

RSA® Conference 2018

Singapore | 25–27 July | Marina Bay Sands



#RSAC

SESSION ID: FLE-F02

HOW A DIVERSE ECOSYSTEM CREATES RESILIENCE IN THE CYBERCRIMINAL UNDERGROUND

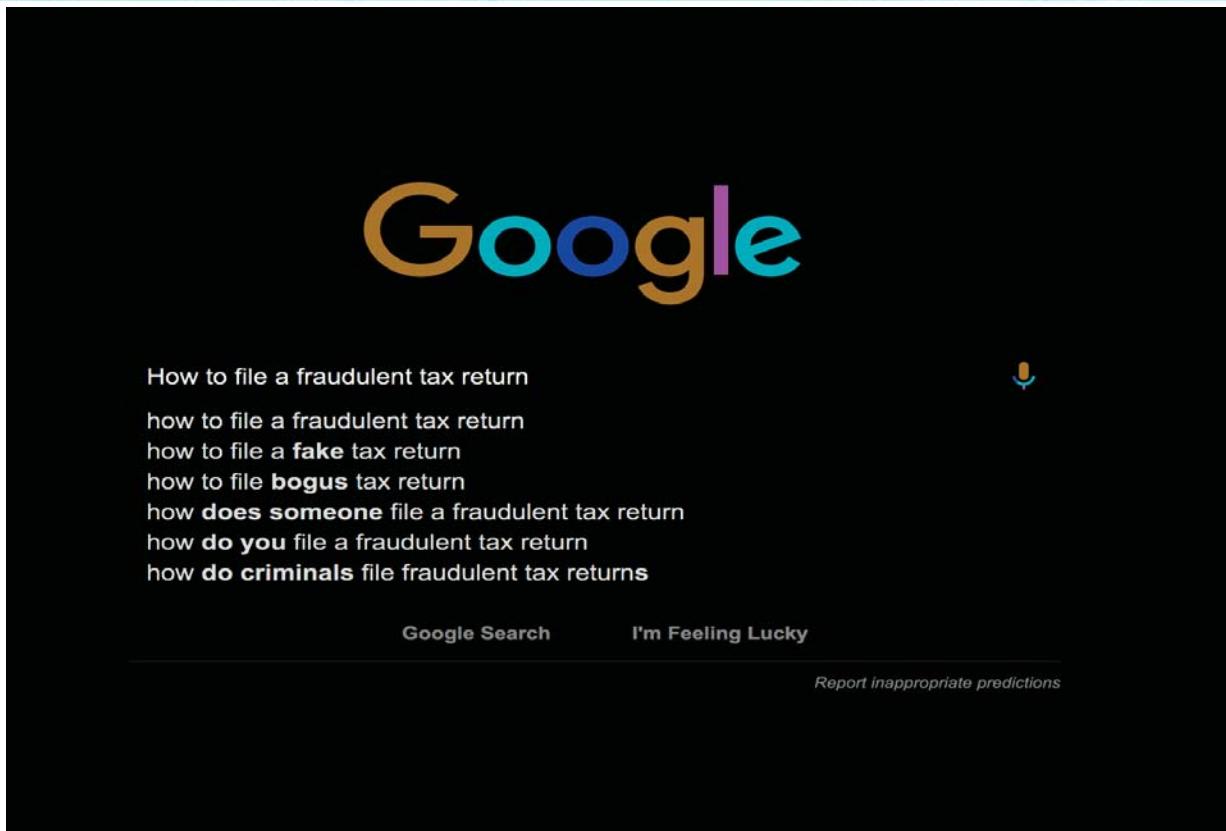
Andrei Barysevich

Director of Advanced Collection
Recorded Future
@DeepSpaceEye

Criminal Underworld Expectation



#RSAC



The image shows a Google search results page with a black background. At the top is the Google logo. Below it is a list of search queries related to filing fraudulent tax returns. At the bottom are standard Google search controls: 'Google Search', 'I'm Feeling Lucky', and a link to 'Report inappropriate predictions'. A small microphone icon is also present.

