Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust center.

Connect2Trust

HSD securitydelta.nl

CYBERVEILIG NEDERLAND

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

telindus
a Proximus company

avit

cisco SECURE

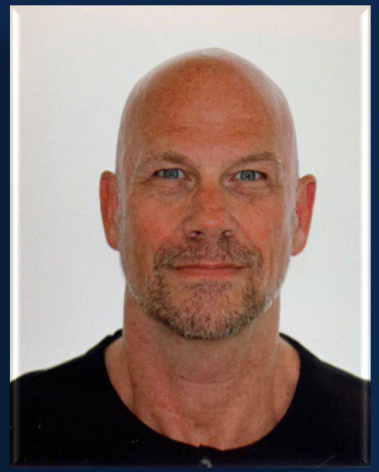
Day in life at the Dutch Tax Office SOC

Karl Lovink
Technical Lead Security Operations Center, Dutch Tax and Customs Administration
September 22, 2023

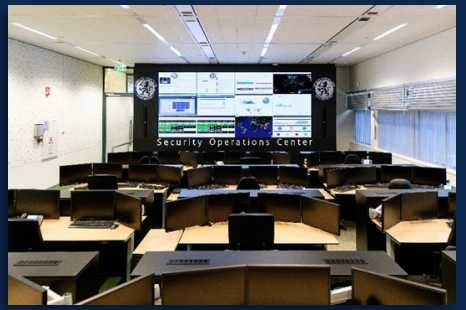
Agenda

1. Organization
2. Security Operations Center
3. Facts, Incidents and Figures
4. Partnerships

$whoami



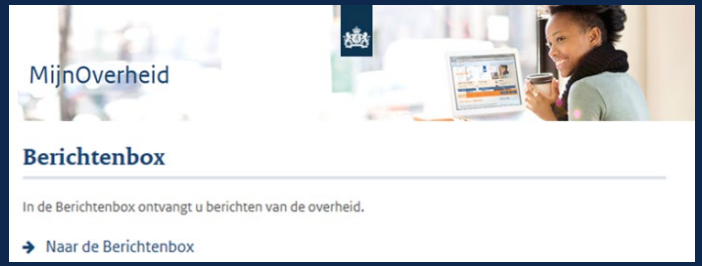
Karl Lovink
Technical Lead SOC
Liaison NCSC
Dutch Tax and Customs Administration
kw.lovink@belastingdienst.nl



18 Security Analisten
Started in june 2010

Share experience. Build resilience.

Who do we work for



- Citizens and companies
- Customers within the service
- Customers outside the service

IT – Facts and Figures

24 Petabyte storage

> 2000 Physical
> 21.500 Virtual

3 locations

43.000 notebooks/pc

1.600 applications

30 million LoC

> 50.000 mobile devices

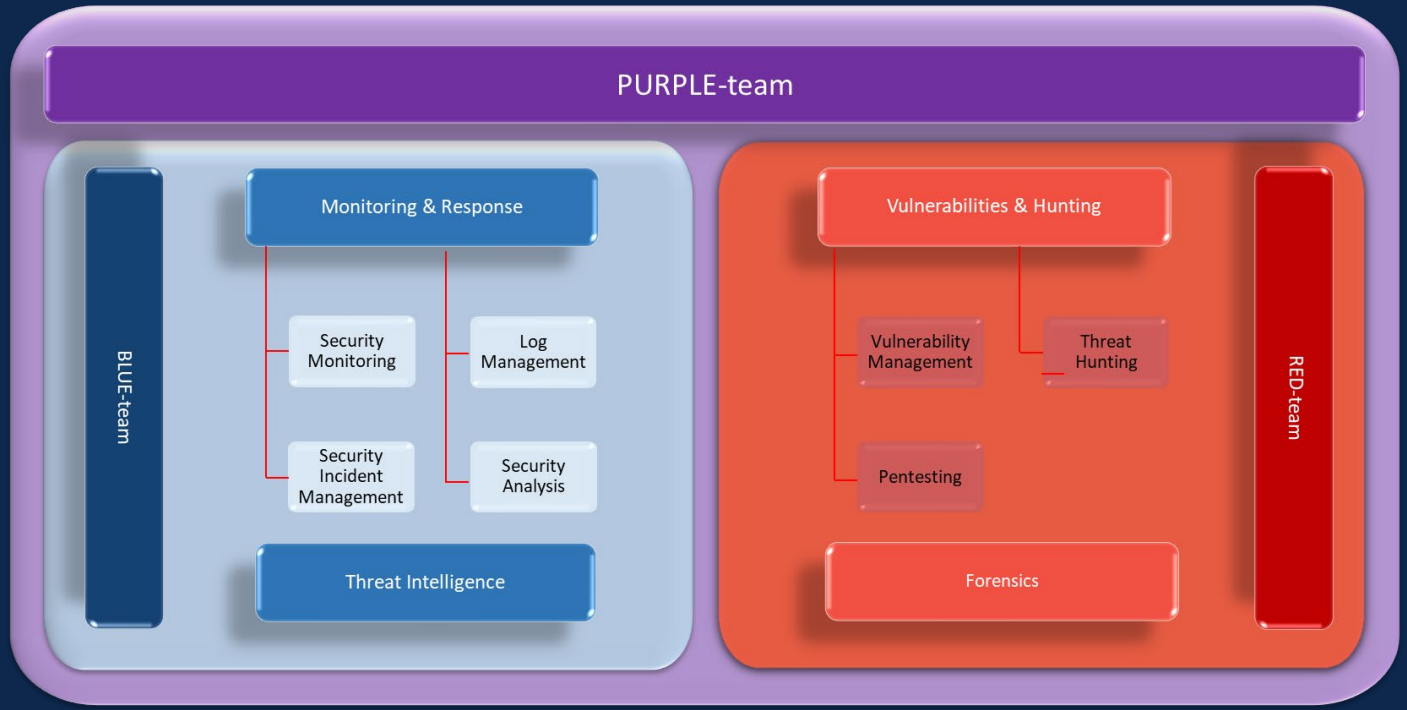
> 300 apps

Share experience. Build resilience.

