



# I Got a Letter From the Government the Other Day...

Unveiling a Campaign of Intimidation, Kidnapping, and  
Malware in Kazakhstan

Eva Galperin, International Policy Analyst, EFF

Cooper Quintin, Staff Technologist, EFF

Morgan Marquis-Boire, Director of Security, First Look Media

Claudio Guarnieri, Technologist, Amnesty International

August 2016 - Black Hat USA

# Table of Contents

[Table of Contents](#)

[Abstract](#)

[Operation Manul](#)

[Victims of Operation Manul](#)

[JRat Malware Family](#)

[JRat Functionality](#)

[Anti-Analysis](#)

[Bandook Malware Family](#)

[Core Functionality](#)

[Network Indicators and Modularity](#)

[Attribution](#)

[Observed Links to the Government of Kazakhstan](#)

[Observed Links to Arcanum Global Intelligence](#)

[Observed Links To Appin](#)

[Other Possible Targets](#)

[Conclusion](#)

[Acknowledgements](#)

[Appendix A: Indicators of Compromise](#)

[C2 Servers](#)

[Hashes](#)

[Appendix B: Further Reading](#)

# Abstract

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

*Opened it and read it*

*It said they were suckers*

Public Enemy, Black Steel and the Hour of Chaos

**UPDATE 01/18/2018:** We now have reason to believe that our original attribution for this campaign to Appin was incorrect. For a more up to date attribution, please read the [Dark Caracal report](#).

This report covers a campaign of phishing and malware which we have named “Operation Manul”<sup>1</sup> and which, based on the available evidence, we believe is likely to have been carried out on behalf of the government of Kazakhstan against journalists, dissidents living in Europe, their family members, known associates, and their lawyers. Many of the targets are involved in litigation with the government of Kazakhstan in European and American courts whose substance ranges from attempts by the government of Kazakhstan to unmask the administrators behind an anonymous website that publishes leaks alleging government corruption (Kazaword)<sup>2</sup> to allegations of kidnapping.

Our research suggests links between this campaign and other campaigns that have been attributed to an Indian security company called Appin Security Group. A hired actor is consistent with our findings on the Command and Control servers related to this campaign, which included web-based control panels for multiple RATs, suggesting that several campaigns were being run at once. A hired actor may also explain the generic and uninspired nature of the phishing, which often took the form of an email purporting to contain an invoice or a legal document with an attachment containing a blurry image. An investigation by the Swiss federal police of some of the emails linked to Operation Manul concludes that they were sent from IP addresses in India, which also suggests a link to Appin.

Hundreds of leaked emails published on the Kazaword website also suggest possible links between this campaign and Arcanum Global Intelligence, a private intelligence company with headquarters in Zurich, which was allegedly hired by the government of Kazakhstan

---

<sup>1</sup> We chose the name Operation Manul because Manul cat is native to the steppes of Kazakhstan, and that this campaign seems to be targeting members of the Kazakhstan diaspora and their associates. We also like cats.

<sup>2</sup> <https://kazaword.wordpress.com/>

to perform a surveillance and data extraction operation against a high-profile dissident. It was *Respublika's* reporting on these connections which led the government of Kazakhstan to request an injunction in a New York court to bar the website from publishing the “stolen” emails.

# Operation Manul

In 2015, EFF's clients in the *Respublika* litigation<sup>3</sup> were the targets of several spearphishing attempts they had received via email (Fig. 1). We analyzed these emails and discovered that they contained malware, which appeared to be coming from a single actor as part of an ongoing targeted hacking campaign which we have named "Operation Manul." Over the last year Operation Manul has repeatedly targeted our clients in the *Respublika* case (Irina Petrushova and Alexander Petrushov), their known associates and family members, and other dissidents involved in litigation with the government of Kazakhstan in European courts, as well as their family members, associates, and attorneys.

We were also able to observe links between Operation Manul and a malware campaign targeting the family of Mukhtar Ablyazov, co-founder of the Democratic Choice of Kazakhstan, a party opposed to the authoritarian rule of Kazakhstan's President Nursultan Nazarbayev. Ablyazov is currently fighting extradition from France, where he lives in exile, to Nazarbayev-allied Russia. In May 2013, Ablyazov's wife, Alma Shalabaeva, and 6-year-old daughter, Alua Ablyazova, were taken into custody by Italian police and forcibly deported despite having legal British and European residence permits. Within 72 hours, they were on a private jet hired by the Kazakh embassy, and taken to Almaty, Kazakhstan's capital. Ablyazov and his supporters have characterized this move as a "kidnapping" and "political hostage-taking" ordered by President Nazarbayev. Spearphishing emails and malware sent to the family and their associates during this period may have been intended to help track Alma and Alua's movements in preparation for this incident.

---

<sup>3</sup> <https://www.eff.org/cases/kazakhstan-v-does>



111 111 <nicprivat4@gmail.com>

---

**Invoice Lexial ATABAYEV**

1 ПИСЬМО

---

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

12 астрыта 2015 р., 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 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

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

*Fig. 1 A spearphishing email sent to Alexander Petrushov. The title of the document “Atabayev Invoice” may refer to Bolat Atabayev, a Khazakh dissident and theater director who was also targeted in this campaign.*

In an appeal filed with a Swiss court earlier this year, members of Ablyazov’s family allege that they have been targeted by a campaign of spearphishing emails containing malware going back to 2012. The campaign against Ablyazov’s family, attorneys, and associates used the same malware as we found in Operation Manul, and sometimes used

the exact same emails as the emails sent to EFF's *Respublika* clients and their associates, on the same dates. Additionally, analysis by GovCERT of other spearphishing emails sent to Ablyazov's family and associates in 2015 concludes that the malware uses the kaliex.net domain and covertly installs Bandook. For this reason we believe both groups are targets of Operation Manul.

