

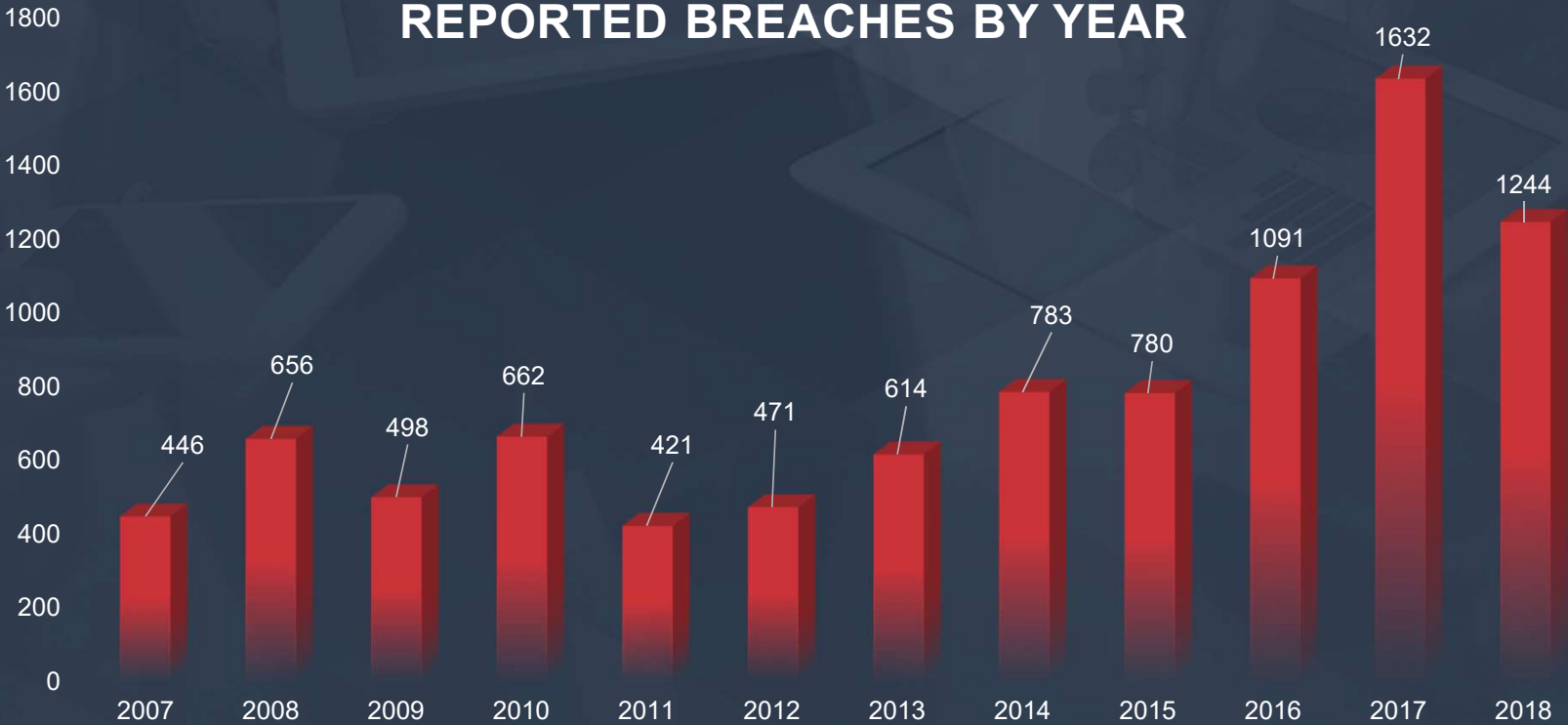
Dark Web: More Connected More At Risk

Addressing Cybersecurity Concerns
for Your Organization

May 7, 2019



Latest Statistics Show Less Breaches



Everyone needs a trusted advisor. Who's yours?



