Secutec
Cyber security intelligence

Credential Leaks

The biggest source for ransomware organizations

Thomas Jannes
SOC Manager, Secutec

Secutec
Cyber security intelligence

Geert Baudewijns
CEO & Founder

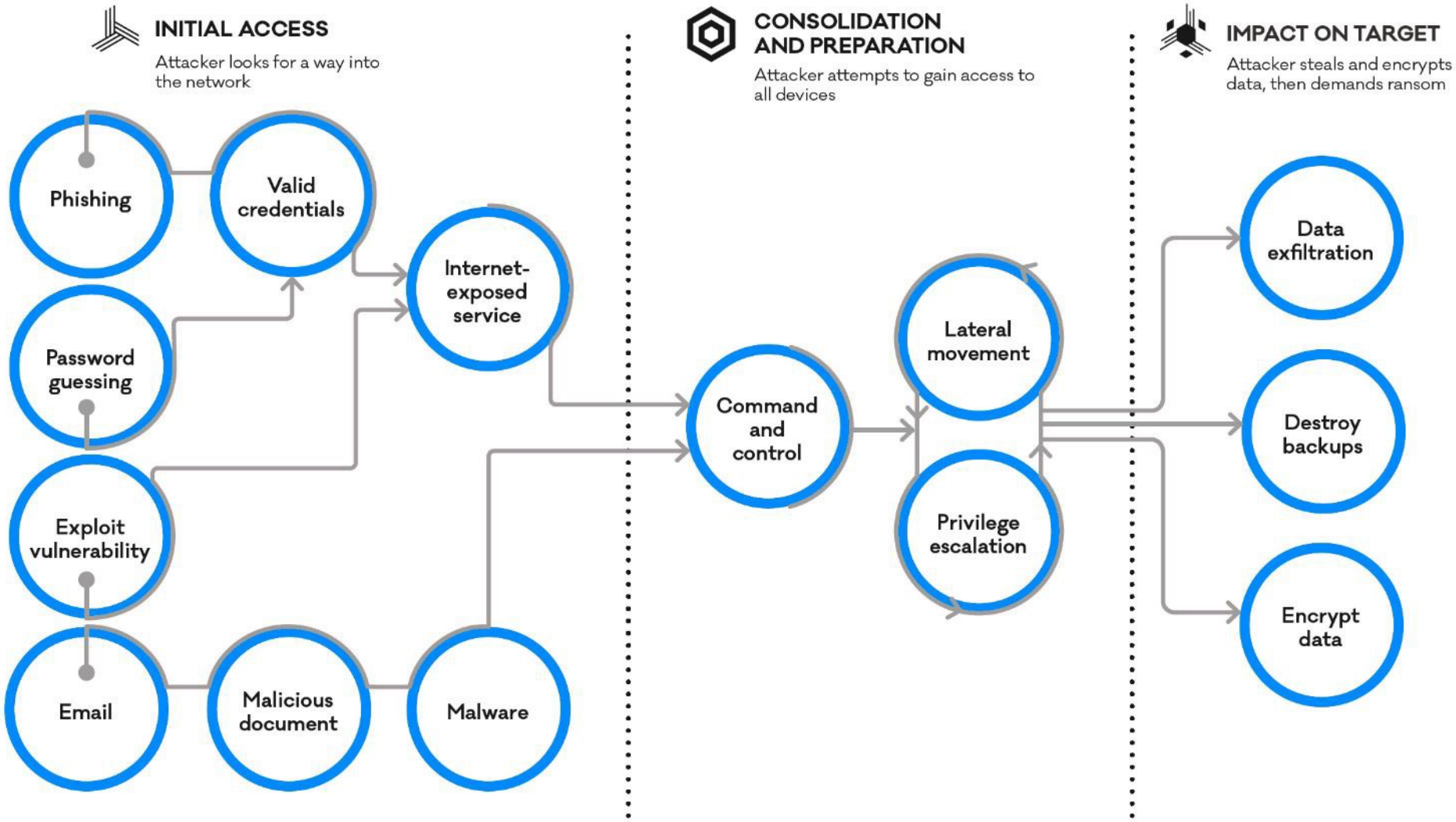
Secutec was founded in 2005 with the vision of bundling global threat knowledge into one technology.

We work for authorities and organizations worldwide and have experience from over 300 negotiations with hacker organizations.

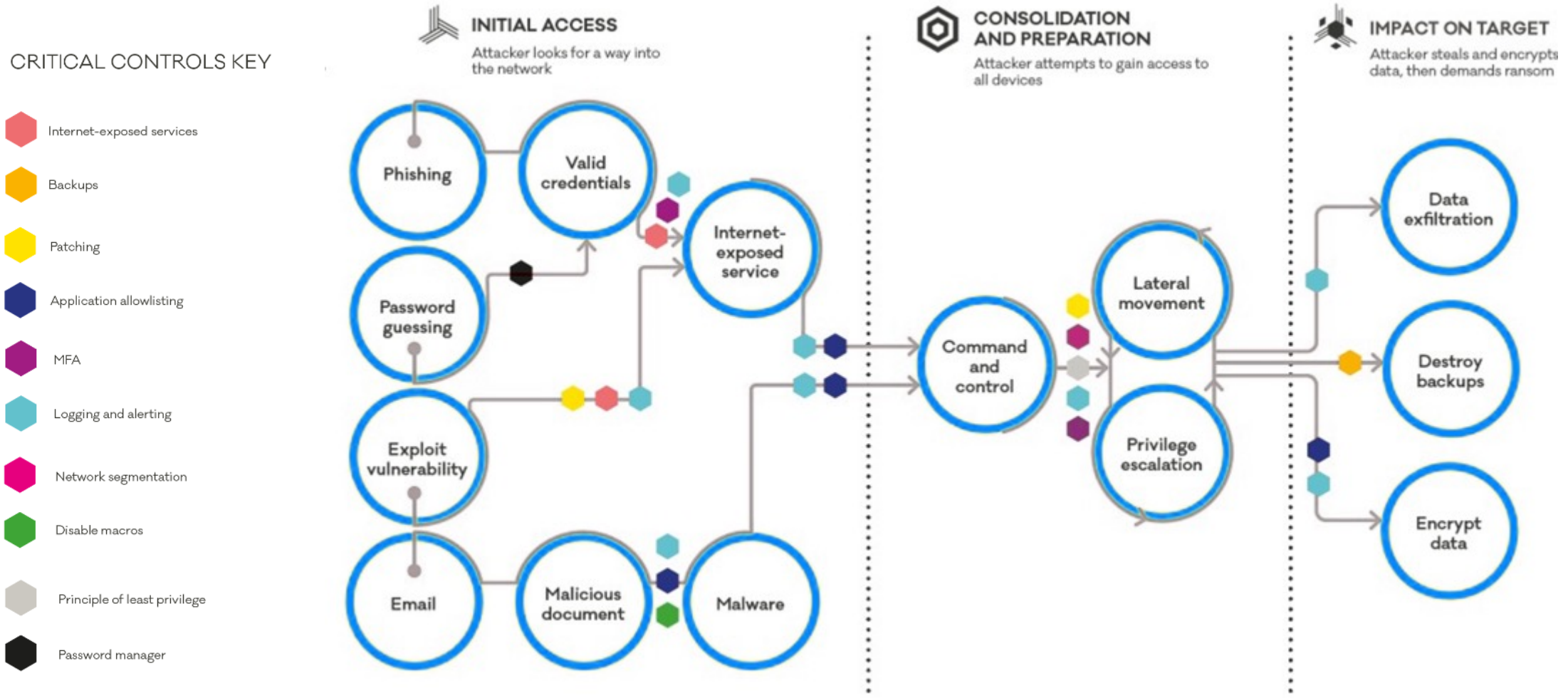
- ✓ Leading European cybercrime negotiator
- ✓ Security Board of the Belgian Government
- ✓ Organizations like Europol, Secret Services, various CERTs
- ✓ Cyber-SOC / 40 Cyber Data Analysts

