[**INSIDE THE SPYWARE CAMPAIGN AGAINST ARGENTINE TROUBLEMAKERS**](https://firstlook.org/theintercept/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/)

[](https://firstlook.org/theintercept/staff/morgan-marquis-boire/)

[Morgan Marquis-Boire](https://firstlook.org/theintercept/staff/morgan-marquis-boire/)

Aug. 21 2015, 10:05 a.m.

Alberto Nisman, the Argentine prosecutor known for doggedly investigating a 1994 Buenos Aires bombing, was targeted by invasive spy software downloaded onto his cellular phone shortly before his mysterious death. The software masqueraded as a confidential document and was intended to infect a Windows computer.

An investigation by *The Intercept* indicates that this targeting was likely not an isolated event. The person or persons behind the attempted monitoring appear to have run other surveillance operations involving various locations throughout South America, at least one apparently targeting a rabble-rousing Argentine journalist. In the process, they created at least four distinct spyware bundles, all communicating with the same server set to receive Nisman’s data. They also left traces showing that their operations were active as recently as March, raising the possibility that the online spying continues today.

Nisman (pictured above) made powerful enemies inside and outside of Argentina. In his decade-long investigation into the suicide bombing of a Jewish organization and community center, Asociación Mutual Israelita Argentina, he indicted a top Hezbollah operative and several Iranian officials, including a former president, former intelligence minister, and a former foreign minister. Four days before his death, he accused the president of Argentina, Cristina Fernández de Kirchner, and her foreign minister, Héctor Timerman, of being involved in a criminal conspiracy to let Iranian officials off the hook for the attack. He was called to testify before Congress.

But the night before he was slated to deliver that testimony, Nisman was found in his apartment dead from a bullet wound to the head. An autopsy ruled his death a suicide. But as details of the police investigation emerged, so did more and more questions into the manner of his demise. There was no suicide note, nor was any gunpowder residue found on Nisman’s hands. A document [requesting](http://www.clarin.com/politica/Documentos-confirman-Nisman-arresto-Cristina_0_1297070348.html) the arrest of Kirchner and Timerman was found in Nisman’s trash. And it seemed much of the evidence had been gathered in a [disorganized and erratic](http://www.newyorker.com/magazine/2015/07/20/death-of-a-prosecutor) manner.

[](https://firstlook.org/wp-uploads/sites/1/2015/08/ProtestNisman.jpg)

Protesters take part in a silent march to honor Nisman in Buenos Aires, February 18, 2015, one month after his death.

Photo: Enrique Marcarian/Reuters /Landov

Nisman’s death, and the circumstances surrounding it, led to a large protest in Argentina and[reportedly](http://www.bbc.com/news/world-latin-america-31515822) in France, Spain, and Israel. News outlets around the world have combed over the case. In an [article](http://tiempo.infonews.com/nota/155284/fein-quiere-saber-quien-llamo-a-lagomarsino-el-dia-que-murio-nisman) focusing on the phone calls Nisman made the day he died, the Argentine news website*InfoNews* revealed that the chief forensic lab technician of the Metroplian Police in Buenos Aires, Ezequiel Sallis, found a malicious file on Nisman’s phone. The file was named “estrictamente secreto y confidencial.pdf.jar,” meaning “strictly secret and confidential.” The filename extension “.pdf.jar” identifies it as a program written in the Java programming language but posing as a PDF document file. The file had been checked against an online anti-virus scanner,*InfoNews* said.

While it seemed like a shot in the dark, I searched [VirusTotal](https://www.virustotal.com/)for the document. VirusTotal is an online anti-virus website run by Google and a popular tool for sharing and analyzing malicious software. People upload files that they think may be suspicious and then these files are run through 56 different anti-virus products, including those made by Symantec, Kasperksy, Sophos, and McAfee. This is exactly what happened with the malicious spyware sent to Nisman. It was uploaded to VirusTotal, where I discovered [one file](https://www.virustotal.com/en/file/aa9aa05af8df2cc99eb936e2d17623a68abdbb60606bb097379457c4a3760116/analysis/) that matched the file name name reported in *InfoNews*. This file, VirusTotal informed me, had been uploaded into the service from Argentina on May 29, 2015. A source close to the investigation confirmed that this was the file that had been found on Nisman’s cellular phone.

