55 Milliarden Euro

According to some reports, U.S banks lost ~\$1.6 billion due to “social engineering wire transfers” between 2013 and 2016¹.



Pressebereich > Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr

November 2019

Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr



Die Motivation der Angreifer für Social Engineering

Die Methoden der Social Engineers werden immer ausgereifter, die Tools immer besser und die Schäden immer höher.

Bei den aktuellen Angriffen werden technische "Hacking-Skills" mit "Social Engineering-Skills" kombiniert. Mal von Einzelpersonen, mal von Gruppen. Hierdurch können hochgradig gefährliche Angriffe entstehen (Advanced Persistent Threat - APT).

Und die Motivation der Angreifer für Social Engineering ist hoch. Die IT wird immer sicherer, direkte IT Angriffe immer schwieriger. Das schwächste Glied in der Kette ist der Mensch. Er handelt emotional und wird dadurch zum Risikofaktor Nr. 1.

Daher ist Social Engineering äußerst interessant für Angreifer.



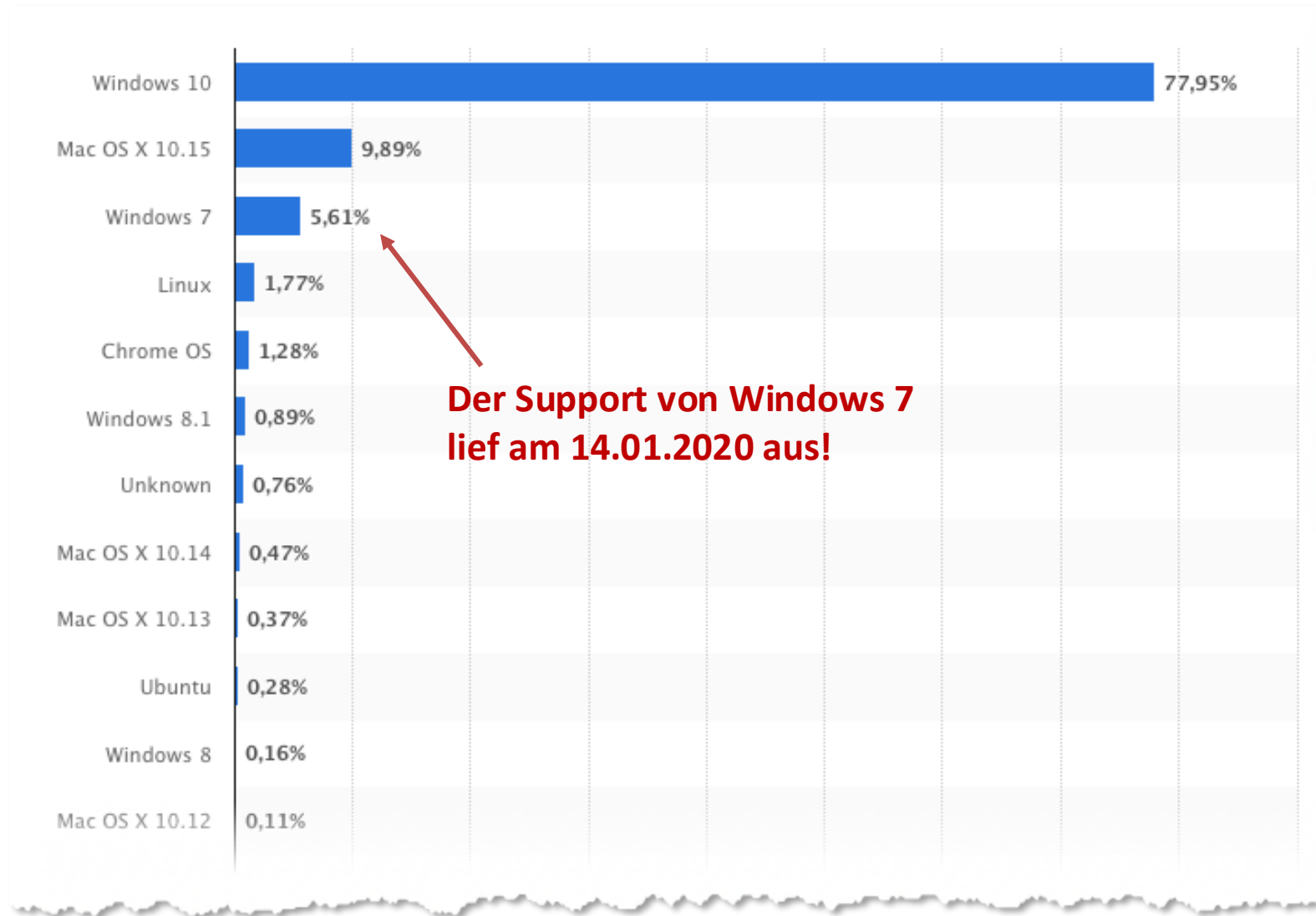
Auf der Grundlage der in der ersten Hälfte des Jahres 2019 beobachteten Trends stellte Webroot fest, dass...

- 1 von 50 URLs bösartig ist
- fast ein Drittel der Phishing-Sites HTTPS verwenden
- die Zahl der Windows® 7-Exploits seit Januar 2019 um 75% gestiegen ist

Windows 7 ist seit 14.01.2020 End of Life. Es sollte jetzt also besser aussehen - oder?



Marktanteile der Betriebssysteme weltweit im Januar 2023





Windows 7 wird noch riskanter: Die Infektionen nahmen um 71% zu. Zwischen Januar und Juni 2019 stieg die Anzahl der IPs, die Windows-Exploits beherbergen, um 75%. Und über 75% der Malware auf Windows-Systemen versteckt sich an einem von drei Orten:

- 41% in %temp%
- 24% in %appdata%
- und 11% in %cache%

Richtlinien, um die Ausführung von Anwendungen aus %temp% und %cache% einzuschränken, könnten einen signifikanten Teil an Infektionen verhindern.



So einfach kann es sein:

Schüler trickst Lehrer bei einer Zoom Video-Session aus.

0-day zoom hacks dropped in YT chat

[Tweet übersetzen](#)



Kozova1 my brother renamed himself to "Zoom" in a zoom call with his teacher and requested access to the teacher's computer. The teacher saw "Zoom is requesting access to your computer" and clicked Allow

6:55 nachm. · 31. Juli 2020 · [Twitter Web App](#)



Vordrängeln am Kopierer:

