



Share experience. Build resilience

Welcome to SECCON NL 2022

digital trust
center.



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

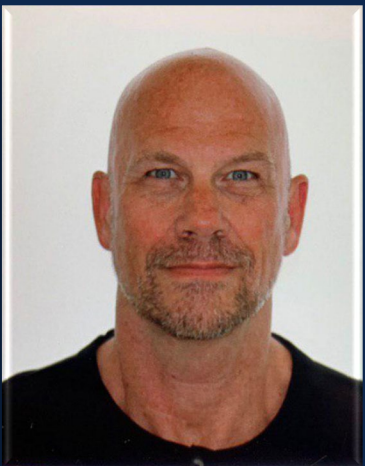


Agenda

- 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





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

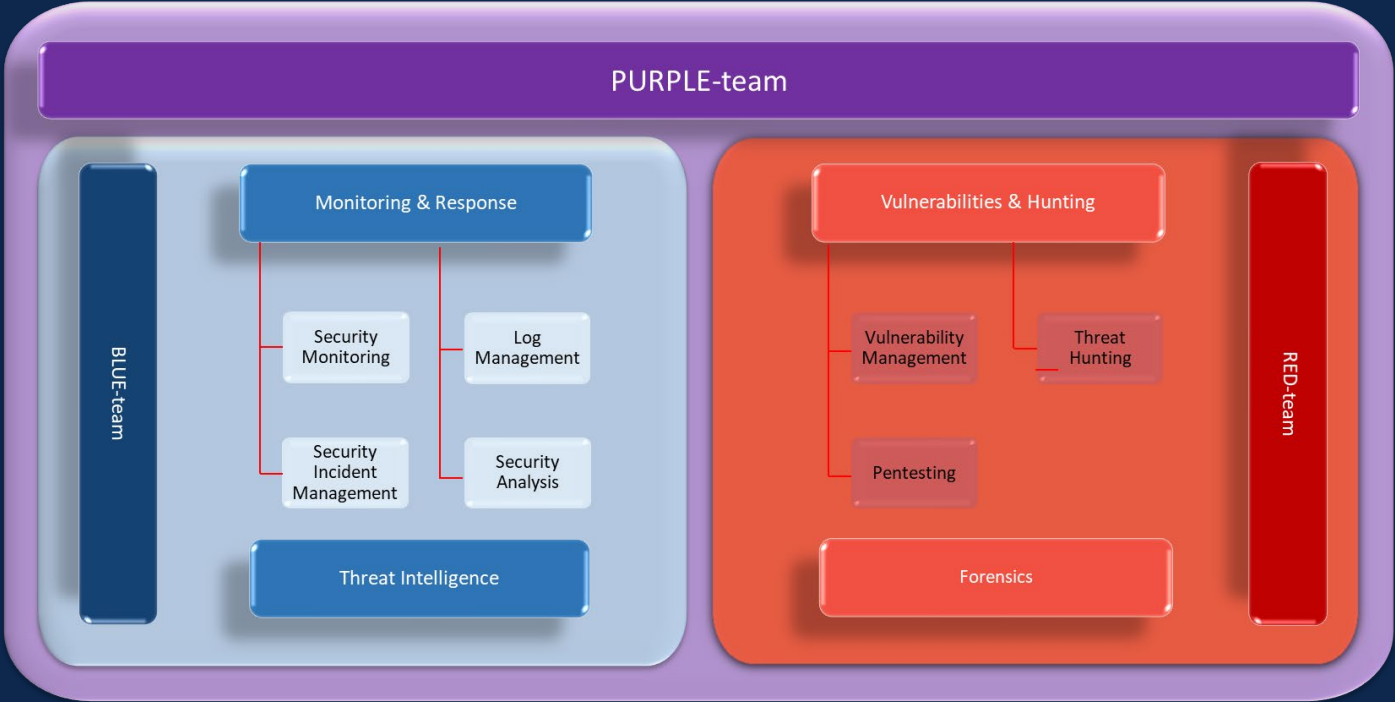


Definition Security Operations Center