The file “estrictamente secreto y confidencial.pdf.jar” would, under the default settings in Microsoft Windows, show up without the file extension, displaying it to an unsuspecting user as “estrictamente secreto y confidencial.pdf” in an attempt to fool the user into believing that the spyware was simply a document in the common PDF format. This file, sent to Nisman, is in fact a piece of spying software that’s been bundled together with a PDF. This “bundling” is a common technique for delivering spyware. The would-be spies have a program that allows them to select a “bait document,” combine it with the spying software, and then, typically, this build of the spyware would be delivered to a target by way of an explanatory email informing the recipient that they should open the attachment, as it contains interesting information.

At the [Black Hat USA 2015](https://www.blackhat.com/us-15/briefings.html#big-game-hunting-the-peculiarities-of-nation-state-malware-research) security conference in Las Vegas, in a talk with Marion Marschalek, a senior malware researcher at the cybersecurity firm Cyphort, I released details of the analysis of this attempt on Nisman, revealing that the software clandestinely packaged together with the tantalizingly named document “estrictamente secreto y confidencial.pdf” is an off-the-shelf commercial digital spying tool or “remote access toolkit” (RAT) known as AlienSpy. This particular build of the spyware appears to have been created on December 1, 2014, approximately six weeks prior to Nisman’s death. AlienSpy boasts an array of intrusive surveillance features, such as recording the victim’s keystrokes, eavesdropping via a digital device’s built-in microphone, remote viewing of the desktop, and the ability to turn on a victim’s webcam “without user notification.” AlienSpy was born as the free “[Frutas](http://www.symantec.com/connect/blogs/cross-platform-frutas-rat-builder-and-back-door)” RAT and was [detected](http://www.symantec.com/connect/blogs/targeted-attacks-delivering-fruit) in a campaign in Mexico. It was redeveloped for sale as a “Premium RAT” known as “[Adwind](https://web.archive.org/web/20130213044621/http:/adwind.com.mx/).” Prices ranged from $75 for a single license to $250 for multiple licenses (for more details see [Appendix: Technical Investigation Details](https://firstlook.org/theintercept/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/?comments=1#appendix) at the bottom of the document).

While this spyware platform supports the Windows, OS X, Linux, and Android operating systems, the particular package that targeted Nisman was tailored for Windows. He may have caught a lucky break by trying to open it on his phone, as it would not have been able to run on his Android device. Had Nisman opened the document on his laptop or desktop — and it’s not established whether he did or did not do so — he would have been disappointed. Despite the enticing name, the file would have shown nothing but a single blank page. While he pondered this, spying software would have been installed on his machine.