However, the Impact is More

2017

1,632 breaches reported

197,612,748 exposed records

2018

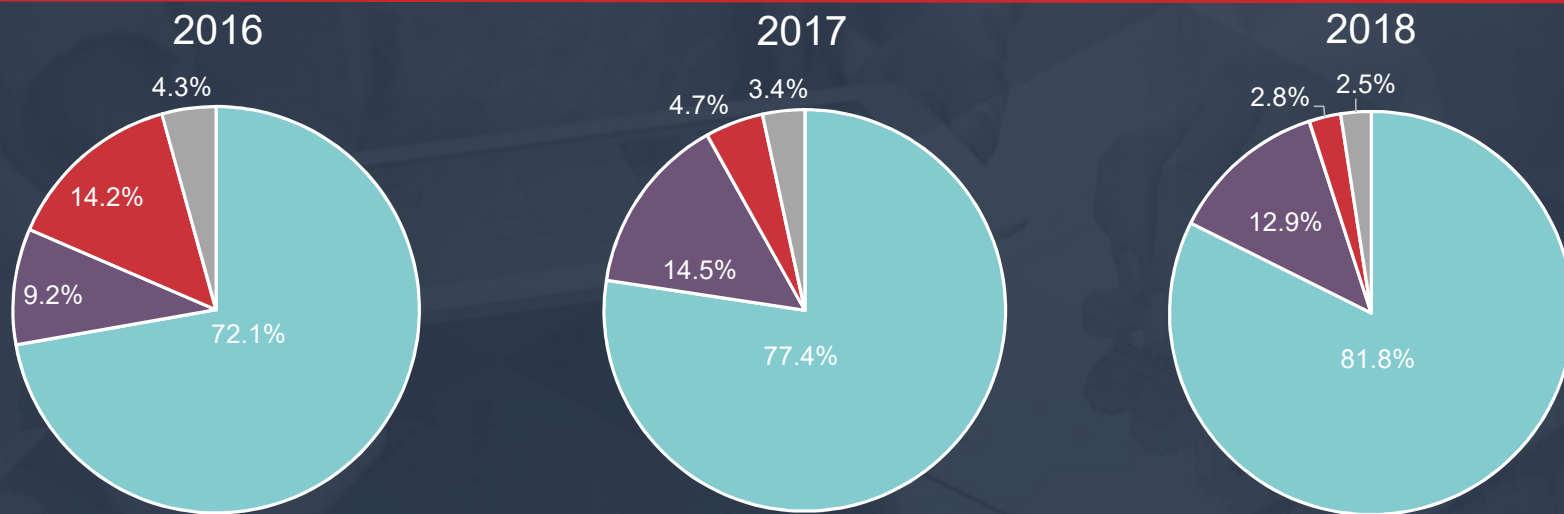
1,244 breaches reported

446,515,331 exposed record

*2018 had over 2.25 times more records
exposed in 76% of the number of breaches*

Cyber Crime is Still the #1 & Growing

Motivations Behind Attacks



- Cyber Crime
- Cyber Espionage
- Hacktivism
- Cyber Warfare

Source: Hackmageddon, <https://www.hackmageddon.com/2018-master-table>

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Breaches Are Costing More & More

Average total cost
of a data breach
\$3.86 million

Up from \$3.62 million

Average cost per
lost or stolen
record
\$148

2017 was \$141

Likelihood of a
recurring breach
within two years
27.9%

27.7% last year

Mean time to
identify a breach
197 days

Mean time to
contain
69 day

Average cost
savings with an
IR team
\$14/record

*Companies that
contained a breach in
less than 30 days
saved more than \$1
million vs. those that
took more than 30 days
to resolve*

Source: Ponemon Institute 2018 Cost of Data Breach Study

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

The Dark Web

What it is, & what it isn't

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

What is the “Dark Web”?

- Less than 10% of the internet is accessible through typical search engines
- The **Deep Web** is a part of the web that contains the most sensitive information
- The **Dark Web** is the part of the deep web that is intentionally hidden
- Requiring an *anonymizer* to access (ex. Tor)
 - Uses .onion link; links often shift
 - **Tor** – The Onion Router
 - **The Black Market of the Internet!**



Source: CISO Platform

<http://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different>

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

What Can I Find on the Dark Web?

Commercial Services

- CStore - The original CardedStore ☞ - Ele
- Apple Palace ☞ low priced Apple Product
- Gold & Diamonds ☞ Genuine Gold, Diam
- Football Money ☞ - Fixed football games
- Mobile Store ☞ - Factory unlocked iphone

Drugs

DREAM MARKET is a SCAM!! REMEMBER THE NAME!! AND NEVER USE IT!

- Alphabay Market ☞ - Anonymous
- Drug Market ☞ Anonymous mark
- Drugs4You ☞ - Drugs and Medic
- Oxycodone, Tramadol, and a lot
- ONION PHARMA ☞ - Pharmacy
- Weed&Co ☞ - Weed / Cigarettes
- CannabisUK ☞ - UK Wholesale C
- Green Road ☞ - Biggest market
- MOMAEurope Mail Order Mariju
- Green Dragon UK ☞ - Cannabis
- EuCanna ☞ - First Class Cannab
- Peoples Drug Store ☞ - The Dark
- Smokeables ☞ - Finest Organic C
- CannabisUK ☞ - UK Wholesale C
- DeDope ☞ - German Weed and H
- EU Drugstore ☞ - Best EU Store
- BitPharma ☞ - EU vendor for coc
- Brainmagic ☞ - Best psychedeli
- NLGrowers ☞ - Coffee Shop grad
- OnionShop ☞ - New anonymous
- Drugstore ☞ - Marketplace with a
- The Pot Shop ☞ - Weed and Pot
- EU Cocaine ☞ - selling Cocaine,
- Weed Store ☞ - well-known deep
- Steroid King ☞ - All the steroids
- Dream Market ☞ Anonymous ma
- Wacky Weed ☞ - Hi Quality Gre

ADULT

- VideosME ☞ - Webcam videos 1
- Cafe Sweet Teens (4-18) ☞ Cam

Phoenix Forum

Home Help Search Login Register

Phoenix Forums

Pineapple (or not)

Pineapples?
A space for all the pineapple themed o
Pineapples: usability, cka

General Category

General Discussion
Feel free to talk about anything dankis

Resources

Harm reduction, DNM's, security forums

- The Hub
- Blackhole
Replacement for The Hub
- The hubs backup
Backup of the hub until 02/03/2016.
- Dread
CLEARNET reddit link; Olympus nazi paid off a dodgy admin and redirected to their own forum

Dream Market

- Browse by category
- Services 4913
 - Hacking 622
 - IDs & Passports 762
 - Money 797
 - Other 633
 - Cash out 1241

- Digital Goods 50771
- Hacking 622
- Drugs Paraphernalia 337
- Services 4913
- Other 3381

