
# When Governments Attack!

Eva Galperin / Global Policy Analyst / eva@eff.org
Cooper Quintin / Staff Technologist / cooperq@eff.org

# Whois?

Eva Galperin

Cooper Quintin

Morgan Marquis-Boire

Claudio Guarnieri

# What is EFF?


"What Binge On does, it includes a proprietary technology and what the technology does is not only detect the video stream but select the appropriate bit rate to optimize to the video, the mobile device. That's part A of my answer. Part B of my answer is, who the fuck are you, anyway, EFF? Why are you stirring up so much trouble, and who pays you?" - John Legere

# Q: Who the Fuck are you, anyway, EFF?

# Legal Work

# Coders' Rights Project

# Q: Why are you stirring up so much trouble?

# Activism


NSA
ILLEGAL SPYING BELOW
StandAgainstSpying.org
GREENPEACE


TELL CONGRESS:
CFAA Is Broken – Don't Make It Worse

# International Work

MAY 28, 2015 | BY NATE CARDOZO AND EVA GALPERIN

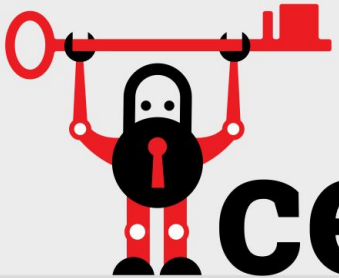
## What Is the U.S. Doing About Wassenaar, and Why Do We Need to Fight It?

On May 20, 2015, the U.S. Department of Commerce's Bureau of Industry and Security (BIS) published its proposed implementation of the December 2013 changes to the Wassenaar Arrangement. What follows is a long post, as we're quite troubled by the BIS proposal. In short, we're going to be submitting formal comments in response, and you should too.

### What is the Wassenaar Arrangement?

The Wassenaar Arrangement is a multi-national agreement intended to control the export of certain

# Technology



certbot

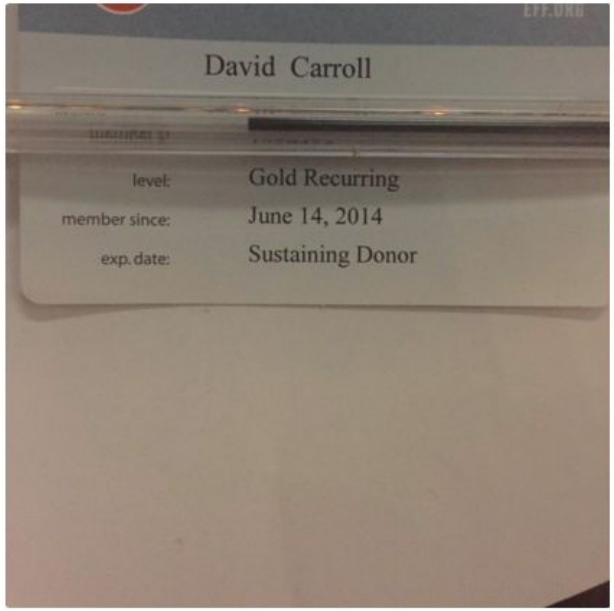
Automatically enable HTTPS on your website.

HTTPS Everywhere

# Q: Who pays you?

david carroll
@davidecarroll
Following

Hi @JohnLegere, it's people like me that pay @EFF. Hope that answers your question. #WeAreEFF




RETWEETS 4 LIKES 7

1:50 PM - 7 Jan 2016

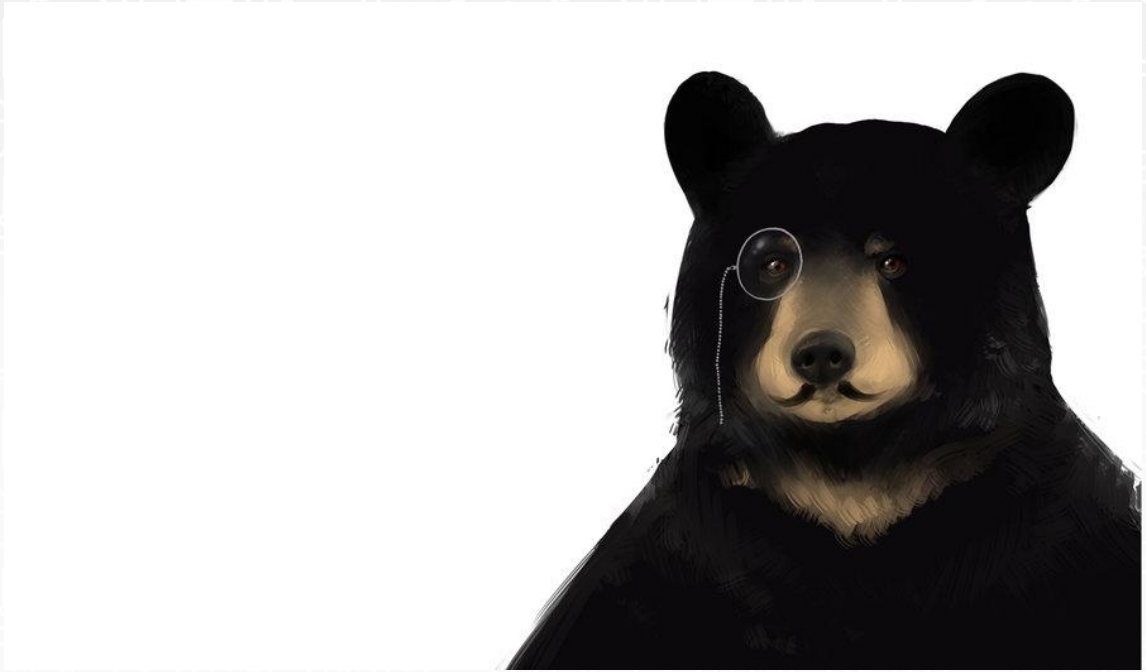
# Targeted Attacks


VIETNAM

# Ethiopia

# Iran

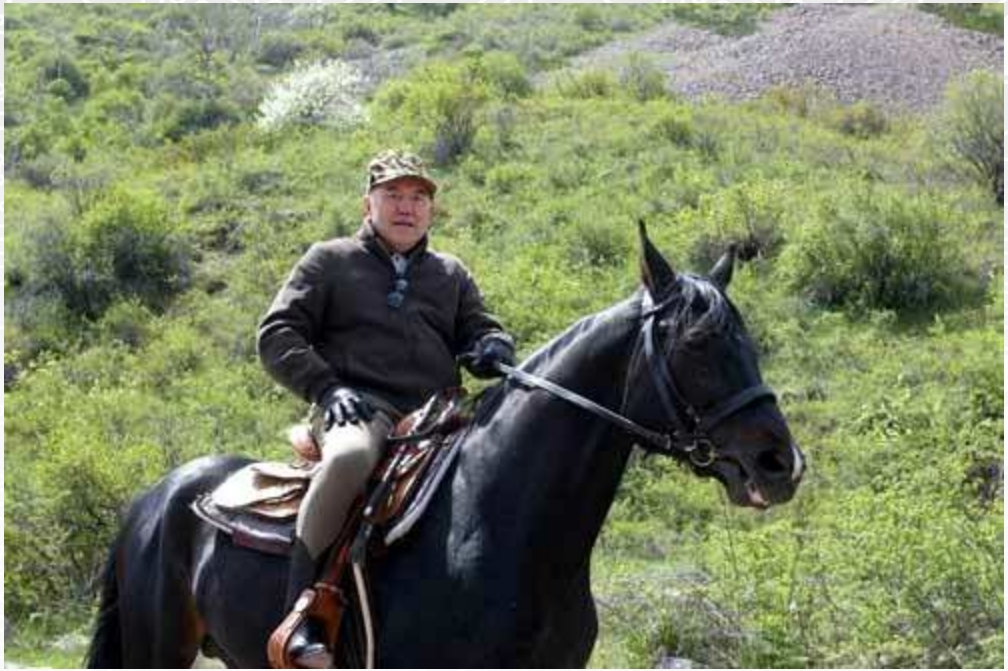
# Pawn Storm / FancyBear / APT28



Nobody Cares About Kazakhstan

# Operation Manul

Kazakhstan is here!




