PandaLabs annual Report

2012 Summary

01| Introduction

The year 2012 has come to an end, and it is time to take a look back and analyze everything that has happened in the security world over the last twelve months. Malware creation showed no sign of slowing down, as shown by the fact that in 2012 we detected a record-high 27 million new malware strains at the laboratory, at an average of 74,000 new samples per day. In addition, cyber-attacks against multinational corporations continued to increase, with victims ranging from companies in the video game industry (Blizzard) to auto giants (Nissan).

We also analyze the most important events in the mobile phone industry. As Android's market share continues to grow, the motivation for cyber-crooks to target the platform also increases.

The report also covers how social media (Facebook especially) was used by cyber-criminals to spread malware by making use of social engineering techniques.

Furthermore, we take a look at the largest Mac infection to date and its consequences.

2012 has seen some remarkable events in the cyber-war/cyber-espionage arena, with Flame grabbing headlines. We analyze this and other attacks that took place in the Middle East.

Summing up, this report recaps the major computer security events that occurred in 2012, and forecasts future trends for 2013. Sit back and enjoy!

02| 2012 at a glance

As Android market share continues to grow, so does the amount of malware targeting the platform. In January, Google had to remove several malicious apps from its Android Market (renamed to 'Play Store'). Basically, cyber-crooks repackaged popular games like Angry Birds or Cut The Rope with malicious code and uploaded them to Play Store. Users then downloaded and installed the apps unaware that they were also installing a Trojan that sent SMS messages to a premium rate number.

Mobile Phone Malware

In fact, we learned that Google, tired of the malicious apps found on Play Store, has started analyzing apps before putting them in their catalog in order to detect anomalous behavior. According to their own sources, they have managed to reduce malicious app downloads by 40 percent.

Unfortunately, despite these efforts, criminals continued to target the Android mobile platform through apps not always accessible through Play Store. This was the case of Bmaster, a remote access Trojan (RAT) on the Android platform that tried to pass itself off as a legitimate application.

We also saw Trojans exclusively designed to steal data from infected devices: from call and text message records to users' contact lists. Android is potentially exposed to far more security risks than its biggest competitor (iPhone and its iOS), as it allows users to get their apps from anywhere their want. However, using the official Android marketplace is no security guarantee either, as it has also been targeted by cyber-crooks luring users into installing Trojans disguised as legitimate apps. Something which, by the way, has also happened to Apple's App Store, but to a lesser extent than to Google's Play Store.

Opera Mini is a Web browser designed primarily for mobile phones. Over the last few months, Opera Mini has gained in popularity as a mobile browser alternative on Android smartphones, becoming a target for cyber-criminals to trick users. In the latest attack, criminals offered the browser to users from a store other than Google's Play store. However, installing the application installed the actual Opera browser, and also a Trojan that sent SMS messages to premium-rate numbers.

Unlike other cases in which Trojans attempted to pass themselves off as popular mobile apps, in this case the malware came bundled with a legitimate version of the Opera Mini mobile browser to help trick users into thinking that nothing was wrong as they could simply use the real software as expected.

FIG.01. *CHINA MOBILE.*

We saw another 'unusual' attack in China, as a Trojan was released that purchased applications from the infected device. The Trojan affected Chinese subscribers to China Mobile, one of the world's largest mobile phone carriers with more than 600 million subscribers. Once infected, the mobile started buying applications from China Mobile's marketplace on behalf of the user. This Trojan was delivered on nine unofficial app stores.

At this point, many users believe that it is safer to buy and install apps from official stores. This is true to some extent, but there have also been instances of malware creeping onto official stores. This quarter, for example, a new malware strain was discovered hiding out in the Play Store, posing as two games: Super Mario Bros and GTA 3 Moscow City. The malware managed to remain undetected for weeks until it was finally removed.

FIG.02. *500 MILLION ANDROID DEVICES NOW ACTIVATED.*

Why is Android the most targeted mobile platform? Well, this is due to a number of reasons: Firstly, Android allows its users to get their apps from anywhere they want. They don't necessarily have to go to the official store, nor must applications be digitally signed as with iOS. Secondly, cyber-crooks would have never set their eyes on this platform if it weren't for the large number of users it has. In June, Google announced that 400 million Android devices had been activated, a figure that reached 500 million at the beginning of September, with 1.3 million activations per day.

Police Virus Scam

One of this year's top threats has undoubtedly been a new malware epidemic that infected hundreds of thousands of computers around the world using fear and blackmailing techniques to extort money from computer users.

While we are used to seeing this kind of fake message in English, in this case the attacks were localized. We saw English, German, Spanish, Dutch and Italian messages (among others) depending on the targeted country. All of the attacks targeted some European nation, so it looks like they were related and the same cyber-criminal gang could be behind them.

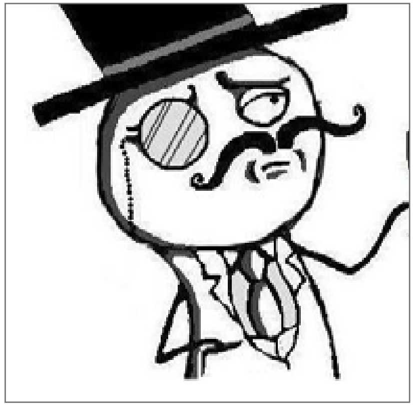
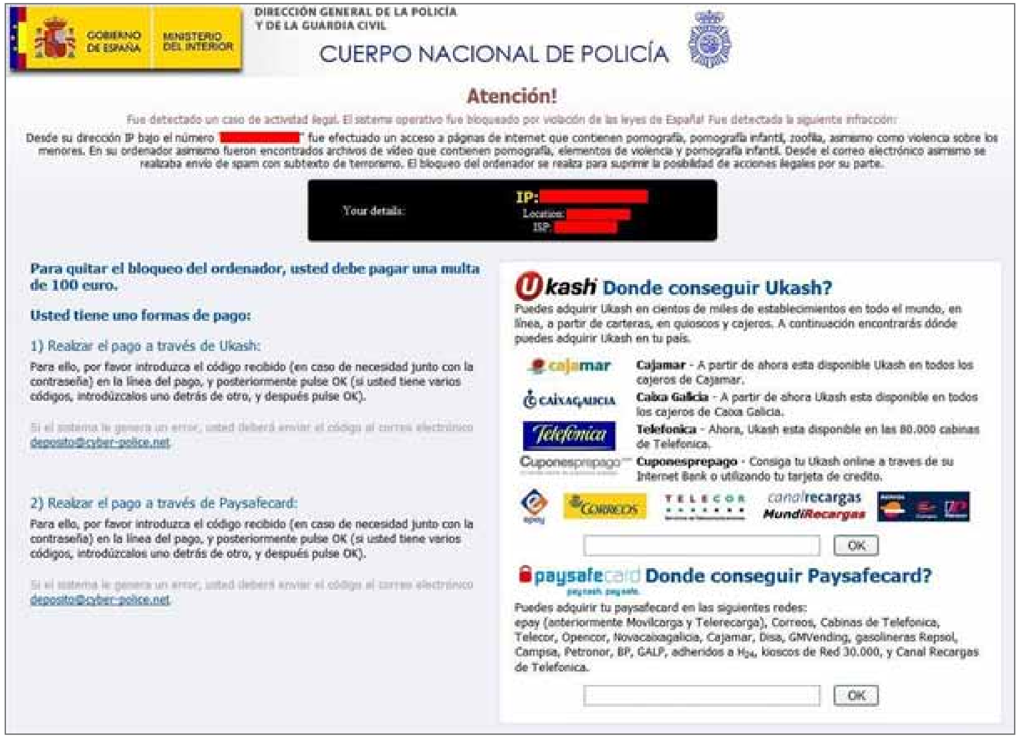


FIG.3. *ICON USED BY ONE OF THE "POLICE VIRUS" VARIANTS.*

Let's take a closer look at one of the attacks. The file's icon was the popular logo used by LulzSec in their communications:

Once their computer was infected, the user was confronted with the following full-screen window covering the entire desktop:



DIRECCIÓN GENERAL DE LA POLICÍA
Y DE LA GUARDIA CIVIL

CUERPO NACIONAL DE POLICÍA

Atención!

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue detectada la siguiente infracción:

Desde su dirección IP bajo el número "[redacted]" fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de video que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Your details: IP: [redacted]
Location: [redacted]
ISP: [redacted]

Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.

Usted tiene uno formas de pago:

1) Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.

2) Realizar el pago a través de Paysafecard:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net.

Ukash Donde conseguir Ukash?

Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.

Cajamar - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.

Caixa Galicia - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.

Telefonica - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.

Cuponesprepago - Consiga tu Ukash online a traves de su Internet Bank o utilizando tu tarjeta de credito.

OK

paysafecard Donde conseguir Paysafecard?

Puedes adquirir tu paysafecard en las siguientes redes:
epay (anteriormente Movilcarga y Telerecarga), Correos, Cabinas de Telefonica, Telecor, Opencor, Novacaixagalicia, Cajamar, Disa, GMVending, gasolineras Repsol, Campsa, Petronor, BP, GALP, adheridos a H_{24}, kioscos de Red 30.000, y Canal Recargas de Telefonica.

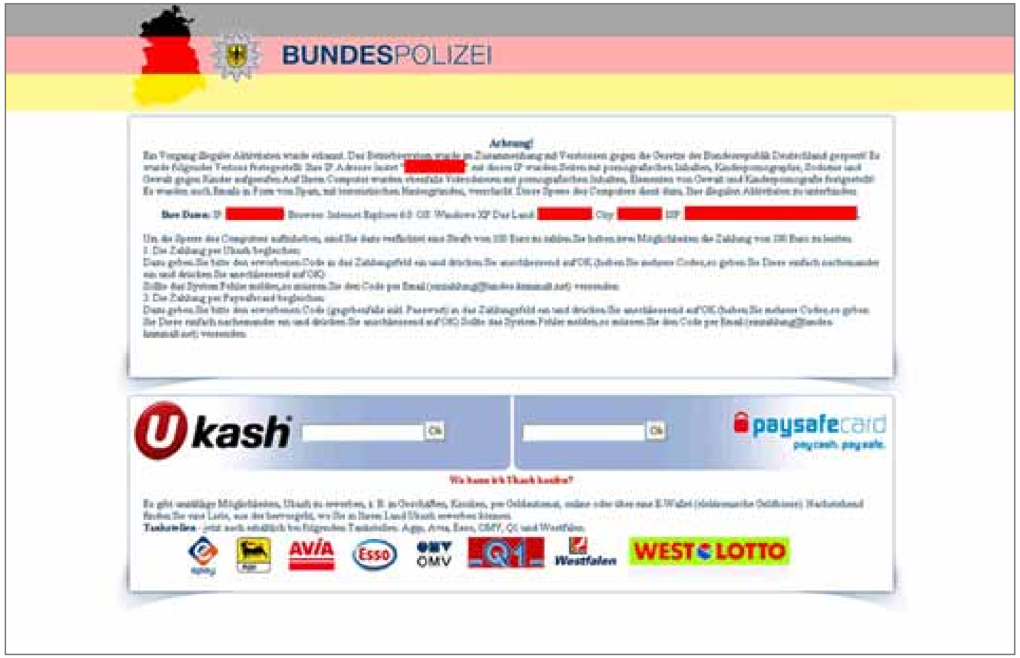
OK

FIG.04. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN.*

The message informed the user that they had accessed illegal material (such as child pornography) or sent spam messages with terrorist motives, and their computer had been locked to prevent further abuse. To unlock their computer, they had to pay a €100 'fine'.

