# The Life and Death of a Carding Kingpin

Nathaniel Beckstead

## whoami

Nathaniel Beckstead

Blue Team

Automation

Legal???

scriptingis.life

github.com/becksteadn

KeyBank

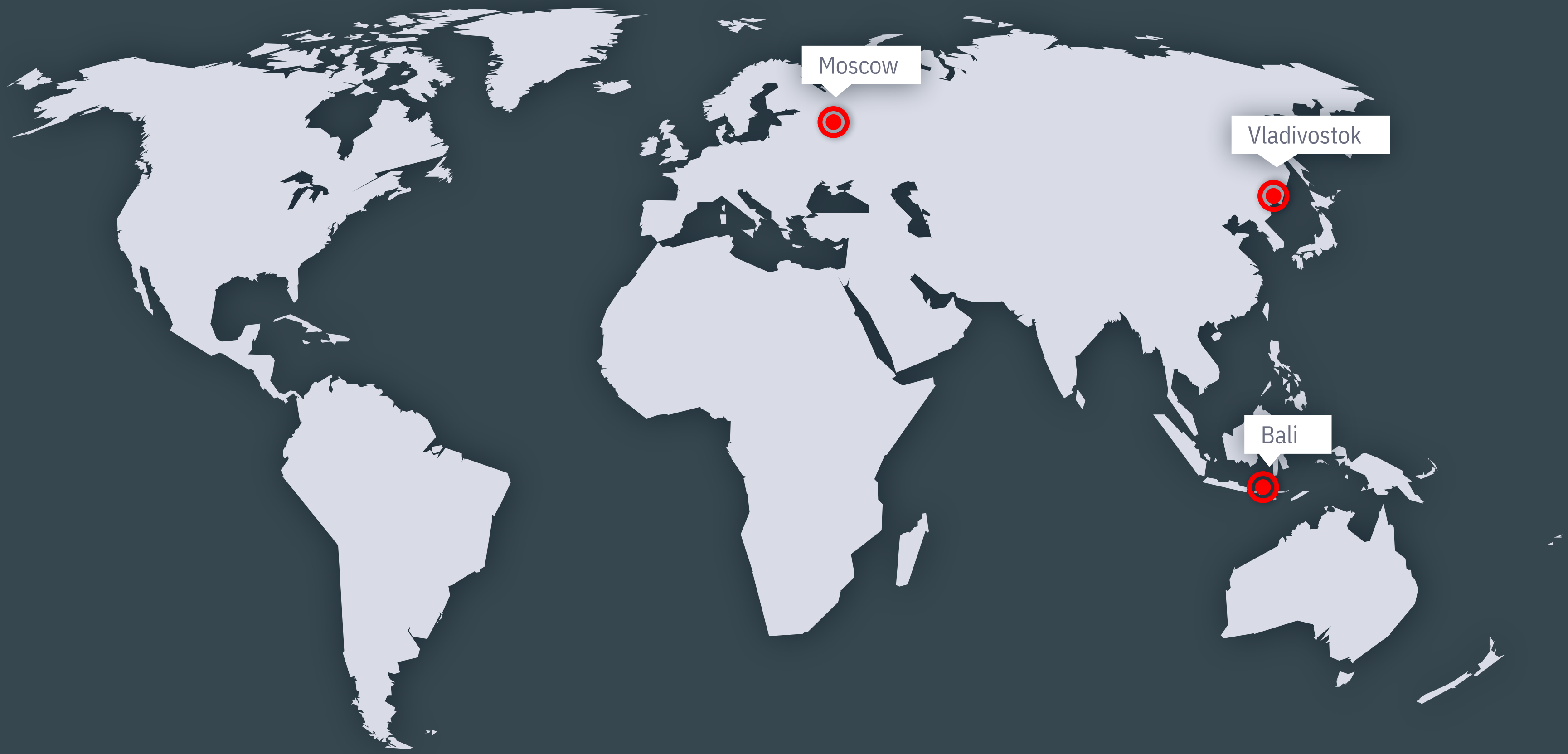
IBM

## whoisthis

Roman Seleznev

Russian native

Currently resides in FCI Butner Medium II in NC


