

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center

The logo consists of the word "BETTER." in a bold, sans-serif font. The letters are white with a subtle gray texture. The letter "B" has a circular pattern of dots and lines behind it, transitioning from blue at the top to yellow at the bottom. The letter "E" has a similar pattern but is mostly yellow. The letter "T" is mostly blue. The letter "R" has a similar pattern to the "B" and "E".

SESSION ID: IDY-W12

How the H@ck R U? A Modern Identity Assurance Approach in a Hacked World

Angel Grant, CISSP

Director, Identity, Fraud & Risk Intelligence
RSA
@AngelsGrant

#RSAC



GRAY WEB

Hiding in Plain Sight

Criminal
Nation State
Hacktivist

DEEP WEB

Closed Network

DARK NET

Anonymous Network

Think Like a Cybercriminal

Services Offering



Cybercriminal Opportunity

Next-day shipping / In-store pickup



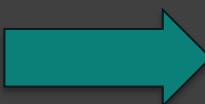
My shipping mule will have it before your fraud team knows its gone!

Real-time payments



I'll cash out before your customer calls about a weird transaction

\$10 for new accounts promotion



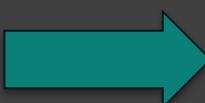
One sounds good but 6,000 sounds great

"Forgot my password" link



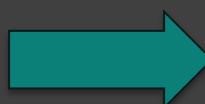
Hmm...we have credential stuffing tools

Account locks after 5 failed logins



Good luck making \$ when I lock your users

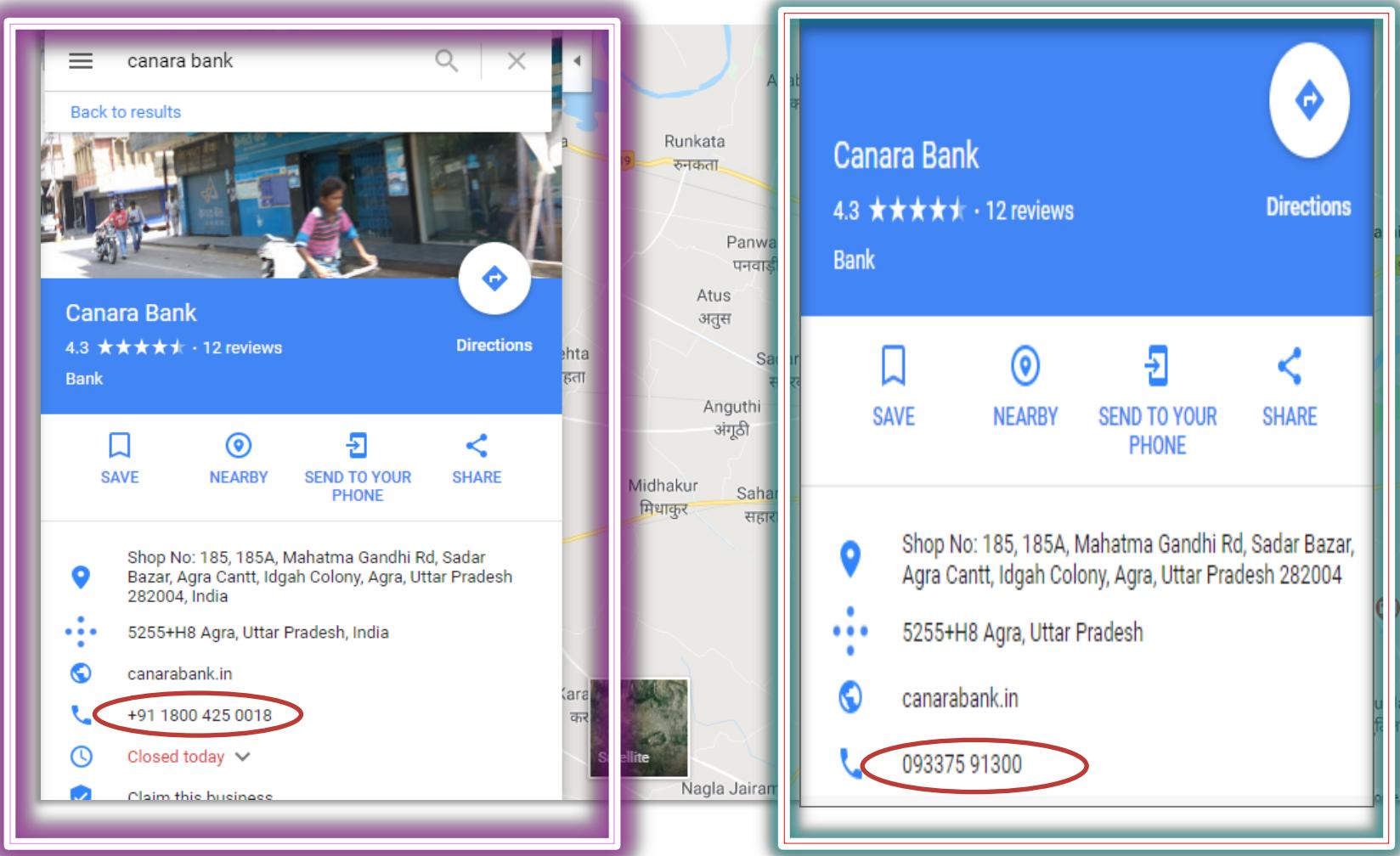
Aggregated online accounts



Cool, identity theft one-stop-shop!

Here is How a Cybercriminal Thinks - Vishing in Reverse

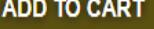
- Customer searches for phone number
- Google Maps present details
- Customer calls fraudster



Why Cybercriminals Target Specific Industries



Customizable Shopping - CVV Store

				NEWS	BUY	ORDERS	BILLING	CHECKERS	BINBASE	SUPPORT	BALANCE 100.83 \$	CART 0				
																
																
	Bin	Exp	First name	Last name	Address	City		State		Zip	Phone	Country	Fullz	Can I refund?	Price	Base Name
	4658: CLASSI DEBIT	12/19	Emma	All	x	SWA		PLEASE SELECT REGION STATE OR PROVINCE		Sa1	0747	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF
	4658: CLASSI DEBIT	07/20	Alannah	Pa	x	TAM		PLEASE SELECT REGION STATE OR PROVINCE		B77	0737	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF
	4658: CLASSI DEBIT	06/20	Charlotte	W	x	STO		CLEVELAND		TS1	0785	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF
	4658: CLASSI DEBIT	09/20	Corina-gearina	Do	x4x2	BRAI		BRĂILA		810	0744	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF
	4658: CLASSI DEBIT	02/19	Alex	Wi	142x	BIRM		PLEASE SELECT REGION STATE OR PROVINCE		B30	0777	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF
	4658:	09/20	Joe	Po	30x	BIRM		WEST MIDLANDS		B44	0785	UNITED KINGDOM	-	No	12.00\$	DEC_#20_UK_US_NO_REF

Shopping for Credentials on Account Stores

Thursday 25 January 2018

News Crime

Most Read **Most Shared**

'No way' jailed brother will be released for funeral of latest Hutch-Kinahan feud... [Crime](#)

Romance fraud: Irish woman lost €37,000 after falling in love with a man claiming to be a US soldier serving in Afghanistan



1 Q

Use search box, to search for sellers, information etc.