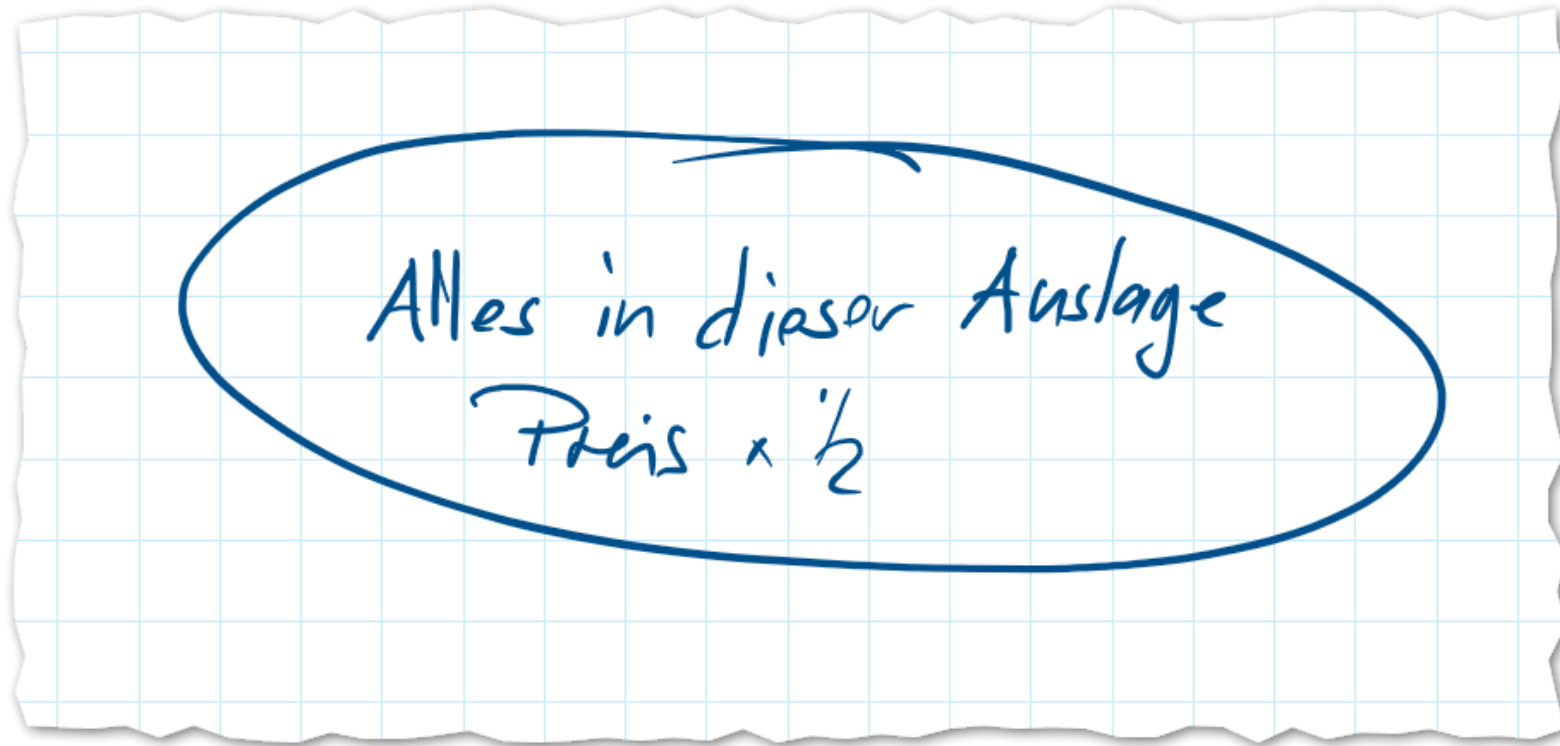
Wenn wir jemanden um einen Gefallen bitten, haben wir mehr Aussicht auf Erfolg, wenn wir unsere Bitte begründen.

Entschuldigung, ich habe fünf Seiten. Könnten Sie mich bitte vorlassen? Weil - ich habe 5 Seiten

Mit Begründung "weil":	94 % Erfolgsrate
Ohne Begründung:	60 % Erfolgsrate



Indianerschmuck - Steine als Ladenhüter:





Social Engineering: Motorola

CEO-Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden. Den CEO-Fraud gibt es schon länger. Einen ähnlichen Hack hat Kevin Mitnick bereits 1992 angewandt, um sich den MicroTac Source Code von Motorola zu beschaffen.

Anruf bei Alicia von Motorola: "Hi Alicia, ich wollte eigentlich Pam anrufen, aber sie scheint schon im Urlaub zu sein. Das ist sehr ärgerlich, sie hatte doch vergangene Woche versprochen, mir noch den Source Code des MicroTac Ultra Light bereitzustellen. Kannst du mir helfen?"

Das Besondere an dieser Masche ist, dass die Täter sehr gut vorbereitet sind und ein ganz bestimmtes Ziel im Auge haben.



Social Engineering: CEO-Fraud (Fake President Fraud)

Die Täter kundschaften ihr Ziel im Vornherein genau aus. Über Soziale Medien, wie Xing, LinkedIn, Facebook und Co. lassen sich besonders gut personenbezogene Daten herausfinden. Die Täter wissen ganz genau, wen sie am besten kontaktieren, um die größten Chancen auf eine schnelle Überweisung zu haben.

Ein bekanntes Beispiel für einen erfolgreichen CEO-Fraud liefert die **Firma LEONI**. 40 Millionen Euro erbeuteten sich die Täter über "betrügerischer Handlungen unter Verwendung gefälschter Dokumente und Identitäten sowie Nutzung elektronischer Kommunikationswege".

Die meisten Angriffe dieser Art werden mit gefälschten Emails durchgeführt. Wie das geht, haben wir bereits gesehen.

Ein paar Tools ...



Wird üblicherweise nur über VPN genutzt!



```
jhancock-mac2:lure jhancock$ ./lure.py -d contoso.com
```

```
  L U R E  | Phishing Target Collection Automation  
            | jhancock@appsecconsulting.com
```

```
-----  
[✓] Hunter.io
```

```
[✓] LinkedIn
```

```
[ ] TheHarvester
```

```
[+] GoPhish Server Online
```

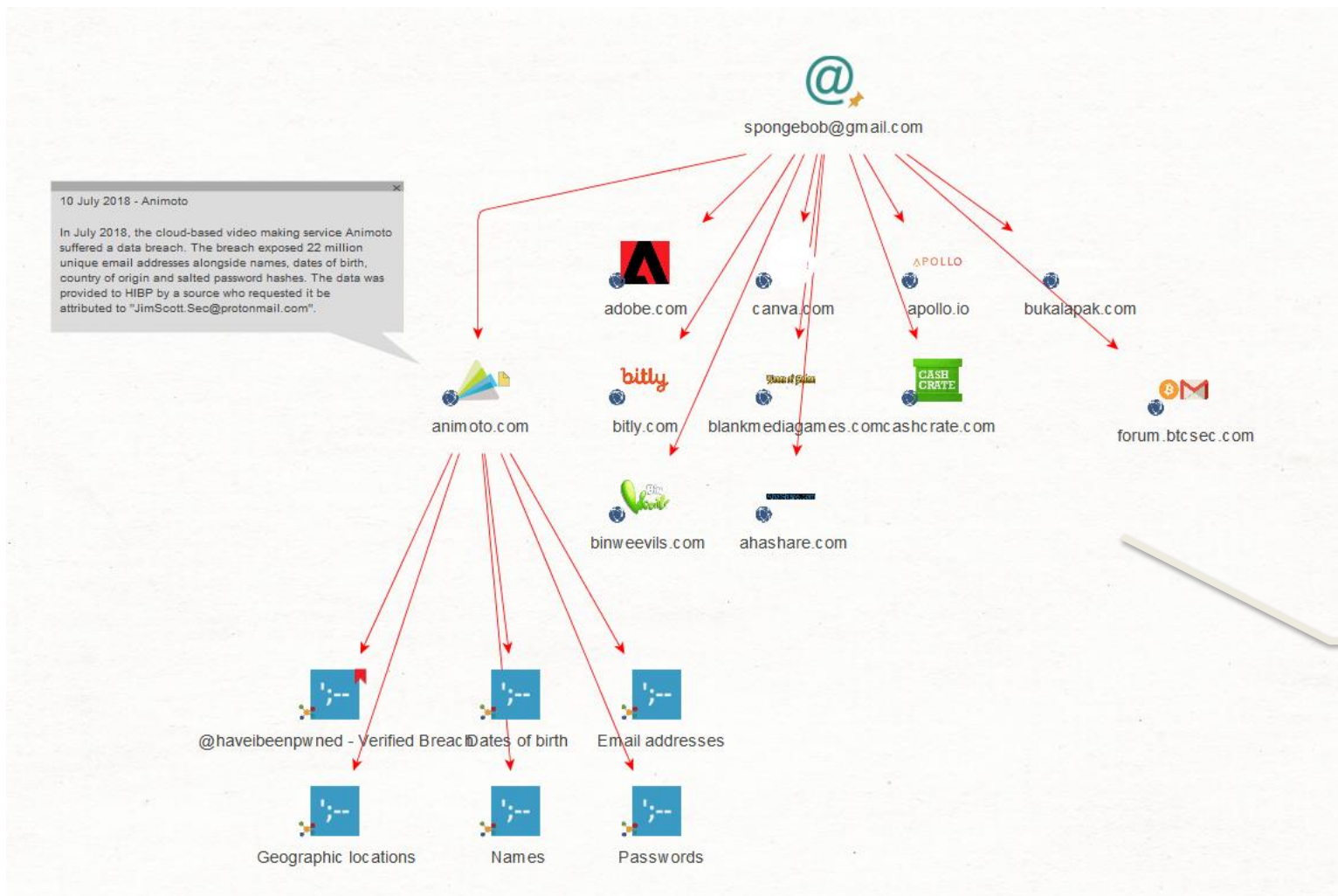
```
-----  
[+] Checking hunter.io (998/1000 queries remaining)
```

```
[+] Checking LinkedIn (via Bing Search)
```

```
[+] Final list contains 56 targets.
```

```
[+] Target list '20190729_Jayme_contoso.com' (ID: 35) added
```

