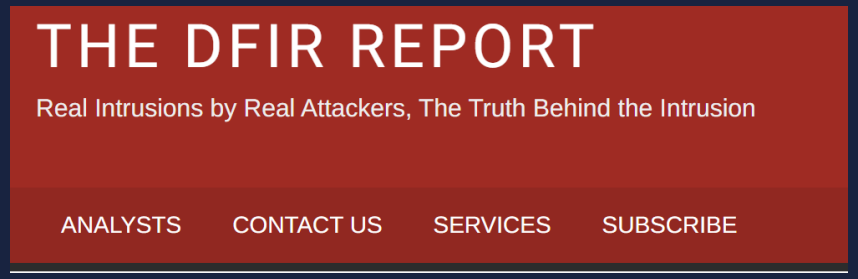
15-6-2023

Social Media from a hacker’s perspective

>whoami

- Rik Dolfing
- Ministerie van Defensie
  - Network Security en Detection Engineering
- Eye Security
  - ‘Managed Detection and Response’ voor het MKB
  - Persoonlijke focus op Incident Response en Threat Intelligence
- The DFIR Report
  - Analist en Schrijver
  - Eerste rapport komt nog ;-)

@Miixxedup



Even snel …

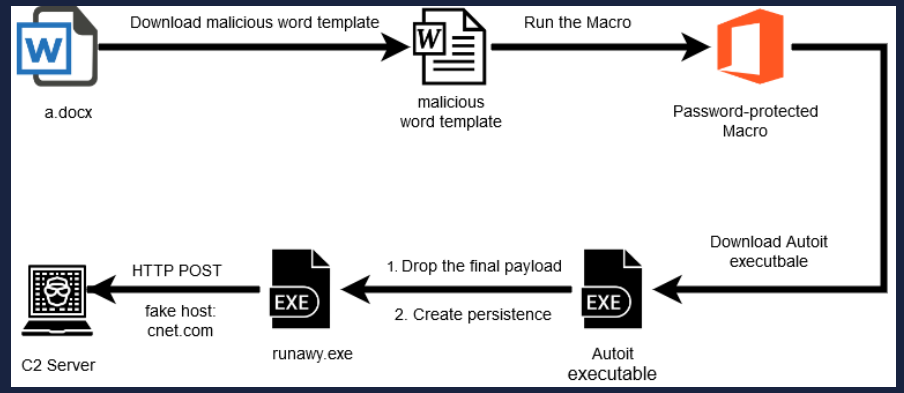
- Interactief en stel vragen, graag zelfs!
- Uitleg van technische aard
  - Informatief en beeldvormend
  - Risico inschatting
  - Mitigatie mogelijkheden

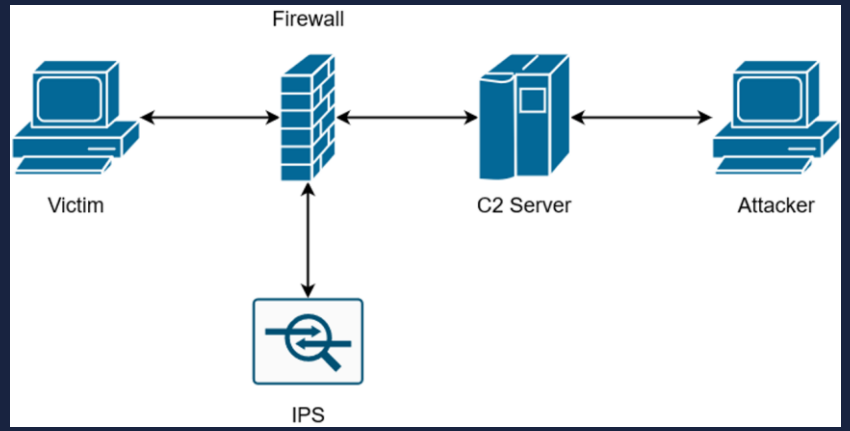
C2

Command and Control aka C&C aka C2

“ A command-and-control [C&C] server is a computer controlled by an attacker or cybercriminal which is used to send commands to systems compromised by malware and receive stolen data from a target network.

Many campaigns have been found using cloud-based services, such as webmail and file-sharing services, as C&C servers to blend in with normal traffic and avoid detection. “