Definition Security Operations Center

"A Security Operation Center (SOC) is a centralized function within an organization employing **people, processes, and technology** to continuously monitor and improve an organization's security posture while **preventing, detecting, analyzing, and responding** to cybersecurity incidents."

Main processes SOC



Monitoring & Response

The SOC deals with Security Monitoring, examples of which are :

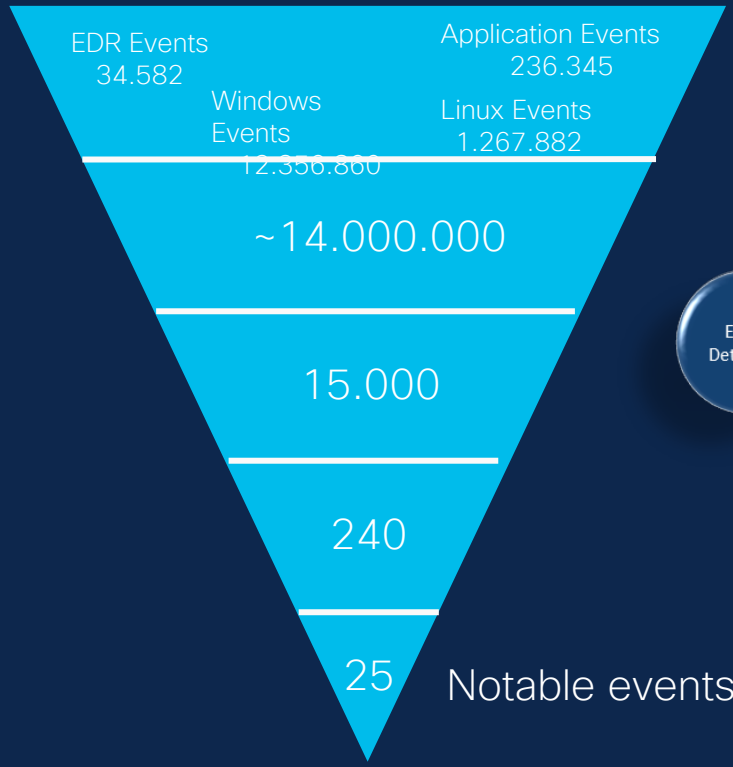
- Unauthorized account creation in the domain “Belastingdienst”
- Use of honey token account

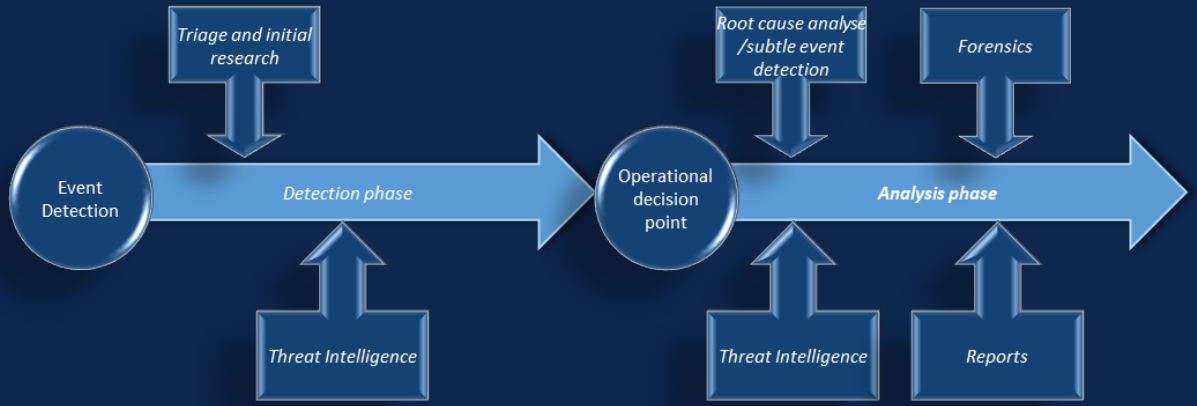
Examples not covered by security monitoring:

- An unexpected restart
- Unexpected restoration of a backup
- Availability of an application
- Abnormalities in behavior

Note: Availability lies with Operations Bridge

Challenge: from events to incidents





Monitoring & Response – Use-cases

What is a SOC use-case?