“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

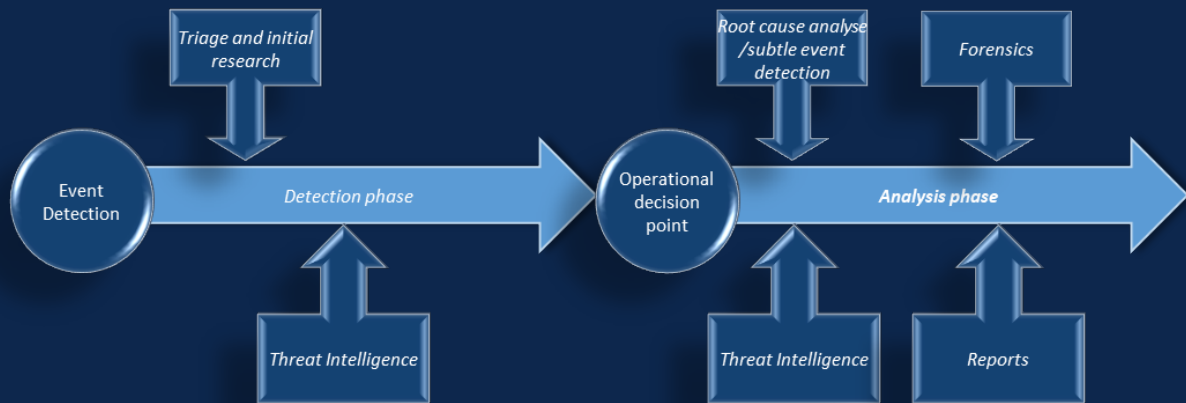
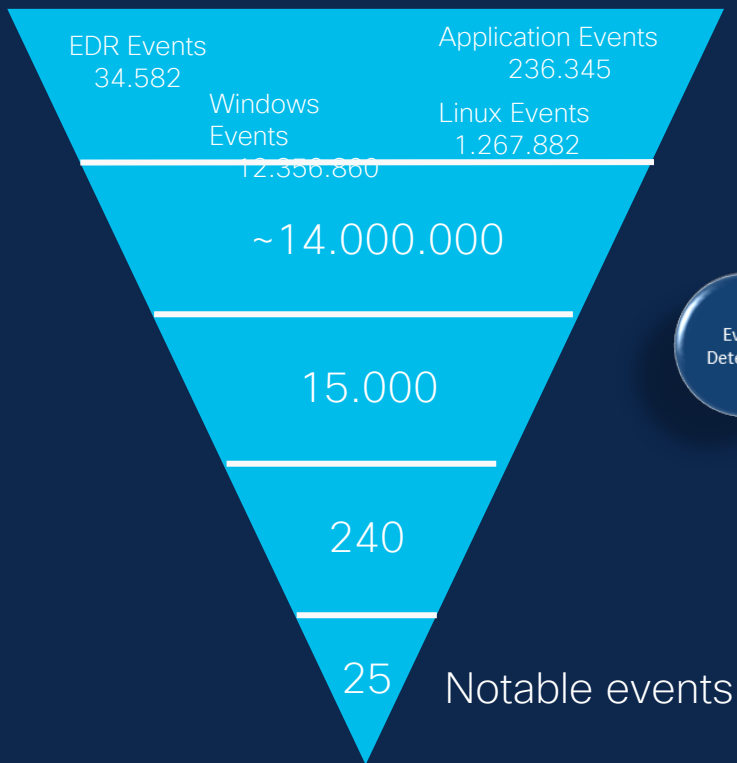
Examples not covered by security monitoring:

- 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



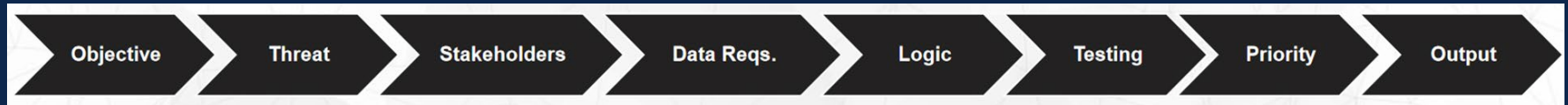


Monitoring & Response – Use-cases

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.....