How to file a fraudulent tax return

how to file a fraudulent tax return

how to file a **fake** tax return

how to file **bogus** tax return

how **does someone** file a fraudulent tax return

how **do you** file a fraudulent tax return

how **do criminals** file fraudulent tax returns

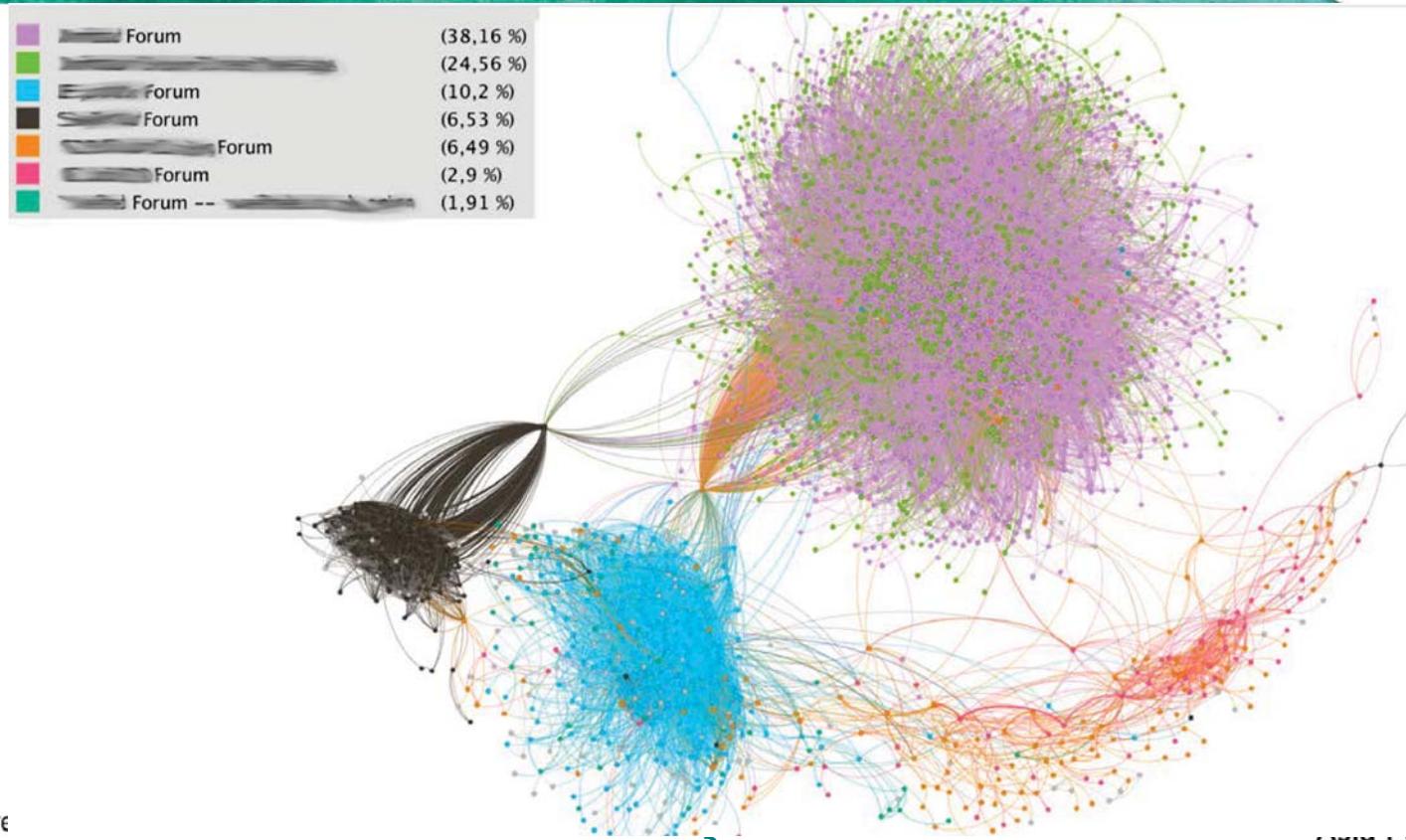
Google Search I'm Feeling Lucky

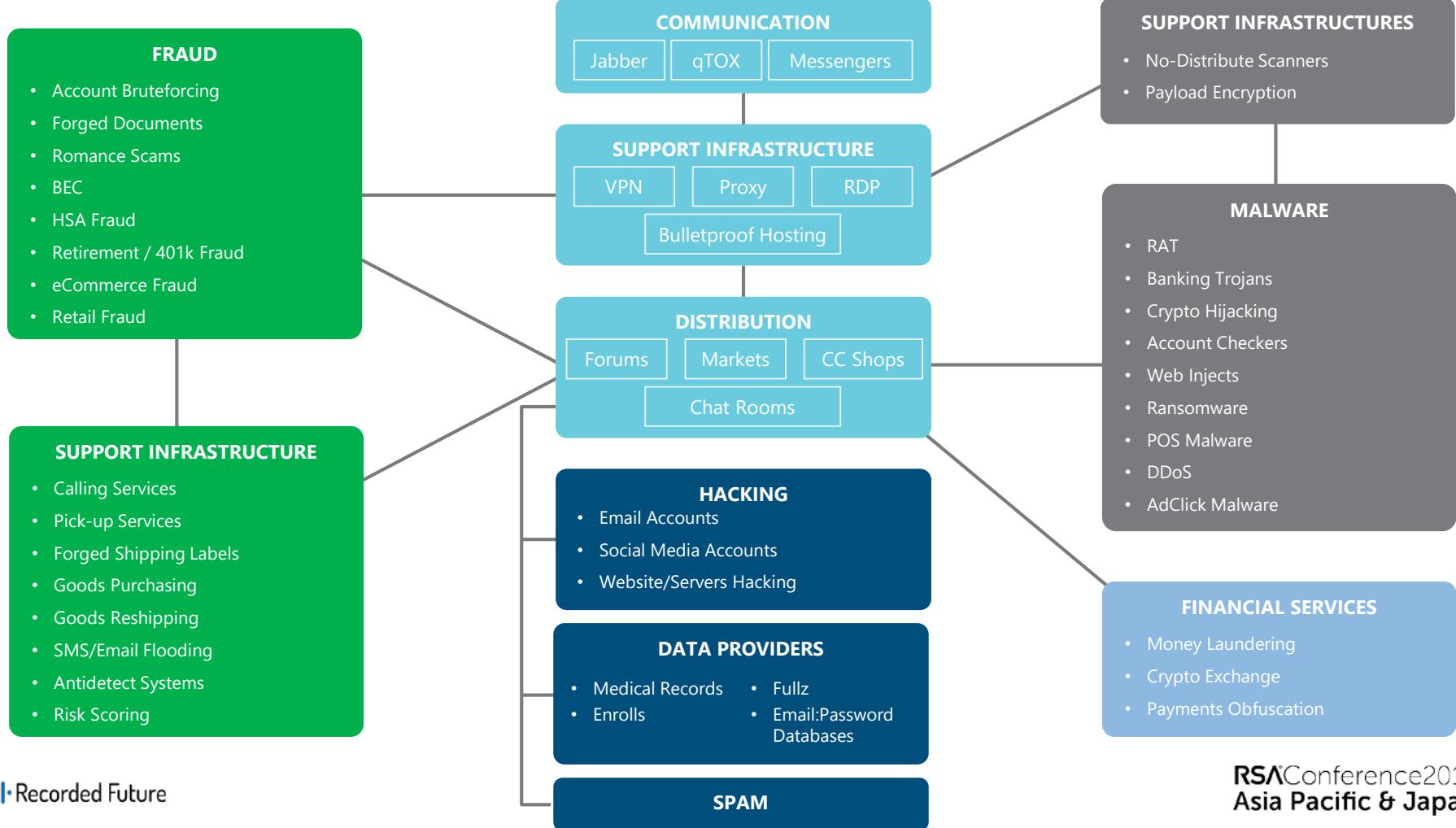
Report inappropriate predictions

Highly Segregated Criminal Underworld



#RSAC





Travel Back in Time to Understand the Cybercrime



#RSAC



e2018
Japan

Godfathers Of Modern Criminal Underground



ROMAN VEGA AKA "BOA"



DMITRY GOLUBOV AKA "SCRIPT"

Address: <http://www.carderplanet.cc/index.html>

CARDERPLANET.COM
ИДЕАЛЫ - СОЗДАНИЕ

FILES ARTICLES 00 UTILITIES FORUM ADVERTS

ЛУЧШИЕ СТАТЬИ

- Visit our new official forum
forum.carderplanet.cc
Sun Mar 07, 2004 10:26 pm
- Тонкости обмана рабочих телефонов
(для новичков)
Tue Jul 13, 2002 02:06 pm
- Комп. враг мой враг и мы учимся подиуматься
Mon Oct 23, 2002 23:24 pm
- Анти-форумные фильтры
Sun Jan 12, 2003 08:55 pm
- Виноват по работе с чеками
Thomas Cook в др. (С Вином 2003.)
Wed Sep 03, 2003 10:26 pm
- Что делать, и кто, бля, виноват? (Учебник для новичков)
Wed Aug 27, 2002 15:40 pm

ФАЙЛОВЫЙ АРХИВ

Здесь Вы сможете скачать самые последние программы, утилиты, которые помогут вам стать настоящим профессионалом, но и новичком.

ЗДРАВСТВУЙТЕ. ВЫ ЗАШЛИ НА САЙТ WWW.CARDERPLANET.COM

MEMBERS AREA

Username:
Password:

JOIN THE POWER!

Быть кардером, не просто кардером в Кардерах (с большой буквой) не так просто, но это же не признаки - это судьба.
Хочешь стать одним из нас?



ПРИСОЕДИНЯЙСЯ!

2001



VLADISLAV KHOROKHORIN AKA
"BADB"

Hard Work Has Paid Off With First Arrest in 2003



#RSAC



ROMAN VEGA AKA "BOA"

ARRESTED in CYPRUS 2003



VLADISLAV KHOROKHORIN AKA "BADB"

ARRESTED in FRANCE 2010

Some Got Very Lucky - The Epitome of Corruption



#RSAC



8

conference2018
Asia Pacific & Japan

hrabro.com

First Major Win for the Law Enforcement



#RSAC

Taken down in 2004

Address: http://www.carderplanet.cc/index.html

The screenshot shows the homepage of CarderPlanet.com. At the top, there's a banner with a globe and the text "CARDERPLANET.COM" and "НАШИ ГРУППЫ". Below the banner is a navigation menu with links for FILES, ARTICLES, UTILITIES, FORUM, ADVERTS, and MEMBERS AREA. A sidebar on the left lists "ЛУЧШИЕ СТАТЬИ" (Top Articles) with titles like "Visit our new official forum", "Тонкости обмана рабочих тем (для новичков)", "Конфиденциальность - враг мои или ученица шифрования?", and "Антифродовные фильтры". Another sidebar at the bottom left is titled "ФАЙЛОВЫЙ АРХИВ" (File Archive). The main content area features a large image of a man in a fedora and suit, and text about the site's purpose of discussing various types of fraud. A "JOIN THE POWER!" section encourages users to become members. The URL in the address bar is http://www.carderplanet.cc/index.html.

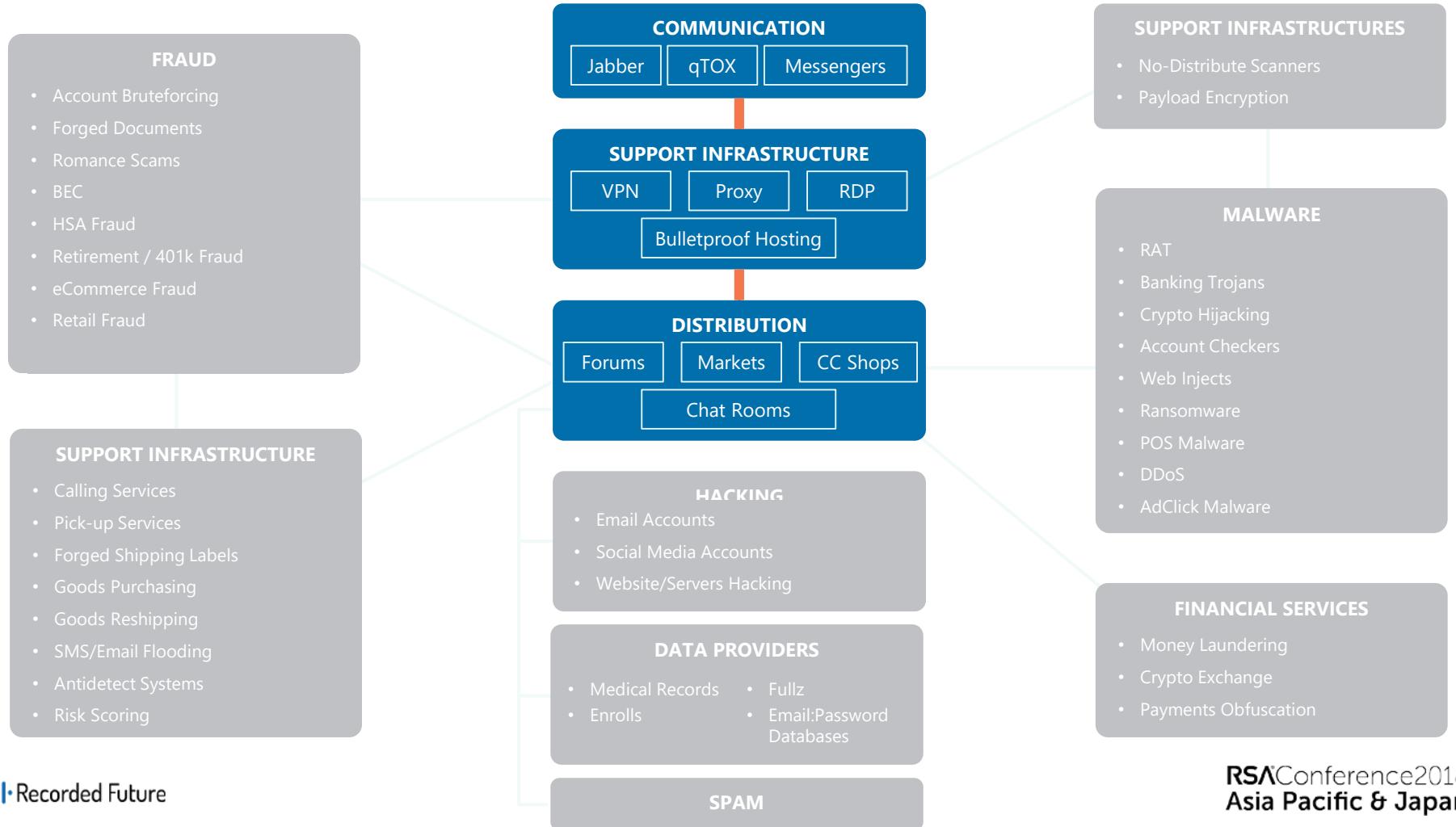
Dozens New Forums Quickly Filled the Void



#RSAC

The image is a collage of screenshots from various dark web forums and marketplaces, illustrating the rapid growth and evolution of these platforms after the shutdown of Silk Road and other major sites.