Lifecycle of a Ransomware Incident

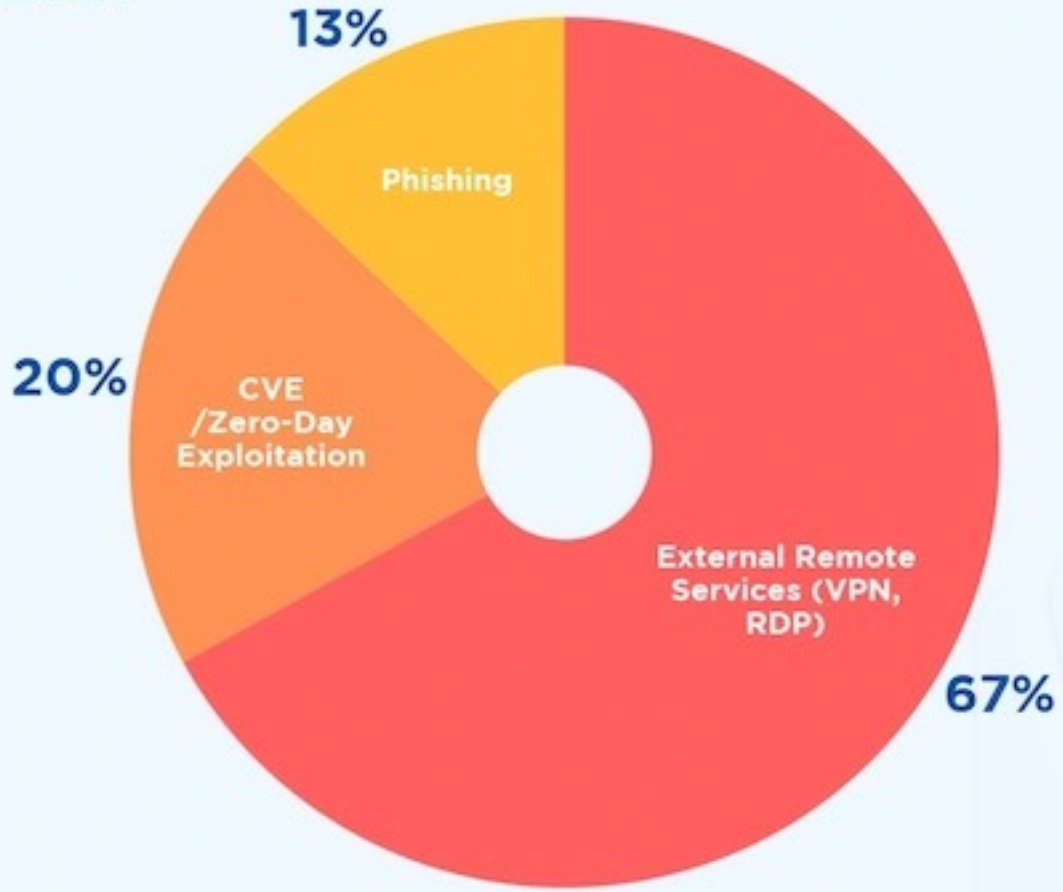
certnz



Lifecycle of a Ransomware Incident



Top Initial Access Methods for Launching Ransomware in 2021



Secutec
Cyber security intelligence

Secutec
Cyber security intelligence

“Darknet & Co.”

Secutec
Cyber security intelligence

4%

Clear Web

-internet known to us

-visible to all users

-accessible via Google & Co.

96%

Deep Web

-restricted or non-indexed sites

-databases, websites & services from Government, Organisations or Universities

Darknet

-not findable in the normal way

-encrypted communication

-Creators and Visitors want to remain anonymous

-Illegal Content, Political Protest, Private Communications

Tor Browser File Edit View History Bookmarks Tools Window Help 58% Fri 10:57 AM

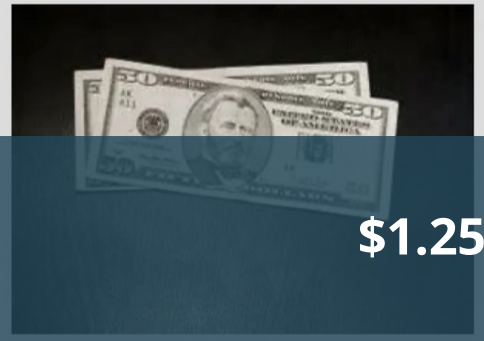
About Tor | Hidden Wiki | Tor .onion url... | Problem loading page | Counterfeit USD - High qua... | Disconnect Search: Search...

Search

Counterfeit USD

Login Register FAQs Products

50 USD BILLS



Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessery security features to be spent at most retailers. Free shipping in the US.

$1.250 fake USD for $600 – 50% Discount

Product	Price	Quantity
25 x 50 USD BILLS	600 USD = 1.652 ฿	1 X Buy now
100 x 50 USD BILLS	2000 USD = 5.506 ฿	1 X Buy now

Counterfeit USD

Secutec
Cyber security intelligence

Tor Browser File Edit View History Bookmarks Tools Window Help 45% Fri 11:35 AM

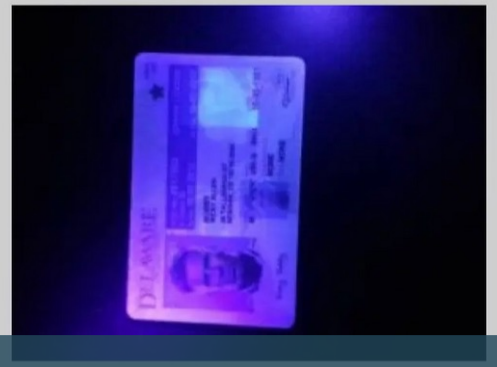
The-Hidden-Wiki.com - Hidden... | Disconnect Search: Search... | US Fake ID Store - Drivers ...