Exchange

Bitcoin	1.5
Bitcoin	1000.0
BCH	7.3
JMR	44.7
USD	7544.1
EUR	6496.1
GBP	5716.7
CAD	9343.1
AUD	5708.0
INR	7301.0
SEK	6827.0
NOK	6247.0
DKK	4827.0
TRY	32018.2
CNH	49245.2
HKD	63968.0
RUB	48740.3
INR	51602.5
JPY	81368.4

Onion mirrors

IDs & Passports (762)

Filter

Ships to: Ships from: Escrow: Category: Cryptocurrency:

Price: Searchtext: Sort by: Vendor:

Apply Filter

10 Spanish IDs \$0.00643

South Carolina Drivers License Template \$0.001654

CardPass (250) (4.65★) WW -- WW

only (14000) (4.74★) GB -- WW

BROWSE CATEGORIES

Fraud	40744
Drugs & Chemicals	221359
Guides & Tutorials	14345
Counterfeit Items	8281
Digital Products	16196
Jewels & Gold	1637
Weapons	4172
Carded Items	3666
Services	7282
Other Listings	3640
Software & Malware	3130
Security & Hosting	758

Forum

Одобрение кредита с плохой КИ

ВТБ24

Фальшивые 5000р для банкоматов!

Техника Apple за 40% от стоимости

- Важно: СС халива (1 2 3 4 5 ... Последняя страница)
- ZloY
- Важно: Халива: мыла, фты, аккунты и прочее...
- [Other] Andamx Keylogger
- IP Ranges
- Empire Team
- DB dumps
- iprozn
- Продам сканн driver id, medical id usa only.
- ce500
- ellin (icq 635990025 / life@sj.ms)
- ellin
- Важно: Приватный софт. (1 2 3 4 5 ... Последняя страница)
- Алашу
- Гюка
- Важно: [Понск] Музыка (1 2 3 4 5 ... Последняя страница)
- Проблемы с vlv
- Сонягор
- [Radioshow] - 22.04.2011 радио эфир
- blzrlh
- [France] Armin van Buuren - A State of Trance
- КарТайп 04eviDn0c-T
- [FAQ] Взлом Девянов (1 2 3 4 5 ... Последняя страница)
- Gladiato
- [Radioshow] - alex.kaz vs. КарТайп 04eviDn0c-T alcohol vol.3 (25.03.2011) (1 2 3 4)
- КарТайп 04eviDn0c-T
- [Radioshow] - D] GrinGoD - Ночь перед Рождеством... (6.01.2011) (1 2 3)
- ЗАДНИЦА

Everyone needs a trusted advisor. Who's yours?



Types of Sites on the Dark Web

Forums

Discussion forums that cover information that could be useful to a hacker

- Common vulnerabilities
- Information about organizations

Search Engines

Just like regular search sites, but for the dark web

Marketplace

Anything is for sale

- Drugs
- Stolen credit cards
- Personal identities
 - Passports
 - Driver's licenses
 - Health insurance cards
- Other compromised information
- Dates

Paste Sites

Large data dumps that are never removed

Social Media/Chat Rooms

A place for hackers to share information more privately

Some Items for Sale

Directv Account with NFL SUNDAY TICKET MAX

Vendor kingshot (3200) (4.72★) (@ 388/3/16) (📍 1307/25/25)
Price ₱0.00489 (\$18.72)
Ships to Worldwide
Ships from Worldwide
Escrow No



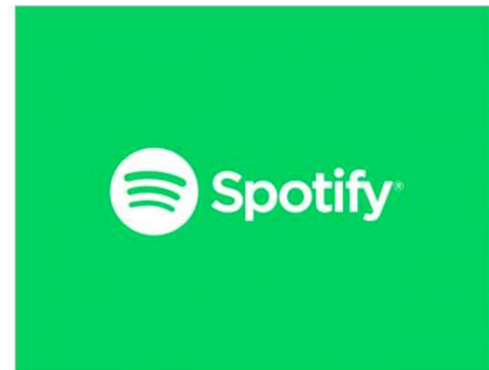
Product description

"Directv goes everywhere you go. Stream live TV, access shows and movies On Demand, 100s of channels to choose from."
Account with NFL SUNDAY TICKET MAX subscription guaranteed

Buy this account now for a fraction of the price.
-High Quality
-Fast delivery

Spotify - premium account - lifetime

Vendor K2000 (780) (4.90★) (@ 119/0/2)
Price ₱0.001358 (\$5.2)
Ships to Worldwide, Worldwide
Ships from Worldwide
Escrow Yes



Product description

Spotify - premium account - lifetime

Your purchase includes:
- Full Access to premium account.
- Lifetime warranty

Username and Password are sent via PM.

All images are actual screenshots from the dark web

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Fake Insurance Card



Forged Auto Insurance Card - Allstate

This is a listing for a forged auto / car insurance card or proof of insurance. In addition to this item being forged car ins...