- Silk Road anonymous market:** A screenshot of the Silk Road website, showing a dark background with a car and the word "HELL". It displays a search bar and categories like Drugs, Cannabiss, Dissociatives, Ecstasy, Opioids, Precursors, Prescription, Stimulants, Art, and Botic materials. Product cards for items like Generic XANAX Alprazolam 1mg, Pure Oxycodeine HCl Powder, TESTOSTERONE CYPROTATE 250mg v10, and 25x 100mg MDMA CAPS are shown.
- LAMPEDUZA:** A screenshot of the LAMPEDUZA forum, which appears to be a political or ideological discussion board. It features a banner for "Dumps, Cards from Rescator" and a section titled "The Republic of Lampedusa".
- inFraud:** A screenshot of the inFraud forum, which is a marketplace for malware. It shows categories like Malware, Ransomware, Exploit, Trojans, and Rootkits. A prominent banner for "RESCATOR.com" and "TOystore.bz" is visible.
- DARKODE:** A screenshot of the DARKODE forum, described as "The best malware marketplace on the net". It features a dark background with a woman's face and a cigarette.
- AlphaBay Market:** A screenshot of the AlphaBay Market, a well-known dark web marketplace. It shows a search bar, categories like Sales, Messages, Listings, Balance, Orders, Feedback, Forums, and Contact, and a sidebar with user information.
- Rescator.com:** A screenshot of the Rescator.com website, which offers "Over 2.5 MILLION DUMPS ONLINE" and "FRESH DUMPS FOR SERIOUS CUSTOMERS ONLY". It features a large image of a stack of cash and a banner for "100% VALID".
- Other Dark Web Screenshot:** A screenshot of another dark web forum or marketplace, showing a list of posts and user profiles.



Credit Card “Shops” Distribute 99% of All Stolen Payment Cards



Главная Карты Проверка Финансы Новости (118) Тикеты FAQ Профиль 3.52 ⚡ ⚡ ⚡

Результаты поиска

Найдено карт 18, ваш лимит 3000

Таймаут на проверку: 0 мин. 02 сек.

(Как увеличить таймаут?)

Номер	Номер карты	Экспл	ФИО	Уровень	Тип	Банк	ЗИП	Адрес
1	4400662xxxxxx695	04/19	Nelida xxxx	SIGNATI	CREDIT <Пусто>	34741	3118 Cran	
2	4355450xxxxxx343	09/17	Dashawn xxx	PLATINI	DEBIT REGIONS B	32867	3878 Whig	
3	4336875xxxxxx415	05/16	Dashawn xxx	BUSINE	CREDIT NATIONAL # 38810	38810	3878 Whig	
4	5196673xxxxxx565	11/19	Michael xxxx	BUSINE	DEBIT SUNTRUST I	32810	7810 Alba	
5	4635761xxxxxx810	06/18	Edel xxxxxx	BUSINE	DEBIT BANK OF A	32822	7148 Curry	
6	4737029xxxxxx985	08/17	Gabriel De La	CLASSIC	DEBIT WELLS FARG	32822	3900 Pintx	
7	5107747xxxxxx308	11/19	Darryl xxxx	STANDA	DEBIT FISERV SOLU	32818	5242 Shal	
8	4339931xxxxxx361	04/17	Edsel xxxxxx	BUSINE	CREDIT FIA CARD SE	32822	7148 Curry	
9	3715550xxxxxx000	08/19	Veronica xxx	PLATINI	CREDIT BANK OF A	32806	1407 Belm	
10	3787503xxxxxx99	07/19	Tim xxxx	SMALL I	CREDIT <Пусто>	32819	2456 Com	

Service code: 1xx 2xx other Credit/Debit: credit debit
(Any) (Any)

ZIP codes (one per line): Excluding BINs (one or more per line): Excluding Last 4 digits (one or more per line):
You need better partner's rating to use this filter

Apply filters **Reset**

B#	BIN	Country	State	City	ZIP	Bank	Brand	Level	Credit?	Tracks	SCode	Price
1	406042 [-]	United States	LA	Monroe	71208 [-]	Jpmorgan Chase Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434256 [-]	United States	AZ	Phoenix	85099 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	420767 [-]	United States	LA	Baton Rouge	70883 [-]	Jpmorgan Chase Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434258 [-]	United States	UT	Riverton	62561 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434257 [-]	United States	OR	Portland	97299 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434257 [-]	United States	MN	Minneapolis	55468 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434256 [-]	United States	CA	Westminster	29693 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434257 [-]	United States	NM	Los Lunas	87031 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434256 [-]	United States	CA	Encinitas	92024 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	483316 [-]	United States	CA	Auburn	30011 [-]	U.S. Bank N.a.	Visa	-	-	TR2	101	\$5.00
1	434258 [-]	United States	TX	Arlington	22234 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434258 [-]	United States	WA	Issaquah	98029 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00
1	434256 [-]	United States	CA	Pittsburg	62974 [-]	Wells Fargo Bank N.a.	Visa	Classic	Debit	TR2	101	\$5.00

E-commerce Innovation Led to a Thriving Underground Commerce



#RSAC

ebay Shop by category Search for anything

TVs Advanced

More than 60" TVs

Shop by Category

TV, Video & Home Audio Electronics

TVs

Cable TV Boxes

DVD & Blu-ray Players

DVRs & Hard Drive Recorders

Home Audio Stereos & Components

Home Speakers & Subwoofers

Home Theater Projectors

Home Theater Receivers

Home Internet & Media Streamers

Home Satellite TV Receivers

TV, Video & Audio Accessories

TV, Video & Audio Parts

Other TV, Video & Home Audio Equipment

Additional Features see all

- 2 Port USB Hub
- Bluetooth
- Curved Screen
- Ethernet Port

Sort: Best Match View:

1-48 of 1,492 Results

Samsung QN82Q8FN 2018 82" Smart Q LED 4K Ultra HD TV with HDR QLED
FREE Fast Shipping, No Sales Tax, 20 Years on eBay
★★★★★ 1 product rating

\$3,294.95 Brand: Samsung

Free shipping 118 sold

11 new & refurbished from \$3,294.95

QLED TV

LG OLED65C8P 65" 2018 OLED 4K UHD HDR Smart TV ThinQ New
Factory sealed! FREE 4K HDMI CABLE! USA warranty!
★★★★★ 8 product ratings

\$2,495.26 Brand: LG

Free shipping 216 sold

10 new & refurbished from \$2,399.00



RUS | ENG MAIN SUPPORT ANONYMITY JABBER

Card Search Buy selected

Name	Orders	Shipping Address	Card	Buy
apple	-Lightning to USB Cable (1 m)	Adress: 4 Vine St postalCode: 01221-1222 City: Billerica Country: United States domain: gmail.com Orders: -Lightning to USB Cable (1 m)		Buy (\$4.88)
apple	-iPhone 6s Silicone Case - Lavender	Adress: 1500 Parkland Dr Unit 516 postalCode: 25414 City: Charleston County: United States domain: gmail.com Orders: -iPhone 6s Silicone Case - Lavender		Buy (\$4.88)
apple	-Apple Composite AV Cable	Adress: 819 Springdale Dr postalCode: 25302 City: Charleston County: United States domain: gmail.com Orders: -Apple Composite AV Cable		Buy (\$4.88)
apple	-Apple Developer Program - Membership for one year	Adress: 477 Smith Mill Rd postalCode: 37334-6546 City: Fayetteville County: United States domain: gmail.com Orders: -Apple Developer Program - Membership for one year		Buy (\$4.88)

Welcome, Balance: In cart: 0 (0\$)

MAKE MONEY

News Add funds PayPal WellsFargo Suntrust eBay Amazon Shopp's Profile

Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

Amazon Balance	Gift Balance	Country	Credit Card	Card Exp	Mall domain	Last order	Seller	Price (\$)
N/A	\$0	United States	+ 7/2015; 2/2018; 2/2012		@aol.com		Loquero	2.5
N/A	\$0	United States	+ 12/2016; 6/2014; 2/2011		@yahoo.com		Loquero	2.5
N/A	\$0	United States	+ 12/2014; 1/2019; 5/2015; 7/2019; 8/2017; 1/2016; 10/2013; 6/2013		@hotmail.com	March 23, 2016, \$248.30	Loquero	2.5
N/A	\$0	United States	+ 5/2019		@yahoo.com	March 19, 2016, \$229.55	Loquero	2.5
N/A	\$0	United States	+ 2/2018; 9/2016		@gmail.com	March 9, 2016, \$220.94	Loquero	2.5

Bulletproof Hosting Services



#RSAC



VPN/RDP/Proxy Providers



#RSAC

Dedicated Servers

Country: Select Country State: Select State City: Select City ZIP: Select ZIP
ISP: Select ISP OS: Select OS Resell: Yes

Direct IP: No Admin Rights: No No PayPal: No No Poker: No
Port: 80: No Port: 25: No

[Search](#) [Reset](#)

Total found: 55394
Показать: 50 [More](#)

IP	Country	State	City	ZIP	OS	RAM	Dwn.	Up.	Direct IP	Admin Rights	Added	Price, \$
83.240.*.*	PT	Faro	Alvor	8500-013	Windows 10 Pro	8 GB	6.54 Mbit/s	4.58 Mbit/s			12.6.2018	14.00
159.134.*.*	IE	Offaly	Banagher	D17	Windows Server 2012 R2 Standard	8 GB	4.74 Mbit/s	3.32 Mbit/s			19.6.2018	12.00
124.123.*.*	IN	Telangana	Hyderabad	500018	Windows 10 Pro	—	10.85 Mbit/s	7.60 Mbit/s			3.6.2018	13.00
177.66.*.*	BR	Para	Tome Acu	68680-000	—	—	—	—			4.7.2018	4.00

[Home](#) [My Account](#) [Sign Up](#) [Plans & Pricing](#) [FAQ](#) [Jabber](#) [Contact Us](#)

Global Coverage

10 серверов, разбросанных по всему миру, всегда к вашим услугам. Вы всегда сможете подобрать наиболее удобный и быстрый сервер для ваших нужд.