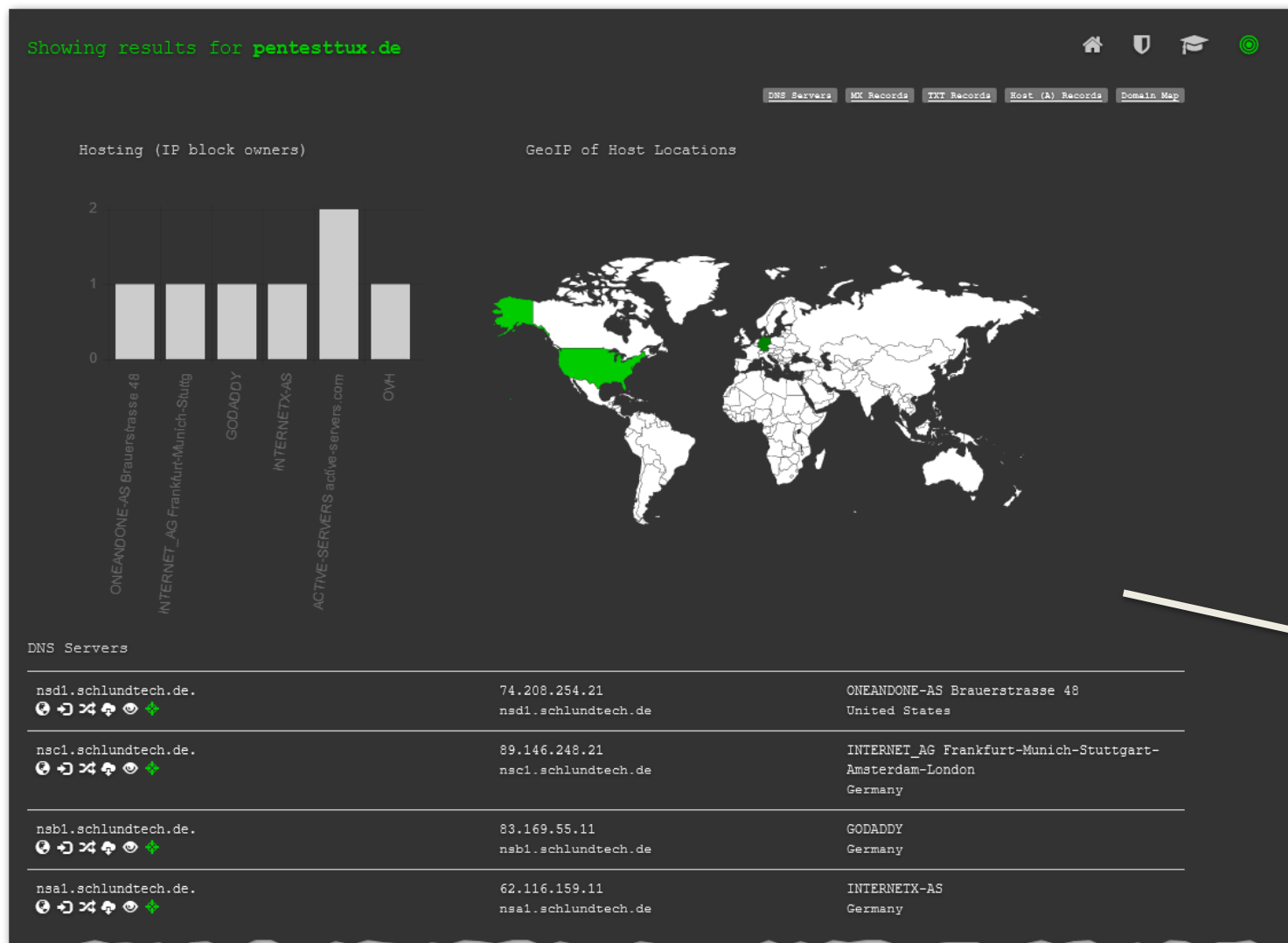
Nutzt weitere Quellen wie z. B.
Hunter.io, LinkedIn und
TheHarvester



Maltego Ergebnissansicht



DNS Dumpster



DNS Servers

nsd1.schlundtech.de. 🌐 🔄 🔍 🛡️ 🟢	74.208.254.21 nsd1.schlundtech.de	ONEANDONE-AS Brauerstrasse 48 United States
nsc1.schlundtech.de. 🌐 🔄 🔍 🛡️ 🟢	89.146.248.21 nsc1.schlundtech.de	INTERNET_AG Frankfurt-Munich-Stuttgart- Amsterdam-London Germany
nsb1.schlundtech.de. 🌐 🔄 🔍 🛡️ 🟢	83.169.55.11 nsb1.schlundtech.de	GODADDY Germany
nsa1.schlundtech.de. 🌐 🔄 🔍 🛡️ 🟢	62.116.159.11 nsa1.schlundtech.de	INTERNETX-AS Germany

Beispiel für pentesttux.de



Personen mit Rocketreach suchen

The screenshot displays the RocketReach search interface. On the left, a search bar contains the text 'joe smith'. Below it, the results are titled 'People results for joe smith • 10,935 results'. A list of six profiles is shown, each with a profile picture, name, and job title. A yellow arrow points from the search bar to the 'Add All' button in the right-hand panel. The right-hand panel, titled 'RocketReach', shows tabs for 'Profiles' and 'Recent Lookups'. Below these, there is a dropdown menu 'Add to List: My Contacts' and a blue button '+ Add All' circled in red. Below this, a list of six profiles is shown, each with a profile picture, name, job title, and a blue '+ Add' button.

Name	Job Title	Location
Joe P. Smith	Division President at Albert's Organics	Greater Los Angeles Area
Joseph Smith	Deputy Fire Safety Director and Front Desk Associate	Greater New York City Area
Joe Smith	Tech Recruiter @ Digitech (Java Software Development)	Kingston upon Thames, United Kingdom
Joe Smith	Account Director at Axciom Digital	San Francisco Bay Area
Joe Smith	Directors at First30 Services	San Francisco Bay Area
Joe Smith	Hoss and a Boss at Hanginout	San Francisco Bay Area

Personensuche mit Rocketreach



Emailadressen zu einer Domain finden

spiegel.de Find email addresses

Most common pattern: {first}.{last}@spiegel.de 867 email addresses

W. I. Schmidt@spiegel.de	1 source
M. Hesse@spiegel.de	2 sources
Stefan Hitz@spiegel.de	1 source
M. Hesse@spiegel.de	2 sources
Anna Joehr@spiegel.de	4 sources

862 more results for "spiegel.de"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get 50 free searches/month.

[Create a free account](#)

Unternehmensstrukturen und
Emailadressen mit Hunter.io



Erreichbarkeit von Emailadressen prüfen

MailTester.com zeigt, ob eine Emailadresse erreichbar ist.

The screenshot shows the MailTester.com interface. On the left, there is a vertical menu with links: "Test Mail", "Download", "FAQ", and "Glossary". The main content area is titled "E-mail address verification". It features an input field for the "E-mail address" containing "test@emailtester.de" and a "Check address" button. Below the input field, the email address "test@emailtester.de" is displayed with a green highlight. To the right, a list of results is shown with arrows pointing from the email address: "Mail server found for domain: - mxlb.ispgateway.de (priority 100, ip address: 80.67.18.126)", "Mailserver identification: mx06.ispgateway.de ESMTP dfex", and "Unknown response from mail server".