Sold by **namedeclined** - 0 sold since February 13, 2018 **Vendor Level 1** **Trust level 1**

Product Class	Features	Origin Country	Features
Quantity Left	Physical Package	United States	World Wide
Ends In	Unlimited	Ships to	Escrow
	Never	Payment	

Priority Domestic - 4 days - USD + 8.00 / order

Purchase price: **USD 60.00**

Qty: 1 **Buy Now** **Buy Now** **Buy Now** **Queue**

0.014957 BTC / 0.975134 LTC / 1.104769 XMR

Description Feedback Refund policy

Forged Auto Insurance Card - Allstate

This is a listing for a forged auto / car insurance card or proof of insurance. In addition to this item being forged car insurance it also will work for motorcycles as well. This is about the size of a credit card and is laminated by the heat seal method and is water proof. It is from Allstate insurance company (check my listings I also do State Farm and Geico insurance cards). The card will have all necessary info on it and will be double sided. It will come in versions for all 50 U.S. states. I can do any form of insurance other than just auto insurance, so if you want another form, request it and I'll get it posted for you and other users to enjoy and purchase. These are excellent to avoid traffic tickets, avoid getting your vehicle towed, avoid having to appear in court for traffic tickets, avoid 100s even 1,000s in potential fines, use these to supplement assuming a false identity, falsely portray the owner of a stolen vehicle, get tickets dismissed that you already got and still have time to fight, use it as a non-photo form of ID for opening a PO box using another fake ID with this and many more uses. Also keep in mind if your car gets towed or impounded for not having proper insurance they will immediately search your car, or do it at the impound lot and may find items you don't want found. With that said if you have pills buy my forged Rx labels to protect from that. When cars are at impound lots they have all kinds of legal liability notices saying "We are not responsible for any lost, stolen, or damaged items in your vehicle. This means they will steal everything. I have even heard of gas being swiped from the tank. These literally have always sold themselves. With this purchase you will get two copies of the insurance card. Both cards will have the same info on them. I will not put different info on each card; you must place an additional order if you want different info.

Here is the order form and info I will need to make you your card.

STATE TO BE INSURED IN:
NAME(S) TO BE ON CARD:
ADDRESS TO BE ON CARD:
YEAR OF CAR:

All images are actual screenshots from the dark web

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

**How Much
Could I Get for
Your Credit
Card On the
Dark Web?**

About \$1

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Carding Forum

 **Joker's Stash**
Write & Swipe
News
Dumps
Cards

DUMPS UPDATE (HIGH VALID)
GEXE (fresh skimmed base) : USA (NY state + few EU) TR1+TR2/TR2, HIGH VALID 99-100%,
uploaded 2018-05-25
TIME FOR REFUNDS: 3 HOURS (GOLD USERS 12H, SILVER 9H, BRONZE 6H)
GEXE db random dumps valid test (try2services checker):

CC info	Auth code	Auth result	Amount	Void	Merchant location
517803XXXXXXXXXX-2030	00	Approval	7.13	OK	64579-ME-SAGADAHOE-WOOLWICH
440668XXXXXXXXXX-1001	00	Approval	2.73	OK	60119-IA-SASPIR-BELLOGG
473752XXXXXXXXXX-2039	00	Approval	3.48	OK	62380-IL-BANKOOK-WEST POINT
643048XXXXXXXXXX-2010	00	Approval	1.20	-	59628-MT-STILLWATER-FISHTAIL
441297XXXXXXXXXX-2039	00	Approval	7.31	-	28712-NC-TRANSYLVANIA-BREVARD
379730XXXXXXXXXX-20592	00	Approval	9.60	-	96837-MI-HONOLULU-HONOLULU
422620XXXXXXXXXX-2107	00	Approval	8.70	OK	76580-TX-BAYLOR-SEYMOUR
410030XXXXXXXXXX-2012	00	Approval	4.27	OK	72850-AR-BRANCY-MARSHALL
438857XXXXXXXXXX-1812	00	Approval	2.12	OK	12472-NY-GREENE-DURHAM
440668XXXXXXXXXX-2037	00	Approval	8.85	OK	07052-NJ-ESSEX-WEST ORANGE

DUMPS UPDATE (HIGH VALID)
TARAMBA (fresh skimmed) : USA (CO,GA,IL,MI,VA,NJ,NC,MT,CA,LA,FL,TX,+ few EU) TR2 ONLY,
HIGH VALID 90-95%, uploaded 2018-05-25
CO,GA,IL,MI,VA,NJ,NC,MT,CA,LA,FL,TX,MD,KS,TN,NV,NM,WA,
MO,DC,UT,PA,CT,WI,WY,DE,WV,MN,AZ,OH,OR,AL,IN,NY,NE,KY,
VT,SD,IT,ND,MA,SC,IA + few EU/ASIA
TIME FOR REFUNDS: 3 HOURS (GOLD USERS 12H, SILVER 9H, BRONZE 6H)
TARAMBA db random dumps valid test (try2services checker):

CC info	Auth code	Auth result	Amount	Void	Merchant location
403310 [-]					USA - Sagadahoc
471283 [-]					United States - SC - Summerville
071282 [-]					United States - AL - Opelika
434257 [-]					United States - NE - Lincoln
131517 [-]					United States - NM - Albuquerque

Filter
Base: **Leads - MAGNUM (fresh skimmed base) : USA (states min) TR2 ONLY, HIGH VALID 95-100%, uploaded 2017-04-01 (time for refunds: 3 hours)**
(Any)

Price (USD)
\$ - \$

Tracks:
TR1+TR2 or TR2

Expiration date (YYYYMM, one or more per line):
Unabled due to security reasons (protection against low performance staff lockups)

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

Apply Filter Reset

Add everything on this page to cart - 1 items - News

Bank	Brand	Level	Credit?	Tracks	S-Code	Refundable?	Price	
[-]	Us. Bank Na	Yes	-	TR2	101	Yes	\$1.00	
[-]	Wells Fargo Bank Na	Yes	Classic	Debit	TR2	101	Yes	\$1.00
[-]	Us. Bank Na	Yes	-	TR2	101	Yes	\$1.00	
[-]	Wells Fargo Bank Na	Yes	Classic	Debit	TR2	101	Yes	\$1.00
[-]	Wells Fargo Bank Na	Yes	Classic	Debit	TR2	101	Yes	\$1.00
[-]	Wells Fargo Bank Na	Yes	Classic	Debit	TR2	101	Yes	\$1.00

Joker's Stash is the most popular "carding" forum on the dark web. Credit cards, just \$1 each!