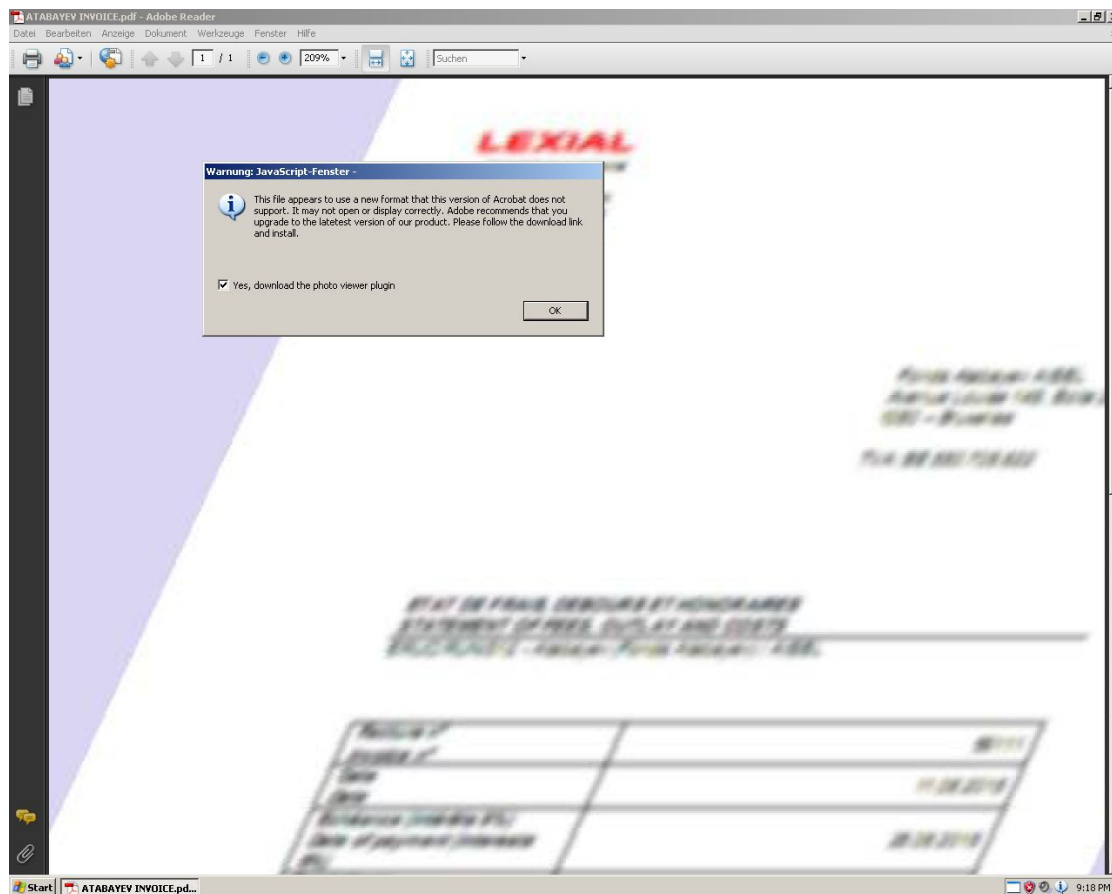


Fig 2. The PDF document from the spearphishing email entices the victim to download a fake update to acrobat.

Operation Manul appears to primarily use two different commercially available malware families: JRat and Bandook.

## Victims of Operation Manul

Some victims of Operation Manul have expressed a desire to preserve their anonymity, which we respect. The victims we are at liberty to identify include Alexander Petrushov and Irina Petroshova, publishers of the independent Kazakh newspaper, *Respublika*, Peter Sahlas, a human rights attorney, several members of Mukhtar Ablyazov's family, Astolfo

Di Amato, an Italian attorney who spearheaded anti-corruption litigation involving allegations of corruption by Kazakhstan, and dissident theater director Bolat Atabayev. Several victims allege that they have been physically followed, had their homes broken into, and been tracked using GPS devices. Mr. Di Amato alleges that his law firm's website has been the victim of several DDoS attacks, which he believes are linked to his litigation involving the government of Kazakhstan.

## JRat Malware Family

One of the common malware samples used over the course of Operation Manul is known as JRat or Jacksbot. JRat is a commercially available remote access tool (RAT), written in Java. JRat is currently available for purchase at [jrat\[.\]io](http://jrat[.]io) for the price of \$40 USD.<sup>4</sup> JRat has been continuously developed for the last four years, seemingly by a single developer who goes by the name “redpoison”. While JRat itself is closed source, many modules and helpful utilities are open source and are available on github.<sup>5</sup>