Type	Country	Seller	Any	Match	ChristianMingle	POF	Jdate	Eharmony	Zoosk																																
Any	Any	Any	FirstMet	Chemistry	MuslimMatch	SingleParentMeet	Mingle2																																		
<input style="width: 100%;" type="text" value="Search: "/>																																									
<table border="1"> <thead> <tr> <th colspan="2">Information</th> <th>Seller</th> <th>Price</th> </tr> </thead> <tbody> <tr> <td colspan="2">Friends Count: 0 // Credit Balance: 0 // NAME: [REDACTED] : Ward // Gender: m // Province: NY</td> <td>[REDACTED]</td> <td>3.00\$</td> </tr> <tr> <td colspan="2">PAID Pof - Gender: Male, Age: 21, Profile: www.pof.com/viewprofile.aspx?profile_id=[REDACTED], Subscription Status: 3 Month Upgrade, Expire: 2017-06-18</td> <td>[REDACTED]</td> <td>10.00\$</td> </tr> <tr> <td colspan="2">Unpaid Account - Wheeling, IL / Age: 75 / DOB: January/ [REDACTED]/1942 / Male</td> <td>[REDACTED]</td> <td>4.00\$</td> </tr> <tr> <td colspan="2">UNPAID Match - Country: United-States, Age: 21, Gender: Male, Zip Code: 90706</td> <td>[REDACTED]</td> <td>2.99\$</td> </tr> <tr> <td colspan="2">UNPAID Match - Gender: Female, Age: 26, Country: United-States, Zip: 56556, DOB: [REDACTED].08.1990</td> <td>[REDACTED]</td> <td>3.00\$</td> </tr> <tr> <td colspan="2">UNPAID - Birthday: 1962-11-21T00:00:00.000Z, Gender: MALE, Country: US</td> <td>[REDACTED]</td> <td>3.00\$</td> </tr> <tr> <td colspan="2">Free Account / Female / Zip Code: 12912 / September-4-1992 / Age: 25 / United States / a [REDACTED] / New York</td> <td>[REDACTED]</td> <td>3.00\$</td> </tr> </tbody> </table>										Information		Seller	Price	Friends Count: 0 // Credit Balance: 0 // NAME: [REDACTED] : Ward // Gender: m // Province: NY		[REDACTED]	3.00\$	PAID Pof - Gender: Male, Age: 21, Profile: www.pof.com/viewprofile.aspx?profile_id=[REDACTED], Subscription Status: 3 Month Upgrade, Expire: 2017-06-18		[REDACTED]	10.00\$	Unpaid Account - Wheeling, IL / Age: 75 / DOB: January/ [REDACTED]/1942 / Male		[REDACTED]	4.00\$	UNPAID Match - Country: United-States, Age: 21, Gender: Male, Zip Code: 90706		[REDACTED]	2.99\$	UNPAID Match - Gender: Female, Age: 26, Country: United-States, Zip: 56556, DOB: [REDACTED].08.1990		[REDACTED]	3.00\$	UNPAID - Birthday: 1962-11-21T00:00:00.000Z, Gender: MALE, Country: US		[REDACTED]	3.00\$	Free Account / Female / Zip Code: 12912 / September-4-1992 / Age: 25 / United States / a [REDACTED] / New York		[REDACTED]	3.00\$
Information		Seller	Price																																						
Friends Count: 0 // Credit Balance: 0 // NAME: [REDACTED] : Ward // Gender: m // Province: NY		[REDACTED]	3.00\$																																						
PAID Pof - Gender: Male, Age: 21, Profile: www.pof.com/viewprofile.aspx?profile_id=[REDACTED], Subscription Status: 3 Month Upgrade, Expire: 2017-06-18		[REDACTED]	10.00\$																																						
Unpaid Account - Wheeling, IL / Age: 75 / DOB: January/ [REDACTED]/1942 / Male		[REDACTED]	4.00\$																																						
UNPAID Match - Country: United-States, Age: 21, Gender: Male, Zip Code: 90706		[REDACTED]	2.99\$																																						
UNPAID Match - Gender: Female, Age: 26, Country: United-States, Zip: 56556, DOB: [REDACTED].08.1990		[REDACTED]	3.00\$																																						
UNPAID - Birthday: 1962-11-21T00:00:00.000Z, Gender: MALE, Country: US		[REDACTED]	3.00\$																																						
Free Account / Female / Zip Code: 12912 / September-4-1992 / Age: 25 / United States / a [REDACTED] / New York		[REDACTED]	3.00\$																																						

Thursday 25 January 2018

 News Crime

[FOLLOW](#) [CONTACT](#)

Romance fraud: Irish woman lost €37,000 after falling in love with a man claiming to be a US soldier serving in Afghanistan



Victims fall in love with what they believe are their perfect partners online – until they discover they have been scammed into handing over a substantial amount of money to help solve a financial problem – in what is known as a 'catfish' scam. Stock picture

 Tom Brady [✉](#)
January 23 2018 11:51 PM



ROMANCE fraud is blooming on the internet and is becoming a worrying problem for members of the Garda National Economic Crime Bureau, who say it is on the increase here.