MailTester.com

E-mail address verification

E-mail address

test@emailtester.de

- Mail server found for domain:
- mxlb.ispgateway.de (priority 100, ip address: 80.67.18.126)
- Mailserver identification:
mx06.ispgateway.de ESMTP dfex
- Unknown response from mail server



Google Hacking - Beispiel

The screenshot shows a Google search interface with the query 'site:berlin.de filetype:pdf Dienstgebrauch' in the search bar. Below the search bar, there are tabs for 'Alle', 'Bilder', 'Videos', 'Shopping', 'News', 'Mehr', 'Einstellungen', and 'Suchfilter'. The search results indicate 'Ungefähr 315 Ergebnisse (0,36 Sekunden)'. Three results are listed, each with a breadcrumb trail 'www.berlin.de > rundschreiben > download.php' followed by a 'PDF' icon. The first result is titled 'Hinweis! - Berlin.de' and dated '04.07.2011', mentioning 'Landesverwaltungsamt Berlin' and 'Dienstgebrauch'. The second result is also titled 'Hinweis! - Berlin.de' and dated '03.05.2016', mentioning 'Landesverwaltungsamt Berlin' and 'Dienstgebrauch'. The third result is titled 'Untitled - Berlin.de' and mentions 'VS - NUR FÜR DEN DIENSTGEBRAUCH'.

Google

site:berlin.de filetype:pdf Dienstgebrauch

Alle Bilder Videos Shopping News Mehr Einstellungen Suchfilter

Ungefähr 315 Ergebnisse (0,36 Sekunden)

www.berlin.de > rundschreiben > download.php PDF

Hinweis! - Berlin.de

04.07.2011 - Landesverwaltungsamt Berlin • 10702 Berlin (Postanschrift). Nur für den **Dienstgebrauch**. An die Teilnehmer des Sammelbestellverfahrens.

www.berlin.de > rundschreiben > download.php PDF

Hinweis! - Berlin.de

03.05.2016 - nach telefonischer Vereinbarung. Landesverwaltungsamt Berlin • 10702 Berlin (Postanschrift). Nur für den **Dienstgebrauch**. An die Teilnehmer.

www.berlin.de > sen > geheimchutz-in-der-wirtschaft PDF

Untitled - Berlin.de

VS - NUR FÜR DEN **DIENSTGEBRAUCH**. - ohne Eintragungen offen -. Familienstand ledig
getrennt lebend geschieden eheähnliche Gemeinschaft verwitwet.

Ergebnis der PDF-Suche nach
"Dienstgebrauch" auf der Site
Berlin.



Google Hacking - Beispiel

Intitle:

Findet Zeichenketten im Seitentitel

Allintitle:

Findet alle Begriffe im Seitentitel

Inurl:

Findet Zeichenketten in der URL einer Seite

Allinurl:

Findet alle Zeichenketten in der URL einer Seite

Filetype:

Findet Dateitypen auf Basis der Dateierweiterung

Link:

Sucht nach Links für eine Site oder URL

Cache:

Zeigt die von Google gecachte Kopie einer Seite

Define:

Zeigt verschiedene Definitionen des Suchbegriffs

Phonebook:

Findet Telefonnummern

Beispiel:

site:berlin.de filetype:pdf Dienstgebrauch



Phishing mit dem Open-Source Framework Gophish

Launch a Campaign in 3 steps



Set Templates & Targets

Gophish makes it easy to create or import pixel-perfect phishing templates.

Our web UI includes a full HTML editor, making it easy to customize your templates right in your browser.



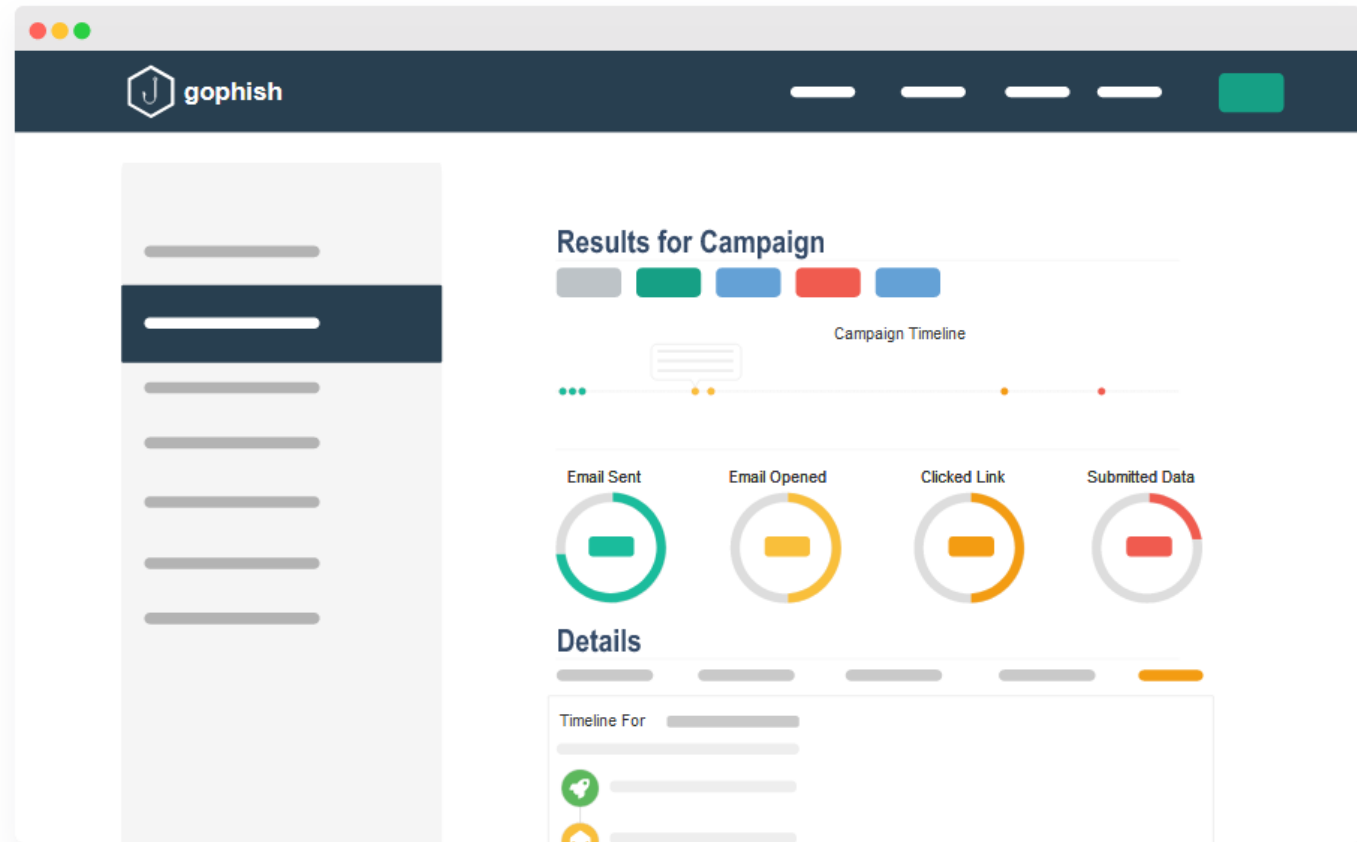
Launch the Campaign

Launch the campaign and phishing emails are sent in the background. You can also schedule campaigns to launch whenever you'd like.



Track Results

Detailed results are delivered in near real-time. Results can be exported for use in reports.





Temporäre E-Mail-Adresse


squizzly.net stellt Ihnen temporäre Wegwerf-E-Mail-Adressen zur Verfügung, um Sie vor Spam zu schützen. Die E-Mail-Adresse verfällt nach 60 Minuten. Sie können innerhalb des Zeitfensters eingehende E-Mails lesen und darauf antworten.

Ihre derzeitige E-Mail-Adresse lautet **hirepaim@squizzly.net**



Es wurden noch keine E-Mails empfangen. Klicken Sie auf den Reload-Button, um zu überprüfen, ob neue E-Mails eingetroffen sind.

