Search

Packrat: Seven Years of a South American Threat Actor

December 8, 2015

Tagged: Argentina, Brazil, Disinformation, Ecuador, Latin America and the Caribbean, Malware, Packrat, Phishing, South America

Categories: Author, Claudio Guarnieri, John Scott-Railton, Morgan Marquis-Boire, Reports and Briefings

51

Authors: John Scott-Railton*, Morgan Marquis-Boire*, Claudio Guarnieri*, and Marion Marschalek**

*Senior Researcher, Citizen Lab, Munk School of Global Affairs; **Cyphort

Read the press release.

Media coverage: Associated Press, Vice Motherboard, CBC, ABC News, Fortune, Security Week, CIO, Softpedia, PC World, Global News, El Universo, The Register, US News & World Report.

Summary

This report describes an extensive malware, phishing, and disinformation campaign active in several Latin American countries, including Ecuador, Argentina, Venezuela, and Brazil. The nature and geographic spread of the targets seems to point to a sponsor, or sponsors, with regional, political interests. The attackers, whom we have named Packrat, have shown a keen and systematic interest in the political opposition and the independent press in so-called ALBA countries (Bolivarian Alternative for the Americas), and their recently allied regimes. These countries are linked by a trade agreement as well as a cooperation on a range of non-financial matters.

After observing a wave of attacks in Ecuador in 2015, we linked these attacks to a campaign active in Argentina in 2014. The targeting in Argentina was discovered when the attackers attempted to compromise the devices of Alberto Nisman and Jorge Lanata. Building on what we had learned about these two campaigns, we then traced the group's activities back as far as 2008.

This report brings together many of the pieces of this campaign, from malware and phishing, to command and control infrastructure spread across Latin America. It also highlights fake online organizations that Packrat has created in Venezuela and Ecuador. Who is responsible? We assess several scenarios, and consider the most likely to be that Packrat is sponsored by a state actor or actors, given their apparent lack of concern about discovery, their targets, and their persistence. However, we do not conclusively attribute Packrat to a particular sponsor.

Part 1: Packrat's Seven Years of Activity

The authors on this report have been independently investigating malware and phishing campaigns in Latin America. This report is the result of discovering that the cases we have been investigating are linked by a common threat actor with targeting in several countries, including Venezuela, Ecuador, Argentina, and Brazil. We refer to this threat actor as Packrat, to highlight their preference for packed, commodity Remote Access Trojans (RATs), and their retention of the same domains and servers over many years.

Image 1: Some of Packrat's known targets and activity types

Packrat has systematically targeted high profile political figures, journalists, and others in several countries with malware and phishing. In total we uncovered 12 different malware command and control domains, and over 30 samples of malware stretching over a seven year time period. Packrat also favors an interesting strategy: create and maintain fake opposition groups and news organizations, then use these to distribute malware and conduct phishing attacks.

Some of these organizations exist in name only, while others have a more elaborate online presence. Packrat has also created elaborate fake news organizations without any evidence we can find of malware or phishing activity.

Image 2: Packrat's major activities

We chart Packrat's activities back to at least 2008. Through correlation of network infrastructure, we identified several waves of activity, coupled with changes in tools and tactics. This section provides a brief chronology of Packrat's network infrastructure and activities. For a detailed chronology of the malware used, see 3. The Evolution of Packrat's Implants.

Packrat's Greatest Hits

2008-2013

Tools and infrastructure used by Packrat suggest that they have been active since at least 2008. During this period, Packrat used hosting services in Brazil, and some of their malware samples were uploaded from Brazilian IP space to popular online virus scanning services. Some of the messages they sent also contained Brazilian bait content. While this is suggestive of Brazilian targeting, we have yet to find confirmed victims from this period.

2014

By 2014, Packrat was targeting high-profile Argentine lawyer Alberto Nisman, and well-known investigative journalist and television news host, Jorge Lanata. Maximo Kirchner, son of Argentina's president, also announced that he was targeted. The screenshot he released of the phishing email he received is consistent with what we have seen, although we have not been able to verify his claims. In addition, a number of phishing domains with Ecuadorian and Venezuelan targeting that we identified became active during this period.

2015

2015 seems to have marked an extensive campaign of phishing and malware attacks targeting civil society and public figures, including parliamentarians in Ecuador. We observed a range of phishing domains and attacks, often using fake organizations during this period. We also found fake organizations and possible disinformation campaigns with targets in Ecuador, Venezuela and the Venezuelan diaspora.

1.1 Nisman and the Argentine Cases

In January 2015, controversial Argentine prosecutor Alberto Nisman was found dead of a gunshot under suspicious circumstances. Argentine news reported that a malicious file was found on his Android phone by the Buenos Aires Metropolitan Police forensic lab. The file was named "estrictamente secreto y confidencial.pdf.jar," or "strictly secret and confidential" in English.

An identically titled file was uploaded to VirusTotal from Argentina on the 29th of May, 2015. The file was a remote access toolkit, known as AlienSpy, which allowed an attacker the ability to record the activities of a target, access their email, their webcam, and more. However, the file was built for the Windows operating system, and could not have infected Nisman's Android phone.

The initial analysis of the alienspy implant by Morgan Marquis–Boire revealed the command and control server of the attackers to be deyrep24.ddns.net. In addition to the malware apparently used to target Nisman, Lanata, and Kirchner (see below), three other samples[1] were found which used deyrep24.ddns.net as a command and control domain. One of these, 3 MAR PROYECTO GRIPEN.docx.jar, was a build of AlienSpy (See Packrat's Implants) which masqueraded as a document containing communication between Ecuadorian President Rafael Correa and Ecuador's Ambassador to Sweden concerning the acquisition of fighter jets.

After the finding was made public, other targets came forward. Prominent investigative journalist and television host Jorge Lanata revealed that he too had been targeted by the same malware. The president's son, Maximo Kirchner, also claimed to have been targeted. We were unable to verify Kirchner's claim, however, a screenshot showing his targeting was included in a report of this claim:

Image 3: A screenshot included in this report showing Maximo
Kirchner's targeting

The email which he claims to have received has an attachment named "Estrictamente Secreto y Confidencial.pdf.jar" (size 67.3kb) which is the same as the malware sent to Nisman and Lanata. Additionally, the sender's email address (claudiobonadio88@gmail.com) purports to be well-known judge Claudio Bonadio. This similar to the targeting of Lanata, who also received an email also claiming to be from Claudio Bonadio (cfed.bonadio@gmail.com).

1.2 Ecuadorian Campaigns

In 2015, we began independently receiving a growing number of reports of phishing attacks via e-mail and SMS targeting journalists and other public figures in Ecuador. Some emails we examined had no political content, but were simple credential phishing for social media and email providers, like Gmail. Others, however, had explicit political content concerning a range of political figures and issues in Ecuador. Further investigation revealed an extensive campaign, as well as many fake organizations (See Section 6: Possible Deception Operations).

One of the authors developed a Gmail search query for strings associated with the attacks (See Appendix A: The Search Query). We shared this query with many potential targets, resulting in hits for phishing attacks, as well as suspicious Microsoft Word (DOCX) files sent to a range of journalists and public figures. These documents contained embedded RATs written in Java, including Adzok and AlienSpy (See Packrat's Implants). Subsequently, using indicators found in the JAR files, as well as an updated Gmail query we were able to identify a larger set of malicious files and domains used by Packrat (See Appendix B: Malware Samples).

We found a dense web of interconnections between phishing and malware sites. Sites often shared registration information, or were hosted from the same servers. We determined that the malware samples typically communicated with daynews.sytes.net, which is linked to the Argentine cases. Ultimately, investigation of this infrastructure also revealed malware and infrastructure in Brazil, and fake sites in Venezuela.
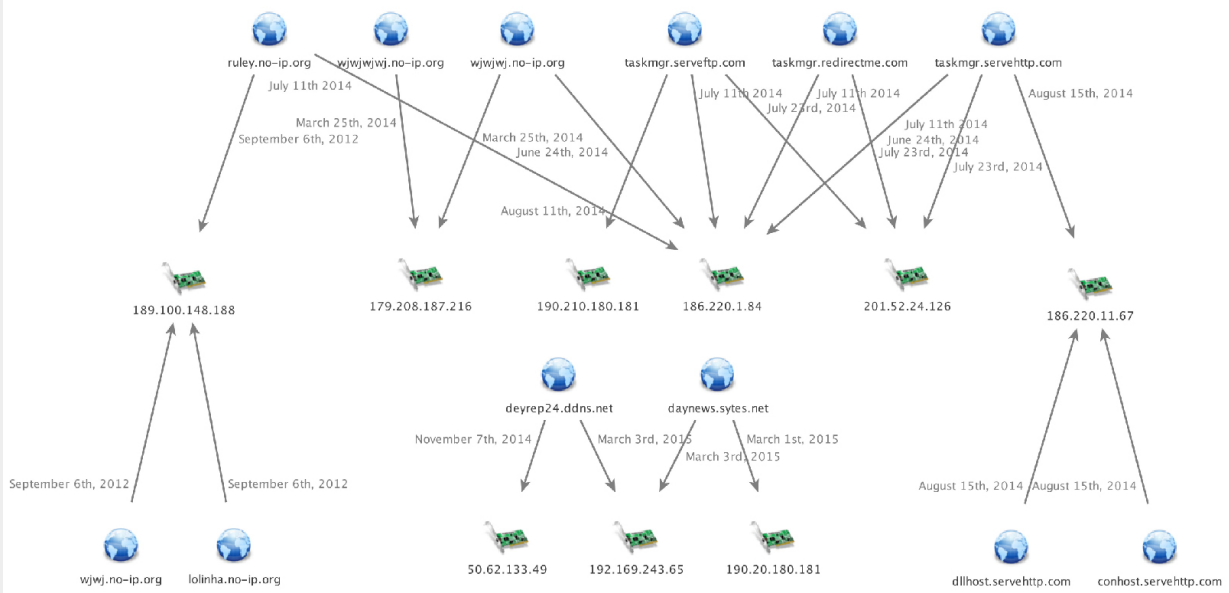
1.3 Shared Command & Control Infrastructure

This section describes Packrat's command and control infrastructure in narrative form, Appendix B provides a full list of Command & Control domains along with the related binaries and malware families.

Packrat's deyrep24.ddns.net domain was created on November 7th, 2014, and at the time of Nisman's targeting, pointed to the IP address: 50.62.133.49. This IP address belongs to a GoDaddy range for dedicated hosting, and on March 3rd, 2015, the domain moved to another GoDaddy IP: 192.169.243.65. Passive DNS records revealed that at the same time as this IP was being used by the deyrep24.ddns.net command and control domain, it was being used by the domain daynews.sytes.net which had been created on March 1st, 2015. Over the course of our joint investigation we found 5 samples of malware using this domain which were used to target journalists and civil society in Ecuador (See Appendix D: Seeding Domains for a larger list).

Packrat's Command & Control Infrastructure

Image 4: Packrat's Command and Control infrastructure [Click image for hires]

Searching for domains related to daynews.sytes.net lead us to taskmgr.serveftp.com which on the August 11th, 2014 was at the IP address 190.210.180.181, an IP address in Argentina, used by daynews.sytes.net for a brief period when it was first registered, before being quickly moved to GoDaddy hosting. The taskmgr.serveftp.com domain also returns to 190.210.180.181 on multiple dates in October of 2014, and May of 2015. On July 23rd, 2014, taskmgr.serveftp.com was hosted at 201.52.24.126, a Brazillian IP address, which was also hosting taskmgr.servehttp.com, and taskmgr.redirectme.com. We found a total of 15 malware samples using either taskmgr.servehttp.com or taskmgr.serveftp.com as command and control domains (or both in the case of several samples). The earliest of these samples had a compile time of December 24th, 2008, providing us with the earliest date we know of that Packrat was active. While it is possible that this timestamp is faked, we have seen no evidence of this on other samples by these attackers.

Packrat's Command and Control Infrastructure

Domain	Relevant Resolution	Relevant Date of resolution
deyrep24.ddns.net	50.62.133.49	November 7th, 2014
	192.169.243.65	March 3rd, 2015
daynews.sytes.net	192.169.243.65	March 3rd, 2015
	190.20.180.181	March 1st, 2015
taskmgr.serveftp.com	190.210.180.181	August 11th, 2014
	201.52.24.126	July 23rd, 2014
	186.220.1.84	July 11th, 2014
taskmgr.servehttp.com	186.220.1.84	June 24th, 2014
	201.52.24.126	July 23rd, 2014
	186.220.1.84	July 11th, 2014
	186.220.11.67	August 15th, 2014
taskmgr.redirectme.com	201.52.24.126	July 23rd, 2014
	186.220.1.84	July 11th, 2014
ruley.no-ip.org	186.220.1.84	July 11th, 2014
	189.100.148.188	September 6th, 2012

lolinha.no-ip.org	189.100.148.188	September 6th, 2012
wjwj.no-ip.org	189.100.148.188	September 6th, 2012
conhost.servehttp.com	186.220.11.67	August 15th, 2014
dllhost.servehttp.com	186.220.11.67	August 15th, 2014
wjwjwj.no-ip.org	179.208.187.216	March 25th, 2014
	186.220.1.84	June 24th, 2014
wjwjwjwj.no-ip.org	179.208.187.216	March 25th, 2014

On July 11th 2014, all 'taskmgr' domains were hosted on 186.220.1.84, an IP address in Brazil. At the same time, this IP address was hosting ruley.no-ip.org. We managed to find a malware sample[2] using both ruley.no-ip.org and taskmgr.servehttp.com as command and control domains. On September 6th, 2012, ruley.no-ip.org was hosted at 189.100.148.188, another Brazillian IP address, along with two other domains lolinha.no-ip.org and wjwj.no-ip.org. We found two samples configured with all three of these domains as command and control servers, three samples which used both ruley.no-ip.org and wjwj.no-ip.org, two samples just using wjwj.no-ip.org, and one sample just using ruley.no-ip.org. On August 15th, 2014, taskmgr.servehttp.com was hosted on 186.220.11.67, another IP address in Brazil. On the same date, this IP hosted both conhost.servehttp.com and dllhost.servehttp.com. We found two samples configured with both conhost.servehttp.com and dllhost.servehttp.com as command and control servers.

In addition to these domains, the domains wjwjwj.no-ip.org and wjwjwjwj.no-ip.org appear to be related. On March 25th, 2014 both wjwj.no-ip.org and wjwjwj.no-ip.org point to 179.208.187.216. On June 24th, 2014, both taskmgr.servehttp.com and wjwjwj.no-ip.org pointed to 186.220.1.84. We didn't manage to find malware samples related to either wjwjwj.no-ip.org or wjwjwjwj.no-ip.org.