 RSocks

Services Apps FAQ News Company [Sign up](#) [Login](#)

RSocks Project
Secure VPN service from \$10 a month

Countries available: 42

 Residential proxy  Exclusive proxy  Personal proxy  Server proxies  VPN

Alternative Communication Channels Alongside Traditional Forums and Markets



#RSAC

14.05 [\$25] Brazil / No discount - CVV

Refund time: Dumps - 6 hours; CVV - 1 hour.

Reserve your bins in support. Enjoy the shopping!

Every Day Update / Price Reduction 10:00 am New York time.

Dan Bizerian news

THE BIGGEST DUMPS & CVV SHOP

BILZERIAN.NET

Recorded Future

Dan Bizerian news

Web : bilzerian.net / bilzerian24.net

CONNECT TO DISCORD

makerhacks

THIS WILL ALLOW MAKERHACKS TO

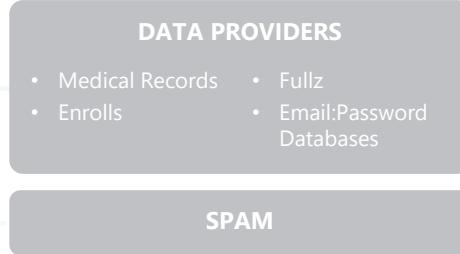
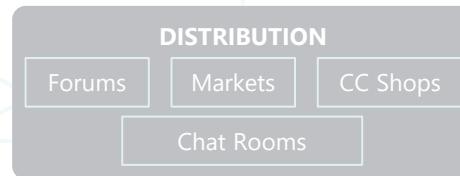
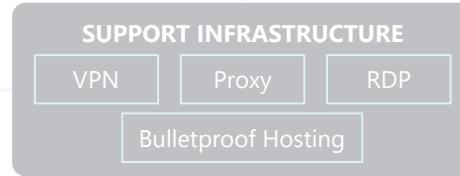
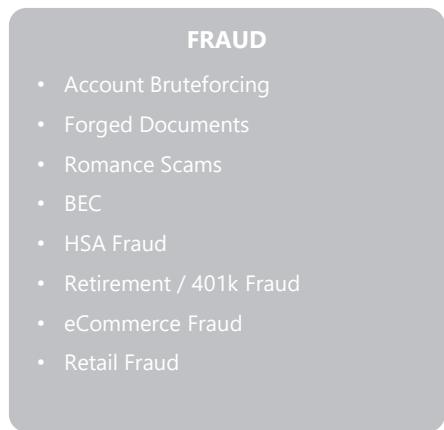
Add a bot to a server
This requires you have Manage Server permission on the server.

Select a server

Have an existential crisis
WHO AM I?

This application cannot read or send messages on your behalf.

[Cancel](#) [Authorize](#)



Banking Trojans Are Common. However, Not as Much as Before



Red Alert 2.0 Cyber attack against Android

SEP

19
2017

Red Alert 2.0: New Android Banking Trojan for Sale on Hacking Forums

The Red Alert 2.0 is currently targeting victims in
Android 6.0 (Marshmallow) and previous versions."

Source [Romanian Security Team... Forums](#) on Sep 1

<https://rstforums.com/forum/topic/100481/red-a&comment=653967> • Reference Actions • 1+ refer

Django administration

WELCOME, ADMIN. VIEW SITE / CHANGE PASSWORD / LOG OUT

Home | Curd | installed apks

Add installed apk +

Select installed apk to change

Q Search

Action: ----- Go 0 of 100 selected

CREATED AT	UPDATED AT	DELETED AT	BOT ID	APK NAME
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.android.chrome
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.apps.magazines
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.youtube
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.play.games
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.android.vending
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.apps.plus
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.whatsapp
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.talk
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.imm.android.imoin
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.videos
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.pierwiastek.gpsdata
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.flashplayer
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.apps.docs
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.cleanmaster.security
2017-05-29 22:40:45	2017-05-29 22:40:45	-	c9406df6-371f-40e7-ab46-443e6b001160	com.google.android.apps.maps

FILTER

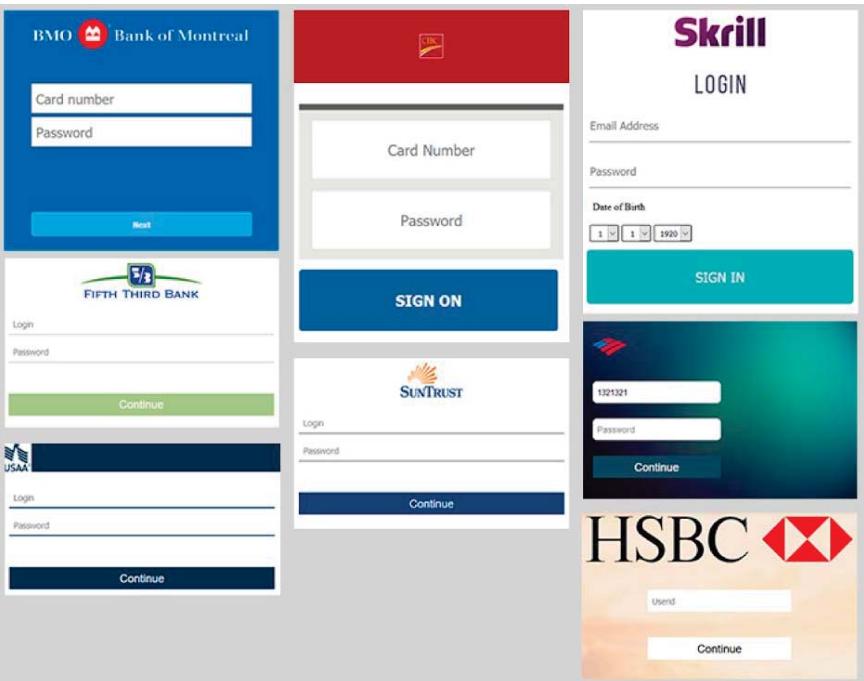
By created at

Any date
Today
Past 7 days
This month
This year
No date
Has date

Credentials Theft Has Shifted From Web To Mobile



#RSAC



The slide shows two examples of mobile banking security challenges:

Capital One: Step 3 of 3. Your account is temporarily locked. We have detected something unusual about this sign-in. For example, may be you signing in from a new location, device, or app. Before you continue, additional verification with security questions is required. Your Challenge Response was invalid. Please verify your response and try again later. Please review the links below to continue your application.

TD Bank: America's Most Convenient Bank. Help & Related Tasks: Help, Privacy and security, View our terms, Online Services Agreement. Security Challenge: For security purposes, please confirm your identity by answering the following question. What is your mother maiden name? Answer: [Redacted] Submit.

Payment Card Compromises Is a Huge Problem (Despite EMV)



JackPOS

Welcome, admin
Log Out

Home Page
View all general Information.

Dumps
Check all dumps.

Bots
Manage all bots.

Settings
Change account settings.

Bot Control

Version Control

Version	Update URL	Delete
Mozilla/4.0 (com	<input type="text"/>	<input type="checkbox"/>

Online Bots

Hardware ID	PC Name	IP	version	last seen on
qWPDP13e	ACERV5	192.168.1.11	Mozilla/4.0 (com	[REDACTED]

Last 12hr Bots

Hardware ID	PC Name	IP	version	last seen on
				Activate Windows Go to PC settings to activate Windows.

Market for Stolen Credit Cards is Stronger Than Ever

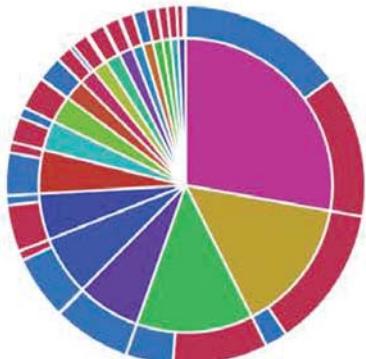


CNP - Number of Records

20,419,177
Count

CNP - Number of Records Sold

16,830,532
Count



CP - Number of Records

47,876,852
Count

CP - Number of Records Sold

24,081,902
Count

Total Cost

1,062,646,441.01
USD

Total Cost - Sold

507,015,806.43
USD

-
- A donut chart showing the distribution of total cost by card type. The chart has three concentric rings. The innermost ring is green, the middle ring is orange, and the outermost ring is blue. A legend on the right side lists the card types with their corresponding colors.
- VISA
 - MASTERCARD
 - AMERICAN EXPRESS
 - DISCOVER
 - MAESTRO
 - CLASSIC
 - PLATINUM
 - SIGNATURE
 - STANDARD
 - GOLD
 - GREEN
 - CONSUMER CARD
 - CONSUMER PREMIUM
 - GIFT
 - LOWES CARD
 - ATM CARD

Ransomware Remains a Major Source of Income



#RSAC

The screenshot shows a search result for "karmen" on the Dark Web. The results include event information, file samples, sessions, statistics, indicators, and domain, URL & IP address information. A specific file sample is highlighted, showing its WildFire verdict as Malware and its SHA256 hash. The file is a PE executable named "GandCrab" with the tag "InitialSystemDataEnumeration". The file size is 320,000 bytes.