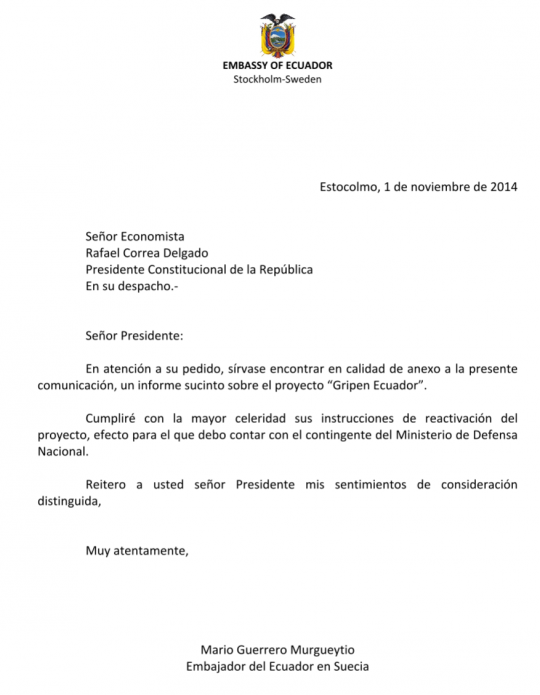
After Black Hat, a summary of my presentation appeared in [*VICE*](http://motherboard.vice.com/read/malware-hunter-finds-spyware-used-against-dead-argentine-prosecutor) and I was interviewed by Argentine dailies [*Clarín*](http://www.clarin.com/politica/Hackers-afirman-descubrir-virus-Nisman_0_1411659104.html) and [*La Nación*](http://www.lanacion.com.ar/1818409-nisman-tenia-en-su-celular-un-potente-virus-para-espiarlo). Subsequently, a well-known Argentine investigative journalist, Jorge Lanata, [revealed](http://pastebin.com/iiAGSMYc) that on December 3, around the time Nisman appears to have been targeted, he was also sent spyware, which appeared to be the same as Nisman’s. Lanata posted the [email](http://pastebin.com/iiAGSMYc) and [attachment](http://www.megafileupload.com/4Ybp/attacheado.txt) he received online. I downloaded both and verified that the spyware was indeed the same.

The spyware that both Lanata and Nisman received spoke to the same “command and control” domain, an Internet address that points to a remote machine used by spies to control the software they have implanted on a victim’s machine. This is where data stolen from a target is received and from which new commands to the spyware are issued. In the case of Nisman and Lanata, their spyware was the same, and it communicated with the same remote domain, “deyrep24.ddns.net,” and thus can be presumed to be controlled by the same people.

Lanata is one of the most prominent critics of government corruption. The email he received containing spyware purported to be from Claudio Bonadio, and was labeled with the subject “Expediente BONADIO.” Bonadio is a well-known Argentine judge who probed the Kirchner family’s hotel company, Hotesur, amid allegations of money laundering stoked by a 2014 report on “Periodismo Para Todos,” the TV news show Lanata hosts. The email from Bonadio to Lanata seems likely to have been specifically forged by whomever was targeting Lanata to make it more probable that the journalist would trust and open the correspondence. While, at this stage, it is unclear why Lanata was targeted, the use of identical spyware indicates that the attempted hack attack against Nisman was likely not an isolated incident.

The president’s son, Máximo Kirchner, has also [claimed](http://www.buenosairesherald.com/article/196727/an%C3%ADbal-m%C3%A1ximo-kirchner-received-same-virus-as-lanata) to have received the same malware, although we were unable to verify this. Anibal Fernandez, a Kirchner ally and politician in the same [political party](https://en.wikipedia.org/wiki/Justicialist_Party), has [characterized](http://www.d24ar.com/nota/358414/anibal-dijo-que-el-virus-que-lanata-denuncio-se-lo-mandaron-a-todo-el-mundo.html) the malware as common and inconsequential. His amateur opinion is incorrect on both counts. This type of malicious code is not similar to the ransomeware and banking crimeware that average computer users commonly receive. It’s used to view the remote activities of a targeted individual and is highly invasive. Additionally, while AlienSpy is relatively easy to obtain, the specific actors behind the attacks on Nisman and Lanata have not been indiscriminate.

During *The Intercept*’s investigation, we discovered, in VirusTotal, three additional spyware bundles, beyond the one sent to Nisman and Lanata, which communicated with the same command and control domain, “deyrep24.ddns.net.” Chronologically, the earliest of these spyware samples,”3 MAR PROYECTO GRIPEN.docx.jar,” was packaged on November 20, 2014. This is a build of AlienSpy that was uploaded from an Internet address in Ecuador on November 22, 2014. The bait document that the spyware was combined with can be seen below:

[](https://firstlook.org/wp-uploads/sites/1/2015/08/Screenshot-from-2015-08-15-2203481.png)