The command and control servers behind these domains were hosted with a variety of providers around Latin America, including: Uruguay Montevideo Administración Nacional De Telecomunicaciones, Argentina Buenos Aires Nss S.A. (IPLAN), and Claro Brazil.

Packrat has also used servers in Europe and the US, including Portlane AB in Sweden and GoDaddy in the United States.

We have notified hosting providers in order to facilitate the shutdown of Packrat's infrastructure.

Part 2: Recent Malware Attacks in Ecuador

Packrat is active in many countries, but it is in Ecuador that we were able to gather the most systematic evidence of their activities, as well as connect directly with targets and victims. We are also tracking active attacks against Ecuadorian targets at the time of writing.

Image 5: Some of Packrat's known target groups in Ecuador

Using email inbox search queries that we shared with potential targets (See: Appendix A), as well as analysis of malware databases and seeding infrastructure, we collected a diverse set of malware and phishing attacks targeting journalists, public figures, politicians, and other prominent individuals (see: 5. Packrat's Persistent Phishing Campaigns for examples).

2.1 Previous Reports of Packrat Malware in Ecuador

There are public reports, as well as social media mentions, that point to politically-linked malware attacks Ecuador by Packrat. For example, Ecuadorian freedom of expression organization Fundamedios reported that public figures, satirical news organizations, the director of Fundamedios, and others, had received suspicious messages and phishing attempts. Fundamedios later updated their reporting to note that Access Now had stated that some of these attacks shared command and control infrastructure with the malware that was reportedly used to target Nisman. There are also indications on Twitter of phishing attacks and malware. We have been able to link many of these reports to Packrat.

2.2 Common Techniques

We observed a range of social engineering techniques used to send malware to Ecuadorian targets. In the cases where we observed seeding, we found that the malware was often accompanied by political bait content, frequently relevant to Ecuador's opposition. In other cases, the seeding was personalized to the intended victim. The most common delivery mechanism was via Microsoft Word DOCX files containing malicious Java. However, in other cases, attackers used fake updates.

Common Seeding Techniques

- Emailed as attached malicious files
- As links to malware hosted on sites controlled by the attackers
- On Google Drive or Onedrive
- Popups or fake update notifications on politically themed / lookalike sites

Packrat often uses email senders and websites in its social engineering that appear similar to real persons and organizations. For example, they registered ecuadorenvivo.co, which looks like the genuine domain of the Ecuador En Vivo news website (ecuadorenvivo.com). Packrat then sent e-mails purporting to be e-mail news updates (a practice by the real Ecuador En Vivo) from the ecuadorenvivo.co domain.

Packrat also sometimes creates identical paths to real news stories, and hides them under clickable links. For example:

Typical Lookalike Domain

What the target sees:
http://ecuadorenvivo.com/videos/el-meme-que-volvio-loco-a-correa.html

HREF of the actual malicious link:
http://ecuadorenvivo.co/videos/el-meme-que-volvio-loco-a-correa.html

2.3 Three Attacks in Detail

To illustrate Packrat's approach, this section describes three recent attacks in detail. The attacks date from between Spring and Fall 2015. Targets of these attacks include Ecuadorian journalists and public figures.

2.3.1 Attack 1: Email from a fake opposition movement

Throughout April 2015, multiple targets received e-mails from the "Movimento Anti Correista" (English: "Anti Correa Movement"), a fictitious group (based on open source searches and consultation with individuals familiar with the region) that purports to be opponents of Ecuador's current president, Rafael Correa. The emails contained a Microsoft Word DOCX attachment containing Adzok malware (See: Section 3. The Evolution of Packrat's Implants), as well as text and graphics to bolster the fiction.

Example Seeding E-mail from "Movimento Anti Correista"

Image 6: Example Seeding E-mail from "Movimento Anti Correista"

Seeding text translation:

Subject: Foul Play by Rafael Correa Against the Opposition
Body:
We are sharing with you this leaked document about President Rafael Correa's dirty tricks against the opposition
(Open on a PC, this cannot be read on a phone.)Coming soon more leaks on: www[.]movimientoanticorreista.com

The e-mail seems intended for several purposes. It is obviously designed to trick the target into downloading and viewing the document, but it also seems to be an effort to establish the legitimacy of the domain, and the identity of the movement.

The Malicious Attachment

Name La jugada sucia De Correa ante la oposición.ppt
Type: Microsoft Word Document file (.docx)
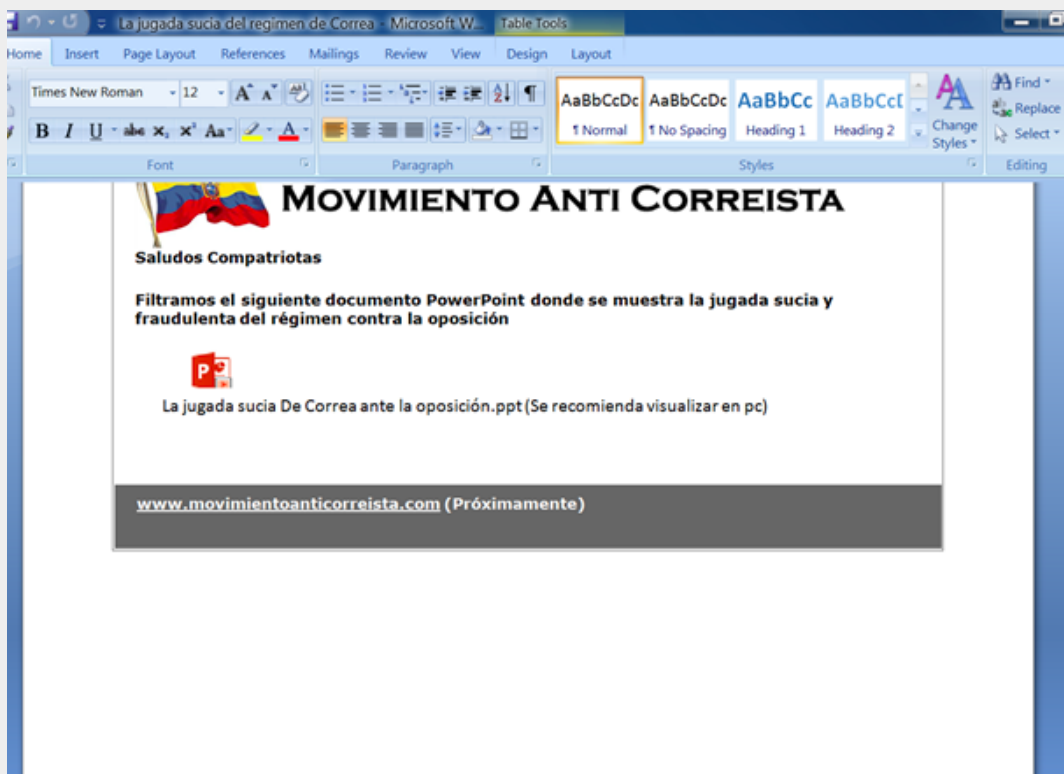MD5: ea7bcf58a4ccdecb0c64e56b9998a4ac

Embedded in this document is software called "Adzok – Invisible Remote Administrator." Analysis of the malware can be found in Section 3: The Evolution of Packrat's Implants and the configuration of this implant can be found in Appendix C: Malware Configuration.

2.3.2 Attack 2: You are being spied on!

This attack is designed to create a sense of fear and concern in the target, leading to the file being opened. The e-mail is customized for the target's name, and claims that the target is being spied on by SENAIN, Ecuador's National Intelligence Secretariat. The attachment purports to be a list of Twitter users spied on by SENAIN. Interestingly, the purported sender is "Guillermo Lasso," the defeated challenger in Ecuador's last presidential election.

From: **Guillermo Lasso** <guillermolasso@tutanota.com>
Date: 2015-09-03 ██████████████
Subject: ████████████ espiada por la SENAIN
To: ██████████████████████████

Saludos.

G.L.

NOTA: Abrir desde computador personal. No está visible para smartphones.
Saludos

LOS TUITEROS
ESPIADOS...NAIN.docx
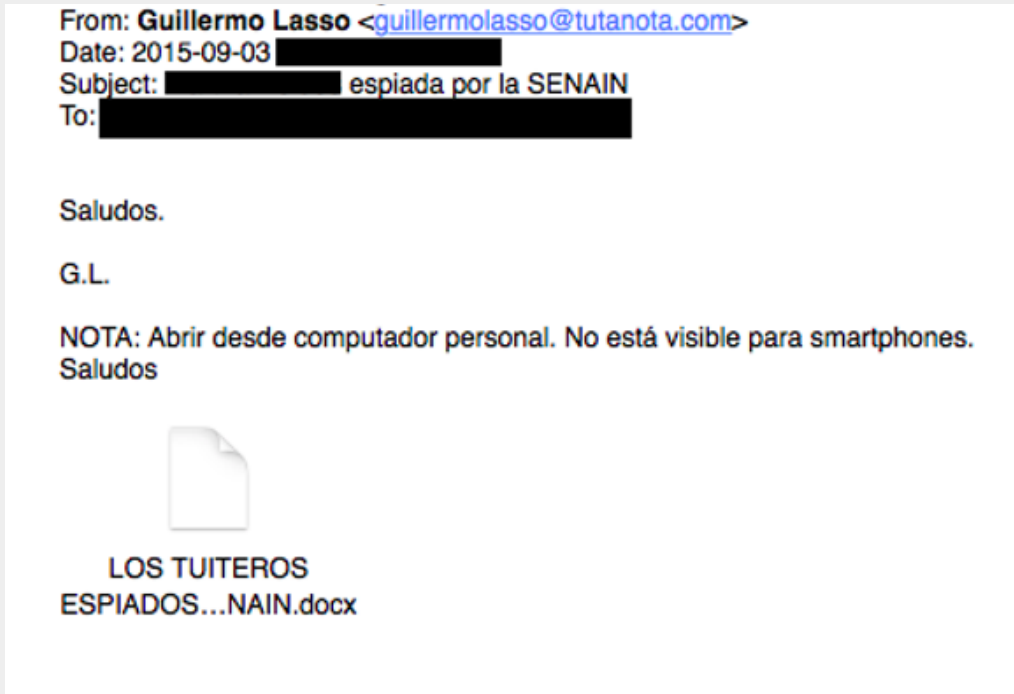
Image 8: Email with the purported sender as "Guillermo Lasso," the defeated challenger in Ecuador's last presidential election

Seeding text translation:

> Subject: [Target's Name] spied on by SENAIN
> Body:
> Greetings,G.L
> Note: Open this on your personal computer. It can't be opened by smartphones.

Like Attack 1, the malware is not delivered with an exploit, but rather requires that the victim double clicks on the file and accepts any prompts before executing it.

The document instructs the target to click:

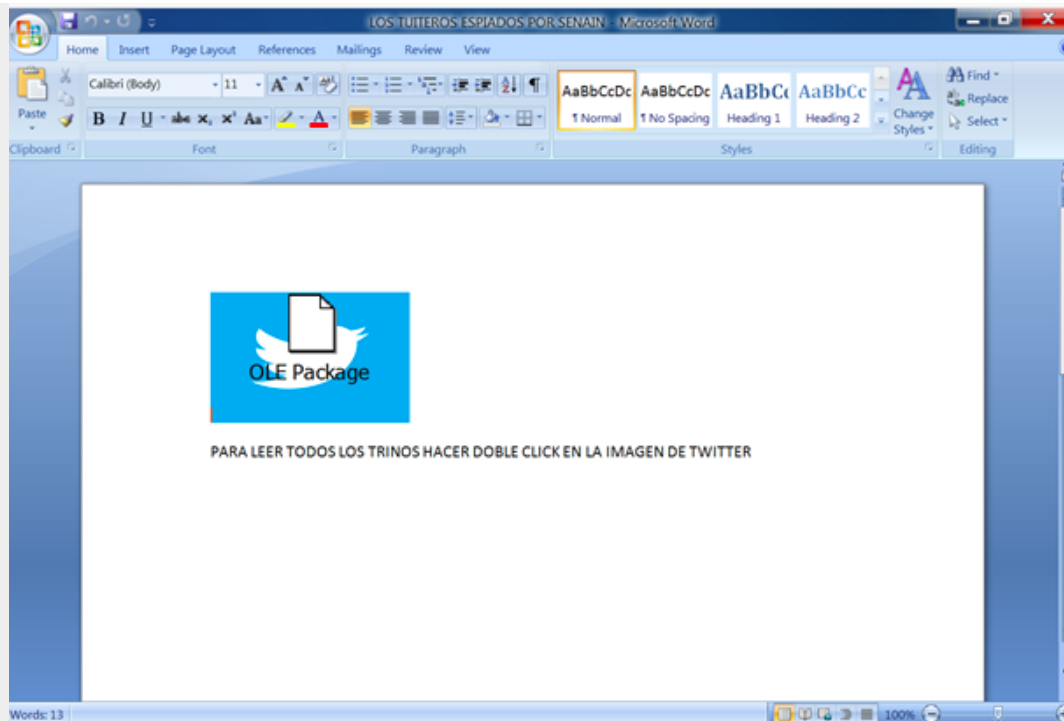*Image 9: Document instructing the target to click*

English Translation

In English: TO READ ALL THE TWEETS DOUBLE CLICK ON THE GRAPHIC OF TWITTER

When the image is double clicked, the victim is infected with malware from the AlienSpy family. Examining the configuration file of the malware reveals that the malware uses the the C2 server daynews.sytes.net, which is a domain common to several Packrat attacks. Interestingly, we found that the same document (identical MD5) was re-purposed for several other attacks.

File Name	MD5
LOS TUITEROS ESPIADOS POR SENAIN.docx	efc0009d76a2057f86c5f00030378c72
Los trinos de Rafael Correa.docx	efc0009d76a2057f86c5f00030378c72

Detailed analysis of the malware can be found in Section 3 and the configuration of this implant can be found in Appendix C.

2.3.3 Attack 3: "Exclusive Information about Correa's Lies"

This attack was served via a link to a fake political website hosting malicious content. The e-mail served to direct the victim to the site. Interestingly, the attack attempts to trick the target into believing that it originates from the legitimate investigative journalism site Focus Ecuador. Packrat appears to have acquired the .tk and .info domains of the same name, just as they had with Ecuador En Vivio.

De: Focus Ecuador <focusedtior1@gmail.com>
Fecha: [September, 2015 REDACTED]
Asunto: FOCUS ECUADOR ADELANTA EL VIDEO DEL ESCANDALO
Para: [REDACTED]

El informe sobre las mentiras de Correa: ver video exclusivo: http://focusecuador.tk/

English Translation

From: Focus Ecuador <focusedtior1@gmail.com>
Date: [September, 2015 REDACTED]
Subject: FOCUS ECUADOR THE VIDEO SCANDAL
To: [REDACTED]

Information on the lies of Correa see the exclusive video: http://focusecuador.tk/

The email also contains a tracking image from the domain mesvr.com, which is commonly used by ReadNotify, a service used to track the delivery of emails. It appears that the attackers were hoping to gain additional information about their targets, such as possibly de-anonymizing the IP addresses of targets who might be reluctant to open files.