EPA

## 2015 SCORES

PRESS STATUS

**Not Free**

PRESS FREEDOM SCORE
(0 = BEST, 100 = WORST)

**85**

LEGAL ENVIRONMENT
(0 = BEST, 30 = WORST)

**29**

POLITICAL ENVIRONMENT
(0 = BEST, 40 = WORST)

**33**

ECONOMIC ENVIRONMENT
(0 = BEST, 30 = WORST)

**23**

DECEMBER 10, 2015 | BY BILL BUDINGTON AND EVA GALPERIN

# Kazakhstan Considers a Plan to Snoop on all Internet Traffic

In an unusually direct attack on online privacy and free speech, the ruling regime of Kazakhstan appears to have mandated the country's telecommunications operators to intercept citizens' Internet traffic using a government-issued certificate starting on January 1, 2016. The press release announcing the new measure was published last week by Kazakhtelecom JSC, the nation's largest telecommunications company, but appears to have been taken down days later—the link above comes courtesy of the Internet Archive, which never forgets. It is unclear whether the retracted press release indicates that Kazakhstan's ruling regime has abandoned the plan in response to widespread criticism, or is simply planning to carry it out at some later date, once attention has died down.

The measure's apparent authority is the country's new communications law. EFF's analysis of the law finds plenty of vague language that could be used to justify this kind of mass surveillance, but nothing that explicitly requires government-issued certificates.

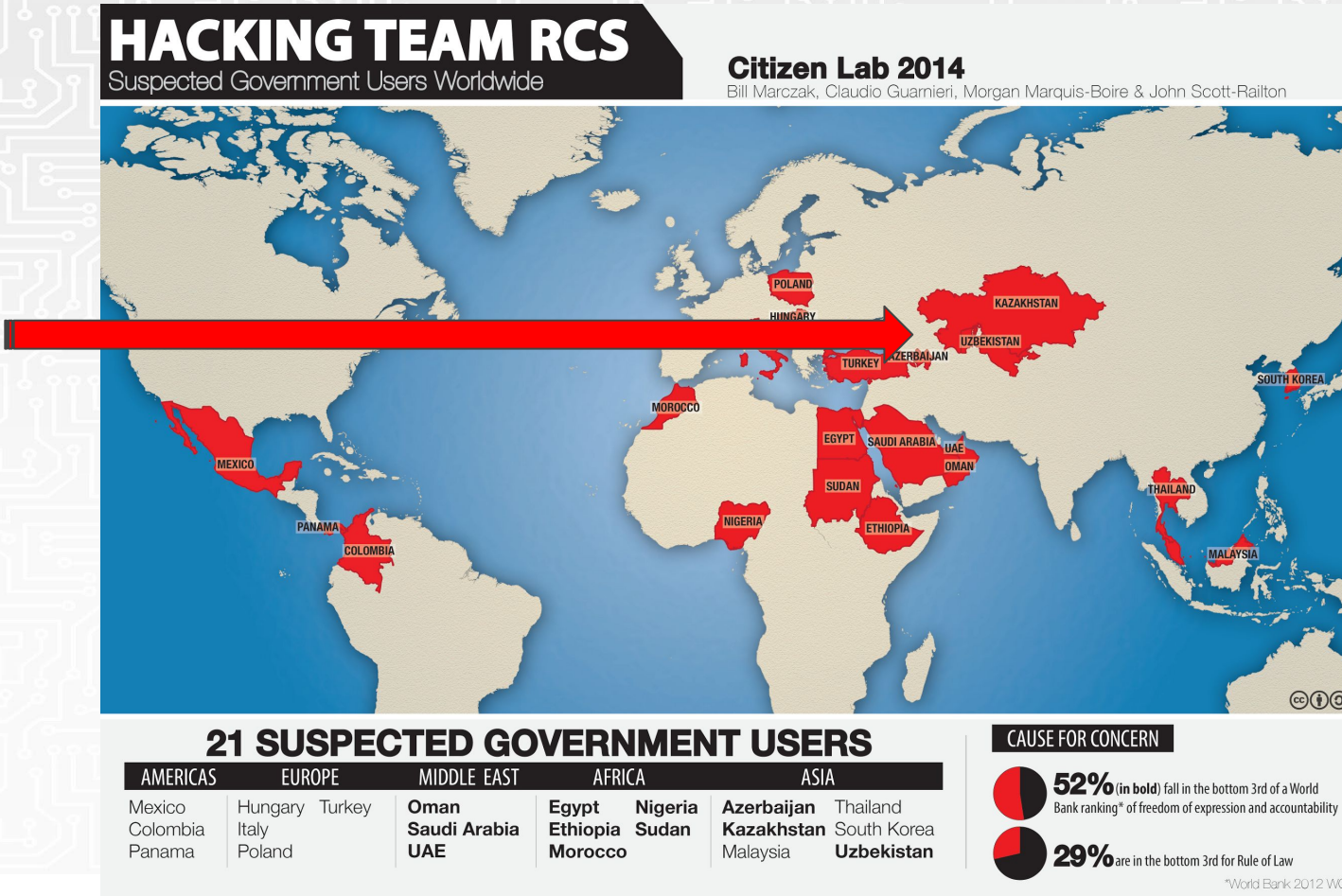
If the country's ruling regime were to successfully implement this plan, it would be able to snoop on, impersonate, and alter the online communications of anyone within their borders—effectively performing a Man in the Middle attack on its entire population. Operating systems and browsers maintain their own list of legitimate root certificates that come bundled with their software. Because of this, it is difficult for ordinary attackers to pull off a Man in the Middle attack successfully on encrypted Internet connections—they have to both be situated in a privileged position within the network (between the user and the remote server), and in