First Seen	WildFire Verdict	SHA256	File Size (Bytes)	File Type	Tags
02/23/2018 8:41:18am	Malware	faf9d96ada73110222d3403f2045d49ad932bd1ac8973192ceb70beb30622e	320,000	PE	GandCrab InitialSystemDataEnumeration
02/23/2018 1:00:44am	Malware	fab9c32dd3ce81ae1ccb133fb7989e29b88e8417018171e3bbfe57188962883d	353,280	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 9:31:28pm	Malware	82087a5f07c87a002a74f89e6e561280de950b0da1d86ef3689e5579c56347b	352,768	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 6:20:25pm	Malware	c75b0744080211db127c917afe0c8459c7b41a8145e8ee410c3960ecd26e3884f	278,016	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 1:55:57pm	Malware	d5854fc6624593c0cae1e36ae#f9706ec2b702e5ca7057ee754265c8723c4cf	352,256	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 7:06:47am	Malware	56360f82d26c04bed4715992c663c5d1870d5eb62f412bf2cef0fc61008a	342,528	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 6:16:33am	Malware	82bf36400e914fd133b90105d389a99d29c07fe0320ff723be92c976309	249,079	PE	GandCrab NetSupportManager SelfExtractingExecutable
02/22/2018 5:45:35am	Malware	7a8cf8c9e31599eac9d873870b1272ba302a9b2d43a66632f582666c34a39e6	342,528	PE	GandCrab InitialSystemDataEnumeration

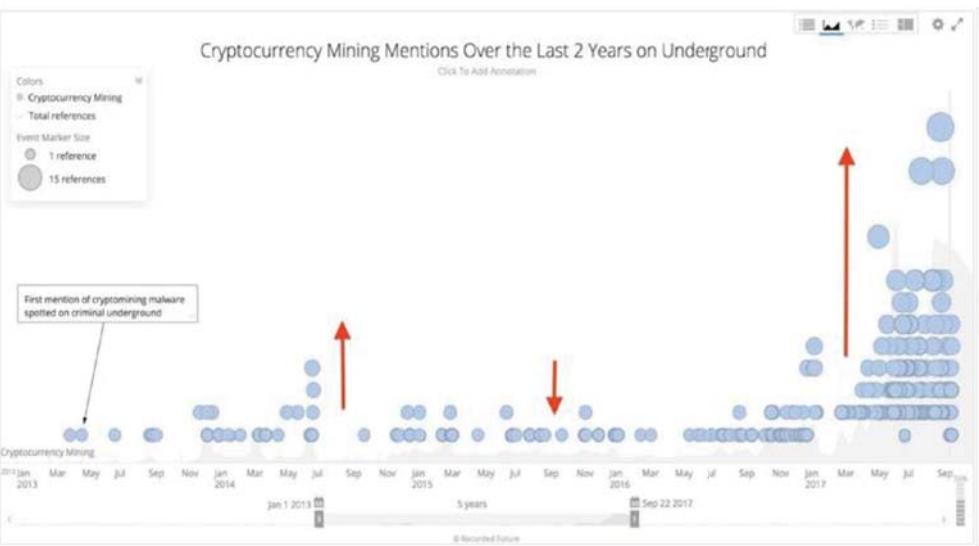
The ransom note is titled "Karmen" and displays the message: "Files encrypted". It instructs the victim to send Bitcoin to the wallet address 3B2f36400e914fd133b90105d389a99d29c07fe0320ff723be92c976309. It also offers to decrypt files automatically. A warning at the bottom states: "Interference with the program - can leave you without files." The note includes language selection buttons for DEU and ENG, and a payment amount field set to 0.00000000.

First Seen	WildFire Verdict	SHA256	File Size (Bytes)	File Type	Tags
02/23/2018 8:41:18am	Malware	faf9d96ada73110222d3403f2045d49ad932bd1ac8973192ceb70beb30622e	320,000	PE	GandCrab InitialSystemDataEnumeration
02/23/2018 1:00:44am	Malware	fab9c32dd3ce81ae1ccb133fb7989e29b88e8417018171e3bbfe57188962883d	353,280	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 9:31:28pm	Malware	82087a5f07c87a002a74f89e6e561280de950b0da1d86ef3689e5579c56347b	352,768	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 6:20:25pm	Malware	c75b0744080211db127c917afe0c8459c7b41a8145e8ee410c3960ecd26e3884f	278,016	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 1:55:57pm	Malware	d5854fc6624593c0cae1e36ae#f9706ec2b702e5ca7057ee754265c8723c4cf	352,256	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 7:06:47am	Malware	56360f82d26c04bed4715992c663c5d1870d5eb62f412bf2cef0fc61008a	342,528	PE	GandCrab InitialSystemDataEnumeration
02/22/2018 6:16:33am	Malware	82bf36400e914fd133b90105d389a99d29c07fe0320ff723be92c976309	249,079	PE	GandCrab NetSupportManager SelfExtractingExecutable
02/22/2018 5:45:35am	Malware	7a8cf8c9e31599eac9d873870b1272ba302a9b2d43a66632f582666c34a39e6	342,528	PE	GandCrab InitialSystemDataEnumeration

Crypto Hijacking Has Replaced Ransomware (For Now)



#RSAC



RAT Malware is Affordable and Readily Available



#RSAC

The screenshot shows the RingRat v1.2 interface. On the left, a sidebar has "Home", "Settings", and "About" buttons. The main area has tabs for "Server ID", "File Manger", "Camera", "Record", "Contacte", "SMS", "App Installer", "History", "Location", and "Mobile". Below these are two package options: "PACKAGE 1 SERVER ONLY" (\$10) and "PACKAGE 2 CLIENT + SERVER" (\$40). Both packages include "Server (.apk) fully configured" and "Client (.exe)". Payment methods shown are Ethereum and Bitcoin. A "PURCHASE NOW" button is at the bottom of each package card.

RingRat v1.2 ,Onlines{0} Port _

Home Server ID File Manger Phone Model Country Android V...

Settings

About

File Manger Camera Record Contacte SMS App Installer History Location Mobile

PACKAGE 1 SERVER ONLY \$10

PACKAGE 2 CLIENT + SERVER \$40

Server (.apk) fully configured Client (.exe)

PURCHASE NOW PURCHASE NOW

Ethereum Bitcoin

Perfect Money

CONTACT TO PURCHASE VIA PERFECT MONEY [EXTRA FEES]

The screenshot shows the WxDosX RAT Server interface. It displays "Connected (1)" and "Server port: 33831". Buttons for "Start server" and "Stop server" are present. To the right, a window titled "WXRat" shows "Client version: 1.6" and "Server version: 2.1". It lists support channels: "Jabber: wdosx@fuckav.in" and "Telegram: @wdosx".

WxDosX RAT Server

Connected (1)

Server port: 33831

Start server Stop server

WXRat

Client version: 1.6
Server version: 2.1

Support:

- Jabber: wdosx@fuckav.in
- Telegram: @wdosx

Non-Distribute AV Scanners Help Keep Malware Undetected



VIRUSCHECKMATE
Fastest comprehensive analysis

Check API Videos Tariffs Affiliate Sign in

Sign up!

Fastest analysis

High speed get partial and full results the scan. Special superfast methods for server-side usage.

Full anonymity

All cloud services are disabled manually. All scanned objects are removed immediately.

Usable report

Most informative results page, both antivirus and for each of the objects to be scanned.

Clever API

Crafted API, giving wide scope when using server-side checks. [More info..](#)

Smart auto scans

No runs by cron! Rescan in antivirus was updated. Continuously watching an object.

Many great apps

Variety of clients, from simple command line to ending DLL library and plug-in.



Main

API

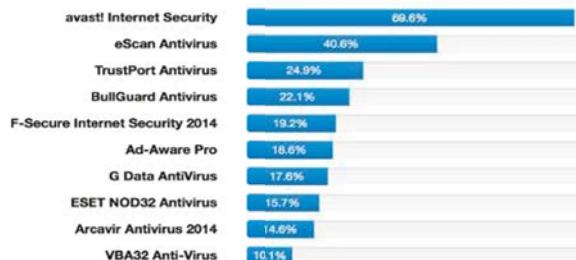
Plans

Terms Of Service

FAQ

Contacts

TOP 10 Ranking Antiviruses



* The rankings based on available statistics and calculated by the formula where the total number of detections divided by the total number of checks