The focusecuador.tk lookalike website contained content scraped from the legitimate site, but also showed victims a Flash update notification. When clicked, the link triggered the download of "plugin_video.jar".

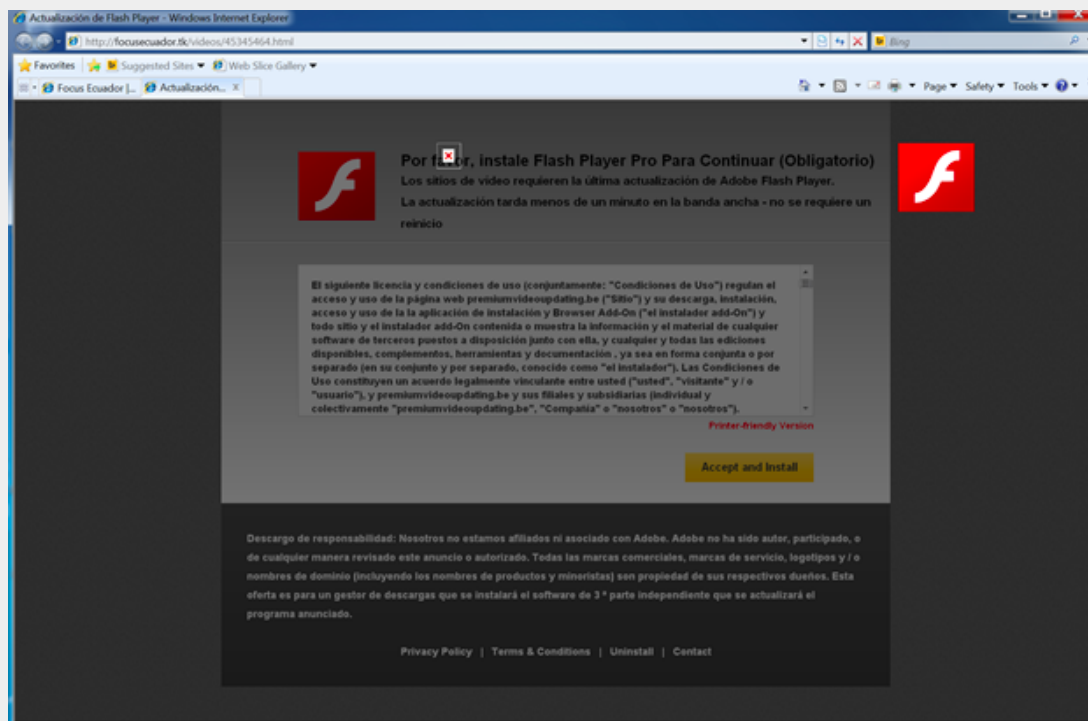The fake Flash update notification

Image 10: Fake Flash update

This is not a flash update, but a bundle of the AlienSpy / Adwind Remote Access Toolkit. When executed, this java-based malware establishes communications with Packrat's familiar Command & Control server at 46.246.89.246 (daynews.sytes.net). Analysis of the malware reveals an identical configuration to the *LOS TUITEROS ESPIADOS POR SENAIN.docx* and the *Los trinos de Rafael Correa.docx* samples.

Attack 3: Binary

Name: plugin_video.jar
Type: Java Archive (JAR)
MD5: 74613eae84347183b4ca61b912a4573f

Detailed analysis of the malware can be found in Section 3 and the configuration of this implant can be found in Appendix C.

2.4 Packrat Speaks!

During the course of our behavioral analysis of Attack 3, a Packrat operator began to communicate to one of the Citizen Lab researchers in Spanish and English on an infected machine.
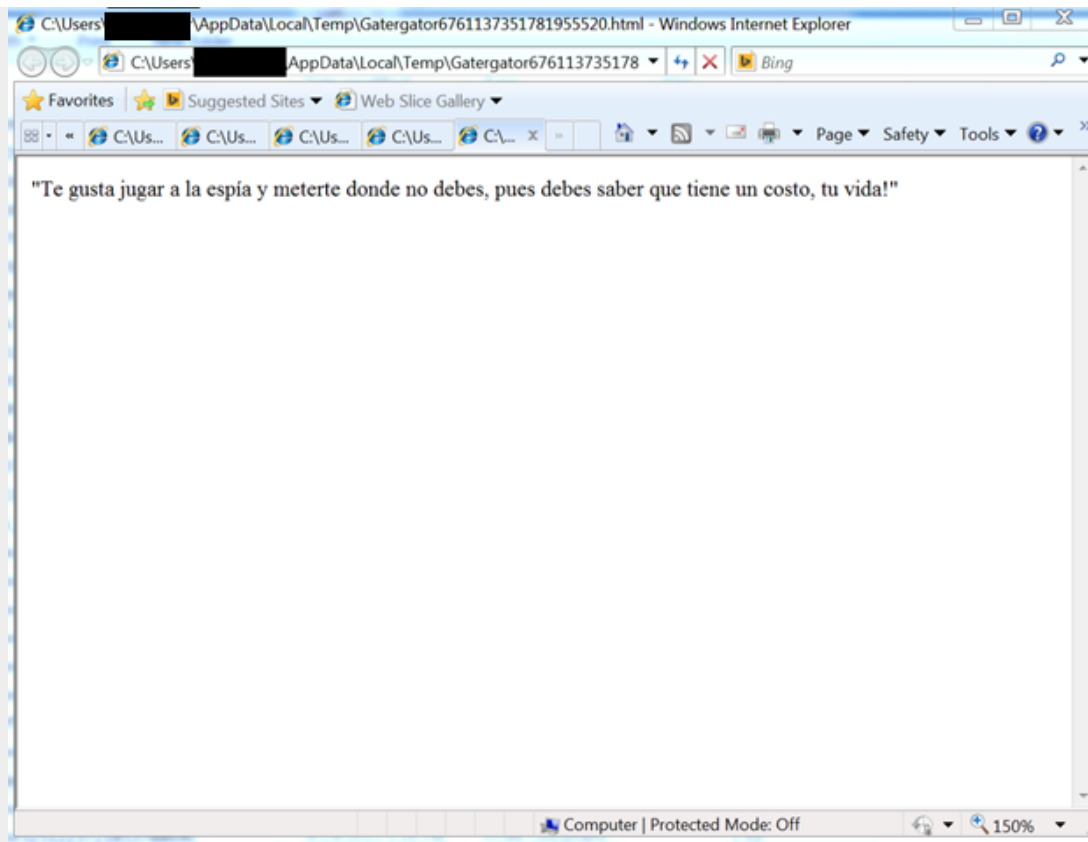
Image 11: Threats and taunts as they appeared on the Citizen Lab researcher's screen

The taunts were delivered as popups and text displayed in Internet Explorer. The tone was threatening and vulgar. This one reads "You like playing the spy where you shouldn't, you know it has a cost: your life!" Some of the messages sound stilted or non-idiomatic in the original Spanish, which might or might not be intentional, or provide clues as to the native dialect (or mother tongue) of the operator.

More Taunts: Translated English and Original Spanish

Translation	Original
Now you are in trouble ! Lammer!	Ahora si estás en líos ! Lammer !
You think you're living, we have your IP!	Te crees vivo, tenemos tu IP
You keep analyzing processes	Tu sigue analizando procesos
We are going to analyze your brain with a bullet and your family too	Vamos a analizar tu cerebro con una bala y en la de tu famila
Take care of your family	Cuida a tu familia!
We have your picture	Ya tenesmos tu fotografia
You like playing the spy where you shouldn't, you know it has a cost, your life!	Te gusta jugar a la espía y meterte donde no debes, pues debes saber que tiene un costo, tu vida!
Take your time and scan processes, we're going to get you quickly	Analiza tranquilo los procesos, que te llega rapido

Several taunts also came through in mangled English:

- "We gou You Punk!!" [sic]
- "Your are playing with fire, will get burn !"

Perhaps aiming for surprise value, the attackers also used Windows text-to-speech functionality to have the infected machine play out some of their Spanish-language taunts.

```
Dim message, sapi
message=" Analiza tranquilo los procesos"
```

```
Set sapi=CreateObject( "sapi.spvoice" )
sapi.Speak message
```

This occurred a second time in October, when the attackers again taunted a researcher, followed by using the implant to issue a remote shutdown command to the infected device.

It is unusual, though not unheard of, for attack operators to engage with researchers. This kind of engagement could be considered a serious breach of operational security. Packrat took exception to these unwritten rules. It may be that Packrat has experienced other cases of individuals touching their infrastructure, or attempting to analyze their files, especially after some of their infrastructure was exposed. Since Packrat prefers to leave the infrastructure online, they may be trying to discourage unwelcome attention.

3. The Evolution of Packrat's Implants

Over the past seven years Packrat has used several different types of malware, much of it off-the-shelf RATs, such as Cybergate, Xtreme, AlienSpy, and Adzok. While these malware families are known to researchers, Packrat typically obfuscates their malware using a range of tools, including: an unknown VB6 crypter, AutoIt3Wrapper, UPX, PECompact, PEtite, and Allatori Obfuscator. This layer of obfuscation means that Packrat's attacks frequently escaped detection by antivirus when the attacks were deployed. This section describes these tools, roughly grouped into distinct time periods.
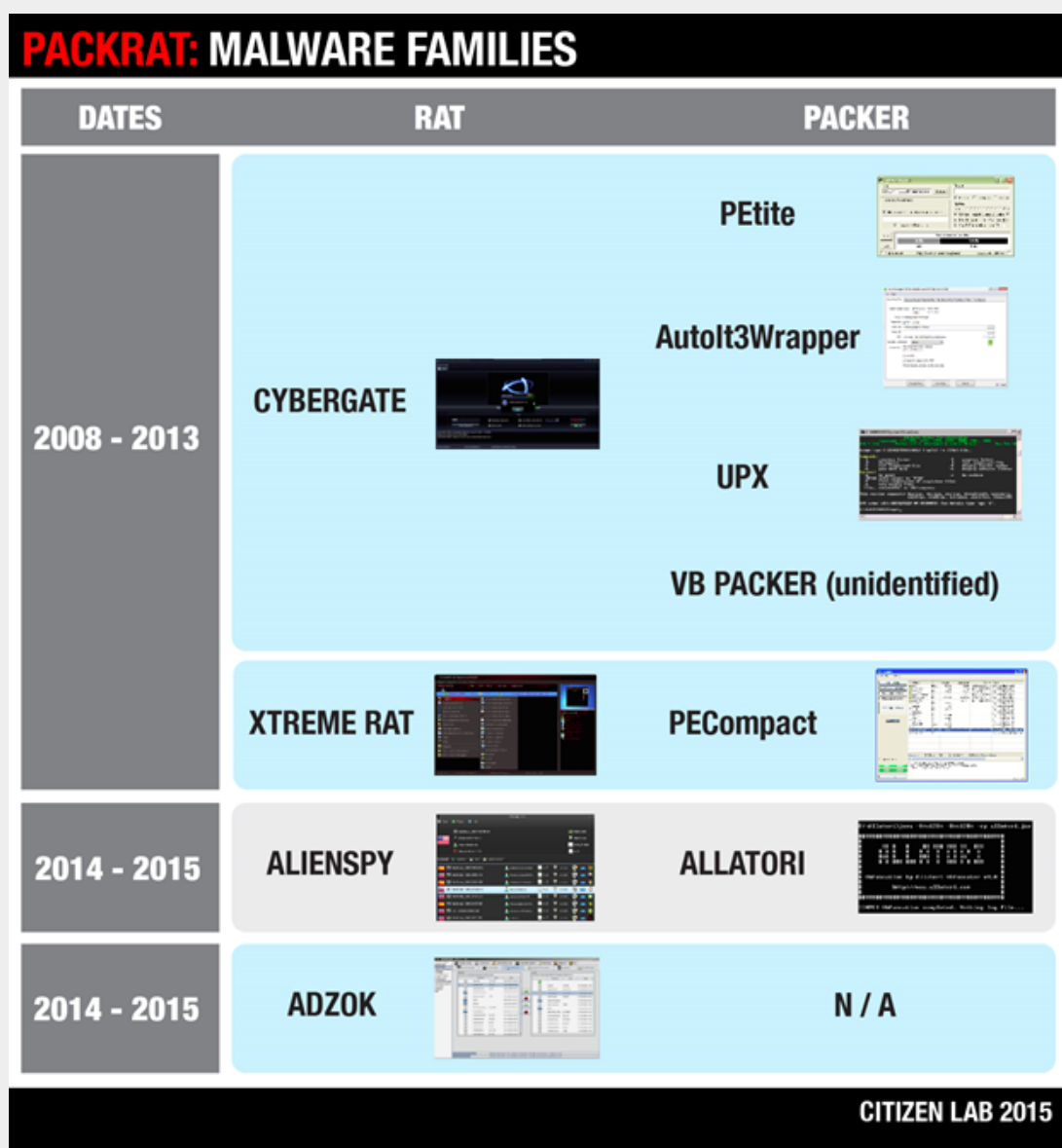
Image 12: Packrat malware families

3.1. 2008-2014: Packed RATS, mostly CyberGate

Between 2008 and 2014, Packrat made extensive use of off-the-shelf RATs encapsulated in AutoIt3Wrapper, a runtime packer. This packer is written in AutoIt, a compilable scripting language for automating tasks in Windows. The use of an initial obfuscation layer seems to have been enough to thwart or at least misguide detection, as well as leverage some basic anti-debugging techniques.

The majority of implants that are then dropped and executed appear to be CyberGate RAT. In 2013 and 2014, Packrat seems to have adopted XtremeRAT as well. Cybergate and Xtreme are both written in Delphi and share code with each other and other Delphi based RATs, SpyNet and Cerberus.

