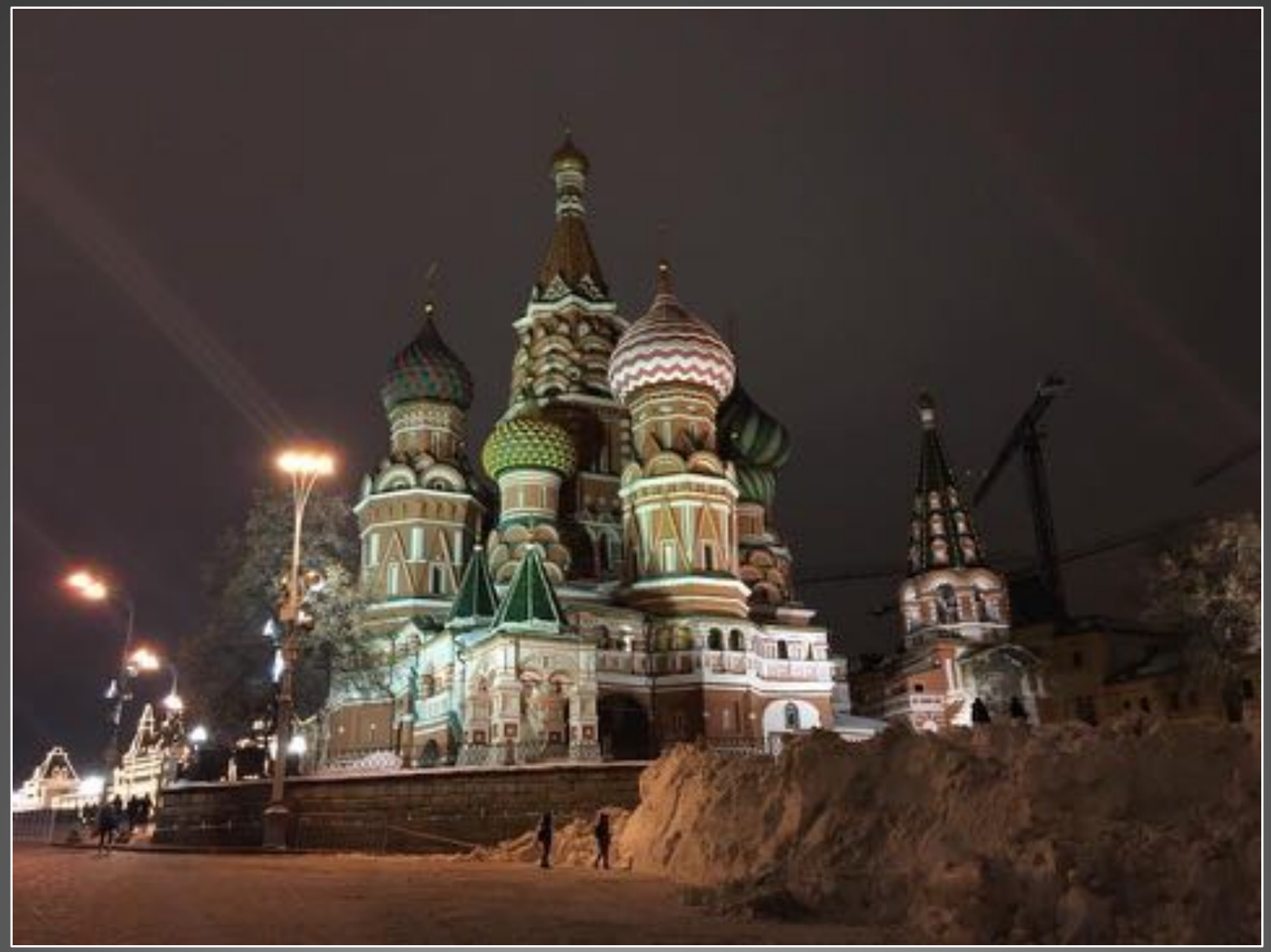
Kimberly Zenz
Deutsche Cyber-Sicherheitsorganisation

Infighting Among Russian Security Services in the Cyber Sphere

(or how Brian Krebs made the FSB search my apartment)

A Note on Russia



The Current Situation

Escalating Infighting

- Not unique to Russia, but more pronounced than in some other countries, or even in Russia a few years ago
- A range of causes, from geopolitical pressures, economic uncertainty, elite conflicts, shifting power from formal institutions, unpredictable future
  - Escalation starting 2014
- A common phrase is “previously unthinkable”

Serious Infighting Outcomes

- Pre-2014(ish): disgrace, departure
- Now: arrest and prison
- Previously safe positions now insecure
- More arrests

National Elites

- 35 high-ranking officials prosecuted
- 25 given prison time
- 18 more than 5 years

Regional Elite:

- 18-20 arrested
- From about 800 regional elites

Why Care?