The worst thing for the user was that the Trojan actually blocked the computer, so it was not easy to remove it. To do it, the user had to restart the computer in safe mode and run a scan with an antivirus solutions that was able to detect it.

How come the message was displayed in the victim's own language and how did the Trojan purport to come from local authorities? Well, that's easy to explain: After infecting the computer, the malware connected to a certain URL and, based on the victim's IP address, retrieved the localized version of the message that appeared on the computer. Most messages pretended to come from European authorities (although we also saw examples targeting users in other countries, like Canada for example). Below are some examples of similar attacks launched in Q1 2012:



BUNDESPOLIZEI

Achtung!

Ein Vorgang illegaler Aktivitäten wurde erkannt. Das Betriebssystem wurde im Zusammenhang mit Verstössen gegen die Gesetze der Bundesrepublik Deutschland gesperrt! Es wurde folgender Verstoss festgestellt: Ihre IP Adresse lautet "[redacted]" mit dieser IP wurden Seiten mit pornografischen Inhalten, Kinderpornographie, Sodomie und Gewalt gegen Kinder aufgerufen. Auf Ihrem Computer wurden ebenfalls Videodateien mit pornografischen Inhalten, Elementen von Gewalt und Kinderpornographie festgestellt! Es wurden auch Emails in Form von Spam, mit terroristischen Hintergründen, verschickt. Diese Sperre des Computers dient dazu, Ihre illegalen Aktivitäten zu unterbinden.

Ihre Daten: IP: [redacted] Browser: Internet Explorer 6.0 OS: Windows XP Das Land: [redacted] City: [redacted] ISP: [redacted].

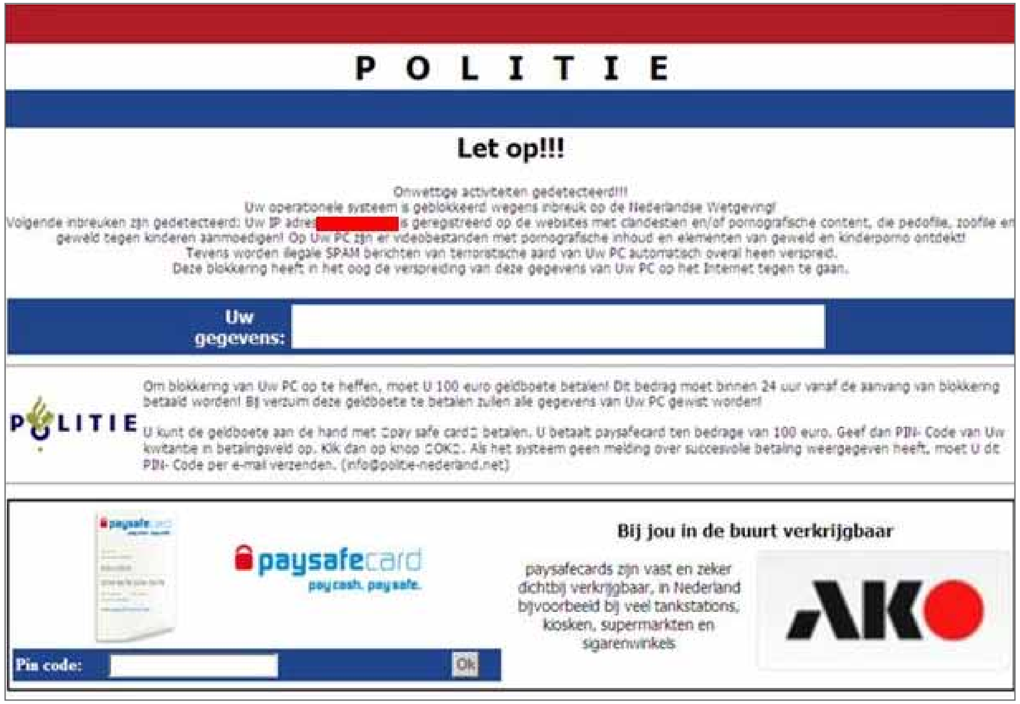
Um die Sperre des Computers aufzuheben, sind Sie dazu verpflichtet eine Strafe von 100 Euro zu zahlen.Sie haben zwei Möglichkeiten die Zahlung von 100 Euro zu leisten:
1. Die Zahlung per Ukash begleichen:
Dazu geben Sie bitte den erworbenen Code in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK)
Sollte das System Fehler melden,so müssen Sie den Code per Email ([illegible]) versenden.
2. Die Zahlung per Paysafecard begleichen:
Dazu geben Sie bitte den erworbenen Code (gegebenfalls mit Passwort) in das Zahlungsfeld ein und drücken Sie anschliessend auf OK (haben Sie mehrere Codes,so geben Sie Diese einfach nacheinander ein und drücken Sie anschliessend auf OK) Sollte das System Fehler melden,so müssen Sie den Code per Email ([illegible]) versenden.

Ok Ok

Wo kann ich Ukash kaufen?

Es gibt unzählige Möglichkeiten, Ukash zu erwerben, z. B. in Geschäften, Kiosken, per Geldautomat, online oder über eine E-Wallet (elektronische Geldbörse). Nachstehend finden Sie eine Liste, aus der hervorgeht, wo Sie in Ihrem Land Ukash erwerben können.
Tankstellen - jetzt auch erhältlich bei folgenden Tankstellen: Agip, Avia, Esso, OMV, Q1 und Westfalen.

FIG.05. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN GERMAN.*



P O L I T I E

Let op!!!

Onwettige activiteiten gedetecteerd!!!
Uw operationele systeem is geblokkeerd wegens inbreuk op de Nederlandse Wetgeving!
Volgende inbreuken zijn gedetecteerd: Uw IP adres [redacted] is geregistreerd op de websites met clandestien en/of pornografische content, die pedofilie, zoofilie en geweld tegen kinderen aanmoedigen! Op Uw PC zijn er videobestanden met pornografische inhoud en elementen van geweld en kinderporno ontdekt!
Tevens worden illegale SPAM berichten van terroristische aard van Uw PC automatisch overal heen verspreid.
Deze blokkering heeft in het oog de verspreiding van deze gegevens van Uw PC op het Internet tegen te gaan.

Uw gegevens:

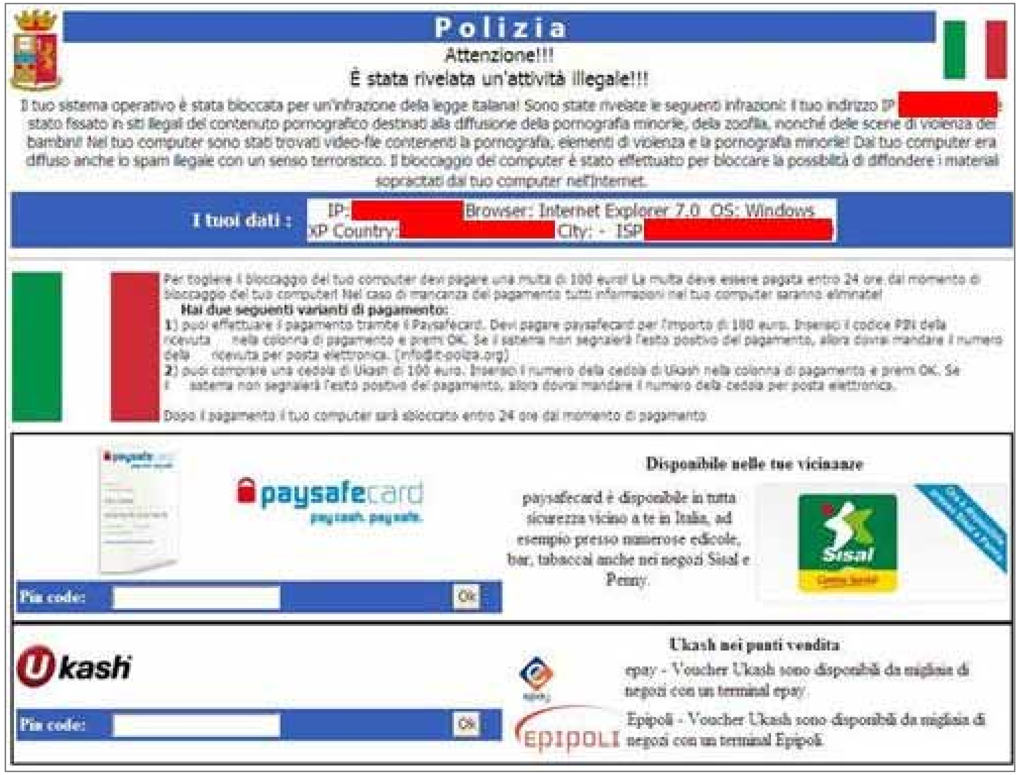
Om blokkering van Uw PC op te heffen, moet U 100 euro geldboete betalen! Dit bedrag moet binnen 24 uur vanaf de aanvang van blokkering betaald worden! Bij verzuim deze geldboete te betalen zullen alle gegevens van Uw PC gewist worden!

U kunt de geldboete aan de hand met □pay safe card□ betalen. U betaalt paysafecard ten bedrage van 100 euro. Geef dan PIN- Code van Uw kwitantie in betalingsveld op. Klik dan op knop □OK□. Als het systeem geen melding over succesvolle betaling weergegeven heeft, moet U dit PIN- Code per e-mail verzenden. (info@politie-nederland.net)

Bij jou in de buurt verkrijgbaar

paysafecards zijn vast en zeker dichtbij verkrijgbaar, in Nederland bijvoorbeeld bij veel tankstations, kiosken, supermarkten en sigarenwinkels

FIG.06. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN DUTCH.*



Polizia

Attenzione!!!
È stata rivelata un'attività illegale!!!

Il tuo sistema operativo è stata bloccata per un'infrazione dela legge italiana! Sono state rivelate le seguenti infrazioni: Il tuo indirizzo IP [redacted] è stato fissato in siti illegali del contenuto pornografico destinati alla diffusione della pornografia minorile, della zoofilia, nonché delle scene di violenza dei bambini! Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile! Dal tuo computer era diffuso anche lo spam illegale con un senso terroristico. Il bloccaggio del computer è stato effettuato per bloccare la possibilità di diffondere i materiali sopracitati dal tuo computer nell'Internet.

I tuoi dati : IP: [redacted] Browser: Internet Explorer 7.0 OS: Windows XP Country: [redacted] City: - ISP [redacted]

Per togliere il bloccaggio del tuo computer devi pagare una multa di 100 euro! La multa deve essere pagata entro 24 ore dal momento di bloccaggio del tuo computer! Nel caso di mancanza del pagamento tutti informazioni nel tuo computer saranno eliminate!