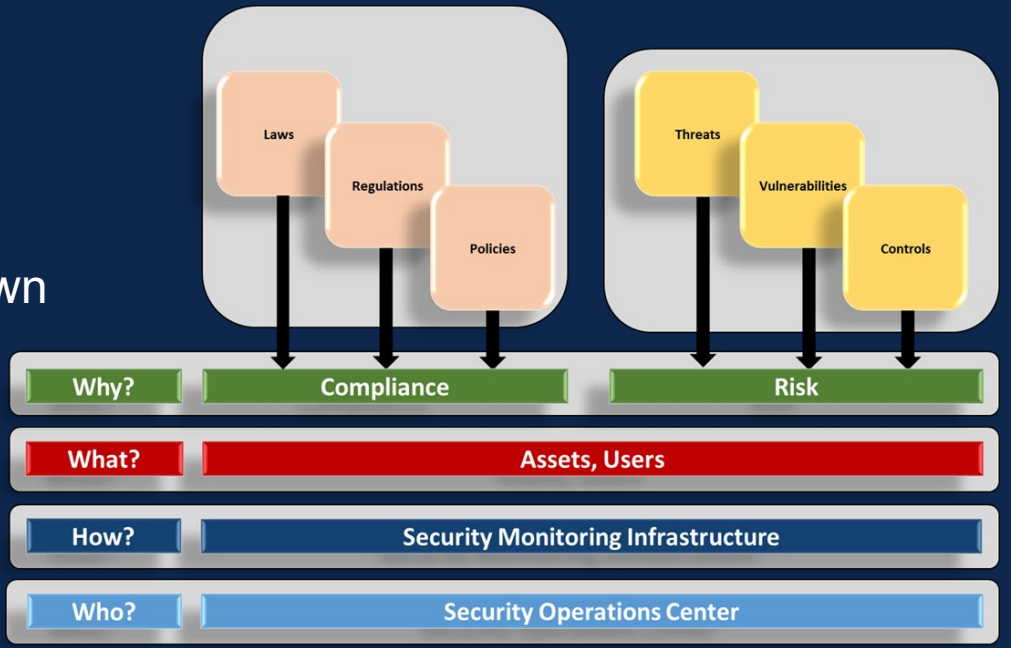
“Methodology used by the SOC team to identify and organize technical and organizational requirements for detection and response to specific threats”

From 3 billion events to 24 notable events……

MAGMA Use-case Framework

The MaGMa Use Case Framework (UCF) is a framework and tool for use case management and administration on security monitoring

