



Emerging Technologies

Phishing, Hacking, Ransomware, and Bitcoin

September 5, 2019

New Orleans, LA

Peter Madsen

Education and Sentencing Practice Specialist

Office of Education and Sentencing Practice

Email – pmadsen@ussc.gov

Phone – (202) 502-4637

HelpLine – (202) 502-4545



Emerging Technology Information

Cryptocurrencies

Three Podcasts –

1. Dark Web
2. Bitcoin,
3. Hacking, Phishing, & Malware

Plus on Online Glossary of terms

<https://www.ussc.gov/education>



Learning Objectives

- Inform you about newest technologies being utilized by defendants and how that may impact guideline calculations
- Areas of focus will be:
 - Dark Web
 - Bitcoin
 - Hacking
 - Phishing
 - Malware



Who is in the Audience?

- A. Circuit Staff Attorney
- B. CJA Panel Attorney/Private Defense Attorney
- C. Federal Public Defender
- D. Judge
- E. Law Clerk
- F. U.S. Probation Officer
- G. U.S. Attorney
- H. Other



Years of Experience with Federal Sentencing?

- A. Less than 2 years
- B. 2 to 5 years
- C. 5 to 10 years
- D. More than 10 years



Having a Difficult Time Keeping Pace with Technology?

What is Bitcoin?
What is a
Cryptocurrency?



Ransomware?



This Attachment
Seems Harmless....
Oh No....



What is The Onion
Router?



Cybercrime Cases – What is your comfort level?

- A. **Excellent** – I can teach this course myself
- B. **Passable** – With help from Google maybe...
- C. **Poor** – Google can't even help
- D. **SOS** – Teach me!



What is Bitcoin?

Cryptocurrencies



Loss

Sophisticated Means

Money Laundering

Tax Evasion

Worldwide Bitcoin Seizures

October 2013
to
October 2018



Date	Country	Department	Amount (BTC)	Amount then (USD)	Already sold	Seized for
October 2013	USA	Marshals Service	144,342	\$48,000,000	Yes	Silk Road
October 2013	USA	Marshals Service	29,657	\$5,900,000	Yes	Silk Road
April 2014	USA	Department of Justice	6,060	\$3,030,000	Yes	Dark Web (Cornelis Jan Slomp)
July 2015	Italy	Europol	11,000	\$900,000	Yes	Dark Web
May 2016	Australia	Government of Australia	24,518	\$16,500,000	Yes	Silk Road merchant
August 2016	USA	Marshals Service	2,719	\$1,600,000	Yes	federal criminal, civil and administrative cases (12 cases)
May 2017	Bulgaria	SELEC	213,519	\$384,000,000	No/Unclear	Organized crime syndicate
December 2017	USA	Department of Justice	513	\$9,000,000	Yes	Dark Web (Aaron Shamo)
December 2017	Germany	Federal Criminal Police Office	126	\$2,300,000	Yes	Darknet (drugs)
January 2018	USA	United States Marshals Service	3,813	\$44,000,000	Yes	federal criminal, civil and administrative cases (17 cases)
January 2018	South Korea	Ministry of Justice	191	\$1,400,000	No/Unclear	child pornography website
February 2018	Finland	The Treasury Department	2,000	\$21,000,000	Yes	Dark Web (Kärkkäinen)
March 2018	USA	Department of Justice	500	\$5,100,000	No/Unclear	forged identification documents
March 2018	USA	Marshals Service	2,170	\$18,000,000	Yes	federal criminal, civil and administrative cases (20 cases)
May 2018	UK	London Metropolitan Police	74	\$700,000	Yes	Phishing attacks (Grant West)
May 2018	Israel	State Attorney's Office	1,071	\$8,500,000	No/Unclear	Money laundering (Halimi Git)
May 2018	Germany	Bavarian State Police	1,312	\$14,000,000	Yes	Illegal sale (Lesen und Lauschen)
June 2018	USA	Department of Justice	4,000	\$17,000,000	Yes	Dark Web (Farace, Swain)
June 2018	USA	Department of Justice	2,000	\$12,200,000	No/Unclear	Dark Web (35 dark web vendors)
June 2018	Spain	Europol	510	\$6,300,000	No/Unclear	Darknet (drugs)
July 2018	UK	Surrey Police	295	\$1,600,000	Yes	Money laundering (Teresko)
September 2018	USA	Department of Justice	1,605	\$10,200,000	No/Unclear	AlphaBay (Alexandre Cazes)
October 2018	USA	Marshals Service	660	\$4,200,000	Yes	federal criminal, civil and administrative cases (31 cases)

NO BULL. JUST GUNS.

Categories

Handguns Rifles Shotgun Accessories Used & Auction Guns Custom Rifles Videos Happy Customers Machine Guns

Zombie Stuff Contact Us

BITCOIN + Guns = HOT

NOW ACCEPTING

bitcoin

Yes, you can buy a gun with BITCOIN!

Also, no fees for credit cards if you still use that

Featured Products

			
TAURUS PT-22 22LR 2.75 GREEN/GLD 1-220031CEG	COBRA DERRINGER 22LR-BLUE/PRL 45ACP 3IN 6RD 55 PATRIOT C28P	COBRA ENTERPRISES INC PATRIOT 45ACP 3IN 6RD 55 PATRIOT 455	Savage 320 PUMP 12G 18.5" PG
\$233.99 Net Rated Add To Cart	\$143.99 Net Rated Add To Cart	\$289.99 Net Rated Add To Cart	\$192.95 Net Rated Add To Cart

Silk Road anonymous market

messages 0 | orders 0 | account \$0.00

Search Go

Category

js 8,670	annabis 2,066	issociatives 165	cstasy 660	pioids 591	ther 455	recursors 50	rescription 2,146	sychedelics 981	stimulants 1,102	arel 264	127	ic materials 1	ks 861	ectibles 5	puter equipment 32	tom Orders 68	tal goods 509
----------	---------------	------------------	------------	------------	----------	--------------	-------------------	-----------------	------------------	----------	-----	----------------	--------	------------	--------------------	---------------	---------------