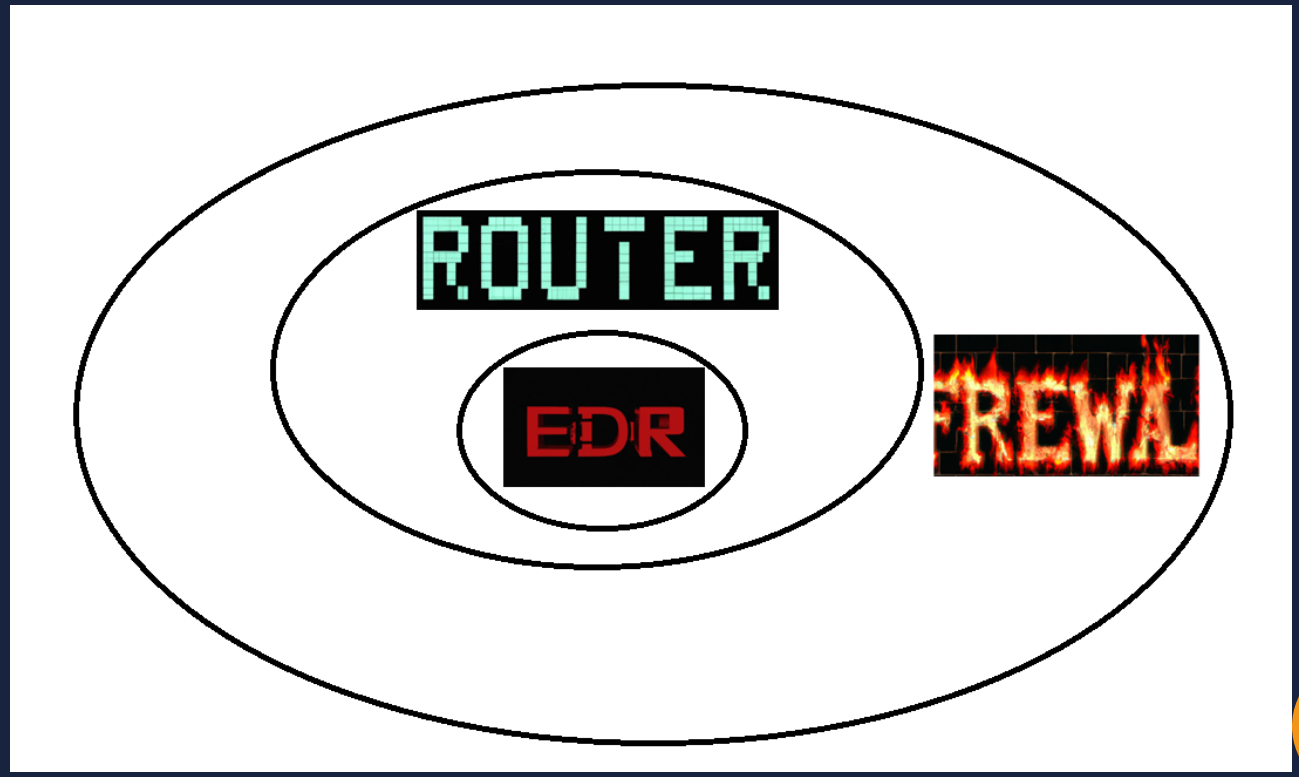
https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server
https://www.bleepstatic.com/images/news/u/1100723/APT/Gaza%20Cybergang/EnigmaSpark-infectionchain.png
https://arszilla.com/images/2021-11-14-hiding-your-c2-traffic-with-discord-and-slack/traditional-c2-infrastructure.png

Je Netwerk als ui …

- EDR Endpoint detection and Response ***(Focus: Host)***
  - Detecteert op de endpoints, traditioneel Anti virus

- Router ***(Focus: Network Intrusion and Detection System)***
  - Span opties voor Netwerk verkeer
  - Metadata generator zoals Zeek
  - NIDS zoals Suricata

- Firewall ***(Focus: Threat Intel)***
  - Next-Gen met Threat intel
  - Soms ook NIDS



Wat sta je toe als werkgever voor (social) media gebruik?

‘Suspicious’ meter

- http://78[.]24[.]222[.]162:37819
- http://www.abn-amro-bankpas.nl
- https://216.239.32.0
- https://www.facebook.com
- https://www.wikipedia.org
  - www.xn--wikipedi-86g.org
- https://www.nos.nl

LOTS and friends (LOLBAS, GTFOBIN, LOLDRIVERS)

Website	Tags	Service Provider
raw.githubusercontent.com	Phishing C&C Download	Github
github.com	Phishing Download	Github
1drv.ms	Phishing	Microsoft
1drv.com	Phishing Download	Microsoft
docs.google.com	Phishing C&C	Google
drive.google.com	Phishing Download Exfiltration	Google
*.azurewebsites.net	Phishing Download Exfiltration C&C	Microsoft
dropbox.com	Phishing Download Exfiltration C&C	Dropbox
mega.nz	Phishing Download Exfiltration	Mega Limited
pcloud.com	Phishing Download Exfiltration	pCloud
*.amazonaws.com	Phishing Download Exfiltration C&C	Amazon Web Services
*.twitter.com	C&C	Twitter

Phishing

Azure web applications allows users to create a customized subdomain on azurewebsites.net. Attackers abuse this functionality by hosting phishing websites using the azurewebsites.net domain.

Command and Control

Malware such as Almaq have used Azure web applications as their C&C servers.

Exfiltration

Attackers can create web applications with upload functionalities hosted on *.azurewebsites.net and exfiltrate data on there.

Download

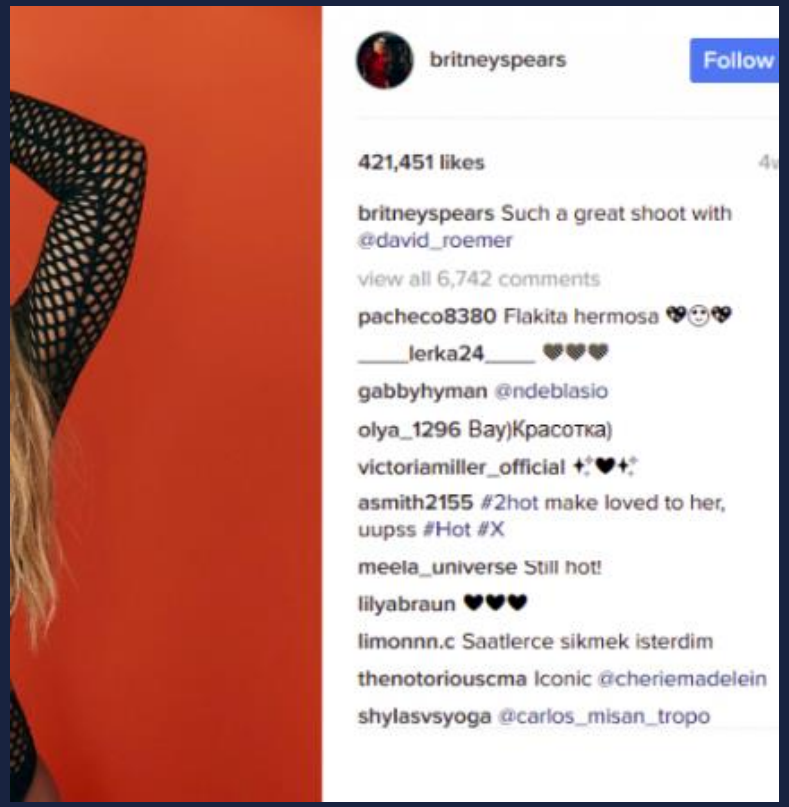
Attackers can host malicious tools on applications hosted on *.azurewebsites.net and download them when needed.