Moscow
Vladivostok
Bali

1

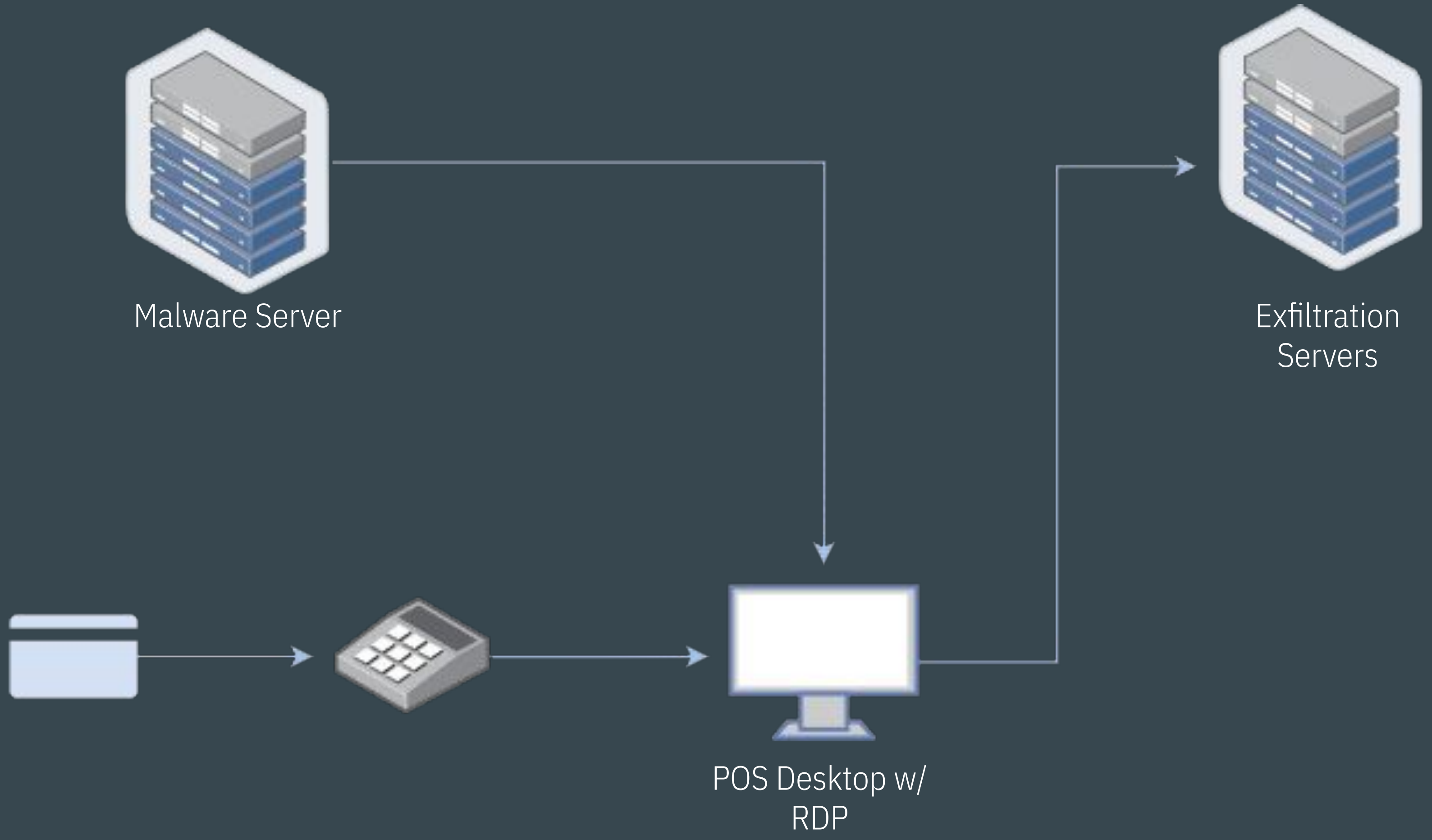
# A Timeline

# A Timeline

2002
nCuX

# nCuX (Psycho)

- Alias used at age 18
- Involved in illegal forums since 2002
- Sold entire identities
  - Name, DOB, SSN
- Started to be tracked in 2005
- Moved to stolen credit card numbers in 2007


