



OPERATION **MANUL**

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?



EFF

@EFF FOLLOW YOU

We're the Electronic Frontier Foundation.
We defend your civil liberties in a digital
world.

📍 San Francisco, CA

🔗 eff.org

📅 Joined August 2006



Legal Work





Coders' Rights Project



Q: Why are you stirring up so much trouble?





Activism





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?

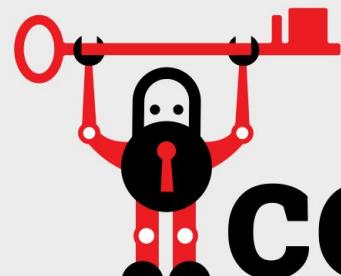
The Wassenaar Arrangement is a multi-national agreement intended to control the export of certain



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016

Technology



certbot

Automatically enable HTTPS on your website.



HTTPS Everywhere



Q: Who pays you?

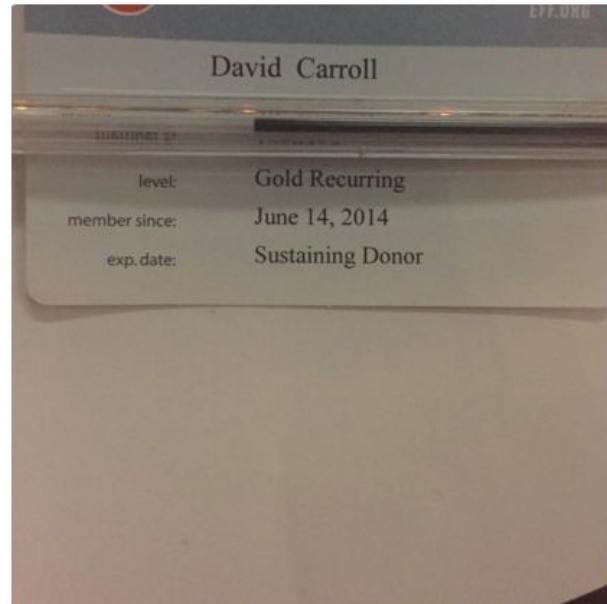


david carroll
@davidecarroll

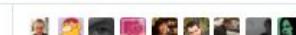


Following

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



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016



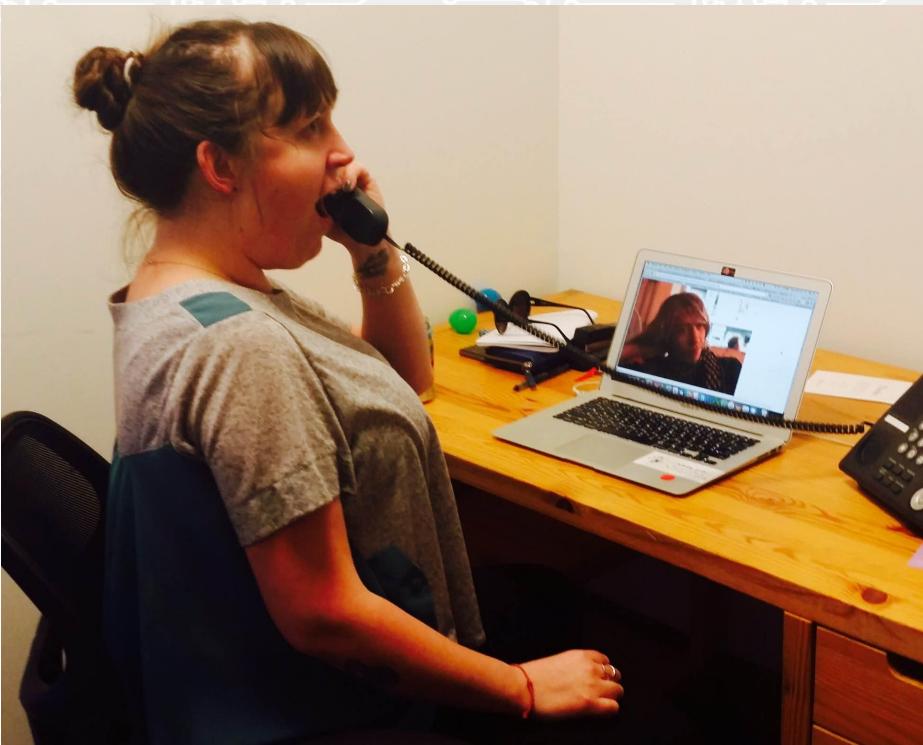


Ethiopia





Iran





Pawn Storm / FancyBear / APT28





Nobody Cares About Kazakhstan

Operation Manul



Kazakhstan is here!





ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016





ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016





2015 SCORES

PRESS STATUS

Not FreePRESS 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**информационно-аналитический портал
РЕСПУБЛИКАKZ23 июня 2016 года
1:44 МСК[RSS](#) · [PDA](#) · [TXT](#) · [Eng](#) · [Каз](#)найти на сайте [twitter](#) [facebook](#) [YouTube](#) [18+](#)

ДОСЛОВНО

• Продавать билеты иностранцам на EXPO-2017 будут россияне...

• В РК более 14 тысяч выпускников не одолели на ЕНТ уровень 50 баллов...

• Иран подаст иск к США из-за отказа вернуть \$2 млрд...

• Доказанные запасы нефти в РК оцениваются в 30 млрд баррелей...

• День России подарят жителям своей страны три выходных...

• Курдские боевики объявили Турцию опасной страной для туристов...