Service Provider

Microsoft

https://lolbas-project.github.io/
https://gtfobins.github.io/
https://www.loldrivers.io/
https://lots-project.com/

APT Turla



asmith2155 #2hot make loved to her, uupss #Hot #X

⇩ Special Hash == 183

```
(?:\\u200d(?:#|@)(\\w)
```

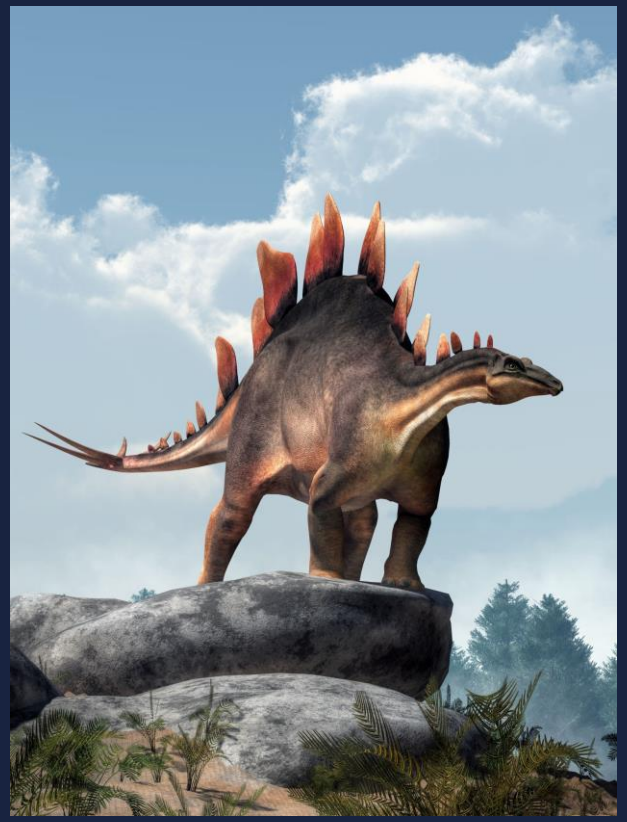
⇩ re.result()

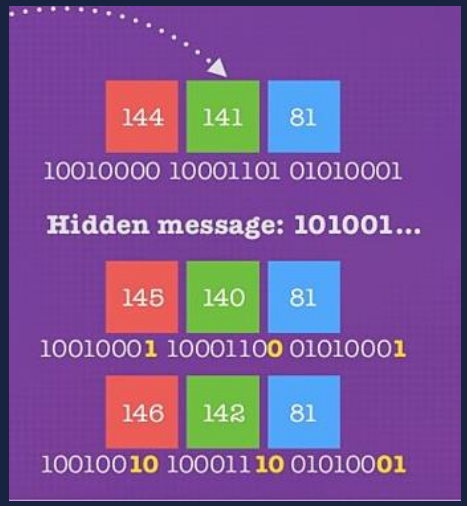
http://bit.ly/2kdhuHX

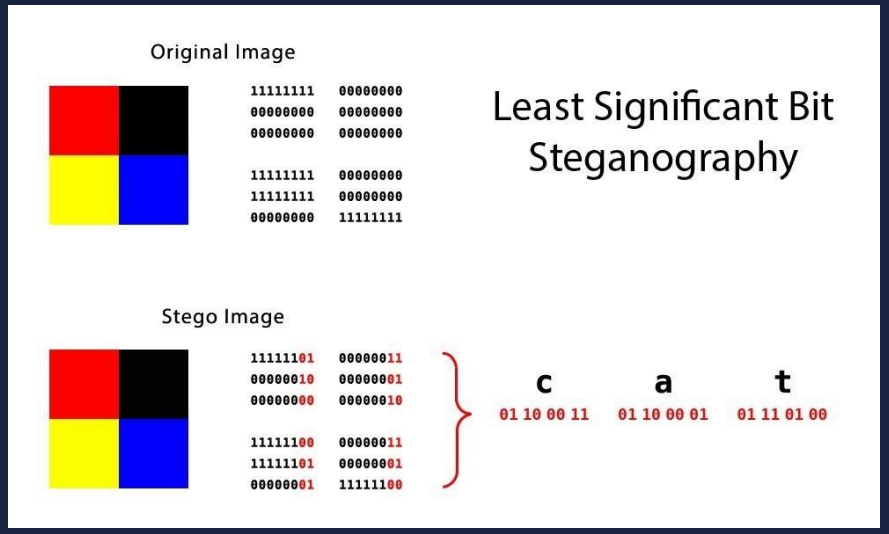
```
smith2155<200d>#2hot ma<200d>ke lovei<200d>d to <200d>her, <200d>uupss <200d>#Hot
<200d>#X
```

- https://www.welivesecurity.com/2017/06/06/turlas-watering-hole-campaign-updated-firefox-extension-abusing-instagram/?utm_source=facebook&utm_medium=cpc&utm_campaign=welivesecurity