### JRat Functionality

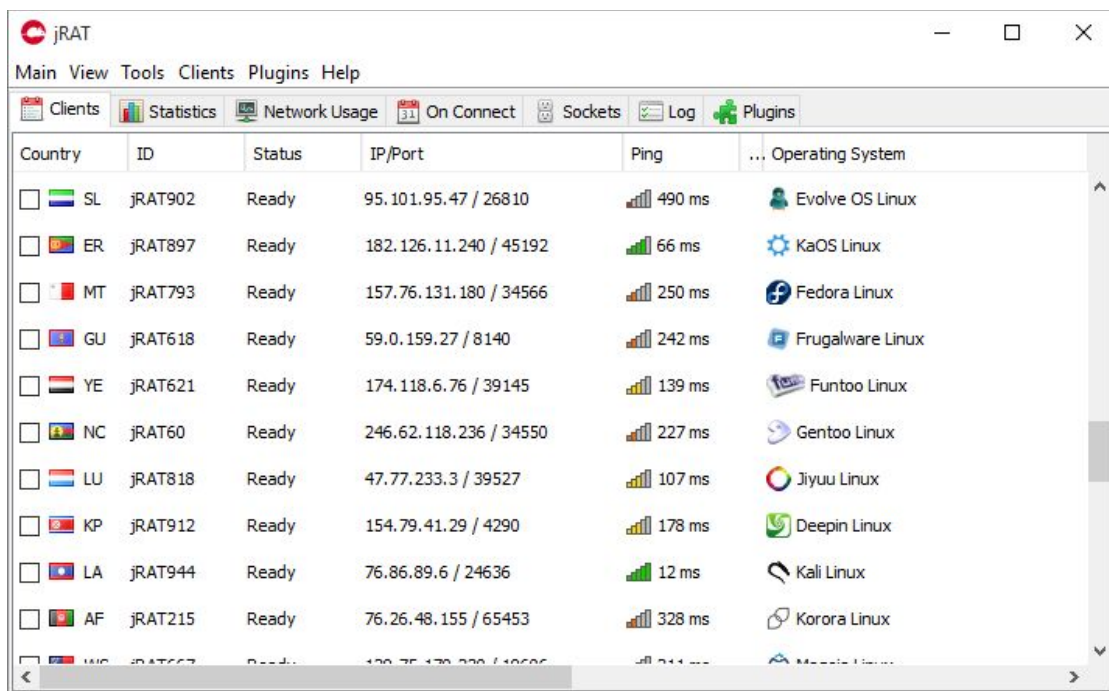


Fig 3. JRat Controller on Windows

<sup>4</sup> Payable only in bitcoin.

<sup>5</sup> <https://github.com/java-rat>



JRat is a cross platform RAT, able to target hosts running Windows, OSX, Linux, BSD, and even Solaris. The RAT is highly modular—it even has an open API so that the attacker may write custom modules to fit their needs. JRat modules include the following functionality: keylogging, reverse proxy, password recovery, turning on the host webcam, disabling webcam indicator light, listing host processes, opening a shell on the host, editing the host registry, and even chatting with the remote host. JRat also provides a controller application, which is written in Java. This controller application allows the attacker to manage all of their JRat instances and view uptime, operating system, and other information about all infected hosts. JRat also provides a web version of the controller, which is open source.<sup>6</sup>

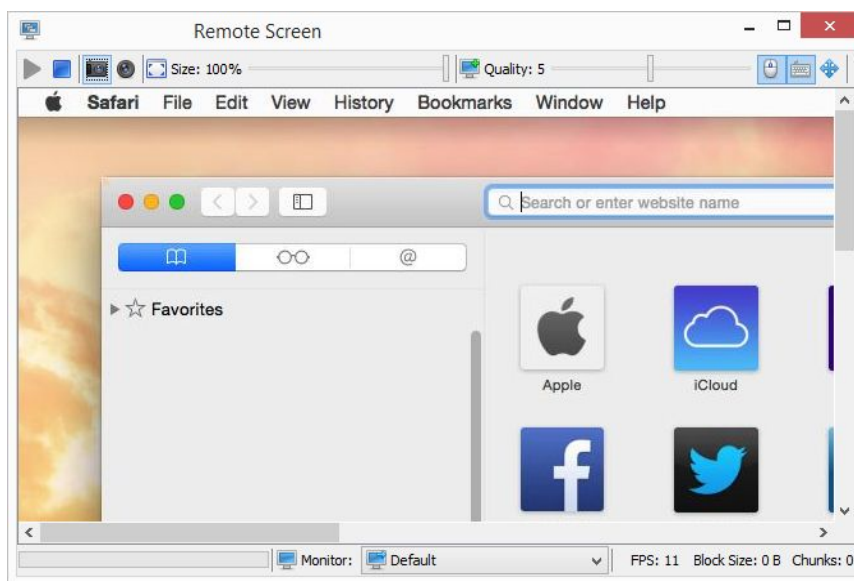


Fig 4. JRat Controller viewing host screen

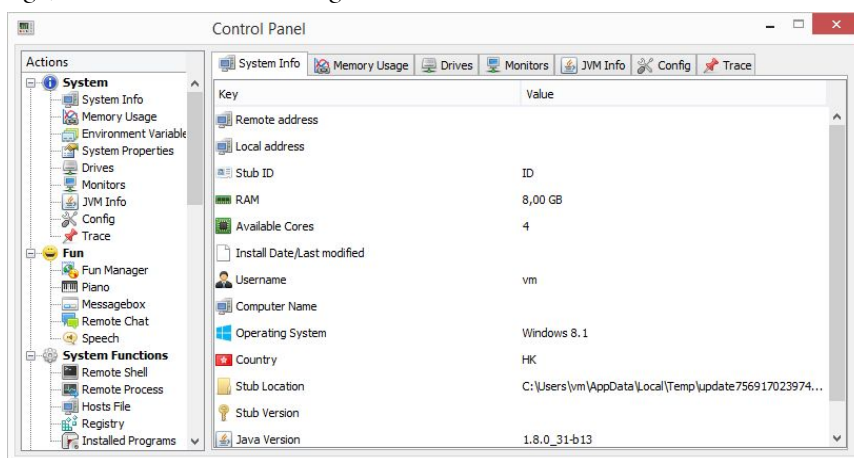


Fig 5. JRat Controller screen for an infected host

<sup>6</sup> <https://github.com/java-rat/web>

## Anti-Analysis

JRat contains a number of interesting features to thwart analysis by a malware researcher.

```
44  /*
43  * Unable to fully structure code
42  * Enabled aggressive block sorting
41  * Lifted jumps to return sites
40  */
39  static {
38      v0 = "\u00be\u00de\u0094\u009f\u0097".toCharArray();
37      var0 = 0;
36      while (v0.length > var0) {
35          v1 = v0;
34          v2 = var0;
33          switch (var0 % 7) {
32              case 0: {
31                  v3 = 235;
30                  ** break;
29              }
28              case 1: {
27                  v3 = 138;
26                  ** break;
25              }
24              case 2: {
23                  v3 = 210;
22                  ** break;
21              }
20              case 3: {
19                  v3 = 178;
18                  ** break;
17              }
16              case 4: {
15                  v3 = 175;
14                  ** break;
13              }
12              case 5: {
11                  v3 = 59;
10                  ** break;
9              }
8          }
7          v3 = 146;
6  lbl26: // 7 sources:
5          v0[v2] = (char)(v0[v2] ^ v3);
4          ++var0;
3      }
2      c.a = new String(v0).intern();
1  }
77
```

Fig. 6 An example of the ZKM obfuscated JRat code.