... still looking for other the comparative factors? We can give you more information

dyncheck.com
Dynamic AV checker

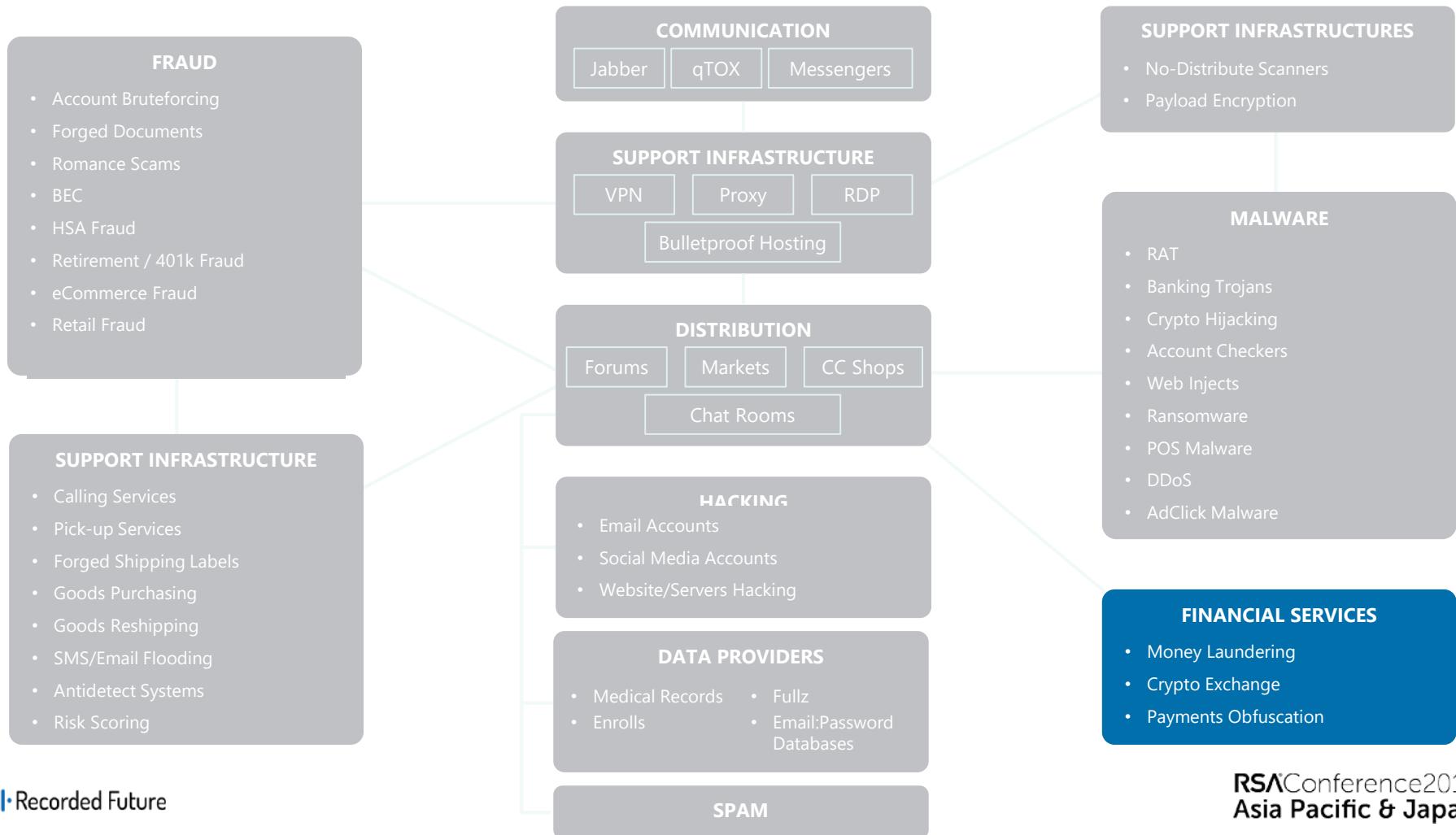
Read more

Sign up

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#).

Recorded Future

RSAConference2018
Asia Pacific & Japan



Money Laundering is Imperative to the Criminal Economy



Need Bank transfer partner. I have fresh bank drops.

Hello fellow thieves

Looking for partner who can successfully make **bank transfers** to newly opened **Bank** of America, suntrust, or capital one **bank**. All cashing out will be handled on my side, and payment will be sent via btc, litecoin, or ether same day. Only those who have serious experience at **transfers** please contact via pm.

Note: For all security and authenticity in business, I am more than welcome to working through moderators, and escrow service.

Thanks.

Ищу обнал нон вбв Японии!!

сабж. репа депозит,гарант...

желательно люди с мерчами. вищевуха не интересна и авиа пока что тоже.

мой % не менее 30%. сроки выплаты индивидуально.

looking for cashout cc non vbv Japan

deposit escrow etc.

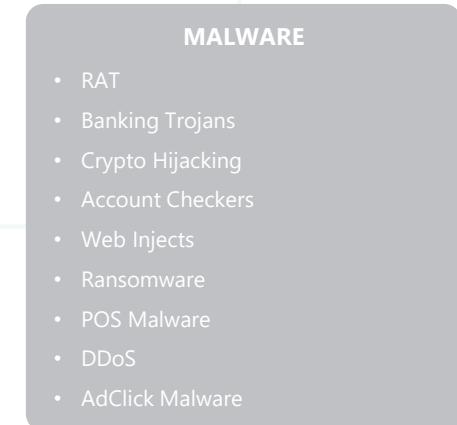
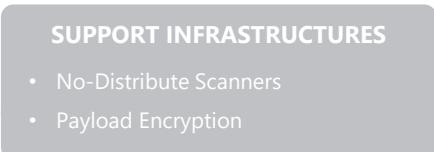
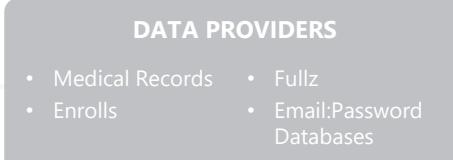
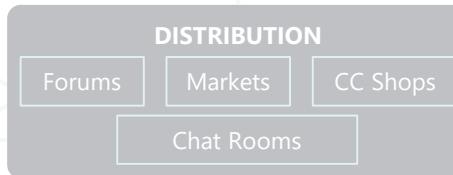
PM

Drops in Colombia under Western Union, Remitly, XOOM. We work only with carded transfers
50/50

Payouts within 1-2 hours.

Payment by status withdrawn / within an hour at the rate of XE.com

Mon-Sun 17.00-00.00 Moscow time

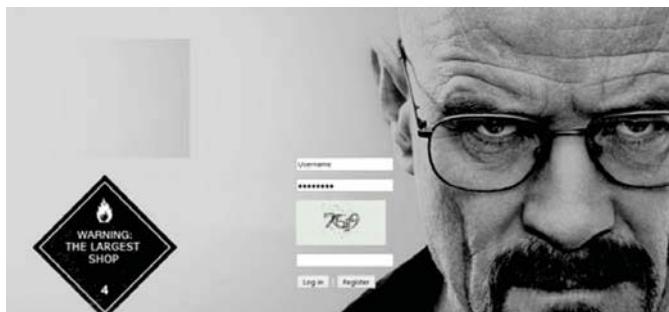


Online Fraud is the Centerpiece of the Dark Web



#RSAC

```
beat3136@a.toshima.ne.jp yama5252  
question@kenban.com yWxUuaLA7I  
takeo@p2222.nsk.ne.jp 7pezu3h  
blog2233@yahoo.co.jp kichan03  
iowa666@andex.ru zambidis  
occhii808@gmail.com lion8080  
castillofrank10@yahoo.com lolmaster1253  
pioneer18@hotmail.com wang6327543  
heiwakankouservice@helen.ocn.ne.jp xqB1hh3LDv  
s501_hj66@yahoo.co.jp uchihiroki  
hiro Miyake@com.home.ne.jp tomyoshi  
pupepo...aya..03_30@docomo.ne.jp 19850330  
xf522ux_k4.7a_xb916ox@softbank.ne.jp boku0916  
hukutoku508@ezweb.ne.jp hukutoku508  
bfzsu3u43@za.ztv.ne.jp yukiivii  
m9i3y8@bma.biglobe.ne.jp po89po89  
sakura43@sea.plala.or.jp xxjdmxdx4  
bcwct397@yahoo.co.jp PYM40TH1II  
jag1060@02.246.ne.jp lqXenadv
```



RSAConference2018
Asia Pacific & Japan

If You Can't Defeat Them, Work With Them



#RSAC

checkIP.ru
check IP on fraudulent

CHECK IP NOW! Check risk shipping address Free utilities Balance: 193 credits [valid till 30 Apr] My Account Logout

Check Billing/Shipping Address

Please enter IP, billing and shipping address you want to check. Try to fill as much as possible

IP address:	108.41.226.114	Shipping address:	2313 Frankford Ave
Billing City:	belmar	Shipping City:	Philadelphia
Billing Region/State:	nj	Shipping Region/State:	pa
Billing Postal/zip code:	07715	Shipping Postal code:	19125
Billing Country:	usa	Shipping Country:	usa
Phone number	212-409-1210	Submit	Reset

Page tips

i Billing and Shipping address fraud risk
Enter billing, shipping address, phone number and IP address of buyer to know a risk of fraud.