Malware Server
Exfiltration Servers
POS Desktop w/ RDP

# nCuX (Psycho)

- Scanned for open RDP
  - Guessed common passwords
    - Some businesses shared the same IT vendor that used one password
- Dropped malware to intercept credit card numbers
- Exfiltrated to Ukraine, Rusia, and Virginia servers
  - US eventually tapped network connection for McLean, VA server

# nCuX (Psycho)

“By 2009, nCuX had become one of the world’s leading providers of stolen credit card data. He was revered in the carding underworld and admired by thousands of other criminals.”

# nCuX (Psycho)

- Discovered to be Roman Seleznev
  - Met with FSB (Russian Federal Security Service) (formerly KGB)
- Announced retirement 4 weeks later
  - Father (Valery) is a member of Russian Duma

“In chat messages between Seleznev and an associate from 2008, Seleznev stated that he had obtained protection through the law enforcement contacts in the computer crime squad of the FSB.”

# A Timeline

2002
nCuX

2009
Track2

# Track2

“The Track2 and Bulba websites achieved instant success, and were perhaps the leading source of stolen credit data during the period they operated.”

# Track2

- Returned and created 2 websites track2[.]name and bulba[.]cc
- Automated purchasing
- In April 2011, posted **1 million** “fresh dumps” in a single day
- Indicted March 2011
- Gained access to his Yahoo email address

# Track2

https://whowhatwhy.org/2017/04/24/price-bp-oil-spill/

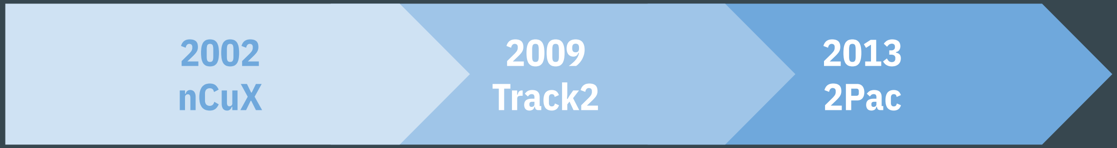
# Track2

Hôtel Restaurant Café de France
Restaurant Panoramique
Terrasse Panoramique
Terrasse Panoramique Café Restaurant
pepsi
Residence La Place
إقامة السّاحة
CENTRE

# Track2

- Injured in Marrakesh, Morocco bombing while on vacation
  - Secret service was set up
- In a coma for 2 weeks. In hospital for 1 year. Wife leaves him.
- Shop closed by partners in 2012