Victims fall in love with what they believe are their perfect partners online – until they

[Most Read](#) [Most Shared](#)

'No way' jailed brother will be released for funeral of latest Hutch-Kinahan feud... [Crime](#)

Romance fraud: Irish woman lost €37,000 after falling in love with a man claiming to be a US soldier serving in Afghanistan

Brother of feud murder victim Derek Coakley Hutch heard him being shot dead via a... [Crime](#)

Gardai arrest man in connection with serious assault that left 35-year old in critical... [Crime](#)

Pictured: Third nephew of Gerry 'The Monk' Hutch killed in gangland shooting [Crime](#)

 **The Daily Digest**
Today's news headlines, directly to your inbox every morning.
[Sign Up](#)

Promoted Links by Outbrain

 How a Canadian City Ended Homelessness With a Simple Idea
Goodnet

 Sir Cliff Richard Knocks €3 Million Off Portuguese Vineyard Estate
Mansion Global

One Stop Simplified Cybercrime Shops



Name: Category: Dedicated servers (RDP) USA ❤ 240 🏷 13973 ★ 100 📈 98 📉 11

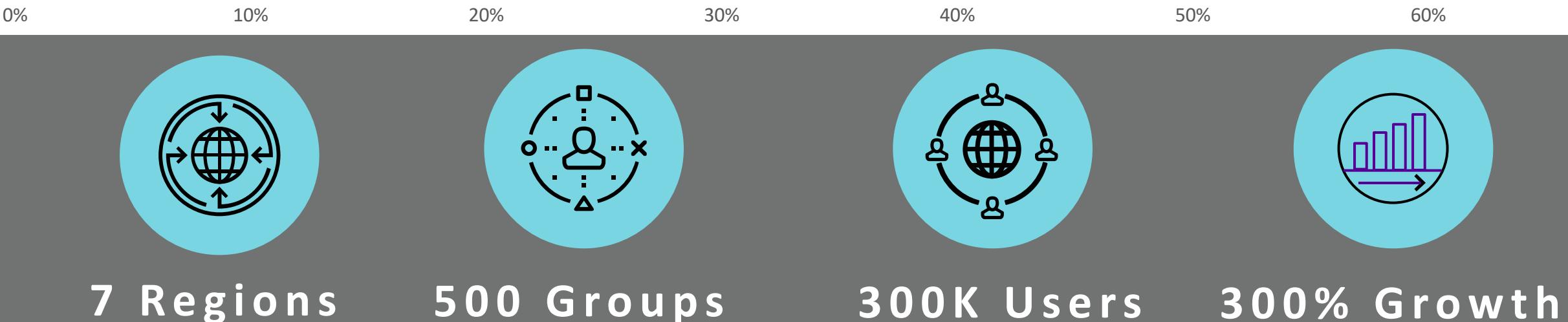
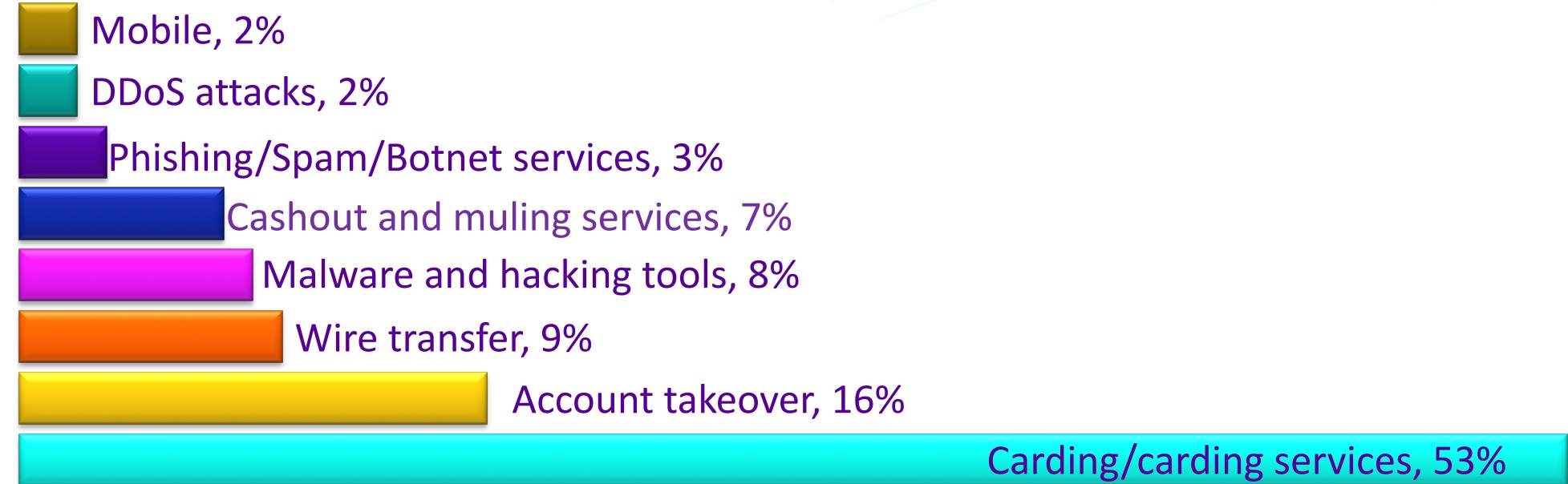
Sort by ▾

You can subscribe to the category updates. When replenishing the product, we will notify you in Jabber

Subscribe

Title	Country	State	Info	Blacklist	Upload		
Dedicated server (RDP) USA and other countries	Thailand	N/A	User, Windows 2012, RAM 16.00 GB, NO Blacklist	NO	21/10/2018 22:04	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	India	Delhi	Administrator, Windows 2012, RAM 64.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$10.00
Dedicated server (RDP) USA and other countries	South Africa	Gauteng	User, Windows 2008, RAM 16.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Japan	Tokyo	User, Windows 2012, RAM 64.00 GB, Yes Blacklist	YES	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Morocco	Grand Casablanca	User, Windows 2007, RAM 24.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Germany	Niedersachsen	User, Windows 2016, RAM 4.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Malta	N/A	User, Windows 2012, RAM 8.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	South Africa	Western Cape	User, Windows 2007, RAM 3.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Kenya	Nairobi Area	Administrator, Windows 2012, RAM 64.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$10.00
Dedicated server (RDP) USA and other countries	France	N/A	User, Windows 2016, RAM 16.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Netherlands	Utrecht	User, Windows 10, RAM 4.00 GB, NO Blacklist	NO	8/10/2018 10:30	+ ⚡	\$8.00
Dedicated server (RDP) USA and other countries	Czech Republic	Hlavni mesto Praha	User, Windows 2012, RAM 32.00 GB, NO Blacklist	NO	7/10/2018 19:37	+ ⚡	\$8.00

Dark Web Morphing into “Gray Web”



Surplus Inventory Selling in Plain Sight

The collage illustrates the dark web market for stolen credit card data. It includes:

- A WhatsApp group chat showing a member's profile and a message of thanks.
- Suggested groups on a platform like Facebook or LinkedIn, including "Tricks By STG" and "freechajg".
- Suggested pages on a platform like VK, featuring a VISA and MasterCard logo.
- A VK login screen with a placeholder email and password field.
- A Weibo-like post with a "Follow" button.
- A forum post with a large image of a credit card.
- A post about "KOREA DUMPS NEW ARRIVE!" with details on card types like Classic, Gold, and platinum.
- A post about "database update!" with a success rate of 90%.
- A post about "收卡, 中电话, 给换!!! I replace HOLD CALL and Pick up card".
- A post about "大量购买者有大折扣!!!!".
- A screenshot of an RSA service page stating "1 item will be shipped to [redacted]".
- A screenshot of a LinkedIn profile with a redacted background image.

