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 Follows 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
Q: Why are you stirring up so much trouble?
Activism

TELL CONGRESS:
CFAA Is Broken — Don’t Make It Worse
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 goods, thus ensuring national security and non-proliferation.
Technology

Certbot
Automatically enable HTTPS on your website.

HTTPS Everywhere
Q: Who pays you?
Targeted Attacks
Ethiopia

FREE ZONE 9 BLOGGERS
Iran
Nobody Cares About Kazakhstan

Operation Manul
Kazakhstan is here!
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

Владимир Путилин
Кампания президента
в США

Политика
23 июня 2016 года
11:44 MSK

Элдорадо
Политический
репрессий
в Казахстане

Редакция "Республики"
Вниманию читателей
14.06.2016

В связи с напряженной ситуацией в стране, в связи с этим техническим пороком в редакции решили приостановить работу портала и уйти в отпуск...

Интервью
Евгения МАЖИТОВА
Синдикат креативных овощей
08.06.2016

Политика. После киевских событий у людей осталось ощущение дискомфорта. А также о том, что никаких решений, считает политолог Андрей Громов...

В поисках истины
Нуркай ХЕНЖЕЕВ
14.06.2016

Политика. Что еще работает на Ахмеду в Британии...

Голод не тетка
13.06.2016

Политика. Нефть.
Кто еще работает на Ахмеду в Британии

Как Ахмед угрозы террористам
13.06.2016

Политика. Главным атакующим Казахстана является в самой стране "Республика". Виктор Арапанов...

От шаблонов несет тяжелой резкостью
14.06.2016

Политика. Транспорт в Австро стал нормальным, но так и не был подключен, теперь Алим Таныбаев...

Нота Бенье
Еще раз про лоббистов Назарбаева во Франции

23 июня 2016 года
11:44 MSK

Кто они, лоббисты намазковского режима во Франции, и какие причины заставили их попытаться притеснить Мухтара Алмазова? Ответ на эти вопросы мы нашли в пресс-службе дипломата Жана-Гийома Грегуар и из него не увидно, какая экономика Аккорд обольщает французскую прессу и общество...

Дословно

Продавать билеты иностранцам на Евро-2017 будет россиянка...

В РК более 14 тысяч выпускников не оценили на ЕНТ уровнем 60 баллов...

Иран переехал в США визы отрицательно вернул 32 штат...

Денежные депозиты на сегодня в РК снижаются до 0,25 процента биржевая...

День России подарил жителям своей ОТВЯЗЬ Но вышли....

Коксовые бластеры объявляют Турчинский опасной для туризма...

Депутаты США не пойдут на экономический форум в Петер...

Касперский

Оставайтесь на волне безопасности!

Нам писать
Дулат МУСАТАЕВ
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 possession of a valid certificate issued by a trusted certificate authority. The Kazakhstan plan could change this, allowing the regime to intercept communications without the knowledge of either party involved.
BlackHat USA 2016

HACKING TEAM RCS
Suspected Government Users Worldwide

Citizen Lab 2014
Bill Marczak, Claudio Guasmi, Morgan Marquis-Boire & John Scott-Railton

KZ!

21 SUSPECTED GOVERNMENT USERS

AMERICAS
Mexico
Colombia
Panama

EUROPE
Hungary
Turkey
Italy
Poland

MIDDLE EAST
Oman
Saudi Arabia
UAE

AFRICA
Egypt
Ethiopia
Nigeria
Sudan
Morocco

ASIA
Azerbaijan
Kazakhstan
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

©

BlackHat USA 2016
NO DOGS WERE HARMED IN THE MAKING OF THIS TALK.

WE LOVE DOGS.

PLEASE ENJOY THIS UNICORN PICTURE.
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.
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-KJM

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, Republika and LLC Media-Consult, have opposed the motion, and Kazakhstan filed a reply brief. (ECF Nos. 22, 24, 28.)

After carefully considering the parties’ written briefing, the court's record, and the applicable law, the court DENIES the motion without prejudice.¹

¹ Based on the parties’ stipulation and for good cause shown, the court approved a special
О нас снова пишут...


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., Ганущиной С.А., Ковалевым С.А., Пономаревым Л.А., Световой З.Ф.

Leave a comment
Unveiling Operation Manul
Dear Boo,

As agreed, please find attached our invoice.

Thank you in advance for the payment.