Steganografie

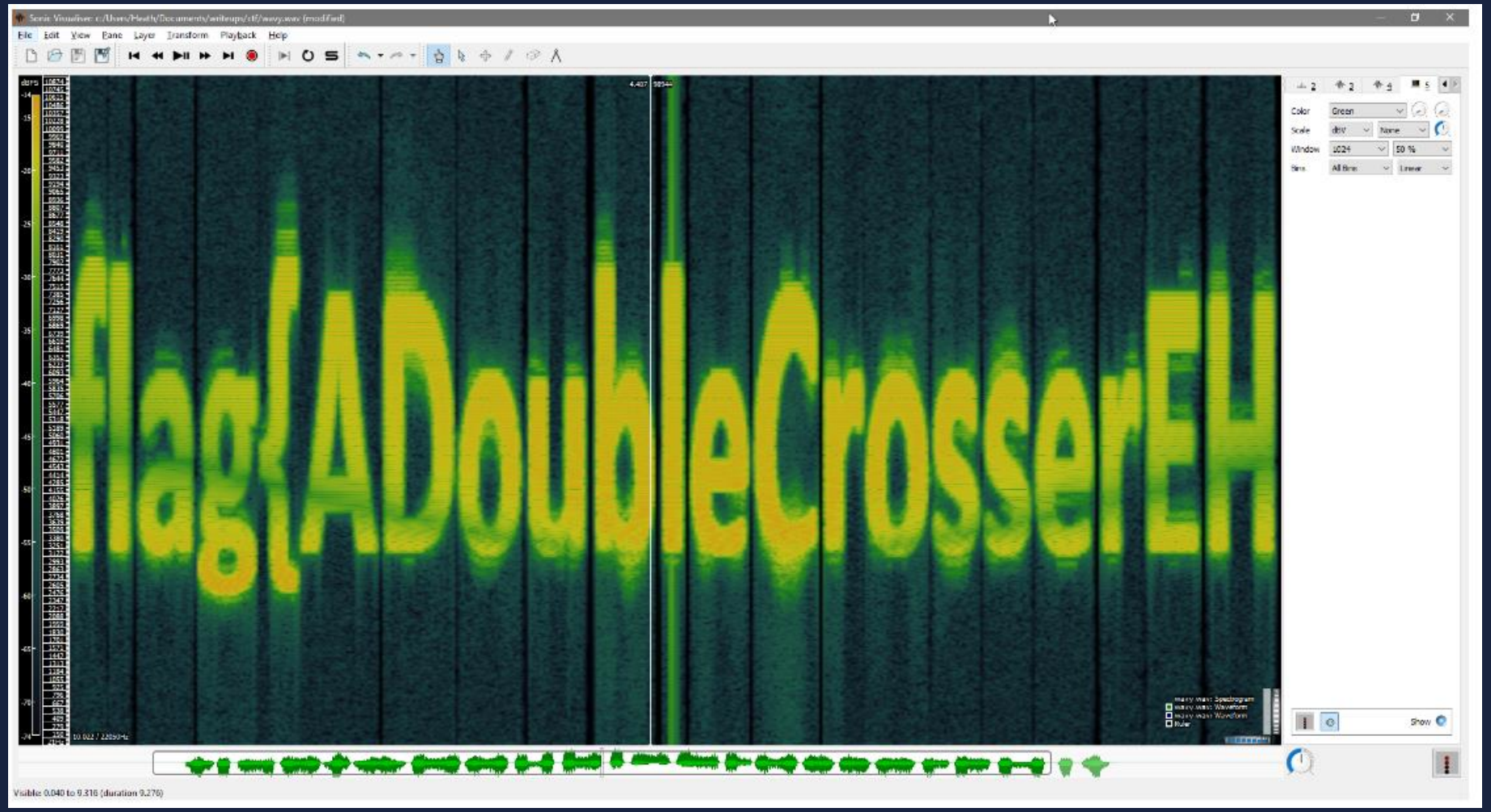






https://qph.cf2.quoracdn.net/main-qimg-ab7cb1be0a6fd23b253e3a50b37ef255-pjlq
https://img.wonderhowto.com/img/02/61/63645877844452/0/steganography-hide-secret-data-inside-image-audio-file-seconds.w1456.jpg

Steganografie (2)



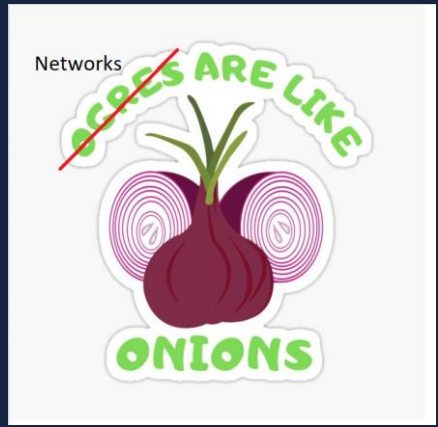
https://veteransec.org/vetsec-takes-first-in-the-hacktober-ctf-summary-steganography-write-up/

Mitigatie C2 Risico’s

- EDR Perspectief
  - Een mogelijke malware raakt waarschijnlijk de schijf
  - Gedrag later in de ‘killchain’ wordt zichtbaar.
  - ‘Last line of defense’

- Netwerk Perspectief:
  - Extracten van documenten vanuit netwerk data en sandboxen.
  - Kost veel resources, data is vaak dubbel
  - Beperkte ingrijp mogelijkheden, vooral retroactief

