Endpoint Protection

symantec.com/connect/blogs/colombians-major-target-email-campaigns-delivering-xtreme-rat

Dec 03, 2015 08:59 AM

A L Johnson

Throughout 2015, Symantec.cloud has been detecting a stream of emails that have the Xtreme remote access Trojan (RAT), which we detect as W32.Extrat, as an attachment. These emails are mainly sent to Colombians who may work in the accounting or finance departments of various-sized organizations. The people behind the attacks are likely attempting to gain access to computers where banking transactions are performed, in order to steal banking credentials.

By examining the global detections from Symantec endpoint products for the past two months, we can confirm that W32.Extrat infections are more prevalent in Colombia than in any other region.

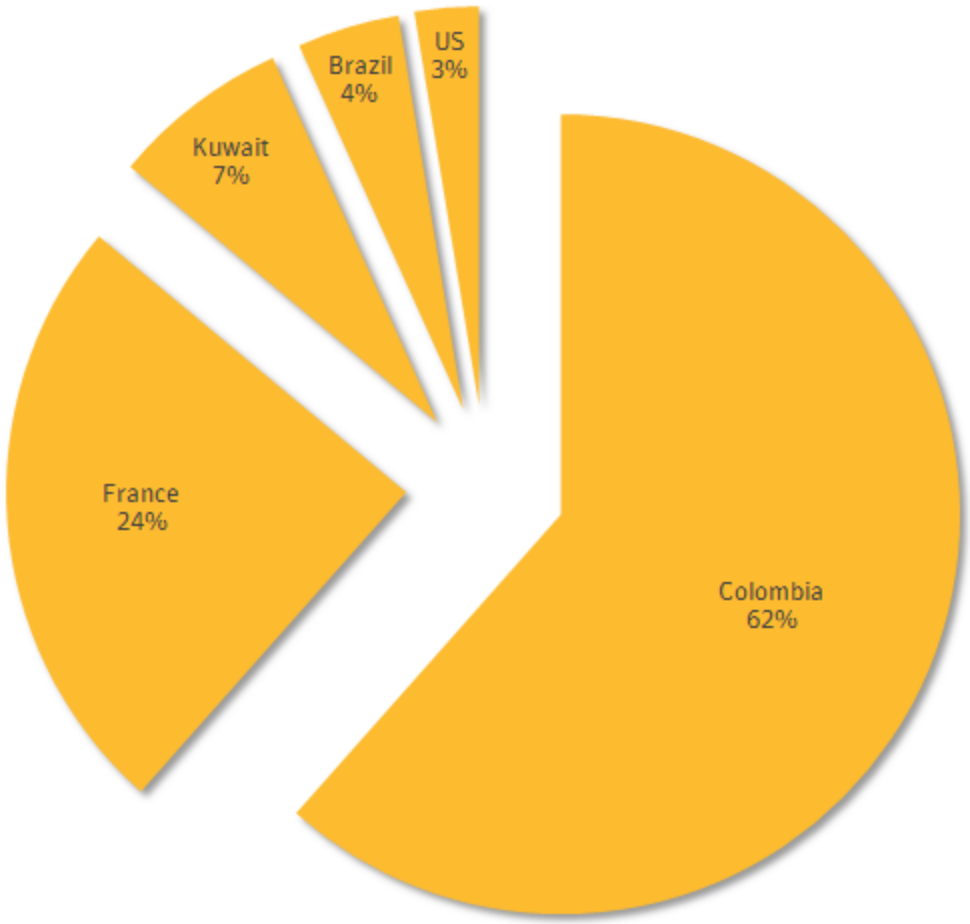

Figure 1. Top five regions reporting W32.Extrat infections

We combined email data from Symantec.cloud with telemetry from Symantec endpoint products to cluster together attack activity. Through our analysis, we identified what appear to be distinct sets of attackers. Over 2015, at least four main groups have been sending emails with W32.Extrat attachments in order to compromise Colombia-based targets. We also found that there are other smaller groups actively distributing this threat in emails. Similar uses of W32.Extrat have been documented in the past.

Symantec calls the four attack teams Caramel, Cuent, Maga, and Molotos. During our research, we grouped clusters of activity according to the attackers' command-and-control (C&C) domains. It is possible that some of these clusters are actually related to each other.