Dumps with pin shop CSU:

... credit cards cvv2,
dumps, dumps with pin, cvv2, buy dumps,
buy credit cards, dumps with pin

12:41 PM - 23 Sep 2018

Macking a carding whatsapp group anyone want to join
1 Like 5 Comments

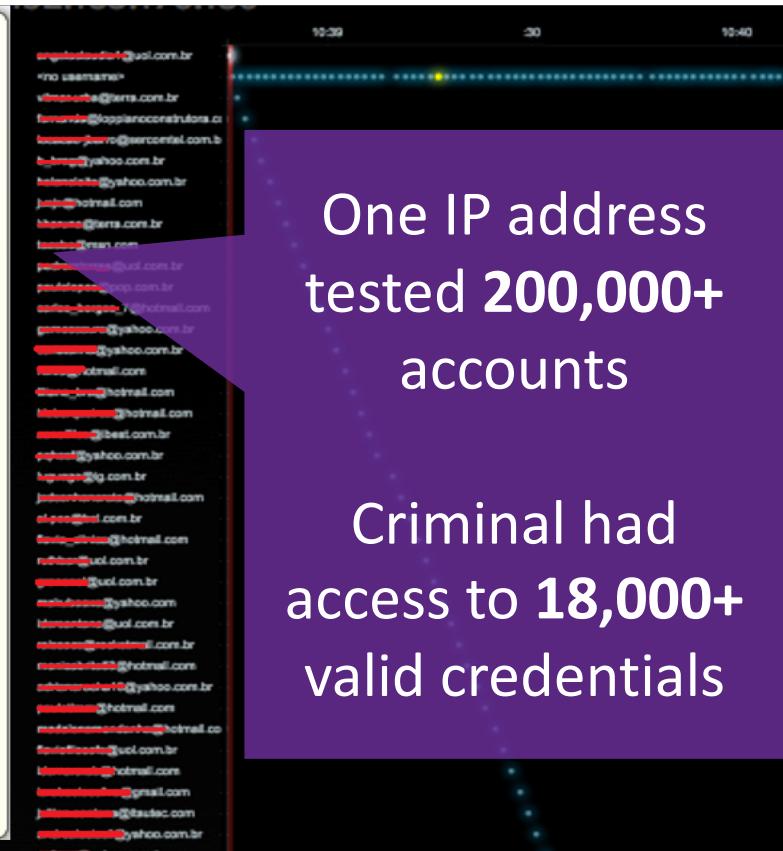
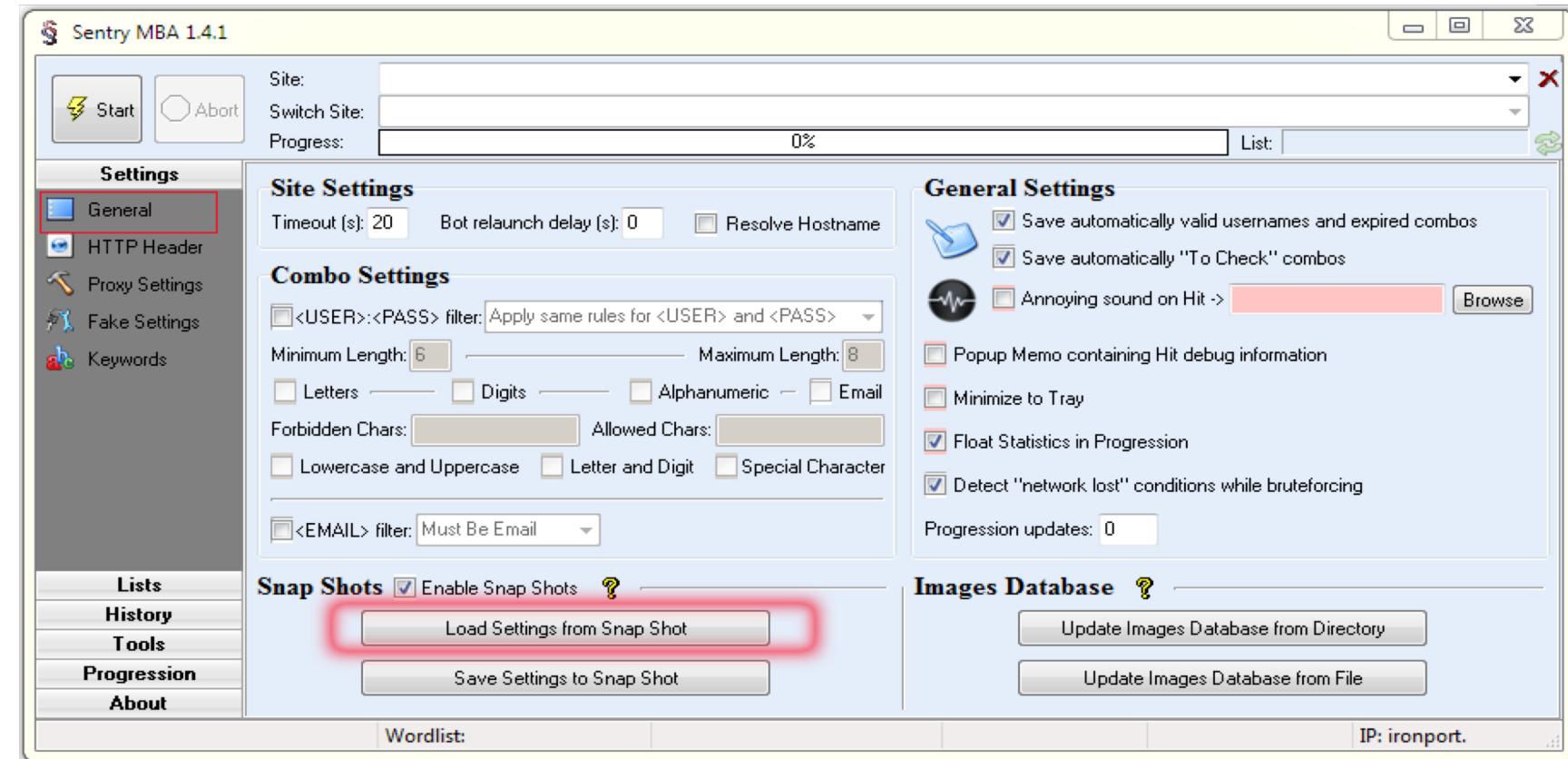
Like Comment

likes this.