Search

USfakeIDs

Products FAQs Register Login

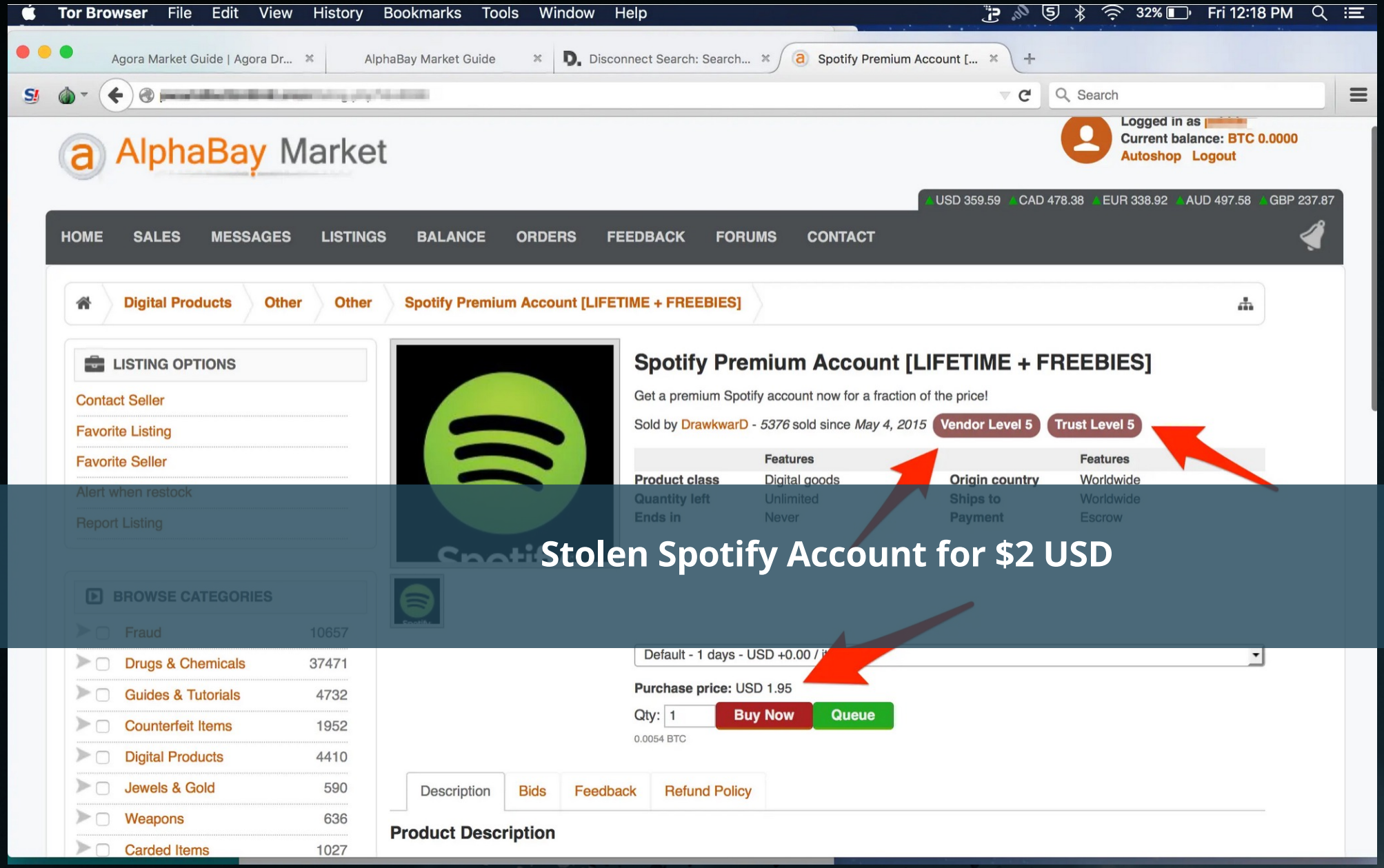
US Fake Drivers Licenses - Scannable, Holograms, UV etc



Our fake drivers licenses are all scannable, contain original hologram and UV, microprint, laser engraving etc.
Shipping from the US within 48 hours!
We only sell the best quality, you wont find any better on the net.

fake Drivers License for $200 USD

Product	Price	Quantity
Delaware	200 USD = 0.551 ฿	1 X Buy now
Illinois	200 USD = 0.551 ฿	1 X Buy now
South Carolina	200 USD = 0.551 ฿	1 X Buy now
New Jersey	200 USD = 0.551 ฿	1 X Buy now
Colorado	200 USD = 0.551 ฿	1 X Buy now


Tor Browser File Edit View History Bookmarks Tools Window Help
Fri 12:18 PM
Agora Market Guide | Agora Dr...
AlphaBay Market Guide
Disconnect Search: Search...
Spotify Premium Account [...
Search
AlphaBay Market
Logged in as
Current balance: BTC 0.0000
Autoshop Logout
USD 359.59 CAD 478.38 EUR 338.92 AUD 497.58 GBP 237.87
HOME SALES MESSAGES LISTINGS BALANCE ORDERS FEEDBACK FORUMS CONTACT
Digital Products Other Other Spotify Premium Account [LIFETIME + FREEBIES]
LISTING OPTIONS
Contact Seller
Favorite Listing
Favorite Seller
Alert when restock
Report Listing
Spotify Premium Account [LIFETIME + FREEBIES]
Get a premium Spotify account now for a fraction of the price!
Sold by DrawkwarD - 5376 sold since May 4, 2015
Vendor Level 5
Trust Level 5
Features
Product class Digital goods
Quantity left Unlimited
Ends in Never
Features
Origin country Worldwide
Ships to Worldwide
Payment Escrow
Stolen Spotify Account for $2 USD
BROWSE CATEGORIES
Fraud 10657
Drugs & Chemicals 37471
Guides & Tutorials 4732
Counterfeit Items 1952
Digital Products 4410
Jewels & Gold 590
Weapons 636
Carded Items 1027
Default - 1 days - USD +0.00 / i
Purchase price: USD 1.95
Qty: 1
Buy Now
Queue
0.0054 BTC
Description
Bids
Feedback
Refund Policy
Product Description

Tor Browser File Edit View History Bookmarks Tools Window Help 95% Fri 4:47 PM

AlphaBay | Deep Dot Web | Search Results | Alphabay ...

pwoah7foa6au2pul.onion/search.php?frc=2

Search

BROWSE CATEGORIES

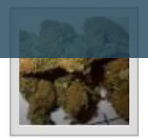
- Fraud 10661
- Drugs & Chemicals 37549
  - Benzos 3009
  - Cannabis & Hashish 11196
  - Dissociatives 836
  - Ecstasy 5684
  - Opioids 2929
  - Prescription 2541
  - Steroids 1050
  - Stimulants 6172
  - Tobacco 158
  - Weight Loss 117
  - Other 652
  - Paraphernalia 270
  - Psychedelics 2935
- Guides & Tutorials 4732
- Counterfeit Items 1952
- Digital Products 4410
- Jewels & Gold 590
- Weapons 637
- Carded Items 1027
- Services 2336
- Other Listings 864

Search Results [Save Search]

[FE 100%] [Sticky] 1g Best MDMA Crystals 84%+ Pure!
Item # 29299 - Ecstasy / MDMA - DrugsFromGermany (1332)
Views: 16472 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 20.43 (0.0568 BTC)

[FE 100%] [Sticky] !5g Amphetamine Paste 100%Speed 74%Pure A++
Item # 16885 - Stimulants / Speed - DrugsFromGermany (1332)
Views: 15010 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 31.83 (0.0886 BTC)

[MS] [Sticky] FB's MED. WEED - PURPLE KUSH (8.5/10) & BLUE DREAM (8.5/10) [7 GRAMS]
Item # 12192 - Cannabis & Hashish / Buds & Flowers - ferrisbueller (385)
Views: 17481 / **Bids:** Fixed price
Quantity left:
Buy price USD 70.00 (0.1947 BTC)