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

All images are actual screenshots from the dark web

Carding Forum

Browse by category

- Services 6182
- Hacking 887
- IDs & Passports 1093**
- Money 1038
- Other 883
- Cash out 1516

- Digital Goods 57018
- Drugs 64959
- Drugs Paraphernalia 296
- Services 6182
- Other 4997

Onion mirrors

ptisz6dxboul2u3z.onion verified

jd6yhucwivehvd4.onion
t3e6iy3uolf4zcw2.onion
7ep7acrkunzdcw3l.onion
vlpqabmvizecjo.onion

Forged Blue Cross Blue Shield Health Care Card

Vendor namedeclined (1150) (4.88★) (@ 92/1/1) (M #6, 10/10) (👉 29/0/0)

Price \$0.00998 (\$62.400000000000006)

Ships to Worldwide

Ships from United States

Escrow Yes



Health insurance card sold for just over \$62



Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Health Insurance Card for Sale

Product description

This listing is for a forged Blue Cross Blue Shield health insurance card / proof of insurance card. These cards are printed double sided and are plastic heat laminated cards. They are waterproof and you will get two cards with the order; both cards will be identical and the second is just a spare or back up in case the first is lost, stolen, damaged, has a defect or is ceased. The back of the card will scan with all the proper info so if real info is used it will show up in the system, or even smart phone applications may be used to scan and read the back of it. These are used to provide proof that you have health insurance in the United States (BCBS may exist outside the US and can be forged to be used outside the US). This item works very well as a back up form of ID to pair with a fake drivers license or fake passport or even one of my forged drivers license, social security cards, auto insurance cards, or school IDs. When using a fake ID or assuming a fake identity it is best to not have a wallet that has simply cash and a fake drivers license only. Having a forged health care card and other forged IDs of mine along with maybe a prepaid debit card from your local store sell your cover identity. If your fake ID is questioned this can be pulled out to back it up and eliminate any question, it may save you. In addition it may be used as a secondary form of ID to open up a PO box under a false identity and fake info. Keep in mind that the post office does not cross check the info you provide them when opening a PO box they merely take down the info that they view on your IDs and log it in the computer. They do not have the power to access BCBS databases to verify nor do they verify any of the info. If say by chance you are able to steal info about a real BCBS insurance policy you may use that info and get a fake from me and use that policy and assume that persons policy, possibly even get a few visits covered before they catch on.

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Hackers for Hire

Government is chasing me - Need Help



@uniter 6 мес. назад

I've been extensively chased by the government for 7 months now... I'm writing this, not interested in a debate or needing to vindicate what I'm claiming. And before this gets to a discussion about my sanity. I am not schizophrenic or any type of mentally ill. Very sane in fact... All of this is happening as described. I am telling nothing but the truth and I am ONLY writing this because I have to reach out to a community of people that can some-what understand .

I am not writing this for attention, or for any sort of egotistical getting my rocks off sort of thing. I'm hoping some open minded people will respond to this because I really need help in the ways that I'm asking.

I desperately need help. I've been running from them for 6-7 months now, chased across north america from coast to coast twice now without money, without food, no resources. It's been hard...

I cannot name the names of the agencies doing this or WHY this is happening, but there are multiple groups working together in different capacities spearheaded by one agency specifically in charge of this all. Please don't ask, that's all I can say.

When this all started, it was just them watching me mostly - and fucking with me / all the people that I was involved with. Trying to intimidate me and my friends. They were Deleting tax records, bank accounts, social's, etc. Stalking and breaking into our houses, etc.

All my friends / people I knew were hacked into from the nsa and we were all being monitored by agencies outside of the nsa who were working with the nsa to use their technology to track us and monitor everyone. The people closest to me were on high priority watch lists and anyone that was involved with what I was doing / knew. Were being attacked the same way that I was. A few of us had / have our lives at stake right now.

Rent-A-Hacker

Products FAQs Register Login

Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my business since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last + 20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:

Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.
Im a professional computer expert who could earn 50-100 euro an hour with a legal job.
So stop reading if you dont have a serious problem worth spending some cash at.
Prices depend alot on the problem you want me to solve, but minimum amount for smaller jobs is 200 euro.
You can pay me anonymously using Bitcoin.

Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successful, if i dont know it, ill learn it very fast
- Anonymity, noone will ever find out who i am.

Social Engineering skills:

- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt believe really often.
- Alot of experience with security practices inside big corporations.

What ill do:

- Ill do anything for money, im not a [redacted] if you want me to destroy some bussiness or a persons life, ill do it!
- Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods.
Economic espionage
Getting private information from someone
Ruining your computers, bussiness or private persons you dont like. I can ruin them financially and or get them arrested, whatever you like.

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

How Are You Targeted?

Things to look out for...