NOTHING

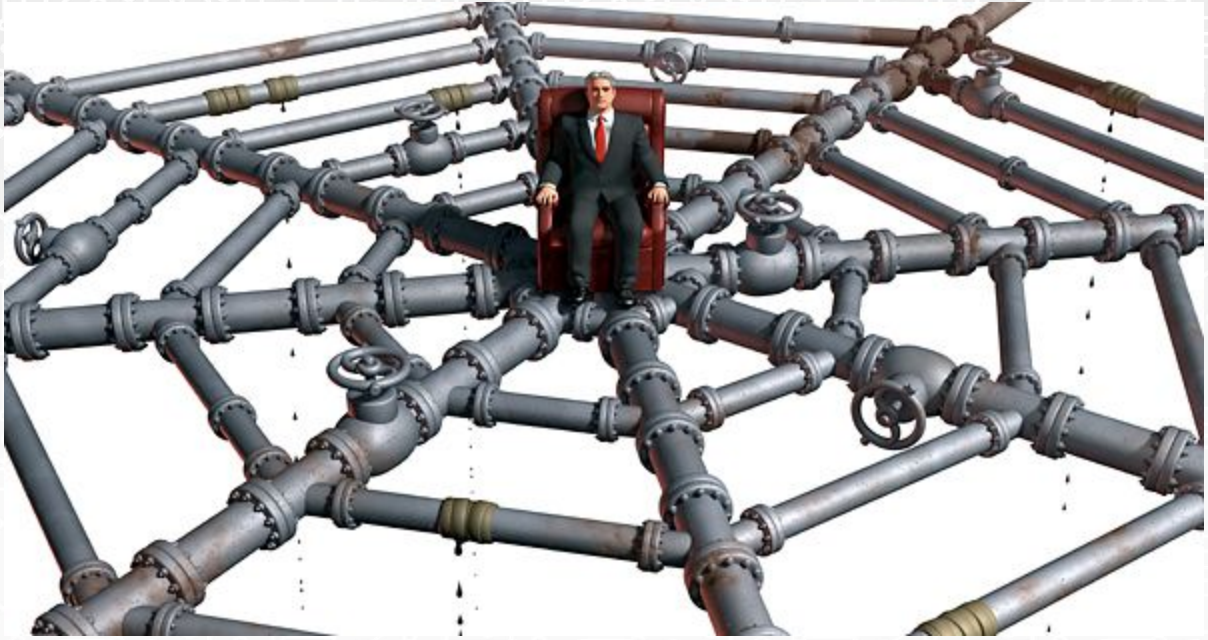
KZ!


KAZAKHSTAN
MONGOLIA
TURKMENISTAN
BOSNIA
SERBIA
ITALY
MACEDONIA
SPAIN
TURKEY
LEBANON
MOROCCO
JORDAN
EGYPT
SAUDI ARABIA
OMAN
BANGLADESH
TAIWAN
MEXICO
VENEZUELA
NIGERIA
ETHIOPIA
MALAYSIA
GABON
KENYA
INDONESIA
ANGOLA
PARAGUAY
SOUTH AFRICA
FINFISHER SPYWARE
Suspected Government Users In 2015
Citizen Lab 2015
Bill Marczak, John Scott-Railton,
Adam Senft, Irene Poetranto & Sarah McKune

KZ!


HACKING TEAM RCS
Suspected Government Users Worldwide
Citizen Lab 2014
Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire & John Scott-Railton
POLAND
HUNGARY
KAZAKHSTAN
UZBEKISTAN
TURKEY
AZERBAIJAN
SOUTH KOREA
MOROCCO
EGYPT
SAUDI ARABIA
UAE
OMAN
MEXICO
SUDAN
THAILAND
NIGERIA
ETHIOPIA
PANAMA
COLOMBIA
MALAYSIA
21 SUSPECTED GOVERNMENT USERS
AMERICAS
Mexico
Colombia
Panama
EUROPE
Hungary
Italy
Poland
Turkey
MIDDLE EAST
Oman
Saudi Arabia
UAE
AFRICA
Egypt
Ethiopia
Morocco
Nigeria
Sudan
ASIA
Azerbaijan
Kazakhstan
Malaysia
Thailand
South Korea
Uzbekistan
CAUSE FOR CONCERN
52% (in bold) fall in the bottom 3rd of a World Bank ranking* of freedom of expression and accountability
29% are in the bottom 3rd for Rule of Law
*World Bank 2012 WG


Irina Petrushova



NO DOGS WERE HARMED IN THE MAKING OF THIS TALK.

WE LOVE DOGS.

PLEASE ENJOY THIS UNICORN PICTURE.

ALERTS | KAZAKHSTAN

# Kazakh authorities seize embattled weekly's print run



New York, September 18, 2009—The Committee to Protect Journalists condemns the seizure of the print run of one of the few remaining independent newspapers in Kazakhstan, which is set to take control of a leading security and human rights organization. The country will become chair of the Organization for Security and Co-Operation in Europe in 2010.

On Friday, court officers in the financial capital Almaty confiscated the entire print run of Almaty-based independent weekly *Respublika-Delovoye Obozreniye*, the Associated Press reported. Authorities also froze the bank accounts of the weekly and its publisher, news Web site *Lenta* reported. Court officials reportedly cited a September 9 verdict from the Medeu District Court in Almaty that ordered the weekly to pay 60 million Kazakh tenge (about US$400,000) to the state-owned BTA Bank in damages. The paper plans to file an appeal next week.


Assandi-Times
ЕЖЕНЕДЕЛЬНАЯ ГАЗЕТА
Назарбаев или его двойник?
«ЧЕРНАЯ МЕТКА»
ЗА КУЛИСАМИ ВИЗИТА

# I got a letter from the government the other day...

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

REPUBLIC OF KAZAKHSTAN,

Plaintiff,

v.

DOES 1 TO 100, INCLUSIVE,

Defendants.

No. 2:15-mc-0159-TLN-KJN

ORDER

Plaintiff The Republic of Kazakhstan ("Kazakhstan"), a sovereign nation, commenced this miscellaneous civil action and filed a motion to compel compliance with a subpoena issued to non-party Facebook, Inc. ("Facebook"). (ECF Nos. 1, 6.) Facebook and other non-parties, Respublika and LLC Media-Consult, have opposed the motion, and Kazakhstan filed a reply brief. (ECF Nos. 22, 24, 28.)[1]

After carefully considering the parties' written briefing, the court's record, and the applicable law, the court DENIES the motion without prejudice.[2]

[1] Based on the parties' stipulation, and for good cause shown, the court approved a special

# KAZAWORD

*Kaz news*

Home About

## О нас снова пишут...

May 6, 2016

http://www.zaprava.ru/201605055852/glavnyie-novosti-dnya/ne-dopusimi-ekstradicziyu-muxtara-ablyazova-iz-franczii-v-rossiyu

Открытое обращение российских правозащитников к представителям французских и британских властей, ООН, ЕС, ОБСЕ, и ПАСЕ, составленное на основании опубликованных в этом блоге документов. Обращение подписано Алексеевой Л.М., Борщевым В.В., Ганнушкиной С.А., Ковалевым С.А., Пономаревым Л.А., Световой З.Ф.

Leave a comment

Search ...

### RECENT POSTS

О нас снова пишут...
Два товарища
Наращиваем темп публикаций
О работе наших коллег
С днем дурака!

### RECENT COMMENTS

### ARCHIVES

May 2016
April 2016
March 2016
April 2015
March 2015
February 2015

Mukhtar Ablyazov


# Unveiling Operation Manul

Gmail by Google

111 111 <nicprivat4@gmail.com>

**Invoice Lexial ATABAYEV**

1 письмо

**eruc@lexial.eu** <eruc@lexial.eu> 12 августа 2015 г., 13:06
Кому: lotus@bp-pb.com

Dear Bota,

As agreed, please find attached our invoice.

Thank you in advance for the payment.