Now: Use-case: bottom-up
Future: Risks/Compliance: top-down

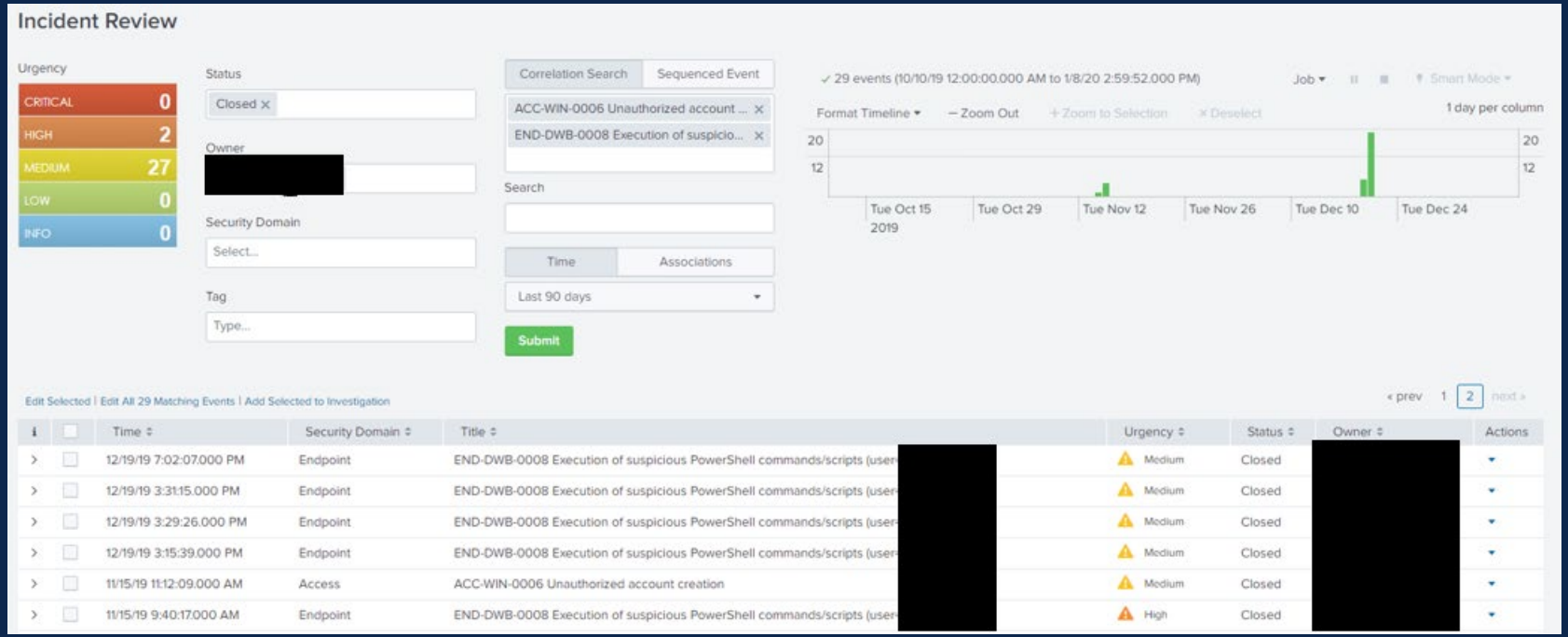


Source: https://www.betaalvereniging.nl/en/safety/magma/

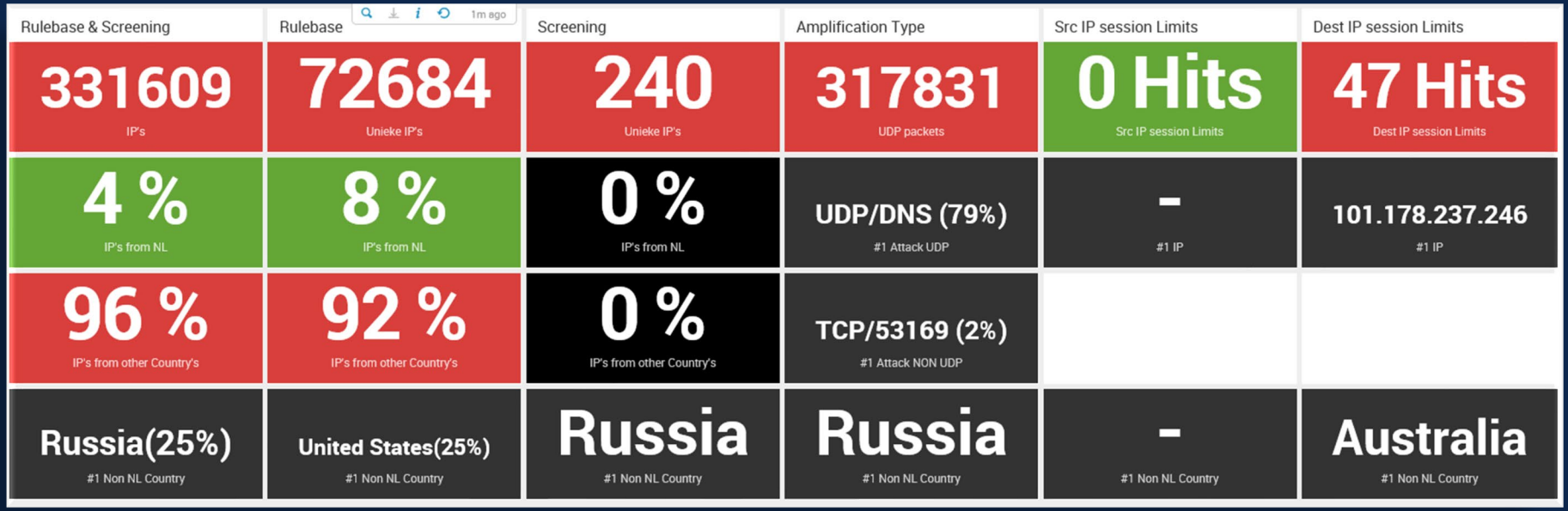
Monitoring & Response – Use-case Examples

- Inside to inside:
  - Unauthorized creation of users
  - Use of "honey token accounts"
- Outside to inside:
  - DDoS detection
  - Inbound malware
  - Hacking attempts, exploiting vulnerabilities, Coordinated Vulnerability Disclosure
- Inside to outside:
  - Detection of network traffic to botnets, malware workstations
- Outside to outside:
  - Reports citizens phishing/smishing

Security Incident and Event Management System



Outside to inside: DDoS detection/mitigation



Outside to Inside – DDoS exercises

Twice a year

- Volume-based DDoS test
- Applicative DDoS test

SURF

Nikhef

T-Mobile

Rijksoverheid

Anti-DDoS Coalition
No More DDoS

POLITIE

kpn

SIDN

T-Mobile

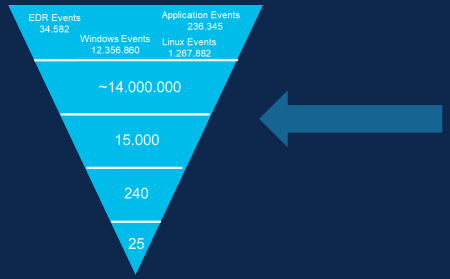
NBIP nationale beheersorganisatie internet providers

NLIX The Interconnect Exchange

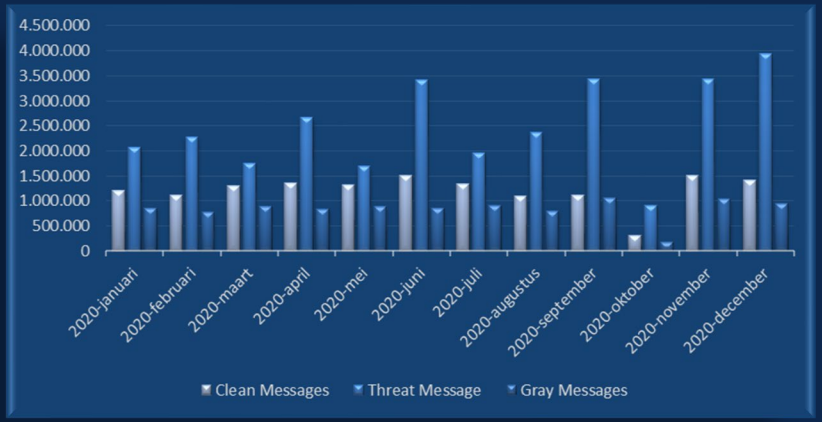
Share experience. Build resilience.