Many of these attacks included embedded decoy Office documents that are opened at execution of the implant, likely in the context of a targeted attack. Among the documents we found are résumés of purported Brazilian citizens, as well as purported payment receipts of the Association of Lawyers of Sao Paulo, Brazil.
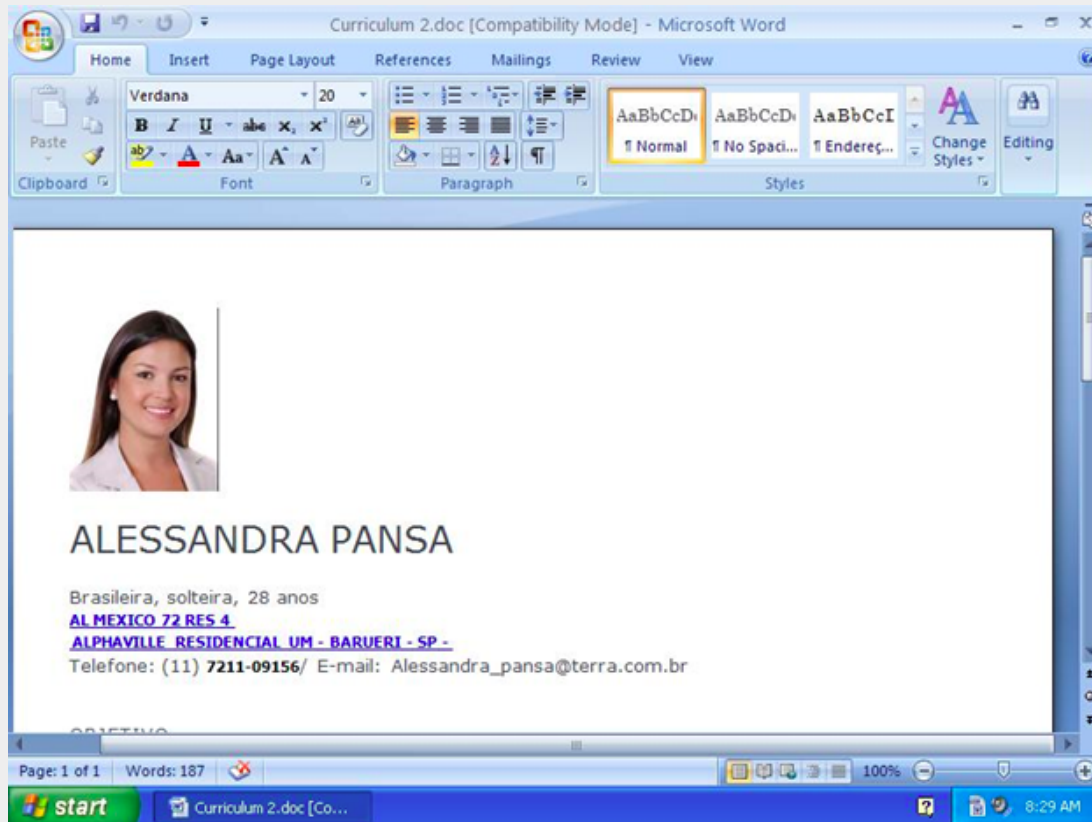

Image 13: A résumé

These attacks suggest that Packrat had Portuguese speaking targets during this period. Based on the specifics of the bait documents, it seems likely that they were Brazilian.
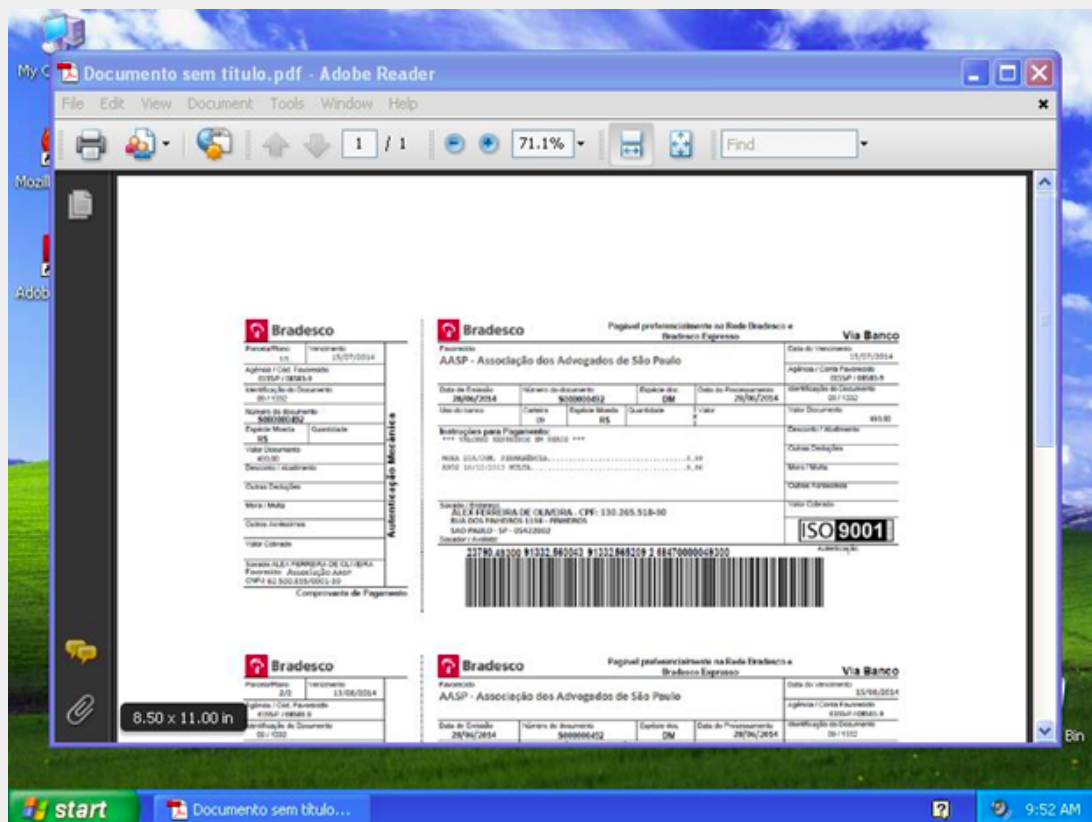
Image 14: Payment receipt

The majority of the implants we found were configured to beacon back to a Command & Control, taskmgr.servehttp.com, although a few others include ruley.no-ip.org, lolinha.no-ip.org, and taskmgr.serveftp.com (See Appendix B for a complete list).

3.1.1 Analysis of CyberGate RAT

The CyberGate RAT samples we analyzed were, as mentioned above, typically wrapped in a layer of AutoIt. Code and strings found in the binary indicate that it is based on the Spy-Net RAT version 2.6. This RAT was developed by a Brazilian hacker using the handle spynetcoder and is outlined on the Spy-Net RAT ‘official’ website.

CyberGate’s Infection Routine
After unpacking from the applied runtime packer, CyberGate runs its second stage, which is likeley the infection routine. This injects the third stage, a DLL, into a running process. Once implanted, CyberGate then deploys a range of techniques for persistence and monitoring.

The third stage module picks from three execution paths (based on mutexes, which can also be set by a prior infection):

- Password gathering (mutex: “_x_X_PASSWORDLIST_X_x_”)
- Block mouse and keyboard input to any other application (mutex: “_x_X_BLOCKMOUSE_X_x_”)
- Infection routine

CyberGate Anti Analysis
The infection routine comes with a set of anti-analysis features packaged in a single function. CyberGate searches for a range of virtual and sandbox environments.[3] It also checks for user space debuggers through the IsDebuggerPresent API, and for SoftICE and Syser through their respective pipes. The malware performs breakpoint detection on the function entries of the listed anti-analysis features by checking whether the first byte of each function equals ‘CC’, the bytecode indicating a breakpoint.

```
xor     eax, eax
push    offset ExcHandler
push    dword ptr fs:[eax]
mov     fs:[eax], esp
mov     eax, 'VMXh'
mov     ebx, 3C6CF712h
mov     ecx, 0Ah
mov     dx, 'VX'
in      eax, dx
mov     eax, 1
```

Image 15: CyberGate Anti Analysis

CyberGate Process Injection
The infection routine fetches the encrypted implant from the resource section, and upon decryption attempts to inject its implant into the Windows system shell process (explorer.exe). If this fails, CyberGate launches an explorer.exe process on its own, injects its implant into it, and then completes the setup. Additionally, another instance of the CyberGate implant is injected into a default browser process, which runs invisibly.

The infection routine drops a copy of itself into different directories, depending on the Windows version: /System, /Windows, or /Program Files. The implant’s name varies: taskhost.exe, regedit.exe, or taskmgr.exe are all common. The infection routine also writes a copy of the encrypted implant into the %TEMP% directory and names it XX–XX–XX.txt.

To achieve persistence, the second stage writes registry keys so that CyberGate is run at startup:

```
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components\%GUID%\StubPath:
  “C:\WINDOWS\System32\regedit.exe”
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run\Policies:
  “C:\WINDOWS\System32\regedit.exe”
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\msconfig:  “C:\WINDOWS\System32\regedit.exe”
```

Password Collection
If tasked with password collection, the second stage binary grabs passwords from a range of locations, including: the No-ip Dynamic Update Client (DUC), MSN messenger, Firefox, and Internet Explorer. The credentials are collected from the Windows Registry, browser profiles, the RAS dial up settings, Local Security Authority (LSA) settings, MS ProtectedStorage, MS IntelliForms, and the credential store.

CyberGate’s Functionality
The CyberGate implant runs two instances. The first runs in the default browser process, and acts as the monitoring

component. Meanwhile, the explorer.exe instance serves as 'watchdog,' ensuring persistence and making sure the infector binary on disk doesn't disappear.

```
push    [ebp+var_10]
push    offset asc_140127EC ; "\\"
push    offset aSpyNet ; "Spy-Net "
push    offset a2_6     ; "2.6"
push    offset a_txt    ; ".txt"
lea     eax, [ebp+var_C]
mov     edx, 5
call    strConcat
mov     eax, [ebp+var_C]
call    findFile
test    al, al
```

Image 16: Searching for indicators of an existing Spy-Net installation

The CyberGate implant comes with the same credential stealing capabilities as the infector, and is extended by routines to spy on Chrome and STEAM credentials as well. Also inherited from the infector, the implant owns the same anti-analysis routine protecting it from sandboxes and debuggers.

Beyond the capabilities seen in the infector, CyberGate has a range of features that provide an attacker with a full spectrum of monitoring and remote control functionality.

CyberGate capabilities include:

- Collecting detailed information about the infected system
- Activation and control of the webcam and microphone
- Screenshot capture
- Blocking user input (e.g. keyboard and mouse)
- Control over processes, windows, applications, devices, drive, ports, TCP & UDP connections, the clipboard, registry keys and values etc.
- Control over the filesystem
- Download and execution of further binaries
- Exfiltration via FTP
- Collection of information on installed security products

Interestingly, CyberGate gathers information on installed security products through the Windows Management Instrumentation (WMI) by launching cscript.exe on a hardcoded .vbs-script. The script requests name and version number of installed antivirus and firewall solutions and dumps the data to a file:

```
Set objSecurityCenter = GetObject("winmgmts:.rootSecurityCenter")
Set colFirewall = objSecurityCenter.ExecQuery("Select * From FirewallProduct",,48)
Set colAntiVirus = objSecurityCenter.ExecQuery("Select * From AntiVirusProduct",,48)
Set objFileSystem = CreateObject("Scripting.fileSystemObject")
Set objFile = objFileSystem.CreateTextFile("%FILEPATH%", True)
Enter = Chr(13) + Chr(10)
CountFW = 0
CountAV = 0For Each objFirewall In colFirewall
CountFW = CountFW + 1
Info = Info & "F" & CountFw & ")" & objFirewall.displayName & " v" & objFirewall.versionNumber & Enter
NextFor Each objAntiVirus In colAntiVirus
CountAV = CountAV + 1
Info = Info & "A" & CountAV & ")" & objAntiVirus.displayName & " v" & objAntiVirus.versionNumber & EnterobjFile.WriteLine(Info)
objFile.Close
```

Collected data is stored in dump files on disk and exfiltrated to the remote server component by HTTP or FTP.

3.1.2 Analysis of XTremeRAT

XTremeRAT is commercial off-the-shelf malware, often available cracked, and used to monitor victim machines. While used by apolitical hackers, XTremeRAT has been extensively used by government-linked malware groups to target the opposition during the ongoing Syrian Civil War, as well as by other politically-motivated groups in the Middle East and

North Africa. It has also been extensively analyzed, and we encourage interested readers to review some of these analyses.

While often packed, XTreme RAT itself has limited stealth and persistence functionality. Its monitoring capabilities are also straightforward. The versions we analyze here have no code obfuscation. XTreme Rat is implemented as client/server architecture, where the infected machine acts as server, while the C&C component is the client.

This version of Xtreme Rat's capabilities include:

- Logging keystrokes
- Logging the name of the foreground desktop application
- Sniffing the clipboard for passwords
- Downloading and executing binaries via HTTP, presumably to install second stage malware
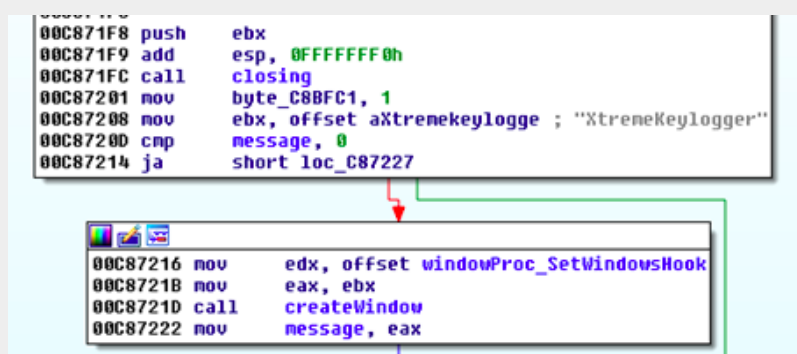

Image 17: Installation of the XTreme RAT keylogger module

Xtreme RAT operation and keylogging functionality

The Xtreme RAT implant sniffs the clipboard contents via the keylogger window, using a clipboard viewer that it also installs. The viewer receives the window message WM_DRAWCLIPBOARD every time the clipboard changes, and provides access to Clipboard contents. Clipboard and keylogger data is dumped to a .dat-file that, along with the configuration file (.cfg), is located in the [···]\Application Data\Microsoft\Windows folder for the current user. Both filenames are dictated by XTreme RAT's configuration.

XTreme RAT data files

C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\RJokLSZBj.cfg
C:\Documents and Settings\Administrator\Application Data\Microsoft\Windows\RJokLSZBj.dat

The dump file is exfiltrated via push to FTP. XTreme RAT comes with preconfigured FTP server credential placeholders (ftpuser/ftppass) to log on to ftp.ftpserver.com, which are then switched for updated values received from the C&C at runtime.

The XTreme RAT implant also creates a mutex named following the same naming scheme as configuration and dump file (e.g. "RJokLSZBjPERSIST"). The RAT's configuration is fetched from the .rsrc-section and encrypted using RC4, with the key "CONFIG". The same algorithm and key combination has been seen in use before in other variants of XTreme RAT.

This variant of XTreme RAT uses explorer.exe as a container for remote threads to carry out specific functions. Thread injection can happen on at least three occasions.