Hai due seguenti varianti di pagamento:

1) puoi effettuare il pagamento tramite il Paysafecard. Devi pagare paysafecard per l'importo di 100 euro. Inserisci il codice PIN della ricevuta nella colonna di pagamento e premi OK. Se il sistema non segnalerà l'esito positivo del pagamento, allora dovrai mandare il numero della ricevuta per posta elettronica. (info@it-polizia.org)

2) puoi comprare una cedola di Ukash di 100 euro. Inserisci il numero della cedola di Ukash nella colonna di pagamento e premi OK. Se il sistema non segnalerà l'esito positivo del pagamento, allora dovrai mandare il numero della cedola per posta elettronica.

Dopo il pagamento il tuo computer sarà sbloccato entro 24 ore dal momento di pagamento

Disponibile nelle tue vicinanze

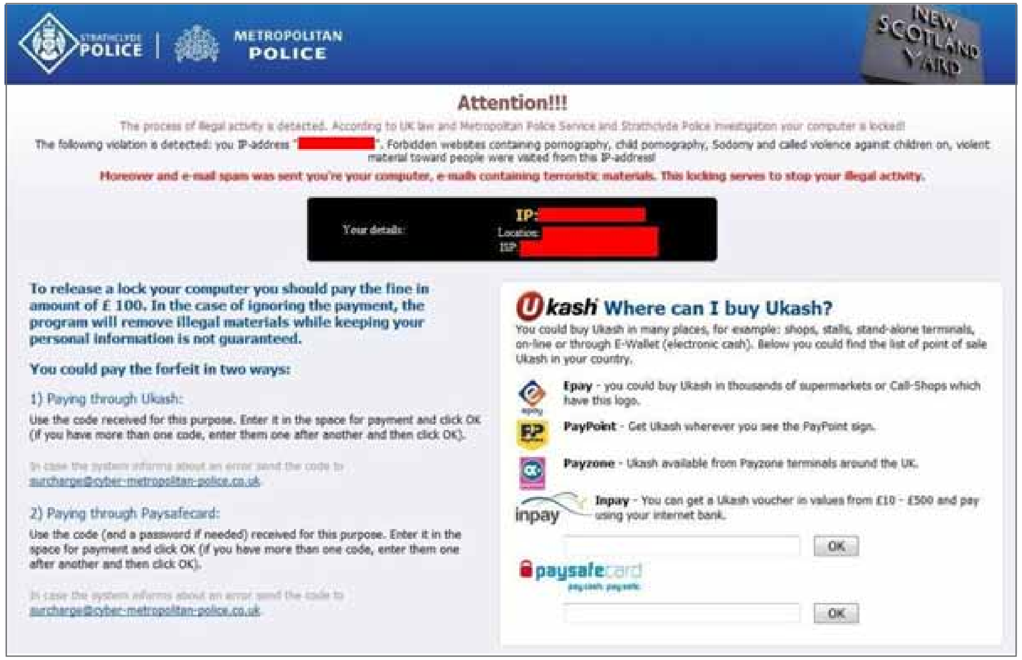
paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.

Ukash nei punti vendita

epay - Voucher Ukash sono disponibili da migliaia di negozi con un terminal epay.

Epipoli - Voucher Ukash sono disponibili da migliaia di negozi con un terminal Epipoli.

FIG.07. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN ITALIAN.*



Attention!!!

The process of illegal activity is detected. According to UK law and Metropolitan Police Service and Strathclyde Police investigation your computer is locked!

The following violation is detected: you IP-address "[redacted]". Forbidden websites containing pornography, child pornography, Sodomy and called violence against children on, violent material toward people were visited from this IP-address!

Moreover and e-mail spam was sent you're your computer, e-mails containing terroristic materials. This locking serves to stop your illegal activity.

Your details: IP: [redacted]
Location: [redacted]
ISP: [redacted]

To release a lock your computer you should pay the fine in amount of £ 100. In the case of ignoring the payment, the program will remove illegal materials while keeping your personal information is not guaranteed.

You could pay the forfeit in two ways:

1) Paying through Ukash:

Use the code received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

2) Paying through Paysafecard:

Use the code (and a password if needed) received for this purpose. Enter it in the space for payment and click OK (if you have more than one code, enter them one after another and then click OK).

In case the system informs about an error send the code to surcharge@cyber-metropolitan-police.co.uk.

Ukash Where can I buy Ukash?

You could buy Ukash in many places, for example: shops, stalls, stand-alone terminals, on-line or through E-Wallet (electronic cash). Below you could find the list of point of sale Ukash in your country.

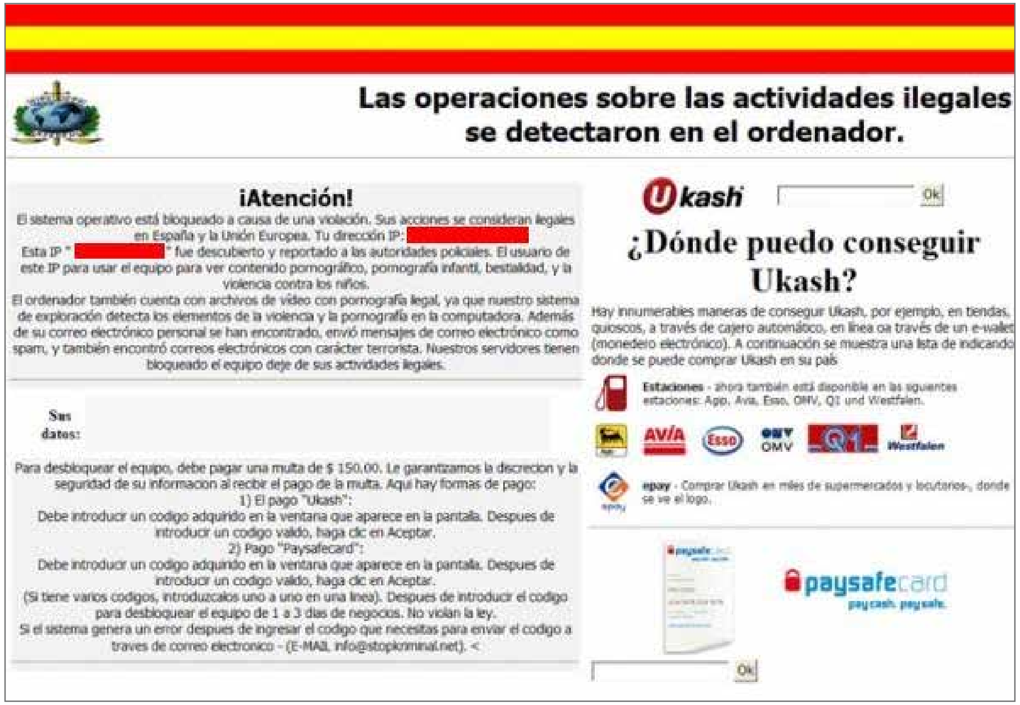
Epay - you could buy Ukash in thousands of supermarkets or Call-Shops which have this logo.

PayPoint - Get Ukash wherever you see the PayPoint sign.

Payzone - Ukash available from Payzone terminals around the UK.

Inpay - You can get a Ukash voucher in values from £10 - £500 and pay using your internet bank.

FIG.08. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN ENGLISH.*



Las operaciones sobre las actividades ilegales se detectaron en el ordenador.

¡Atención!

El sistema operativo está bloqueado a causa de una violación. Sus acciones se consideran ilegales en España y la Unión Europea. Tu dirección IP: [redacted]
Esta IP "[redacted]" fue descubierto y reportado a las autoridades policiales. El usuario de este IP para usar el equipo para ver contenido pornográfico, pornografía infantil, bestialidad, y la violencia contra los niños.
El ordenador también cuenta con archivos de vídeo con pornografía ilegal, ya que nuestro sistema de exploración detecta los elementos de la violencia y la pornografía en la computadora. Además de su correo electrónico personal se han encontrado, envió mensajes de correo electrónico como spam, y también encontró correos electrónicos con carácter terrorista. Nuestros servidores tienen bloqueado el equipo deje de sus actividades ilegales.

Sus datos:

Para desbloquear el equipo, debe pagar una multa de $ 150,00. Le garantizamos la discrecion y la seguridad de su informacion al recibir el pago de la multa. Aqui hay formas de pago:
1) El pago "Ukash":
Debe introducir un codigo adquirido en la ventana que aparece en la pantalla. Despues de introducir un codigo valido, haga clic en Aceptar.
2) Pago "Paysafecard":
Debe introducir un codigo adquirido en la ventana que aparece en la pantalla. Despues de introducir un codigo valido, haga clic en Aceptar.
(Si tiene varios codigos, introduzcalos uno a uno en una linea). Despues de introducir el codigo para desbloquear el equipo de 1 a 3 dias de negocios. No violan la ley.
Si el sistema genera un error despues de ingresar el codigo que necesitas para enviar el codigo a traves de correo electronico - (E-MAIL info@stopkriminal.net). <

¿Dónde puedo conseguir Ukash?

Hay innumerables maneras de conseguir Ukash, por ejemplo, en tiendas, quioscos, a través de cajero automático, en línea oa través de un e-wallet (monedero electrónico). A continuación se muestra una lista de indicando donde se puede comprar Ukash en su país

Estaciones - ahora también está disponible en las siguientes estaciones: Agip, Avia, Esso, OMV, Q1 und Westfalen.

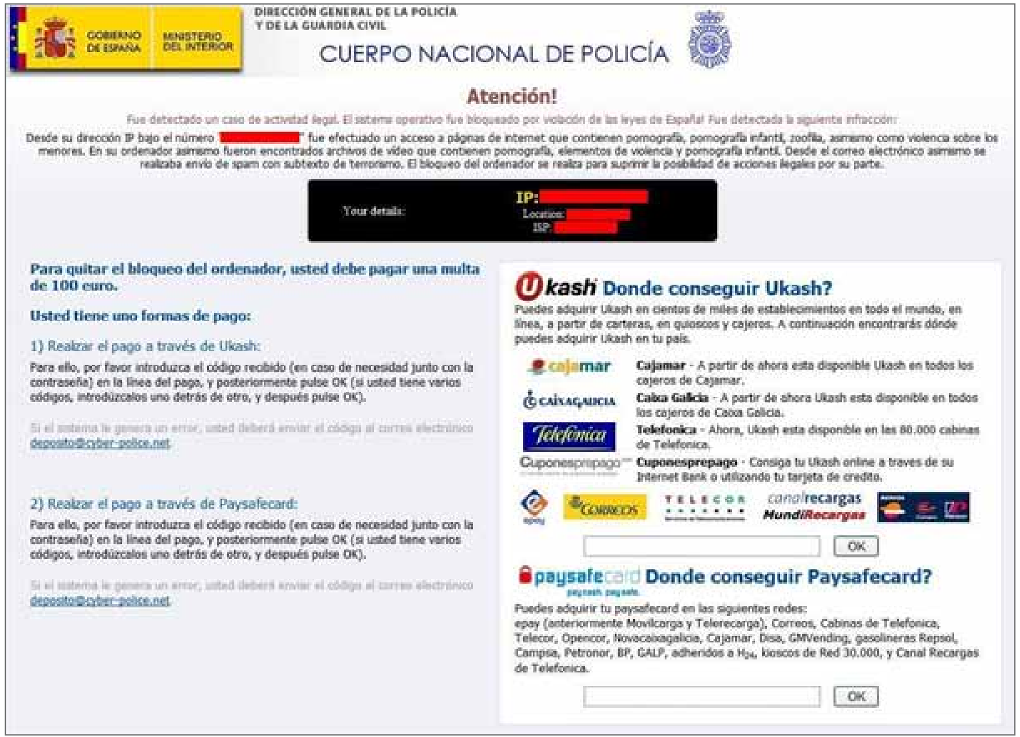
epay - Comprar Ukash en miles de supermercados y locutorios, donde se ve el logo.