(Automatischer E-Mail-Check ist aktiviert. Der Reload-Button muss nicht angeklickt werden.)

 Aktualisieren

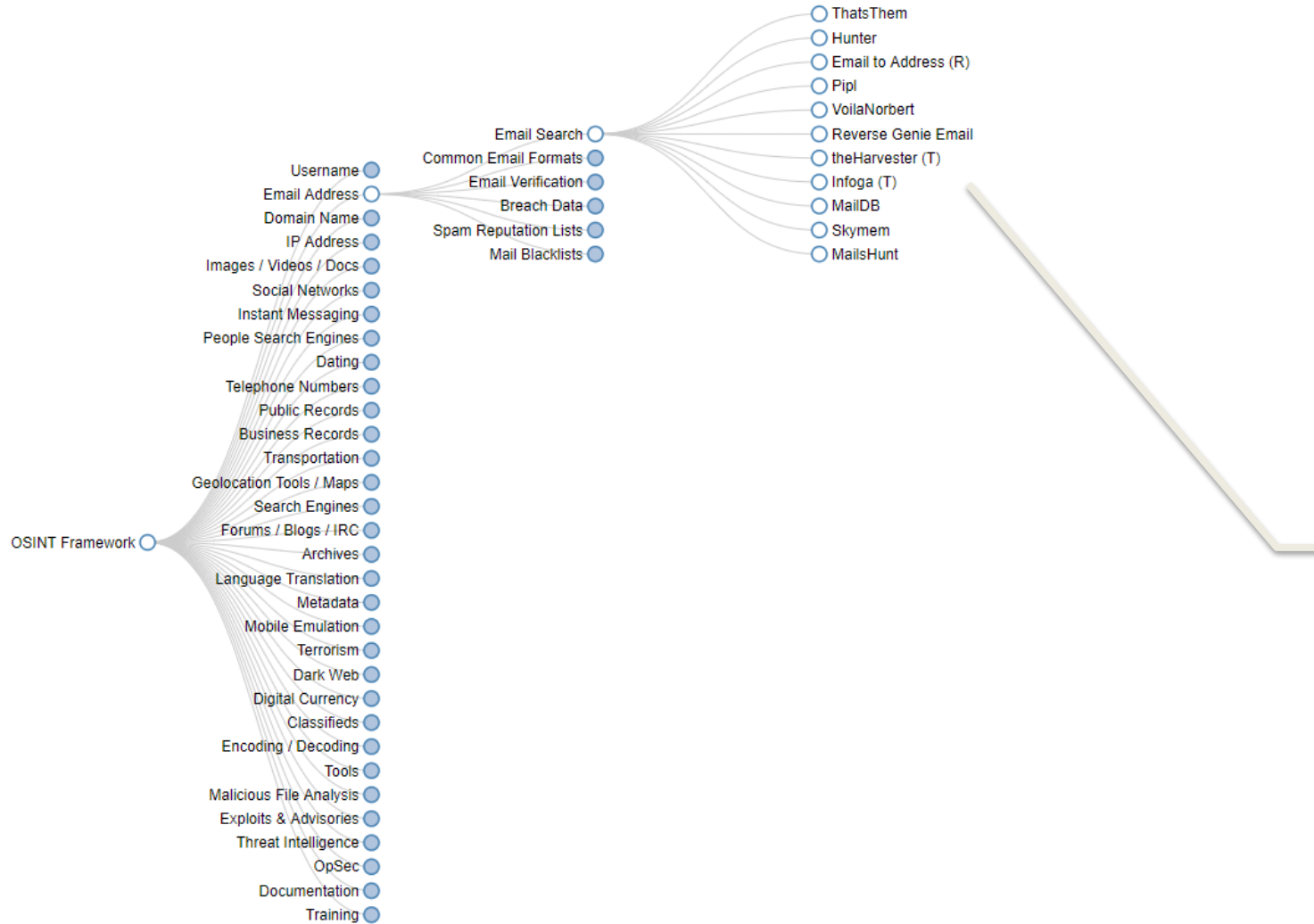
Die E-Mail-Adresse läuft ab in: 59 Min 52 Sek

Gib mir 60 weitere Minuten

E-Mail-Adresse wegwerfen



Weitere Tools finden mit dem OSINT Framework



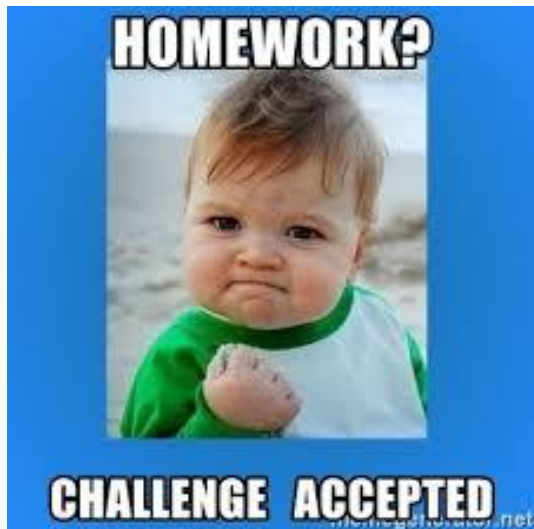
Aufgeklappter Baum zur Anzeige von Tools zur Email Suche.

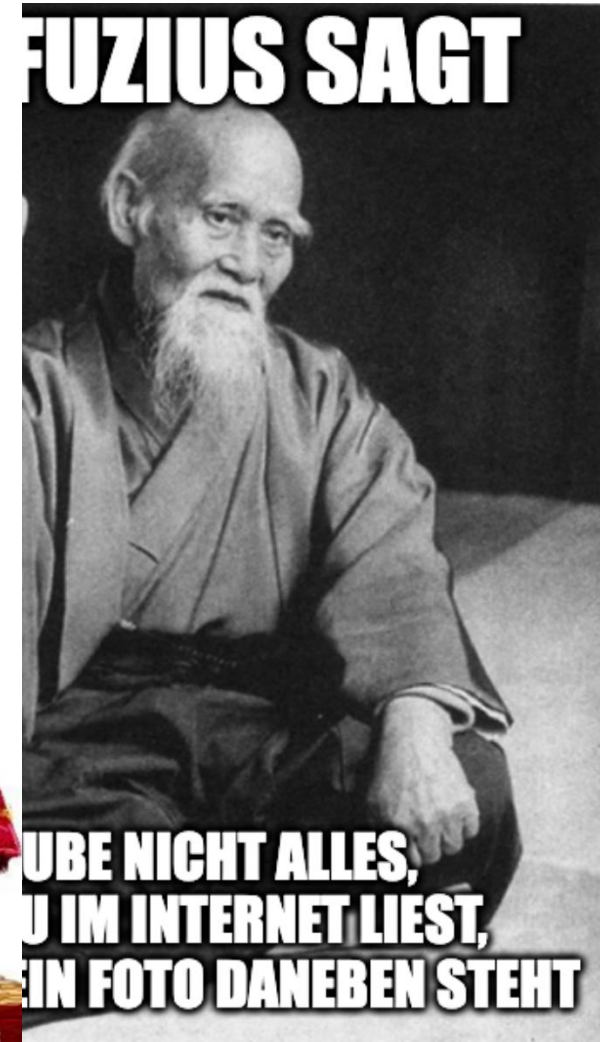
Fake Pictures & Videos



Memes

Das Verbreiten kleiner Medieninhalte mit einer meist humoristischen, aufheiternden oder manchmal auch satirischen oder gesellschaftskritischen Aussage.







Fake Pictures





Fake Pictures





Fake Videos / Deep Fake

Die nächste Stufe des Social Engineerings. Mit Hilfe von künstlicher Intelligenz erstellte Fake Pictures, Audios und Videos.



Dies wird von Angreifern auch schon aktiv genutzt - zum Beispiel für den COE Fraud.