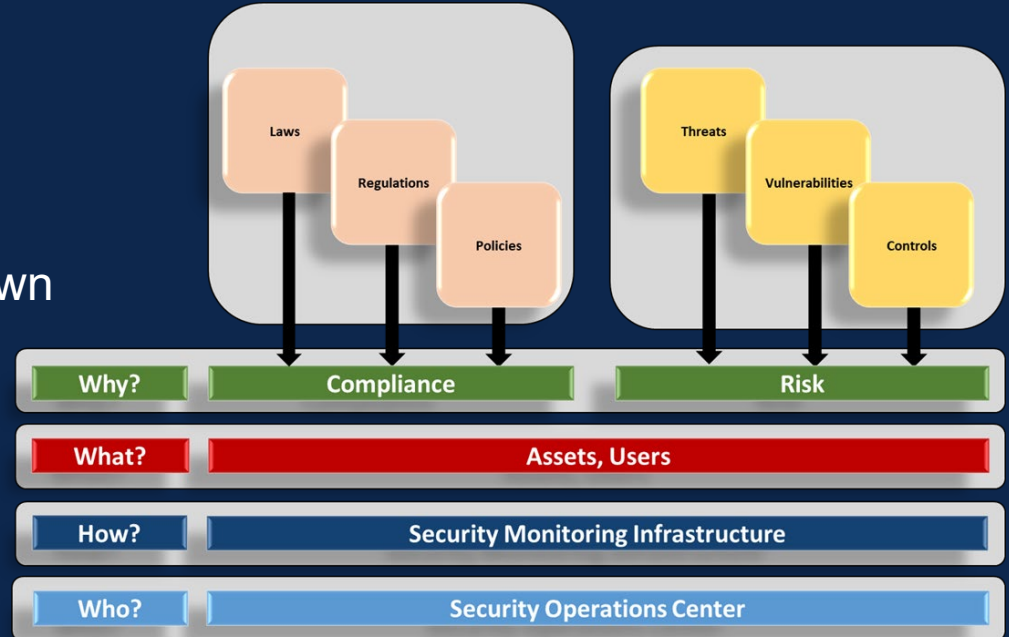




MAGMA Use-case Framework

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



Share experience. Build resilience.



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

Incident Review

Urgency

CRITICAL	0
HIGH	2
MEDIUM	27
LOW	0
INFO	0

Status

Closed x

Owner

[Redacted]

Security Domain

Select...

Tag

Type...

Correlation Search

Sequenced Event

- ACC-WIN-0006 Unauthorized account ... x
- END-DWB-0008 Execution of suspicio... x

Search

Time

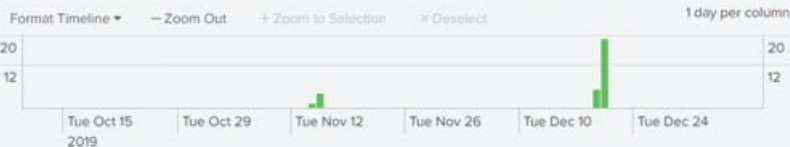
Last 90 days

Associations

Submit

✓ 29 events (10/10/19 12:00:00.000 AM to 1/8/20 2:59:52.000 PM)

Job ▾ || Smart Mode ▾



Edit Selected | Edit All 29 Matching Events | Add Selected to Investigation

< prev 1 2 next >

i		Time	Security Domain	Title		Urgency	Status	Owner	Actions
>	<input type="checkbox"/>	12/19/19 7:02:07.000 PM	Endpoint	END-DWB-0008 Execution of suspicious PowerShell commands/scripts (user [Redacted])	[Redacted]	⚠ Medium	Closed	[Redacted]	▾
>	<input type="checkbox"/>	12/19/19 3:31:15.000 PM	Endpoint	END-DWB-0008 Execution of suspicious PowerShell commands/scripts (user [Redacted])	[Redacted]	⚠ Medium	Closed	[Redacted]	▾
>	<input type="checkbox"/>	12/19/19 3:29:26.000 PM	Endpoint	END-DWB-0008 Execution of suspicious PowerShell commands/scripts (user [Redacted])	[Redacted]	⚠ Medium	Closed	[Redacted]	▾
>	<input type="checkbox"/>	12/19/19 3:15:39.000 PM	Endpoint	END-DWB-0008 Execution of suspicious PowerShell commands/scripts (user [Redacted])	[Redacted]	⚠ Medium	Closed	[Redacted]	▾
>	<input type="checkbox"/>	11/15/19 11:12:09.000 AM	Access	ACC-WIN-0006 Unauthorized account creation	[Redacted]	⚠ Medium	Closed	[Redacted]	▾
>	<input type="checkbox"/>	11/15/19 9:40:17.000 AM	Endpoint	END-DWB-0008 Execution of suspicious PowerShell commands/scripts (user [Redacted])	[Redacted]	⚠ High	Closed	[Redacted]	▾