As seen in the malware sample, the “Proyecto Gripen” document purports to be a communication between Mario Guerrero Murgueytio, the Ecuadorian ambassador in Sweden, and the president of Ecuador, Rafael Correa Delgado. The subject is alleged negotiations for the Ecuadorian purchase of the multi-role fighter, “Gripen,” produced by the Swedish aeronautics company Saab. Neighboring Brazil had previously placed an order for 36 such aircraft. Argentina [was looking into](http://www.janes.com/article/51023/saab-not-selling-gripens-to-argentina-official-says) purchasing 24 of the Gripen fighters, however, it seemed that the deal was unlikely to be completed due to a lurking veto from the United Kingdom related to the disputed Falkland Islands. The alleged information contained in the document is particularly intriguing because Ecuador is harboring, in its London embassy, WikiLeaks cofounder Julian Assange, who Sweden has requested be extradited on sexual offense allegations. That said, it is common for spies to bundle spyware with interesting bait, real and forged. At this stage, we have been unable to establish whether the document, or any information contained within it, is authentic. (Ecuador’s U.S. embassy did not respond to a request for comment.)

[](https://firstlook.org/wp-uploads/sites/1/2015/08/Screenshot-from-2015-08-15-220446.png)

The second additional spyware bundle we found also uses the same command and control domain as the software used to target Nisman but is not the same type of program. “Documentos.pdf.jar” was built on December 23, 2014, and uploaded to VirusTotal from an Internet address in Argentina on June 4, 2015. Instead of AlienSpy, the remote access toolkit that this spyware bundle uses is software called “[Adzok – Invisible Remote Administrator](http://adzok.com/).” Similar to AlienSpy in functionality, the website shows that Adzok is based in Bolivia. The [premium version](http://adzok.com/?pg=buy) costs $990, but the spies elected to use the “free” version (see the [appendix](https://firstlook.org/theintercept/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/?comments=1#appendix) for more details). When opened, the target would see a file with a single blank page.

The third additional spyware we found is also controlled via “deyrep24.ddns.net” and is called “Reporte Confidencial.pdf.jar.” It appears to have been built on January 9, 2015. It was uploaded to VirusTotal from an Internet address in Ecuador on January 10, 2015. It contains a document with a single blank page.

In addition, we discovered that the spies in March created a new command control domain, “daynews.sytes.net,” that we could tie back to the command and control server used in the attack on Nisman and Lenata and link to the other spyware samples. The two servers were hosted at the same Internet protocol, or “IP,” address at the same time, and even moved together to a new IP address at a new hosting company. (For more information, see the[appendix](https://firstlook.org/theintercept/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/?comments=1#appendix).) It is common practice to move the servers behind a command and control domain in order to frustrate tracking of the origins of a spying campaign. This related infrastructure was created weeks after Nisman’s death.

[](https://firstlook.org/wp-uploads/sites/1/2015/08/Nisman_timeline_v6.jpg)

Activities of the person(s) that were trying to spy on Alberto Nisman.

Conclusively attributing of this type of activity is a tricky problem. It is difficult to reliably place blame on a specific country, agency, or group based on analysis of suspicious software alone. What we can say about the spy or spies who targeted Nisman is that their efforts spanned at least several months, are linked to various locations in South America and involve low-end commercial tools and multiple high-profile targets, two of whom were Argentine troublemakers.

**Appendix: Technical Investigation Details**

This spy tool used to target Nisman began life as a free Remote Access Toolkit known as “[Frutas](http://www.symantec.com/connect/blogs/cross-platform-frutas-rat-builder-and-back-door)” and was [detected](http://www.symantec.com/connect/blogs/targeted-attacks-delivering-fruit) in a campaign in Mexico. It was later redeveloped for sale as a “Premium RAT” known as “[Adwind](https://web.archive.org/web/20130213044621/http:/adwind.com.mx/).” Prices ranged from $75 for a single license to $250 for multiple licenses. In November 2013, AdWind was rebranded to [UNRECOM](http://blog.crowdstrike.com/adwind-rat-rebranding/) (UNiversal REmote COntrol Multi-platform), which was [spotted](http://blog.crowdstrike.com/adwind-rat-rebranding/) in targeted attacks in the Middle East. The latest version, called “AlienSpy,” has been [found](http://contagiodump.blogspot.ch/2014/11/alienspy-java-rat-samples-and-traffic.html) by security researchers in targeted spying operations. This [report](http://www.fidelissecurity.com/sites/default/files/FTA_1015_Alienspy_FINAL.pdf) details the current features of AlienSpy.