• Делегация США не поедет на экономический форум в Пилтер...

НЕТ! ПОЛИТИЧЕСКИМ РЕПРЕССИЯМ В КАЗАХСТАНЕ

NOTA BENE

Редакция
"Республики"

Вниманию читателей

14.06.2016

В связи с непрекращающимися атаками хакеров и возникшими в связи с этим техническими проблемами редакция решила приостановить работу портала и уйти в отпуск...



Политика 13.06.2016

Еще раз про лоббистов Назарбаева во Франции

Кто они, лоббисты назарбаевского режима во Франции, и какие причины заставили их помогать преследовать Мухтара Аблязова? Ответ на эти вопросы мы нашли в переписке дипломата Жана Галиева. Из нее же узнали, как именно Акорда обрабатывает французскую прессу и общество...

ИНТЕРВЬЮ

Евгения
МАЖИКОВА

Синдром кровавого воскресенья

08.06.2016

ПОЛИТИКА - После жаноозенских событий у людей осталось ощущение несправедливости. А это именно то, с чего начинаются революции, считает политолог Андрей Грозин...



Политика 14.06.2016

Котировки на нефть за пять месяцев поднялись на 60%, а тенге к доллару укрепился всего лишь на 10%....



Политика 14.06.2016

Главных латифундистов Казахстана назвал в своем интервью "Республике" Виктор Храпунов...



Политика 13.06.2016

Трагедия в Актобе стала водоразделом, но точно не была случайностью, считает Адил Тойланбаев...

В ПОИСКАХ ИСТИНЫ

Нурахмет
КЕНЖЕЕВ

Политика



Бизнес

Нефть задержится на достигнутом уровне



Политика

КНР лучше с «хардом», чем с «софтком»



Оставайтесь на волне безопасности!

KASPERSKY

НАМ ПИШУТ

Дулат
МУСАТАЕВ



SEARCH

HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM

TAKE ACTION

SHOP

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

Donate to EFF



Stay in Touch

 Email Address Postal Code (optional)

SIGN UP NOW

NSA Spying

eff.org/nsa-spying

EFF is leading the fight against the NSA's illegal mass surveillance program. [Learn more](#) about what the program is, how it works, and what you can do.

Follow EFF



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016





KZ!