Outside to inside: DDoS detection/mitigation

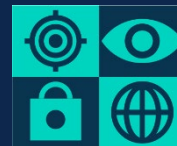
Rulebase & Screening	Rulebase	Screening	Amplification Type	Src IP session Limits	Dest IP session Limits
331609 IPs	72684 Unieke IPs	240 Unieke IP's	317831 UDP packets	0 Hits Src IP session Limits	47 Hits Dest IP session Limits
4 % IP's from NL	8 % IP's from NL	0 % IP's from NL	UDP/DNS (79%) #1 Attack UDP	- #1 IP	101.178.237.246 #1 IP
96 % IP's from other Country's	92 % IP's from other Country's	0 % IP's from other Country's	TCP/53169 (2%) #1 Attack NON UDP		
Russia(25%) #1 Non NL Country	United States(25%) #1 Non NL Country	Russia #1 Non NL Country	Russia #1 Non NL Country	- #1 Non NL Country	Australia #1 Non NL Country



Outside to Inside – DDoS exercises

Twice a year

- Volume-based DDoS test
- Applicative DDoS test



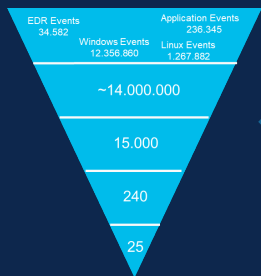
Anti-DDoS Coalition
No More DDoS



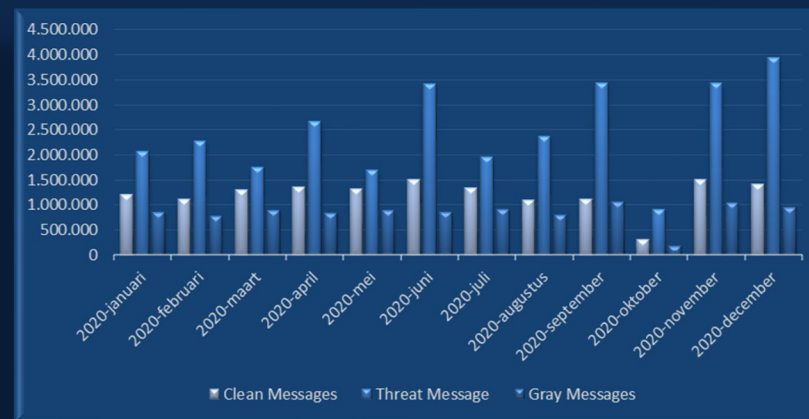


Outside to Inside – External Mail

Totals 2020



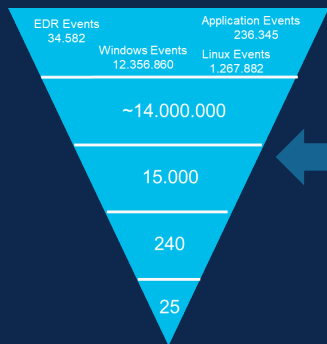
Threat Messages	29.974.532	54,75%
Gray Messages	10.105.605	18,46%
Clean Messages	14.663.156	26,79%
Total	54.743.293	100.00%



Share experience. Build resilience.