The code itself is obfuscated using Zendix Class Master (ZKM),<sup>7</sup> a commercially-available Java obfuscator. ZKM obfuscates the code by giving it generic class, method, and variable

<sup>7</sup> <http://www.zelix.com/klassmaster/featuresZKMScript.html>

names, it also encodes the strings by xoring them with a series of random bytes, and includes extraneous code-paths. All of this is done to make the java bytecode harder to decompile and analyze for the reverse engineer.

The JRat JAR file contains an encrypted config file named `config.dat`. The JRat config file is encrypted using AES in CBC mode. The encryption key and IV are cleverly hidden in the “extra” field for the zipped `config.dat` file. As illustrated in the example below (Fig. 7), the extra field begins at offset `0x30` of the file header for a given file in the compressed JAR. Within the 32 byte `extra` field, the first 16 bytes are the AES decryption key, and the last 16 bytes store the IV.

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0000	Signature			Version		Flags	Compression	Mod:time	Mod: date	CRC-32						
0x0010	CRC-32	Compressed size			Uncompressed size			File name len	Extra field len							
0x0020	File name (variable size)															
0x0030	Extra field (variable size)															

Fig. 7 An example file header in a compressed Zip or JAR file.

Once it is decrypted, we are able to extract the plaintext configuration information including the domain of the command and control server and port number (Fig 8). JRat also employs anti-virtualization features to detect and shut down if it is being run in VirtualBox, VMware, or other virtualization software.

JRat is low cost, versatile, extensible, and feature rich. Given these facts and the diversity of systems that JRAT can infect it is perhaps not surprising that the attackers chose this particular RAT.

```
delayms=-1
addresses=axroot.com:5006,
hiddenfile=false
icon=-1
mutex=false
error=true
title=
runnextboot=false
timeout=false
droppath=2
tititle=jRAT
melt=false
toms=-1
reconsec=10
mport=-1
perms=-1
id=Name5006
per=false
os=win mac linux
pass=7110eda4d09e062aa5e4a390b0a572ac0d2c0220
debugmsg=true
message=
delay=false
ti=true
vm=false
timsgfail=Disconnected from controller
name=japs
timsg=Connected to control controller
window=false
```

*Fig. 8 A decrypted JRat config file*

## **Bandook Malware Family**

The other malware family used in this campaign is the commercially available RAT known as “Bandook.” Bandook has been available since roughly 2007. This sample seems to have been continuously developed and improved over the course of the last couple of years. Unlike JRat, Bandook is only able to target Windows computers.

### **Core Functionality**

All Bandook executables are similar in size. Generally, they are masqueraded with fake Flash Player, Office document, or PDF document icons. None of the Bandook samples we have found in this campaign have been configured so as to execute an actual decoy document.

Normally, Bandook is distributed with an initial stub. This executable would contain another PE32 binary as an embedded PE resource. Bandook makes use of a common technique referred to as “process hollowing.” It instantiates several suspended browser processes and then replaces the loaded executable memory with the code contained in the embedded resource previously mentioned.

As an example for analysis, we take the original binary with hash `b002e8b6406fbdf3de9bfc3493e61c8a44b331f53125e8fed9daa351c49fd34` and, more importantly, the embedded resource named “O9897DDD” with hash `c447fd4d6e1deb794acde683bb2176becf353c6e1b2acdfced27c4413711f6f0`.

Interestingly, this binary was uploaded on [malwr.com](http://malwr.com) in early June 2016 with the file name “Form13.exe” (which might suggest a development version). Currently, the same binary doesn’t seem to be available in any other malware repository to which we have access. In this case, the malware did not execute after having successfully identified a virtualized environment, which might suggest the upload was potentially done by the authors as an attempt to verify the evasion technique.

It is also worth noting that while normally the embedded resource is obfuscated in binaries distributed in the wild, this specific case is the only one we identified with the resource embedded in the clear.

## Network Indicators and Modularity

After some initialization, Bandoob performs an initial beacon with the general information and configuration details it previously collected. Then it expects a command in response from the Command & Control server. If idle, the C&C will reply with "@0000", and the malware will keep beaoning back the title bar of the currently active window, until it is instructed to do something else.

Interestingly, the basic payload isn't provided with the code to perform any significant action. If instructed to do so, Bandoob will download additional DLL files which provide the specifically desired functionality. This is probably meant to limit the exposure of the core modules to analysts, and to vet the infection before performing a full deployment.

In this case the available DLLs can have the names:

```
cap.dll  
extra.dll  
pws.dll  
tv.dll  
Ammyy.dll
```

We were able to obtain the first three DLLs, which were located at the URL <http://axroot.com/plgro/>.

The following is a list of overall features available in this version of Bandoob:

- Screen capture
- Webcam recording
- Audio recording
- File search, creation, deletion and exfiltration
- Spawn a shell
- Get list of available Wireless networks
- Get list of MTP devices
- Monitor USB devices

# Attribution

## Observed Links to the Government of Kazakhstan

Given the common thread tying together the targets we find it likely that this campaign was carried out by—or on the behalf of—the government of Kazakhstan, or forces allied with the government. The majority of the targets of the malware campaign are currently embroiled in legal disputes with the government of Kazakhstan in European courts or are the family members or associates of people involved in these disputes. The titles of spearphishing emails often indicate that the targets are being singled out specifically for their interest in matters pertaining to Kazakhstan, such as “Information KZ,” “Press document KZ,” and “Kazakh NEWS of importance - Vladimir.”

## Observed Links to Arcanum Global Intelligence

Leaked emails published by Kazaword<sup>8</sup> allege that the government of Kazakhstan had previously hired a private intelligence company known as Arcanum to perform a surveillance and data extraction mission (codenamed “Raptor”) targeting Mr. Ablyazov and his family. Among the services offered by Arcanum are “Full Spectrum Cyber Operations” which they describe using the following language:

When the need exists, we overlay Full Spectrum Cyber Operations on these core capabilities, our principals’ experience, and special technical activities. We do this in order to offer a potent resource to support cyber and information operations planning and execution virtually anywhere in the world.