[](https://firstlook.org/wp-uploads/sites/1/2015/08/6a0147e41f3c0a970b01a3fd0dd84a970b-pi.jpeg)

Screenshot of UNRECOM

Each of the AlienSpy samples identified as related to the Nisman attack is built in roughly the same way. There’s an outer .jar file containing a folder named META-INF and two files: Favicon.ico and Principal.class. Upon execution, Principal.class unzips the contents of “Favicon.ico” (which is not actually an icon file, but a zip archive), and looks for a filename containing “.jar”. When found, it drops it to a randomly-named temp file starting with a constant string and invokes java to run it. Inside the .jar file from “Favicon.ico,” “Main.class” is obfuscated using “Allatori,” a Russian-origin JVM obfuscator used by Adwind / AlienSpy. This reads part of an RC4 key from the file “ID.” To this it appends a constant string, and then uses the full RC4 key to decrypt the contents of MANIFEST.MF giving the actual Adwind implant JAR file. You can read more about how Allatori works and how to deobfuscate it, [here](https://boredliner.wordpress.com/2014/02/07/cracking-obfuscated-java-code-adwind-3/) and [here](https://www.moparscape.org/smf/index.php?topic=238584.0).

[](https://firstlook.org/wp-uploads/sites/1/2015/08/Screenshot-from-2015-08-15-212251.png)

Screen shot of Allatori Obfuscator 5.1 DEMO

There is no encryption on the Adzok sample, you can unzip “Documentos.pdf.jar,” then unzip “Favico.ico,” then you just unzip the file “0Java.jar” and can see the implant’s files including configuration.

**Nisman and Lanata sample:**

**Name: estrictamente secreto y confidencial.pdf.jar**

file hash: aa9aa05af8df2cc99eb936e2d17623a68abdbb60606bb097379457c4a3760116

Submission: AR

First seen: 2015-05-29 18:48:24

From timestamps inside the malware, this appears to have been built on the December 1, 2014.

contents of Favicon.ico:

-rw-r--r--  55381 Dec  1  2014 0doc.jar  
-rw-r--r--   8134 Dec  1  2014 1Estrictamente Secreto y Confidencial.pdf

**Related samples:**

The following samples speak to the same command and control domain as the piece of malware which targeted Nisman.

**Name: 3 MAR PROYECTO GRIPEN.docx.jar**

file hash: ca5481e56de4b78348c008c36803fc044baea9ea5a5ea8534b3e88ce35f0958a

Submission: EC

First seen: 2014-11-22 13:52:31

contents of Favicon.ico:

-rw-r--r--   49019 Nov 20  2014 0cliente.jar  
-rw-r--r-- 223819 Nov 20  2014 13 MAR PROYECTO GRIPEN.docx

**Name: Documentos.pdf.jar**

file hash: 0776cc9d22730006c5a818afe78f78e578107eccc5322424f49e2d4fff3efec4

Submission: AR

First Seen: 2015-06-04 17:24:33 UTC

contents of Favico.ico:

-rw-r--r--  Dec 23 2014 0Java.jar  
-rw-r--r--  Dec 23 2014 1Informe Reservado.pdf

**Name: Reporte Confidencial.pdf.jar**

file hash: c0664ca05a351388c903d7e989257fe244b25098bf74394a9325f4b0a7c5472b

Submission: EC

First Seen:  2015-01-10 02:00:33 UTC

contents of Favico.ico:

-rw-r--r-- 8132 Jan  9  2015 0Documento.pdf  
-rw-r--r-- 56200 Jan  9  2015 1server2.jar