Best regards,

E. Ruchat

LEXIAL
SOCIETE D'AVOCATS

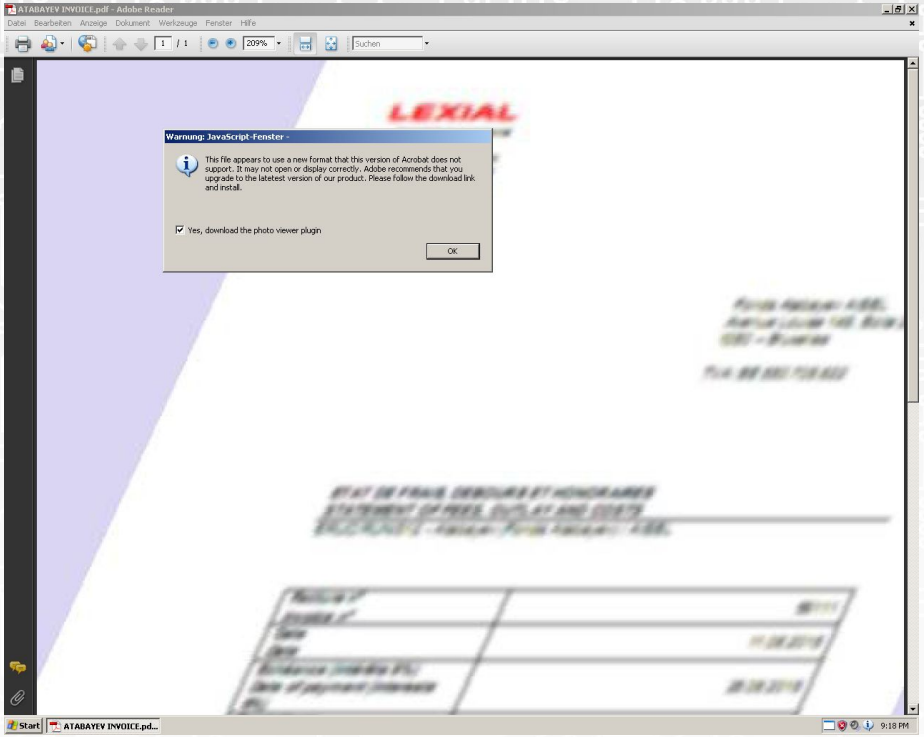
**Brussels office** : chaussée de Louvain 467, B-1030 Bruxelles - Tél. (English) (32)(0)2 880 79 52 – Tél. : (French) (32)(0)2 732 53 61 - Fax (32)(0)2 706 54 18

**Paris office** : 2 bis rue Guénégaud, F-75006 Paris - Tél. (33)(0)1 42 60 04 31 - Fax (33)(0)1 77 74 62 69

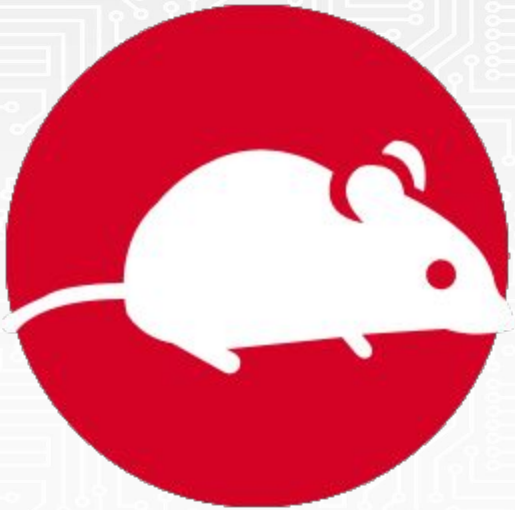
**Geneva office:** Route de St-Julien 184A, 1228 Plan-les-Ouates (Genève), Tel. : (41)(0) 951 08 25 - Fax : (41)(0) 22 594 80 88



ATABAYEV INVOICE.pdf
31K



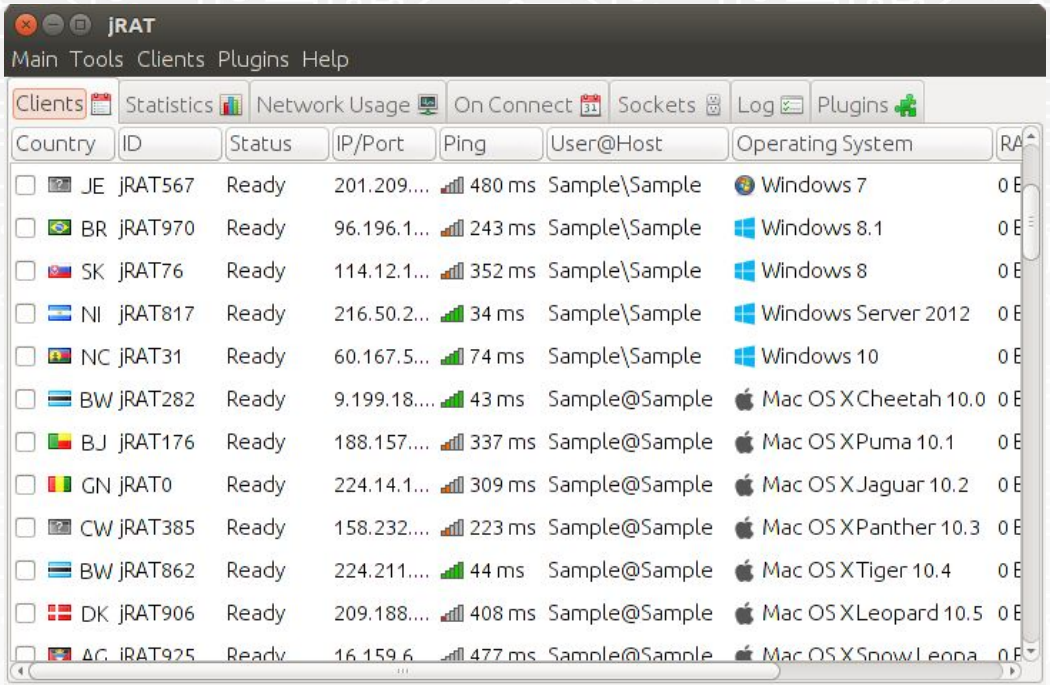
# JRat / Jacksbot



# JRat / Jacksbot

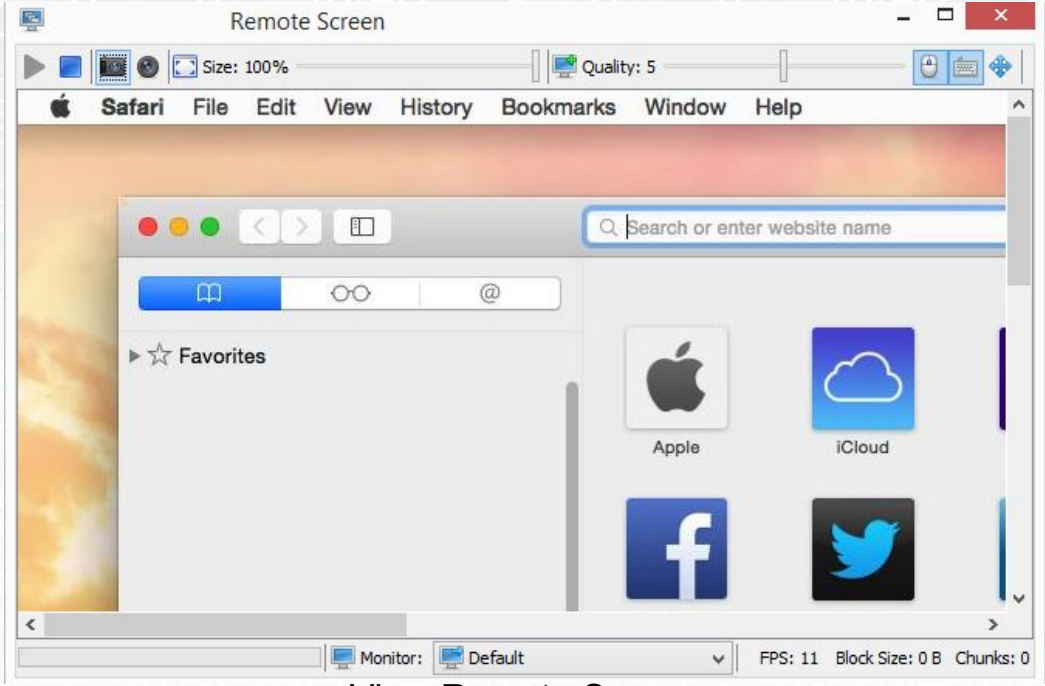
- Java Based
- Multi Platform
  - Win, Mac, Linux, Solaris, *BSD
- Plugin Architecture and API
- Cheap!