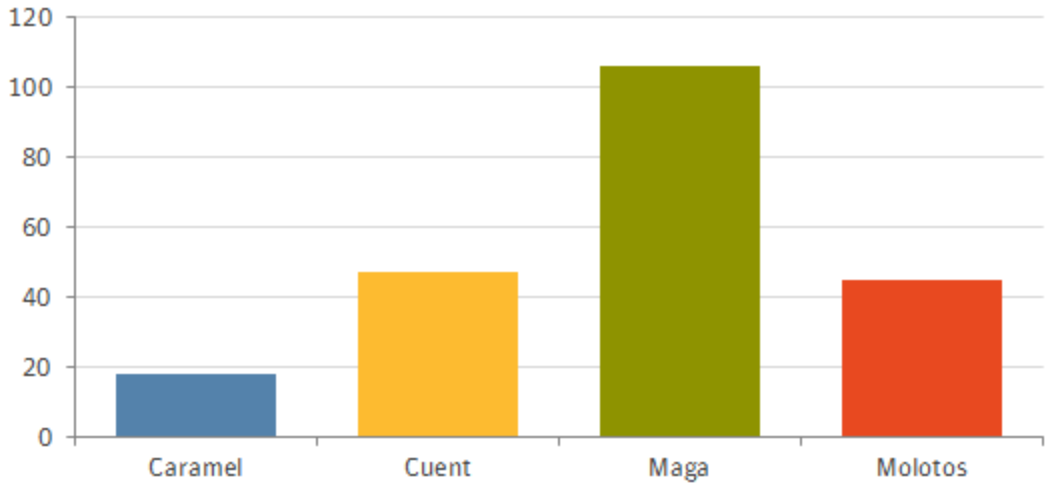

Figure 2. Number of computers infected with W32.Extrat per attack group for one month

The attack groups generally use similar email subjects in their W32.Extrat campaigns.

Subject	Group
NOTIFICACION FOTO COMPARENDO	Caramel
FORMATO CORRECTO TERCERA CITACION AUDIENCIA PUBLICA	Caramel
CITACION AUDIENCIA PUBLICA DENUNCIA CIVIL	Caramel
Detalles Informacion	Cuent
Informacion Detallada	Cuent
Demanda Asignada	Cuent
Estado de cuenta	Cuent
Juzgado Citacion	Cuent
Cobro Juridico	Cuent
Citacion Juzgado	Cuent
Quiero que todos vean este archivo	Cuent
Quiero que vean este archivo	Cuent
Carta De Cobro	Cuent
Recibos En Mora	Cuent
Proceso En Mora	Cuent
Estado De Cuenta	Maga

Subject	Group
Soporte de Consignacion	Maga
COBRO JURIDICO	Maga
Cuenta de Cobro	Maga
Vinculados Por Corrupcion	Maga
NIT SUSPENDIDO	Molotos
Soporte de Consignacion	Molotos
Suspencion de la Inscripcion en el Registro Unico Tributario	Molotos
Invitacion a pagar de manera urgente sus Obligaciones	Molotos

Table 1. W32.Extrat email subjects per attack group

The email subjects usually have a legal connotation or are related to payments and tax. The contents of the messages continue with these themes and appear as legitimate emails. One example email was sent from what appeared to be a compromised email account and its subject matter was relevant to the recipient organization's industry.