Outside to Inside – External Mail

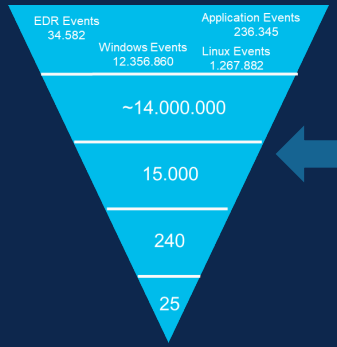
Totals 2020



Threat Messages	29.974.532	54,75%
Gray Messages	10.105.605	18,46%
Clean Messages	14.663.156	26,79%
Total	54.743.293	100.00%

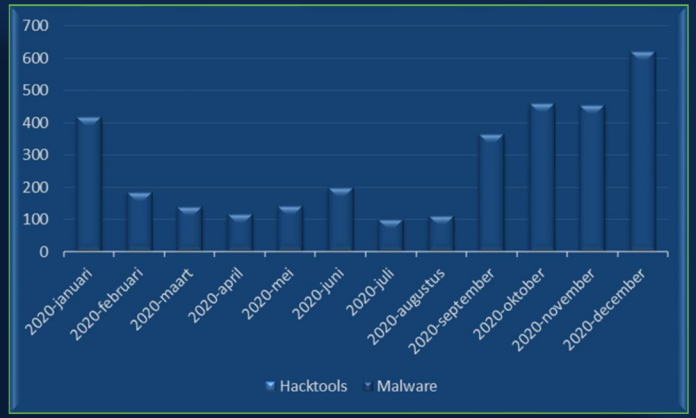


Inside to outside/inside – Malware workstations



Totals 2020

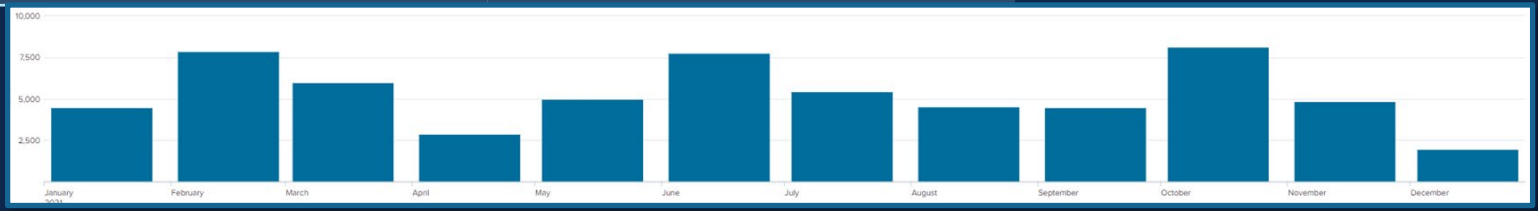
- Malware 5799
- Hacktools 29



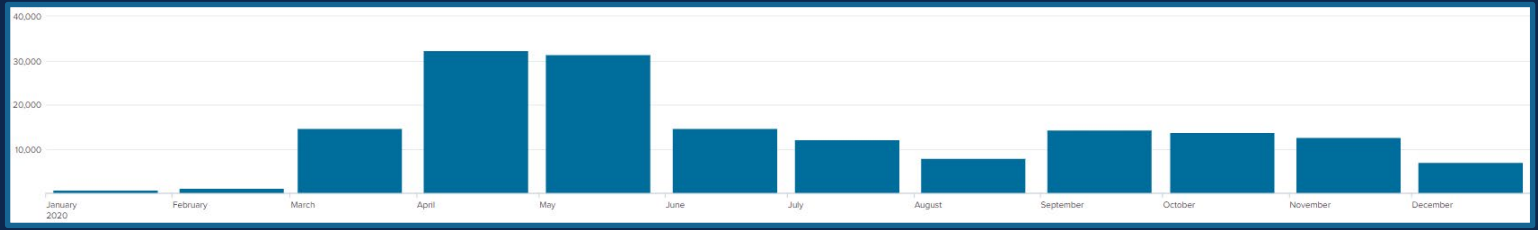
Outside to outside – Phishing, Smishing

# e-mail received	2017	2020	2021
Valse-email@belastingdienst.nl	7.791	162.624	63.200

2021



2020



Outside to outside – Phishing, Smishing

Link naar betaalverzoek

Link shortener

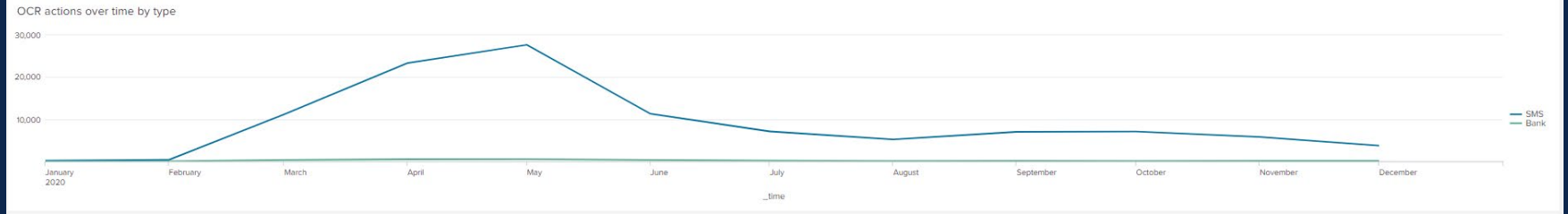
E-mail phishing

Fake websites

Share experience. Build resilience.

Outside to outside – Phishing, Smishing

Bank accounts blocked [total]	Mobile numbers blocked [total]	SMS screenshots	Bank screenshots
695	1,466	109,863	2,235



Share experience. Build resilience.

Outside to outside – Phishing, Smishing

Ik heb helaas dit bedrag overgemaakt!