# JRat / Jacksbot



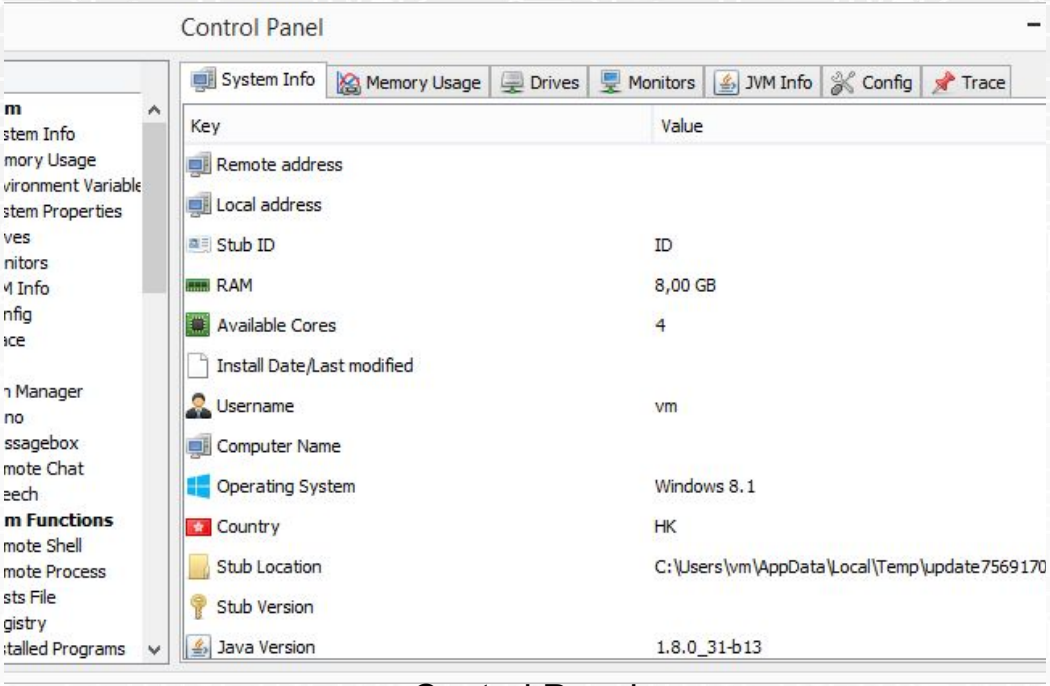

Server UI

# JRat / Jacksbot




View Remote Screen

# JRat / Jacksbot




Control Panel

# JRat / Jacksbot - Other Features

- Process List
- Remote Shell
- Chat
- Edit Registry
- Manage Remote Filesystem

# JRat / Jacksbot - Plugins

- Turn on remote webcam
- Disable webcam indicator light
- Password Recovery
- Keylogger
- Reverse SOCKS Proxy
- Roll Your Own...

# JRat / Jacksbot - Anti Analysis

- Bytecode obfuscated with Zendix Klass Master
- Encrypted config file
- Decryption key hidden in zip file metadata
- Detect Virtualization

# Bandook

- Another off the shelf, commodity RAT
- Continuously developed over a number of years
- Only targets Windows
- Modular:
  - Start shell, record sound, record video, keylogger, take screenshots, etc. etc.

# C&C Servers

Axroot.com, Adobeair.net, kaliex.net…

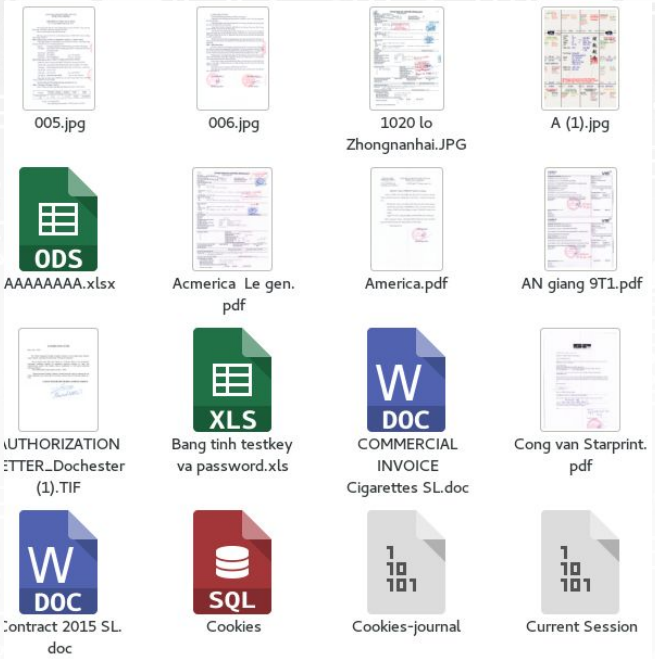
- Windows servers, running XAMPP
- Do not appear to be shared hosts
  - Not many domains / shared document root
- But they are not sitting idle!
  - Many open ports and many open directories

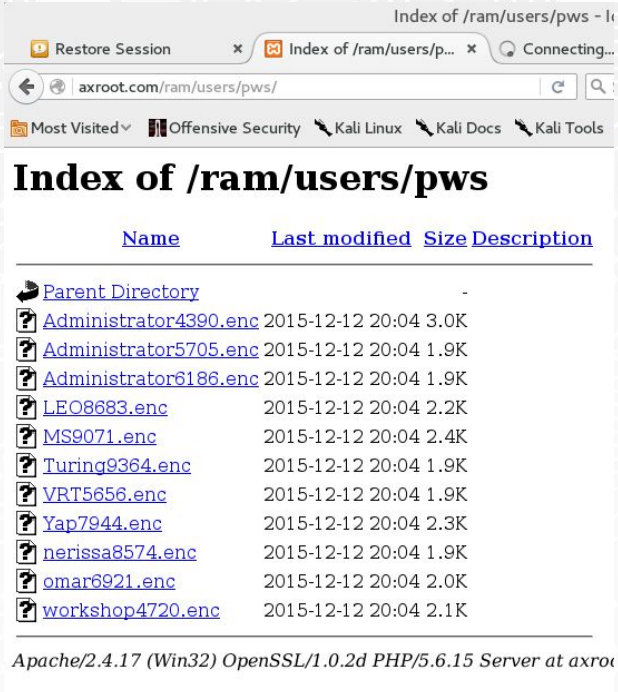
# C&C Servers

Axroot.com, Adobeair.net, kaliex.net…

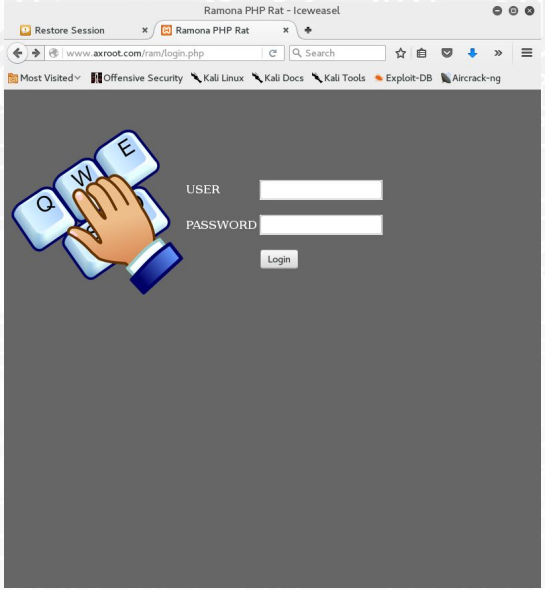
- Windows servers, running XAMPP
- Do not appear to be shared hosts
  - Not many domains / shared document root
- But they are not sitting idle!
  - Many open ports and many **open directories**