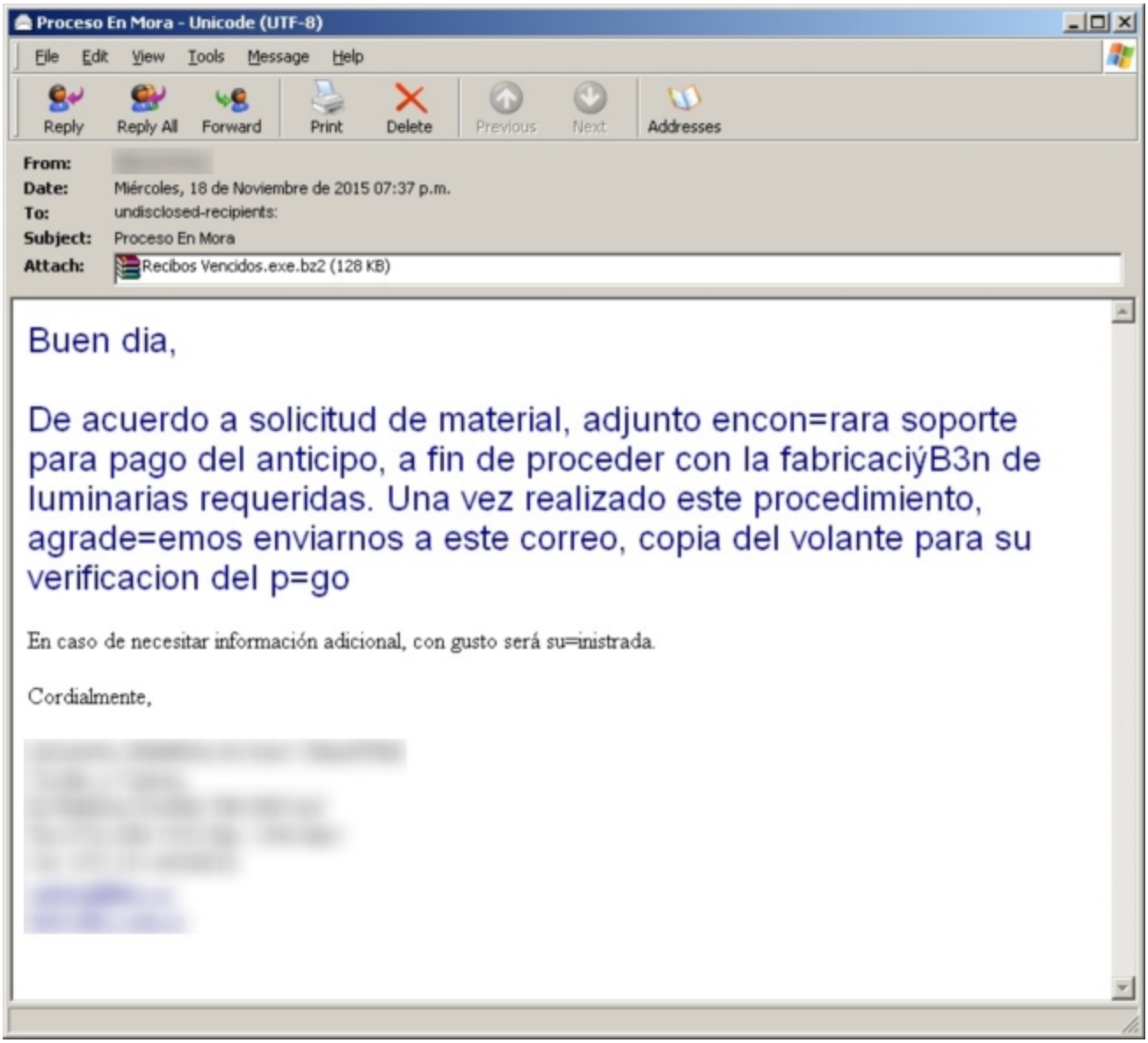

Figure 3. An example of a malicious email with a W32.Extrat attachment, which was sent from a compromised account

It is likely that the various attackers are based in Colombia, as they consistently use Colombian IP addresses for command and control. All of the attackers use dynamic DNS domains for their C&C infrastructure. These dynamic DNS domains resolve to IP addresses that are assigned to internet service providers (ISPs), not hosting facilities.

The lifespan of the IP addresses reflect these findings. The majority of the attackers' domains change to a new IP address in 24-hour periods, with some lasting from three to four days.

Some example hashes and domains for each group are listed in the following table.

MD5	C&C domain	Group
084299bef9f83f42b9281c9c6155a4f3	auxilio.duckdns.org	Maga

MD5	C&C domain	Group
8fef5053d9d96637ccc26c452aaf73dc	magalyamaya.mooo.com	Maga
516186e260d8cba116a470efcf84cf34	caramelochpetinnew2.ddns.net	Caramel
00adadf595c062ebaaa05a1c23a1c13a	cuentadns.mooo.com	Cuent
0f0d4493705264ddcc337f22abe50266	yiyik13.no-ip.biz	Cuent
629725ca22c9b2bcfb086d4593214e01	molotos4.no-ip.biz	Molotos

Table 2. MD5 hashes of samples and domains per group

Mitigation

Attacks targeting the financial departments of businesses are a regular occurrence. The approaches that the attackers take include emails with malicious attachments, phishing attacks claiming to be from senior management, and social engineering involving phone calls. Employees should take the following precautions to prevent these campaigns from succeeding:

- Do not open attachments or click on links in suspicious email messages
- Avoid providing any personal information when answering an email
- Never enter personal information in a pop-up web page
- Keep security software up to date
- If you're uncertain about an email's legitimacy, contact your internal IT department or submit the email to Symantec Security Response through this portal.

Protection

A full protection stack helps to defend against these attacks, including Symantec.cloud email blocking, web gateway security, and endpoint security.

Symantec and Norton products detect the payload of these attacks through the following detections:

AV

W32.Extrat

IPS