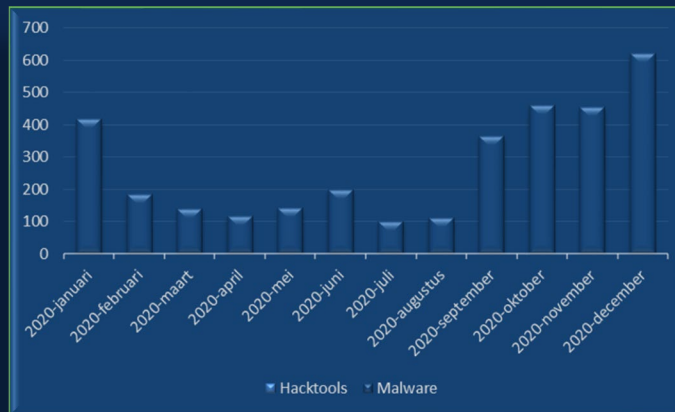


Inside to outside/inside – Malware workstations



Totals 2020

- Malware 5799
- Hacktools 29





Outside to outside – Phishing, Smishing

e-mail received

2017

2020

2021

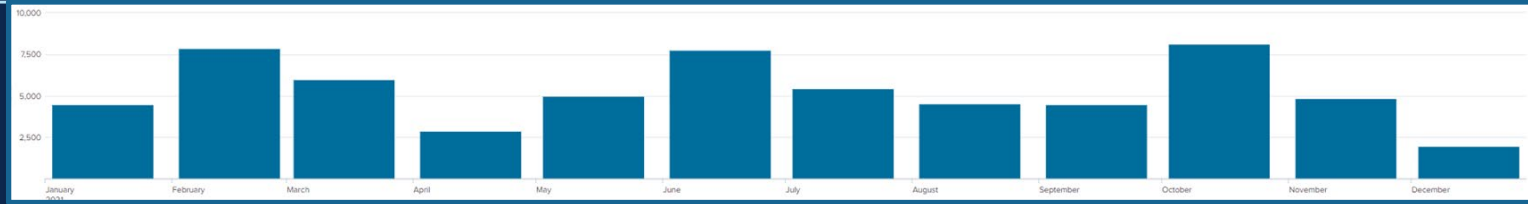
Valse-email@belastingdienst.nl

7.791

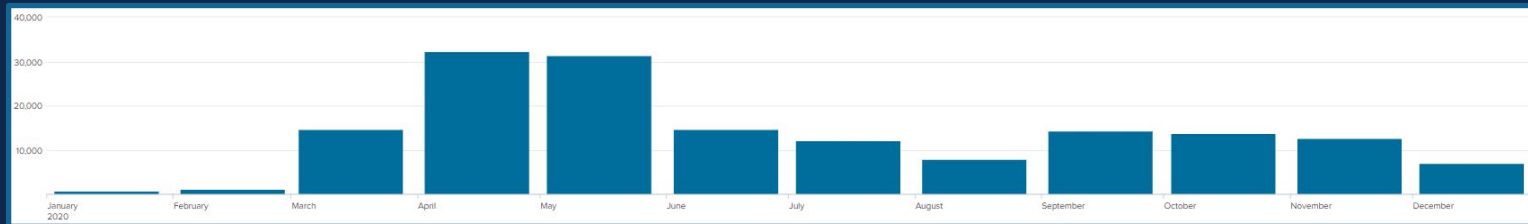
162.624

63.200

2021



2020





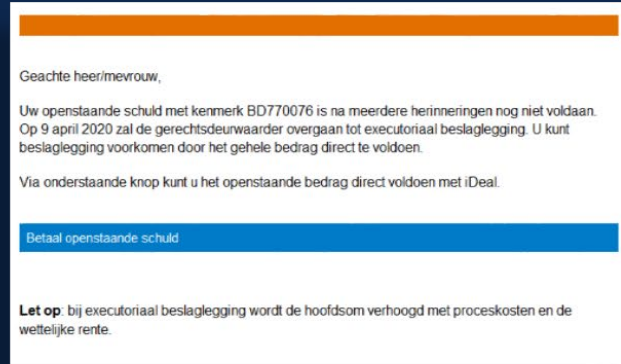
Outside to outside – Phishing, Smishing



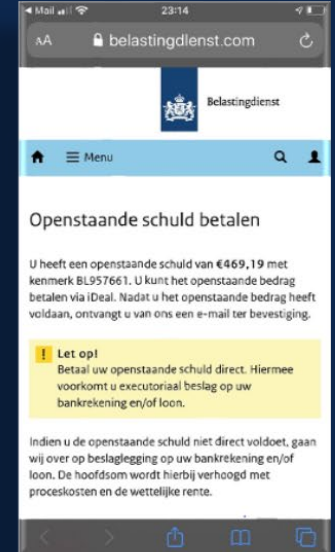
Link naar betaalverzoek



Link shortener



E-mail phishing



Fake websites



Outside to outside – Phishing, Smishing

Bank accounts blocked [total]

