Facebook: The Knowledge Coop
LinkedIn: NathanKnottingham
Email: nathan@knowledgecoop.com
Thank you so much for allowing us to bring this information to you at the AARMR 30th Anniversary 2019 Conference.

We do not recommend anyone attempting to enter the Dark Web at any time on any device. This information is provided for educational purposes. This is the “Don’t Try This At Home” message.

To inquire on having Knowledge Coop train your organization, either through online or in person, please reach out to jim@knowledgecoop.com and reference the 2019 AARMR presentation.
Videos Referenced -

- **Adobe VoCo - Voice Editing System**: [https://youtu.be/I3l4XLZ59iw](https://youtu.be/I3l4XLZ59iw) (I mistakenly said VFX from stage, the key Adobe word is #VoCo)

- **Google Duplex AI Voice Assistant**: [https://youtu.be/D5VN56jQMWM](https://youtu.be/D5VN56jQMWM)

- **Knowledge Coop LO Down - Deep Fakes** -
  - [https://blog.knowledgecoop.com/fraud-is-in-the-air-0](https://blog.knowledgecoop.com/fraud-is-in-the-air-0)

- **Knowledge Coop - Deep Fakes: Mortgage Issue?** -

- **Knowledge Coop LO Down - Are Your Devices Listening to You?** -
  - [https://blog.knowledgecoop.com/lodownhomeaudiodevice](https://blog.knowledgecoop.com/lodownhomeaudiodevice)

- **2019 Red Flags and Cyber Concerns** - [https://youtu.be/OlfQ93VAQnQ](https://youtu.be/OlfQ93VAQnQ)
EQUIPOCALYPSE

001,199,620
2018 Overall Statistics

**IMPORTANT STATS**

IC3 Complaints Last 5 Years

- 2014: 100,000
- 2015: 200,000
- 2016: 300,000
- 2017: 400,000
- 2018: 400,000

# Of Complaints Reported Since Inception ('00)

4,415,870

Approximately 300,000 Complaints Received Per Year On Average

$2.71 Billion Victim Losses in 2018

Over 900 Complaints Received Per Day On Average
## 2018 Victims by Age Group

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Total Count</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 20</td>
<td>9,129</td>
<td>$12,553,082</td>
</tr>
<tr>
<td>20 - 29</td>
<td>40,924</td>
<td>$134,485,965</td>
</tr>
<tr>
<td>30 - 39</td>
<td>46,342</td>
<td>$305,699,977</td>
</tr>
<tr>
<td>40 - 49</td>
<td>50,545</td>
<td>$405,612,455</td>
</tr>
<tr>
<td>50 - 59</td>
<td>48,642</td>
<td>$494,926,300</td>
</tr>
<tr>
<td>Over 60</td>
<td>62,085</td>
<td>$649,227,724</td>
</tr>
</tbody>
</table>
Who’s behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.
What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.
Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.
What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.
Cyber-Espionage
Attacks linked to state-affiliated actors, and/or with the motive of espionage.

Welcome to the long game
A malicious email is the cyber spy’s favored way in. But this is no smash and grab. The initial email is typically followed by tactics aimed at blending in, giving the attacker time to collect the data that they need.

What you can do
Throw your weight behind security awareness training and encourage your teams to report phishy emails. Make it difficult for the adversary to pivot from a compromised desktop to other devices on your network.
Denial of Service

Any attack intended to compromise the availability of networks and systems.

Being hit where it hurts
DDoS attacks are nearly always (98%) targeted at large organizations. And while some unlucky souls face a constant barrage all year round, most attacks are over within a couple of days.

What you can do
Check that you have DDoS mitigation services in place to thwart any attacks, that they’re regularly tested, and that they actually work.
Insider and Privilege Misuse

Any unapproved or malicious use of organizational resources.

The enemy within
In 60% of cases, insiders abscond with data in the hope of converting it to cash in the future. But sometimes it’s a case of unsanctioned snooping (17%), or taking data to a new employer or to start a rival company (15%).

What you can do
Implement limiting, logging and monitoring of use, and watch out for large data transfers and use of USB devices.
Crimeware
All instances involving malware that did not fit into a more specific pattern.

Ransomware is big business
In the 2014 DBIR, ransomware was the 22nd most common form of malware. This year it’s number five, and the most common in the Crimeware pattern. For the attacker, holding files for ransom is fast, low risk and easily monetizable – especially with Bitcoin to collect anonymous payment.