When our government clients come under threat, Arcanum Global’s embedded specialists and capabilities support them with a full suite of response options, including (in consonance with applicable laws and regulations) an array of countermeasures as well as both in-kind and asymmetric responses.

We invite you to schedule a comprehensive and completely confidential discussion of your cyber concerns and objectives with our specialists. After

---

<sup>8</sup> The emails themselves were hosted on Megaupload and have since been taken down as a result of litigation by the government of Kazakhstan, but they have been reported on extensively. You can find an extended discussion of their contents here: <http://www.viktor-khrapunov.com/en/publications-en/mediapart/>.

analyzing closely your requirements and the physical and cyber environments in which you must operate, Arcanum Global's holistic team of technical, operational and management specialists will recommend specific (and potentially sensitive) solutions – and then stand beside you to implement them and assure you realize your goals and achieve mission success.

Emails published by Kazaword and analyzed by Mediapart allege that Arcanum employed Bernard Squarcini, head of France's domestic intelligence agency, the Direction centrale du renseignement intérieur (DCRI) from 2007 to 2012, to inform the Kazakh authorities of the progress of the legal proceedings against Ablyazov and to lobby certain figures in France. Squarcini confirmed to Mediapart that the government of Kazakhstan is a client, but Arcanum spokeswoman Yael Hartmann denied that the company was responsible for the spearphishing attempts, insisting that the company has complied with Swiss law.

There is certainly some strong evidence consistent with there being a link between Operation Manul and the government of Kazakhstan and between the government of Kazakhstan and Arcanum. However, we observe no direct links between Operation Manul and Arcanum. The technical evidence discussed below, we believe points instead to an Indian company: Appin.

## **Observed Links To Appin**

We examined the behavior of the command and control domains used by Operation Manul as they moved from IP to IP. Using Passive Total, we observed that the C2 domains from Operational Manul used a total of 76 IPs from 2008-07-20 to 2016-05-11. We must consider that these domains could have been used by other actors over this time period.

While considering attribution of the actors behind Operation Manul, we investigated the possibility of infrastructure overlap with known actors. Gathering data from existing APT reports<sup>9</sup> we automated gathering of historical data from known APT domains from the Passive Total API and comparison with the historical data from Operational Manul domains.

From this we were able to observe overlaps between Operation Manul and an actor known as Appin. Appin is an Indian company that allegedly provides offensive

---

<sup>9</sup> <https://github.com/kbandla/APTnotes>



cyber-capability on a contract basis. A 2013 report by the cybersecurity firm Norman Shark, titled “Operation Hangover: Unveiling an Indian Cyberattack Infrastructure”<sup>10</sup>, describes multiple campaigns linked to this actor. The campaigns included attacks on Punjabi separatists, Norwegian telecom Telenor, and multiple other companies.

Appin is an exceptionally noisy actor, which might be expected given the contract nature of their work. Prior research<sup>11</sup> revealed 607 domains related to Appin which we were able to link via historical passive DNS to 1345 IPs. Of these, there were direct overlaps for two of the Operational Manul domains. There were indirect overlaps (same IP, at different times) with 110 of the Operation Hangover domains and all but two of the domains associated with Operation Manul.

The domains [researchwork.org](http://researchwork.org) and [dropboxonline.com](http://dropboxonline.com) were both on 64.202.189.170 on 2011-01-14. Additionally, the domains [adobeair.net](http://adobeair.net) and [bikefanclub.info](http://bikefanclub.info) both resided on 50.63.202.94 from 2014-04-24 to 2014-04-25. The [researchwork.org](http://researchwork.org) and [bikefanclub.org](http://bikefanclub.org) domains were attributed to Appin in the Operation Hangover report, while [adobeair.net](http://adobeair.net) and [dropboxonline.com](http://dropboxonline.com) were observed during the investigation of Operation Manul. Additionally there was a near overlap between [abobeair\[.\]net](http://abobeair[.]net) (one of the Operation Manul domains) and [appinsecurity\[.\]com](http://appinsecurity[.]com) (attributed to Appin in the Operation Hangover report) both hosted at 174.120.120.151 just five days apart in August of 2010.

What’s more, according to an appeal filed in a Swiss court on behalf of the Ablyazov family, several of the malware samples sent to Mr. Ablyazov’s son-in-law and his attorney and linked with this campaign were variants of the HackBack Trojan. This Trojan is in the same malware family as the Trojan found on an Angolan activist’s computer at the Oslo Freedom Forum in 2013—which was also linked to Appin by researchers at ESET and Norman Security<sup>12</sup>. We were unable to obtain the samples mentioned in the legal documents at the time of this writing.

A report written by the Swiss federal police, which investigated the origin of several of the spearphishing emails sent to Ablyazov’s family and associates, concluded that the emails were sent from IP addresses in India.

---

<sup>10</sup>[http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling\\_an\\_Indian\\_Cyberattack\\_Infrastructure.pdf](http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyberattack_Infrastructure.pdf)

<sup>11</sup><http://veroo7.com/tools/APTnotes/2013/Unveiling%20an%20Indian%20Cyberattack%20Infrastructure%20-%20appendixes.pdf>

<sup>12</sup><http://www.welivesecurity.com/2013/06/05/operation-hangover-more-links-to-the-oslo-freedom-forum-in-cident/>

While there are links to Appin, it's not conclusive that Operation Manul was carried out by this actor. Both 50.63.202.94 and 64.202.189.170 are very busy domains. Passive Total tells us that 50.63.202.94 has hosted 4535 unique domains since 2012, while 64.202.189.10 has hosted 4213 unique domains since 2009. Additionally, while the overlap with Appin exists, the fact that domains used the same IP at the same time is insufficient for concrete attribution. The evidence is consistent with links to Appin, but remains inconclusive. Certainly, the sort of targeting we have seen in Operation Manul appears to be consistent with other efforts targeting activists that have been associated with the same actor.