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



21 SUSPECTED GOVERNMENT USERS

AMERICAS

Mexico
Colombia
Panama

EUROPE

Hungary
Italy
Poland
Turkey

MIDDLE EAST

Oman
Saudi Arabia
UAE

AFRICA

Egypt
Ethiopia
Sudan
Morocco

ASIA

Azerbaijan
Kazakhstan
Thailand
South Korea
Malaysia
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



Irina Petrusheva



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016





NO DOGS WERE HARMED IN THE MAKING OF THIS TALK.

WE LOVE DOGS.

PLEASE ENJOY THIS UNICORN PICTURE.





ELECTRONIC FRONTIER FOUNDATION eff.org

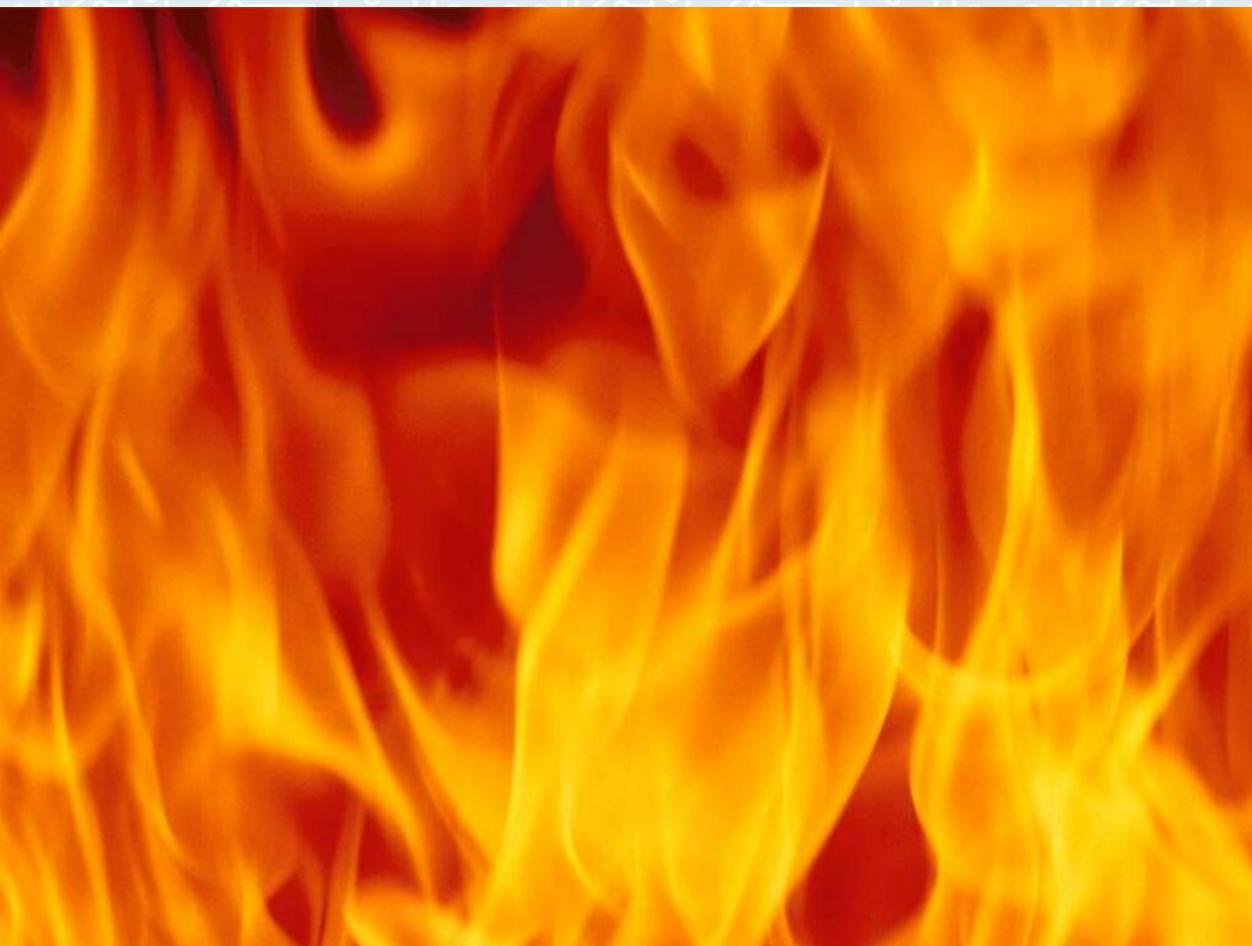
BlackHat USA 2016





ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016



[News & Analysis](#)[Data & Research](#)[Services & Resources](#)[Advocacy & Action](#)[About CPJ](#)[Countries & Regions](#)