IP	Country	Distance (?)	Risk ShippAddr (?)	Billing PostMatch (?)	Shipping PostalMatch (?)	Phone in postal (?)	Anonymous	ProxyScore (?)	Risk Score (?)
108.41.226.114	United States (US)	62 km.	No	Yes	Yes	No	No	0.00	32.00%

Need To Confirm a Bank Transfer? No Problem!



sparta
Vendor of:
call service
dating calls



sparta is offline
Join Date: 04.09.2011
Posts: 190
Deposit: 0\$ 2
Trust Limit: 0\$ 2

Позвон от носителей: EN,DE,IT,FR,ES,PT,PL от 8\$
ВНИМАНИЕ ТУТ КИДАЛА!!! SPARTA@JABBER.DK RIPPER/КИДАЛА!!!
РЕЗЕРВНЫЙ ЖАББЕР SPARTA@JABBER.SCHA.DE

УСЛУГИ ПОЗВОН СЕРВИСА
дропов, шопов, банков и казино

UK (м/ж голос, носитель языка) + датинг
US (м/ж голос, носитель языка) + датинг
DE (ж голос, специалист) + датинг
FR (ж голос, специалист) + датинг
IT (ж голос, носитель языка) + датинг
ES (м голос, носитель языка) + датинг
PT (м голос, специалист)
PL (м голос, специалист)

EN - \$10 DE, FR, IT, ES, PT, PL - \$12
SPARTA@JABBER.AT

УСЛОВИЯ

- ✓ Сервис не несет ответственности если вы дали не полные данные для осуществления звонка
- ✓ Сервис не несет ответственности за отсутствие звона, если вы сами понимаете, есть много фактов
- ✓ Звонок только после предоплаты для нас
- ✓ Оплата принимается в PM/Webmail
- ✓ Мы не принимаем звонки если время ожидания превышает 24 часа
- ✓ Мы не звоним заказы которые прямо связаны с РУ или СНГ
- ✓ Повторный перезвон считается как новый звонок

F-CALL
SERVICE

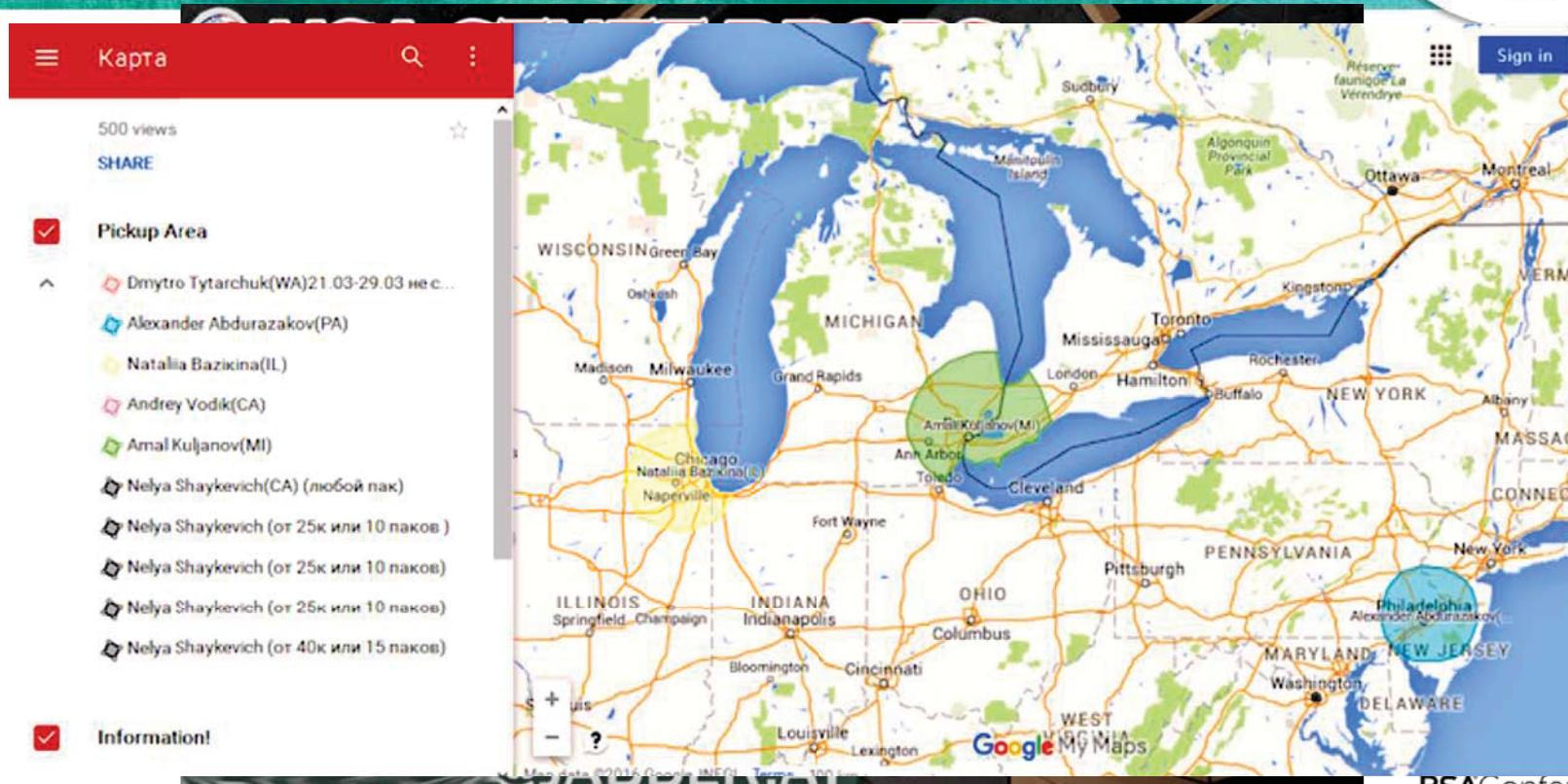
ПОЛНОСТЬЮ АВТОМАТИЧЕСКИ

MADE IN RUSSIA

Well Developed Network of the Shipping Mules



#RSAC



Automated Call/Email Flooding Services are Used to Hide Unauthorized Transactions



#RSAC

МылOFF Flood archive News Referral program Balance: 10.00\$ [Email](#) [RU](#)

Flood

Email Total Work time (hh:mm) In progress 0\$ Add Current time: 2016-04-26 01:20:39

Email	Sent	Time	Job	Actions
@mail.com	1017	Done in: 190518 4...	1000 inbox mails in 00:05 Start time <input type="button" value="Start time"/>	Stopped

Advanced Custom Made Browser Antidetect Software



Session setup

Create new session provider

NEW Session name:

If you want to copy current session, please enter new session name. notice, that old session will saved in bar.

comments:

Load anonymity checker after setup
 Enable HTML5 local storage
 Save HTML5 local storage data

Network connectivity settings

No proxy

Enable fake webRTC leak Proxy connection ip and proxy ip are same Disable webRTC

Useragent client settings Chrome Safari MSIE Other

Mozilla/5.0 (iPhone; CPU iPhone OS 10_0 like Mac OS X) AppleWebKit/602.1.38 (KHTML, like Gecko) Version/10.0 Mobile/14A300 Safari/602.1

Disable popups Enable service worker
750

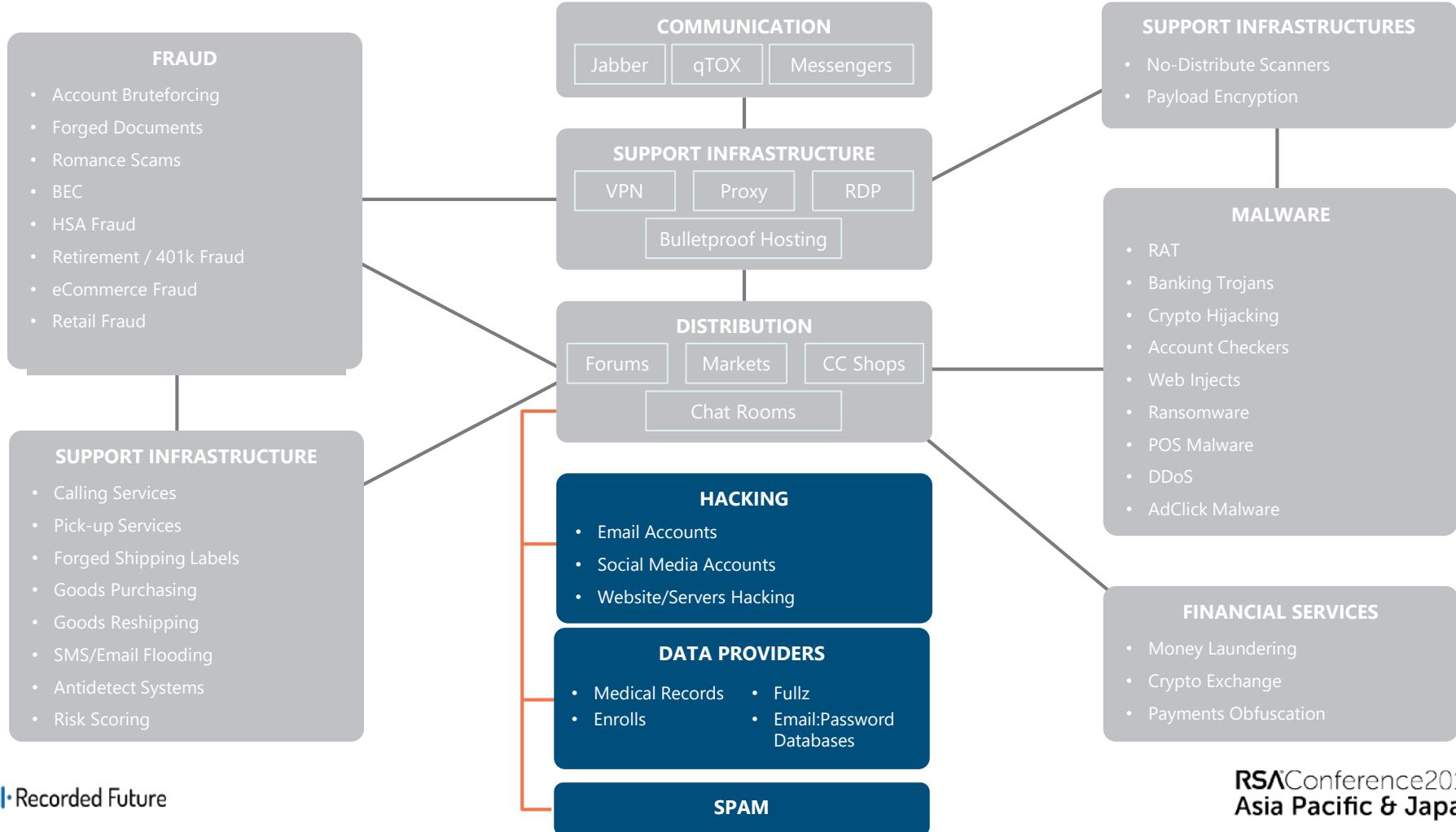
Emulate screen resolution Emulate touch screen

Latitude

GPS position works only with custom data, when fields of coords are not empty.