Possible injections of explorer.exe by XTreme RAT:

- A 'watchdog' thread to restore persistence keys, and to locate and run the infector binary. To increase stealth, the dropping module changes the timestamp of the dropped infector.
- A thread for deleting of XTreme RAT's files on disk
- The entire keylogging code and FTP push functionality

3.2: 2014- 2015 AlienSpy Dominates

Over the past two years, Packrat has been using an evolving family of off-the-shelf malware known as AlienSpy. The software began as the free RAT "Frutas," and was identified in 2013 during a campaign in Mexico. This was subsequently adapted for commercial sale as the "Premium RAT" Adwind. Adwind could be purchased for $75 for a

single license, and up to $250 for multiple licenses. Then, by 2013, AdWind was renamed UNRECOM (UNiversal REmote COntrol Multi-platform), and was detected in targeted attacks in the Middle East.

The software was most recently branded "AlienSpy," and was again found by security researchers in targeted spying operations. At the time of this report, the latest re-packaging of this RAT is known as JSocket. For the purposes of this report, we'll refer to all variants of this spyware as "AlienSpy." AlienSpy is a relatively full-featured RAT with a range of features, such as recording the victim's keystrokes, audio eavesdropping via a device's built-in microphone, remote viewing of the desktop, and the ability to turn on a victim's webcam "without user notification." Alienspy has been extensively analyzed by malware researchers, including reports by ProofPoint and Fidelis.

3.2.1 Packrat's Alienspy Deployment

From 2014 to early 2015, Packrat's preferred technique was to send AlienSpy implants as attachments in phishing emails with the extension '.pdf.jar.' The default setting in Windows is to hide file extensions, thus making it appear to be a ".pdf" file. With some minor differences, all the samples from this time period are built in a similar manner. There's an outer .jar (Java archive) 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" (not an icon file, but a .zip archive), and looks for a filename containing ".jar".

Contents of Favicon.ico

```
0doc.jar
1Estrictamente Secreto y Confidencial.pdf
```

Once it finds the right file (in this case 0doc.jar), 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"

```
META-INF/MANIFEST.MF
MANIFEST.MF
ID
plugins/Server.class
Main.class
Estrictamente Secreto y Confidencial.pdf
```

"Main.class" is obfuscated using Allatori, a Russian-origin JVM obfuscator used by AlienSpy.

This reads part of an RC4 key from the file "ID." To this it appends a constant string, then uses the full RC4 key to decrypt the contents of MANIFEST.MF, which yields the actual Adwind implant JAR file. Others have written about the operation and deobfuscation of Allatori, including how to deobfuscate it, here, here, and here.

AlienSpy in MS Office Documents

In 2015, Packrat started sending AlienSpy implants embedded in .docx files. The method used to obfuscate these files is more complex, but ultimately similar to previous techniques. Uncompressing an infected MS Word document reveals a file named "oleObject1.bin" under the directories word/embeddings. Opening this file, which is a jar, reveals:

```
a
abcdefghijka.class
abcdefghijkf.class
abcdefghijkj.class
abcdefghijks.class
abcdefghijku.class
abcdefghijkz.class
a.txt
b.txt
c.dat
kjmhs
Main.class
META-INF
```

Similar to the obfuscation described above in Packrat's earlier uses of AlienSpy, half the decryption key is in a.txt. The other half is a string which is decrypted iteratively by the abcdefghijk[a,f,j,s,u,z].class files with the method and class names from the caller.

Persistence is achieved by adding the following registry value:

```
"reg.exe"  (Access type: "SETVAL" , Path:
"\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN" , Key: "JAVASE" , Value:
"" C:\Users\PSPUBWS\Cas436FlashJava\RoUndCuBe\bin\javaw.exe"  -jar
"C:\Users\PSPUBWS\Cas436FlashJava\Cas436FlashJava\Cas934FlashJava.
```

3.2.2 Adzok makes an appearance

Between 2014-2015, Packrat also used Adzok – Invisible Remote Administrator. Similar to AlienSpy in functionality, the java-based Adzok is apparently from Bolivia. The premium version costs $990, but it appears that Packrat is using the "free" version. This version of Adzok does not use obfuscation, which makes it possible to simply uncompress the jar files within the docx and read the clear-text configuration file. Given the obfuscated nature of the other RATs that Packrat has used, their use of Adzok is surprising. It is possible that they were having stability, compatibility, or detection problems with other RATs and that Adzok served a specific requirement.

4. Packrat's Persistent Phishing Campaigns

Packrat is active in phishing, often against the same groups and individuals whom they target with malware. For example, when examining one target of malware attacks, we found this individual had been targeted by dozens of phishing attempts by Packrat during the same period. The same domains and fake identities that Packrat uses to seed malware are also used to serve phishing, although Packrat also maintains dedicated phishing sites and servers. While phishing e-mails appeared to be regularly sent, we also observed particular cases of the phishing apparently sent to targets in response to contacts they made during our investigation.

We have been able to achieve the most systematic visibility of Packrat's campaign against Ecuadorian targets, but have found evidence of targeting in neighboring countries including Venezuela. Packrat uses both e-mails and social media messages, as well as SMSes to send phishing messages.

This section describes these phishing campaigns, and describes both Politically-Themed and Non-Politically Themed phishing attacks.

Category	Example Domain	Note
Politics & News	lavozamericana.info	Fake news website
Governmental – Ecuador	asambleanacional-gob-ec.cu9.co	Lookalike to the Ecuadorian National Assembly's e-mail login
Political Movement – Ecuador	movimientoanticorreista.com	Fake political movement
Free E-mail	mgoogle.us	Fake Google login

4.1 Non-Politically Themed Phishing Content

One of the most common phishing techniques is lookalike communications from popular webmail and social media sites containing requests for password verification, notifications of unauthorized logins, and so on. Packrat uses a wide range of templates for the major email providers, including Gmail, Yahoo and Hotmail. A majority of the e-mails are in Spanish. The messages are typically personalized to the targets, including both their names and e-mail addresses.

Image 18: Example phishing email

Translated Message

From: Gmail Team no.response.delivery.es@gmail.com
Subject: [Victim Name], you have a pending warning !
To: [victim email]

[Victim email],

[Victim Name]for security reasons we request that you verify your account below.

To ensure proper use of your account, we request that you verify it.

Click here to verify your account.

Depending on the attack, the phishing either contains a direct link to the phishing URL, or uses a shortener.

4.1.1 Most Recent Non-Political Phishing

Recently, the attackers appear to have slightly varied their technique. We have observed them making extensive use of tinyurl as a shortener, as well as moving their phishing pages to the free host cu9.co. The attackers may have concluded that using a free provider reduced costs and increased flexibility.

Example recent phishing URL and shortener:

tinyurl.com/nww83ov Yields: main-latam-soporte-widget-local.cu9[dot]co

4.1.2 Example Non-Political Phishing SMSes

A number of Packrat's targets also received phishing SMSes. The SMSes often use similar language to the phishing e-mails, and in some cases use the same shortened URL. In other cases, the attackers push harder, warning the targeted user that their accounts will be terminated if they fail to follow the link. In at least one case we observed that the messages contained improperly formatted e-mail addresses.
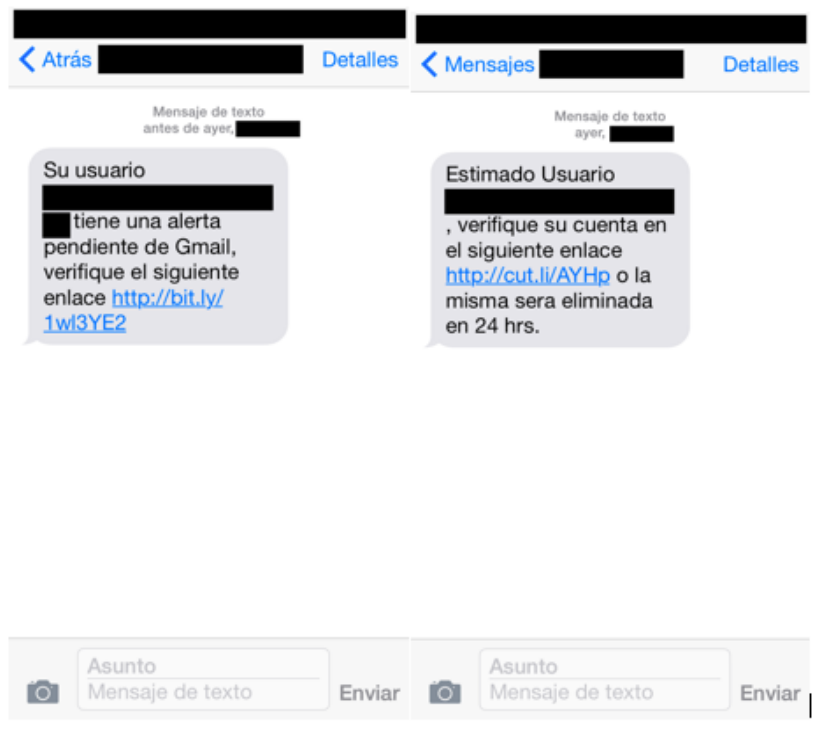
Image 19: Example of non political phishing

4.2 Politically Themed Phishing

We observed a wide range of e-mails and messages that contained content with political overtones. Packrat takes two basic approaches in the attacks we have examined. First approach: create fake political and media organizations. Second approach: impersonate well-known groups and high-profile individuals. Attacks typically took the form of messages and e-mails containing information either in 'solidarity,' upsetting information, or other relevant news. A majority of what we observed seemed to be crafted to appeal to opposition elements.

While much of the phishing seems to mimic common free webmail and social media sites, in specific cases, Packrat mimicked e-mail services of high-profile targets, like the Ecuadorian National Assembly.

4.2.1 Targeting Ecuadorian Parliamentarians

A group we believe to be Packrat has operated a phishing campaign that mimics the Ecuadorian national assembly's webmail portal. This malicious site prompts the target(s) to enter their email credentials, which are captured via formmail, a technique seen repeatedly in the phishing pages we identified (see below).

> asambleanacional-gob-ec.cu9.co

The legitimate domain is:

http://mail.asambleanacional.gob.ec/

4.2.2 A Typical Credential Harvesting Page

Whatever the bait, the links on the messages typically lead victims (often via a shortener) to a lookalike domain for a free email provider. During the summer of 2015, a frequently observed domain was a lookalike for Google, although there have been many others:

> mgoogle.us

While the attacks were active, mgoogle.us hosted a Spanish-language lookalike Google login.
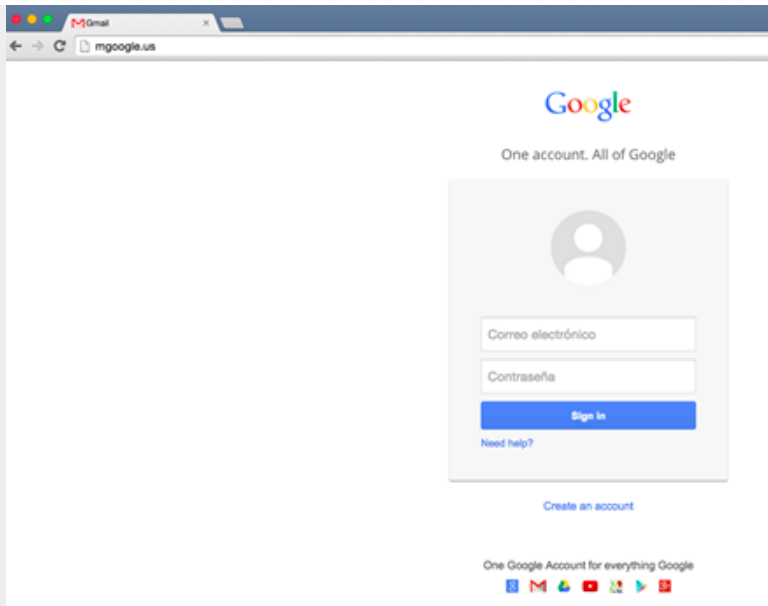
Image 20: mgoogle.us hosted a Spanish-language lookalike Google login

Once a victim's credentials are entered, they are shown a Spanish language note "confirming" that their gmail has been "unblocked" and thanking the victim for "choosing us."

Image 21: A Spanish language note "confirming" that their Gmail
has been "unblocked"

In other cases, Packrat sends "confirmation" emails to the original victim, congratulating them on "successfully" verifying their account after credentials are entered. In specific cases, we found that this e-mail arrived several hours before phished accounts were accessed.

While the phishing has used different tools to harvest credentials, we find that Packrat makes repeated use of the legitimate online website form service formmail.com to receive phished credentials. Formmail is a legitimate HTML-based form processor that receives the contents of data entered into forms, then sends them to an e-mail address.

4.3 A Sample of Phishing & Malware Seeding Sites

The attackers control a range of domains that they use to serve both phishing and malware. This section outlines elements of this infrastructure. A more complete list is in Appendix D, but we describe certain domains of interest here. The phishing page mgoogle.us, for example, has resolved to a range of IPs, including:

IP	First Seen	Last Seen	WHOIS
198.12.150.249	5/19/2015 6:16:00	9/4/2015 9:51:00	Godaddy
50.63.202.57	9/4/2015 12:52:00	10/8/2015 21:44:00	Godaddy

Of these IPs, the first (198.12.150.249) is particularly interesting. We find that the same IP was used to host a range of other

suspect domains with similar themes. For a full list of associated domains, see Appendix D. While some of these domains are lookalikes for logins, or update pages (e.g. sopporte-gmail.com or login-office365.com) others seem to have a more political angle.

WHOIS

Name Pedro Luis
Organization Reterg is
Address teredotr
City berlin
State berlin
Country DE Germany
Phone +49.454545445
Private no

The registrant of the site is enripintos123@outlook.es, whom we find listed as the registrant for a range of other domains. All but two are lookalike to the login pages of major online services, or suggestive of updates to services like Java and Android (see Appendix D). The two exceptions are lavozamericana.info and pancaliente.info (see Section 6. Possible Deception Operations). Both of those domains were registered within the timeframe of other registrations of lookalike or confirmed phishing domains.

4.3.1 Lookalike Fake News Sites

The website Ecuador En Vivio (ecuadorenvivo.com) is a legitimate news site, however the attackers control the lookalike ecuadorenvivo.co domain. Packrat has used this fake domain to send emails to targets, either containing attachment-based malware, or links to the site which has also been used to seed malware via a plugin error.