# MANUL SERVERS IPS DOMAINS ASSOCIATED WITH HANGOVER

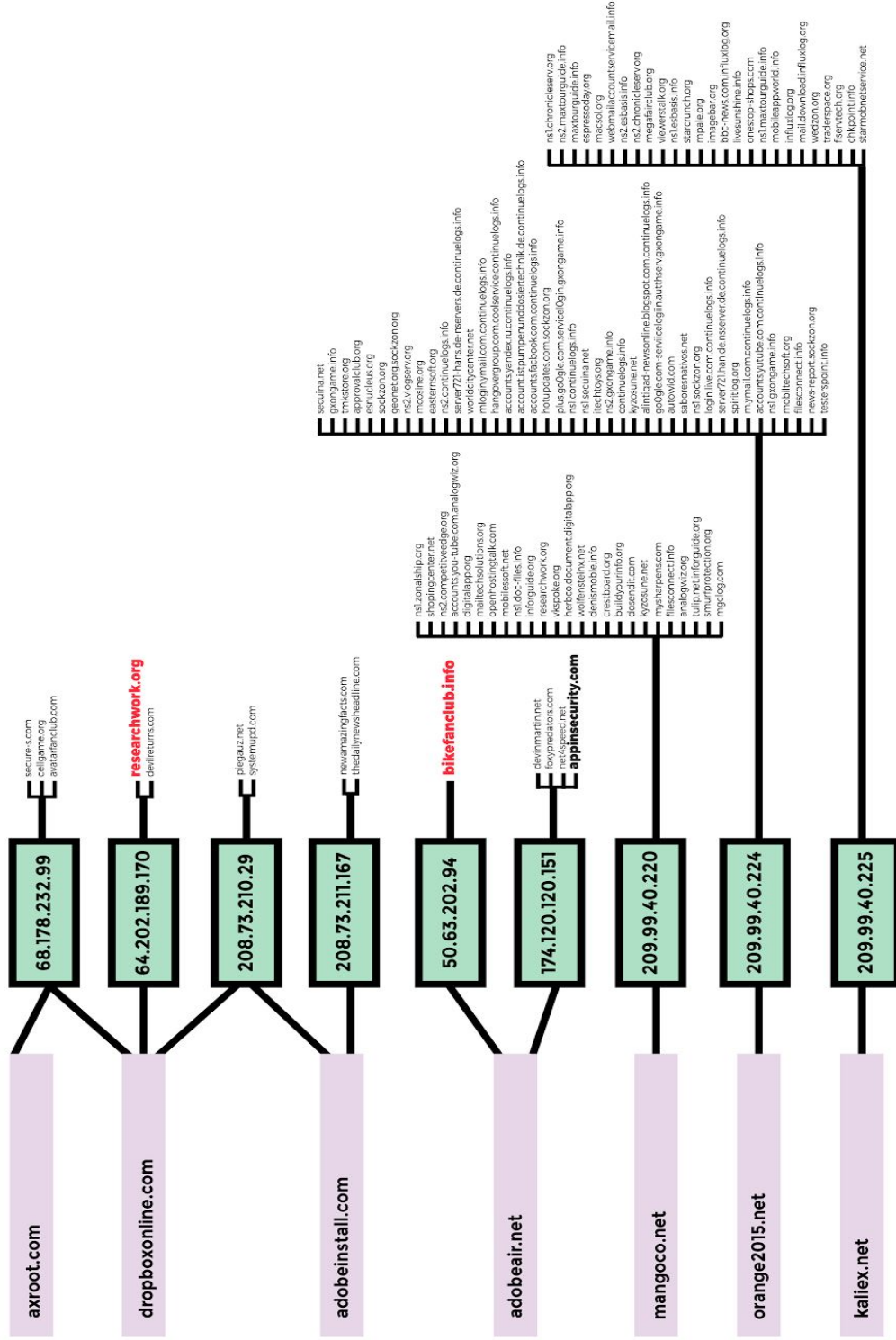


Fig 9. An illustration of the shared network infrastructure between Operation Manul and Operation Hangover. Domains highlighted in red shared servers with Operation Manul domains at the same time.