1g MDMA 82%+ High Quality -Made in Germany- \$1.30	50 gr. Crystal MDMA Rocks \$23.33	Valium 10mg/ Diazepam (100 Pills) \$2.32	3g XxX AAA QUA WEED AMAZING \$0.98

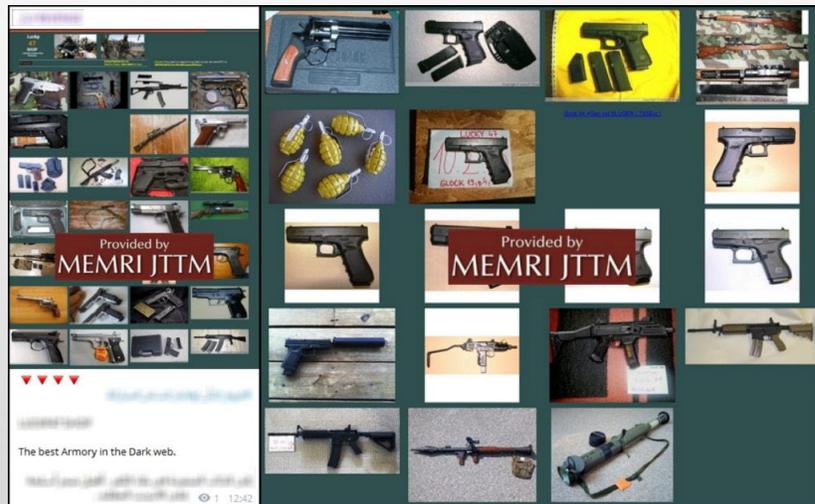
Kamagra jelly (India), 1 week pack 1 TheBen	Honeycomb Wax (85+%	1 gram Moroccan Hash	Citalopram 10x 2T

How are criminals using Bitcoin? The dark web

MEMRI JTTM

Provided by MEMRI JTTM

The best Armory in the Dark web.



NEW YORK STATE DRIVER LICENSE

Colorado Driver License

Alberca OPERATOR'S LICENCE

CALIFORNIA DRIVER LICENSE

Texas DRIVER LICENSE

South Carolina DRIVER'S LICENSE

DRIVING LICENCE

Driver Licence

SETH AGUES MCCALL

GOVERNMENT EXHIBIT 402

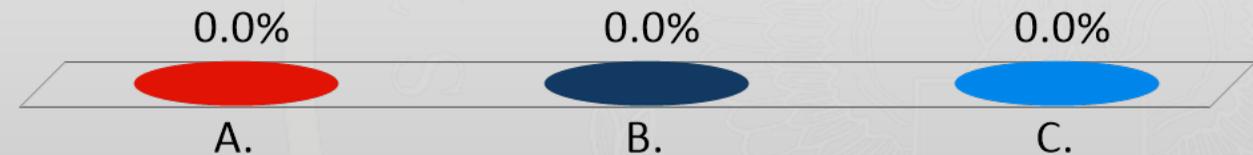



Ransomware Scenario

- An Iranian national executed a “WannaCry” Ransomware Attack on a hospital, demanding \$20,000 in Bitcoin.
- The hospital’s computing system was encrypted and inaccessible for a six hour period while a cybersecurity firm was retained to conduct a network assessment – the Hospital ultimately agreed to pay the \$20,000 in Bitcoin.
- Due to the network outage, the Hospital lost \$500,000 in revenue and later incurred additional costs to participate in the investigation and prosecution of the Iranian national.

What costs will be excluded in your loss analysis?

- A. The costs of retaining a Cybersecurity Firm and the \$20,000 Bitcoin Ransom
- B. The \$500,000 in lost revenue incurred as a direct result of the Ransomware Attack
- C. The costs of participating in the FBI Investigation and Testifying at Sentencing



U.S. v. Schuster 467 F.3d 614 (7th Cir. 2006)

- \$6,014 in lost business productivity and costs - permitted
- \$2,700 in victims' travel costs for meetings with the FBI and \$1,400 in costs for victims testifying at sentencing hearing – not permitted.

Bitcoin Scenario 1

The ransomware attack occurred on November 25, 2018. The victim paid 25 Bitcoin to the attacker. On this date, Bitcoin was valued at \$3,850.19

At sentencing on July 10, 2019, Bitcoin had increased significantly and was now valued at \$13,057.90

<https://www.coinbase.com/>

<https://www.coindesk.com/>

What is the loss amount for the Bitcoin payment?

- A. **\$96,250** – the value of the Bitcoin at the time of the offense
- B. **\$47,000** – The average value of Bitcoin between the time of the offense and sentencing
- C. **\$326,425** – the value of Bitcoin at sentencing
- D. **I don't know**



Bitcoin Scenario 2

The ransomware attack occurred on December 20, 2017. The victim paid 25 Bitcoin to the attacker. On this date, Bitcoin was valued at \$16,334.52

At sentencing on June 6, 2019, Bitcoin had decreased significantly and was now valued at \$7,939.24

What is the loss amount for the Bitcoin payment?

- A. **\$408,363** – the value of the Bitcoin at the time of the offense
- B. **\$245,000** – The average value of Bitcoin between the time of the offense and sentencing
- C. **\$198,481** – the value of Bitcoin at sentencing
- D. **I don't know**



Bitcoin Ponzi Scheme

Calculating Loss – One Option

Bitcoin raised –	50,000
Bitcoin returned to investors –	45,000
Bitcoin loss –	5,000
Average value of Bitcoin during the Instant Offense -	\$5,345
Approximate loss in dollars –	$5,000 \times \$5,345 = \$26,725,000$

Bitcoin

Guideline Implications

- Money Laundering §2S1.3 (a)(2) – it is the value of the funds (not loss per se, but you are using §2B1.1 loss table)
- Tax Evasion – is Bitcoin income or something has to be reported
 - Per IRS - Wages paid in virtual currency are subject to withholding to the same extent as dollar wages.