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Attackers Try Easiest Way to Penetrate

- Phishing/spear phishing
- Social engineering
 - Job opportunities
 - Accounts on LinkedIn, Facebook
- Malware campaigns
- SQL injections on websites
- Public Wi-Fi

The screenshot shows the Dream Market website interface. The main content area displays search results for 'Wi-Fi FREE'. The results are organized into a grid of items, each with a red 'Wi-Fi FREE' icon and a price tag. The items are:

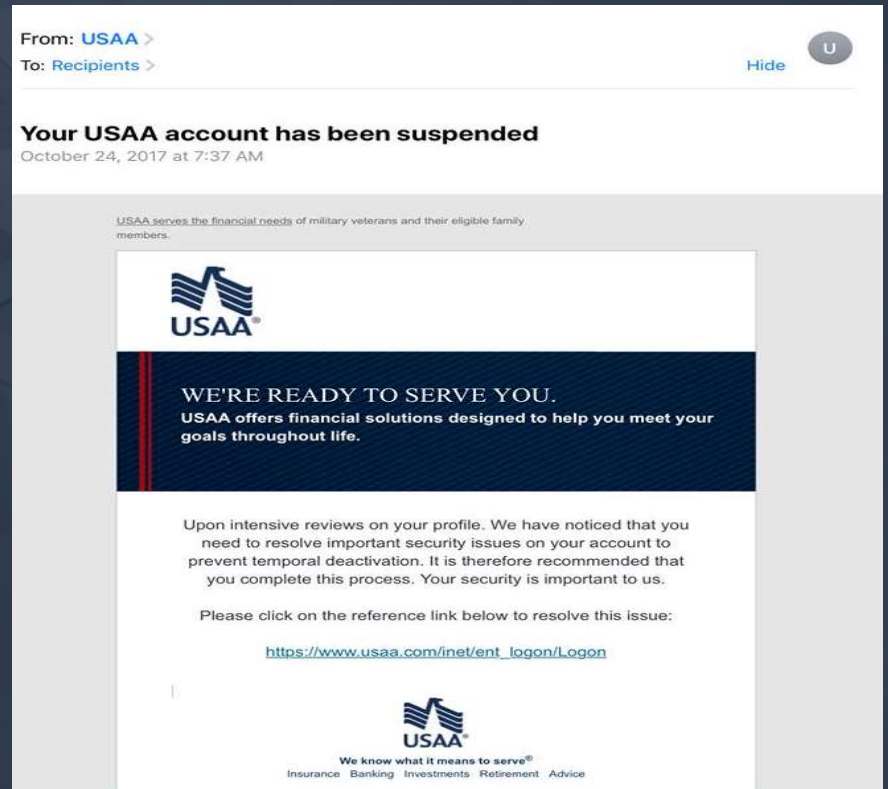
- THE BEST PRO WIFI HACKING TOOLS PACK 2018: Price \$0.000687, 5400 reviews, 4.82 rating.
- THE BEST PRO WIFI HACKING TOOLS PACK 2017: Price \$0.000687, 5400 reviews, 4.82 rating.
- THE BEST PRO WIFI HACKING TOOLS PACK 2017: Price \$0.000687, 5400 reviews, 4.82 rating.
- ACCESS ANY IPHONE BYPASS CODE: Price \$0.001378, 12000 reviews, 4.71 rating.
- NOOB-TO-EXPERT HACKING COURSE [FROM A-Z]: Price \$0.001102, 6000 reviews, 4.69 rating.
- THE BEST PRO WIFI HACKING TOOLS PACK 2018: Price \$0.000687, 5400 reviews, 4.82 rating.

The left sidebar contains navigation links for various categories: Безопасность и взлом, Вирусологии, Wardriving & WiFi, IM мессенджеры, Социальная, Анонимность, Криптографы, Спам, рассылки, and Деньги. The top navigation bar includes 'Shop', 'Messages: 0', 'UltraManNogo', and a search bar.

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

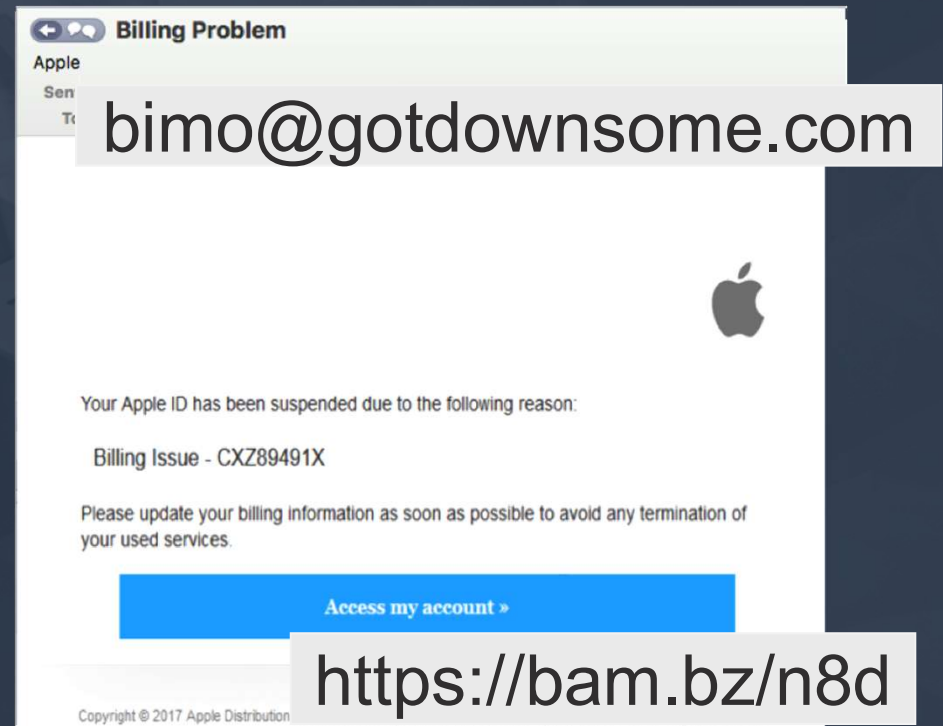
Phishing Schemes are Most Popular



Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Always Check...