FIG.09. *FAKE WARNING MESSAGE DISPLAYED BY THE TROJAN IN SPANISH.*

However, the attack became more complex over time. The malware went on to use ransomware techniques, ‘taking over’ infected computers by encrypting some of their content and forcing users to pay a fine or lose access. Basically, attackers took this functionality from the PGPCoder Trojan, a malicious code designed to encrypt files and keep them locked unless the victim agreed to pay a ransom.

The first versions of the new Police Virus only encrypted .doc files, and the encryption wasn’t too hard to crack, so it was possible to decrypt the files without the key. Now, however, a more sophisticated encryption is being used, and the decryption key is required to unlock the files. And not only that, the files are encrypted with a different key for each infected computer, so, unless you are able to access the server that stores all keys, it is absolutely impossible to access the files. Additionally, the range of files being encrypted is also most sophisticated. Some variants use a blacklist of extensions to encrypt; others use a whitelist of critical system files not to encrypt.

The question is, how much further can this malware go? In the end, the purpose of scareware is simply to frighten the user into paying the money (or, as attackers call it, "thefine"). A new variant of the Police Virus takes over the user's webcam. What for? Well, the malware has changed the screen it displayed so far to warn the user that 'illegal activity' had been traced to their computer…



GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA
Y DE LA GUARDIA CIVIL

CUERPO NACIONAL DE POLICÍA

Atención!

Fue detectado un caso de actividad ilegal. El sistema operativo fue bloqueado por violación de las leyes de España! Fue detectada la siguiente infracción:

Desde su dirección IP bajo el número [redacted] fue efectuado un acceso a páginas de internet que contienen pornografía, pornografía infantil, zoofilia, asimismo como violencia sobre los menores. En su ordenador asimismo fueron encontrados archivos de vídeo que contienen pornografía, elementos de violencia y pornografía infantil. Desde el correo electrónico asimismo se realizaba envío de spam con subtexto de terrorismo. El bloqueo del ordenador se realiza para suprimir la posibilidad de acciones ilegales por su parte.

Your details:
IP: [redacted]
Location: [redacted]
ISP: [redacted]

Para quitar el bloqueo del ordenador, usted debe pagar una multa de 100 euro.

Usted tiene uno formas de pago:

1) Realizar el pago a través de Ukash:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net

2) Realizar el pago a través de Paysafecard:

Para ello, por favor introduzca el código recibido (en caso de necesidad junto con la contraseña) en la línea del pago, y posteriormente pulse OK (si usted tiene varios códigos, introdúzcalos uno detrás de otro, y después pulse OK).

Si el sistema le genera un error, usted deberá enviar el código al correo electrónico deposito@cyber-police.net

Ukash Donde conseguir Ukash?

Puedes adquirir Ukash en cientos de miles de establecimientos en todo el mundo, en línea, a partir de carteras, en quioscos y cajeros. A continuación encontrarás dónde puedes adquirir Ukash en tu país.

Cajamar - A partir de ahora esta disponible Ukash en todos los cajeros de Cajamar.

Caixa Galicia - A partir de ahora Ukash esta disponible en todos los cajeros de Caixa Galicia.

Telefonica - Ahora, Ukash esta disponible en las 80.000 cabinas de Telefonica.

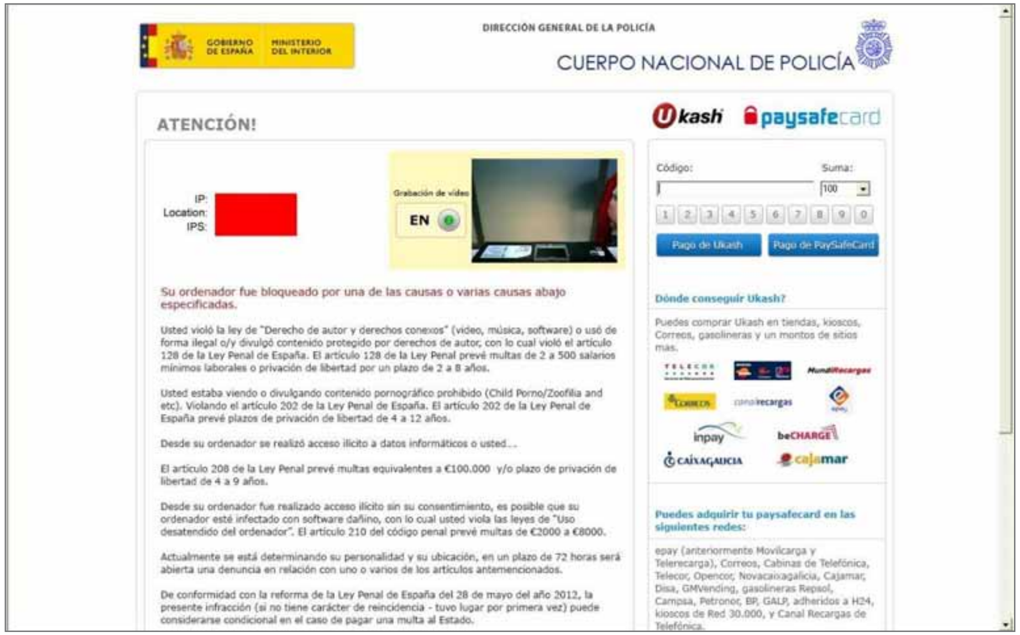
Cuponesprepago - Consiga tu Ukash online a traves de su Internet Bank o utilizando tu tarjeta de credito.

Donde conseguir Paysafecard?

Puedes adquirir tu paysafecard en las siguientes redes:
epay (anteriormente Movilcarga y Telerecarga), Correos, Cabinas de Telefonica, Telecor, Opencor, Novacaixagalicia, Cajamar, Disa, GMVending, gasolineras Repsol, Campsa, Petronor, BP, GALP, adheridos a H_{24}, kioscos de Red 30.000, y Canal Recargas de Telefonica.

FIG.10. *WARNING USED BY THE POLICE VIRUS UNTIL NOW.*

And replaced it with one including images taken by their webcam:



GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

DIRECCIÓN GENERAL DE LA POLICÍA

CUERPO NACIONAL DE POLICÍA

ATENCIÓN!

IP: [redacted]
Location:
IPS:

Su ordenador fue bloqueado por una de las causas o varias causas abajo especificadas.

Usted violó la ley de "Derecho de autor y derechos conexos" (video, música, software) o usó de forma ilegal o/y divulgó contenido protegido por derechos de autor, con lo cual violó el artículo 128 de la Ley Penal de España. El artículo 128 de la Ley Penal prevé multas de 2 a 500 salarios mínimos laborales o privación de libertad por un plazo de 2 a 8 años.

Usted estaba viendo o divulgando contenido pornográfico prohibido (Child Porno/Zoofilia and etc). Violando el artículo 202 de la Ley Penal de España. El artículo 202 de la Ley Penal de España prevé plazos de privación de libertad de 4 a 12 años.

Desde su ordenador se realizó acceso ilícito a datos informáticos o usted…

El artículo 208 de la Ley Penal prevé multas equivalentes a €100.000 y/o plazo de privación de libertad de 4 a 9 años.

Desde su ordenador fue realizado acceso ilícito sin su consentimiento, es posible que su ordenador esté infectado con software dañino, con lo cual usted viola las leyes de "Uso desatendido del ordenador". El artículo 210 del código penal prevé multas de €2000 a €8000.

Actualmente se está determinando su personalidad y su ubicación, en un plazo de 72 horas será abierta una denuncia en relación con uno o varios de los artículos antemencionados.

De conformidad con la reforma de la Ley Penal de España del 28 de mayo del año 2012, la presente infracción (si no tiene carácter de reincidencia - tuvo lugar por primera vez) puede considerarse condicional en el caso de pagar una multa al Estado.

Código:
Suma: 100

Dónde conseguir Ukash?

Puedes comprar Ukash en tiendas, kioscos, Correos, gasolineras y un montos de sitios mas.

Puedes adquirir tu paysafecard en las siguientes redes:

epay (anteriormente Movilcarga y Telerecarga), Correos, Cabinas de Telefónica, Telecor, Opencor, Novacaixagalicia, Cajamar, Disa, GMVending, gasolineras Repsol, Campsa, Petronor, BP, GALP, adheridos a H24, kioscos de Red 30.000, y Canal Recargas de Telefónica.

FIG.11. *NEW WARNING USED BY THE POLICE VIRUS, SHOWING THE IMAGES CAPTURED BY THE COMPUTER'S WEBCAM.*

As you can see, the page includes a small window showing the images taken by the webcam in real time, together with the text: "Live recording". However, no images are actually being recorded or sent to law enforcement. The warning just displays the images currently captured by the webcam. Users, however, don't know this, and most of them will start to panic and be willing to pay the 'fine' to stop law enforcement from spying on them, as they are made to believe. As previously said, this new variant doesn't use encryption, probably because cyber-criminals think that the webcam trick is enough to scare potential victims.

Social Networks

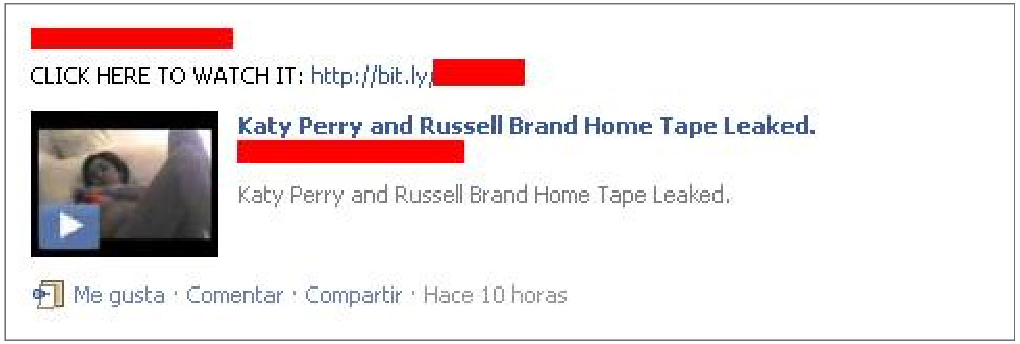
Facebook continues its reign as the number one social networking site but it also is a favorite target of cyber-crooks. In January, a worm was discovered that had stolen over 45,000 Facebook login credentials. Researchers fear that the criminals used these 'infected' accounts to send links to people's Facebook friends, spreading the computer worm further.

Meanwhile, what does Facebook do to protect users? Well, the good news is that at least they take the fight against cyber-crime seriously.

FIG.12. *FACEBOOK REVEALED THE NAMES OF THE SUSPECTS BEHIND THE KOOBFACE ATTACK.*

In January, Facebook finally revealed the full names and online names of the perpetrators behind the Koobface botnet that has affected the social site for a few years. The identities of those responsible for the attacks are: Stanislav Avdeyko (leDed), Alexander Koltysehv (Floppy), Anton Korotchenko (KrotReal), Roman P. Koturbach (PoMuc) and Svyatoslav E. Polichuck (PsViat and PsycoMan). Unfortunately, the men live comfortable lives in St. Petersburg (Russia), and have become rich from their various online schemes. All five have yet to be charged with a crime, nor has any law enforcement agency confirmed they are under investigation.