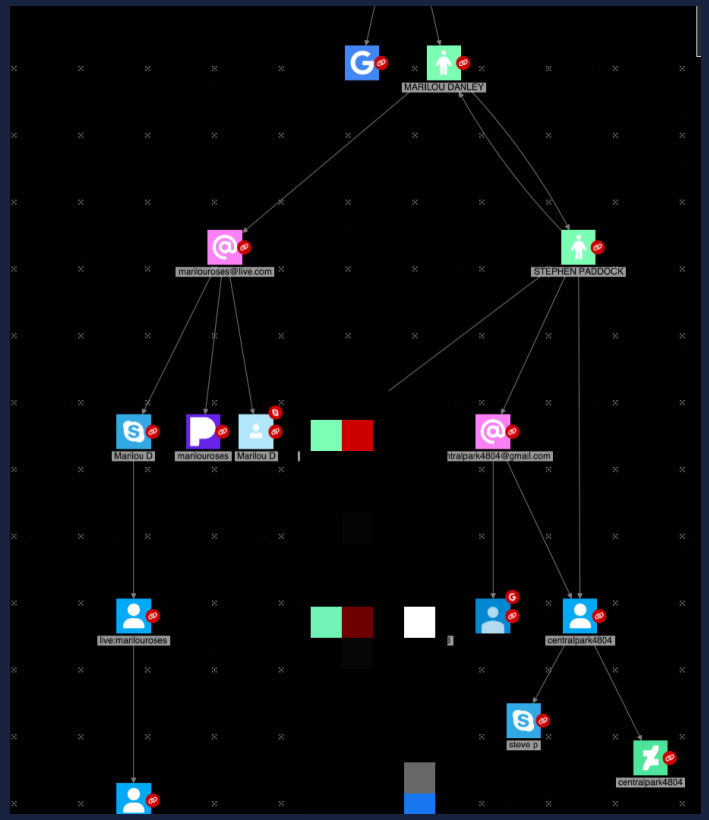
- Threat Intelligence Perspectief
  - Goeie indicatie van specialisten
  - Duur
  - False positive gevoelig



whoareu

Gebruik Social Media

- Belangrijke risico factoren:
  - Is het gericht op een individu / groep ?
  - Wat is de ‘awareness’ in de organisatie ?
- Bewust of onbewust geplaatste data
  - Bewust
    - Vakantie kiekjes
    - Promoties
    - Nieuw huis
    - Andere mijlpalen
- Risico’s ?

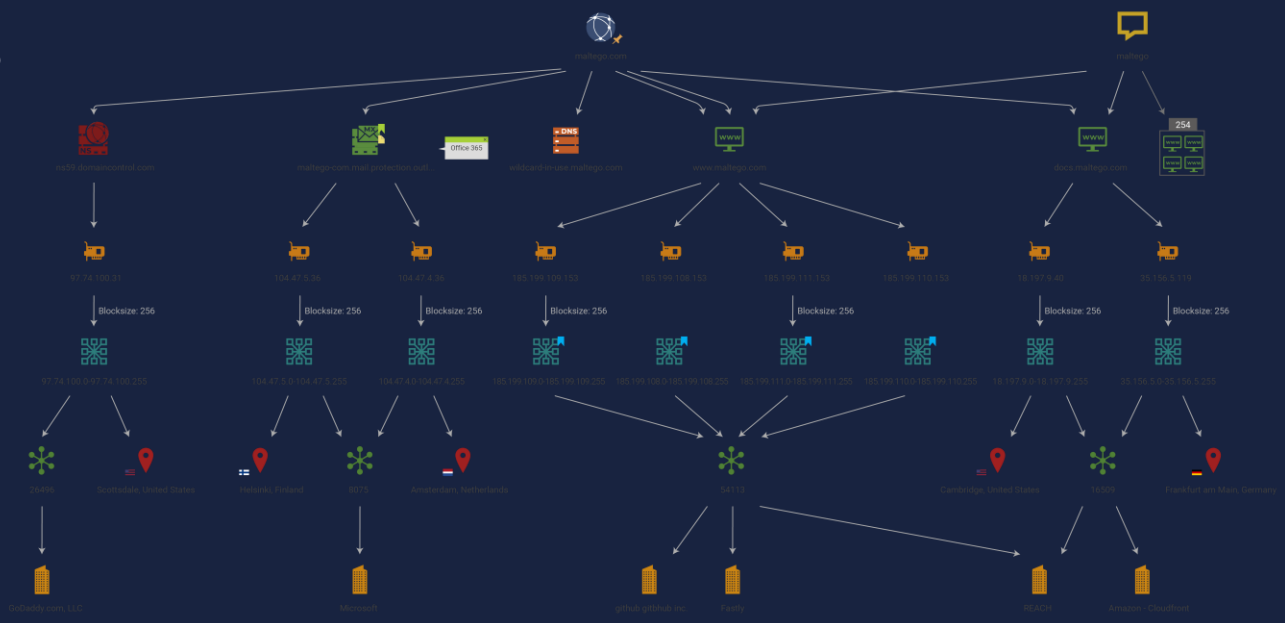


Sleutel Kopie

https://www.youtube.com/watch?v=pohVT1nKZig&ab_channel=ITSTactical%2FImminentThreatSolutions