Mvg M. [redacted]
Tel:06-2[redacted]

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

Van: "Belastingdienst" <belastingaangifte@belastingdienst.nl>
Datum: 23 augustus 2015 11:05:10 CEST
Aan: [redacted]
Onderwerp: Belastingaangifte 2014
Antwoord aan: belastingaangifte@belastingdienst.nl

Onderwerp: Fwd: Belastingaangifte 2014
Van: [redacted]t.nl>
Datum: 4-8-2015 21:40
Aan: [redacted]nistration[redacted]nl>

GEBOEKT

graag meteen betalen

Moet dit worden ingeboekt?

-------- Doorgestuurd bericht --------
Onderwerp: Belastingaangifte 2014
Datum: Tue, 4 Aug 2015 21:39:52 +0200
Van: Belastingdienst <belastingaangifte@belastingdienst.nl>
Antwoord-naar:belastingaangifte@belastingdienst.nl
Aan:[redacted]

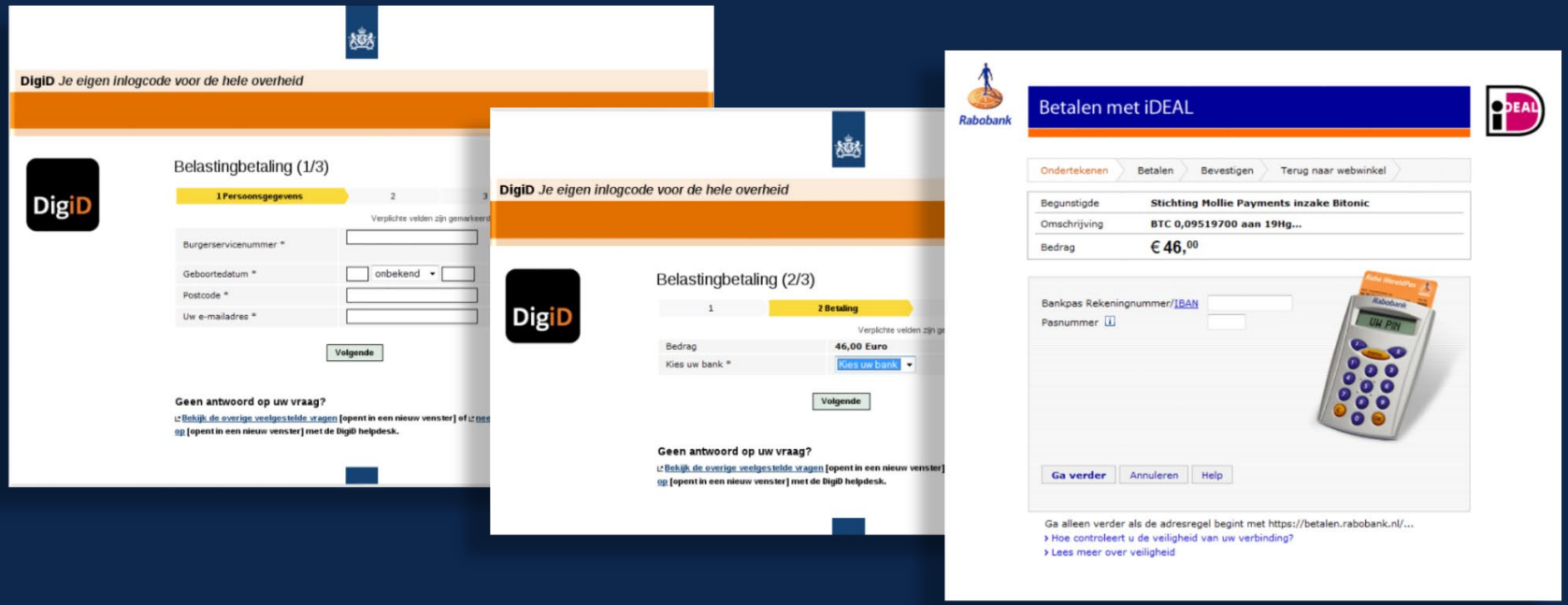
BETAALD PER [redacted] 05 AUG 2015

BETAALD PER [redacted] 05 AUG 2015

Geachte heer/mevrouw,

Bij controle van onze administratie hebben wij geconstateerd dat er een betaling achterstand

Outside to outside – Phishing, Smishing



Outside to outside – Phishing, Smishing

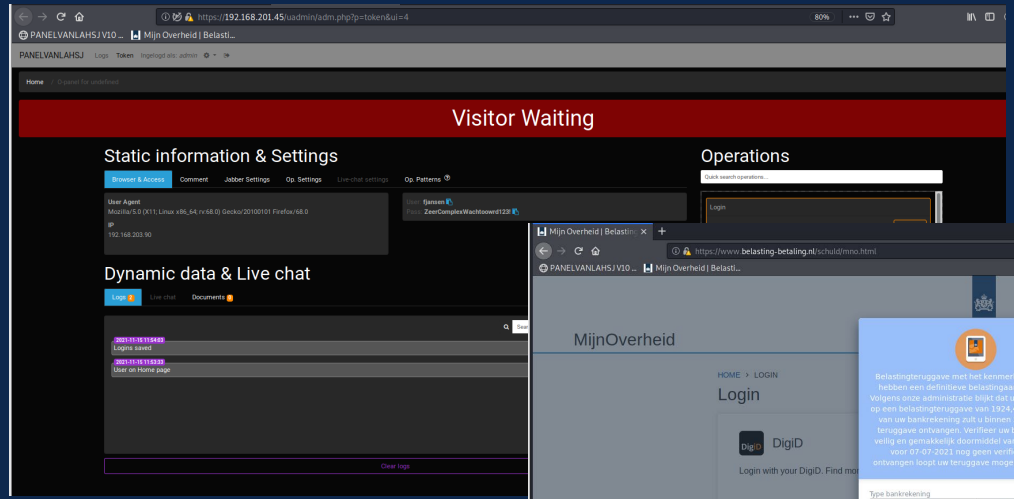
[Success] BTC Address: <bitcoin wallet>
idc: <ssn>
dbd: 01
dbm: 9
dby: <geboortejaar>
zip: <zipcode>
eml: <email adres>
bid: ideal_RABONL2U