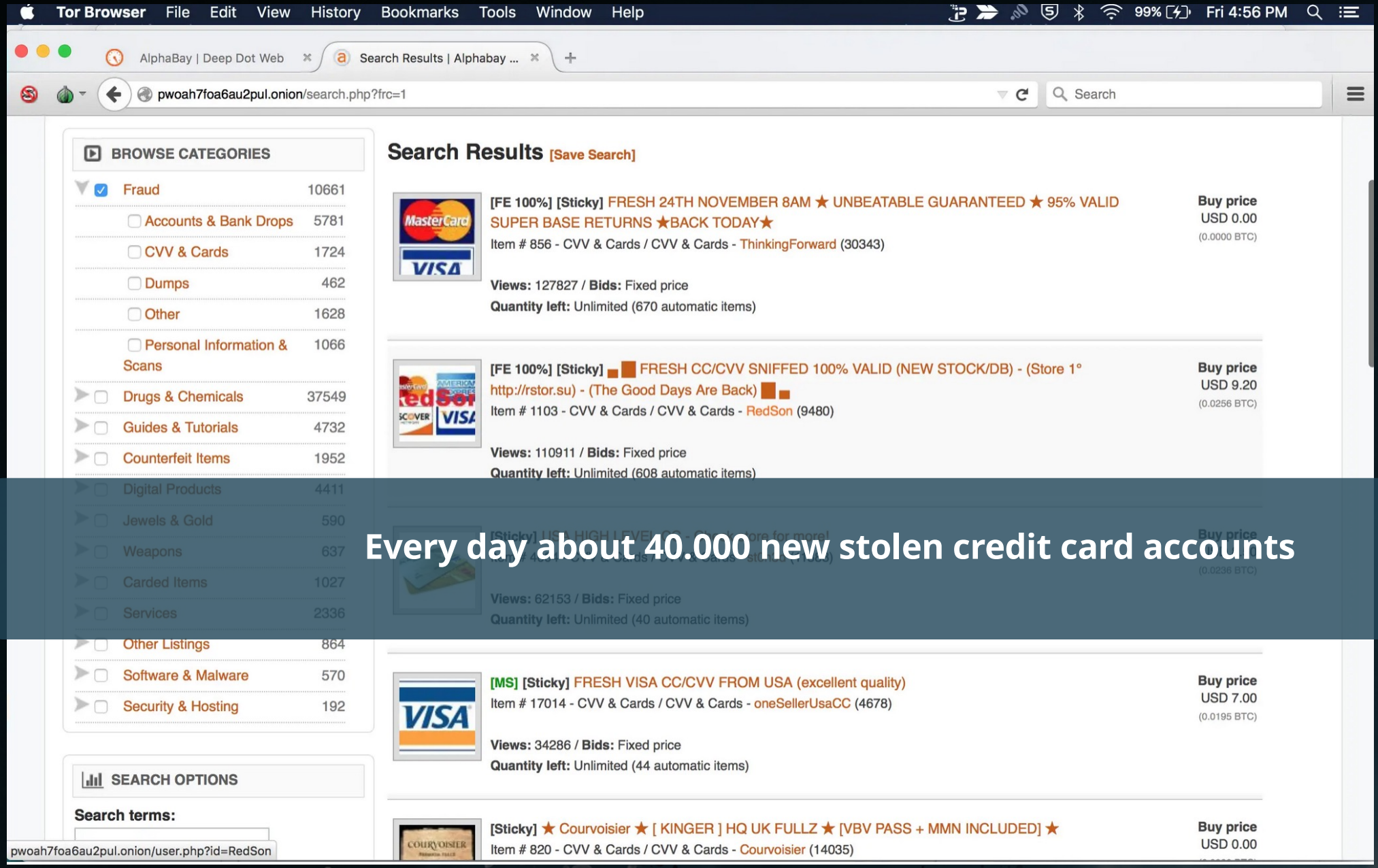


[MS] [FE 50%] [Bulk] [Sticky] 1 oz (28g) Orange Bud AA+ INDOOR GROWN ($150)
Item # 55497 - Cannabis & Hashish / Buds & Flowers - CHEST (203)
Views: 18976 / **Bids:** Fixed price
Quantity left: 20
Buy price USD 150.00 (0.4173 BTC)

[MS] [Sticky] FULL ESCROW 100 x Hello Kitty 220MG Free Shipping
Item # 36850 - Ecstasy / Pills - Etos (768)
Views: 6010 / **Bids:** Fixed price
Quantity left: Unlimited
Buy price USD 234.99 (0.6538 BTC)

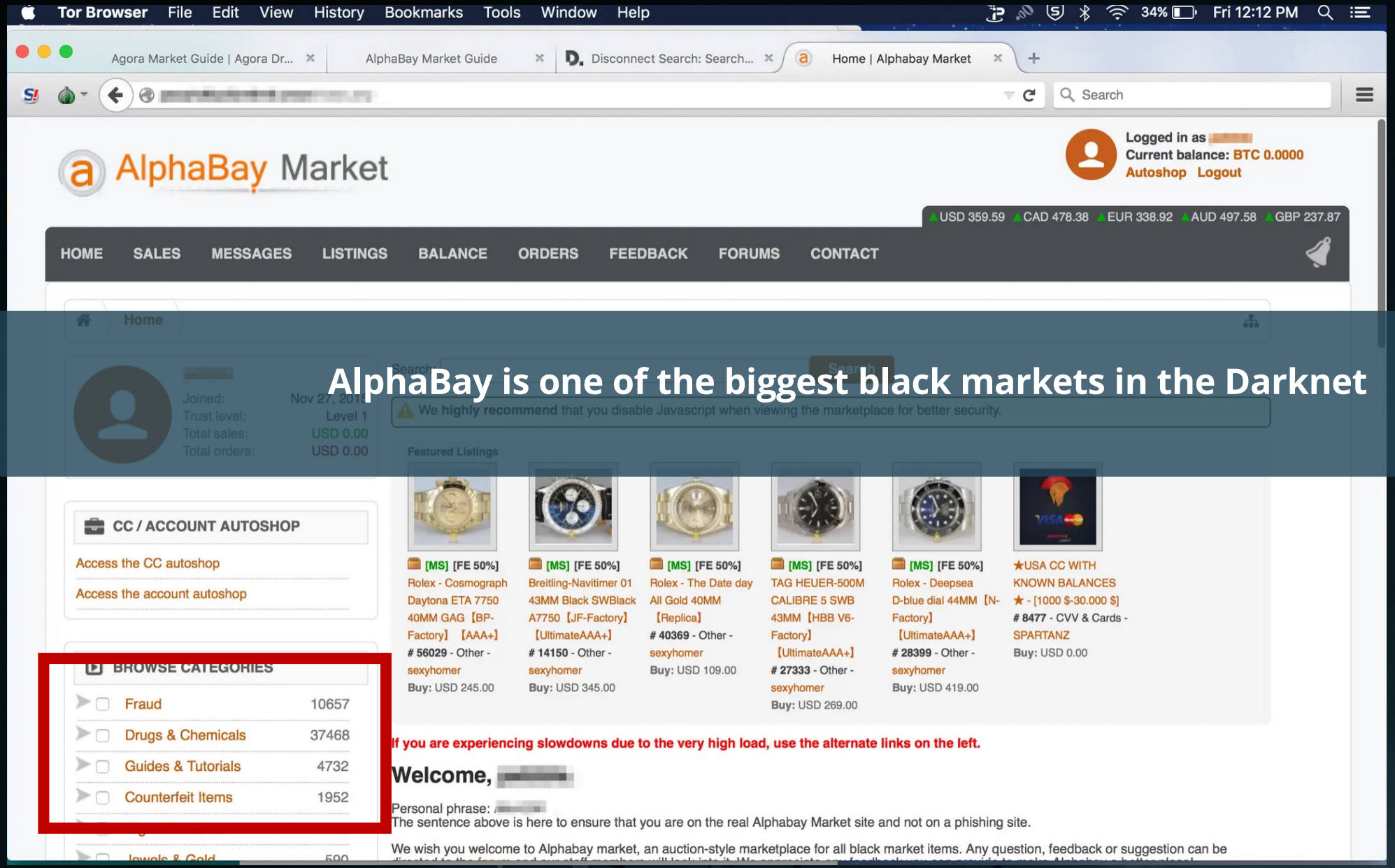
a whole range of illegal drugs

Secutec
Cyber security intelligence



Every day about 40.000 new stolen credit card accounts

Secutec
Cyber security intelligence



AlphaBay is one of the biggest black markets in the Darknet

The Ransomware - Stolen Credentials Connection

Recent incidents, such as the Colonial Pipeline attack, have highlighted the problem of weak or stolen credentials.

(Attackers used a stolen password to access the network via an employee's VPN)

Specialized groups aid ransomware operators by selling initial access (stolen creds).

The Ransomware – Stolen Credentials Connection

The Uber data breach began with a hacker purchasing stolen credentials belonging to an Uber employee from a dark web marketplace.

An initial attempt to connect to Uber's network with these credentials failed because the account was protected with MFA.

The Ransomware – Stolen Credentials Connection

To overcome this security obstacle, the hacker contacted the Uber employee via What's App and, while pretending to be a member of Uber's security, asked the employee to approve the MFA notifications being sent to their phone.

The hacker then sent a flood of MFA notifications to the employee's phone to pressure them into succumbing to this request.