Despite the myriad malware and spam scams preying on Facebook, curiosity still gets users into trouble. This year we saw a new scam involving a supposed tape of Katy Perry and Russell Brand posted to the walls of hundreds of users. The malicious post looked as follows:



[redacted]

CLICK HERE TO WATCH IT: http://bit.ly/[redacted]

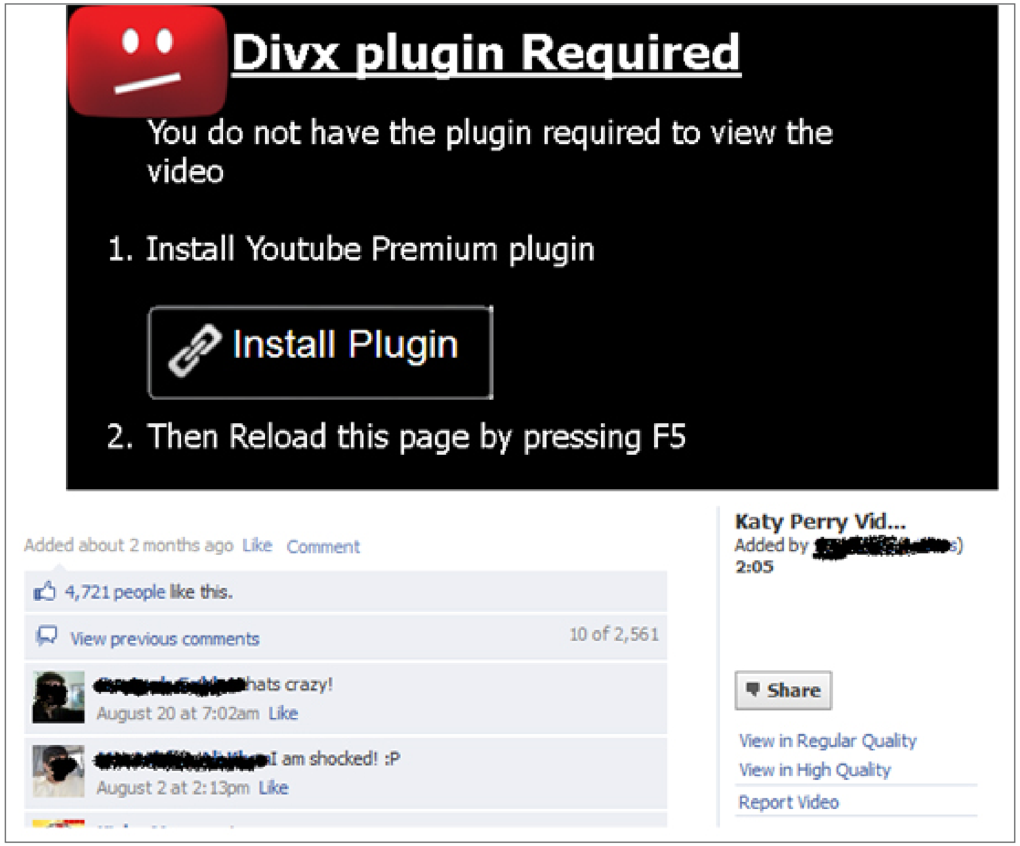
Katy Perry and Russell Brand Home Tape Leaked.

[redacted]

Katy Perry and Russell Brand Home Tape Leaked.

Me gusta · Comentar · Compartir · Hace 10 horas

FIG.13. *MALICIOUS MESSAGE.*



Divx plugin Required

You do not have the plugin required to view the video

1. Install Youtube Premium plugin

Install Plugin

2. Then Reload this page by pressing F5

Added about 2 months ago Like Comment

4,721 people like this.

View previous comments 10 of 2,561

[redacted]hats crazy!
August 20 at 7:02am Like

[redacted]I am shocked! :P
August 2 at 2:13pm Like

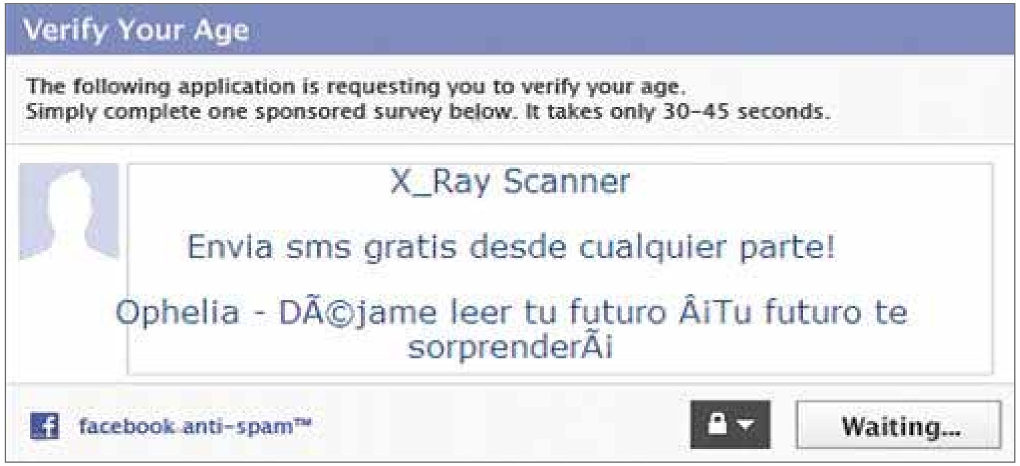
Katy Perry Vid...
Added by [redacted]s)
2:05

Share

View in Regular Quality
View in High Quality
Report Video

FIG.14. *MALICIOUS WEBSITE.*

However, all the 'Likes', comments, etc. displayed on the page were false as the 'page' itself didn't exist, it was simply an image. If you clicked on "Install Plugin" and you were using Firefox or Chrome, the worm installed a browser plug-in and used it to post the scam to the victims' friends' pages. On Internet Explorer, as there was no plug-in that could carry out this task, the worm displayed an age verification page to access an application called 'X-Ray Scanner'.



Verify Your Age

The following application is requesting you to verify your age.
Simply complete one sponsored survey below. It takes only 30-45 seconds.

X_Ray Scanner

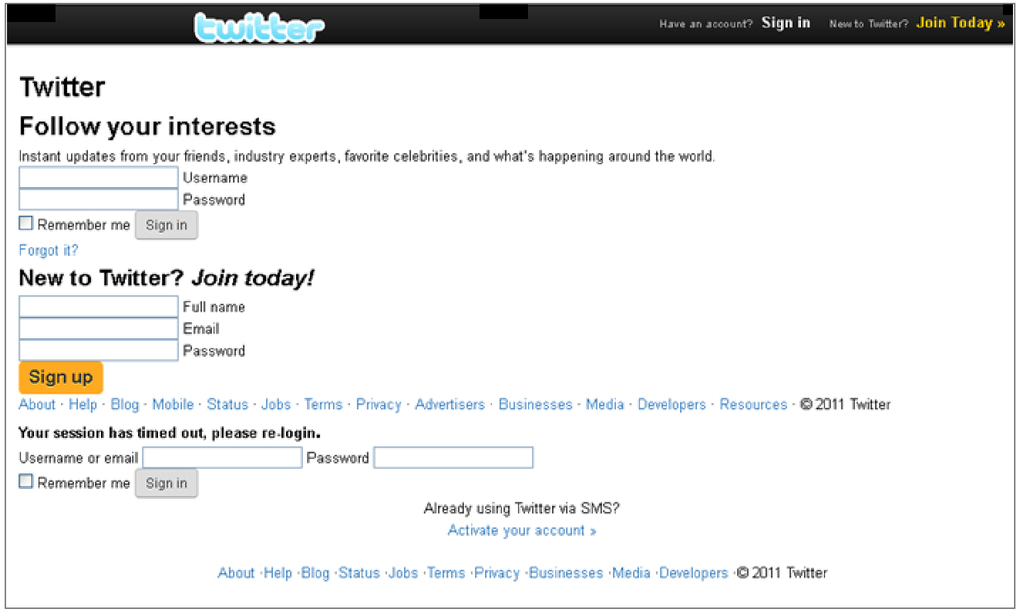
Envia sms gratis desde cualquier parte!

Ophelia - DÃ©jame leer tu futuro ÂiTu futuro te sorprenderÃi

FIG.15. *MESSAGE.*

As you can see, the page looked like a Facebook page to trick users into believing they were still on the social networking site. If the victim clicked any of the links they were taken to a page where they were asked to enter their cell phone number. However, after doing so, they started receiving unwanted premium rate text messages.

One of the primary objectives cyber-crooks have when launching attacks on social media sites is to gain access to users' accounts so that they can impersonate them and access their personal details or information shared with other users. On Twitter, for example, accessing a user's account will allow them to send direct messages (DMs) to the victims' friends. A typical example would be as follows: You receive a DM from one of your contacts informing you that someone has just posted some embarrassing pictures of you. If you click the link, you'll be taken to the following page:



Twitter

Follow your interests

Instant updates from your friends, industry experts, favorite celebrities, and what's happening around the world.

Username
Password
□ Remember me Sign in
Forgot it?

New to Twitter? *Join today!*

Full name
Email
Password
Sign up

About · Help · Blog · Mobile · Status · Jobs · Terms · Privacy · Advertisers · Businesses · Media · Developers · Resources · © 2011 Twitter

Your session has timed out, please re-login.

Username or email Password
□ Remember me Sign in

Already using Twitter via SMS?
Activate your account »

About ·Help ·Blog ·Status ·Jobs ·Terms ·Privacy ·Businesses ·Media ·Developers ·© 2011 Twitter

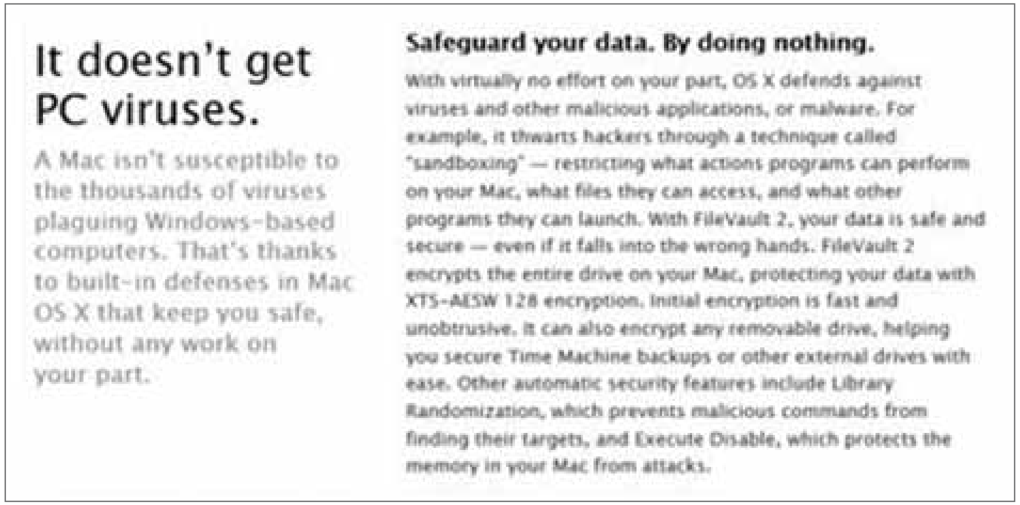
FIG.16. *PHISHING PAGE THAT STEALS TW ITTER CREDENTIALS.*

This page informs you that your Twitter session has timed out and asks that you log in again. To make the phishing scam look as real as possible, all the links displayed on the page are actually Twitter links except for the "Sign in" and "Sign up" buttons, which will transmit the user data to the attackers. Once they have your Twitter login and password, they will begin sending the same misleading Twitter DM to all of your followers. This way, they will steal their Twitter login as well, and use their accounts to spread malware, send spam or turn those credentials into money by selling them to other cyber-crooks.