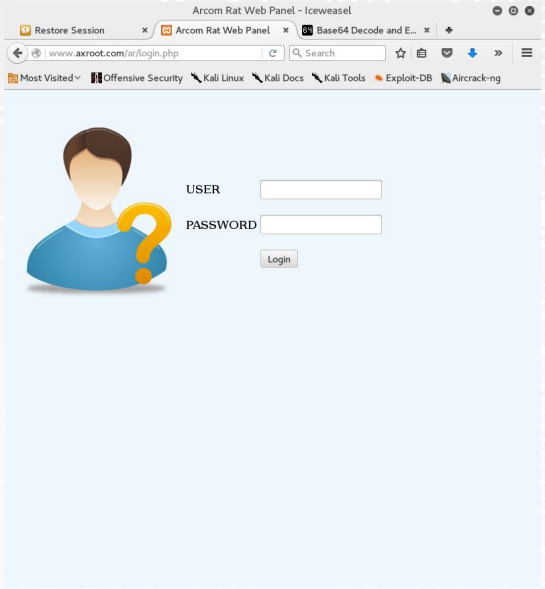
# Other Targets

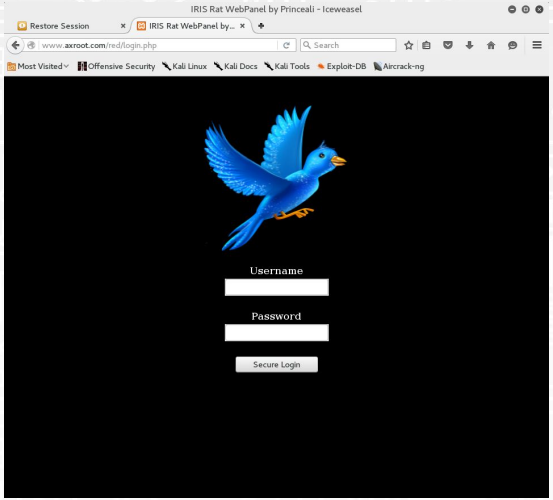


# Other Targets



# Attribution Is Hard

# Links to Kazakhstan

- Common thread between targets
  - Legal disputes against KZ government
- Phishing at private email address
  - Subpoenaed by Kazakhstan
- Arcanum Global Intelligence
  - Cyber Intelligence Operations
  - Hired by KZ to gather intel on Ablyazov family

# OPERATION HANGOVER

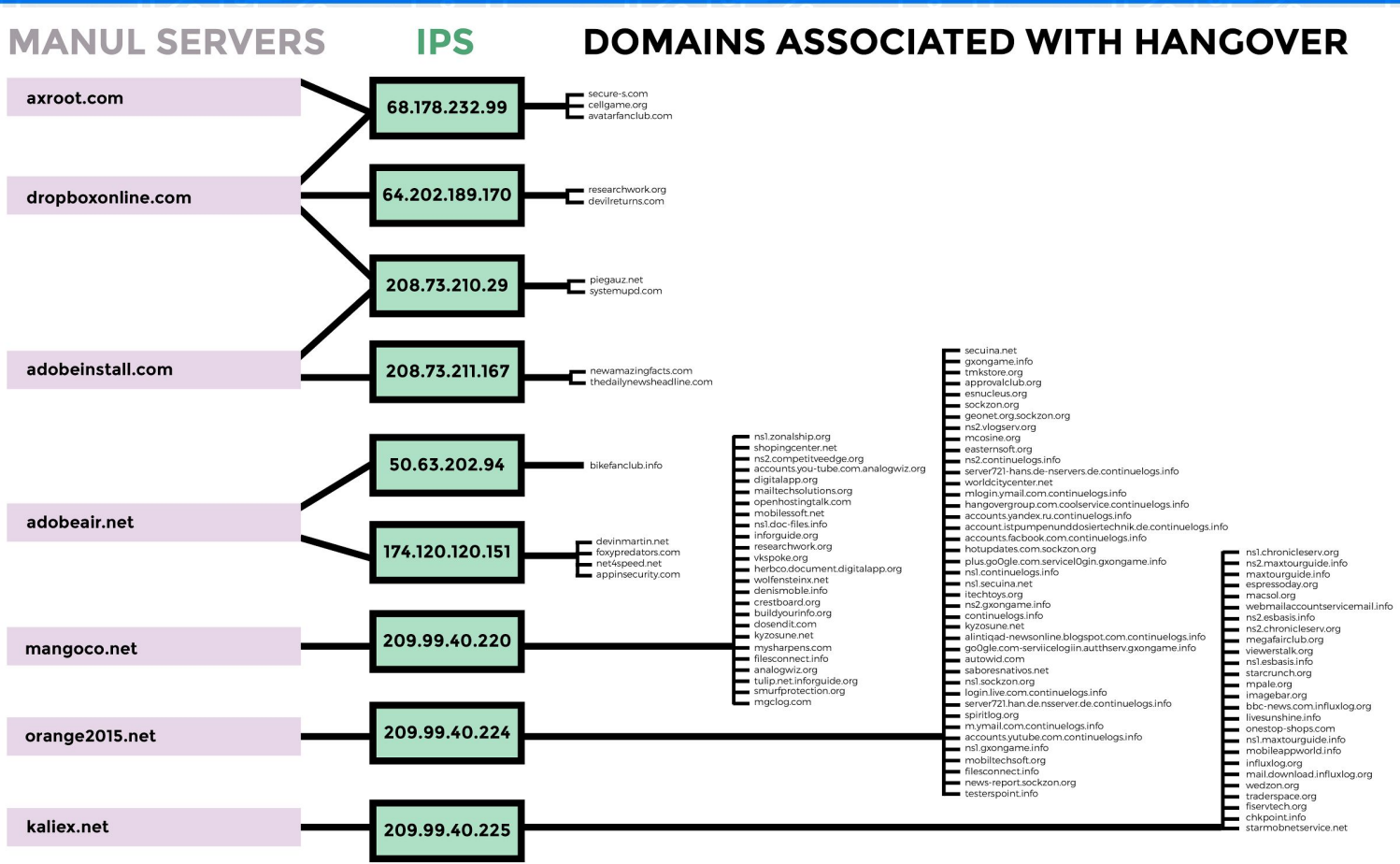
## Unveiling an Indian Cyberattack Infrastructure