To finally put an end to this notification storm, the Uber employee approved an MFA request, granting the hacker network access, which ultimately led to the data breach.

Example with recent data

Data for fortinet.com

Data records matching this domain.

Corporate Records (26,960) | Infected Employee Records (311) | Infected Consumer Records (38,009)

Raccoon Stealer 2023-04-18 - techsupport@splusmedia.in

Raccoon Stealer

Raccoon is a type of malware (or stealer) affecting Windows users. The Stealer has risen in popularity among cyber criminals as a means to procure credit card information, passwords, and cryptocurrency. The tool was first detected in April 2019. The payload is generally to victims via exploit kits, phishing and compromised software downloads.

Breach ID: 43045

Remediation Overview

2,783,685

Total Number of Records

Malware

Private Data

SpySight	1,459,421	2,783,685	2,783,315	1,324,264	2,783,685	Geographic Location	Phone Numbers	1,083,901
	Emails	Passwords	IP Addresses	Usernames	PII			Financial

Secutec
Cyber security intelligence

Example with recent data

SPLUS MEDIA PVT LTD

Download Reciept

Splus Media Pvt Ltd is one of the largest distribution company with a strong emphasis on quality of service and content. This has enabled us to cater to millions of subscribers who are spread across Tamil Nadu in a very short span of time. With fiber optic backbone across its networks and state-of-the-art distribution set ups, we bring the digital age through Cable transforming the way viewers receive information and entertainment.

S Plus

Splus Media Pvt Ltd is one of the largest distribution company with a strong emphasis on quality of service and content. This has enabled us to cater to millions of subscribers who are spread across Tamil Nadu in a very short span of time. With fiber optic backbone across its networks and state-of-the-art distribution set ups, we bring the digital age through Cable transforming the way viewers receive information and entertainment.

Contact Us

Mail : enquiry@splusmedia.in

Address : No.14, Venugopal Avenue, Spurtank Road, Chetpet, Chennai - 600 031. Tamilnadu

Phone : 8939 536 536

Information on techsupport@splusmedia.in
Result: 10 Records

	title	email	ip_addresses	target_url	infected_machine_id
0	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	accounts.zoho.in	5adc68d2-7c02-4116-b0ad-efd7fe039991
1	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	customersso1.fortinet.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
2	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	login3.id.hp.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
3	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	www.hik-connect.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
4	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	www.airtel.in	5adc68d2-7c02-4116-b0ad-efd7fe039991
5	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	support.vizrt.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
6	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	login.live.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
7	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	id.cisco.com	5adc68d2-7c02-4116-b0ad-efd7fe039991

techsupport@splusmedia.in

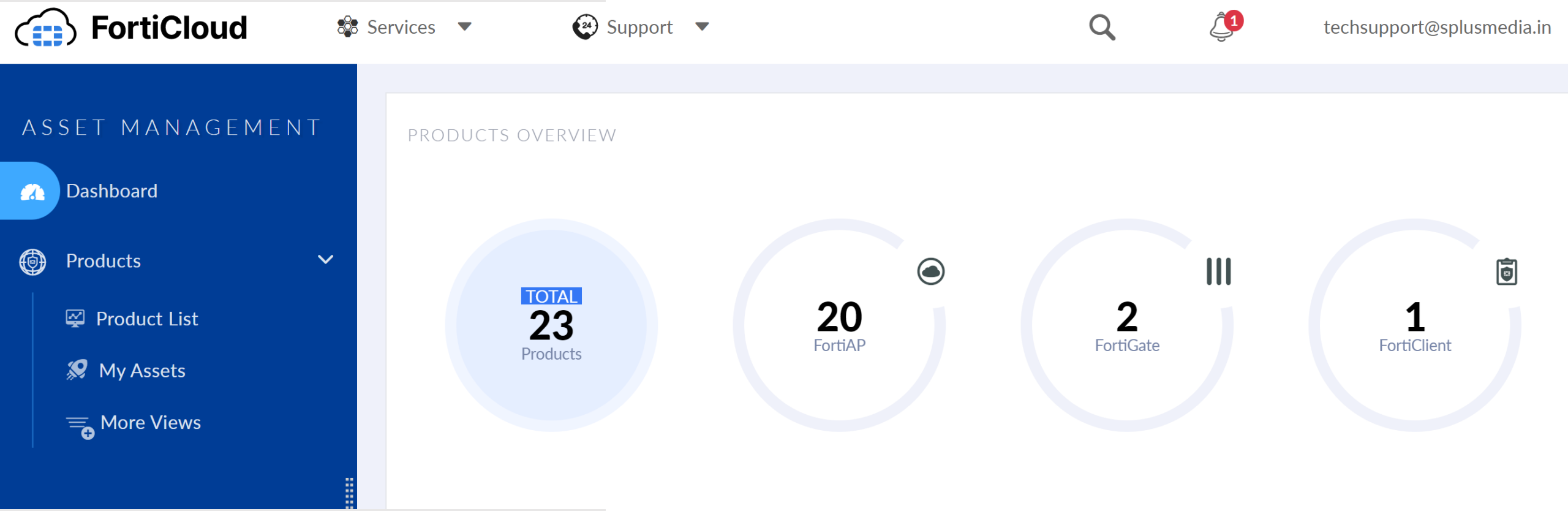
Information on Infected_Machine_ID: 5adc68d2-7c02-4116-b0ad-efd7fe039991
Result: 79 Records

	username	title	email	ip_addresses	target_url	infected_machine_id
0	NaN	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	accounts.zoho.in	5adc68d2-7c02-4116-b0ad-efd7fe039991
56	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.153	5adc68d2-7c02-4116-b0ad-efd7fe039991
55	NaN	Raccoon Stealer	ramananethiraje@gmail.com	103.98.62.162	accounts.google.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
54	NaN	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	www.airtel.in	5adc68d2-7c02-4116-b0ad-efd7fe039991
53	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.13.2	5adc68d2-7c02-4116-b0ad-efd7fe039991
52	NaN	Raccoon Stealer	mohanaramananethiraj@gmail.com	103.98.62.162	membership.commscope.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
51	NaN	Raccoon Stealer	newstamiltv24x7@gmail.com	103.98.62.162	accounts.google.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
50	NaN	Raccoon Stealer	manikandan@splusmedia.in	103.98.62.162	www.jio.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
57	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.88	5adc68d2-7c02-4116-b0ad-efd7fe039991
49	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.19	5adc68d2-7c02-4116-b0ad-efd7fe039991
47	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.31.3	5adc68d2-7c02-4116-b0ad-efd7fe039991
46	admin	Raccoon Stealer	NaN	103.98.62.162	103.98.62.162	5adc68d2-7c02-4116-b0ad-efd7fe039991
45	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.16.42	5adc68d2-7c02-4116-b0ad-efd7fe039991
44	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.84	5adc68d2-7c02-4116-b0ad-efd7fe039991
43	8080	Raccoon Stealer	NaN	103.98.62.162	169.254.9.180	5adc68d2-7c02-4116-b0ad-efd7fe039991
42	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.20	5adc68d2-7c02-4116-b0ad-efd7fe039991
41	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.81	5adc68d2-7c02-4116-b0ad-efd7fe039991
48	NaN	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	www.hik-connect.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
40	operator	Raccoon Stealer	NaN	103.98.62.162	172.18.1.111	5adc68d2-7c02-4116-b0ad-efd7fe039991
58	NaN	Raccoon Stealer	techsupport@splusmedia.in	103.98.62.162	customersso1.fortinet.com	5adc68d2-7c02-4116-b0ad-efd7fe039991
60	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.36	5adc68d2-7c02-4116-b0ad-efd7fe039991
76	essl	Raccoon Stealer	NaN	103.98.62.162	10.2.2.11	5adc68d2-7c02-4116-b0ad-efd7fe039991
75	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.16.21	5adc68d2-7c02-4116-b0ad-efd7fe039991
74	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.15.51	5adc68d2-7c02-4116-b0ad-efd7fe039991
73	admin	Raccoon Stealer	NaN	103.98.62.162	10.2.12.123	5adc68d2-7c02-4116-b0ad-efd7fe039991