**Command and Control**

The command and control server for the malware that targeted Nisman was:**deyrep24. ddns.net**and appears to have been created on 2014-11-07. Using a domain tracking and threat research platform called “[PassiveTotal](https://www.passivetotal.org/),” we learned that at the time of Nisman’s death this domain pointed to 50.62.133.49. This IP address is owned by GoDaddy and used for dedicated hosting. The domain moved to 192.169.243.65 (also a GoDaddy address) on March 2, 2015. The domain **daynews.sytes.net**appears to have been created onMarch 1, 2015 and was using the address 192.169.243.65 at the same time it was being used by deyrep24.ddns.net. We later see both hosts move to 46.246.89.246, which is used by Portlane Networks, a Swedish hosting provider.

**AlienSpy Configuration**

<?xml version="1.0" encoding="UTF-8" standalone="no"?>  
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">  
<properties>  
<comment>AlienSpy</comment>  
<entry key="pluginfolder">cOzdAJCuee</entry>  
<entry key="reconnetion\_time">3000</entry>  
<entry key="ps\_hacker">false</entry>  
<entry key="restore\_system">false</entry>  
<entry key="pluginfoldername">cOzdAJCuee</entry>  
<entry key="dns">**deyrep24.ddns.net**</entry>  
<entry key="install\_time">3000</entry>  
<entry key="port2">1040</entry>  
<entry key="port1">1030</entry>  
<entry key="taskmgr">false</entry>  
<entry key="vmware">true</entry>  
<entry key="jarname">documentos</entry>  
<entry key="msconfig">false</entry>  
<entry key="mutex">wMiSl1X1o423a2hh45Uifk8duasdf2S</entry>  
<entry key="install">true</entry>  
<entry key="instalar">true</entry>  
<entry key="vbox">true</entry>  
<entry key="password">ca19d6a81d35685b87547898c5e000a5fc9be554</entry>  
<entry key="NAME">Localhost</entry>  
<entry key="extensionname">jHs</entry>  
<entry key="prefix">officce</entry>  
<entry key="jarfoldername">0o86gb96</entry>  
<entry key="uac">false</entry>  
<entry key="win\_defender">false</entry>  
<entry key="connetion\_time">3000</entry>  
<entry key="folder">0o86gb96</entry>  
<entry key="jar">documentos</entry>  
<entry key="pluginextension">jHs</entry>  
<entry key="registry">389032</entry>  
<entry key="ps\_explorer">false</entry>  
<entry key="p2">1040</entry>  
<entry key="p1">1030</entry>  
<entry key="registryname">389032</entry>  
<entry key="wireshark">false</entry>  
<entry key="desktop">true</entry>  
<entry key="nickname">officce</entry>  
</properties>

**Adzok Configuration**

<?xml version="1.0" encoding="UTF-8" standalone="no"?>  
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">  
<properties>  
<comment>Adzok Free</comment>  
<entry key="dir">Java</entry>  
<entry key="reg">Java</entry>  
<entry key="pass">7854</entry>  
<entry key="hidden">true</entry>  
<entry key="puerto">7777</entry>  
<entry key="ip">**deyrep24.ddns.net**</entry>  
<entry key="inicio">true</entry>  
</properties>

**Email Targeting of Jorge Lanata**

The full email can be found [here](http://pastebin.com/iiAGSMYc).

Received: by 10.43.144.69 with HTTP; Wed, 3 Dec 2014 09:03:28 -0800 (PST)  
Date: Wed, 3 Dec 2014 15:03:28 -0200  
Message-ID: <CAFP1fxRwjW1xb4xfQo-kV0UDkDm9s5YuysEym3Am4SZGhgN34A@mail.gmail.com>  
Subject: Expediente BONADIO  
From: Claudio Bonadio <cfed.bonadio@gmail.com>  
To: jorgel....@gmail.com  
Content-Type: application/java-archive;  
name="Estrictamente Secreto y Confidencial.pdf.jar"  
  
*Thanks to Nico Waisman of Immunity for additional technical research and analysis. Additional thanks to Adam Meyers of Crowdstrike.*