Obama Fake



Fake News (Hoaxe)



Fake News (Hoaxe)

Ein Hoax - ursprünglich ein „Jux“ oder „Scherz“ – ist eine Falschmeldung. Der Begriff wird heute nur noch selten verwendet - er ist in den letzten Jahren durch „Fake News“ abgelöst worden.

Einige Beispiele:

1. McDonalds Kaffee
2. Verbrannte Zigarren
3. SULFNBK.EXE (auf den nächsten Seiten)



Im Internet weiß keiner, dass
Du ein Hund bist.

(Peter Steiner, 1993)



Fake News (Hoaxe)

Hallo ihr Lieben!

bitte mal Systeme checken... das ist kein Fake oder Scherz! Nach einer Warnung vor einem "schlafenden Virus" habe ich diesen Virus auf meinem Rechner gefunden und jetzt gelöscht - ohne ihn zu öffnen! Er wird wohl von vielen Virenprogrammen nicht erkannt und aktiviert sich zu einem späteren Zeitpunkt.

Er verbreitet sich durch Emails, infiltriert C:\Windows\command und löscht - wenn er sich aktiviert - alle Dateien/Ordner auf der Festplatte.

Ich bitte alle, die in den letzten Monaten von mir eine Mail bekommen haben, ihn zu suchen und ggf. zu löschen. Dabei wie folgt verfahren:



Fake News (Hoaxe)

Ist der Rechner infiziert erscheint die Datei im Ergebnisfeld. AUF KEINEN FALL ÖFFNEN! (durch Doppelklick oder ausführen) sondern wie folgt verfahren:

[...]

Dann auf jeden Fall noch den Papierkorb leeren. Wenn die Datei gefunden wurde, alle Empfänger/Innen von E-Mails der letzten Monate informieren.

Diese Virenwarnung hab ich auch von anderen bekommen. Ich hatte den Virus auch. Also bitte ernst nehmen und weiterleiten.

Habe den Virus eben gelöscht!!!! Unter Garantie habt ihr den auch! Also seht nach. Geht ganz schnell!



Fake News (Hoaxe)

1. Der Adressat wird aufgefordert, die "Warnung" an möglichst viele Menschen weiterzuleiten.
2. Der Betreff enthält etwas reißerisches (z. B. "Virus Warnung").
3. Die Wirkung des Virus wird sehr drastisch dargestellt.
4. Als Quelle wird gerne eine namhafte Firma oder Organisation genannt, um die Glaubwürdigkeit zu verbessern (a.k.a. False Authority Syndrome). Bei diesen Firmen finden sich jedoch keine Hinweise auf eine solche Warnung.
5. Es wird mit Aktualitätsangaben wie "gestern" oder "am Freitag" gearbeitet, die keinen Bezug zu einem bestimmten Datum haben. Man erkennt so nicht, wie alt die Meldung tatsächlich schon ist.



Holländerin fälscht Ferien

FÜNF WOCHEN ASIEN IN AMSTERDAM

Holländerin fälscht Ferien und täuscht damit alle

Sie teilte Strandfotos auf Facebook, schwärmte von der Unterwasserwelt in Thailand und skypepte ihre Familie aus einem lokalen Restaurant an. Doch die Holländerin Zilla van den Born war gar nie weg! Sie täuschte ihrem gesamten Umfeld die Asien-Reise nur vor.





Unechte Influencerin – Deep Fake für das Geschäft

SAMSTAG, 12. SEPTEMBER 2020

Neues Social-Media-Phänomen

Unechte Influencerin bringt Machern Millionen

Von Jakob Schreiber



Sie ist 19 Jahre alt und führt ein Leben, von dem viele träumen. Das Internetphänomen Miquela besitzt fast drei Millionen Follower, hat mehrere Songs veröffentlicht und sieht aus wie ein Top-Model. Das schlanke Mädchen ist jedoch eine Illusion – ihre Erschaffer verdienen mit ihr Millionen.

Die Werbebudgets für Social-Media-Werbung werden immer größer: Letztes Jahr haben Unternehmen rund 80 Milliarden Euro in Werbung auf sozialen Netzwerken investiert. Ein Teil dieses wachsenden Kuchens landet in den Kassen sogenannter "Influencer", die auf ihren Kanälen Produkte und Dienstleistungen bewerben. Viele Menschen folgen Influencern, weil sie lustig, inspirierend oder schlicht schön sind - die Werbung gibt es scheinbar beiläufig dazu. Kylie Jenner 23-jähriges Mitglied des Kardashian-Clans, hat mit ihren Social-Media-Aktivitäten bereits hunderte Millionen Euro verdient.

Das Instagram-Profil der US-Amerikanerin hat jedenfalls die gleiche Zielgruppe wie das von Miquela. Dementsprechend ähnlich sieht das Profil mit dem Namen "lilmiquela" auch aus: Mal grinst das Gesicht einer 19-Jährigen mit Milkshake in der Hand und ausgestreckter Zunge in die Kamera. Dann fotografiert sie sich in High-Fashion-Klamotten im Spiegel. Und auf einigen Fotos blickt sie leicht bekleidet und mit verführerischem Blick in die Augen ihrer Follower.

Doch im Gegensatz zu Jenner ist sie kein richtiger Mensch, sondern das Produkt einer künstlichen Intelligenz. Die Website onbuy.com hat berechnet, dass ihre Erschaffer rund 6500 Euro umsetzen - pro Post. Bei 847 Posts kommt da eine stolze Summe zusammen. Das Team von onbuy.com prognostiziert den Machern einen Jahresumsatz von fast 9 Millionen Dollar.



Deep Fake für das Geschäft:

Miquela: 19 Jahre alt, 3 Millionen Follower und ein Jahresumsatz von schätzungsweise 9 Millionen Dollar - aber nicht real. Entstanden mit Hilfe von künstlicher Intelligenz (KI).

Was kann Social Engineering noch?



Wie erkennt man Fake?





Mit einer Bilderrückwärtssuche



Nationalpark Ao
Phang-nga

Nationalpark in Thailand



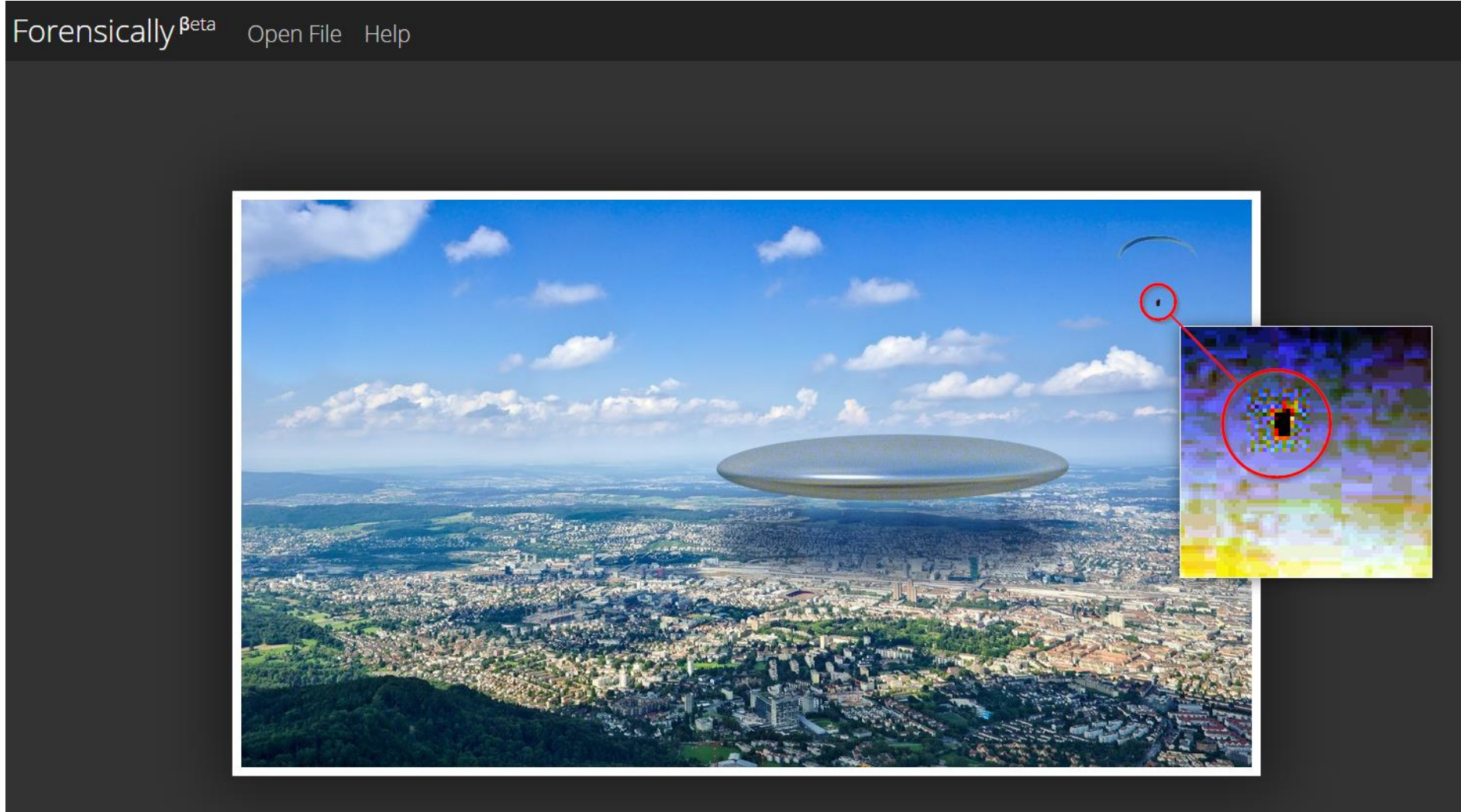
Deutschland von oben - ZDF - TV-Programm - Prisma