Search



ALERTS | KAZAKHSTAN

Kazakh authorities seize embattled weekly's print run

[Text Size](#)[Print](#)

Share



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.

RELATED STORIES





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





Case 2:15-mc-00159-TLN-KJN Document 33 Filed 03/03/16 Page 1 of 10

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

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

25

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](#)



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016



Mukhtar Ablyazov



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016



OPERATION MANUL

Unveiling Operation Manul



Gmail
by Google

111 111 <nicprivat4@gmail.com>

Invoice Lexial ATABAYEV
1 письмо

eruc@lexial.eu <eruc@lexial.eu>
Komy: lotus@bp-pb.com

12 августа 2015 г., 13:06

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 Guénigaud, 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

This e-mail is sent from Lexial law firm. The content of this email and any attachments are confidential to the intended recipient. They may not be disclosed to or used by or copied in any way by anyone other than the intended recipient. If this e-mail is received in error, please contact us quoting the name of the sender and the email address to which it has been sent and then delete it.

ATABAYEV INVOICE.pdf
31K

ATABAYEV INVOICE.pdf - Adobe Reader

1 | 1 209% Suchen

LEXIAL

Warning: JavaScript-Fenster -
This file appears to use a new format that this version of Acrobat does not support. It may not open or display correctly. Adobe recommends that you upgrade to the latest version of our product. Please follow the download link and re-read.

Yes, download the photo viewer plugin OK

Start ATABAYEV INVOICE.pdf 9:18 PM



ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016

jRat / Jacksbot





JRat / Jacksbot

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



JRat / Jacksbot

jRAT

Main Tools Clients Plugins Help

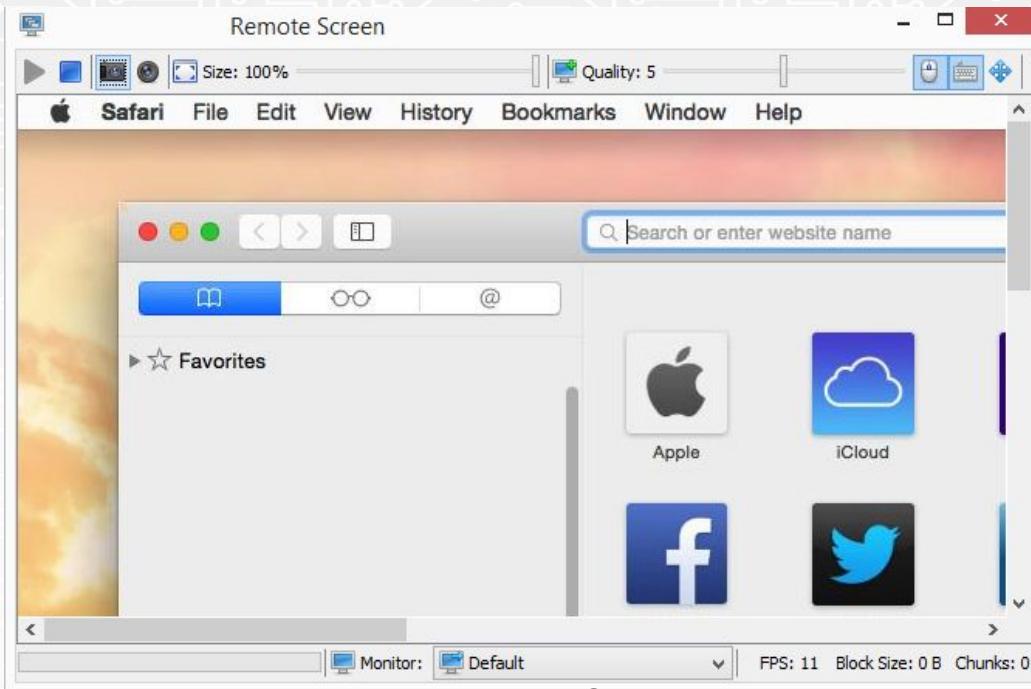
Clients Statistics Network Usage On Connect Sockets Log Plugins