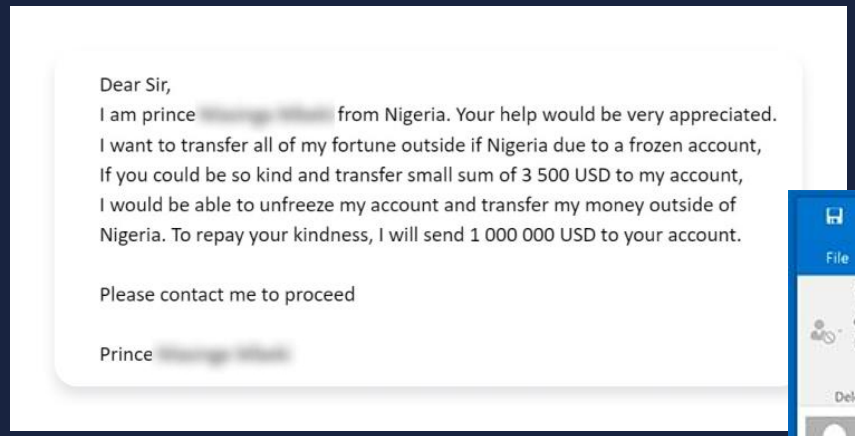
Gebruik Social Media

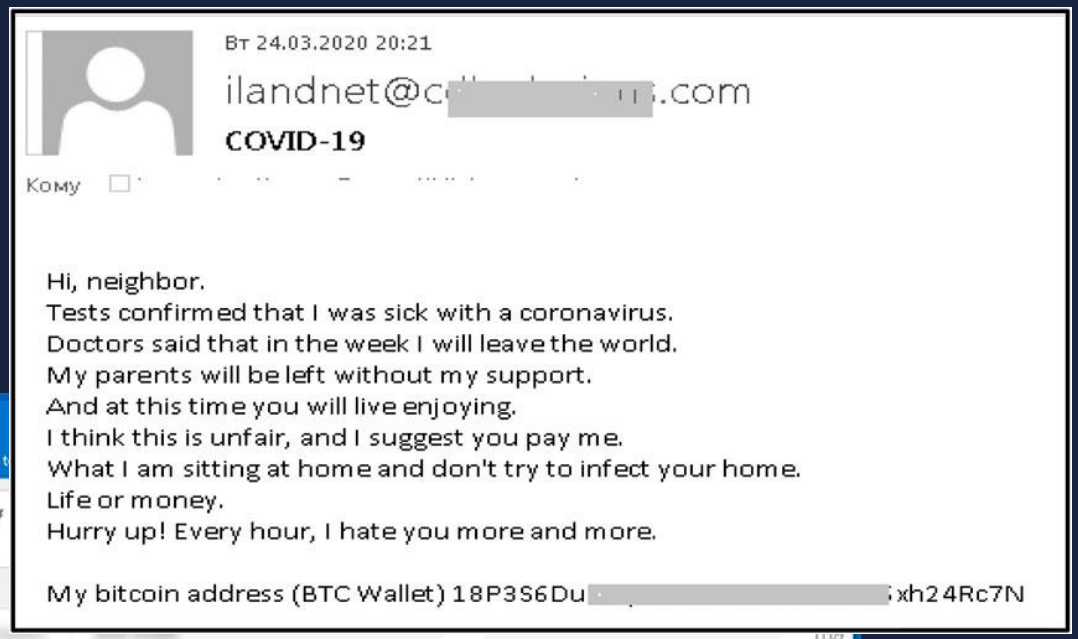
- Belangrijke risico factoren:
  - Is het getarged op een individu / groep ?
  - Wat is de ‘awareness’ in de organisatie ?
- Bewust of onbewust geplaatste data
  - Onbewust
    - Data lekken
    - Dark web / Dark Net forum
    - Google Dork
    - https://pipl.com/
    - https://rocketreach.co/
    - https://www.clearview.ai/
    - https://www.dehashed.com/
- Risico’s ?