## Other Possible Targets

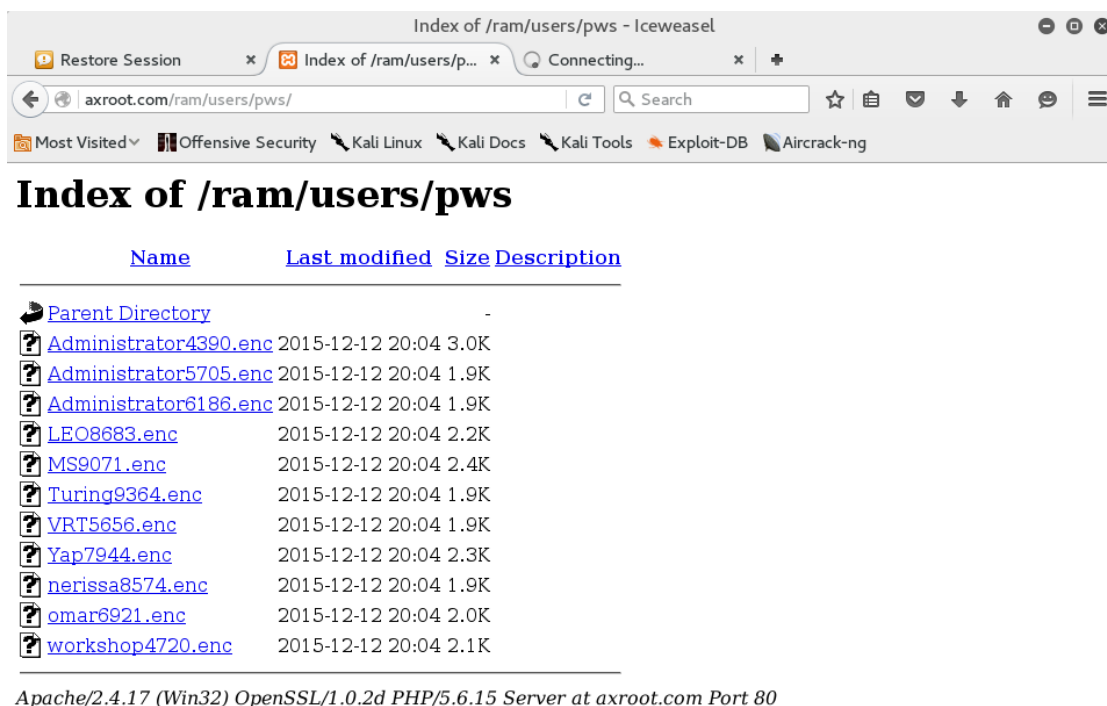


Fig 10. Uploaded password files from other victims

While investigating the C2 servers associated with Operation Manul, we discovered several open directories which contained files presumably related to other operations being run by this same actor (Fig 10). Additionally, we discovered web control panels for several different commodity RATs located under directories that appeared to be code-names for different operations (Fig 11). We also discovered several files which were presumably uploaded from other victims' computers (Fig 12). Lastly, we discovered encrypted data dumps from yet more campaigns, which we were unable at the time of this report.

We found many related samples of the Bandoock Trojan while we were doing our research. For example, 65af112ce229ad888bf4bbba1e3dba701e0e68c9caf81543bb395a8b8192ba8e contains references to Al Qaeda/ISIS material and the forged document is from an Arabic language pack. This sample however is associated with the same C2 servers used by Operation Manul.

We also found several uploaded log files which indicate the presence of an Android RAT. Unfortunately we were to find samples of this RAT at the time of this report.

The discoveries that we made while investigating the command and control infrastructure associated with this campaign suggest that these attackers are “hired guns” and have multiple operations against different targets going on at the same time.

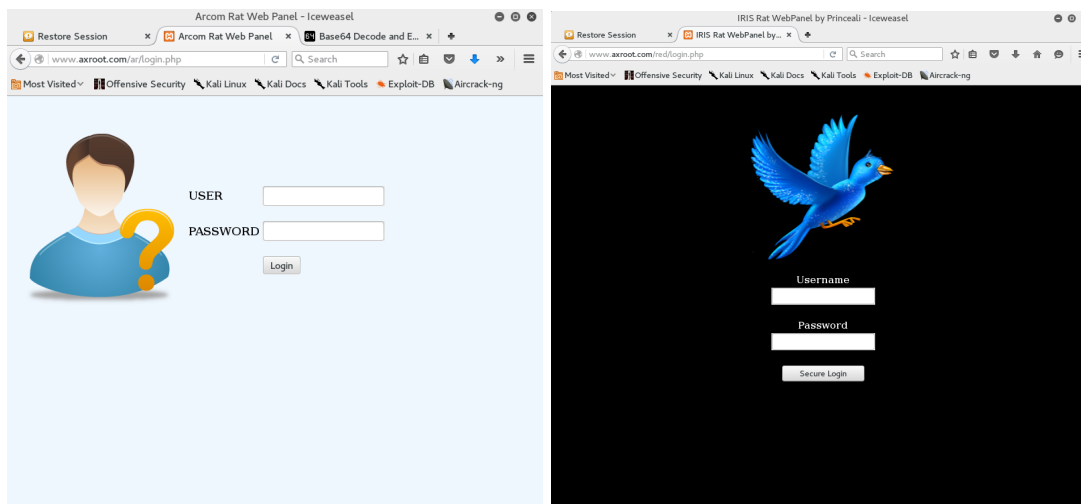


Fig 11. Web based RAT control panels found on Operation Manul C2 Servers

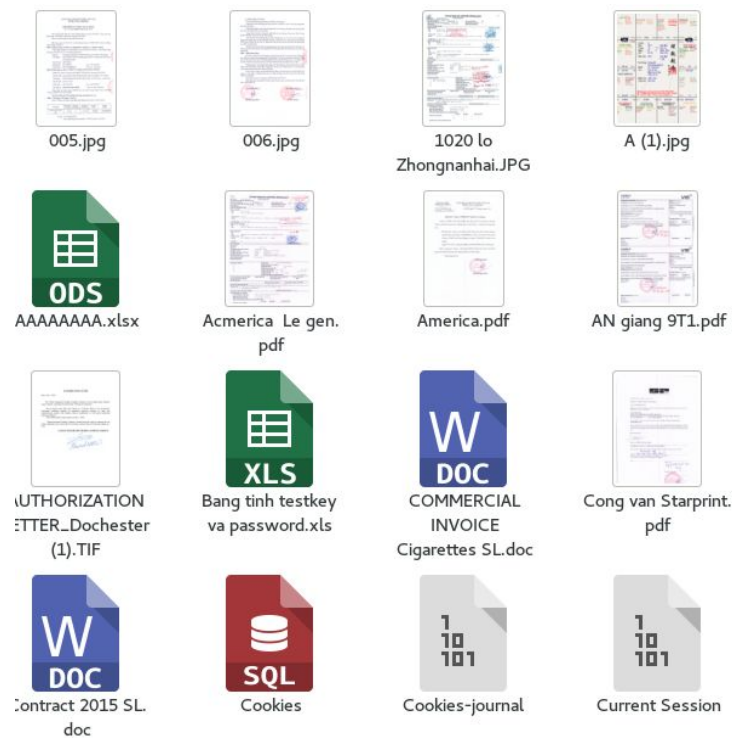


Fig 12. Uploaded documents from the victim of another campaign found on Operation Manul C2 servers.

## Conclusion

Operation Manul is not particularly sophisticated, but it is well-understood that attacks don't need to be sophisticated in order to be effective. Not a single sample that we have found in this campaign has employed a 0-day vulnerability. Unlike the lawful interception software that companies such as FinFisher and Hacking Team sell to governments and law enforcement, the RATs employed in this campaign are not only commercially-available to anyone, they're cheap.