3981

Like · Reply · October 4 at 4:50pm

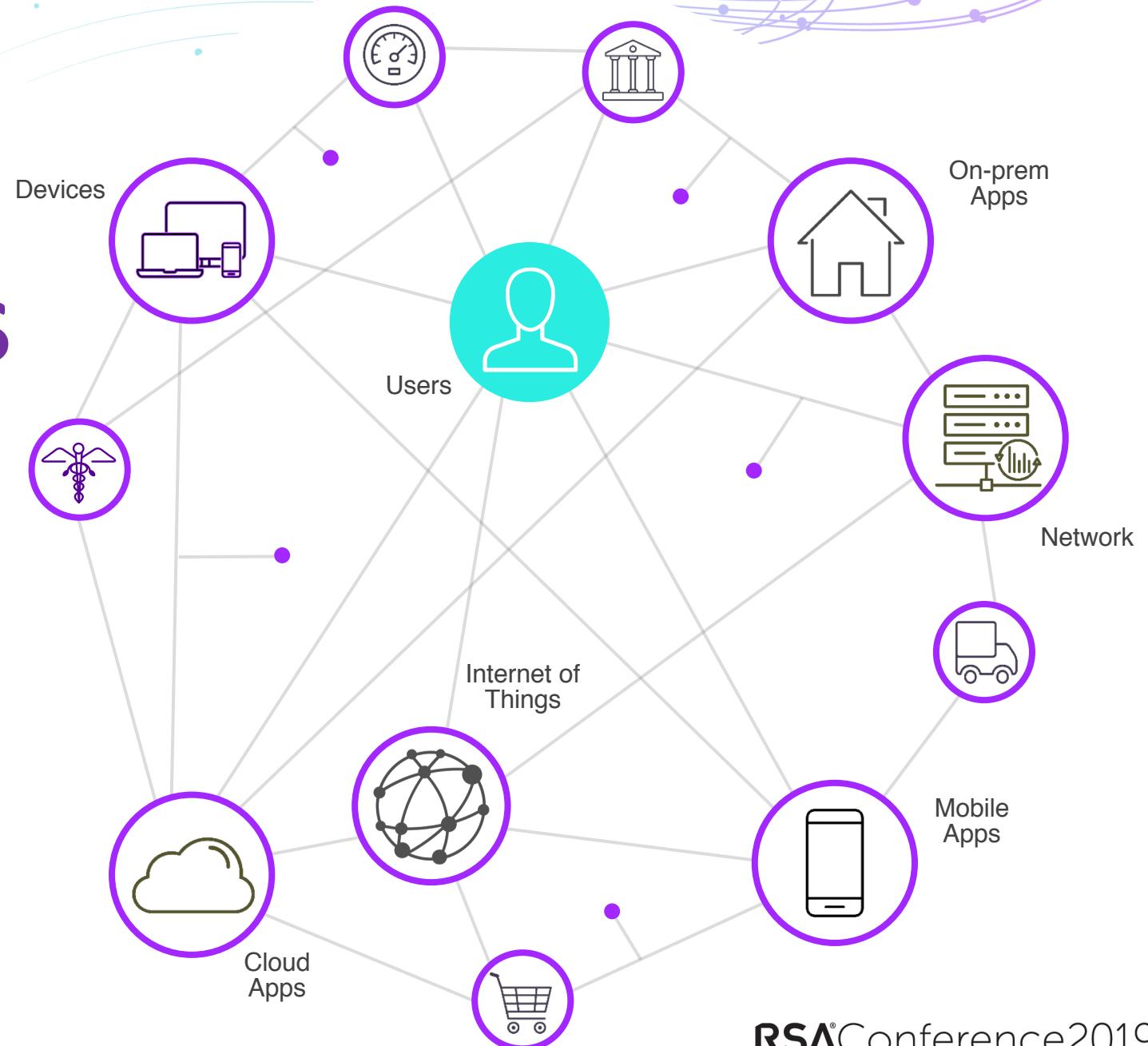
Why Steal It When You Can Stuff It



- New Account has 15x higher fraud rates in 1st 10 days
- Fraud rates 3x higher from new device