Social networking site **LinkedIn** had 6.5 million user passwords stolen and leaked online. Fortunately enough, however, these passwords were not stored in plain text files, but were encrypted. The bad news is that there was no other additional protection, so in case you haven't already done so, we advise that you change your LinkedIn password right now. And if you use that password for any other service as well, change it too, and always use different passwords for different programs and services.

Mac

Every time we discuss **Mac** threats, we present you with the cases that most caught our attention. Luckily enough, these infections are not massive, as despite the growth of Mac malware, the PC remains the biggest target for cyber-criminals. Unfortunately, many Mac users still believe they are immune to threats, even though little by little people, even at Apple, are beginning to realize that that is not the case. The Apple page that explains the reasons why Macs are better than PCs previously boasted that Mac systems 'don't get viruses' (a false statement, since macro viruses, for example, affect both platforms).



It doesn't get PC viruses.

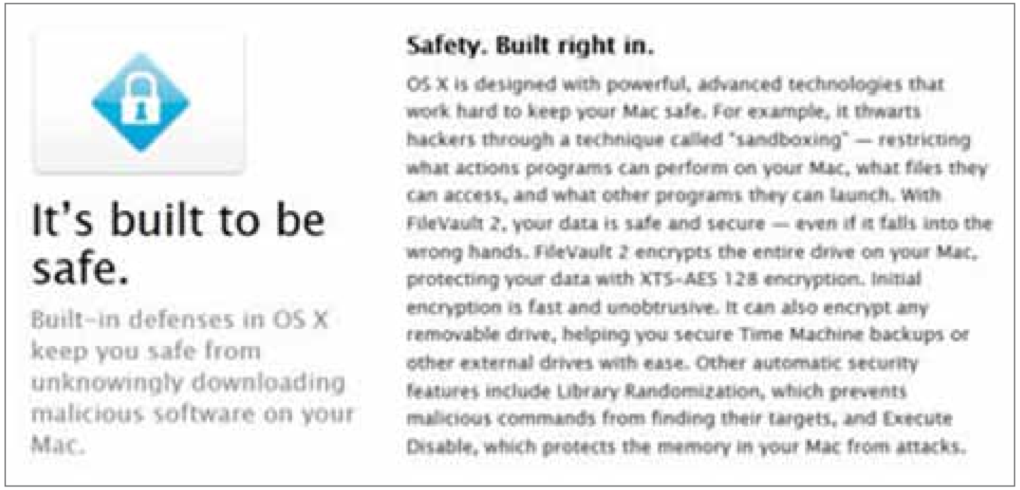
A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part.

Safeguard your data. By doing nothing.

With virtually no effort on your part, OS X defends against viruses and other malicious applications, or malware. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch. With FileVault 2, your data is safe and secure — even if it falls into the wrong hands. FileVault 2 encrypts the entire drive on your Mac, protecting your data with XTS-AESW 128 encryption. Initial encryption is fast and unobtrusive. It can also encrypt any removable drive, helping you secure Time Machine backups or other external drives with ease. Other automatic security features include Library Randomization, which prevents malicious commands from finding their targets, and Execute Disable, which protects the memory in your Mac from attacks.

FIG.17. *APP LE'S WEBSITE SAID ITS OPERATING SYSTEM WAS VIRUS FREE.*

However, it seems that Apple is beginning to acknowledge the truth, as they have replaced the previous text with this one:



It's built to be safe.

Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac.

Safety. Built right in.

OS X is designed with powerful, advanced technologies that work hard to keep your Mac safe. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch. With FileVault 2, your data is safe and secure — even if it falls into the wrong hands. FileVault 2 encrypts the entire drive on your Mac, protecting your data with XTS-AES 128 encryption. Initial encryption is fast and unobtrusive. It can also encrypt any removable drive, helping you secure Time Machine backups or other external drives with ease. Other automatic security features include Library Randomization, which prevents malicious commands from finding their targets, and Execute Disable, which protects the memory in your Mac from attacks.

FIG.18. *APP LE REMOVES CLAIM OF VIRUS IMMUNITY.*

This change is probably related to the recent outbreak of the Flashback Trojan, a malware specimen responsible for the single most significant malware infection to ever hit the Mac community. This malware infected up to 600,000 Mac computers around the world, creating the largest botnet ever to target Apple computers. One of the Trojan's most unique features was that before infecting a computer, it checked to see if it had some kind of antivirus installed. If the computer was protected, Flashback didn't infect it; otherwise, it infected the Mac and triggered its payload.

This attack has once again demonstrated that, contrary to popular belief, Macs are in fact not immune to virus infection and malware, a myth largely exploited by cyber-criminals.

Cyber-crime

In a typical phishing attack, offenders usually steal consumers' identities to impersonate them and empty their bank accounts. However, the year started off with quite an unusual case. The first mayor cyber-crime of 2012 took place in South Africa, as hackers got away with about $6.7 million from South African Postbank. The robbery took place over three days, from Jan 1 to Jan 3. The hackers, who had planned the attack for months, used stolen login details from a Postbank teller to transfer the stolen money into multiple bank accounts that were opened across the country.

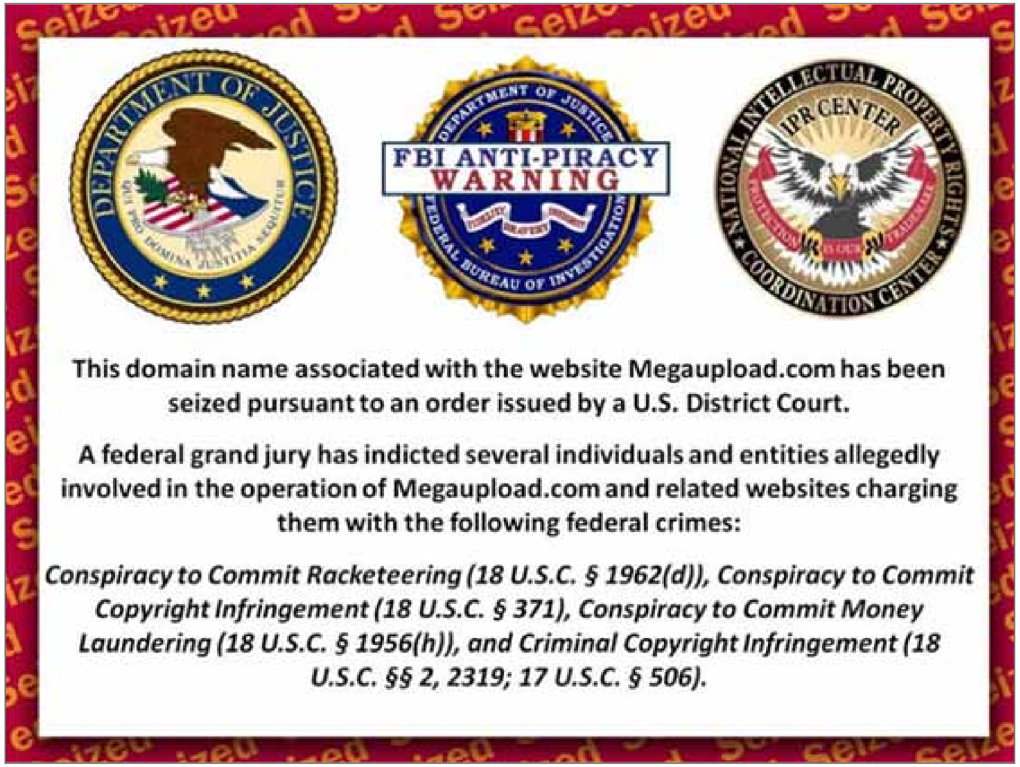
Megaupload case

In January, the FBI shut down the popular Megaupload file-sharing website, charging the founders for “copyright infringement” (you can read the FBI press release here, with more information about the case). If convicted, those involved face up to 50 years in prison on all charges.

Hacker group Anonymous reacted swiftly to the news, launching DDoS attacks on several Web pages, including the sites of the U.S. Department of Justice, RIAA (Recording Industry Association of America) and Universal Music Group.

Going back to the press release, the FBI stated that:
“This case is part of efforts being undertaken by the Department of Justice Task Force on Intellectual Property (IP Task Force) to stop the theft of intellectual property.”

Well, as we all know, in the ‘real world’ cyber-criminals are siphoning millions of dollars into their pockets every year by attacking hundreds of thousands of computers. However, it seems that authorities consider copyright infringement to be far more serious. As always, this is a question of priorities, and it seems that in this case the highest priority of law enforcement agencies is not exactly to protect the individual.


Seized
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
FBI ANTI-PIRACY WARNING
FEDERAL BUREAU OF INVESTIGATION
NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER
IPR CENTER

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by a U.S. District Court.

A federal grand jury has indicted several individuals and entities allegedly involved in the operation of Megaupload.com and related websites charging them with the following federal crimes:

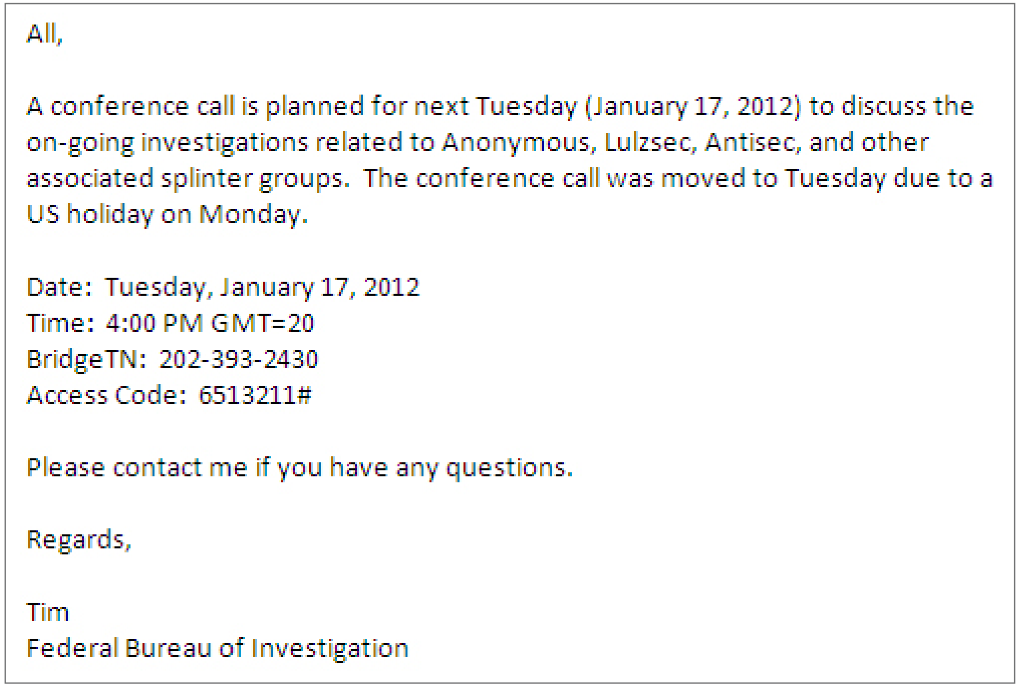
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

FIG.19. *IMAGE DISPLAYED ON ACCESSING MEGAUPLOAD’S SITE AFTER THE FB I’S INTERVENTION.*

Both Anonymous and LulzSec have been very busy over the last year.