695

Mobile numbers blocked [total]

1,466

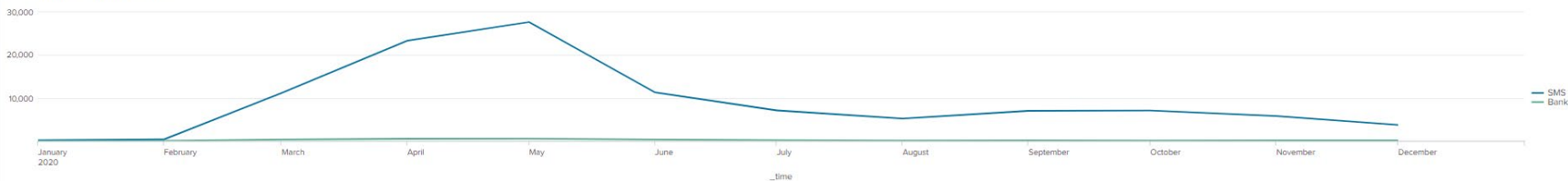
SMS screenshots

109,863

Bank screenshots

2,235

OCR actions over time by type



Emails containing Smishing keywords in the subject





Outside to outside – Phishing, Smishing

Ik heb helaas dit bedrag overgemaakt!

Mvg M. [redacted]
Tel:06-20001000

Verstuurd vanaf mijn iPhone

Begin doorgestuurd bericht:

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



Onderwerp: Fwd: Belastingaangifte 2014
Van: [redacted]@rt.nl>
Datum: 4-8-2015 21:40
Aan: [redacted]administration@belastingdienst.nl>

graag meteen betalen

----- 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:belastingaangifte@belastingdienst.nl

GEBOEKT

Moet dit worden
ingebaat?

BETAALD PER BANK 05 AUG 2015

BETAALD PER BANK 05 AUG 2015

Geachte heer/mevrouw,

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



Outside to outside – Phishing, Smishing

DigiD Je eigen inlogcode voor de hele overheid

Belastingbetaling (1/3)

1 Persoonsgegevens

Verplichte velden zijn gemarkeerd

Burgerservicenummer *

Geboortedatum * onbekend

Postcode *

Uw e-mailadres *

Volgende

Geen antwoord op uw vraag?
↳ [Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] of
↳ [Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] met de DigiD helpdesk.

DigiD Je eigen inlogcode voor de hele overheid

Belastingbetaling (2/3)

2 Betaling

Verplichte velden zijn gemarkeerd

Bedrag **46,00 Euro**

Kies uw bank *

Volgende

Geen antwoord op uw vraag?
↳ [Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] of
↳ [Bekijk de overige veelgestelde vragen](#) [opent in een nieuw venster] met de DigiD helpdesk.

Rabobank **Betalen met iDEAL**

Ondertekenen > Betalen > Bevestigen > Terug naar webwinkel

Begunstigde **Stichting Mollie Payments inzake Bitonic**

Omschrijving **BTC 0,09519700 aan 19Hg...**

Bedrag **€46,00**

Bankpas Rekeningnummer [IBAN](#)

Pasnummer



Ga verder **Annuleren** **Help**

Ga alleen verder als de adresregel begint met [https://betalen.rabobank.nl/...](https://betalen.rabobank.nl/)
↳ [Hoe controleert u de veiligheid van uw verbinding?](#)
↳ [Lees meer over veiligheid](#)



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

Static information & Settings

Dynamic data & Live chat

Visitor Waiting

Operations

MijnOverheid

Login

Type bankrekening

Persoonlijk Zakelijk

U ontvangt:
Totaal € 1924,49

jouw bank
Kies je bank

NAAR JOUW BANK

Aangeboden door **D** onze **reclamemaatschappij** van MediaMedics BV

Over deze site Gegevensverwerking Service Partners

> Wat is MijnOverheid > Veiligheid > Mededelingen > Aangesloten organisaties

Phishing Panels

Forwarded from HelpDeskFraude (Gefixt)
PANEL VERHUUR/VERKOOP

Kwaliteit op 1.

Langer termijn werker 👍

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

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

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

🇺🇸 - 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.