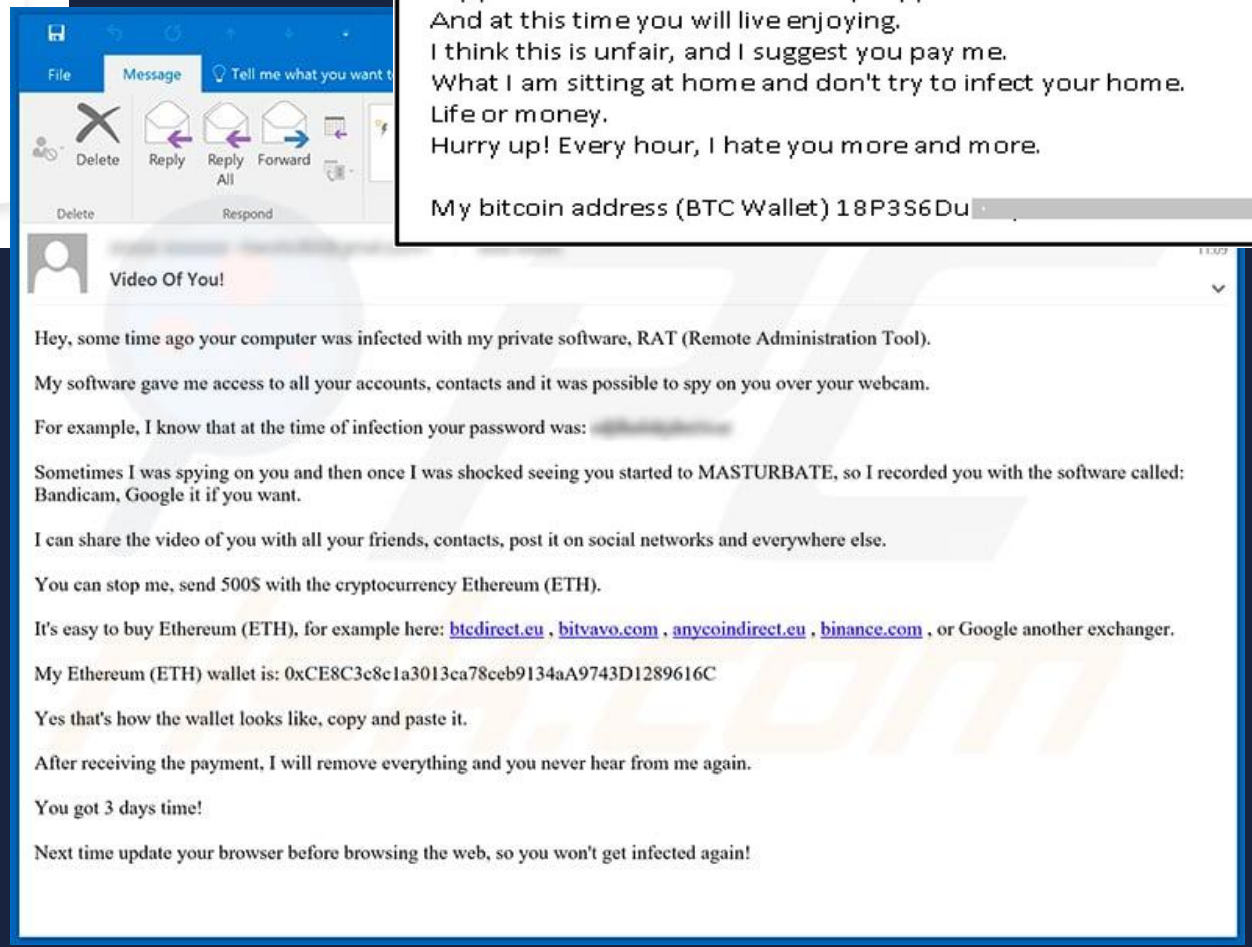


https://upload.wikimedia.org/wikipedia/commons/3/3e/Maltego-example-Graph-L_%281%29.png

Hagel en Duct Tape







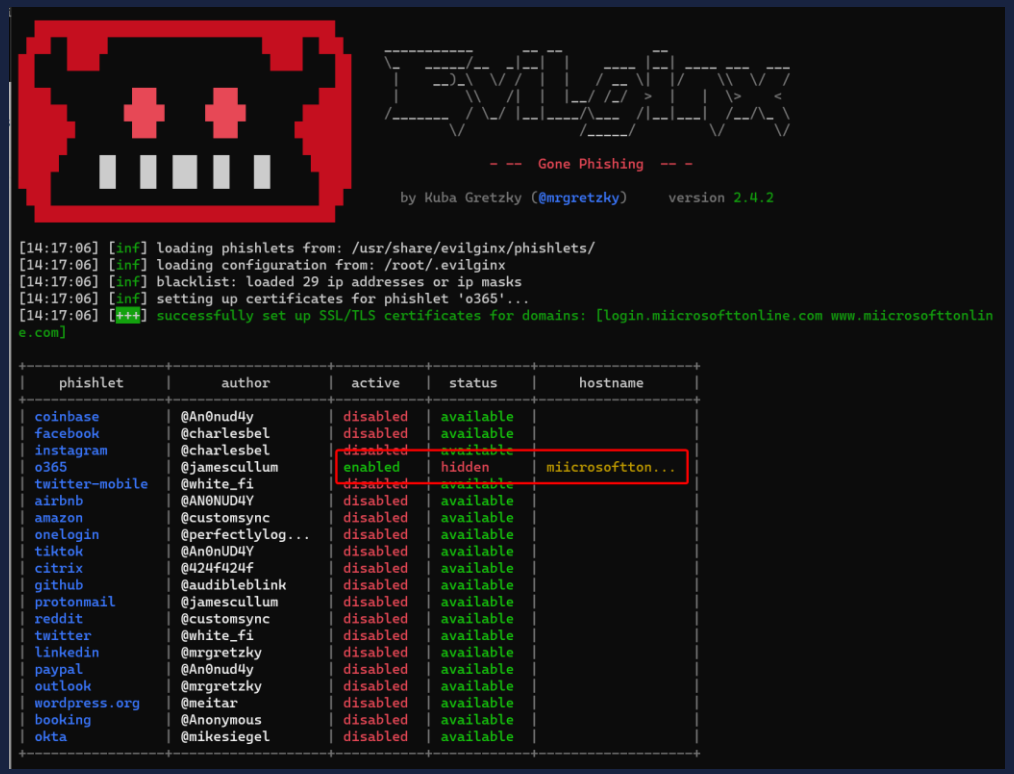
- Hoe gaan we dit verbeteren ?
  - Persoonlijker
  - Dringender
  - Opmaak

Hagel en Duct Tape (2)

Meer overtuiging? Gebruik Social Media!

- Van (gebruikers)naam naar persoon:
  - https://github.com/sherlock-project/sherlock
  - https://github.com/piaolin/DetectDee
- Persoonlijke eigenschappen in kaart brengen
  - Targeted Phishing
  - https://github.com/kgretzky/evilginx2
- Timing timing timing!
  - Nieuw in organisatie
  - Op vakantie, noodzaak duidelijk maken
- (Correct) taalgebruik
  - https://www.deepl.com/en/translator
  - Chatgpt ... (toch even op de hype train)

Hagel en Duct Tape (3)