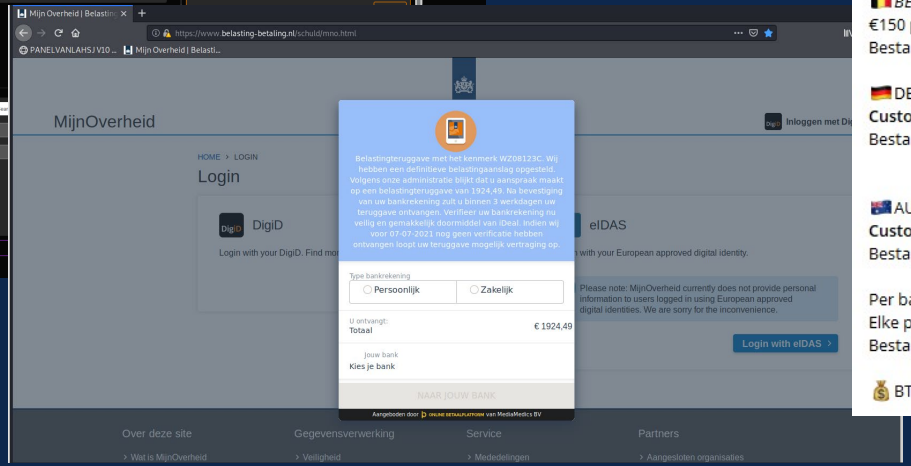
IP : 84.26.XX.XX9
USERAGENT : Mozilla/5.0 (Windows NT 6.1; WOW64) (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36
==========

Success] BTC Address: <bitcoin wallet>
idc: <ssn>
dbd: 21
dbm: 11
dby: <geboortejaar>
zip: <zipcode>
eml: <email adres>
bid: ideal_RABONL2U

IP : 77.169.XXX.XX8
USERAGENT : Mozilla/5.0 (compatible; MSIE 10.0;
==========

Outside to outside – Phishing, Smishing





Phishing Panels

Forwarded from HelpDeskFraude (Gefixt)

PANEL VERHUUR/VERKOOP

Kwaliteit op 1.

Langer termijn werker 👍

🇳🇱 *NL - 2022 Reliable PANEL -*
€150 per week.
Bestanden: €350

🇧🇪 *BE - 2022* Reliable *PANEL -*
€150 per week.
Bestanden: €350

🇩🇪 DE - 2022 uAdmin PANEL-
Customized: met anti-bot €150 per week.
Bestanden: €350

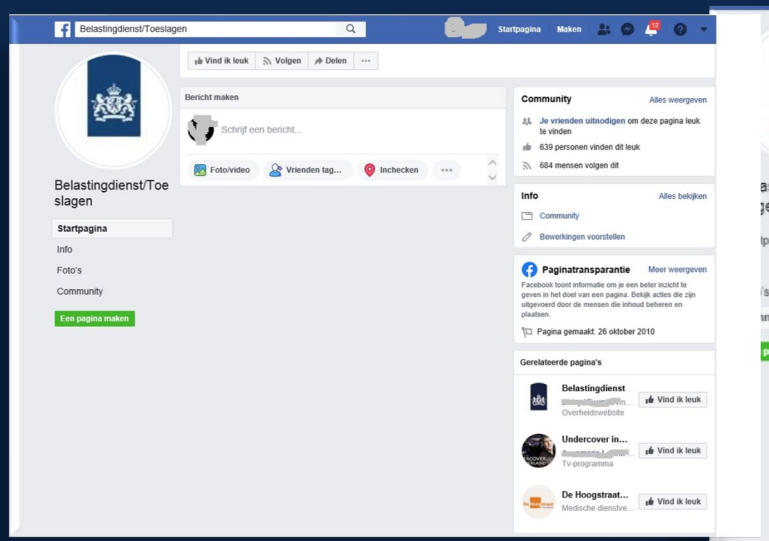
🇦🇺 AUS - 2022 uAdmin PANEL -
Customized up-to-date €150 per week.
Bestanden: €400