A Twitter user spotted the fake plugin notification in May 2015 and alerted their followers, and included a screenshot purporting to show one of the fake plugin alerts.
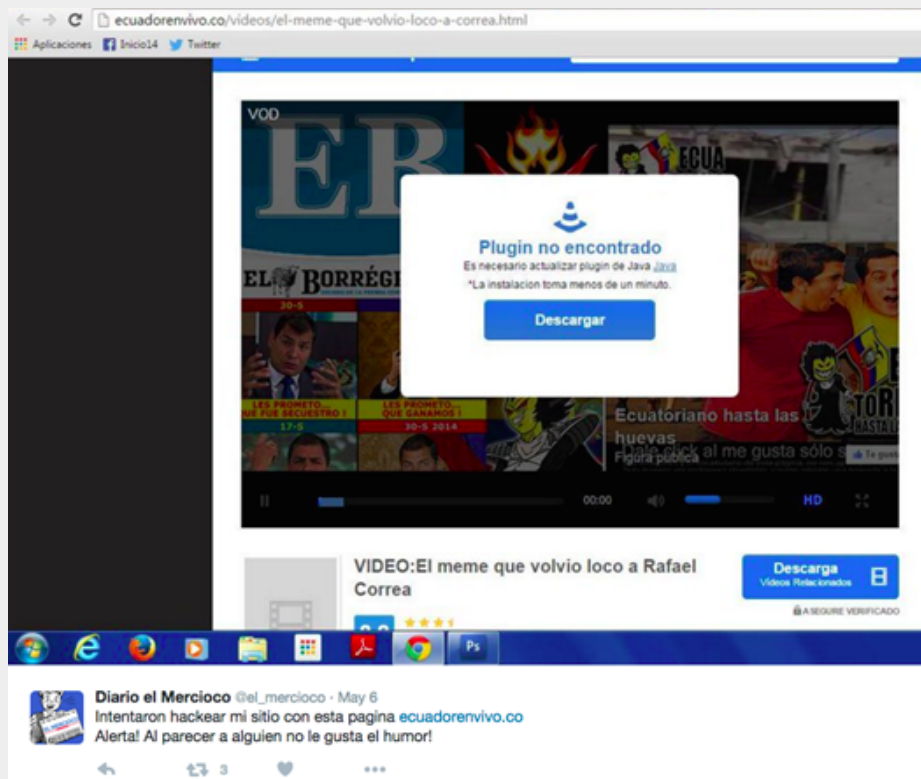
Image 22: Fake plugin notification

Similarly, Focus Ecuador (focusecuador.net) is a genuine news website, however the domain focusecuador.tk, is controlled by the attackers, and has been observed seeding malware using a fake popup. Examination of the IP hosting focusecuador.tk (193.105.134.27) reveals a long list of obvious lookalike domains (See Appendix D).

4.3.2 A Fake News Organization: The American Voice?

A second interesting domain is lavozamericana.info, which is no longer active. However we were also able to find a Twitter identity and string of tweets suggesting that there may have been an effort to establish the legitimacy of the site.

https://twitter.com/voz_americana

Interestingly, the fake identity appears to have had at least some success, as some of the followers of the account appear to be genuine. While the site is no longer active, Google's cache indicates that a phishing page was hosted on the site.
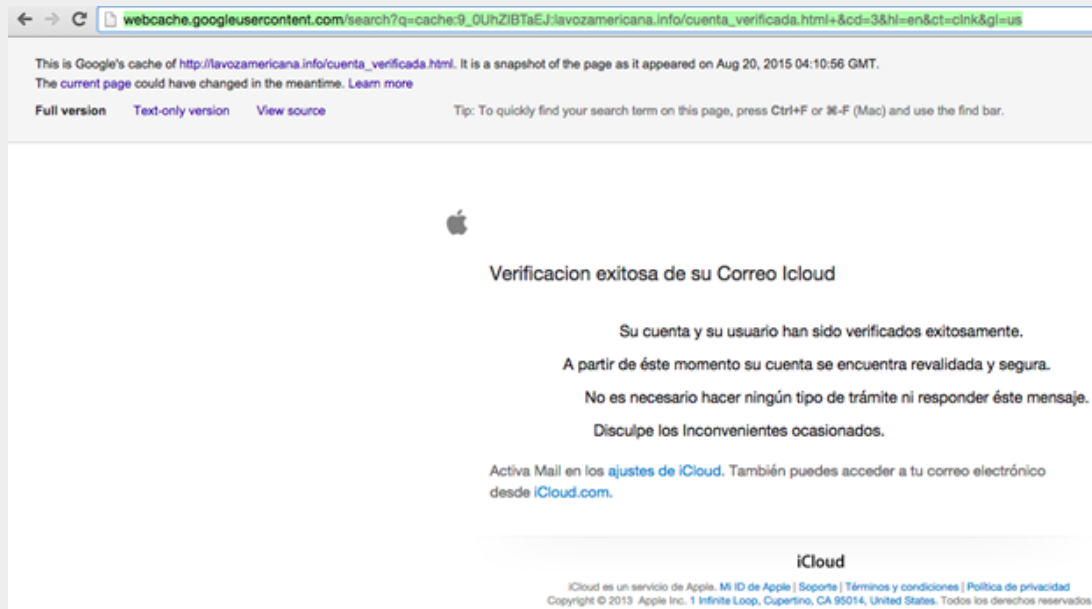

Image 23: Google's cache indicates that a phishing page was hosted on the site

While we have received reports that individuals targeted by Packrat lost access to their iCloud accounts during the timeframe of this attack, we have been unable to verify conclusively whether Packrat was responsible.

4.3.3 A Fake Opposition Movement

A number of the targets we identified had received e-mails and messages purporting to come from movimientoanticorreista.com, including the example **Attack 1** above. The same domain was also mentioned in a recent report by an Ecuadorian NGO of malware attacks against journalists in Ecuador. We found malware seeding messages associated with this domain, typically sent by movimiento.anti.correista@gmail.com.

Another Anti Correa Movement E-mail

De: Movimiento Anti Correista <movimiento.anti.correista@gmail.com>
Fecha: [REDACTED: April 2015]
Asunto: DOCUMENTOS FILTRADOS DEL GOBIERNO CORREISTA – EL SILLON MILLONARIO Y LAS ACTIVIDADES CORRUPTAS
Para: [REDACTED]SALUDOS ESTIMADO,Compartimos con usted nuestro nuevo sitio web en el cual estaremos publicando información del corrupto gobierno de Rafael Correa.DESCARGUE LOS DOCUMENTOS DE:www.movimientoanticorreista.com

Translated E-mail

From: Anti Correa Movement <movimiento.anti.correista@gmail.com>
Subject: LEAKED DOCUMENTS FROM THE CORREISTA GOVERNMENT – THE ARMCHAIR MILLIONAIRE AND CORRUPT ACTIVITIES
To: [REDACTED]ESTEEMED GREETINGS,We are sharing with you our new website where we will publish information about the corrupt government of Rafael Correa.DOWNLOAD DOCUMENTS:www.movimientoanticorreista.com

4.4 A Window Into Campaign Scope

Several moves by Packrat gave us access to some more systematic information about the scope of their attacks. During

much of 2015, we observed that Packrat regularly used the same bit.ly link in a range of attacks.

http://bit.ly/1wl3YE2

This link was created Oct. 31, 2014 by an anonymous sharer. Examining statistics for the bit.ly link, we were able to see a superficial overview of the volume, timeframe, and basic geographic distribution of clicks.

Image 25: An overview of the volume, timeframe, and basic geographic distribution of clicks

The distribution of clicks is particularly interesting, and suggests that a majority of the hits were located in Ecuador, with others in Argentina, Germany, the United States, Spain, Uruguay, and Venezuela. The absence of Brazil is not necessarily surprising, as it is likely that the attackers, if they continue to phish in Brazil, may be using separate, Portuguese language sites. This provides an indirect window into the location of Packrat's targets.

A majority of clicks (322) came from direct link clicks, rather than link shares elsewhere. While this particular bitly link was not extensively clicked on social media sites, Packrat does use social media for some seeding.

4.5 Note: Lots of Phishing, Not All of it Linkable

The investigation yielded a high volume of Spanish-language phishing attacks against the same individuals that Packrat targeted, however for a number of reasons we were unable to link much of the phishing activity to Packrat. One of the most notable and high volume campaigns that we identified used the domain gmail.com.msg07.xyz and masqueraded as a range of account notifications from popular providers including Gmail. Typically these messages displayed as originating from e-mail addresses like "no-responder@supportgmai1.com."   In some cases, individuals received these messages almost weekly over long periods of time.

5. Possible Deception Operations

Not all of the domains associated with this group appear to have been built to spread malware, or to trick victims into entering their passwords. Several domains are extensively built out, and currently maintained, which appear to be designed to convey the impression of active, news media sites. Some of these sites contain 'original' news stories and 'leaks' about political figures. At least two of these sites seem Venezuela-specific, while a third is Ecuador-oriented.

What makes these three fake organizations exceptionally interesting is that we have found no evidence that they are used to seed malware or conduct phishing, either directly, or as pretexts for messages. While it may be that we simply

lack visibility on the targeting, it may be that the pages and identities serve another function. They may be attempts to seed false information, or might serve as watering holes to attract individuals that Packrat or its sponsors wish to monitor. They may also be coupled with other operations on which we have no visibility.

5.1 Anti-Chavez: The Very Strange Case of pancaliente.info

Update: immediately prior to the publication of this report the Pancaliente.info site went offline. The site is still viewable in Google's cache. The second domain of this type (chavistas24.com) remains online.

One of the most interesting domains also hosted on 198.12.150.249 is pancaliente.info. At first glance this is a Venezuela-focused news and information site. Unlike all of the other sites hosted on this IP that we could verify, this site appeared to have a large volume of original content that was presented in a news format.

Nevertheless, the site has many links to the other domains. While the domain registration is currently masked, the registration e-mail is shared with other phishing sites.

pancaliente.info	GoDaddy.com,LLC(R171-LRMS)	enripintos123@outlook.es	ns1.hostinger.ru	10/25/2014	49454545445

The registration can be verified, although pancaliente.info's WHOIS has since been made private.

Image 26: Pan caliente website as it appeared in October 2015

Examining more closely, much of the content seems to be intended to appeal to Venezuelans at home and abroad who oppose the Partido Socialista Unido de Venezuela (PSUV: the party of Hugo Chavez). Some of the reports are intriguing because they describe private documents seemingly obtained by the site (and of questionable veracity), but without further information about their origins.

In other cases, the site has published purportedly "leaked" documents. Many of these stories are critical of individuals linked to the PSUV. Many reports also concern the "Expat" community of Venezuelans who oppose the regime from overseas, especially the diaspora in Spain.

PanCaliente is referenced elsewhere online, such as an apparently leaked document hosted on Slideshare. Some of their reports also appear to have been excerpted or cited by other online news sites.

Although there seems to be a great deal of content, PanCaliente's articles do not have bylines. While the site is linked

with a very active Twitter account (https://twitter.com/pancalienteve), the associated Facebook profile (facebook.com/pancalienteok) is sparse. The WayBack Machine makes it clear that PanCaliente has only recently become active.
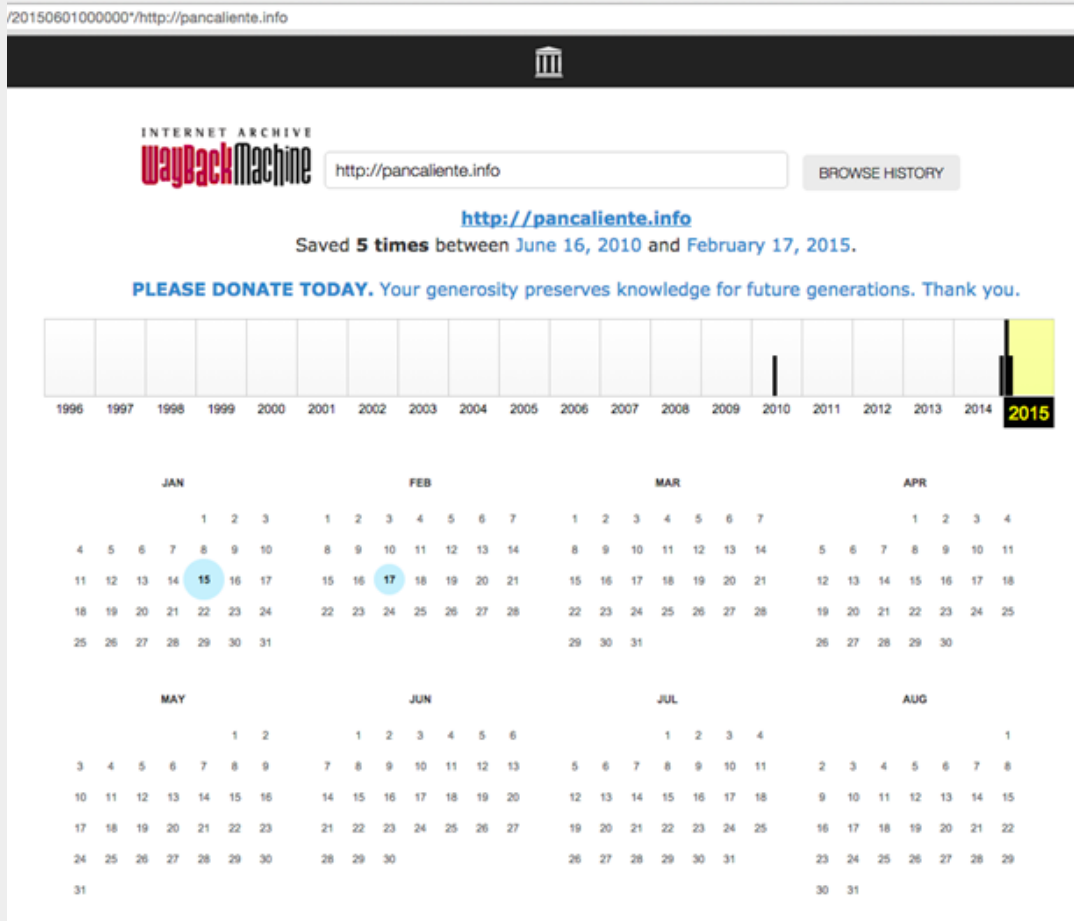

Image 27: The Wayback Machine on Pan caliente

Interestingly, some of the first reports published on the site appear to have been written when the site was being demoed as having a different name and identity "Venezuela365.com."

Image 28: Early logos, still visible in the website's directory structure

Image 29: Variation on the current PanCaliente logo

The many images of this alternate logo as it went through its iterations are publicly visible. Also still online is at least one report that still refers to the site as venezuela365. Interestingly, that first 'report' refers to "secret" information, including reproducing a purported cheque, without explaining its provenance.

> http://pancaliente[.]info/los-negocios-secretos-de-leocenis-garcia-y-gonzalo-tirado/

"García demandó a Tirado en un corte de Miami cuando el empresario le dio al periodista un cheque falso al cual Venezuela365 tuvo acceso."