IDENTITY OF CONNECTED THINGS

Opens Business Opportunities And Vulnerabilities



IDENTITY ASSURANCE



ACCESS ASSURANCE



ACTIVITY ASSURANCE

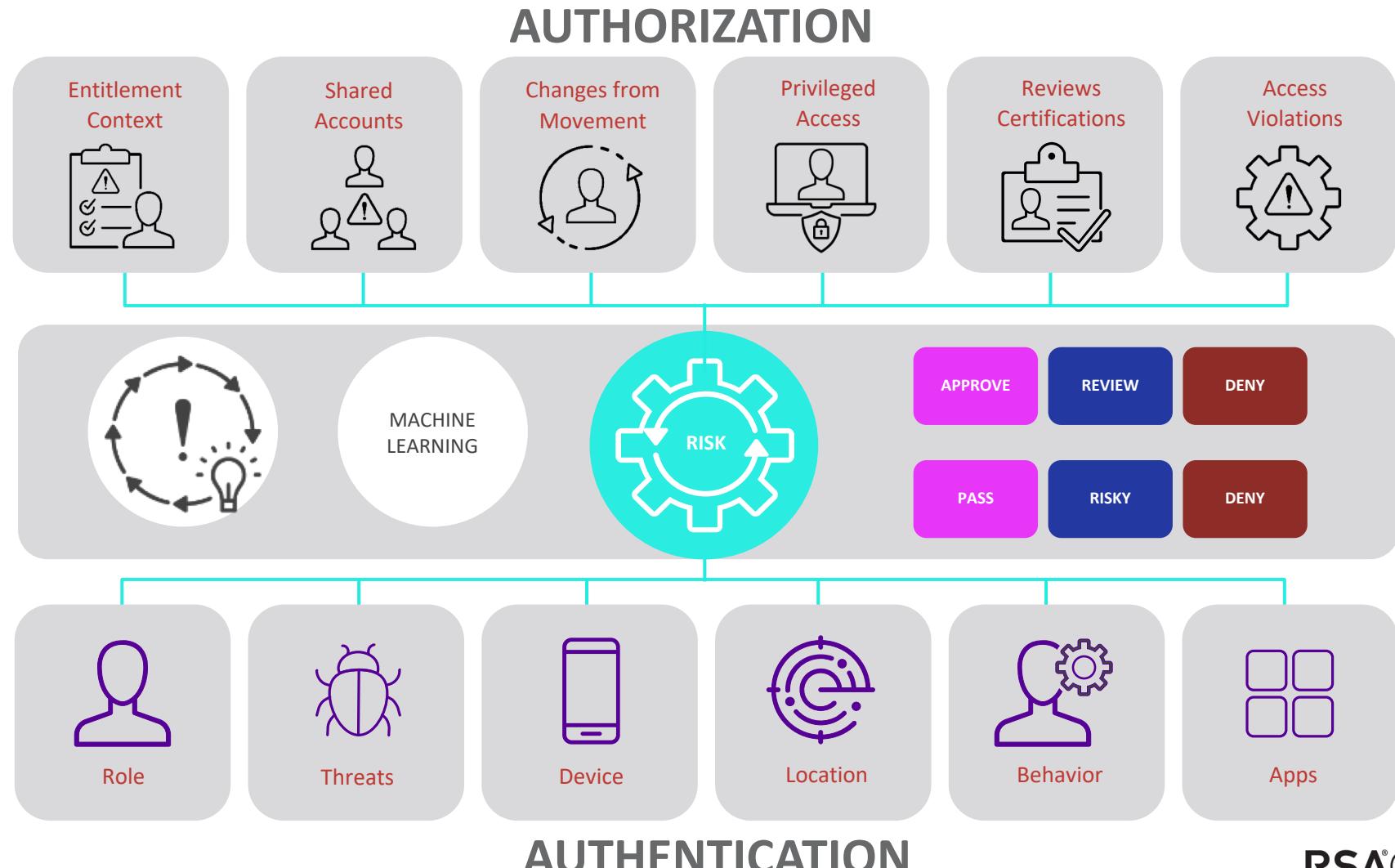


is the user or entity who
they claim they are?

what level of access to
applications and data is ok?

is what they are doing
appropriate or not?

TRANSLATE VISIBILITY INTO INSIGHTS BY CORRELATING ACCESS DATA



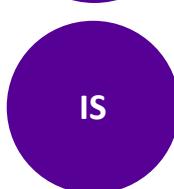
IDENTITY & ACCESS MANAGEMENT



is the user?

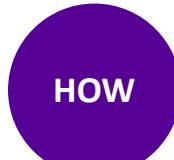


can they access?



what they are doing ok?

NETWORK & PERIMETER SECURITY



do you take threats into account?



FRAUD INTELLIGENCE



known fraud is this user or device associated with?



should I care?
Is there a risk to my business?

Use Case #1: Identity Assurance

Trust a simple 4 digit PIN for VPN access?

Th1\$2\$4ck\$!

Apply Identity Analytics
How about now?

We weren't able to update your password.
Please make sure your new password follows the guidelines on this page.

Username

Enter a new password

Confirm your new password

Here are the guidelines for creating a new password:

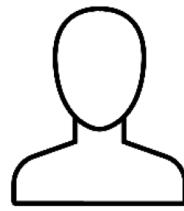
• At least 8 characters long.
• It must contain at least 2 of the following criteria:
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 number
- At least 1 special character (! # \$ % + / = - ^ & _)
• It must be different than your previous 5 passwords.
• It can't include consecutive characters (for example: 123 or abc).
• It can't use the name of the financial institution (for example: [Bank Name]).
• It can't be a commonly used password (for example: password1).

1234

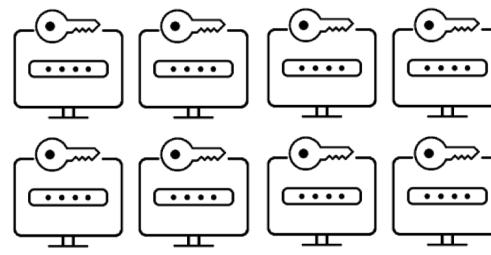
- Role
- Threats
- Device
- Location
- Behavior
- Apps