In January, in the wake of controversial legislation such as SOPA and ACTA, the hacking group posted the following Twitter message: “If you hated #SOPA, you’ll burst into flames about #ACTA http://is.gd/Bo68r4 Negotiated in secret. iPod searches at border crossings.” Soon after, they launched an unprecedented string of attacks on government and business sites around the world.

In February, they recorded and released a sensitive conference call between the FBI and Scotland Yard. Amid growing speculation about how the hackers had been able to obtain the recording, Anonymous published an email purportedly sent by an FBI agent to international law enforcement agencies, with a phone number and password for accessing the call.



All,

A conference call is planned for next Tuesday (January 17, 2012) to discuss the on-going investigations related to Anonymous, Lulzsec, Antisec, and other associated splinter groups. The conference call was moved to Tuesday due to a US holiday on Monday.

Date: Tuesday, January 17, 2012
Time: 4:00 PM GMT=20
BridgeTN: 202-393-2430
Access Code: 6513211#

Please contact me if you have any questions.

Regards,

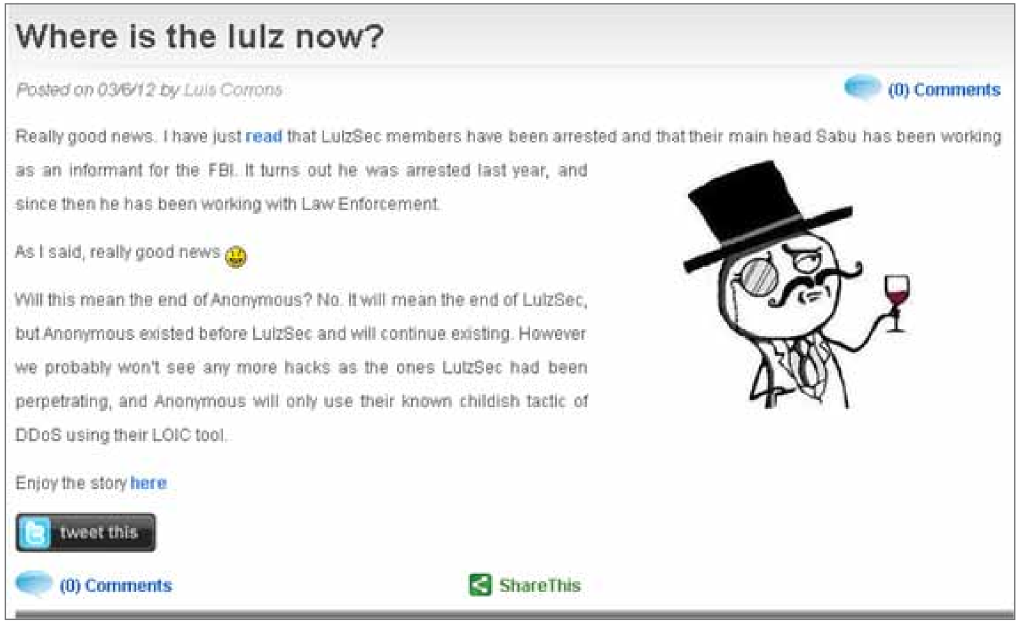
Tim
Federal Bureau of Investigation

FIG.20. *FB I MESSAGE INTERCEPTED BY ANONYMOUS.*

In February, Anonymous published the source code of PCAnywhere and Norton, stolen in 2006. The theft was committed by a group of cyber-criminals who aimed to blackmail Symantec. However, once it became clear the American security firm was not going to give in to the blackmail, they decided to pass the data to Anonymous to make it public.

In March, several alleged members of LulzSec were arrested in the course of a police operation launched in 2011. It was immediately discovered that Sabu, the alleged leader of LulzSec, had been secretly arrested by the FBI and had been working for the government to arrest other members of the hacker collective.

Luis Corrons, technical director of PandaLabs, lauded the arrests on the laboratory's blog and Anonymous reacted swiftly by breaking into the external server that hosted the blog and defacing it. Anonymous make a big deal about freedom of speech, calling themselves 'the Voice of Free Speech' and 'aggressive proponents for the Freedom of Speech'. However, in reality, the selfappointed defenders of free speech shut down people's websites when they don't like what they read. Uhmm… It is ironic, isn't it? It seems that Anonymous are only interested in defending freedom of speech when it serves their own interests. Actually, a British journalist asked them about this apparent contradiction on Tweeter but his question, unsurprisingly, went unanswered.



Where is the lulz now?

Posted on 03/6/12 by Luis Corrons

(0) Comments

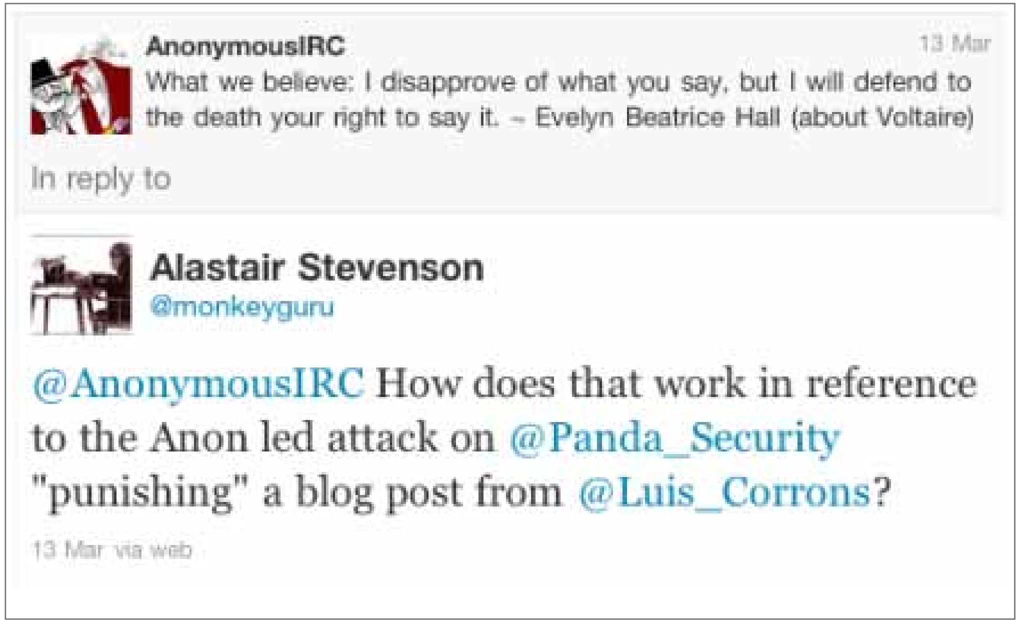
Really good news. I have just read that LulzSec members have been arrested and that their main head Sabu has been working as an informant for the FBI. It turns out he was arrested last year, and since then he has been working with Law Enforcement.

As I said, really good news

Will this mean the end of Anonymous? No. It will mean the end of LulzSec, but Anonymous existed before LulzSec and will continue existing. However we probably won't see any more hacks as the ones LulzSec had been perpetrating, and Anonymous will only use their known childish tactic of DDoS using their LOIC tool.

Enjoy the story here

FIG.21. *PANDALABS BLOG POST PRAISING THE LATEST LULZSEC ARRESTS.*



AnonymousIRC 13 Mar

What we believe: I disapprove of what you say, but I will defend to the death your right to say it. – Evelyn Beatrice Hall (about Voltaire)

In reply to

Alastair Stevenson
@monkeyguru

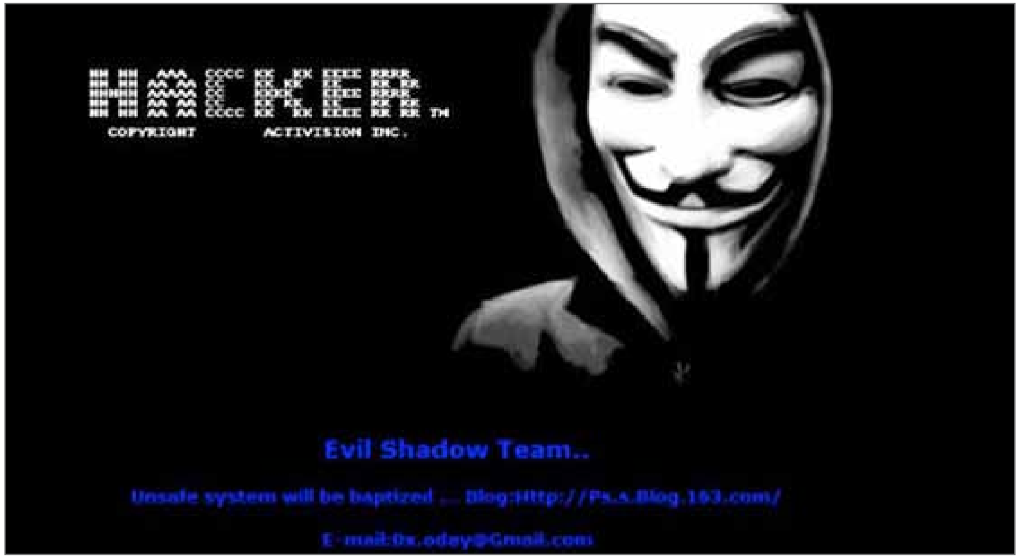
@AnonymousIRC How does that work in reference to the Anon led attack on @Panda_Security "punishing" a blog post from @Luis_Corrons?

13 Mar via web

FIG.22. *UNANSWERED QUESTION TO ANONYMOUS FROM A BRITISH JOURNALIST.*

One day later, they launched an attack on the main website of the Vatican, rendering it inaccessible. And five days later they attacked the Vatican again, this time breaking into the Vatican Radio database and posting user names and passwords.

Unfortunately, Anonymous and Lulzsec are not the only ones who launch these types of attacks. In February, the online Microsoft Store in India was compromised by a group of Chinese hackers. The team of hackers defaced the site and stole data from thousands of Microsoft customers.