Country	ID	Status	IP/Port	Ping	User@Host	Operating System	RA
JE	JRAT567	Ready	201.209....	480 ms	Sample\Sample	Windows 7	0 E
BR	JRAT970	Ready	96.196.1...	243 ms	Sample\Sample	Windows 8.1	0 E
SK	JRAT76	Ready	114.12.1...	352 ms	Sample\Sample	Windows 8	0 E
NI	JRAT817	Ready	216.50.2...	34 ms	Sample\Sample	Windows Server 2012	0 E
NC	JRAT31	Ready	60.167.5...	74 ms	Sample\Sample	Windows 10	0 E
BW	JRAT282	Ready	9.199.18....	43 ms	Sample@Sample	Mac OS X Cheetah 10.0	0 E
BJ	JRAT176	Ready	188.157....	337 ms	Sample@Sample	Mac OS X Puma 10.1	0 E
GN	JRAT0	Ready	224.14.1...	309 ms	Sample@Sample	Mac OS X Jaguar 10.2	0 E
CW	JRAT385	Ready	158.232....	223 ms	Sample@Sample	Mac OS X Panther 10.3	0 E
BW	JRAT862	Ready	224.211....	44 ms	Sample@Sample	Mac OS X Tiger 10.4	0 E
DK	JRAT906	Ready	209.188....	408 ms	Sample@Sample	Mac OS X Leopard 10.5	0 E
AC	IRAT925	Ready	16.159.6...	477 ms	Sample@Sample	Mac OS X Snow Leopard	0 E

Server UI



JRat / Jacksbot





JRat / Jacksbot

Control Panel

System Info Memory Usage Drives Monitors JVM Info Config Trace

Key	Value
Remote address	
Local address	
Stub ID	ID
RAM	8,00 GB
Available Cores	4
Install Date/Last modified	
Username	vm
Computer Name	
Operating System	Windows 8.1
Country	HK
Stub Location	C:\Users\vm\AppData\Local\Temp\update7569170
Stub Version	
Java Version	1.8.0_31-b13

Control Panel

- m stem Info
- mory Usage
- vironment Variable
- stem Properties
- ves
- nitors
- Info
- nfig
- ice
- Manager
- no
- ssagebox
- note Chat
- ech
- m Functions**
- note Shell
- note Process
- sts File
- gistry
- installed Programs



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



005.jpg



006.jpg

1020 lo
Zhongnanhai.JPG

A (1).jpg



AAAAAAA.xlsx

Acmerica Le gen.
pdf

America.pdf



AN giang 9T1.pdf

AUTHORIZATION
LETTER_Dorchester
(1).TIFBang tinh testkey
va password.xlsCOMMERCIAL
INVOICE
Cigarettes SL.docCong van Starprint.
pdfContract 2015 SL.
doc

Cookies



Cookies-journal



Current Session

Index of /ram/users/pws - l

Restore Session Index of /ram/users/pws Connecting...

axroot.com/ram/users/pws/

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools

Index of /ram/users/pws

Name	Last modified	Size	Description
Parent Directory		-	
Administrator4390.enc	2015-12-12 20:04	3.0K	
Administrator5705.enc	2015-12-12 20:04	1.9K	
Administrator6186.enc	2015-12-12 20:04	1.9K	
LEO8683.enc	2015-12-12 20:04	2.2K	
MS9071.enc	2015-12-12 20:04	2.4K	
Turing9364.enc	2015-12-12 20:04	1.9K	
VRT5656.enc	2015-12-12 20:04	1.9K	
Yap7944.enc	2015-12-12 20:04	2.3K	
nerissa8574.enc	2015-12-12 20:04	1.9K	
omar6921.enc	2015-12-12 20:04	2.0K	
workshop4720.enc	2015-12-12 20:04	2.1K	