Secutec
Cyber security intelligence

techsupport@splusmedia.in

Results



Secutec
Cyber security intelligence

Product Information

General | Version & Update

Serial Number	FG4H0E5819901246
Product Model	FortiGate 400E
Description	Splus_Fortinet_Master
Partner	Raksha Technologies Pvt. Ltd.
Registration Date	2021-04-23
Ship Date	2020-03-31
Warranty	Standard
Warranty Support Start Date	2020-07-09
Warranty Support Start Event	Auto-started 99 days after ship date

Entitlement

- Hardware
- Firmware & General Updates
- Enhanced Support
- Telephone Support
- Advanced Malware Protection
- NGFW
- Web & Video Filtering
- AntiSpam

Registration

Renew Contract

Add Licenses

Threat Protection Statistics

Past 30 days

TOP 20 VIRUS	TOP 20 IPS	TOP 20 BOTNET
15	474	438

Example with data from 2 months ago

Data for barracudanetworks.com

Data records matching this domain.

Raccoon Stealer	2023-03-02	-	-	imperatech_msp@barracudamsp

Raccoon Stealer

Raccoon is a type of malware (or stealer) affecting Windows users. The Stealer has risen in popularity among cyber criminals as a means to procure credit card information, passwords, and cryptocurrency. The tool was first detected in April 2019. The payload is generally to victims via exploit kits, phishing and compromised software downloads.

Breach ID: 43045

Remediation Overview

2,783,685

Total Number of Records

Malware

Private Data

SpySight

1,459,421 Emails

2,783,685 Passwords

2,783,315 IP Addresses

1,324,264 Usernames

2,783,685 PII

Geographic Location

Phone Numbers

1,083,901 Financial

Secutec
Cyber security intelligence

Security Assessments

- Consulting
- Firewall/UTM/IDS / IPS
- Web application Firewall
- Identity & Access Management
- End point security solutions
- Mobile Device Management
- Vulnerability Assessment
- Penetration Testing
- Email Security
- Email Threat Protection
- End Point Protection

We provide a full range

Of modern services and solutions

IMPERATECH SOLUTIONS

Home About Services Partners Recruitment Contact Us

Service Management Partners

- Ivanti
- Cherwell
- Solarwinds Partner
- Connectwise
- Micro Focus Premier Partner

LAN / WAN / Wireless Partners

- Netgear
- Ubiquiti
- Dell EMC
- Mikrotik
- Lenovo Partner

Hyper Convergence Partners

- Nutanix
- Vmware
- Dell EMC
- HPE

It Security Partners

- Mimecast
- CSAT
- Fortinet Partner
- Bitdefender
- Panda
- Sophos

Back Up / DR Partners

- Veeam
- Acronis
- Soteria
- Comm Vault
- Microsoft Azure
- APC Partner

Information on username: imperatech_msp@barracudamsp
Results: 3 records (2 infections)

	username	title	infected_time	ip_addresses	target_url	infected_machine_id
0	imperatech_msp@barracudamsp	Raccoon Stealer	NaN	105.185.158.214	auth.barracudanetworks.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
1	imperatech_msp@barracudamsp	Russian Password Stealer	2021-05-05T09:24:05Z	129.205.131.194	login.barracudanetworks.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
2	imperatech_msp@barracudamsp	Russian Password Stealer	2021-05-05T09:24:05Z	129.205.131.194	auth.barracudanetworks.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c

Secutec
Cyber security intelligence

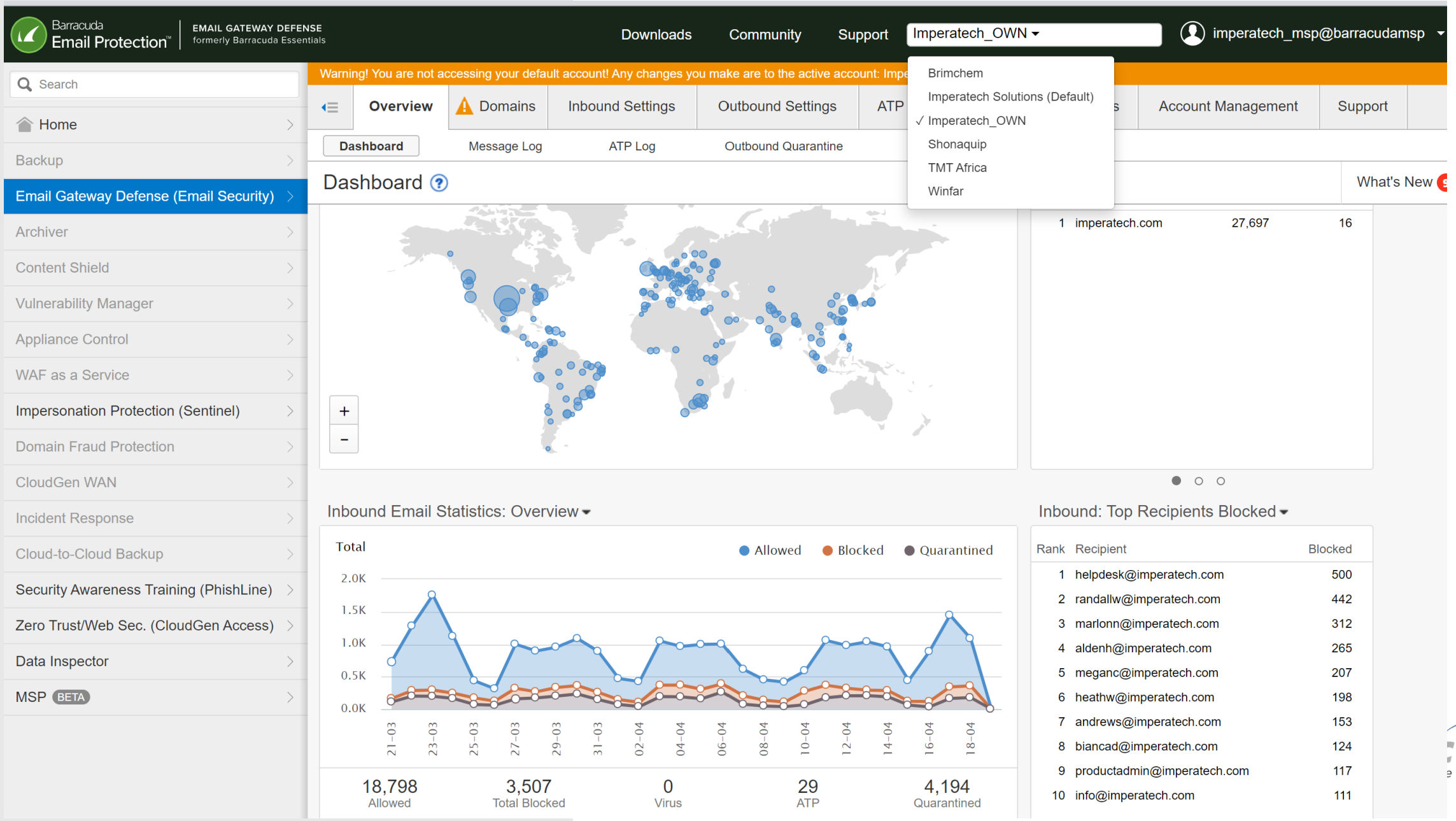
Information on Infected_Machine_ID: 688108b8-5df0-4ab4-a49d-c1d7006c1ef6
Result: 37 Records