Use Case #2: Access Assurance

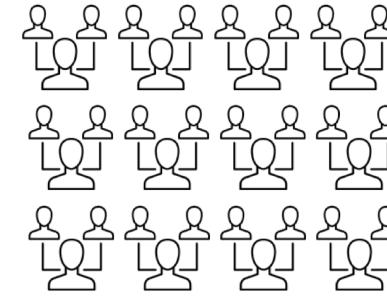
USERS



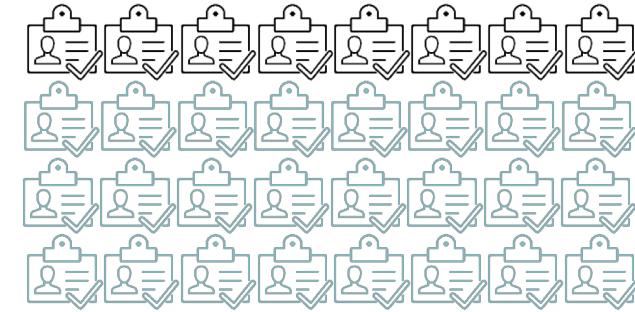
ACCOUNTS



ROLES



ENTITLEMENTS

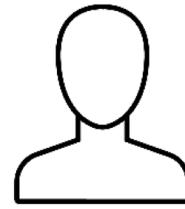


DECISION

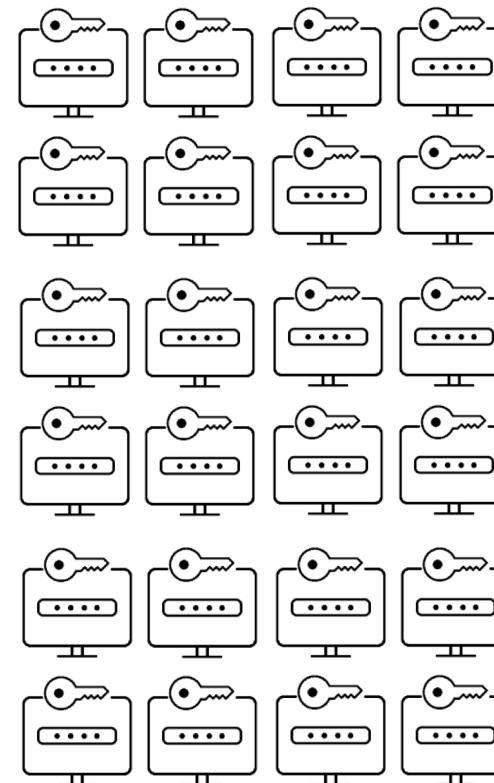
APPROVED

Use Case #2: Access Assurance

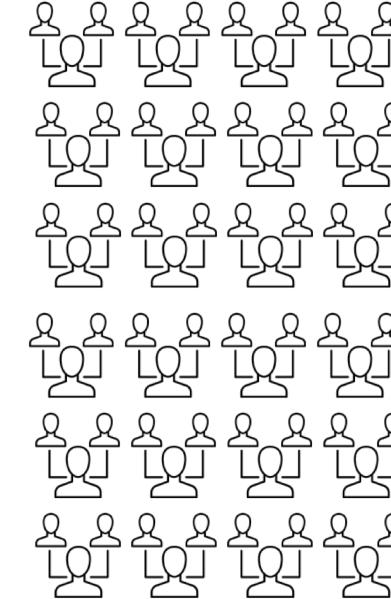
USERS



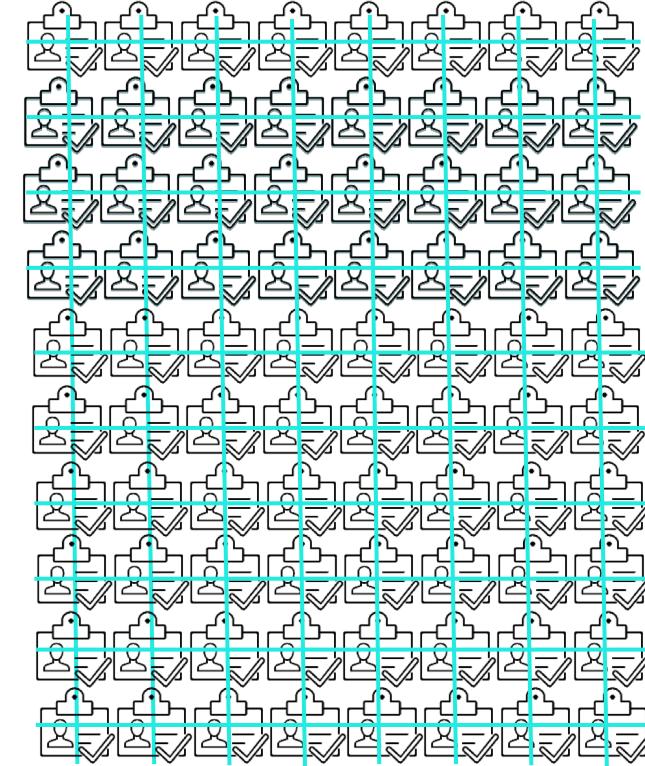
ACCOUNTS



ROLES



ENTITLEMENTS

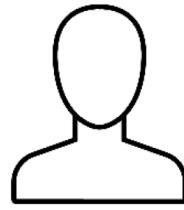


DECISION

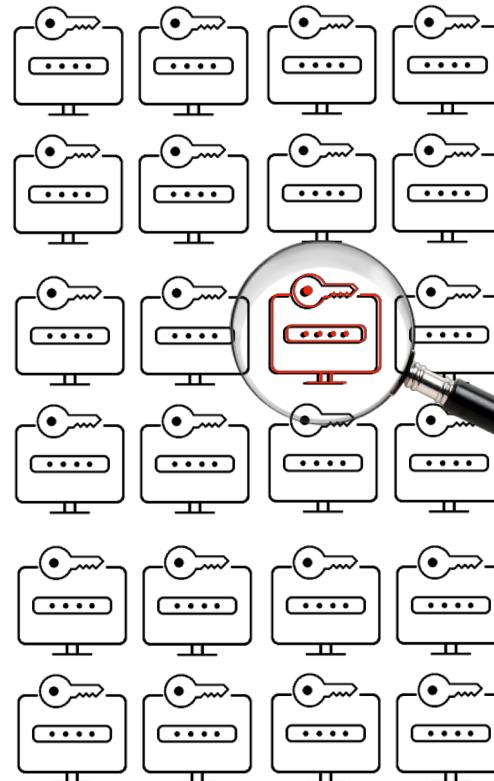


Use Case #2: Access Assurance

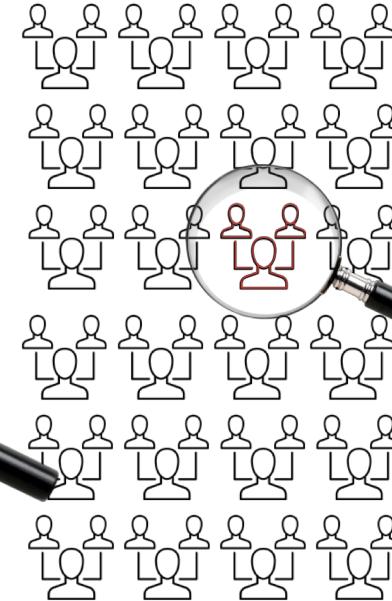
USERS



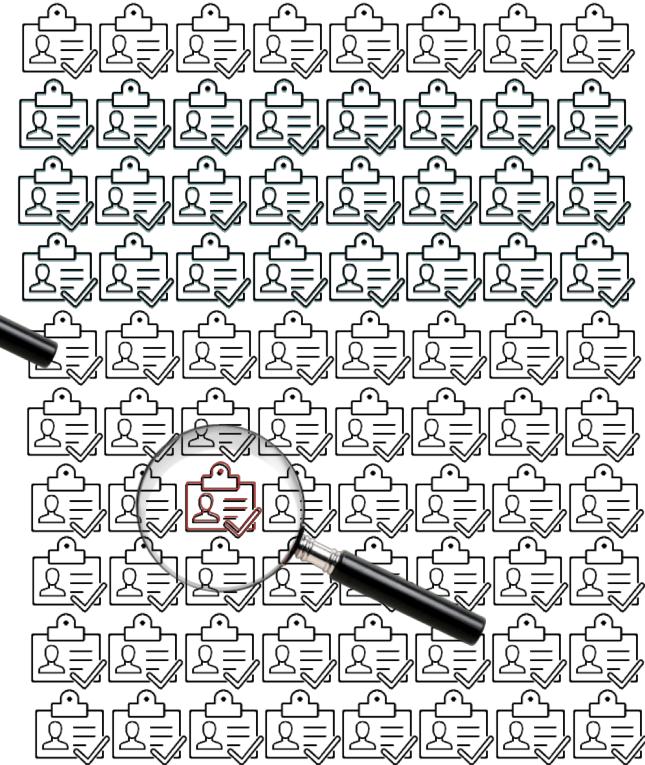
ACCOUNTS



ROLES



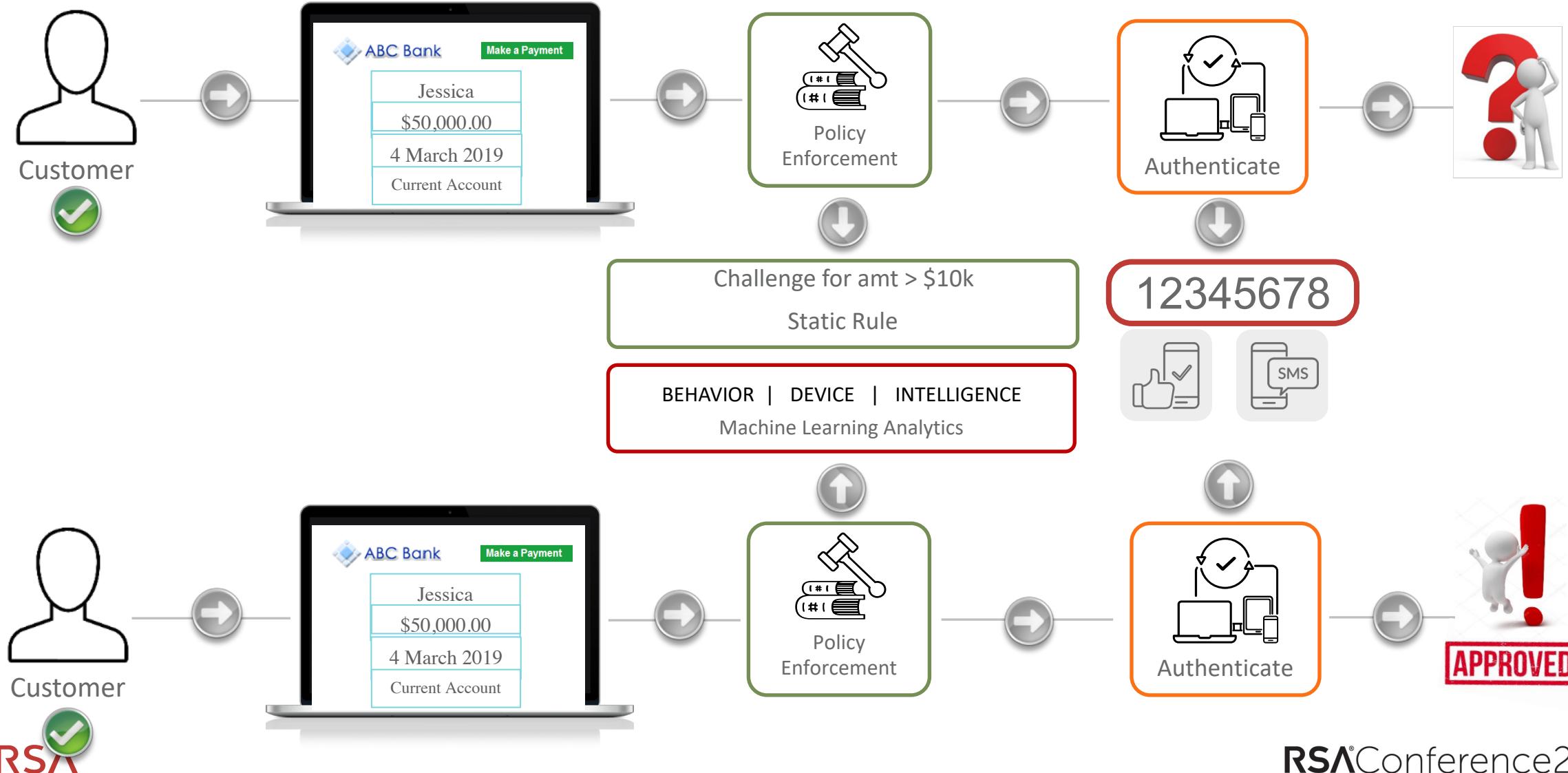
ENTITLEMENTS



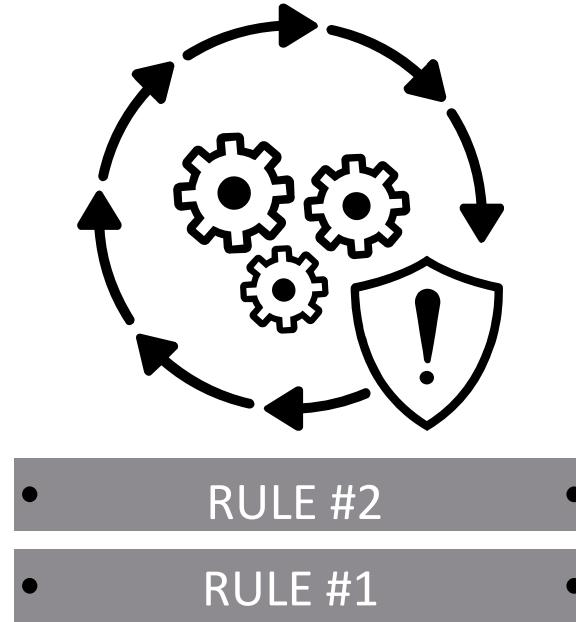
DECISION



Use Case #3: Activity Assurance



What Should You Do to Transform Your Identity Assurance Strategy?



Augment static-rules
with analytics

Expand visibility & insight to
take Action



Harness the power
across your security village

How the H@CK R U Now?

Apply What You Have Learned Today

- **Next week you should:**

- Identify who is monitoring cybercrime underground for your company

- **In first three months you should:**

- Investigate new potential points of vulnerabilities
 - (e.g. Shadow IoT, islands of identities, credentials sold on social media)
 - Create plan to mitigate account takeover
 - Augment static-based IAM rules with identity analytics

- **Within six months you should:**

- Unite your security village
 - including threat detection, GRC and fraud prevention tools



Angel Grant, CISSP
RSA, Director
@Angelsgrant