The fact that these attacks are not sophisticated should not discourage other researchers from doing similar work. For activists and journalists who are being surveilled by authoritarian governments, surveillance is often just the first step in a campaign of intimidation, threats, and even direct violence. This kind of security research has the potential to have a real impact on vulnerable people. We suspect that the use of malware by governments to spy on political dissidents, especially exiles who live outside of their government's direct sphere of influence is increasingly common, which presents many opportunities for further research.

The possible connections between the government of Kazakhstan and companies that provide "hackers for hire" suggest that the problem of governments using malware to spy on political exiles and independent journalists goes beyond the sale of lawful interception software. We hope that further research will help to shed light on this practice and the companies that make these services available.

## Acknowledgements

There are many people without whom this work would not have been possible. The authors wish to thank the researchers behind Operation Hangover, whose work we depended heavily upon: Snorre Fagerland, Morten Kråkvik, Jonathan Camp, and Ned Moran.

The authors wish to give special thanks VirusTotal, Joe Security, Hex-Rays, and Passive Total for providing access to their software and services.

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.

We would also like to thank our friends and family who supported us throughout this research.

# Appendix A: Indicators of Compromise

## C2 Servers

The samples from the Operation Manul campaign described in this paper use the following command and control (c2) domains.

axroot.com
kaliex.net
adobeair.net
mangoco.net
jaysonj.no-ip.biz
orange2015.net
accountslogin.services
adobeinstall.com
adobe-flashviewer.accountslogin.services
dropboxonline.com

## Hashes

The following are hashes of malware samples discovered during our research which are associated with Operation Manul.

0491f4e55158d745fd1653950c89fcc9b37d3c1102680bd3ce67616a36bb2592
06529ac1d3388732ebca75b8ee0adf0bc7f45d4c448ec98223dd7a258a0f1f33
1192b5111f7c75417215a1285a20147f5ab085368fa95d74e7603d26736057ac
1192b5111f7c75417215a1285a20147f5ab085368fa95d74e7603d26736057ac
1e3966e77ad1cbf3e3ef76803fbf92300b2b88af39650a1208520e0cdc05645b
2431ff8ba00923a9c115a57e541d9d20e0a68b6cb1b48b87e7797864cf07dfab
345773dc4215c8c189d21536755614ca7b89082b96563239e363dd72c0cd8c68
373231f5be17e09e4ce94f76b35e5be57c961d6c8a9286b2e20e203d53b3c9dd
39802d53ae4a29c528626b0870872040dc5c994fb3b6b9e4a3b982144ad56e6c
40d30bc2db27e2a8a12cdeb5aae19f04064e5a1775bd3e6cf61a7070b797d3b3
40e9c694901aeb27993a8cd81f872076ee430e151f64af06993eb79442103ef8



4730c6033d8644c0aae46003bab3254e4beb62187573ffb5ba5bc95a28ddcd93
4f1923485e8cdd052467d335a6384f93cd1d50b5d927aea471e56290be29ffa3
576ca2b0c5fe1c756c245cb82d6a2ecce7f6976d5c3f3b338f686e06955032cb
5e322d208d61dcbf17914e24103710c52878e8cf50957f3d336736f4a1851951
652ec150db9a191942807ee5cf4772e75dfac562739477eacc6655fbec880ad7
65af112ce229ad888bf4bbba1e3dba701e0e68c9caf81543bb395a8b8192ba8e
6eea4a67305f67cc7c016256e93eb816de32b6e9ad700f75828be9f97c28c0e0
75ee00a36d324a89fc9ef4d7dbe606b885ec072388ef7b55d39112af7dbca665
75f51845de4d0deae8aaab737a71bb8aed14bfa4919712bcdea212f62b70c07f
778a01389b17a8ff20c445e0856b3704ac50844faa8d36c01e0ff02518e4c6d3
8c33b645e6362ab7e8c8a9989715193b4c9655fd576812218f3957c3fff8c429
8d054753e0ed754398835bed794ba4fae64a2efb018f98d3c61064de8aaa231d
91d251b11c59b5e25e0c1ae55421893fcef8f180a97e2eef88122c61e8cdf1bae
926a0196e4a72ed6eb20b51953cc17e8856ea9c0ef554681b7d7f0ecad870a2e
926a0196e4a72ed6eb20b51953cc17e8856ea9c0ef554681b7d7f0ecad870a2e
99e699e358be9e59cfad6124f44a96d3d1577edf9767afe17281adb37d901e22
a91c2cad20935a85d6eed72ef663254396914811f043018732d29276424a9578
ade5bd96bfba79051f8e8ed8fe973edd89e5f1ec6469393967c3ad7519a95650
b002e8b6406fbdf3de9bfc3493e61c8a44b331f53125e8fed9daa351c49fd34
d803c4d736bcb247d23735a7160b93c2f3d98de5d432680f5eaf9212f965248c
e4381ad27b10d895ad8338ba399221d385653b83b8d5dbd5a32cb86a0c318d44
eccb3d7d1e8a7cd27c7caf21885c95122eed28361651e8e47b8c02828b232c7e
f56c545a3157f1cf753de5ac56bb52e5af42bc6b8225d26aafdce3b430287f34
fc49b37b879af6e675f223d324d32c894ba83952b2ee109d52bfa9bd8212e005
f9dd8ebb062842798d53e78633ed9ca296f4a93dafb0fe60320a34a3d58d78d4

## Appendix B: Further Reading

<http://www.viktor-khrapunov.com/en/publications-en/mediapart/>

[http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling\\_an\\_Indian\\_Cyber\\_attack\\_Infrastructure.pdf](http://enterprise-manage.norman.c.bitbit.net/resources/files/Unveiling_an_Indian_Cyber_attack_Infrastructure.pdf)

[https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling\\_Patchwork.pdf](https://s3-us-west-2.amazonaws.com/cymmetria-blog/public/Unveiling_Patchwork.pdf)

<http://www.welivesecurity.com/2013/05/16/targeted-threat-pakistan-india/>

<https://www.eff.org/deeplinks/2015/11/judge-rules-respublika-cannot-be-forced-take-down-articles-kazakhstan-proceed>