What is the Dark Web?

What happens there?



TOR – it's how you get there

CP – buy/sell w/bitcoin

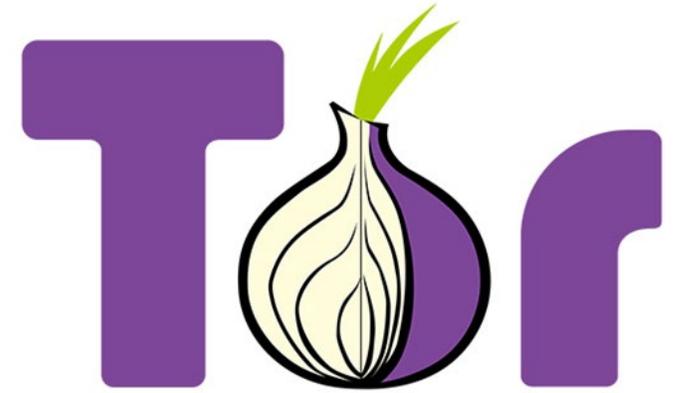
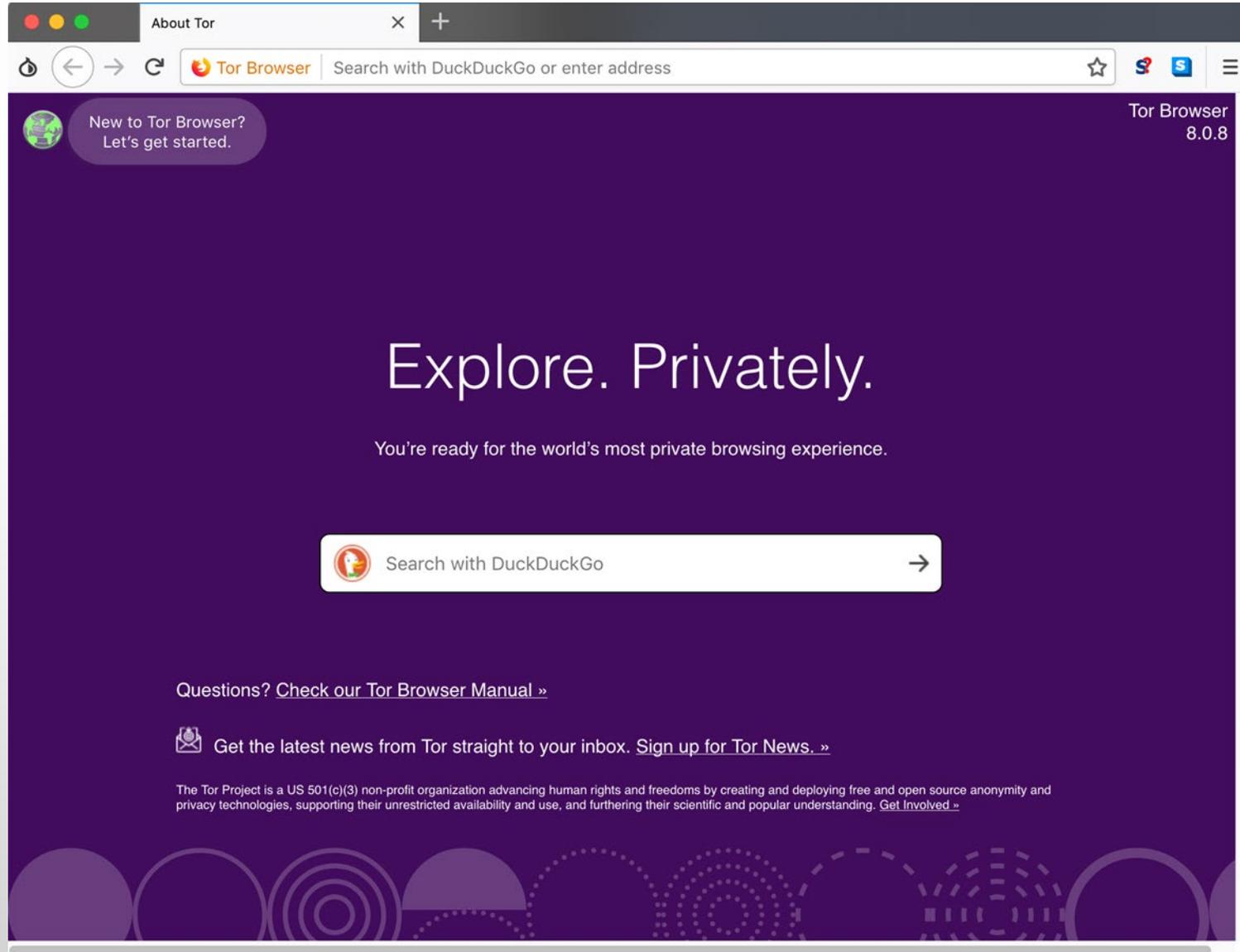
Sophisticated Means – fraud and tax