The source of this page also contains links to the now-defunct venezuela365.com

> "http://venezuela365.com/wp-content/uploads/2014/10/tirado-g-300×169.jpg "

An identically named image is now hosted on pancaliente.info, in an identical directory.

The venezuela365.com domain was registered behind DomainsByProxy, however previous WHOIS names Sistekon Corp as a prior registrant. Sistekon Corporation seems to now be defunct, although its information is still on archive.org, and indicates that it develops IT software as well as selling various security solutions. Given that the domain expired in 2013, but was re-registered in 2014 at around the same time as pancaliente.info, the link may be coincidental.

We found no evidence that PanCaliente or venezuela365 was ever used to seed malware or conduct phishing attempts, either directly, or as a pretext for malicious content.

5.2 And Pro-Chavez: Chavistas 24.com

The domain, chavistas24.com, which seems to refer to supporters of former Venezuelan president Hugo Chavez, also has a range of content that is apparently supportive of the party.

Image 30: Screenshot of Chavistas24.com showing articles tagged "Traitors of the Revolution" on Chavistas24.com

Chavistas24.com similarly has an associated Twitter account that pushes out tweets, mostly referencing stories published on the website.

> https://twitter.com/chavistas24/

Image 31: The Chavistas 24 Twitter Feed

We found no evidence that chavistas24.com was used to phish or send malware, either directly, or as a pretext for malicious content or messages.

5.3 Seeking Angry Police?

Packrat appears to be interested in attracting dissatisfied members of Ecuador's National Police, and has created a website (justicia-desvinculados.com) and social media identity built around "Los Desvinculados," referring to police let go from Ecuador's National Police, possibly in the context of corruption inquiries. The website, which also includes a login section, contains news and highly critical reports about the Ecuadorian government.

Ecuador's police have previously been involved in protests over benefit cuts that some have seen as one of the strongest threats to Ecuadorian President Rafael Correa's rule.

Image 32: Screenshot of Los Desvinculados website

The social media component of this creation, including a Twitter page of the same name (twitter.com/justdesvincula2) further develops the identity.

Image 33: Screenshot of Desvinculados Twitter page

As with the two other operations described in this section, we have been unable to identify malware or phishing associated directly or indirectly with Justicia Desvinculados.

Part 6: The Challenge of Attribution

The evidence presented in this report points to a coordinated and persistent campaign with a regional focus. Naturally, this raises questions about attribution. This section assesses two competing hypotheses: Hypothesis 1: Packrat is State-Sponsored and Hypothesis 2: Packrat is Not State-Sponsored. For each hypothesis we provide one or more scenarios that we consider plausible versions of the hypothesis.

6.1 Hypothesis 1: Packrat is State-Sponsored

6.1.2 Examining the Target List

The list of known targets is full of influential people whose activities could have an impact on the domestic and regional political standing of regimes in several countries. Where we have been able to identify individuals who have been targeted, we find vocal, strong regime critics and independent journalists in Ecuador and Argentina. Interestingly, Packrat has also targeted parliamentarians, and others within the government of Ecuador. This diversity of targets with (possibly) opposing positions is a common theme in the data.

In other cases, we find phishing and malware-seeding websites, emails and messages with obviously political themes. Packrat created fake political organizations, whose identities, logos, and websites are then used to seed phishing attacks and malware. These materials seem designed to appeal primarily to both critics and (some) members of governments in Ecuador and Venezuela. We also believe that there are targets in other countries, including Brazil, but have limited information about who they are.

These are the kinds of targets who would be of interest to an intelligence or security service in the region, especially one not equipped to directly and passively monitor all of the communications of their targets. The multiple nations reflected in the seeding and targeting suggest, further, that the sponsor(s) of this activity would be interested in the opponents of several regimes.

6.1.3 Motivation for Disinformation Campaigns

We see a range of fake websites touching on political themes, but not obviously used to seed malware. While some of these sites share the same registrations as malware serving sites, they differ by having extensive content, and show no evidence of having hosted malicious files or phishing pages, or of having been used as pretexts for campaigns, as is common with Packrat. The content reflects extensive effort, as does the backstopping with identities on social media sites.

There seem to be three possible explanations for these pages. First, the pages may be an attempt to create credible fake organizations that can be used to actively promote disinformation, interspersed with real news. Second, the pages may serve as honeypots, used to attract targets, either to identify and possibly manipulate them, or to build trust that could then be used in malware attacks. Finally, the pages may be part of information gathering operations that have other components of which we are not aware.

While it would not be surprising for a political movement or well-funded set of interests to engage in these activities in one country, Packrat has done so in multiple countries. It is not clear what group beyond a state, would be interested in this kind of activity, and have the resources to support it.

6.1.4 Ability to Pay

The hosting and domain registrations necessary to maintain this campaign infrastructure for more than seven years clearly have associated costs. The human labor associated with creating and maintaining the many fake websites we have observed is also costly. This is especially true for the websites with substantial "original" content, such as PanCaliente. Finally, the extensive and personalized targeting clearly reflects substantial human effort.

The cost of this campaign suggests that Packrat is either well-resourced, or has sponsors who can pay for server space and time, as well as the costs of Packrat' s operators. We see no evidence of targeting with out-of-scope seeding materials, such as industry, business or the financial sector. Given the cost of the campaign, it is difficult to see who, beyond a state or an organized entity with political aspirations, would both want the information, and be in a position to pay for it.

6.1.5 Clues That Packrat Feels 'Safe'

When the first reports were published on the Nisman and Argentine targeting in early 2015, some of Packrat' s infrastructure was exposed. Nevertheless, much of the infrastructure has remained online. From a pragmatic point of view this makes sense. If Packrat had successful implants operational at that time, taking the infrastructure offline would close that access. Packrat would have had to engage in a process of pushing out updated implants to the infected computers that connected to a new host. This time-consuming process would also be prone to failure and possible detection.

If Packrat were afraid of criminal punishment in their country of residence, it would have been natural to take the servers offline once exposed. Their interlinked infrastructure can be used to investigate, as we did, the broader structure of their campaigns. In the hands of a law enforcement agency, these active servers could potentially be traced back to the responsible parties.

The fact that the servers remain online suggests that Packrat is operating purely on practical concerns, which do not include fear of the authorities. We take this to suggest that they may enjoy a degree of protection in the country or countries in which they operate.

While it is less conclusive, their taunts of a Citizen Lab researcher also suggest a degree of confidence that these actions will not have consequence for them. Given their decision to keep their infrastructure online, this researcher may not have been the first (or the last) to bother them by analyzing one of their attacks.

6.1.6 Two Scenarios of State Sponsorship

In this section we present two possible scenarios for state sponsorship. The data we have presented in this report could be explained by either of these possibilities (or by the scenario outlined for Hypothesis 2: Non State Sponsor).

Scenario 1: A Single State Sponsor
There are several possible explanations for the targeting we see. It is possible that Packrat is working for a single intelligence or security service, and that these activities all reflect that service' s targeting. Such a service would,

potentially, wish to keep tabs on many groups, including both its opponents, the opponents of friendly governments, and possibly friendly governments themselves.

The strong representation of ALBA (Bolivarian Alternative for the Americas) countries, and their recent "fellow-travelers" (Argentina included, although it has recently changed ruling parties), among the locations of targeting may be instructive. The leaders of these countries are widely seen as political allies on the leftist spectrum, although Argentina's most recent election in November 2015 elected a president who seems to reject this relationship. The governments of Ecuador and Venezuela, meanwhile, are especially close allies, although it is unclear how this will evolve given Venezuela's very recent elections.

Some may jump to interpret public reports of malware attacks targeting opponents of the Ecuadorian government as conclusive evidence of official Ecuadorian government involvement with Packrat. They may also point to previous reports that Ecuador's domestic intelligence agency reportedly used the commercial trojan made by Hacking Team to target at least one dissident. However, the presence of targets within the Ecuadorian parliament and possibly elsewhere in the government challenges any simplistic theory of Ecuadorian government sponsorship, but does not completely rule it out as intra-governmental rivalries or other dynamics could be at play.

Scenario 2: Mercenary Work for One or More Government Sponsors
The range and diversity of regional targets, which includes the opponents of several regimes, as well as those same governments supporters in some cases, could be taken as indicating that the threat actor group is reusing the same infrastructure for campaigns on behalf of multiple client governments at once. It is possible, for example, that Packrat is in the "address book" of multiple clients, and reuses the same infrastructure for multiple campaigns.

6.2 Hypothesis 2: Packrat is Not a State Actor

Although some of the evidence we have outlined above provides circumstantial support for state sponsorship, other features of Packrat's activity are not so clear. This section briefly lays out the most salient of these pieces of evidence: lack of technical sophistication. We evaluate this fact, and then briefly note a potential scenario for non-state sponsorship.

6.2.1 Lack of Use of technically sophisticated tools

The malware used by this campaign is primarily Commercial Off-The-Shelf (COTS) RATs, not boutique or tailor-made implants. Nor is it the commercial malware sold to governments by companies like FinFisher and Hacking Team. Additionally, the attackers do not make use of exploits for their malware seeding. The lack of exploits very likely hampers the efficacy of many attacks. For example some of the bait documents instruct victims to double click on an icon in the document. This is cumbersome, and is more likely to result in failed attacks or discovery. A threat actor with the direct support of a government might have access to more sophisticated malware, and exploits.

However, it is well documented that not all government-linked malware groups make use of sophisticated malware or exploits. Prior research by Citizen Lab, for example, has shown that state-sponsored groups targeting civil society often use the minimum necessary technical sophistication in their campaigns. Why use more sophisticated or esoteric technique when simpler tools suffice? Other research on government-linked hacking groups in the Middle East also suggests that these groups persist in exploit-less targeting, perhaps because it is inexpensive, and that it nevertheless achieves a minimum satisfactory level of infections.

Ultimately, the reliance on COTS malware and lack of exploits does not enable us to draw many conclusions. However, it does have one feature worth noting: by extensively obfuscating COTS malware, the attackers are nevertheless able to deliver malware that is effective at evading detection while simultaneously being difficult to attribute. That said, since obfuscated malware is also common in criminal hacking, the pairing of crimeware and obfuscators does not tell either way towards this hypothesis.

6.2.2: Scenario: Non-State Group

It is impossible to reject the possibility that Packrat is a criminal or non-state group. Such a group could, in theory, be a supporter of an opposition political movement, or have other interests in the critics of regimes. There are a range of powerful non-state groups in South America, including cartels and others involved in illegal trafficking, who would certainly have the ability to pay for these operations. Nevertheless, given the particular targets we are aware of, we are unsure of why these individuals would be of primary interest to groups involved in illegal activities.

Another possibility, also unfalsifiable, is that a non-government group with political ambitions is responsible for Packrat. Such a group might be particularly interested in potential allies or sources of instability, as well as governments.

6.3 Adjudicating between competing hypotheses

Ultimately, this report does not provide sufficient data to conclusively adjudicate between hypotheses. However, we

think that the best fit, which is still circumstantial, is that the ultimate recipient of the information collected by Packrat is likely one or more governments in the region.

7. Conclusion

This report described a seven year campaign with targets in several Latin American countries. While there are many well-known threat actors in Latin America, many of the most visible are engaged in cybercrime. What distinguishes Packrat is the extensive and often ingenious targeting of political figures, journalists and others. They are also distinguished by their ability to remain active over such an extended period, seemingly unfazed by discovery.

Packrat highlights the extent to which multi-year campaigns can be run using limited technical sophistication, and a lot of creativity. From a technical perspective, they rely almost entirely on off-the-shelf RATs and packers to evade antivirus detection. Where they excel is in the time and effort spent to create detailed and moderately convincing fake organizations to seed their malware.

Their persistence, and their willingness to keep using domains even after they are exposed suggests that exposure of their infrastructure is not an existential threat. Their threats and taunts are similarly brazen. This strongly suggests, but does not prove, that Packrat operates with a perception of safety.

Ultimately, this report does not conclusively attribute Packrat's activities, however we hope that by exposing their activities, we have provided encouragement to others to continue to follow the thread.

Note: The Precarious Position of Media in Latin America

While we discourage a direct link between specific incidents of non-digital harassment of journalists and Packrat, the case highlights the difficult situation faced by journalists and freedom of expression supporters in countries like Ecuador.

In Ecuador, for example, numerous observers, including the United Nations Special Rapporteur for Freedom of Expression, have expressed concern that the freedoms afforded to journalists continue to be constricted. In Ecuador journalists, and even cartoonists, have faced apparent retaliation for political speech. Journalist Martha Roldos, for example, had personal e-mails exposed in the press, and recordings of her conversations played in public. Freedom of expression and journalism organization Fundamedios, which has documented over 600 attacks against journalists from 2008-2012, has face forced shutdown. Interestingly, both of these individuals were also targets of Packrat. While we have no evidence linking the perpetrators of these actions to Packrat, nor reason to believe the sponsor is the same, the targeted malware that we describe only adds to the threats these individuals and organizations face.

Footnotes

[1] See **Appendix B** for details.

[2] bc97437fec7e7e8634c2eabae3cc4832

[3] Sandboxes include *ThreatExpert*, *Anubis*, *CWSandbox*, *JoeBox* and *Norman Sandbox*. Virtual machines include *VMWare*, *VirtualBox* and *VirtualPC*.

Acknowledgements

Ron Deibert, Masashi Crete-Nishihata, Adam Senft, Irene Poetranto, Jakub Dalek and Sarah McKune of the Citizen Lab for helpful feedback and editing assistance.

Kevin Breen for helping with the analysis of CyberGate RAT samples.

PassiveTotal and Brandon Dixon.

Steven Adair/ Volexity.

Cisco's AMP Threat Grid Team for data correlation.

Other researchers and investigators who wished to remain anonymous but provided exceptionally helpful assistance, especially PFlash.

IOCs

The Citizen Lab Github has a range of Packrat IOCs available here for download as CSVs.

Appendix A: Search Query

This is a version of our search that can be run in your inbox to determine whether you have received *some* of the e-mails we know of from this group. It is very possible that the query may yield false positives, so a "hit" is not itself a cause for alarm. We encourage you to carefully scrutinize any results before drawing conclusions. Importantly, even if the query fails to find results, this does not indicate that you have not been targeted, only that your inbox does not contain the targeting materials that we are familiar with, and that can be searched for without an overwhelming false positive rate.

You can complete this query by following the steps described in this Google Document, which is based off indicators found in previous Packrat e-mails (like email senders and malicious URLs). Note that some of the sender emails look very similar to legitimate e-mails of real people.