- Russian security agencies often approached as a monolithic whole, but they aren’t that
- Internal politics drives interests of people within Russia's security services
- Security agencies are incentivized to take risks and act aggressively

What We Know

Some Major Players

MVD

GRU

FSB

CIB

Military Unit №43753

CZI

Military Unit №43753

KASPERSKY lab

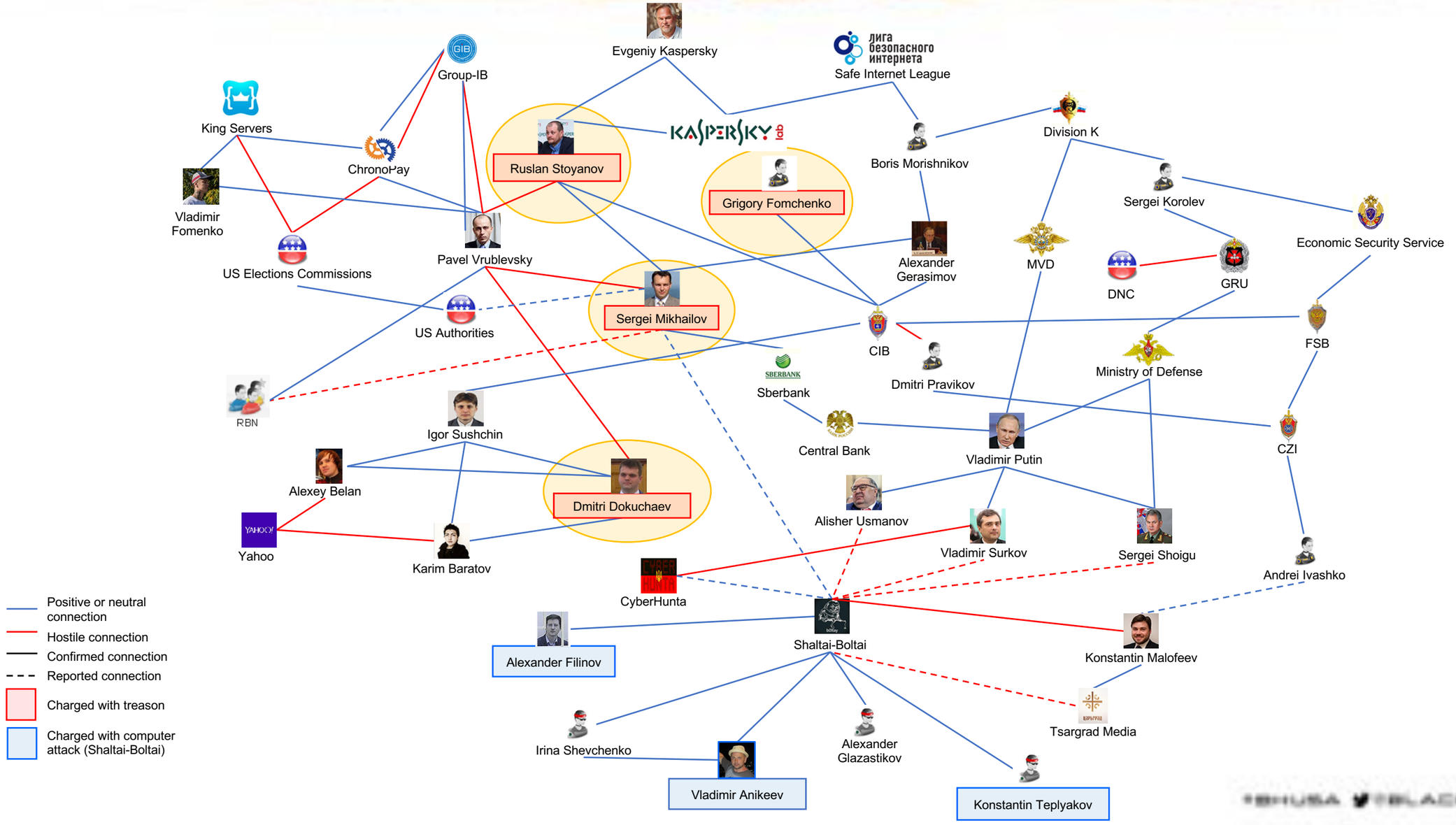
Observable Infighting - Public

- Media reports of takeover attempts
- Reports of transferred responsibilities
- Competing cyber doctrines
- Similar responsibilities given to multiple divisions
- Arrests and their results

Observable Infighting – Overlapping Attacks

- Multiple cases of multiple Russian agencies going after the same sectors and even the same organizations
- In Germany, best-known case is that of the German Bundestag hacks
- In US, Democratic National Committee (DNC)