Drugs – dealing on dark web SOC

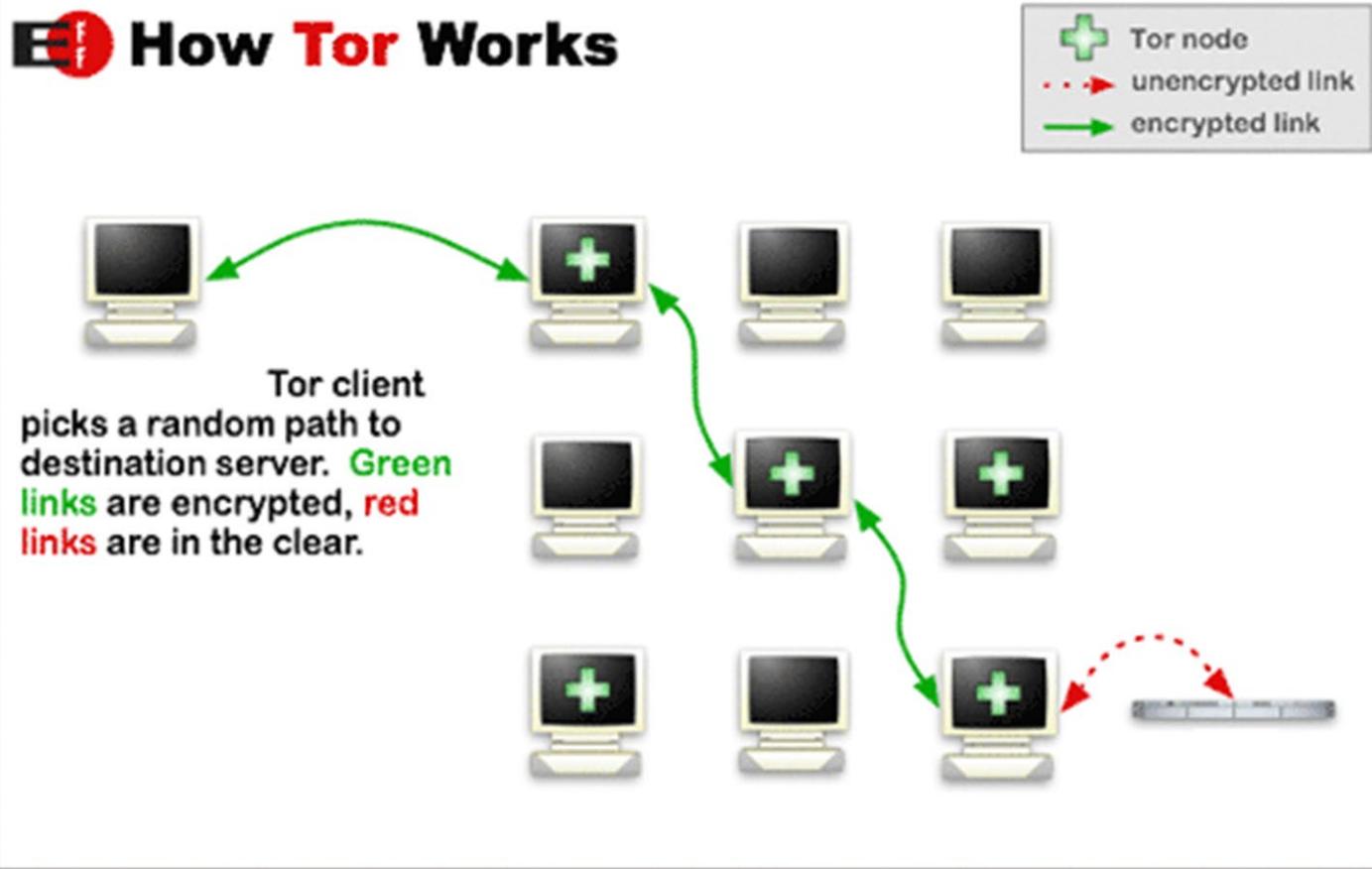
Firearms and ID's

Special Skill

What is the Dark Web?



How Tor Works

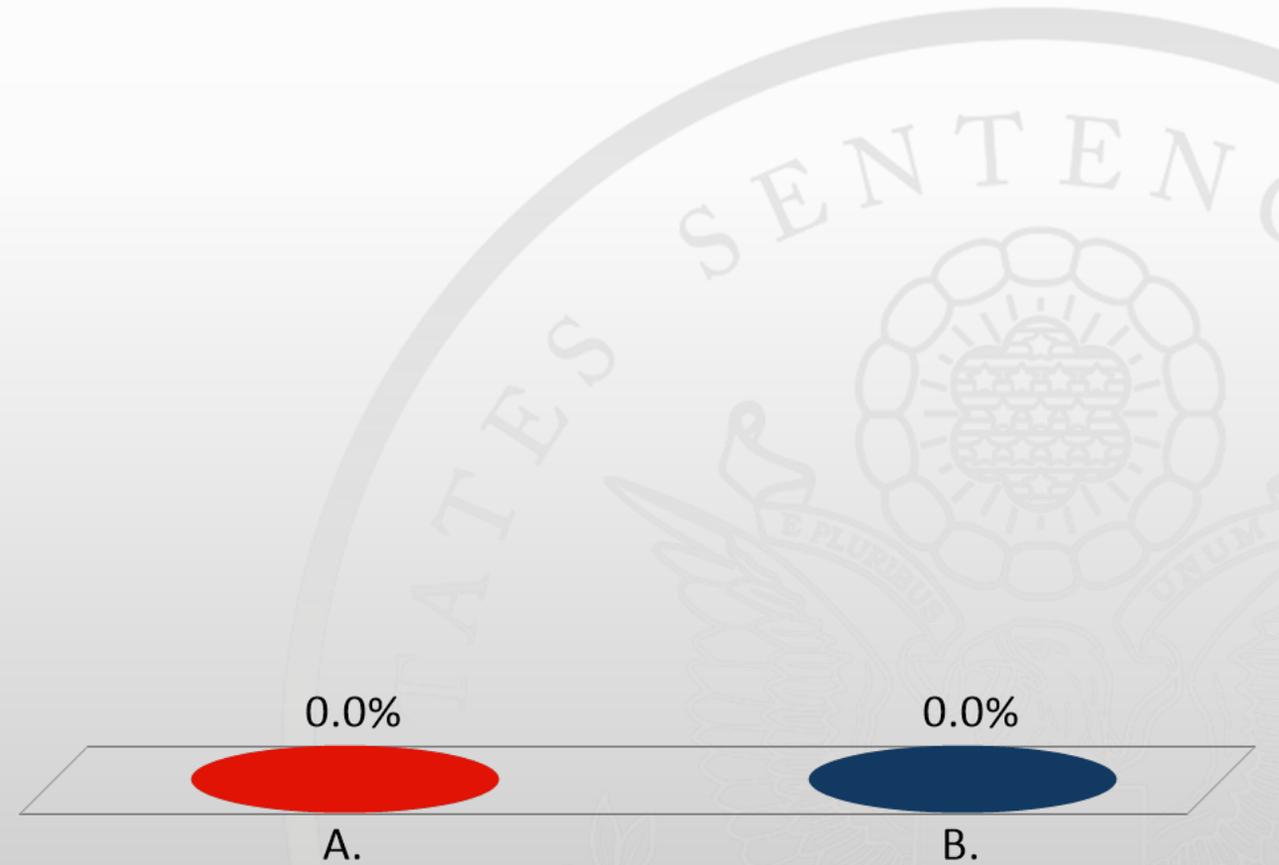


Example of Tor data transmission and encryption. Notice the red line indicating the lack of encryption outside the Tor network.