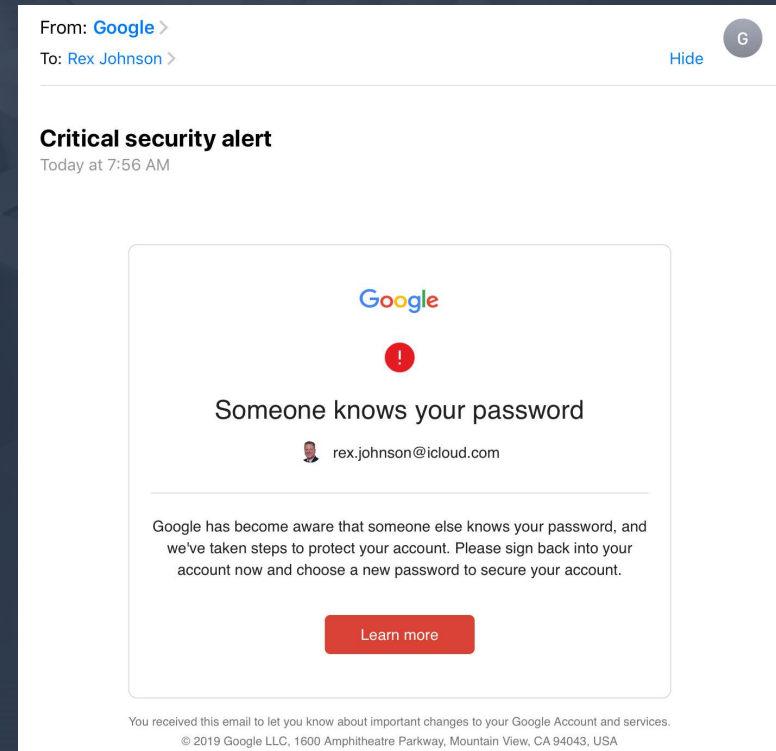


Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Some Emails Are Legitimate, but...

- Never select the link in the email
- Call or go to a site that you know is official

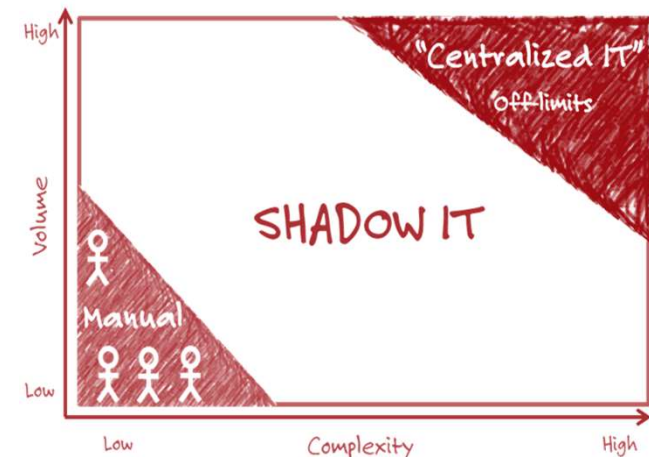


Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Shadow IT

- Shadow IT refers to IT devices, software & services outside the ownership or control of IT organizations
- Departments will often do this to
 - Circumvent bottlenecks
 - Avoid slow processes
 - Rely on familiar software
 - Compatible with mobile devices
 - Work with legacy applications that are no longer supported
- It is easy to attain software as a service (SaaS) solutions



Source: Gartner IT Glossary, <https://www.gartner.com/it-glossary/shadow>

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Risks of Shadow IT

- Rutter Networking identified
 - Increased risk of data loss
 - Increased risk of data breach
 - Inefficiencies
 - Cybersecurity risks
- Since acquired outside of IT procurement channels, security is often overlooked
- Gartner predicts that by 2020, a third of all successful attacks will be against their shadow IT resources

Source: <https://www.rutter-net.com/blog/4-security-risks-of-shadow-it>



Everyone needs a trusted advisor. Who's yours?

BKDCYBER

What Would a Hacker Take?

Knowing how a hacker would
compromise your environment

Everyone needs a trusted advisor. Who's yours?

