Cybersecurity and the Dark Web
Addressing Cybersecurity Concerns for Your Organization

Everyone needs a trusted advisor. Who’s yours?
Presenter

Rex Johnson
Director
Cybersecurity Practice Leader
rjohnson@bkd.com
Latest Statistics Shows Less Breaches

Reported Breaches by Year

Source: https://www.idtheftcenter.org/2018-data-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 #1 and growing

Motivations Behind Attacks

- **2016**
  - Cyber Crime: 72.1%
  - Cyber Espionage: 9.2%
  - Hacktivism: 14.2%
  - Cyber Warfare: 4.3%

- **2017**
  - Cyber Crime: 77.4%
  - Cyber Espionage: 14.5%
  - Hacktivism: 4.7%
  - Cyber Warfare: 3.4%

- **2018**
  - Cyber Crime: 81.8%
  - Cyber Espionage: 12.9%
  - Hacktivism: 2.8%
  - Cyber Warfare: 2.5%

Breaches Are Costing More & More

- Average total cost of a data breach: $3.86 million (up from $3.62 million in 2017)
- Average cost per lost or stolen record: $148
- 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 days
- 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
Polling Question #1

How did the cyber threat statistics change from 2017 to 2018?

A. The number of breaches and exposed records increased
B. The number of breaches decreased, but exposed records increased
C. The number of breaches increased, but exposed records decreased
D. They remained the same
Polling Question #1

How did the cyber threat statistics change from 2017 to 2018?

A. The number of breaches and exposed records increased

B. The number of breaches decreased, but exposed records increased

C. The number of breaches increased, but exposed records decreased

D. They remained the same
The Dark Web

What it is, and what it isn’t...
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!**
What Can I Find on the Dark Web?

Commercial Services
- CS Store - The original CardedStore - Elite
- Apple Palace - low priced Apple Products
- Gold & Diamonds - Genuine Gold, Diamond
- Football Money - Fixed football games
- Mobile Store - Factory unlocked phones
- Fake Passport/ID sale - Good website
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

- **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

- **Search Engines**
  Just like regular search sites, but for the dark web

- **Social Media/Chat Rooms**
  A place for hackers to share information more privately
Some items for sale

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 will be sent via PM.

DirecTV Account with NFL SUNDAY TICKET MAX

Vendor: kingshot (3200) (4.72) (@ 388/3/16) (@ 1307/25/25)
Price: $0.004899 ($18.72)
Ships to: Worldwide
Ships from: Worldwide
Escrow: No

Product description
"Directly 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

All images are actual screenshot from the dark web
Fake Insurance Card

This is a listing for a forged auto insurance card or proof of insurance. In addition to this item being forged car insurance, it 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 waterproof. This is from Allstate insurance company (check my listings). I also do State Farm and Geico insurance cards. The card will have all necessary information on it and will be drabbled. It will come in versions for all 50 U.S. states. It 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.”

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

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

Everyone needs a trusted advisor. Who’s yours?
Something to Think About

• How much could I get for your credit card on the dark web?

About $1
Joker’s Stash is the most popular “carding” forum on the dark web. Credit cards, just $1 each!

<table>
<thead>
<tr>
<th>DUMPS UPDATE (HIGH VALID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (NY state + few EU) TR1+TR2/TR3, HIGH VALID 99-100%.</td>
</tr>
<tr>
<td>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</td>
</tr>
</tbody>
</table>

Time for refunds: 3 hours (cold users 12h, silver 9h, bronze 6h)
Health Insurance Card for Sale

Health insurance card sold for just over $62
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.
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 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 way 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.
Polling Question #2

What can you purchase on the Dark Web?

A. A credit card
B. Fake passport
C. A Hacker for hire
D. All of the above
Polling Question #2

What can you purchase on the Dark Web?

A. A credit card
B. Fake passport
C. A Hacker for hire
D. All of the above
How Are You Targeted

Things to look out for...
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
Phishing Schemes are Most Popular

From: USAA
To: Recipients

Your USA
October 24, 2023

baw83800@uga.edu

WE'RE READY TO SERVE YOU.
USAA offers financial solutions designed to help you meet your goals throughout life.

Upon intensive reviews on your profile, we have noticed that you need to resolve important security issues on your account to prevent temporal deactivation. It is therefore recommended that you complete this process. Your security is important to us.

Please click on the reference link below to resolve this issue:
https://www.usaa.com/inet/ent_logon/Logon
Always Check…

bimo@gotdownsome.com

https://bam.bz/n8d
Some emails are legitimate, but...

- Never select the link in the email
- Call or go to a site that you know is official
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
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
Polling Question #3

Which of the following is **False**?

A. A hacker may try to connect to you via social media
B. Public Wi-Fi may increase your risk to cyber attack
C. Any email with a link included is from hackers
D. Shadow IT is predicted to 1/3 of attacks next year
Polling Question #3

Which of the following is **False**?

A. A hacker may try to connect to you via social media
B. Public Wi-Fi may increase your risk to cyber attack
C. **Any email with a link included is from hackers**
D. Shadow IT is predicted to 1/3 of attacks next year
What would a Hacker take?

Knowing how a hacker would compromise your environment
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

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
Polling Question 4

• Which of the following is a more effective way to see what a hacker would do in your network?
  A. External penetration test
  B. Social engineering
  C. Red team/digital simulation exercise
  D. Physical security walk-through
Polling Question 4

Which of the following is a more effective way to see what a hacker would do in your network?

A. External penetration test
B. Social engineering
C. Red team/digital simulation exercise
D. Physical security walk-through
Mitigation Steps

A few things you can do to reduce risk…
• **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
Recommendations – Basics

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

• **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
Recommendations – Basics

• Human factor 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
Recommendations – Basics

• 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
Recommendations – Basics

• 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.bankofmerica.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

https://www.uscyberpatriot.org/
http://www.northropgrumman.com/CorporateResponsibility/Pages/CyberPatriot.aspx

Everyone needs a trusted advisor. Who’s yours?
Questions?
Thank You!

bkd.com | @BKDNFP @BKDHigherEd
@BKDCyber @RexSecurity