It anonymizes
your internet
traffic

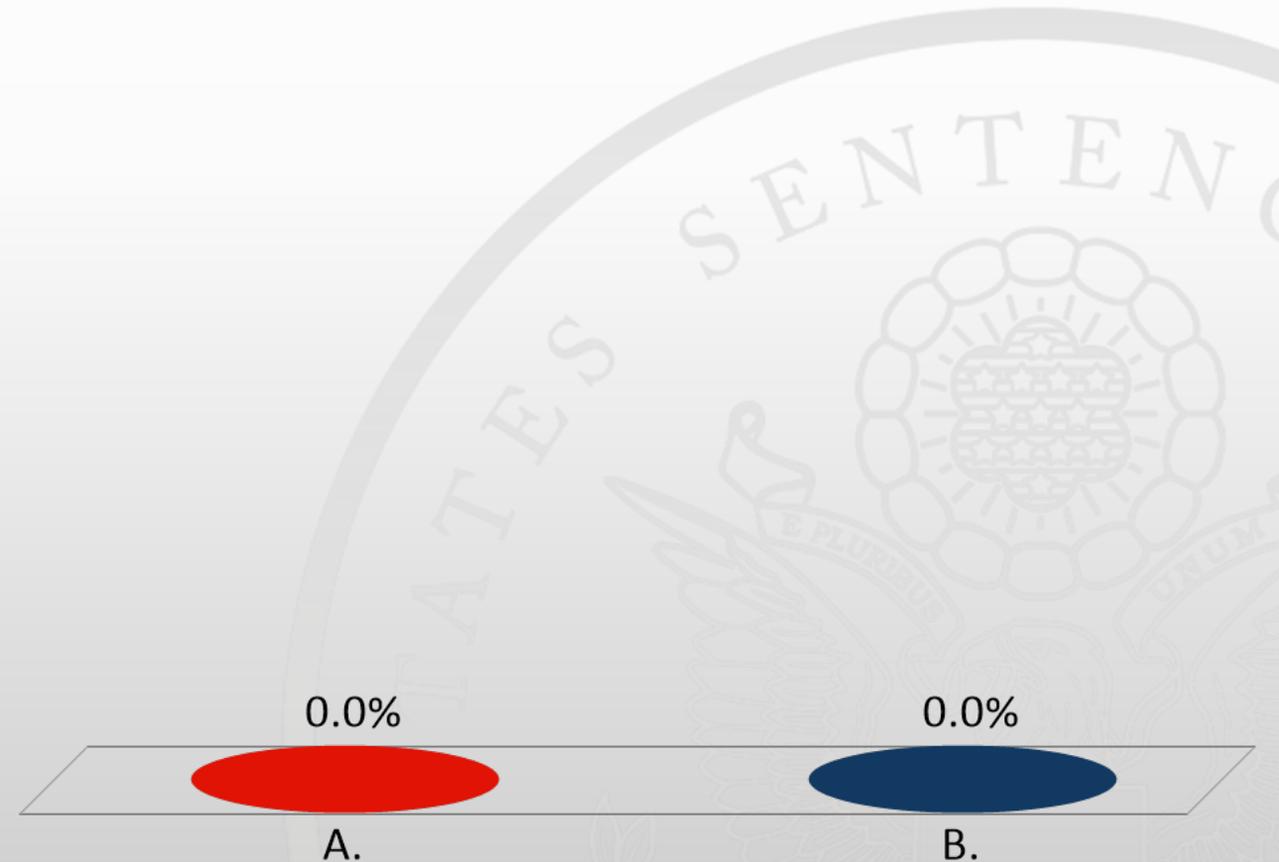
Going on the dark web or using TOR is illegal

- A. True
- B. False



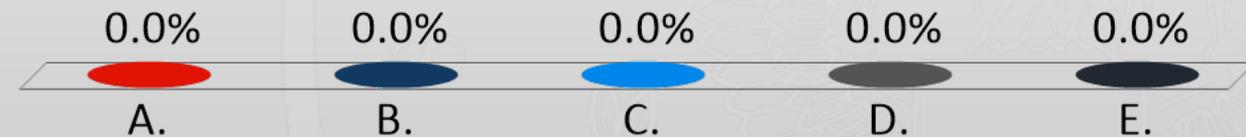
Every case that involves the dark web also involves sophisticated means.

- A. True
- B. False



What is the most common item bought on the dark web?

- A. Guns
- B. Drugs
- C. Credit Card Numbers
- D. Child Porn
- E. Ricin



What is the Hacking, Phishing, and Malware?

How does it affect the Guidelines?



Loss – Restitution
Sophisticated Means
Special Skill





YAHOO!

What do all of these have in common?



EQUIFAX



Application of Loss in Data Breach Cases

USSG §2B1.1, App. Note 3(A)(v)(III)

Actual loss includes:

- Any reasonable cost to any victim, including the cost of responding to an offense, and conducting a damage assessment,
- Cost to restoring the data, program, system, or information to its condition prior to the offense, and
- Any revenue lost, cost incurred, or other damages incurred because of interruption of service.



Payment will be raised on

5/15/2017 16:25:02

Time Left

02: 23: 58: 28

Your files will be lost on

5/19/2017 16:25:02

Time Left

06: 23: 58: 28

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)

You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>. If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?