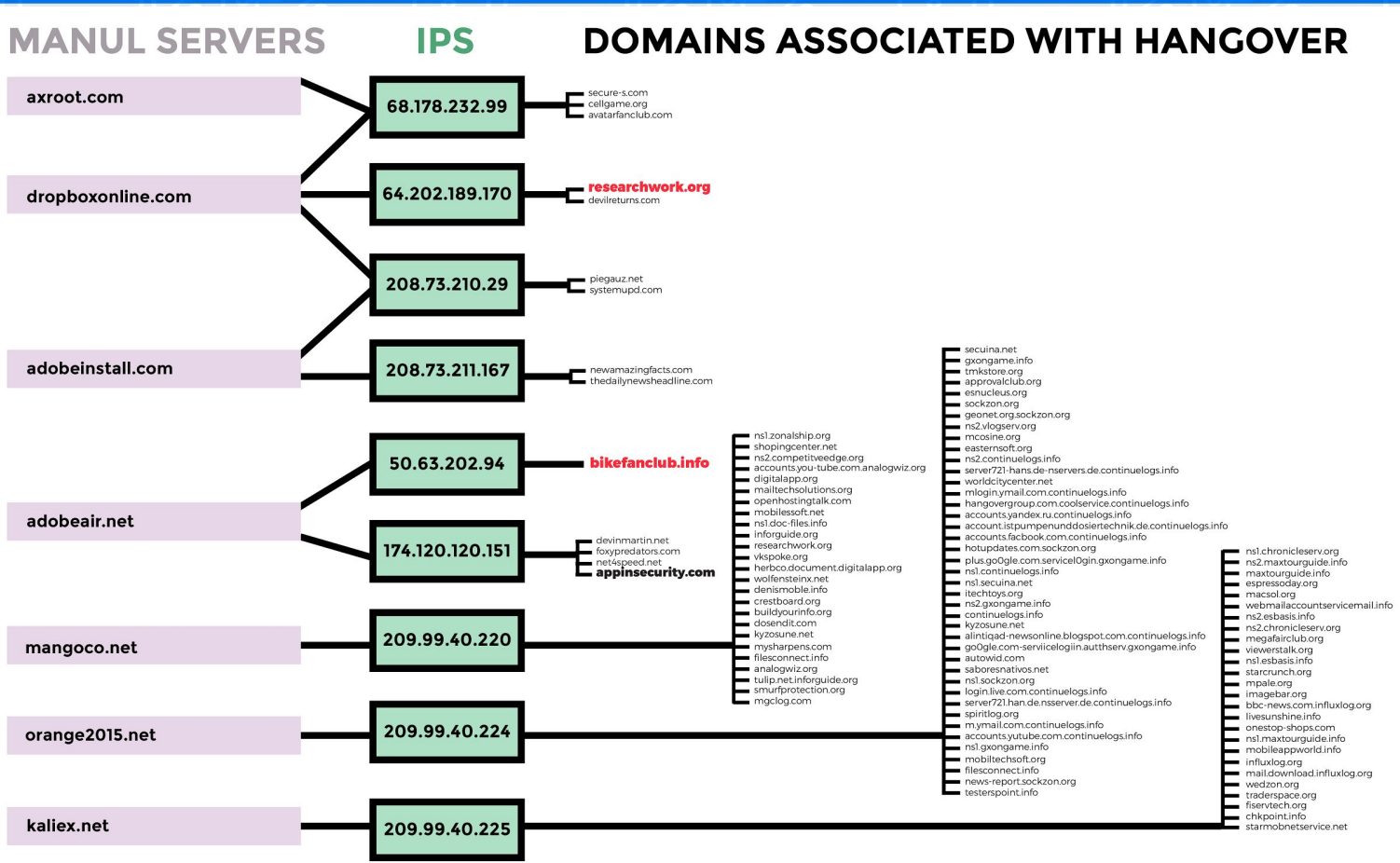
Snorre Fagerland, Morten Kråkvik, and Jonathan Camp
Norman Shark AS

Ned Moran
Shadowserver Foundation

# Links Between Operation Manul and Appin

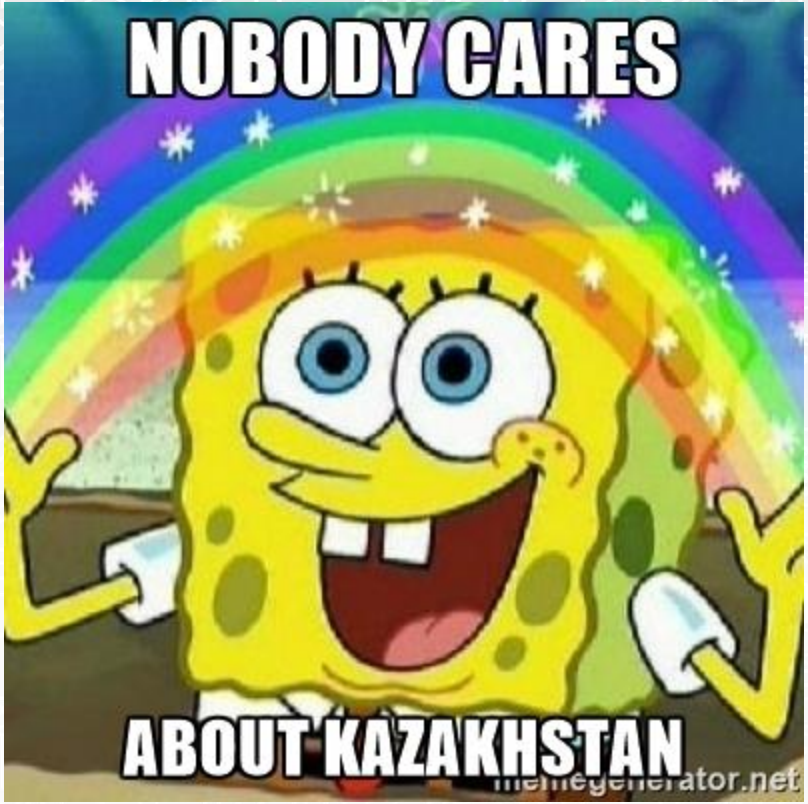
- Overlapping domains with hangover, including appinsecurity.com
- Alleged use of Hackback trojan / similar to trojan used in Oslo
  - Unable to verify this