Appendix B Malware Samples

MD5	C&C	Family
dd1101adc86fd282f5f183942cc2f3b7	wjwj.no-ip.org ruley.no-ip.org lolinha.no-ip.org	CyberGate
2d722592a4e3c8030410dccccb221ce4	wjwj.no-ip.org	CyberGate
d2adecc6287dd4d559fe6ce2ce7a7e31	wjwj.no-ip.org ruley.no-ip.org lolinha.no-ip.org	Cybergate (suspected)
93b630891db21a4a2350280a360c713d	ruley.no-ip.org wjwj.no-ip.org lolinha.no-ip.org	CyberGate
a73351623577f44a2b578fed1e78e37e	ruley.no-ip.org wjwj.no-ip.org	CyberGate
5a8975873f52436377d8fb0b5ab0d87a	ruley.no-ip.org	CyberGate
ed8d7ed45b64890b8901b735018318f3	ruley.no-ip.org wjwj.no-ip.org	CyberGate
c2237e9d415f542ce6e73adb260af123	wjwj.no-ip.org	Xtreme RAT
2827450763b55c5e71fda3caaf8e75f9	wjwj.no-ip.org	Xtreme RAT
bc97437fec7e7e8634c2eabae3cc4832	ruley.no-ip.org taskmgr.serveftp.com	CyberGate
d7f34168b1a7dd7cbd8e62a5ab1ebc0e	taskmgr.serveftp.com taskmgr.servehttp.com	Xtreme RAT
6c34d4296126679d9c6a0bc2660dc453	taskmgr.servehttp.com taskmgr.serveftp.com	CyberGate
efc0009d76a2057f86c5f00030378c72	daynews.sytes.net	AlienSpy
74613eae84347183b4ca61b912a4573f	daynews.sytes.net	AlienSpy
d2f151312f7dee2483ddcab9766b56db	daynews.sytes.net	AlienSpy
ea7bcf58a4ccdecb0c64e56b9998a4ac	daynews.sytes.net	Adzok
1e4265a0c37773c2372b97bb6630ae57	daynews.sytes.net	Adzok
08a3bb5b220eb1e0dc2ecccbbc6859f5	daynews.sytes.net	Adzok
2de51e74fd571319bbf763ec62781096	deyrep24.ddns.net	AlienSpy
8fb96dfab7e4c0acb1eb9f4e950ba4b9	deyrep24.ddns.net	AlienSpy
4a23a1d6779d199aaa582cf0a5868ad1	deyrep24.ddns.net	Adzok
0ae0038ffe8cf5c3170734a71ff2213d	deyrep24.ddns.net	AlienSpy
8e0f021dcbbfa586a1c6780e77ac0fb6	taskmgr.servehttp.com	CyberGate
a74ef893b1bf21c9df6d8e31285db981	taskmgr.servehttp.com	CyberGate
a988235ad7d47acbeca5ccb4ea5a1ed5	taskmgr.servehttp.com	CyberGate
15ebe16cd9500de534d5bfd5eeceaf73	taskmgr.servehttp.com	CyberGate
01dec1b1d0760d5a1a562edcfeb478d1	taskmgr.servehttp.com	CyberGate
1e6d0b59d4fb7650453c207688385f3a	taskmgr.servehttp.com	CyberGate
e03be1849ad7cecba1e20923074cd22f	taskmgr.servehttp.com	CyberGate
779a79c11f581b84e7c81f321fd8d743	conhost.servehttp.com	CyberGate
13d939b2412c6adbab3cc1b539166671	conhost.servehttp.com dllhost.servehttp.com	CyberGate

7b2cb5249d704cb1df8d4210e7c3d553	dllhost.servehttp.com conhost.servehttp.com	CyberGate
a09f100ddc7cf29f8a93a3d7a79c58b9	taskmgr.servehttp.com	CyberGate
ce6065346a918a813eeb58bbb0814a23	taskmgr.servehttp.com	CyberGate
ea50bf8abcf9c0c40c4490dc15fb0a2a	taskmgr.servehttp.com	CyberGate
3a61d64986ee6529cee271ab6754faa5	taskmgr.servehttp.com	CyberGate
695db7dd3b1daf89f2c56d59faecc088	taskmgr.servehttp.com	CyberGate

Appendix C: Malware Configuration

CyberGate RAT Configuration

All Packrat's CyberGate samples seem to have been configured roughly in the same way, with only occasional changes in the Command & Control domains and port. The following configuration, for example, has been extracted from 01dec1b1d0760d5a1a562edcfeb478d1:

Key	Value
Activate Keylogger	TRUE
Active X Startup	{C452W6HW-7DQ6-8U8P-2730-EI158IF7748K}
Change Creation Date	TRUE
CyberGate Version	
Domain	taskmgr.redirectme.net|taskmgr.servehttp.com|
Enable Message Box	FALSE
FTP Address	ftp.server.com
FTP Directory Value	./logs/
FTP Interval	30
FTP Password	+
FTP Port	21
FTP UserName	ftp_user
Google Chrome Passwords	
Hide File	TRUE
Install Directory	System32
Install File Name	taskhost.exe
Install Flag	TRUE
Install Message Box	Arquivo Extraido com sucesso
Install Message Title	Ok
Keylogger Backspace = Delete	FALSE
Keylogger Enable FTP	FALSE
Melt File	FALSE
Message Box Button	0
Message Box Icon	64
Mutex	***MUTEX***
P2P Spread	
Password	abcd1234
Persistence	TRUE
Port	2012|2008|
Process Injection	Disabled
REG Key HKCU	msconfig
REG Key HKLM	msconfig
ServerID	desp

Startup Policies	Policies
USB Spread	FALSE

When no decoy Office document is added to the AutoIt3 stub, they normally enabled the Message Box and used "Arquivo corrompido " as message. Additionally, the ServerID value seems to change, including additional values like ley, vtima, Emais 10.

Xtreme RAT Configuration

Following is the configuration for one of the XtremeRAT samples employed by Packrat (c2237e9d415f542ce6e73adb260af123):

Key	Value
ActiveX Key	{5460C4DF-B266-909E-CB58-E32B79832EB2}
Domain1	wjwj.no-ip.org:200
Domain2	wjwj.no-ip.org:250
Domain3	lolinha.no-ip.org:200
Domain4	lolinha.no-ip.org:250
Domain5	:0
FTP Folder	
FTP Password	ftppass
FTP Server	ftp.ftpserver.com
FTP UserName	
Group	Servers
HKCU	HKCU
HKLM	HKLM
ID	Server
Injection	%DEFAULTBROWSER%
Install Dir	InstallDir
Install Name	regedi.exe
Msg Box Text	Ocorreu um erro inesperado ao iniciar o programa.
Msg Box Title	Erro
Mutex	RJokLSZBj
Version	3.5 Private

Adzok Configuration

MD5: ea7bcf58a4ccdecb0c64e56b9998a4ac

```
Adzok Free
Chrome
Java
7854
true
7777
daynews.sytes.net
true
```

Adwind variant configuration

efc0009d76a2057f86c5f00030378c72 LOS TUITEROS ESPIADOS POR SENAIN.docx

```
'DELAY_CONNECT' : 1,
'DELAY_INSTALL' : 1,
'INSTALL' : true,
'JAR_EXTENSION' : 'Java.txt' ,
'JAR_FOLDER' : 'Cas436FlashJava' ,
```

'JAR_NAME' : 'Cas934FlashJava' ,
'JAR_REGISTRY' : 'JavaSE' ,
'JRE_FOLDER' : 'RoUndCuBe' ,
'NETWORK' : [{ 'DNS' : 'daynews.sytes.net' , 'PORT' : 1090}],
'NICKNAME' : 'Java' ,
'PLUGIN_EXTENSION' : 'txt' ,
'PLUGIN_FOLDER' : 'Cas754FlashJava' ,
'VBOX' : false,
'VMWARE' : false

Appendix D: Seeding Domains

Domains resolving to 198.12.150.249

| Domain	First Seen	Last Seen
soporte-yahoo.com	10/20/2014 0:00:00	10/20/2014 0:00:00
update-outlook.info	10/21/2014 0:00:00	10/21/2014 0:00:00
deyrep.com	12/19/2014 0:00:00	12/19/2014 0:00:00
support-whatsapp.com	1/23/2015 20:39:00	1/23/2015 20:39:00
deyrep.com	1/30/2015 14:23:00	9/8/2015 5:19:00
blackboxmusic.co	1/31/2015 0:00:00	1/31/2015 0:00:00
www.blackboxmusic.co	1/31/2015 0:00:00	1/31/2015 0:00:00
blackboxmusic.co	1/31/2015 10:11:00	2/21/2015 6:08:00
www.blackboxmusic.co	1/31/2015 10:11:00	2/7/2015 1:14:00
mail-account-update.com	2/1/2015 1:59:00	2/1/2015 1:59:00
soporte-yahoo.com	2/6/2015 6:57:00	9/8/2015 5:30:00
soporte-gmail.com	2/6/2015 7:20:00	10/8/2015 5:03:00
login-office365.com	2/24/2015 0:00:00	2/24/2015 0:00:00
lavozmericana.info	2/26/2015 0:00:00	2/26/2015 0:00:00
support-java.com	2/28/2015 0:00:00	2/28/2015 0:00:00
pancaliente.info	3/6/2015 16:02:00	10/18/2015 5:42:00
pancaliente.info	3/10/2015 0:00:00	3/10/2015 0:00:00
pancaliente.info	3/10/2015 9:02:00	10/17/2015 5:31:00
logon-outlook.com	4/1/2015 0:00:00	4/1/2015 16:50:00
movimientoanticorreista.com	4/24/2015 0:00:00	4/24/2015 0:00:00
login-office365.com	5/19/2015 4:26:00	9/8/2015 5:24:00
logon-outlook.com	5/19/2015 6:15:00	9/8/2015 5:24:00
mgoogle.us	5/19/2015 6:16:00	9/4/2015 4:36:00
lavozamericana.info	5/19/2015 6:21:00	9/8/2015 5:24:00
deyrep.com	5/25/2015 0:48:00	5/25/2015 0:48:00
n3.pancaliente.info	6/25/2015 23:56:00	10/19/2015 19:28:00
n4.pancaliente.info	6/25/2015 23:56:00	10/19/2015 19:28:00
ns1.deyrep.com	6/29/2015 20:47:00	9/9/2015 19:53:00
ns2.deyrep.com	6/29/2015 20:47:00	9/9/2015 19:53:00
n1.login-office365.com	7/9/2015 6:27:00	7/9/2015 6:27:00
n2.login-office365.com	7/9/2015 6:27:00	7/9/2015 6:27:00
1.lavozamericana.info	8/7/2015 4:36:00	8/31/2015 3:50:00
2.lavozamericana.info	8/7/2015 4:36:00	8/31/2015 3:50:00
n1.update-outlook.info	8/10/2015 19:35:00	8/10/2015 19:35:00
ns.update-outlook.info	8/10/2015 19:35:00	8/10/2015 19:35:00
1.chavistas24.com	8/16/2015 11:54:00	10/19/2015 0:24:00

2.chavistas24.com	8/16/2015 11:54:00	10/19/2015 0:24:00
s1.mgoogle.us	8/30/2015 5:04:00	8/30/2015 5:04:00
s2.mgoogle.us	8/30/2015 5:04:00	8/30/2015 5:04:00
chavistas24.com	9/1/2015 5:12:00	10/18/2015 5:19:00

Domains resolving to 193.105.134.27

Domain	First Seen	Last Seen
support-login-validate-outlook.tk	10/23/2015 14:45:40	11/4/2015 17:06:00
verify-gmail-support-secure.tk	10/10/2015 0:00:00	10/13/2015 3:48:18
soporte-login-account-gmail.tk	9/26/2015 20:55:49	10/3/2015 1:02:29
soporte-login-account-yahoo.tk	9/20/2015 14:57:09	9/21/2015 18:42:14
focusecuador.tk	9/19/2015 20:56:29	9/21/2015 5:16:06
1.update-outlook.info	9/13/2015 4:34:45	9/15/2015 9:19:06
2.update-outlook.info	9/13/2015 4:34:45	9/15/2015 9:19:06
1.desk-yahoo.com	9/10/2015 5:32:50	9/12/2015 5:31:16
2.desk-yahoo.com	9/10/2015 5:32:50	9/12/2015 5:31:16
2.mlogin-outlook.com	9/10/2015 5:08:37	9/12/2015 5:11:16
1.mlogin-outlook.com	9/10/2015 5:08:37	9/12/2015 5:11:16
1.soporte-google.com	9/12/2015 3:28:30	9/12/2015 3:28:30
2.soporte-google.com	9/12/2015 3:28:30	9/12/2015 3:28:30
mlogin-outlook.com	9/12/2015 0:55:17	9/12/2015 0:55:17
ns2.mlogin-outlook.com	9/12/2015 0:55:17	9/12/2015 0:55:17
ns1.mlogin-outlook.com	9/12/2015 0:55:17	9/12/2015 0:55:17

Domains registered by enripintos123@outlook.es

Domain	Registrar	E-mail	Nameserver	Date	Phone
support-java.com	GODADDY.COM,LLC	enripintos123@outlook.es	n1.support-java.com	2/24/2015	49454545445
lavozamericana.info	GoDaddy.com,LLC(R171-LRMS)	enripintos123@outlook.es	n1.lavozamericana.info	2/22/2015	49454545445
login-office365.com	GODADDY.COM,LLC	enripintos123@outlook.es	n1.login-office365.com	2/21/2015	49454545445
support-whatsapp.com	GODADDY.COM,LLC	enripintos123@outlook.es	s1.support-whatsapp.com	10/30/2014	49454545445
mgoogle.us	GODADDY.COM,INC.	enripintos123@outlook.es	s1.mgoogle.us	10/30/2014	1454545445
android-flash.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns03.domaincontrol.com	10/30/2014	1454545445
pancaliente.info	GoDaddy.com,LLC(R171-LRMS)	enripintos123@outlook.es	ns1.hostinger.ru	10/25/2014	49454545445
soporte-gmail.com	GODADDY.COM,LLC	enripintos123@outlook.es	n1.soporte-gmail.com	10/19/2014	49454545445
soporte-yahoo.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns33.domaincontrol.com	10/17/2014	49454545445
autorizacion-gmail.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns1.hostinger.ru	10/17/2014	49454545445
support-gmail.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns1.ukraine.com.ua	10/15/2014	49454545445
support-gmail.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns1.hostinger.ru	10/15/2014	49454545445
login-outlook.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns1.hostinger.ru	10/9/2014	49454545445
logon-outlook.com	GODADDY.COM,LLC	enripintos123@outlook.es	ns1.hostinger.ru	9/27/2014	1454545445
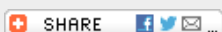
Post a Comment

Your email is *never* shared. Required fields are marked *

Name *

Email *

Website

Comment

Post Comment

© Citizenlab 2013 | Contact | RSS