What you can do
Watch out for macro-enabled MS Office documents and stress the importance of software updates to anyone who’ll listen.
How do they get data?
Social Engineering
Cosmo the God

- UFC & Coach (SOPA)
- CA, WA, NY, DC
- Papa John’s
- NASDAQ
- CIA
- Twitter
- 4Chan
- 500,000 credit cards released
"You can pretty much do it at any company—impersonate an agent," he shrugs and smiles. "Most people will fall for it unless they've been trained not to. But most companies aren't doing that."

—Cosmo the god on Social Engineering
Phishing

DocuSign
From: Bossert, Thomas P. EOP/WHO
Sent: Thursday, July 27, 2017 6:13 pm
Subject: Re: [SUSPECTED_SPAM] August 26th
To: Jared Kushner

Thanks, Jared. With a promise like that, I can't refuse. Also, if you ever need it, my personal email is [redacted].

-Tom

Sent from my iPhone

> On Jul 26, 2017, at 4:54 PM, Jared Kushner [redacted] wrote:
> Tom, we are arranging a bit of a soirée towards the end of August.
> It would be great if you could make it, I promise food of at least comparable quality to that which we ate in Iraq!
> Should be a great evening.
> Jared
> Sent from my iPad
>
Malvertising

- NY Times
- BBC
- NFL
- AOL
- Spotify
- Google AdWords
- Yahoo
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don’t waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:
   1Mz7153HMuxXTuR2R1t78mGSDzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
   74fZ96-2Mx1Gm-yHQRWv-S8gaN6-8Bs1td-U2DKui-Z2pKJE-kE6sSN-o8tizV-gUeUMa

If you already purchased your key, please enter it below.
Key: _
The Future of Ransomware…
The FUTURE is NOW
CARS

Chinese group hacks a Tesla for the second year in a row

Elizabeth Weise, USATODAY  Published 8:45 p.m. ET July 27, 2017 | Updated 10:04 a.m. ET July 28, 2017

ANDY GREENBERG  SECURITY  07.21.15  06:00 AM

Hackers remotely kill a Jeep on the highway—with me in it
Medical Devices

FDA warns that certain pacemakers are vulnerable to hacking
Transmitters made by St. Jude Medical could be modified to send nefarious code to cardiac devices.

Johnson & Johnson warns of insulin pump hack risk

Elizabeth Weise, USA Today
Published 12:57 p.m. ET Oct. 4, 2016 | Updated 7:35 a.m. ET Oct. 5, 2016
A Look Into the Dark Web
TORCH: Tor Search Engine

Search!
1. BitCredit - Buy Credit Cards [10.369%]
   To Order? Welcome to the most trusted Credit cards store in darknet! We use the... Read: We do not provide cloned/stolen credit cards. We are specialized in pre-paid cards. We have pre-loaded the cards with...
   [Cached copy]

2. BitCredit - Buy Credit Cards [10.368%]
   To Order? Welcome to the most trusted Credit cards store in darknet! We use the... Read: We do not provide cloned/stolen credit cards. We are specialized in pre-paid cards. We have pre-loaded the cards with...
   [Cached copy]

3. CC Galaxy - Cloned Credit Cards - Us / Eu / Uk | WorldWide Shipping [10.280%]
   Cloned Credit Card, WU/MC Transfers PayPal... Carding f0 / $0 f0 Login Menu Home Credit Cards
US Cloned Credit Cards
$150 – $1,000
Us Cloned Credit Card + Pin Number Worked Worldwide At ATM's & Stores

Balance  
Choose an option

SKU: N/A  
Category: Credit Cards  
Tags: ATM, Pin Number, Store, US Cloned Credit Card, Worldwide

Description
The American clone credit card comes with a magnetic stripe and no chip. The card is...
A bit about us...

RoyalCards is a large group located in Europe and USA since 2015. We are skimming cards from ATMs by professional skimming tools in many countries in Europe and USA. Service what we are providing is just an protection for us by making sure the cards aren’t cashing out only in single area by us. It makes it easier for us to cash them out safely. We can't really cash out all of cloned cards, the amount of cards can lure some unwanted bank investigation. So... we aren't “Money Givers” or peoples with Gold Hearts who giving money for free like others bullshit deepweb websites... We are providing this service only for our protection giving at the same time help to others. Maybe in your mind you have vision with us: "Wow, how big mafia they are...", but not... We are plain, grey peoples maybe like you who want a little more money.