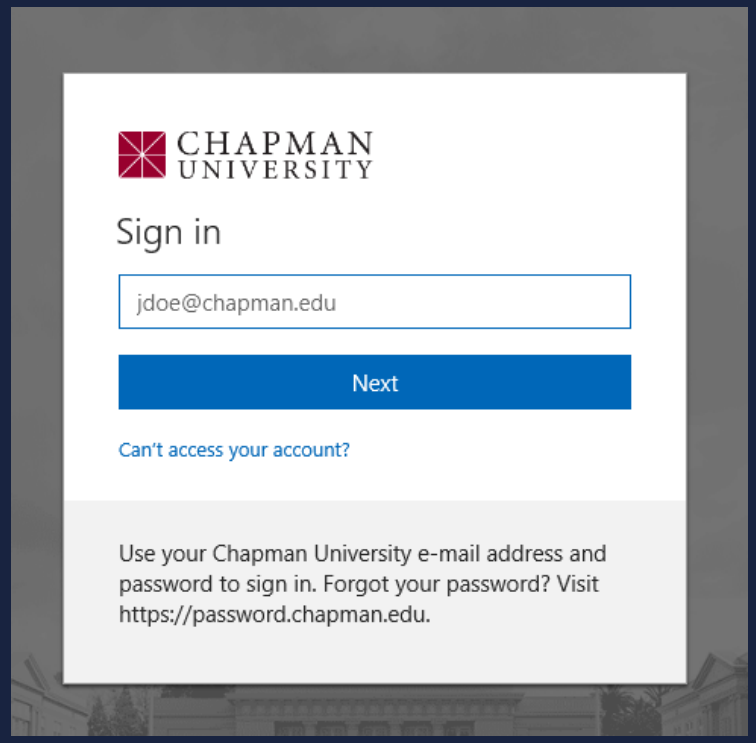
```
 ___________           __ __                  __
 \_   _____/__  __ __ |__|  |   ____ |__| ____ ___  ___
  |    __)_\  \/ /  |  |  |  / __ \|  |/    \\  \/  /
  |        \\   /|  |  |  |__/ /_/  >  |   |  \>    <
 /_______  / \_/ |__|____/\___  /|__|___|  /__/\_ \
         \/                   /_____/     \/      \/

 - --  Gone Phishing  -- -

by Kuba Gretzky (@mrgretzky)     version 2.4.2

[14:17:06] [inf] loading phishlets from: /usr/share/evilginx/phishlets/
[14:17:06] [inf] loading configuration from: /root/.evilginx
[14:17:06] [inf] blacklist: loaded 29 ip addresses or ip masks
[14:17:06] [inf] setting up certificates for phishlet 'o365'...
[14:17:06] [+++] successfully set up SSL/TLS certificates for domains: [login.miicrosofttonline.com www.miicrosofttonline.com]
```

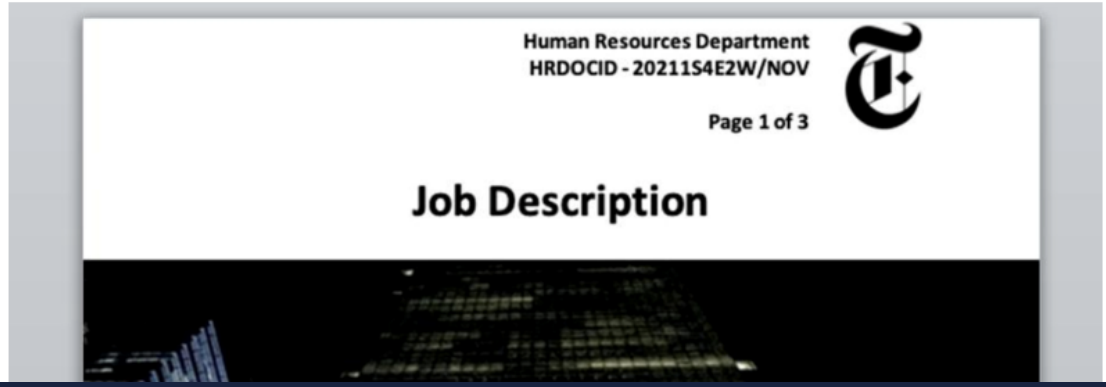
phishlet	author	active	status	hostname
coinbase	@An0nud4y	disabled	available	
facebook	@charlesbel	disabled	available	
instagram	@charlesbel	disabled	available	
o365	@jamescullum	enabled	hidden	miicrosoftton...
twitter-mobile	@white_fi	disabled	available	
airbnb	@AN0NUD4Y	disabled	available	
amazon	@customsync	disabled	available	
onelogin	@perfectlylog...	disabled	available	
tiktok	@An0nUD4Y	disabled	available	
citrix	@424f424f	disabled	available	
github	@audibleblink	disabled	available	
protonmail	@jamescullum	disabled	available	
reddit	@customsync	disabled	available	
twitter	@white_fi	disabled	available	
linkedin	@mrgretzky	disabled	available	
paypal	@An0nud4y	disabled	available	
outlook	@mrgretzky	disabled	available	
wordpress.org	@meitar	disabled	available	
booking	@Anonymous	disabled	available	
okta	@mikesiegel	disabled	available	



Targeted LinkedIn

The hackers start their attack by approaching targets over LinkedIn, posing as job recruiters. Ultimately, they shifted to WhatsApp to continue the "recruitment" process, sharing a Word document embedded with malicious macros.

Mandiant says that in some cases, these Word documents are stylized to fit job descriptions that they are promoting to targets. For example, one of the lures shared by Mandiant impersonates the New York Times, as shown below.



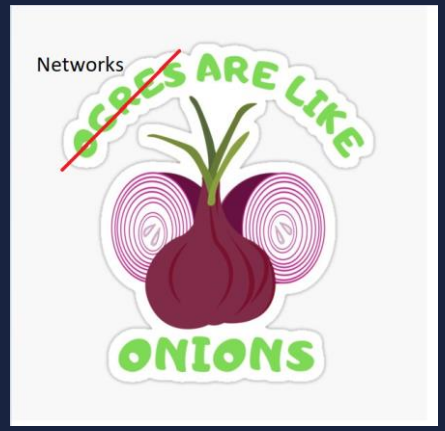
https://www.bleepingcomputer.com/news/security/security-researchers-targeted-with-new-malware-via-job-offers-on-linkedin/

Mitigatie Communicatie buiten het zicht

- EDR Perspectief
  - Een mogelijke malware raakt waarschijnlijk de schijf
  - Stukken moeilijker in cloud omgevingen

- Netwerk Perspectief:
  - Monitoren van social media, via gespecialiseerde partij
  - Lastig buiten eigen kantoor

- Threat Intelligence Perspectief
  - Dreigingsbeeld van bepaalde organisaties delen
  - Duur
  - False positive gevoelig
  - Onrust binnen bedrijf



Vragen?

“Social media in the media”

- Youtube:
  - Max Fosh
  - Social Engineering at Defcon
  - […]
- https://www.dutchosintguy.com/ Nico “Dutch_Osintguy” Dekens
- Bellingcat
- [..]