The Treason Case


Evgeniy Kaspersky
Group-IB
Safe Internet League
King Servers
ChronoPay
Ruslan Stoyanov
Boris Morishnikov
Division K
Vladimir Fomenko
Grigory Fomchenko
Sergei Korolev
Economic Security Service
US Elections Commissions
Pavel Vrublevsky
Alexander Gerasimov
MVD
DNC
GRU
Sergei Mikhailov
CIB
FSB
US Authorities
Dmitri Pravikov
Ministry of Defense
Sberbank
RBN
Igor Sushchin
Central Bank
Vladimir Putin
CZI
Alexey Belan
Dmitri Dokuchaev
Alisher Usmanov
Vladimir Surkov
Sergei Shoigu
Andrei Ivashko
Yahoo
Karim Baratov
CyberHunta
Shaltai-Boltai
Konstantin Malofeev
Alexander Filinov
Tsargrad Media
Irina Shevchenko
Alexander Glazastikov
Vladimir Anikeev
Konstantin Teplyakov
Positive or neutral connection
Hostile connection
Confirmed connection
Reported connection
Charged with treason
Charged with computer attack (Shaltai-Boltai)

The Accused

- Ruslan Stoyanov
- Sergei Mikhailov
- Dmitri Dokuchaev
- Grigory Fomchenko
- Me (indirectly)


The Accusations

- Russian reports: In 2010, FBI paid FSB officers Sergei Mikhailov and Dmitri Dokuchaev $10,000,000 to deliver two CDs containing information about well-known Russian cybercriminal Pavel Vrublevksy
  - Shortly before Vrublevsky's arrest and conviction in Russia
  - Fomchenko said to have flew to America to deliver one
  - Stoyanov said to have given it to an "American (me) at a cybercrime conference
- Problematic

So Why Then?

- INFIGHTING
- More than “Vrublevsky’s revenge”
- Stepping on other toes?
- Treason as a tool
  - Chilling effect on information sharing
- Pressure on Kaspersky to re-form and formalize relationship with winners and the state
- Still, something happened to weaken FSB leaders and Kaspersky Lab

Infighting at the FSB

- CIB and CZI have areas of overlapping responsibilities, compete
- Reaction to Dmitri Pravikov Case?
- CZI visibly influential now
- Head of CZI to lead new FSB cyber defense center

Shaltai-Boltai

- “Hacktivist” (extortion) group
- Compromised Russian leadership, some businesspeople
- Blackmailed some, posted some
- Arrested around same time as treason defendants
- Leader Anikeev reported cooperating, charges and sentence surprisingly low, already free
- Rumor
  - Mikhailov and Dokuchaev (not Stoyanov or Fomchenko!) investigated them, turned them for money and patron’s politics
  - Complication: one victim (oligarch Usmanov) caught them doing something else…

Collaboration with the United States

- Two versions of the rumors – both assume FSB-GRU infighting
- Also just Mikhailov and Dokuchaev
- Rumor One: Source of King Servers-ChronoPay connection
- Rumor Two: Source of Mueller GRU indictment for hacking DNC
- Possibly just an indication of perceived infighting levels

Why Stoyanov?

- Stoyanov not mentioned even in the wildest rumors
- He opposed working with cybercriminals
- Pressure on Kaspersky
  - Kaspersky a close ally of CIB
- Ruslan Stoyanov well known
- Bad luck

Results

- Ruslan Stoyanov – denied guilt, 14 years in prison
- Sergei Mikhailov – denied guilt, 22 years in prison
- Dokuchaev - plead guilty, 6 years in prison
- Fomchenko – testified for the prosecution 7 years in prison
- Extra
  - General Alexander Gerasimov resigned

Lessons Learned

Lessons Learned

- Some people just want to be difficult
- Not all the “good guys” are good
  - Some media will get it wrong
  - Can you trust Brian Krebs?
  - Can you trust Group-IB?

A Shakeup in Russia’s Top Cybercrime Unit

My book *Spam Nation* identified most of the world’s top spammers and virus writers by name, and I couldn’t have done that had someone in Russian law enforcement not leaked to me and to the FBI tens of thousands of email messages and documents stolen from ChronoPay’s offices.

To this day I don’t know the source of those stolen documents and emails. They included spreadsheets chock full of bank account details tied to some of the world’s most active cybercriminals, and to a vast network of shell corporations created by Vrublevsky and ChronoPay to help launder the proceeds from his pharmacy, spam and fake antivirus operations.

ВЕДОМОСТИ

База пользователей процессинговой системы Chronopay взломана 28 декабря 2010 00:38

запрос «Ведомостей» не ответили. Около трех недель назад база данных Directnic была взломана, злоумышленники получили доступ к информации, позволяющей управлять рядом сайтов, в том числе и Chronopay, в расследовании этого инцидента принимала участие Group-IB, говорит ее гендиректор Илья Сачков. Он уверен, что пострадала только «витрина» Chronopay – процессинг остался невредим, утечки персональных данных также не было. Хакеры могли получить доступ к данным о кредитных картах

Lessons Learned

- Some people will surprise you
  - American journalists
  - Russian journalists
- All plans may not be enough
- Your broader networks' risks are also your risks
- Good work can be real trouble (but is still worth it!)

Black Hat Sound Bytes

Infighting among Russian security services increasing

•

Drives riskier and more aggressive action abroad

•

It discourages international cooperation and dialogue

•

This makes us all less safe

Questions?