# A Timeline


2002
nCuX

2009
Track2

2013
2Pac

# 2Pac

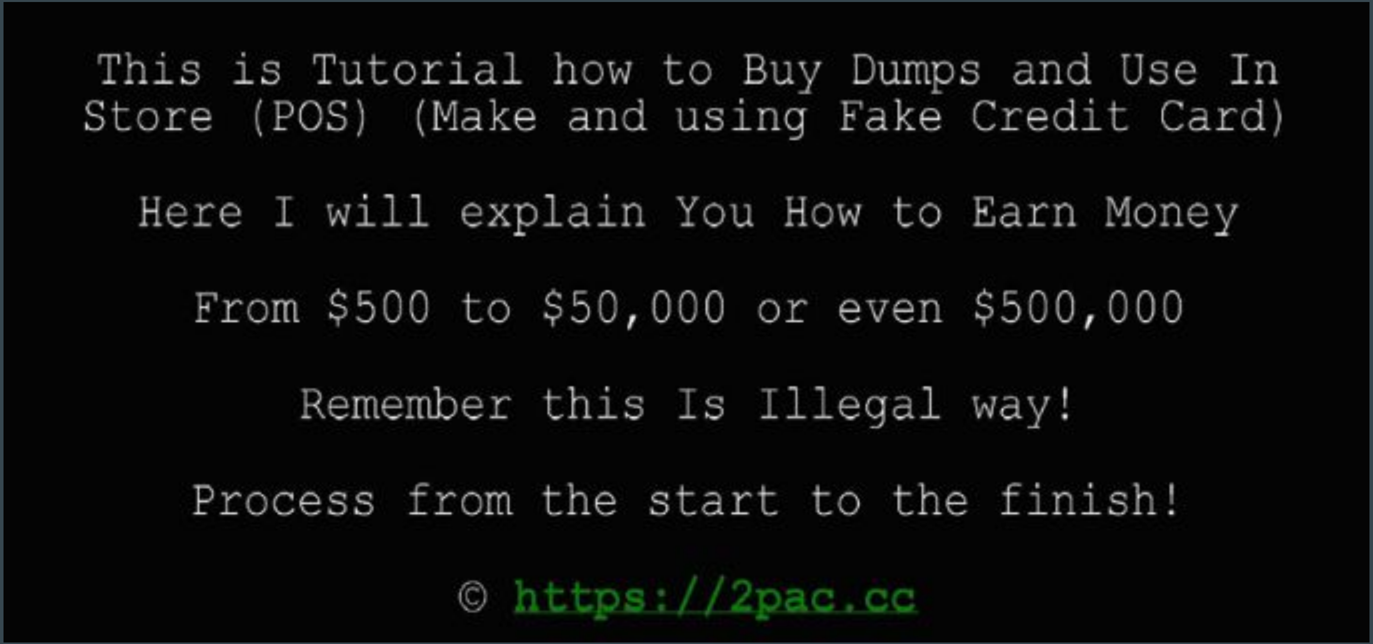
“Seleznev resold credit data stolen by some of the world’s most notorious hackers, including data stolen in the breaches of Target, Michaels, and Nieman Marcus.”

# 2Pac

Several new improvements

- Started reselling for other hackers
    - Previously only sold first-hand dumps
    - Sold cards from breaches like Target, Michaels, and Home Depot
- 24/7 support!

Likened to Amazon



This is Tutorial how to Buy Dumps and Use In Store (POS) (Make and using Fake Credit Card)

Here I will explain You How to Earn Money

From $500 to $50,000 or even $500,000

Remember this Is Illegal way!

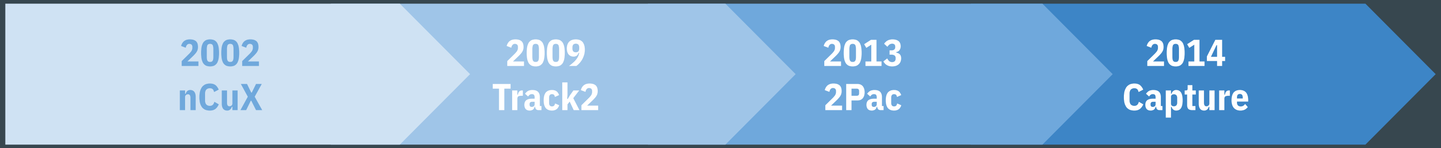
Process from the start to the finish!

© https://2pac.cc

# 2Pac

- Created ‘POS Dumps’ as a tutorial site
  - Taught n00bs how to use stolen cards
    - Write to blank cards
    - Find zip code and credit limit
  - Advertised 2Pac site
- In first month, 3,369 unique visitors

# A Timeline



2002
nCuX

2009
Track2

2013
2Pac

2014
Capture

# Capture

“…in imposing sentence, the Court should consider the near-impossibility of apprehending Seleznev again if he returns to crime after his release.”