Send \$300 worth of bitcoin to this address:

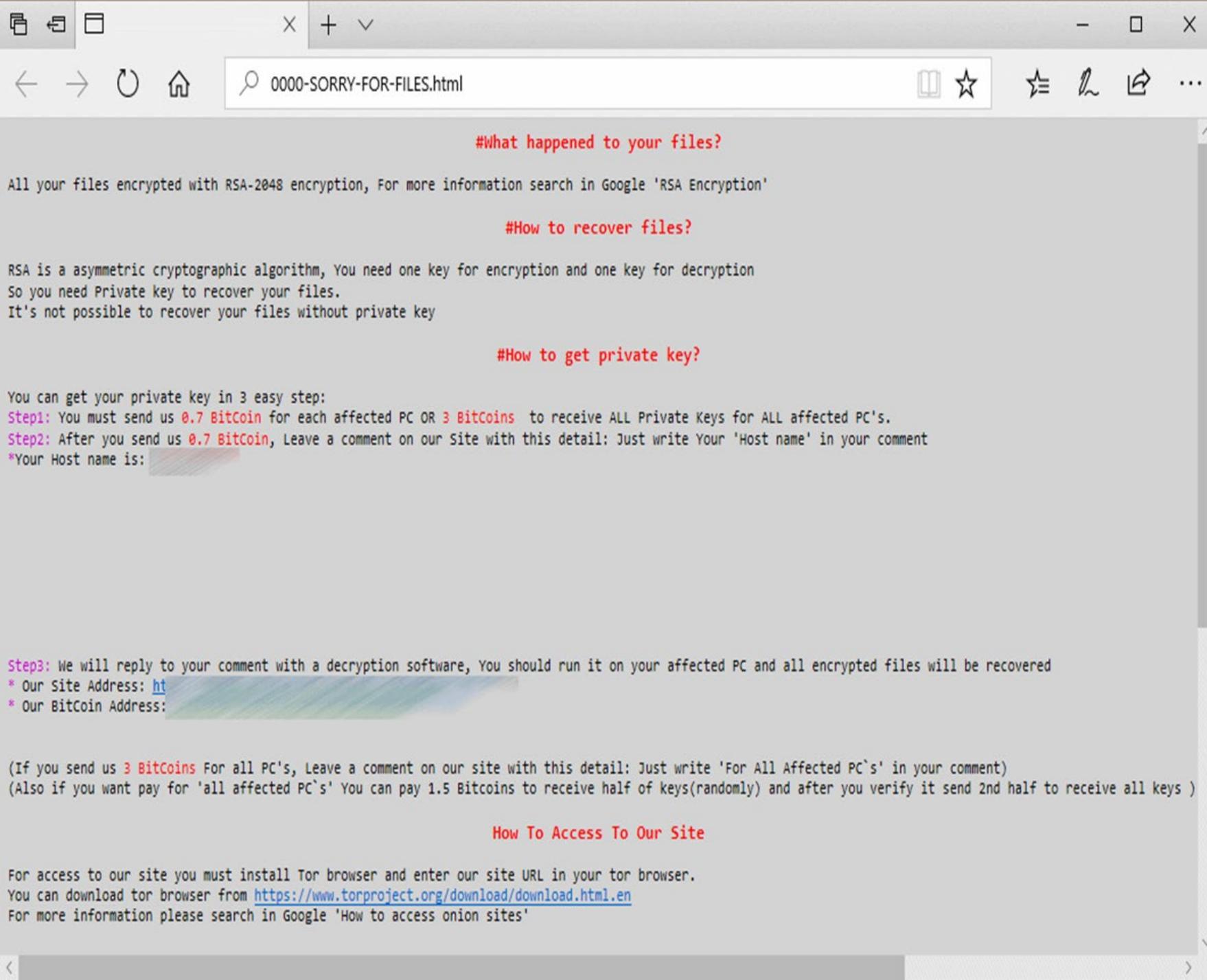
[QR Code](#)

15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Copy

Check Payment

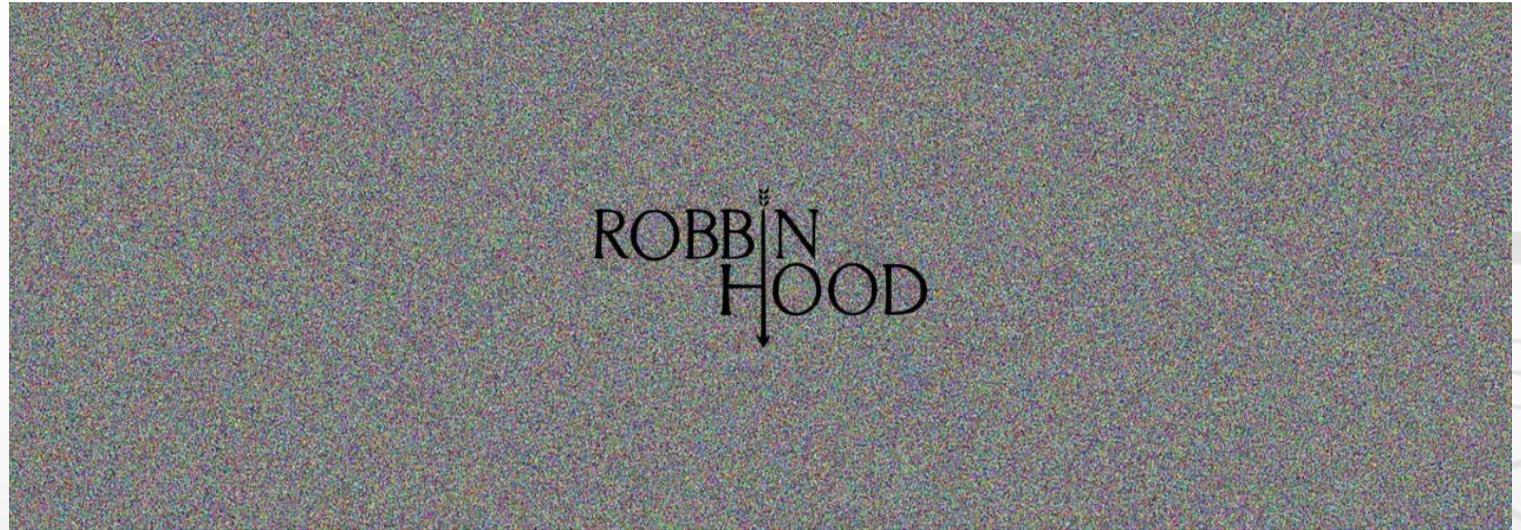
Decrypt



- March 22, 2018 – May 31, 2018
- Water or sewer bills
- Court fines/tickets
- Business licenses
- City counsel correspondence
- Also CO, IN, NM, etc.
- Healthcare companies
- Educational institutions
- Government entities