Some photos with our onion domain address and shop name on pieces of paper for verification:
CLONED CHIPPED CARDS

5 CARDS

$440

Packages are packed in anti X-RAY and anti magnetic field foil

Balance per card: 2500$

Transaction limit: 1500$

Discount: 12%

1 CARD

$100

Packages are packed in anti X-RAY and anti magnetic field foil

Balance per card: 2300$

Transaction limit: 1000$

Discount: 0%

10 CARDS

$760

Packages are packed in anti X-RAY and anti magnetic field foil

Balance per card: 3000$

Transaction limit: 2000$

Discount: 24%

MOST FREQUENTLY BOUGHT
SHIPPING

REGULAR COURIER WITH TRACKING

$7

Packages are packed in anti X-RAY and anti magnetic field foil

Shipping to: WORLDWIDE

Delivery time: Around a week

EXPRESS SHIPPING WITH TRACKING

$14

Packages are packed in anti X-RAY and anti magnetic field foil

Shipping to: WORLDWIDE

Delivery time: Up to 3 days

THE BEST OPTION

OVERNIGHT SHIPPING WITH TRACKING

$29

Packages are packed in anti X-RAY and anti magnetic field foil

Shipping to: USA, Canada and Europe

Delivery time: 1 day
So this is a bit of a late update but when I finally received my order I got carried away with using the cards. I spent the whole weekend at our local mall with my gf, after blowing through the first 3 cards we ran out of things to buy there so we when on Amazon and finished out the last of the cards. I saved on and made a withdrawal every day for the last 4 days so I could put some more money into buying more cards. I've got to admit, this is the craziest thing I've ever experienced in my life it really does feel too good to be true. Another thing, it's harder to spend thousands of dollars all in a few days on random stuff, my gf didn't have a problem with it though :D These cards are a huge life changer, I hope you guys are around for a really long time! Thank you and cheers!
Welcome to the greatest place on TOR!

Site News

- 07/23/2017: New accounts has arrived today, feel free to look.

- 07/09/2017: It is always a nice job reading your honest feedbacks, because we're not doing this service just for the profit, we're also making people happy here. That said, we updated the Feedback page with some of your comments we liked the most. :) Don't get us wrong, all feedbacks are welcome, we are grateful for every single one of them. But here are our current favourites. :)

- 06/30/2017: We have some fresh new accounts today, we hope it will satisfy you again. :)
Main Page

Welcome to The Hidden Wiki New hidden wiki url 2017
http://zqktlwi4feco6ri.onion Add it to bookmarks and spread it!!!!

Editor’s picks

Bored? Pick a random page from the article index and replace one of these slots with it:

1. The Matrix - Very nice to read.
2. How to Exit the Matrix - Learn how to Protect yourself and your rights, online and off.
5. Terrific Strategies To Apply A Social media Marketing Approach - Great tips for the internet marketer.

Volunteer

Here are six different things that you can help us out with:

1. Plunder other hidden service lists for links and place them here!
2. File the SnapBBSIndex links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
5. Perform Dead Services Duties.
6. Remove CP shitness.

Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services (allows you to add new sites to
Welcome to **Documents Service** - the unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, ID cards, VISA, stamps and other products for following countries: Australia, Belgium, Brazil, Canada, Finland, France, Germany, Ireland, Italy, Netherlands, Norway, Spain, Sweden, Switzerland, UK, USA and some others.

If you want to learn more about what kinds of documents can be found in our website please visit the sections "Services" and "Samples". You can find more details about ordering procedure and additional details visiting the sections "FAQ" and "Order".
**Cocaine (85%) & Crack**

People's Drug Store pride ourselves on the **HIGH QUALITY** of our amazing, **HIGH PURITY COCAINE**

Just like our Heroin, we get our cocaine **DIRECT** from the importer (usually from Peru but sometime its from Columbia) and we always get our product given to us right off of the kilogram bricks as they come in so we can be **ABSOLUTELY POSITIVE** that it was not cut or stepped on locally in any way!!

It is our policy to **NEVER** cut or add any kind of adulterant to any of our products so you can rest assured that any cocaine you buy from us will be as pure as it was when it left on the boat from South America to cross the ocean.