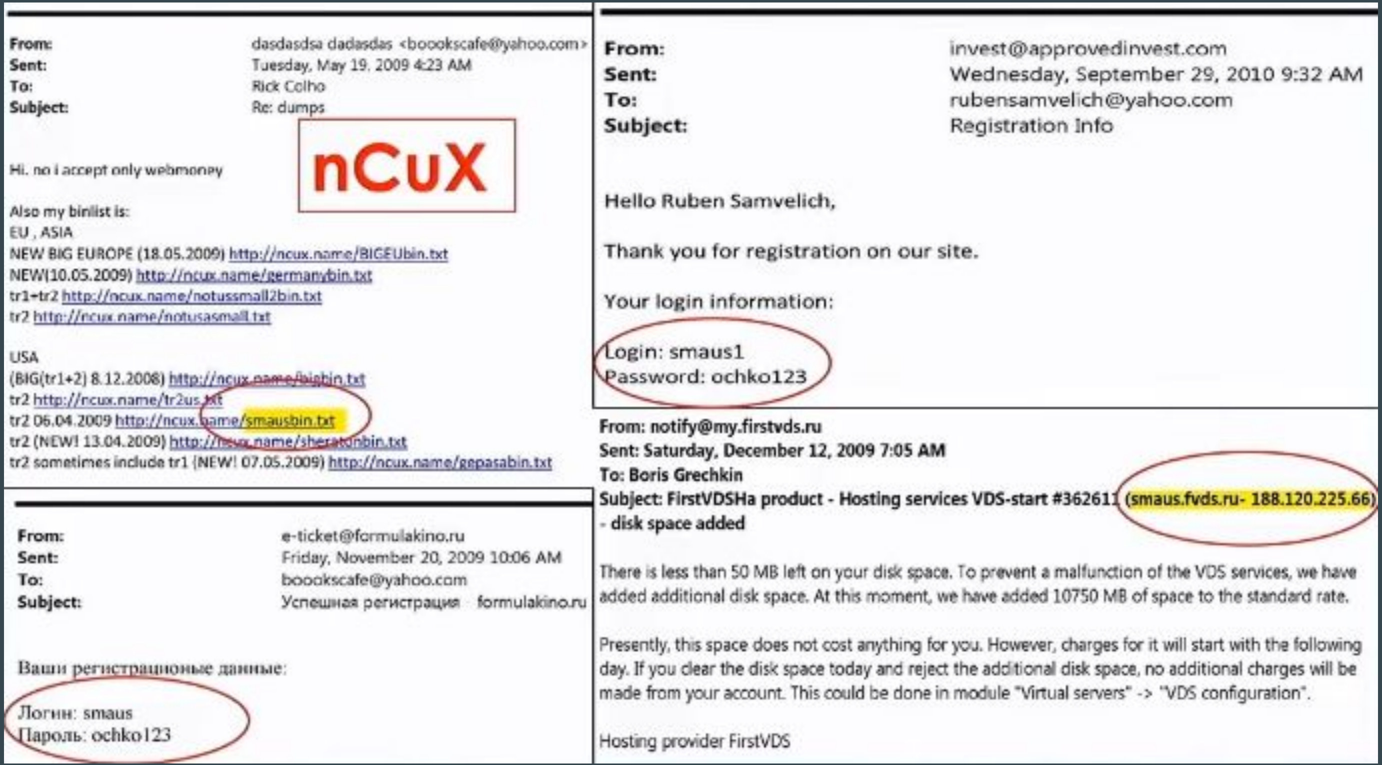
# Capture

- Received tip that Seleznev was in Maldives on July 1st and would be leaving on the 5th
    - No extradition treaty
    - 18 hour flight from Hawaii
- Intercepted at airport
- Flown to Guam