Baltimore
Ransomware

May 7, 2019



Hacker ransom - 13 bitcoin ~ \$100,000

Paid out thus far - **\$18 million!**

Ransomware Attacks on US Cities Just in 2019 so far...

- June 2019 – Lake City, FL paid 42 bitcoins (\$500,000)
- April 2019 – Cleveland Hopkins Airport – fixed on their own
- April 2019 – August, Maine – froze city's entire network
- April 2019 – Hackers stole \$498,000 from Tallahassee, FL payroll system
- March 2019 – Riviera City, FL – paid 65 bitcoins (\$600,000)
- March 2019 – Jackson County, GA paid \$400,000 to cybercriminals who shut down their computer systems

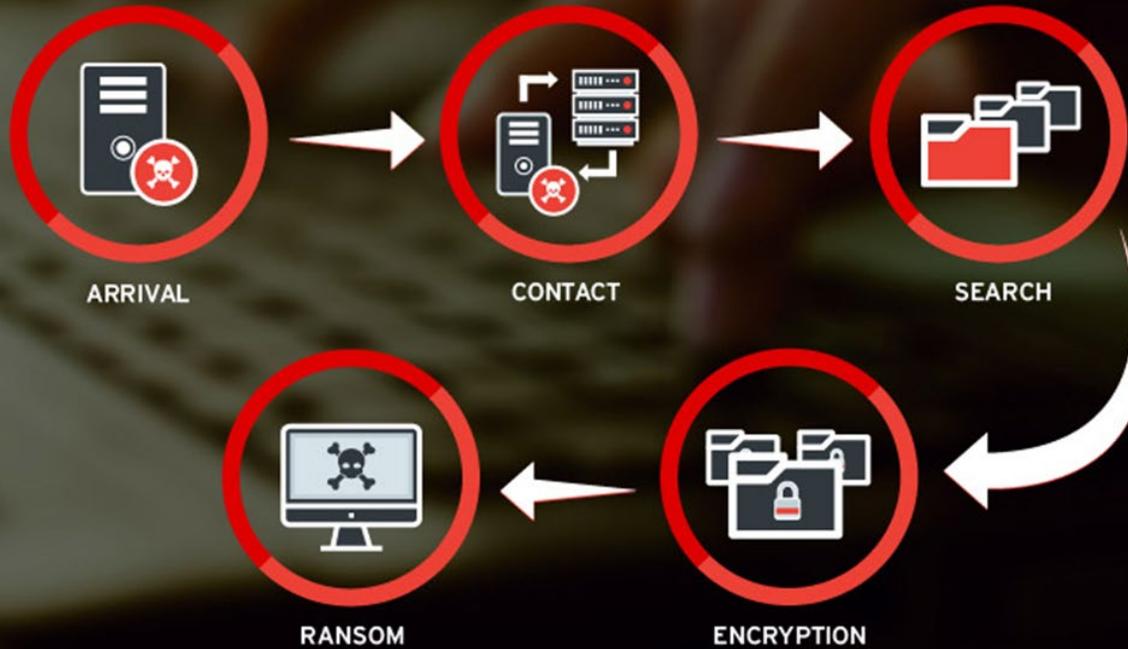


RANSOMWARE

BEHIND THE SCENES

By the time victims see the ransom note, it's already too late—ransomware has already encrypted files before they know it's there.

Here's what happens between infection and the ransom demand.



Take less than
10 minutes to
orchestrate

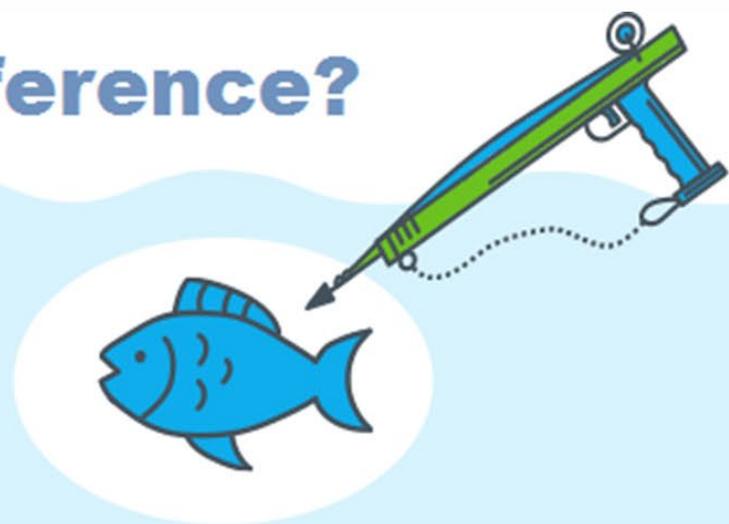


What's The Difference?



PHISHING

IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY

Phishing and SMS Phishing Attacks

From: "AppleID" <5i7dubsebj7p3iu7syd7oz71l@txev7wiufbg7a4qb.servicemailidsecuritywebappss.com>
Date: April 7, 2018 at 1:12:14 PM EDT
To: [REDACTED]@yahoo.com>
Subject: [New Statement report] Your AppleID has been disabled at Sat, 07 Apr 2018, 10:12:12 AM .
Service ID#9RW3-R

Your Apple ID Has Been Disabled

Dear [REDACTED]@yahoo.com,

Review the recent login attempts on your account :

Date and Time : 07 April 2018, 10:12:13 AM
Location : Nigeria
Browser : iPhone

If you never access with the device please log into your account and verify your account.