Outside to outside: Fake social media pages

This screenshot shows the profile page of 'Belastingdienst/Toeslagen' on Facebook. The profile picture is the Dutch coat of arms. The page has a cover photo and a bio. The 'Community' section shows 639 likes and 684 followers. The 'Info' section indicates the page was created on October 26, 2010. The 'Pagina transparantie' section provides information about the page's activity. The 'Gereleerde pagina's' section lists related pages like 'Belastingdienst Overheidswebsites', 'Undercover in...', and 'De Hoogstraat...'. A green button labeled 'Een pagina maken' is visible at the bottom.

This screenshot shows a post from the 'Belastingdienst/Toeslagen' page. The post text reads: 'Now I am in R Moldova how is possible to pay? Help!!'. The post includes a photograph of a document, which appears to be a tax form or receipt, with some redacted areas. The post has a 'Vind ik leuk' button and a 'Volgen' button. The page name 'Belastingdienst/Toeslagen' is visible at the top of the post.

This screenshot shows a Facebook post warning about a fake page. The text reads: 'Deze Pagina is niet van de Belastingdienst, dus misleidend!'. The post includes a 'Leuk' button, an 'Opmerking' button, and a 'Delen' button. The page name 'Belastingdienst/Toeslagen' is visible at the top of the post.



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 SOC's 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

09:00 - 10:00

Opening Keynote Sadie Creese (Professor Cybersecurity @ Oxford University)

Main stage (Zilvermederij 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)

10:00 - 10:15

Break - switch to main stream

Threat Intell

Threat Intel

Post Quantum Security

Threat Intel

AI

10:15 - 10:45

Threat Intel update from Talos - Martin Lee (Talos Threat intelligence organization)

No More Leaks Project - Felix Nijpels (Dutch Police)

The Impact of Quantum on security - a general outlook - Sam Samuel (Cisco)

Threat management at the Dutch Railway - Dimitri van Zantvliet Rozemeijer (Chief Cyber Dutch Railway)

Get ready for the AI attack bot - Richard de Vries (Tata Steel)

10:45 - 11:00

Break - switch to main stream

Detection and Response

SOAR

Post Quantum Security

Detection and Response

Detection and Response / AI

11:00 - 11:30

Day in life at the Dutch Tax Office SOC - Karl Lovink (Belastingdienst)

Stay Ahead of the Game: Automate your Threat Hunting Workflows - Christopher van der Made (Cisco)

Quantum hurdles: an optimistic view of post-quantum security - Sander Dorigo (Fox Crypto)

What Cyber can learn from Biology? - Koen Hokke (KPN)

Unsupervised Anomaly-Based Network Intrusion Detection Using Auto Encoders for Practical Use - Julik Keijer (Northwave)

11:30 - 11:45

Break - switch to main stream

Detection and Response

Detection and Response

DevSecOps/ Detection and Response

DevSecOps

11:45 - 12:15

Compliancy vs security. Pentesting is dead - Edwin van Anel (ZeroCopter)

Incident Response without compromise. How to prepare for the worst day of your career with dice! - Wouter Hindriks (Avit)

Threat Modelling: it's not just for developers - Timothy Wadhwa-Brown (Cisco)

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

Threat intel / Detection and Response

Threat Intel

Detection and Response

DevSecOps

14:00 - 14:30

CERT in Ukraine experience sharing by Andrii Bezverkhyi (SOCPrime)

This is why you will fail: Most successful attack scenarios and their defenses - Tijme Gommers (Northwave)

Risk-based Auth & ZTA - Frank Michaud (Cisco)

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

Detection and Response

Detection and Response

Detection and Response

Threat Intel

Detection and Response / AI

14:45 - 15:15

Advanced Attacker Automation: Botnet capabilities and techniques used to evade your defences - David Warburton (F5)

Security Maturity: from XDR to SIEM - Gilles van Heijst (Orange Cyber Defense)

Improving Business Security by implementing Security.txt - Julius Offers (Digital Trust Center)

Tackling the challenge of translating threat intelligence into actual action - Raymond Bierens (Connect2Trust)

Fostering emerging technologies in cybersecurity, to reinforce our strategic autonomy - Christian van der Woude (Dcypher)

15:15 - 16:00

Closing Keynote - Wendy Nather