Other Targets

Ramona PHP Rat - Iceweasel

Restore Session Ramona PHP Rat

www.axroot.com/ram/login.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng



USER
PASSWORD

Arcom Rat Web Panel - Iceweasel

Restore Session Arcom Rat Web Panel Base64 Decode and E...

www.axroot.com/ar/login.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng



USER
PASSWORD

IRIS Rat WebPanel by Princelsi - Iceweasel

Restore Session IRIS Rat WebPanel by...

www.axroot.com/red/login.php

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng



Username

Password



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

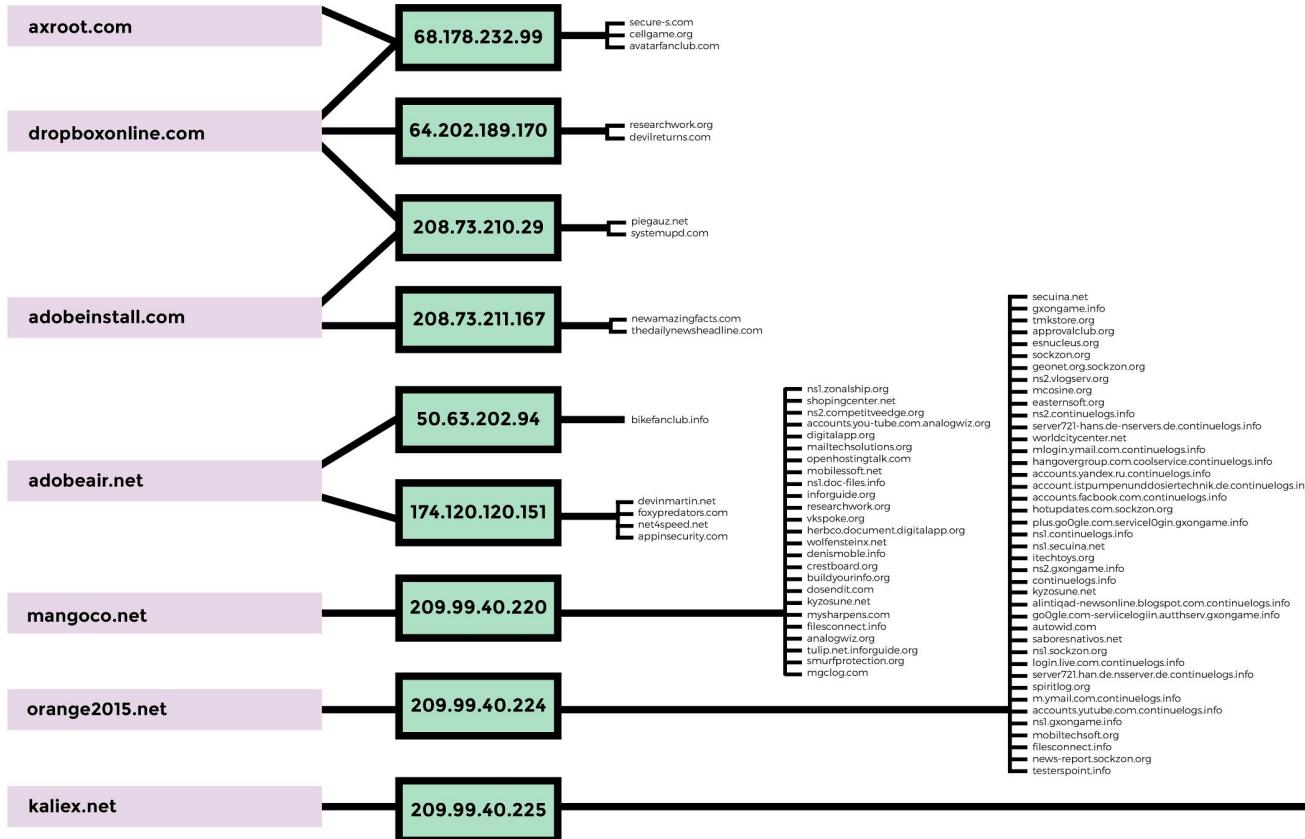
- Overlapping domains with hangover, including appinsecurity.com
- Alleged use of Hackback trojan / similar to trojan used in Oslo
 - Unable to verify this