MANUL SERVERS
IPS
DOMAINS ASSOCIATED WITH HANGOVER
axroot.com
dropboxonline.com
adobeinstall.com
adobeair.net
mangoco.net
orange2015.net
kaliex.net
68.178.232.99
64.202.189.170
208.73.210.29
208.73.211.167
50.63.202.94
174.120.120.151
209.99.40.220
209.99.40.224
209.99.40.225
secure-s.com
cellgame.org
avatarfanclub.com
researchwork.org
devilreturns.com
piegauz.net
systemupd.com
newamazingfacts.com
thedailynewsheadline.com
bikefanclub.info
devinmartin.net
foxypredators.com
net4speed.net
appinsecurity.com
ns1.zonalship.org
shopingcenter.net
ns2.competitveedge.org
accounts.you-tube.com.analogwiz.org
digitalapp.org
mailtechsolutions.org
openhostingtalk.com
mobilessoft.net
ns1.doc-files.info
inforguide.org
researchwork.org
vkspoke.org
herbco.document.digitalapp.org
wolfensteinx.net
denismobile.info
crestboard.org
buildyourinfo.org
dosendit.com
kyzosune.net
mysharpens.com
filesconnect.info
analogwiz.org
tulip.net.inforguide.org
smurfprotection.org
mgclog.com
secuina.net
gxongame.info
tmkstore.org
approvalclub.org
esnucleus.org
sockzon.org
geonet.org.sockzon.org
ns2.vlogserv.org
mcosine.org
easternsoft.org
ns2.continuelogs.info
server721-hans.de-nserver.de.continuelogs.info
worldcitycenter.net
mlogin.ymail.com.continuelogs.info
hangovergroup.com.coolservice.continuelogs.info
accounts.yandex.ru.continuelogs.info
account.istpumpenunddosiertechnik.de.continuelogs.info
accounts.facbook.com.continuelogs.info
hotupdates.com.sockzon.org
plus.go0gle.com.serviceI0gin.gxongame.info
ns1.continuelogs.info
ns1.secuina.net
itechtoys.org
ns2.gxongame.info
continuelogs.info
kyzosune.net
alintiqad-newsonline.blogspot.com.continuelogs.info
go0gle.com-serviicelogiin.autthserv.gxongame.info
autowid.com
saboresnativos.net
ns1.sockzon.org
login.live.com.continuelogs.info
server721.han.de.nsserver.de.continuelogs.info
spiritlog.org
m.ymail.com.continuelogs.info
accounts.yutube.com.continuelogs.info
ns1.gxongame.info
mobiltechsoft.org
filesconnect.info
news-report.sockzon.org
testerspoint.info
ns1.chronicleserv.org
ns2.maxtourguide.info
maxtourguide.info
espressoday.org
macsol.org
webmailaccountservicemail.info
ns2.esbasis.info
ns2.chronicleserv.org
megafairclub.org
viewerstalk.org
ns1.esbasis.info
starcrunch.org
mpale.org
imagebar.org
bbc-news.com.influxlog.org
livesunshine.info
onestop-shops.com
ns1.maxtourguide.info
mobileappworld.info
influxlog.org
mail.download.influxlog.org
wedzon.org
traderspace.org
fiservtech.org
chkpoint.info
starmobnetservice.net


MANUL SERVERS
IPS
DOMAINS ASSOCIATED WITH HANGOVER
axroot.com
dropboxonline.com
adobeinstall.com
adobeair.net
mangoco.net
orange2015.net
kaliex.net
68.178.232.99
64.202.189.170
208.73.210.29
208.73.211.167
50.63.202.94
174.120.120.151
209.99.40.220
209.99.40.224
209.99.40.225
secure-s.com
cellgame.org
avatarfanclub.com
researchwork.org
devilreturns.com
piegauz.net
systemupd.com
newamazingfacts.com
thedailynewsheadline.com
bikefanclub.info
devinmartin.net
foxypredators.com
net4speed.net
appinsecurity.com
ns1.zonalship.org
shopingcenter.net
ns2.competitveedge.org
accounts.you-tube.com.analogwiz.org
digitalapp.org
mailtechsolutions.org
openhostingtalk.com
mobilessoft.net
ns1.doc-files.info
inforguide.org
researchwork.org
vkspoke.org
herbco.document.digitalapp.org
wolfensteinx.net
denismobile.info
crestboard.org
buildyourinfo.org
dosendit.com
kyzosune.net
mysharpens.com
filesconnect.info
analogwiz.org
tulip.net.inforguide.org
smurfprotection.org
mgclog.com
secuina.net
gxongame.info
tmkstore.org
approvalclub.org
esnucleus.org
sockzon.org
geonet.org.sockzon.org
ns2.vlogserv.org
mcosine.org
easternsoft.org
ns2.continuelogs.info
server721-hans.de-nserver.de.continuelogs.info
worldcitycenter.net
mlogin.ymail.com.continuelogs.info
hangovergroup.com.coolservice.continuelogs.info
accounts.yandex.ru.continuelogs.info
account.istpumpenunddosiertechnik.de.continuelogs.info
accounts.facbook.com.continuelogs.info
hotupdates.com.sockzon.org
plus.go0gle.com.servicel0gin.gxongame.info
ns1.continuelogs.info
ns1.secuina.net
itechtoys.org
ns2.gxongame.info
continuelogs.info
kyzosune.net
alintiqad-newsonline.blogspot.com.continuelogs.info
go0gle.com-servicelogiin.autthserv.gxongame.info
autowid.com
saboresnativos.net
ns1.sockzon.org
login.live.com.continuelogs.info
server721.han.de.nsserver.de.continuelogs.info
spiritlog.org
m.ymail.com.continuelogs.info
accounts.yutube.com.continuelogs.info
ns1.gxongame.info
mobiltechsoft.org
filesconnect.info
news-report.sockzon.org
testerspoint.info
ns1.chronicleserv.org
ns2.maxtourguide.info
maxtourguide.info
espressoday.org
macsol.org
webmailaccountservicemail.info
ns2.esbasis.info
ns2.chronicleserv.org
megafairclub.org
viewerstalk.org
ns1.esbasis.info
starcrunch.org
mpale.org
imagebar.org
bbc-news.com.influxlog.org
livesunshine.info
onestop-shops.com
ns1.maxtourguide.info
mobileappworld.info
influxlog.org
mail.download.influxlog.org
wedzon.org
traderspace.org
fiservtech.org
chkpoint.info
starmobnetservice.net

# Other Considerations


WHAT DOES IT ALL MEAN?
@theblogges
memegenerator.net


NOBODY CARES
ABOUT KAZAKHSTAN


MORE RESEARCH
IS NEEDED
memegenerator.net

# It doesn't need to be sophisticated to work.

# We could(n’t) be heroes

# What do we do?

- Outreach community relations/trust building
- Incident response malware analysis /forensics/threat intel
- Education training/IT support/help desk
- Policy research legal/law enforcement
- Advocacy awareness/policy change
- Follow up with other affected parties

# What do we do?

- Outreach community relations/trust building
- Incident response **malware analysis** /forensics/threat intel
- Education training/IT support/help desk
- Policy research legal/law enforcement
- Advocacy awareness/policy change
- Follow up with other affected parties

# What is to be done?

# What industry can do

- Anti-virus state sponsored warnings
- Better state-sponsored warnings

# What you can do

# Pick a cause you care about


# and get involved.

# What Else Can You Do?

- If you have research related to the actors behind Operation Manul publish it, or send it to us!
- Donate to EFF!

# Takeaways

- None of this research is “sexy”. The tools and the actors aren’t sophisticated.
- Attacks don’t need to be sophisticated to work.
- But it’s not every day that malware research can prevent people from getting kidnapped or killed, and expose state crimes.

# Acknowledgements


- Huge thanks to our fellow researchers: Morgan Marquis-Boire and Claudio Guarnieri.
- Operation Hangover: Snorre Fagerland, Morten Kråkvik, Jonathan Camp, Ned Moran.
- Hex-Rays, Joe Sandbox, Virus Total, Passive Total for donation of their services and software.
- Additionally we'd like to thank David Greene, Jamie Lee Williams, Meghan Fenzel, Nate Cardozo, Kurt Opsahl, Soraya Okuda, and Marion Marschalek, for their patience, help, support, and advice.

# Further Reading

Operation Hangover: http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_India...

Oslo Freedom Forum: https://www.f-secure.com/weblog/archives/00002554.html

Iran 2FA Spearphishing: https://citizenlab.org/2015/08/iran_two_factor_phishing/

Pawn Storm EFF Report: https://www.eff.org/deeplinks/2015/08/new-spear-phishing....

Wassenaar: https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-impl....

Kidane V. Ethiopia: https://www.eff.org/cases/kidane-v-ethiopia

Ethiopia and FinFisher: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global...

Human Rights Watch Report on Kazakhstan: https://www.hrw.org/world-report/2015/country-chapters/kazakhstan