2

# Forensics

# Emails



**From:** dasdasdsa dadasdas <boookscafe@yahoo.com>
**Sent:** Tuesday, May 19, 2009 4:23 AM
**To:** Rick Colho
**Subject:** Re: dumps

nCuX

Hi. no i accept only webmoney

Also my binlist is:
EU , ASIA
NEW BIG EUROPE (18.05.2009) http://ncux.name/BIGEUbin.txt
NEW(10.05.2009) http://ncux.name/germanybin.txt
tr1+tr2 http://ncux.name/notussmall2bin.txt
tr2 http://ncux.name/notusasmall.txt

USA
(BIG(tr1+2) 8.12.2008) http://ncux.name/bigbin.txt
tr2 http://ncux.name/tr2us.txt
tr2 06.04.2009 http://ncux.name/smausbin.txt
tr2 (NEW! 13.04.2009) http://ncux.name/sheratonbin.txt
tr2 sometimes include tr1 (NEW! 07.05.2009) http://ncux.name/gepasabin.txt

**From:** e-ticket@formulakino.ru
**Sent:** Friday, November 20, 2009 10:06 AM
**To:** boookscafe@yahoo.com
**Subject:** Успешная регистрация - formulakino.ru

Ваши регистрационые данные:

Логин: smaus
Пароль: ochko123

**From:** invest@approvedinvest.com
**Sent:** Wednesday, September 29, 2010 9:32 AM
**To:** rubensamvelich@yahoo.com
**Subject:** Registration Info

Hello Ruben Samvelich,

Thank you for registration on our site.

Your login information:

Login: smaus1
Password: ochko123

**From: notify@my.firstvds.ru**
**Sent: Saturday, December 12, 2009 7:05 AM**
**To: Boris Grechkin**
**Subject: FirstVDSHa product - Hosting services VDS-start #362611 (smaus.fvds.ru- 188.120.225.66) - disk space added**

There is less than 50 MB left on your disk space. To prevent a malfunction of the VDS services, we have added additional disk space. At this moment, we have added 10750 MB of space to the standard rate.

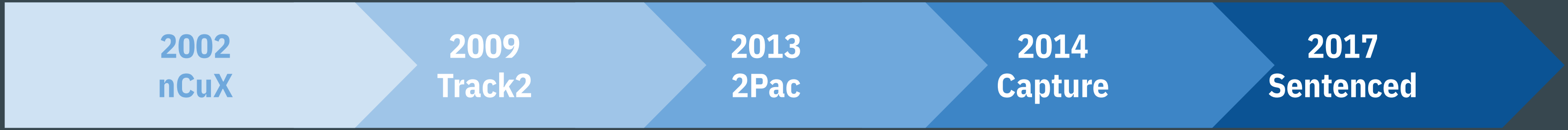
Presently, this space does not cost anything for you. However, charges for it will start with the following day. If you clear the disk space today and reject the additional disk space, no additional charges will be made from your account. This could be done in module "Virtual servers" -> "VDS configuration".

Hosting provider FirstVDS

ochko123

# 1.7M Credit Card Numbers

# A Timeline



2002
nCuX

2009
Track2

2013
2Pac

2014
Capture

2017
Sentenced

# Sentencing

"…the high probability that he will return to his life as a criminal mastermind requires a substantial sentence…"

# Sentencing

- Consistently tried to delay court dates by being uncooperative
  - Went through multiple lawyers
  - Cut off communication
  - Committed perjury
- Tried to bribe prosecutors $10M

- Forced small businesses to close
- Offense level of 59 according to Federal Sentencing Guidelines
  - Recommends life sentence
  - Guidelines max out at 43

# 27 Years in Prison

Most time given for a cybercrime

# 38 Counts

Acquitted of 2 counts

# $169,418,843 in Restitution

$465,742.95 to victim businesses

# Sentencing

- Most prison time ever given to an individual convicted of cybercrime charges in the United States.
- 9 counts of hacking
- 10 counts of wire fraud
- Charged with Possession of Fifteen or More Unauthorized Access Devices (Had 1.7M)
- Other cases in Nevada, Atlanta, and Washington state

# Questions?