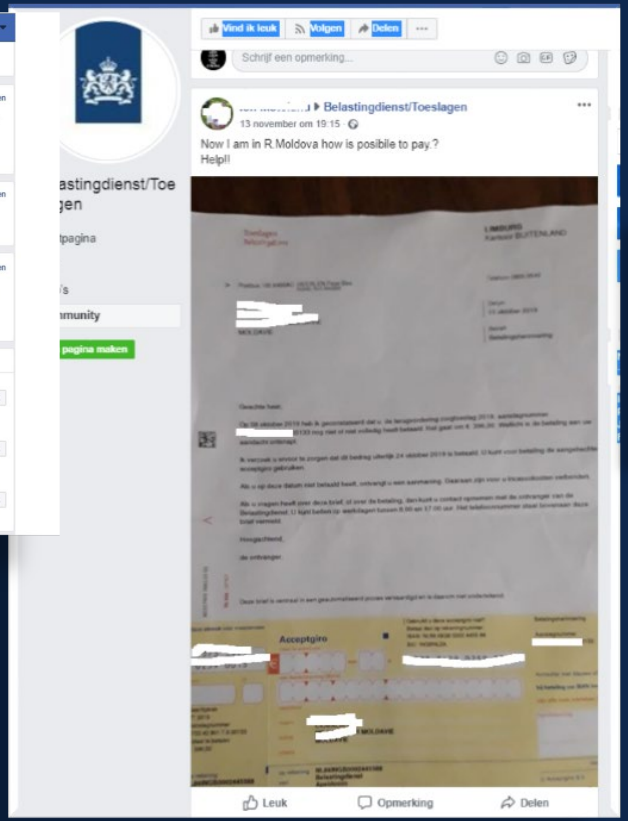
Per bank alle tokens en functies.
Elke panel source is clean (vps gaat niet offline)
Bestanden kan in overleg worden gekocht.

💰 BTC / CRYPTO VOUCHER ONLY.

Share experience. Build resilience.

Outside to outside: Fake social media pages





Share experience. Build resilience.

Partnerships

- National Response Network
  - Goal: The National Response Network (NRN) is a collaborative effort with the goal of strengthening the joint response to cybersecurity incidents.
- J-SOC, operational cooperation between SOCs within the Dutch National Government
- o-IRT-o, public-private partnership between SOC/CERT within the Netherlands
- NCSC liaison consultation, PPS at tactical level
- ISACs, including the RijksISAC.
- Splunk ISAC with Norway, Denmark, Netherlands and the UK
- Dutch antiDDoS Coalition

Ask me anything

Share experience. Build resilience.

No pincode, no SSN, no password (you know it already, it’s welcome01)

SECCON-NL 2022

Share experience. Build resilience

Time	Main stage (Zilversmederij 300 seats)	Breakout room 1 (Penningzaal 80 seats)	Breakout room 2 (Depot 80 seats)	Breakout room 3 (Stempelkamer 60 seats)	Breakout room 4 (Schatkamer 30 seats)
09:00 - 10:00	Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)				
10:00 - 10:15	Break - switch to main stream				
10:15 - 10:45	Threat Intell Threat Intel update from Talos - Martin Lee (Talos Threat intelligence organization)	Threat Intel No More Leaks Project - Felix Nijpels (Dutch Police)	Post Quantum Security The Impact of Quantum on security - a general outlook - Sam Samuel (Cisco)	Threat Intel Threat managemen at the Dutch Railway - Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)	AI Get ready for the AI attack bot - Richard de Vries (Tata Steel)
10:45 - 11:00	Break - switch to main stream				
11:00 - 11:30	Detection and Response Day in life at the Dutch Tax Office SOC - Karl Lovink (Belastingdienst)	SOAR Stay Ahead of the Game: Automate your Threat Hunting Workflows - Christopher van der Made (Cisco)	Post Quantum Security Quantum hurdles: an optimistic view of post-quantum security - Sander Dorigo (Fox Crypto)	Detection and Response What Cyber can learn from Biology? - Koen Hokke (KPN)	Detection and Response / AI Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use - Julik Keijer (Northwave)
11:30 - 11:45	Break - switch to main stream				
11:45 - 12:15	Detection and Response Compliancy vs security. Pentesting is dead - Edwin van Andel (ZeroCopter)	Detection and Response Incident Response without compromise. How to prepare for the worst day of your career with dice! - Wouter Hindriks (Avit)	DevSecOps/ Detection and Response Threat Modelling: it's not just for developers - Timothy Wadhwa-Brown (Cisco)	DevSecOps Changed responsibilities in modern software development environments - Martin Knobloch (Microfocus)	 How to break a data center? Fred Streefland (Secior)
12:15 - 13:00	LUNCH				
13:00 - 13:45	Panel Discussion with Liesbeth Holterman (host CVNL) Koen Sandbrink (NCSC), Jochem Smit (Northwave), Oscar Koeroo (Min Ezk), Jan Heijdra (Cisco)				
13:45 - 14:00	Break - switch to main stream				
14:00 - 14:30	Threat intel / Detection and Response CERT in Ukraine exeperience sharing by Andrii Bezverkhyi (SOCPrime)	Threat Intel This is why you will fail: Most successful attack scenarios and their defenses - Tijme Gommers (Northwave)	Detection and Response Risk-based Auth & ZTA - Frank Michaud (Cisco)	DevSecOps Creating clarity and unity in security standards and guidelines - OpenCRE.org - Rob van der Veer (Software Improvement Group)	 (Placeholder) WICCA Breakout (with Wendy joining)
14:30 - 14:45	Break - switch to main stream				
14:45 - 15:15	Detection and Response Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences - David Warburton (F5)	Detection and Response Security Maturity: from XDR to SIEM - Gilles van Heijst (Orange Cyber Defense)	Detection and Response Improving Business Security by implementing Security.txt - Julius Offers (Digital Trust Center)	Threat Intel Tackling the challenge of translating threat intelligence into actual action - Raymond Bierens (Connect2Trust)	Detection and Response / AI Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy.- Christian van der Woude (Dcypher)
15:15 - 16:00	Closing Keynote - Wendy Nather				