720 × 1080 - **Lichtenstein** castle. Fotoquelle: © Creative Commons Free for commercial use No attribution required.



Mit forensischen Tools

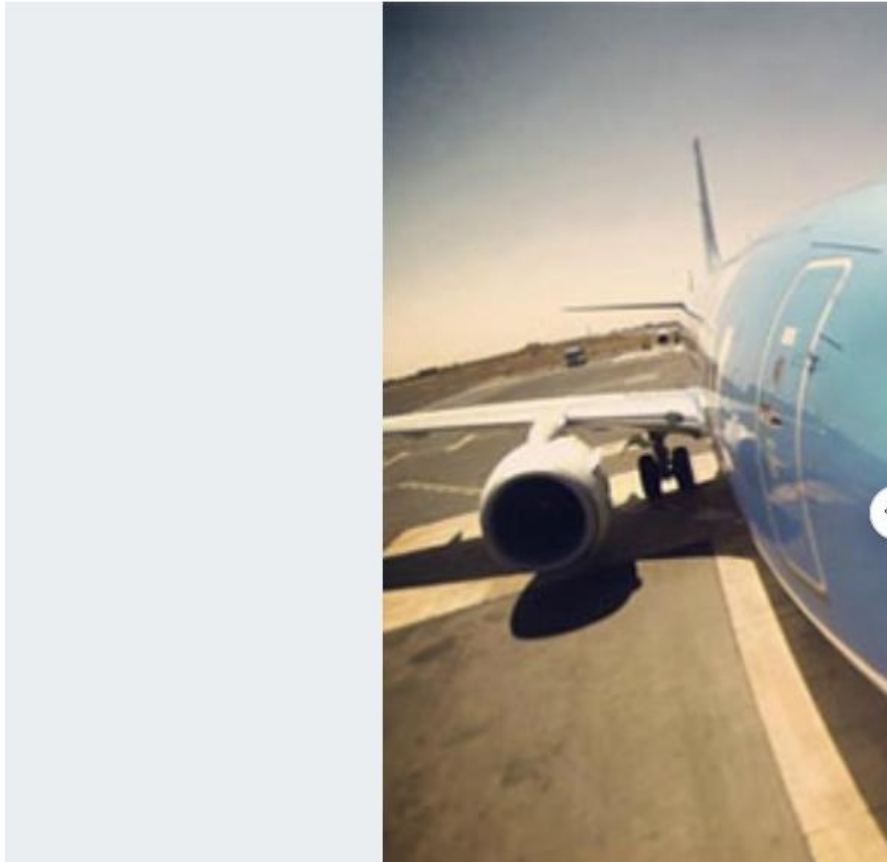




Mit Bildvergleichstools

☐ Split ☐ Fade ☒ Slider ☐ Difference ☐ Downloadable

Pilot Selfie - Fake.png



Pilot Selfie - Original.png





An den EXIF bzw. Metadaten

 **exifdata**

SUMMARY
DETAILED
UPLOAD

Penn-State-Onward-e1511895148681.jpg

(click for original!)
Resolution
960x525

File Size	89 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	960
Image Height	525
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	96
Y Resolution	96
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)

SUMMARY

Was kann man dagegen tun?



Was kann man gegen Angriffe unternehmen?

- ⇒ Misstrauisch sein
- ⇒ Regelmäßige Updates
- ⇒ Backups auf externe Datenträger
- ⇒ Verschlüsselung nutzen
- ⇒ Passwortmanager
- ⇒ Dokumenten prüfen, die man freigeben will (altes ist nicht immer gelöscht)
- ⇒ Keine PDFs öffnen, die man nicht erwartet oder von unbekannten Absendern
- ⇒ Zurückhaltung beim Veröffentlichen von vertraulichen und/oder persönlichen Informationen. Diese können leicht mit Google Hacking und anderen Tools gefunden werden.



Was kann man gegen Angriffe unternehmen?

- ⇒ Keine illegalen Apps/Games herunterladen und installieren
- ⇒ Grundsätzlich keine Adminrechte, um Manipulationen zu verhindern
- ⇒ 2-Faktor Authentifizierung - besonders für Passwortdatenbanken
- ⇒ lokaler Virenschutz und lokale Firewall

Für Fortgeschrittene:

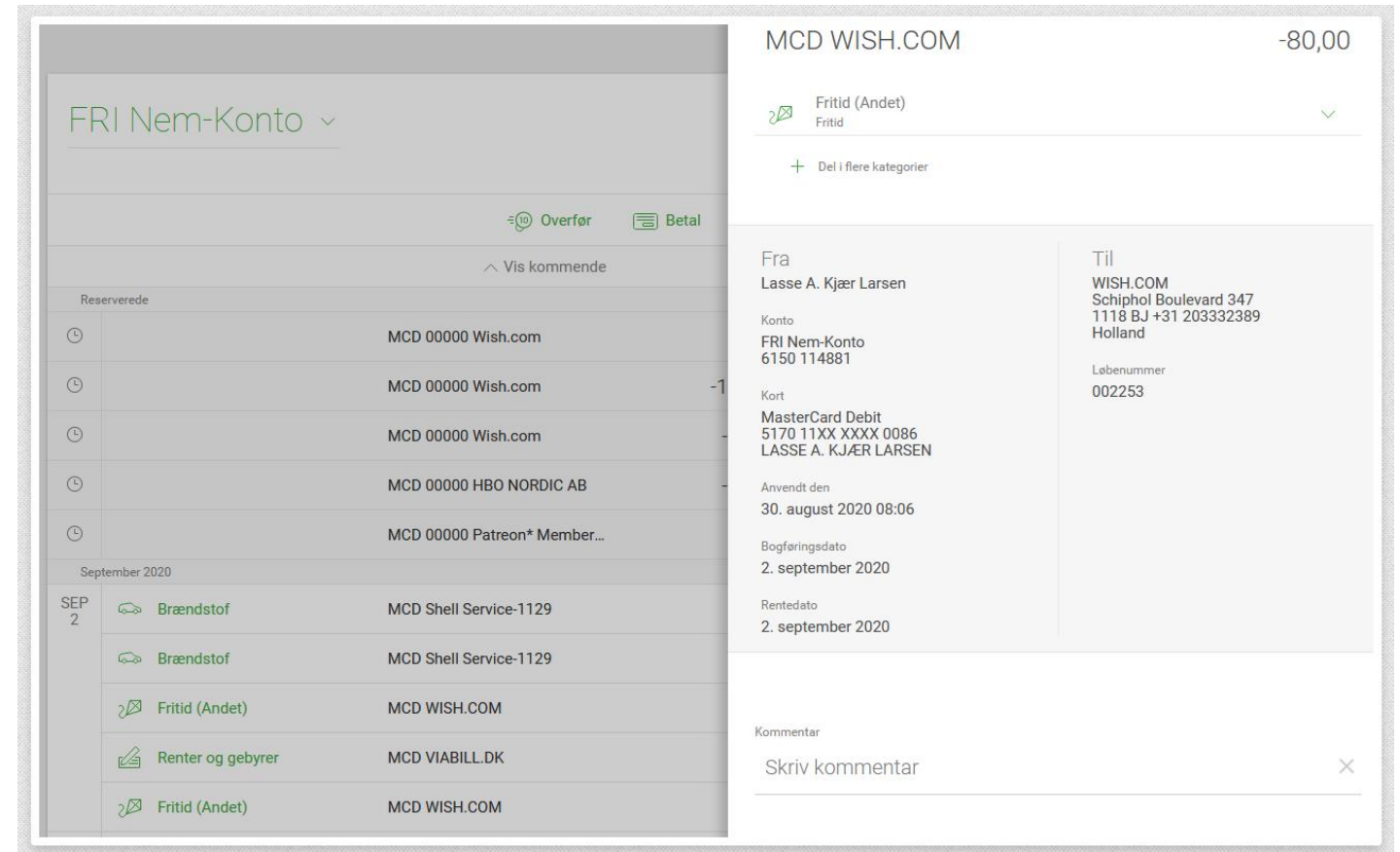
- ⇒ AdGuard / PiHole im Homenet
- ⇒ Homenet segmentieren