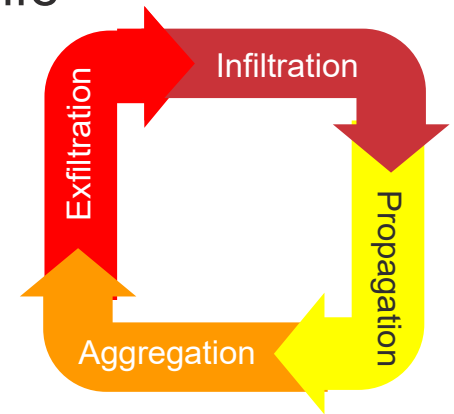
BKDCYBER

Red Team Digital Attack Simulation

- An attack simulation that mimics the real activities a hacker would take in your environment.
- Still provides the network penetration testing results
- Collects data and information a hacker would want
- Ability to place notional malware and threats
- Also known as Purple Team or Digital Attack Simulations

Breach Life Cycle

- Attacks are generally carried out in four stages
- These four stages are often referred to as the “breach life cycle”
- The further the progression, the greater the risks
 - Infiltration: breaking in & establishing foothold
 - Propagation: in the network & moving around
 - Aggregation: collecting data & critical information
 - Exfiltration: taking the information outside of the organization



Breach Life Cycle in Action

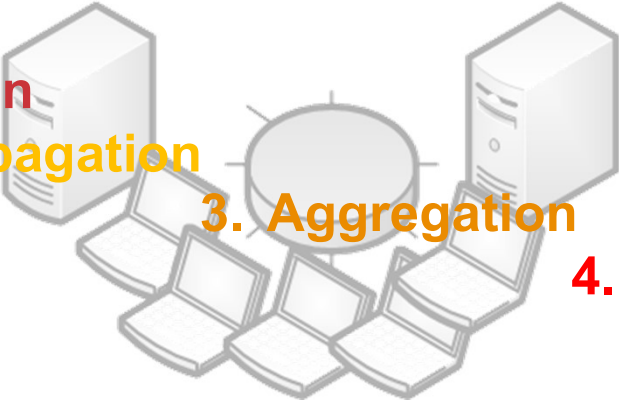


MINIMAL
IMPACT

MAXIMUM
IMPACT



- 1. Infiltration
- 2. Propagation
- 3. Aggregation
- 4. Exfiltration



How the Red Team Works

Leadership engages red team



Red team hackers break in (infiltrate)

Red team propagates & aggregates

Once detected, red team shows exfiltration data

Provides feedback to security team

Publishes the report



Red Team Benefits

- Simulated attack scenarios from real-world threats
- Demonstrates true offensive techniques to organizations
- Identify return on investment for cybersecurity solutions
- True 'quantitative' risk analysis
- Focuses on what's valuable, data & assets
- Designed to improve a security team
- Still get the penetration test report plus more

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Mitigation Steps

A few things you can do to
reduce risk...

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Know Your Inventory

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- Classification of inventory

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Educate Your Team

- Technology is no substitute for employee education
- Include the board, executives & vendors
- Knowledge is power
- Do not discourage false-positive reporting
- Document & distribute security policies
- Develop & rehearse a robust incident response program

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Patch Your Systems

- Applications
- Databases
- Operating systems – servers, workstations, etc.
- Anti-virus/anti-malware – engines & signatures
- Third-party applications

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Limit Access

- Control use of administrative privileges
- Limit access based on need-to-know (least privilege)
- Limit & control remote access
- Do not share credentials
- Consider multifactor authentication
- Limit the use of portable media
- Don't forget physical security
- Encryption is key, especially when data leaves your organization

Human Fact is Still the Weakest Link

- Remember physical security & limiting access when the following arrive
 - UPS
 - Coming in from corporate IT
 - Service people or technicians
 - Exterminator
 - Flower delivery



Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Plan, Prevent & Prepare

- Lock your laptop whenever you are away from your workstation
- Filter out suspicious email addressed to employees
- Be careful how you share company information
- Develop cyber incident response program (CIRT)
- Consider cyber insurance

Everyone needs a trusted advisor. Who's yours?

BKDCYBER

Backup

- Implement a regularly scheduled backup program that meets your business & records retention requirements
- Put some distance between your primary & secondary sites
- For critical applications, perform a full restoration or fail-over test at least annually
- Backup & restore not only data, but also the applications
- Understand the differences between cloud storage & cloud backup

Personal Recommendations

- Always ask why someone needs your information
- Avoid clicking links within unsolicited emails or text messages; go to the legitimate site & type in URL
 - <https://www.bankofamerica.com> – correct
 - <http://www.bankofamerica.com> – **incorrect**
- ***Be aware of cyber fatigue in your organization***
- Use strong passwords & change them often
- Avoid geolocation tagging in photos or tweets
- **Don't talk publicly about your company:** happy hours are perfect targets

The Next Generation

- CyberPatriot is the National Youth Cyber Education Program
- Created by the US Air Force and sponsored by Northrop Grumman
- Inspires K-12 students towards careers in cybersecurity or other science, technology, engineering, and mathematics (STEM)
- Preparing youth with skills critical to our future



The background of the slide is a dark blue, semi-transparent image showing several hands interacting with tablets. One tablet in the foreground displays a pie chart and a bar chart. Another tablet in the background shows a grid of data points. The overall scene suggests a collaborative work environment focused on data analysis.

Questions?

Everyone needs a trusted advisor. Who's yours?

BKDCYBER



Thank you!

bkd.com | [@BKDLLP](https://twitter.com/BKDLLP)

[@RexSecurity](https://twitter.com/RexSecurity)

[@BKDCyber](https://twitter.com/BKDCyber)

The information contained in these slides is presented by professionals for your information only and is not to be considered as legal advice. Applying specific information to your situation requires careful consideration of facts & circumstances. Consult your BKD advisor or legal counsel before acting on any matters covered.

Everyone needs a trusted advisor. Who's yours?

BKDCYBER