<table>
<thead>
<tr>
<th>Product</th>
<th>Price</th>
<th>Quantity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GRAND OPENING SPECIAL</strong> QUARTER GRAM COCAINE (0.25g)</td>
<td>22 USD = 0.008 B</td>
<td>Sold out</td>
</tr>
</tbody>
</table>
Silk Road is Gone
### Services

Then you will see a list of all services currently available from PirateSec. If you are interested in any service just contact us through our email address encrypting your messages with PGP and don't forget include your public key to receive an answer.

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emails Hacking</td>
<td>We can get any password, from any email address. Doesn't matter if it's a free email (outlook, hotmail, gmail, yahoo, etc) or private/corporate.</td>
<td>0.15 BTC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Media Hacking</td>
<td>We can get any password of Facebook, Twitter or Instagram accounts. Based in sophisticated phishing and brute force.</td>
<td>0.12 BTC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Development</td>
<td>We can develop softwares as per your request and we love to create hacking tools. Starting from $100 the charges may vary depending on the project.</td>
<td>0.7 BTC</td>
</tr>
<tr>
<td>Grades Change</td>
<td>This service consist in access in to any university/educative system in order to change their grades, missed classes, among other things.</td>
<td>0.7 BTC</td>
</tr>
</tbody>
</table>
What Else Is Coming?

Deep Fakes
We're an independent voice delivering concise, accessible, and relevant cyber security news to people all across the globe. We separate the signal from the noise.
Experts: Spy used AI-generated face to connect with targets

By RAPHAEL SATTER  June 13, 2019
Indistinct background, close crop

Other potential artifacts

Halo effect or painterly quality around hair

Smudges/striations/drip marks on cheek

Cockeyed, heterochromatic eyes

Strange scale-like effect on upper earlobe

Earring is blurry or melted
The Age Where Imagination Becomes Reality
“Do you have anything between 10 am and 12 pm?”

Google Duplex A.I.  
Clip trimmed for timing
BEFORE THE DIRECTOR OF THE DEPARTMENT OF FINANCE
OF THE STATE OF IDAHO

STATE OF IDAHO, DEPARTMENT OF FINANCE, CONSUMER FINANCE BUREAU,

Complainant,

vs.

ALEJANDRO FLORES, dba FULL SPECTRUM LOANS

Respondent.

Docket No. 2018-8-03

ORDER TO CEASE AND DESIST
6. In June 2018, a Vice President of Compliance for Nationstar Mortgage, LLC (Nationstar), contacted the Conference of State Bank Supervisors (CSBS) regarding an incident whereby someone from an entity called Full Spectrum Loans (FSL) had contacted a consumer about a debt consolidation loan. FSL’s representative identified himself as a loan officer named “Jonathan McGrail” and utilized an identifying NMLS number. This NMLS number did belong to one of Nationstar’s loan officers, Jonathan McGrail, who had no affiliation with Respondent nor with FSL.
8. Since the consumer was a resident of Idaho, the CSBS passed the information/complaint on to the Department. The Department contacted the consumer, R.M., who then filed a formal written complaint. The complaint was substantially similar to the information provided by Nationstar. R.M. indicated that he received a phone call from a person identifying himself as “Jonathan McGrail,” of FSL. R.M. stated that the person also represented himself as a loan officer specializing in helping veterans refinance their homes. R.M. further stated that he and “Mr. McGrail” spoke several times over the phone and since R.M. was unable to make his house payments, they discussed a refinancing agreement. “Mr. McGrail” sent a “Second-Chance Mortgage Refinance Approval” document to R.M., who signed it and sent it back to FSL along with a check for $3,200.00.
9. An examiner for the Department determined that the host for the domain name “fullspectrumloans.com” was GoDaddy. Through a subpoena issued to GoDaddy, the examiner identified Respondent as the registrant for the domain name “fullspectrumloans.com.” Upon information and belief, Alejandro Flores was the person who represented to R.M. that he was “Jonathon McGrail.”
Your Fish Tank???
What Do We Do?

- Deal with this as a business problem, not an IT problem
- TRAIN!
- Get your documents backed up and off your hard drive
- Patch.... IMMEDIATELY! (Stop using IE5)
- TRAIN!
- Hire a hacker
- TRAIN!