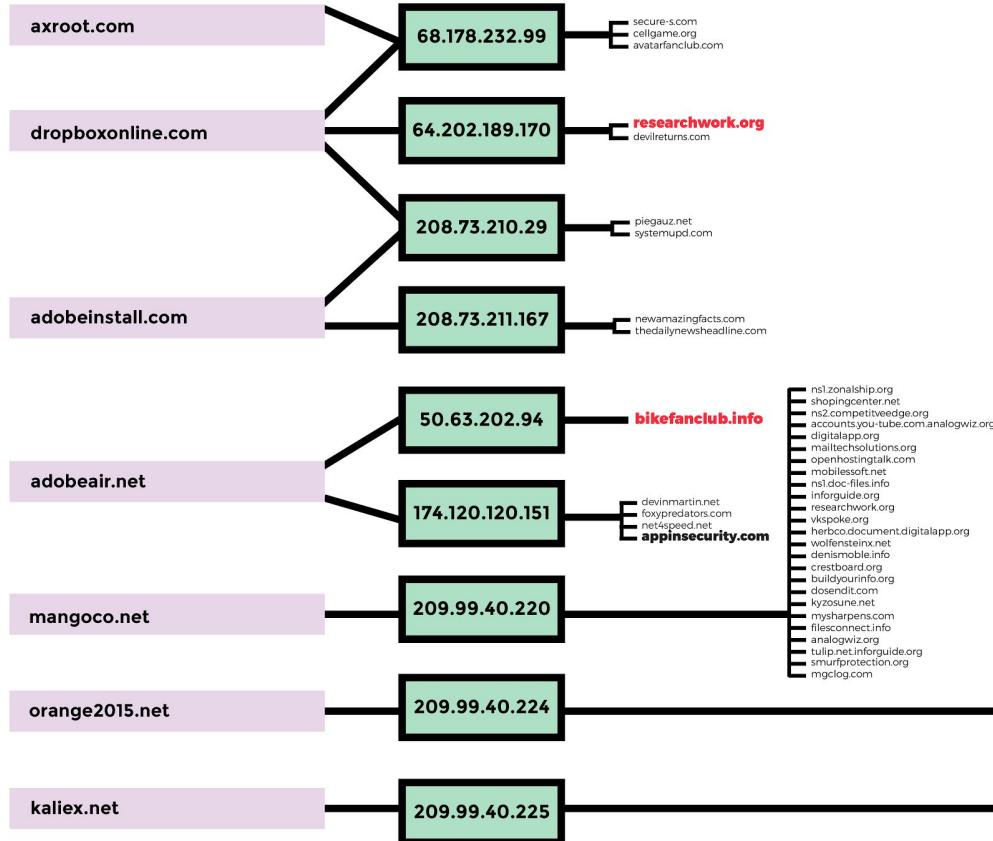


MANUL SERVERS

IPS

DOMAINS ASSOCIATED WITH HANGOVER



**MANUL SERVERS IPS DOMAINS ASSOCIATED WITH HANGOVER**

secuina.net
gxongame.info
tmkstore.org
approvalclub.org
esnucleus.org
sockzon.org
geekzone.sockzon.org
ns2.vigilant.org
mcslive.org
easternsoft.org
ns2.continuelogs.info
server721.hans.de-hservers.de.continuelogs.info
worlddcitycenter.net
mlloginymall.com.continuelogs.info
hangoverhangover.com.cooservices.continuelogs.info
account.istpumpenunddosientechnik.de.continuelogs.info
accounts.facebook.com.continuelogs.info
hotupdates.com.sockzon.org
plus.google.com.service0igin.gxongame.info
ns1.secunia.net
ns2.secunia.net
ns2.gxongame.info
continuelogs.info
alintiqad-newsonline.blogspot.com.continuelogs.info
goQoogelsercivelogin.autthserv.gxongame.info
goQoogelsercivelogin.autthserv.gxongame.info
saboresnotables.net
ns1.sockzon.org
login.live.com.continuelogs.info
server721.hans.de-hservers.de.continuelogs.info