Kein Online Clipboard für sensible Informationen verwenden

<https://prnt.sc/uevhaa>

<https://prnt.sc/uaaaat>





Kein Online Clipboard für sensible Informationen verwenden

Hey! Paste it

Clip number : [Get it!](#)

Copy-Paste anything you want, then get it from anywhere.

Welche Nummer kommt als nächstes?

33 chars.

Clip number : **0IV5LH**
Direct URL : <https://www.heypasteit.com/clip/0IV5LH>

[Paste online](#)

[Follow us on Twitter](#)

© 2020 HeyPasteIt.com - All rights reserved.

https://www.heypasteit.com/clip/0IV5LA

Hey! Paste it

Clip number : **0IV5LA** [Get it!](#)

Copy-Paste anything you want, then get it from anywhere.

Clip number : **0IV5LA**
Direct URL : <https://www.heypasteit.com/clip/0IV5LA>
Date : 2020-09-28 19:28:59 GMT [Download as file](#)

xtoystore.com/fuzz50 | rricbahr@aol.com
xtoystore.com/blazer0096 | adtman34@gmail.com
xtoystore.com/lovestolick174 | tmason157@yahoo.com
xtoystore.com/anjinhad | mc.dezza@gmail.com
xtoystore.com/torajakuss2002 | jakuss2002@hotmail.com
xtoystore.com/91502479 | manohomemodopedasso@hotmail.com
xtoystore.com/obiwan745 | j.osea74@hotmail.com
xtoystore.com/yoursexymaster | sterdoggie@yahoo.com
xtoystore.com/stripbisher7 | stripbisher@gmail.com
xtoystore.com/needsomemore6910 | buford8888@live.com
xtoystore.com/Necessityevil | snugsend@yahoo.com
xtoystore.com/vishal221095 | vishalrocks2210@gmail.com
xtoystore.com/dehanson1105 | daniel_e_hanson@yahoo.com
xtoystore.com/horehound101 | franksta2008@hotmail.com
xtoystore.com/694u2injoy | christopherschappell@gmail.com
xtoystore.com/eling5955 | robmelting@yahoo.com
xtoystore.com/partime1976 | partime1976@gmail.com
xtoystore.com/Good604times | Smoothnammer@hotmail.com
xtoystore.com/abooood19 | mohamedabooood@yahoo.com
xtoystore.com/hunter201987 | awesome184@gmail.com
xtoystore.com/properkennedy | properkennedy@gmail.com
xtoystore.com/brownizze | tdagain@hotmail.com
xtoystore.com/mithrasfallen | phateshand@yahoo.com
xtoystore.com/canario046 | daniel-1977@hotmail.es
xtoystore.com/dva5862 | e574jones@aol.com
xtoystore.com/leo01977 | leandro_villanueva_465@hotmail.com
xtoystore.com/Gwavy1988 | gerod23@aol.com
xtoystore.com/subanerj | sbanerjee.111@gmail.com
xtoystore.com/two4you100 | morales.mekink@yahoo.com
xtoystore.com/dousthanks | richard_corariddell@yahoo.com
xtoystore.com/llovinlife | llovinlife@yahoo.com



```
Sitemap: https://www.nike.com/sitemap-us-help.xml
Sitemap: https://www.nike.com/sitemap-landingpage-index.xml
Sitemap: https://www.nike.com/sitemap-pdp-index.xml
Sitemap: https://www.nike.com/sitemap-launch-index.xml
Sitemap: https://www.nike.com/sitemap-wall-index.xml
Sitemap: https://www.nike.com/sitemap-article-index.xml
```

[illegible]

Weitere Empfehlungen



Kevin Mitnicks Motorola Hack

<https://www.vice.com/de/article/wie-hacker-kevin-mitnick-motorola-einen-geheimen-quellcode-abschwatzte/>

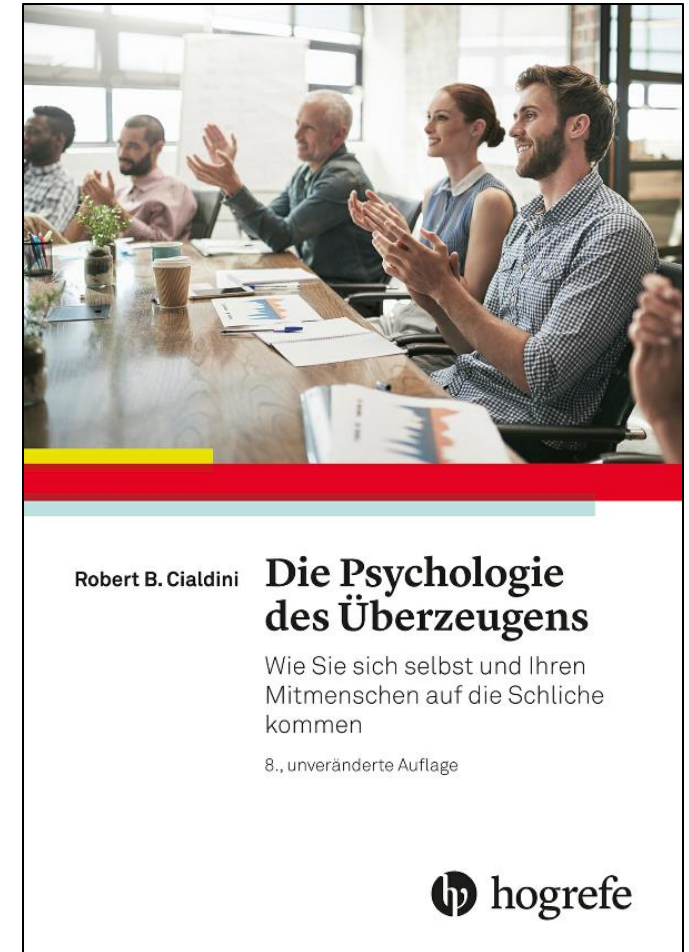
<https://youtu.be/UBaVek2oTtc>





<https://youtu.be/-YpwsdRKt8Q>

Reverse Engineering von Spiegel-Online



Anmerkungen oder Fragen?