Best regards,

E. Rustic

Lexial

This email is sent from Lexial Liance. The content of this email and any attachments are confidential to the intended recipient. They may not be disclosed to or used by or in any way by anyone other than the intended recipient. If this email is mistaken in any way, 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
JRat / Jacksbot
JRat / Jacksbot

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

A screenshot of the JRat / Jacksbot server UI is shown. The UI displays a list of clients with their details such as ID, status, IP/Port, ping, user@host, and operating system. The table includes columns for country, status, IP/Port, ping, user@host, and operating system. Some of the clients listed include:

- **RAT567**: Ready, IP/Port 201.209..., Ping 480 ms, Sample\Sample, Windows 7
- **RAT970**: Ready, IP/Port 96.196.1..., Ping 243 ms, Sample\Sample, Windows 8.1
- **RAT76**: Ready, IP/Port 114.12.1..., Ping 352 ms, Sample\Sample, Windows 8
- **RAT871**: Ready, IP/Port 216.50.2..., Ping 34 ms, Sample\Sample, Windows Server 2012
- **RAT31**: Ready, IP/Port 60.167.5..., Ping 174 ms, Sample\Sample, Windows 10
- **RAT282**: Ready, IP/Port 9.199.18..., Ping 43 ms, Sample@Sample, Mac OS X Cheetah 10.0
- **RAT176**: Ready, IP/Port 188.157..., Ping 337 ms, Sample@Sample, Mac OS X Puma 10.1
- **RAT90**: Ready, IP/Port 224.14.1..., Ping 309 ms, Sample@Sample, Mac OS X Jaguar 10.2
- **RAT385**: Ready, IP/Port 158.232..., Ping 223 ms, Sample@Sample, Mac OS X Panther 10.3
- **RAT662**: Ready, IP/Port 224.21..., Ping 44 ms, Sample@Sample, Mac OS X Tiger 10.4
- **RAT906**: Ready, IP/Port 209.188..., Ping 408 ms, Sample@Sample, Mac OS X Leopard 10.5
JRat / Jacksbot

View Remote Screen
# JRat / Jacksbot

## Control Panel

### System Info

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote address</td>
<td></td>
</tr>
<tr>
<td>Local address</td>
<td></td>
</tr>
<tr>
<td>Stub ID</td>
<td>ID</td>
</tr>
<tr>
<td>RAM</td>
<td>8.00 GB</td>
</tr>
<tr>
<td>Available Cores</td>
<td>4</td>
</tr>
<tr>
<td>Install Date/Last modified</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>vm</td>
</tr>
<tr>
<td>Computer Name</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows 8.1</td>
</tr>
<tr>
<td>Country</td>
<td>HK</td>
</tr>
<tr>
<td>Stub Location</td>
<td>C:/Users/vm/AppData/Local/Temp/update756917/</td>
</tr>
<tr>
<td>Java Version</td>
<td>1.8.0_31-b13</td>
</tr>
</tbody>
</table>

## JRat / Jacksbot

The image shows a screenshot of the JRat/Jacksbot control panel. The table provides various system information details such as remote and local addresses, stub ID, RAM, available cores, install date, username, computer name, operating system, country, Java version, and a path to a temporary file. The visual layout includes a control panel interface with tabs for system info, memory usage, drives, monitors, JVM info, config, and trace.
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

Index of /ram/users/pws

<table>
<thead>
<tr>
<th>Name</th>
<th>Last modified</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.Parent Directory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator4385.enc</td>
<td>2015-12-12 20:04</td>
<td>3.0K</td>
<td></td>
</tr>
<tr>
<td>Administrator5705.enc</td>
<td>2015-12-12 20:04</td>
<td>1.0K</td>
<td></td>
</tr>
<tr>
<td>Administrator8185.enc</td>
<td>2015-12-12 20:04</td>
<td>1.0K</td>
<td></td>
</tr>
<tr>
<td>EOF883.enc</td>
<td>2015-12-12 20:04</td>
<td>2.2K</td>
<td></td>
</tr>
<tr>
<td>MS8071.enc</td>
<td>2015-12-12 20:04</td>
<td>2.4K</td>
<td></td>
</tr>
<tr>
<td>Turing2284.enc</td>
<td>2015-12-12 20:04</td>
<td>1.8K</td>
<td></td>
</tr>
<tr>
<td>VRT5656.enc</td>
<td>2015-12-12 20:04</td>
<td>1.6K</td>
<td></td>
</tr>
<tr>
<td>Yap9944.enc</td>
<td>2015-12-12 20:04</td>
<td>2.3K</td>
<td></td>
</tr>
<tr>
<td>perissa8574.enc</td>
<td>2015-12-12 20:04</td>
<td>1.9K</td>
<td></td>
</tr>
<tr>
<td>smart8921.enc</td>
<td>2015-12-12 20:04</td>
<td>2.0K</td>
<td></td>
</tr>
<tr>
<td>workshop4720.enc</td>
<td>2015-12-12 20:04</td>
<td>2.1K</td>
<td></td>
</tr>
</tbody>
</table>

Apache/2.4.17 (Win32) OpenSSL/1.0.2d PHP/5.6.15 Server at axr...
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
Other Considerations

I'M NOT SAYING IT WAS ALIENS

BUT IT WAS ALIENS
MORE RESEARCH IS NEEDED
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.
• 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...
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...