	username	title	email	ip_addresses	target_url	infected_machine_id
0	etnice	Raccoon Stealer	NaN	105.185.158.214	eu-cloud.acronis.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
1	standard policy	Raccoon Stealer	NaN	105.185.158.214	aether.pandasecurity.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
2	justin john	Raccoon Stealer	NaN	105.185.158.214	platform.easyequities.io	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
3	imperatech-product-admin	Raccoon Stealer	NaN	105.185.158.214	lastpass.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
4	NaN	Raccoon Stealer	productadmin@imperatech.com	105.185.158.214	accounts.pandasecurity.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
5	NaN	Raccoon Stealer	alex@alphen.co.za	105.185.158.214	account.ui.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
6	admin	Raccoon Stealer	NaN	105.185.158.214	192.168.1.70	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
7	NaN	Raccoon Stealer	justinjohn1021@gmail.com	105.185.158.214	login.live.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
8	NaN	Raccoon Stealer	justinjohn1021@gmail.com	105.185.158.214	identity.yourhcm.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
9	NaN	Raccoon Stealer	justinjohn1021@gmail.com	105.185.158.214	www.sterkinekor.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
10	NaN	Raccoon Stealer	justinj@imperatech.com	105.185.158.214	imperatech-team.myfreshworks.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
11	NaN	Raccoon Stealer	biancad@imperatech.com	105.185.158.214	www.bitrasercloud.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
12	admin_imperatech	Raccoon Stealer	NaN	105.185.158.214	mw.tepsa.co.za	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
13	justin john	Raccoon Stealer	NaN	105.185.158.214	support.freshdesk.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
14	justin john	Raccoon Stealer	NaN	105.185.158.214	identity.openeasy.io	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
15	justin john	Raccoon Stealer	NaN	105.185.158.214	support.euphoria.co.za	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
16	admin	Raccoon Stealer	NaN	105.185.158.214	fgt30e5620023122.device.fortigate.forticloud.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
17	justin_imperatech	Raccoon Stealer	NaN	105.185.158.214	mw.tepsa.co.za	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
18	justin-john	Raccoon Stealer	NaN	105.185.158.214	cloud.acronis.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
19	NaN	Raccoon Stealer	justinj@imperatech.com	105.185.158.214	login.microsoftonline.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
20	NaN	Raccoon Stealer	ithelpdesk@imperatech.com	105.185.158.214	lastpass.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
21	rei174	Raccoon Stealer	NaN	105.185.158.214	rcp.axxess.co.za	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
22	NaN	Raccoon Stealer	justinj@imperatech.com	105.185.158.214	vmstarcommunity.force.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
23	NaN	Raccoon Stealer	justinjohn1021@gmail.com	105.185.158.214	login.microsoftonline.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6
24	NaN	Raccoon Stealer	wesleyb@imperatech.com	105.185.158.214	lastpass.com	688108b8-5df0-4ab4-a49d-c1d7006c1ef6

Information on Infected_Machine_ID: 44c61bdc-3cce-4b6f-af46-a31b669ffd6c
Result: 242 Records

	username	title	email	infected_time	ip_addresses	target_url	infected_machine_id
0	NaN	Russian Password Stealer	anathim@imperatech.com	2021-05-05T09:24:05Z	129.205.131.194	auth.tuya.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
153	NaN	Russian Password Stealer	anathim@imperatech.com	2021-05-05T09:24:05Z	129.205.131.194	www.gotomeeting.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
154	anathimaliti	Russian Password Stealer	NaN	2021-05-05T09:24:05Z	129.205.131.194	learningweek.amityfutureacademy.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
155	NaN	Russian Password Stealer	admin@paymaster.co.za	2021-05-05T09:24:05Z	129.205.131.194	login-za.mimecast.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
156	NaN	Russian Password Stealer	siphamamdlagampe@gmail.com	2021-05-05T09:24:05Z	129.205.131.194	eurous.net	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
157	admin	Russian Password Stealer	NaN	2021-05-05T09:24:05Z	129.205.131.194	10.10.1.37	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
158	NaN	Russian Password Stealer	compassops@shonaquip.co.za	2021-05-05T09:24:05Z	129.205.131.194	login.microsoftonline.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
159	anathim	Russian Password Stealer	NaN	2021-05-05T09:24:05Z	129.205.131.194	moses.happychappy.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
160	NaN	Russian Password Stealer	maliti.kellz@gmail.com	2021-05-05T09:24:05Z	129.205.131.194	accounts.pandasecurity.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
161	info	Russian Password Stealer	NaN	2021-05-05T09:24:05Z	129.205.131.194	moses.happychappy.com	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
162	NaN	Russian Password Stealer	maliti.kellz@gmail.com	2021-05-05T09:24:05Z	129.205.131.194	knowledgetrust.org	44c61bdc-3cce-4b6f-af46-a31b669ffd6c
163	NaN	Russian Password Stealer	maliti.kellz@gmail.com	2021-05-05T09:24:05Z	129.205.131.194	www.sportingbet.co.za	44c61bdc-3cce-4b6f-af46-a31b669ffd6c

Results


Barracuda Email Protection
EMAIL GATEWAY DEFENSE
formerly Barracuda Essentials
Downloads
Community
Support
Imperatech_OWN
imperatech_msp@barracudamsp
Brimchem
Imperatech Solutions (Default)
Imperatech_OWN
Shonaquip
TMT Africa
Winfar
Warning! You are not accessing your default account! Any changes you make are to the active account: Impe
Search
Home
Backup
Email Gateway Defense (Email Security)
Archiver
Content Shield
Vulnerability Manager
Appliance Control
WAF as a Service
Impersonation Protection (Sentinel)
Domain Fraud Protection
CloudGen WAN
Incident Response
Cloud-to-Cloud Backup
Security Awareness Training (PhishLine)
Zero Trust/Web Sec. (CloudGen Access)
Data Inspector
MSP BETA
Overview
Domains
Inbound Settings
Outbound Settings
ATP
Account Management
Support
Dashboard
Message Log
ATP Log
Outbound Quarantine
Dashboard
What's New
1 imperatech.com 27,697 16
Inbound Email Statistics: Overview
Total
Allowed
Blocked
Quarantined
2.0K
1.5K
1.0K
0.5K
0.0K
21-03
23-03
25-03
27-03
29-03
31-03
02-04
04-04
06-04
08-04
10-04
12-04
14-04
16-04
18-04
18,798 Allowed
3,507 Total Blocked
0 Virus
29 ATP
4,194 Quarantined
Inbound: Top Recipients Blocked
Rank Recipient Blocked
1 helpdesk@imperatech.com 500
2 randallw@imperatech.com 442
3 marlonn@imperatech.com 312
4 aldenh@imperatech.com 265
5 meganc@imperatech.com 207
6 heathw@imperatech.com 198
7 andrews@imperatech.com 153
8 biancad@imperatech.com 124
9 productadmin@imperatech.com 117
10 info@imperatech.com 111

Barracuda
Cloud Control

Downloads Community Support Shonaquip imperatech_msp@barracudamsp

Search

Warning! You are not accessing your default account! Any changes you make are to the active account: Shonaquip.

- Home
- Backup
- Email Gateway Defense (Email Security)
- Archiver
- Content Shield
- Vulnerability Manager
- Appliance Control
- WAF as a Service
- Impersonation Protection (Sentinel)
- Domain Fraud Protection
- CloudGen WAN
- Incident Response
- Cloud-to-Cloud Backup
- Security Awareness Training (PhishLine)
- Zero Trust/Web Sec. (CloudGen Access)
- Data Inspector
- MSP BETA

Admin | My Profile

Profile

imperatech_msp@barracudamsp

Signed in as: imperatech_msp@barracudamsp
Company: Shonaquip

Change Current Password

Cancel Save

Current Password: Current Password
New Password: New Password
Confirm New Password: New Password

Language

Set Preferred Language: English (US)

Multi-Factor Authentication

Help

Click "Add New Device" to configure and enable multi-factor authentication.