spiritlog.org
mymail.com.continuelogs.info
ns1.secunia.info
ns1.gxongame.info
mobiletechsoft.org
filesconnect.info
news-report.sockzon.org
testerspoint.info

ns1.chronicleserv.org
ns2.maxtourguide.info
maxtourguide.info
expressday.org
ns1.secunia.org
webmailcountercustemail.info
ns1.esbasis.info
ns2.esbasis.info
ns2.chronicleserv.org
megafairclub.org
viewerstalk.org
ns1.esbasis.info
starchurch.org
mpsalis.org
imagegear.org
bbc-news.com.influxlog.org
livesunshine.info
onestop-shops.com
ns1.maxtourguide.info
mobileappworld.info
ns1.secunia.org
mail.download.influxlog.org
wedzion.org
traderspace.org
fisertech.org
chkpoint.info
starmobnetservice.net



Other Considerations



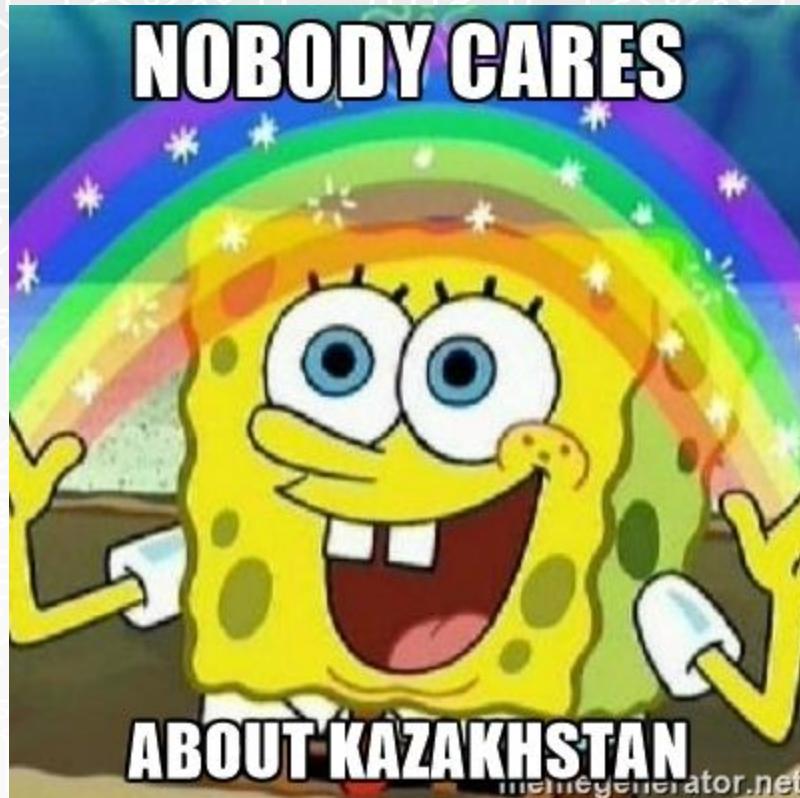


**WHAT DOES IT ALL
MEAN?**



@thebloggess

memegenerator.net





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





ELECTRONIC FRONTIER FOUNDATION eff.org

BlackHat USA 2016





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>