For quick access verify your account we suggest to go to this link [Manage account >](#)

Regards

Apple Support



What is truly new and cutting edge...

- Doxing –
 - what can I find out?
- Jackpotting –
 - Free cash
- New Dark Web –
 - Selling doctor's identities to help orchestrate insurance fraud or get prescription medication
- DDoS Services for Attacks –
 - paying for services



What are they looking for?

Personal Information

Username

E-mail

Full Name

City

Zip/Postal

State/Province

Country

IP Address

ISP

Home Address

Phone Numbers

Social Networks

Other



Jackson Cosko • 3rd
Democratic Political Professional &
Cybersecurity Graduate Student
Washington D.C. Metro Area • 374

InMail



Experience



United States Senate

2 yrs 5 mos

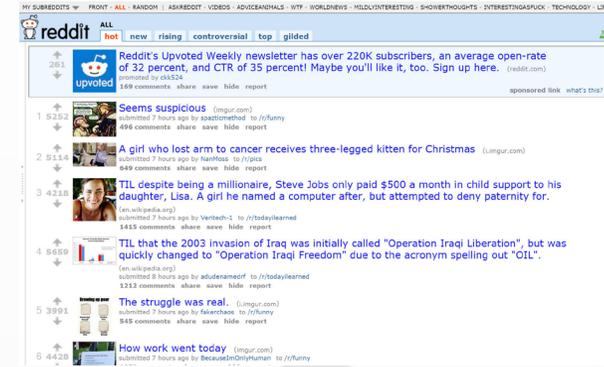
Legislative Correspondent | Systems Administrator

Jan 2017 - May 2018 • 1 yr 5 mos

Press Assistant | Systems Administrator

Jul 2016 - Jan 2017 • 7 mos

Doxing - Short for dropping documents





Jackpotting Why and How?

- A huge percentage of ATMs still run on Windows XP
- Thousands of vulnerabilities

New Dark Web Information



Info

Vendor: [blurred]
★★★★★ (0)

[Any questions about the offer](#)

Ships from: US
Ships Worldwide
Escrow

bitcoin
★ Add to favorites

Amount
1

[Buy](#)

Scroll down for prices

US Fullz - 1998-2008 - Minors - Kids

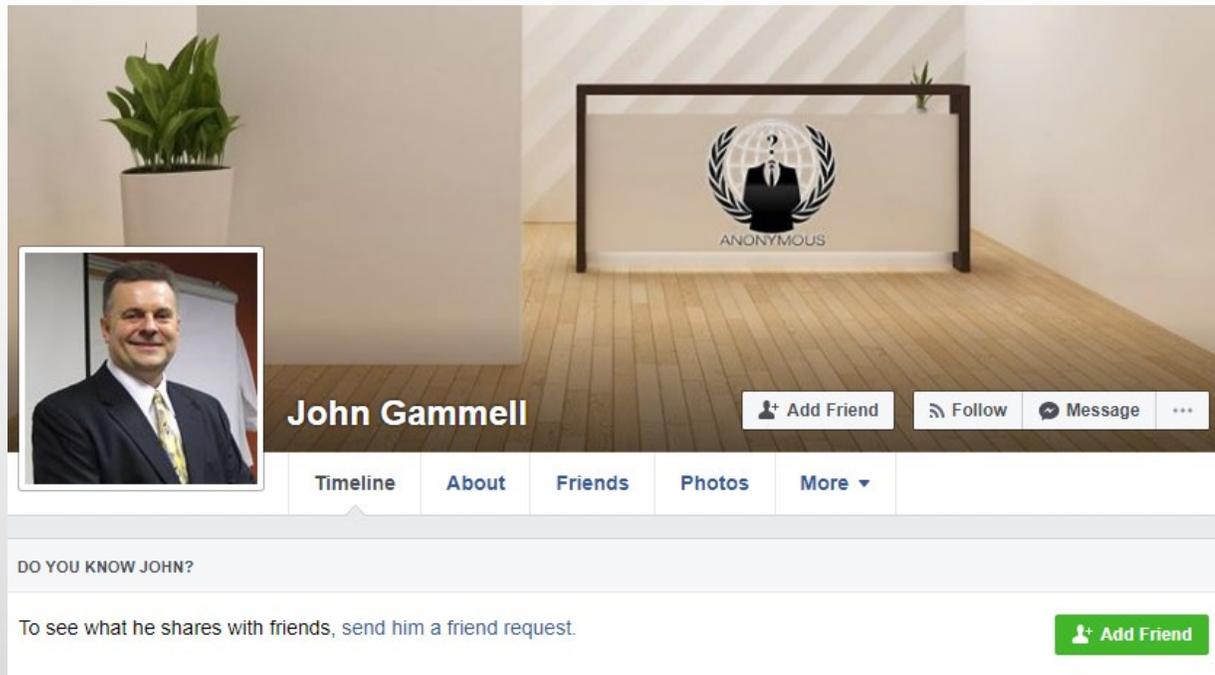
[Description](#) [Refund policy & Vendor information](#)

This listing is for plain personal info including Social Security Number and Date of birth (SSN DOB) also known as fullz that came from pediatricians databases. This means that the kids are born 2000+ and generally speaking come from good families that can provide medical support.

- Selling doctor's identities
- helping to orchestrate insurance fraud or
- get prescription medication (Opiates)

DDoS Attacks

A DDoS attack is a malicious attempt to disable or interrupt service to a computer or website, usually by causing large amounts of Internet traffic to be directed to the computer or website.



- Almost \$1 million in losses to numerous victims
- Sophisticated?

Operation Hackerazzi



“Questions or Comments?”



www.ussc.gov

HelpLine (202) 502-4545



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

training@ussc.gov



#USSCSeminar19