Fingerprint, plugins and other settings

Enable unique canvas fingerprint Enable unique rects fingerprint Enable flash (WARNING: It's not safe!)
 Enable unique audio fingerprint Use custom plugins and mimeTypes Use dynamic fingerprints
 Enable unique fonts fingerprint Save and encrypt cookies before exit Block canvas output



Hacking Services is the Essential Part of the Underground



Scammed Blue Cross Blue Shield Health Care Card

▲ ← → ▾

#RSAC

I Am Offering Legits Hack Service and Hacking Tools, CCV, CC, PayPal, WU, MG, Fullz

x

Posted [REDACTED] Forum

Posts in thread 20

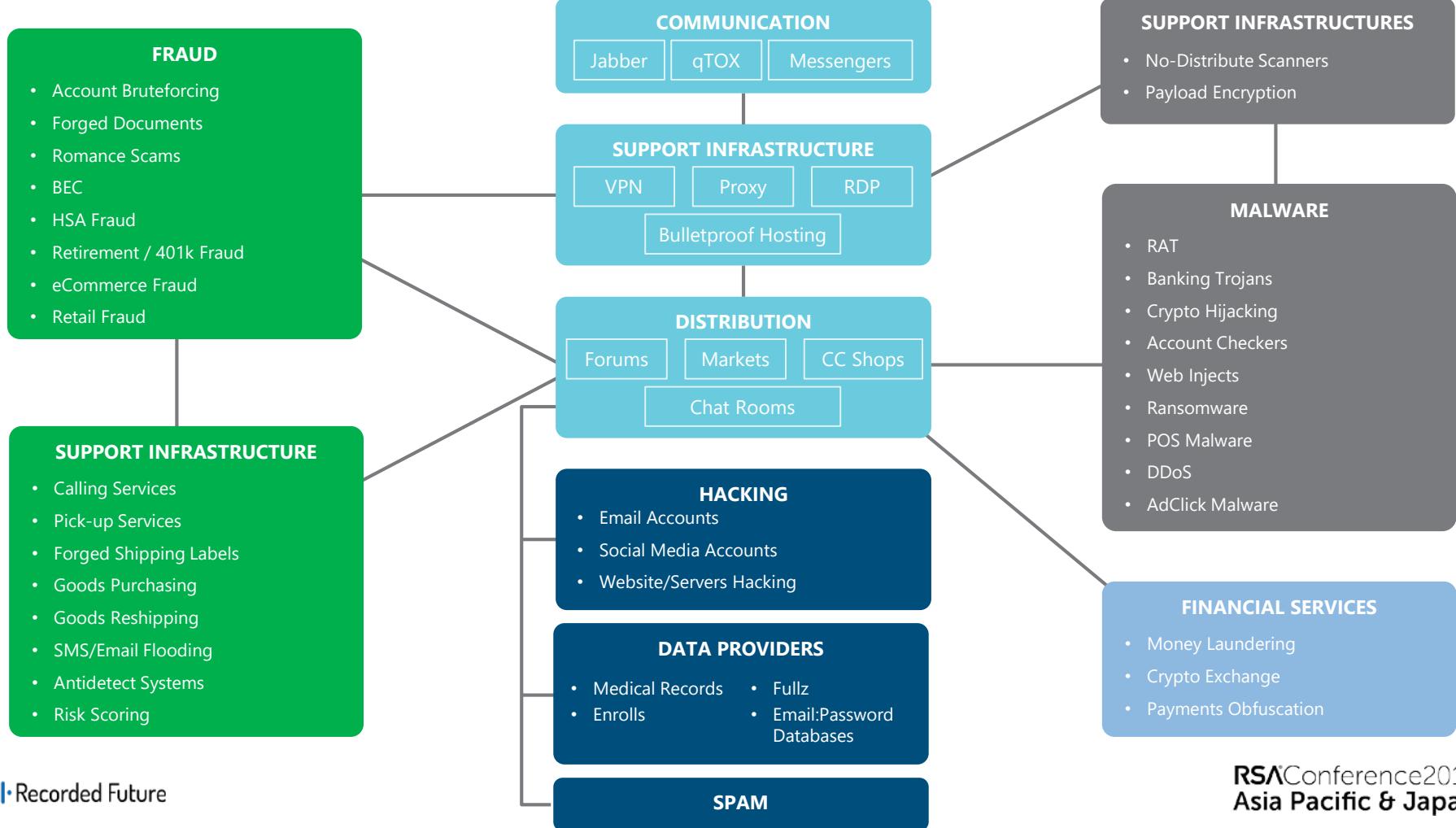
First posting Apr 15 2018, 00:17

Most recent posting Jun 18 2018, 18:45

Previous 50 Next 50

Do you need to keep an eye on your spouse by gaining access to their emails? As a parent do you want to know what your kids do on a daily basis on social networks. Also introducing: Introduction to **Ethical Hacking**, Different **Kinds of Games** and Software hacking, Games server files + database, **Social Engineering**, Scanning Networks, Evading **IDS**, Firewalls, and **Honeypots**, Sniffing, **Hacking Mobile Platforms**, **Hacking** Web Applications, **Hacking** Web servers, **Hacking Wireless** Networks Cloud - Threats & Opportunities, Malware Threats, **Session Hijacking**, **SQL** Injection, Enumeration, **Denial of Service**, Footprinting and Reconnaissance, System **Hacking**. I'm a Professional seller, more than 6 years experience, I have sold **cvv** credit card to many customers all over the world. I give proofs of jobs both past and presents and I also have 100% money return warranty.

Post 8 of 20 by [REDACTED] on Apr 15 2018, 00:25



Overwhelming Daily Volume of Activity



#RSAC

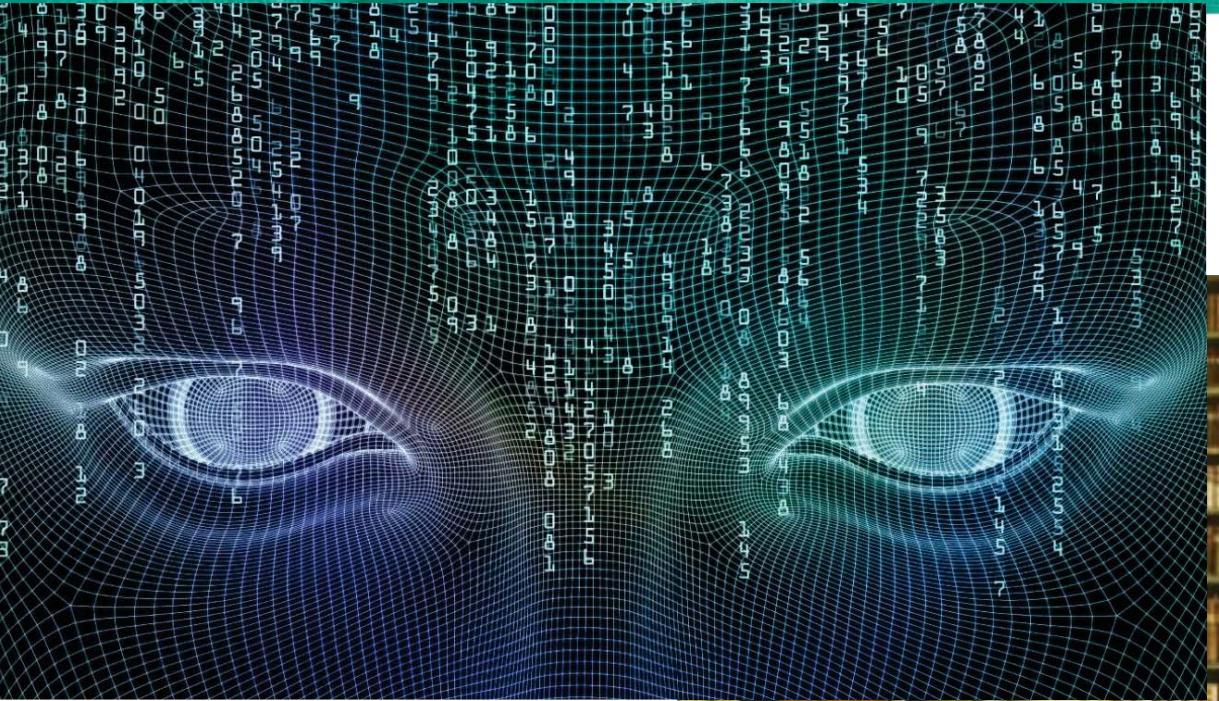


Dark Web - All

Click To Add Annotation



Success = Symbiosis of Manual Research + Technology



Be Calm and Get Threat Intelligence



- Not every company has equal exposure on the dark web.
- Intel teams have the different skill levels and appetite for information.
- Can they handle semi-processed or raw data feed, or would they rather receive a finished intelligence only?
- How will you measure the success or failure?