Device Name	Date Added	Options
		Add New Device

Time Zone Details

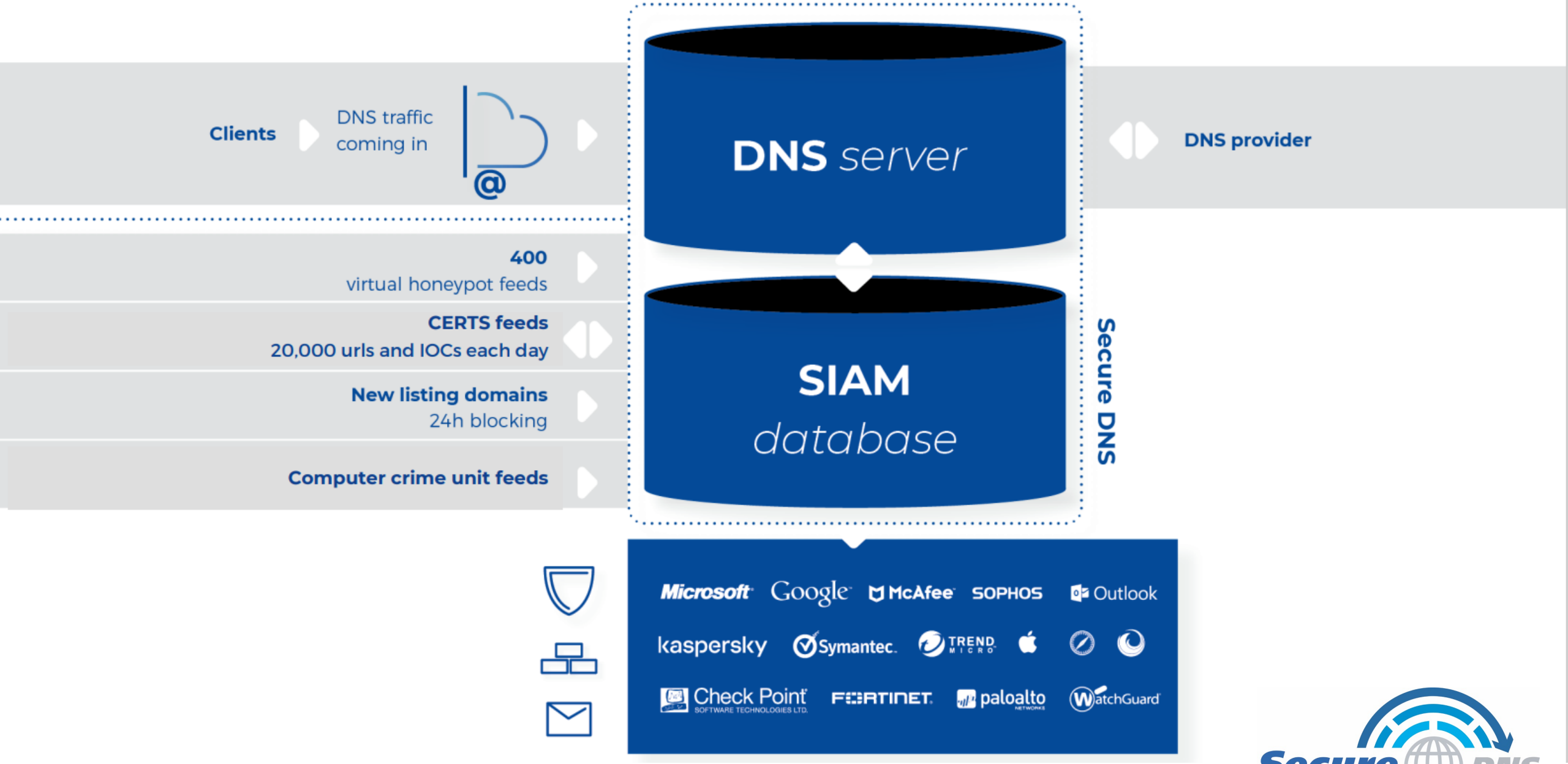
Cancel Save Help

Here you can set the time zone for your user account.

Time Zone: America/Detroit

Secutec SecureDNS

DETECT AND BLOCK NEW THREATS FASTER THAN YOUR CURRENT SECURITY SOLUTION.



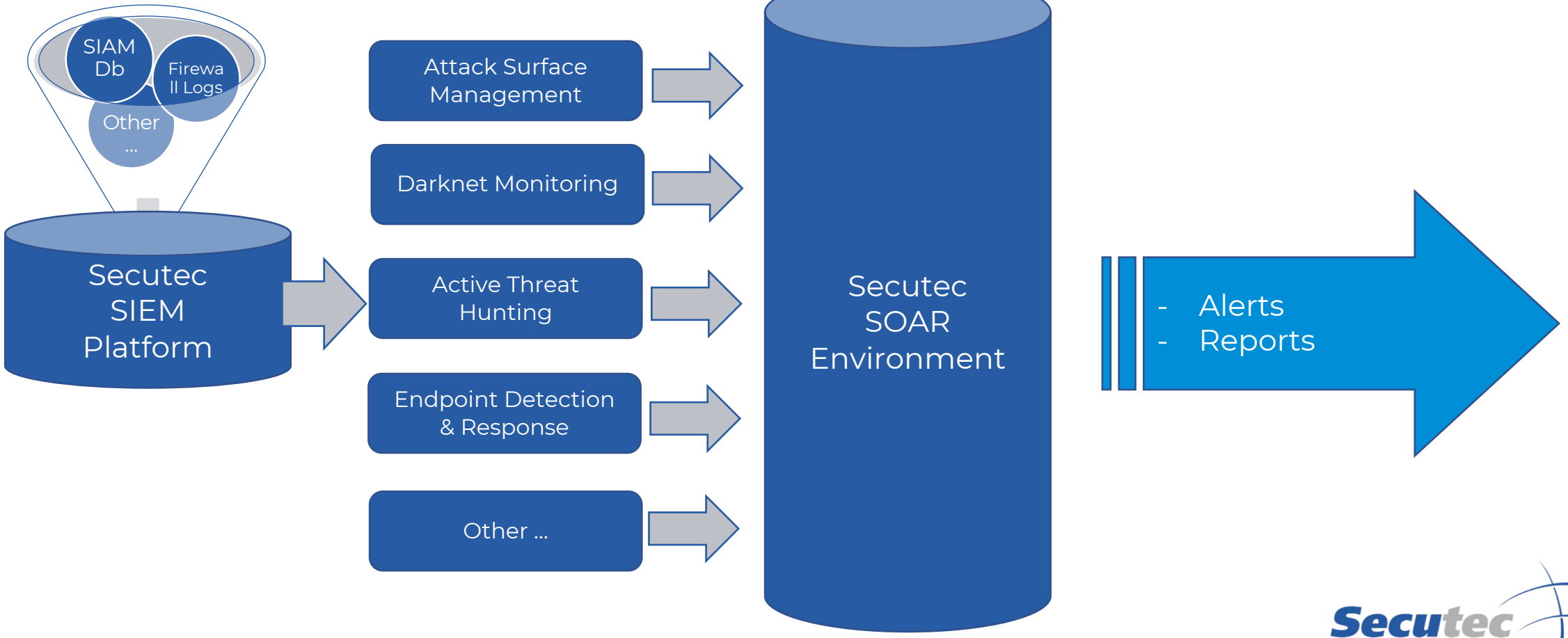
Employees will never stop clicking bad links

Secure DNS
POWERED BY SECUTEC

Secure SIGHT

by Secutec

Secure SIGHT



Secutec
Cyber security intelligence

Secure DNS
POWERED BY SECUTEC

Secure SIGHT

Questions?

info@secutec.be

Contact us

Secutec
Cyber security intelligence

Secutec

Cyber security intelligence