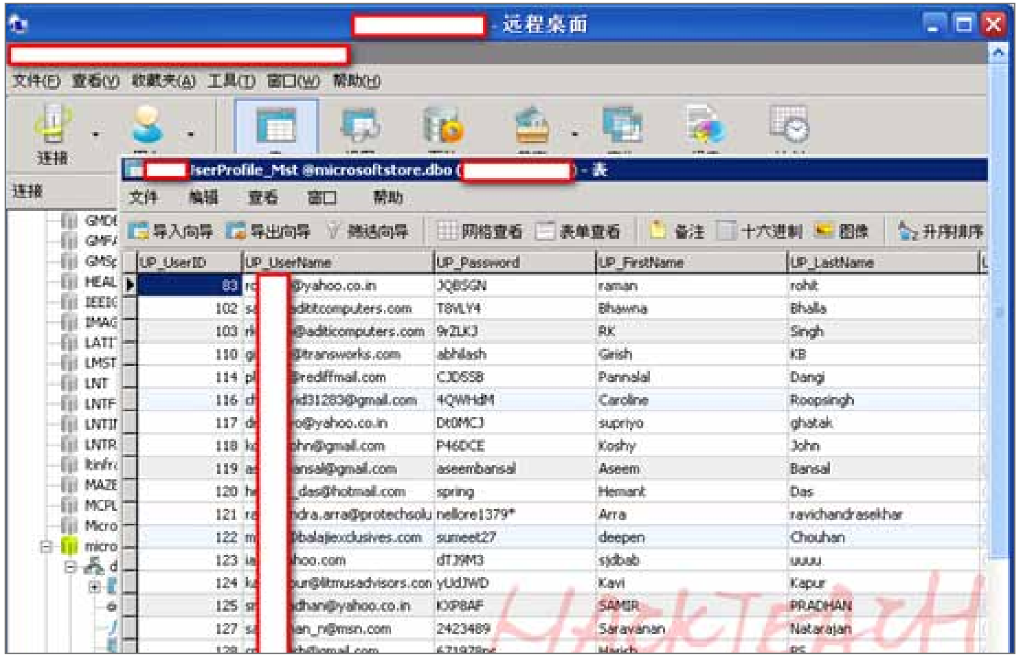


Evil Shadow Team..

Unsafe system will be baptized ... Blog:Http://Ps.s.Blog.163.com/

E-mail:0x.0day@Gmail.com

FIG.23. *MI CROSOFT INDIA WEB STORE HACKED.*


文件(F) 查看(V) 收藏夹(A) 工具(T) 窗口(W) 帮助(H)
连接
连接
GMD
GMF
GMS
HEAL
IEEI
IMAG
LATT
LMST
LNT
LNTF
LNTI
LNTR
ltinfr
MAZE
MCPL
Micro
micro
文件 编辑 查看 窗口 帮助
导入向导 导出向导 筛选向导 网格查看 表单查看 备注 十六进制 图像 升序排序
HACKTEACH

[redacted] - 远程桌面

[redacted]

[redacted]serProfile_Mst @microsoftstore.dbo ([redacted]) - 表

UP_UserID	UP_UserName	UP_Password	UP_FirstName	UP_LastName
83	rc[redacted]@yahoo.co.in	JQBSGN	raman	rohit
102	sa[redacted]adititcomputers.com	T8VLY4	Bhawna	Bhalla
103	ri[redacted]@aditicomputers.com	9rZLKJ	RK	Singh
110	gi[redacted]@transworks.com	abhilash	Girish	KB
114	pl[redacted]@rediffmail.com	CJDSS8	Pannalal	Dangi
116	ch[redacted]nd31283@gmail.com	4QWHdM	Caroline	Roopsingh
117	de[redacted]o@yahoo.co.in	Dt0MCJ	supriyo	ghatak
118	ko[redacted]ohn@gmail.com	P46DCE	Koshy	John
119	as[redacted]ansal@gmail.com	aseembansal	Aseem	Bansal
120	he[redacted]_das@hotmail.com	spring	Hemant	Das
121	ra[redacted]ndra.arra@protechsolu	nellore1379*	Arra	ravichandrasekhar
122	m[redacted]@balajiexclusives.com	sumeet27	deepen	Chouhan
123	ia[redacted]hoo.com	dTJ9M3	sjdbab	uuuu
124	ka[redacted]our@litmusadvisors.con	yUdJWD	Kavi	Kapur
125	sn[redacted]dhan@yahoo.co.in	KXP8AF	SAMIR	PRADHAN
127	sa[redacted]an_n@msn.com	2423489	Saravanan	Natarajan
128	cr[redacted]ch@gmail.com	[illegible]	[illegible]	RS

FIG.24. *SCREENSHOT SHOWN BY CYBER-CRIMINALS TO PROVE THEY HAD STOLEN DATA FROM MICROSOFT'S CUSTOMERS.*

Also in February, it was reported that attackers stole information from millions of users of YouPorn, one of the world's most popular porn video websites. This data was posted on Pastebin, a popular dumping ground for cyber-attackers, potentially compromising the security of thousands of users who reuse passwords on multiple sites.

In March, it was revealed that Michael Jackson's entire back catalogue had been stolen from Sony Music, including some previously unreleased material. This follows last year's attacks on Sony that exposed personal data from more than 100 million accounts at Sony Online Entertainment and the PlayStation Network (PSN).

FIG.25. *MI CHAEL JACKSON'S ENTIRE MUSIC CATALOGUE STOLEN IN SONY MUSIC HACK.*

It seems that the cyber-criminals who hacked into Sony Music's systems thought it would be easy to access the company's information. Unfortunately, they were right, although in this case they were arrested and are due to stand trial in 2013.

FIG.26. *ROGUE GOOGLE CHROME EXTENSION INJECTED ADS INTO WIKIPEDIA.*

Wikipedia suffered an attack that forced the organization to release a statement warning its users that seeing ads on its website meant their computers had been infected. The attackers used a rogue Google Chrome add-on that inserted ads into the site. The foundation behind Wikipedia took the opportunity to remind users that Wikipedia is funded by donors and they don't run advertisements on their pages.

We have mentioned on many occasions how cyber-criminals are becoming more sophisticated and are constantly improving their techniques. An example of this was the appearance of a new variant of the **SpyEye** banking Trojan, which hijacked the webcam of infected computers. What for? To monitor how victims reacted when they read the socially-engineered messages displayed by the malware on spoof banking websites, and see how effective their social engineering turned out to be.

Nissan Motor Company fell victim to a breach of employee information. The attackers compromised user IDs and passwords, which seems to indicate that the malware was designed for industrial espionage.

Khosrow Zarefarid, an Iranian security expert, discovered a critical flaw in Iran's banking system, providing affected institutions with the details. When the affected banks didn't respond, he hacked 3 million accounts across at least 22 banks. He then dropped these details – including card numbers and PINs– on his blog. Google took down Zarefarid's Blogger-hosted blog, whereas affected institutions warned customers to change their debit card PINs.

Hackers, perhaps from Eastern Europe, stole the personal details of over 900,000 of Utah's Medicaid beneficiaries from a server operated by Utah's Health Department

The Dropbox filesharing service suffered a huge security breach that led to theft of usernames and passwords from thousands of users. According to reports, it was users themselves that raised the alarm after starting to receive spam at addresses used only for Dropbox.

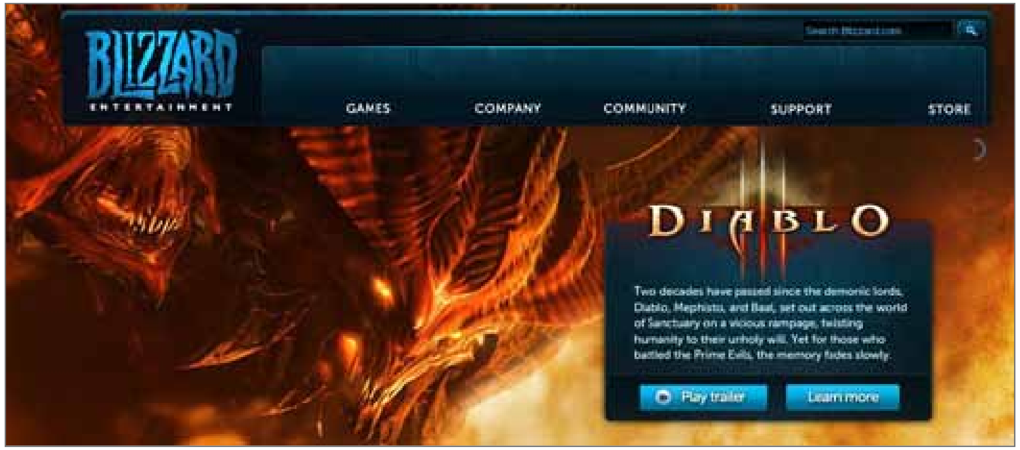
FIG27. *DROPBOX.*

In South Korea, mobile carrier KT Corporation suffered a data breach which exposed personal information of over 8.7 million customers. Shortly after the hack, South Korean police announced the arrest of two programmers who were allegedly involved with the theft.

The Reuters news service suffered two successful hacker attacks on its blogging platform. The news agency was first hit at the beginning of August when a false interview with a Syrian rebel leader was published. As a result, Reuters took its blogging platform offline for a few hours. Two weeks later, a similar incident took place involving an article that falsely claimed Saudi Arabia's foreign minister Saud al-Faisal had died.

FIG.28. *REUTERS.*

Blizzard, the American video game developer and publisher of titles like World of Warcraft, Starcraft or Diablo, confirmed in August that they had suffered a security breach and urged users to change the login credentials to its online gaming service Battle.net. They confirmed that hackers were able to obtain users' email addresses and encrypted passwords.



Two decades have passed since the demonic lords, Diablo, Mephisto, and Baal, set out across the world of Sanctuary on a vicious rampage, twisting humanity to their unholy will. Yet for those who battled the Prime Evils, the memory fades slowly.

FIG.29. *BLIZZARD.*

In September, it was revealed that Adobe had also been attacked by hackers. In this case though, the attackers were not interested in stealing customer data, but in accessing one of the company's internal servers to be able to sign their malware with a valid digital certificate from Adobe. The attack took place in July.

U.S. insurer Nationwide suffered a data breach that revealed the personal information of over one million customers and employees. This information included their full names, home addresses, social security numbers and other personal information.

In addition to private companies, public institutions have also suffered targeted attacks and data breaches. In November, the UN nuclear watchdog International Atomic Energy Agency was attacked by a group called "Parastoo", which later published the stolen data on Pastebin. Also in November, the Japan Aerospace Exploration Agency said it had found evidence that one of its computers had been infected by a virus that collected information and transmitted it externally. The computer in question contained specifications and information on the agency's solid-fuel rocket program.

Nevertheless, apart from all these attacks, there has also been good news in the fight against cyber-crime: Interpol has announced they are planning to open a "Global Cybercrime Center" in Singapore in 2014 to improve global cooperation among law enforcement.

UK cyber-crook Edward Pearson was jailed for 26 months after stealing the personal information of about 8 million people. Also in the UK, Lewys Martin, a Brit who distributed a Trojan horse that posed as a patch for the popular Call of Duty game, was jailed for 18 months for stealing user data and selling it on the black market.

Ryan Cleary - a 19-year-old from Essex, United Kingdom, who was arrested last year for participating in various LulzSec attacks-, was sent back to jail for breaching his bail conditions. Cleary, who isn't allowed to access the Internet, used it last Christmas to contact Hector Xavier Monsegur (a.k.a "Sabu"), the LulzSec hacker who the FBI used as a secret informant for months last year.

Higinio O. Ochoa III, from Galveston, Texas, was arrested by the FBI for allegedly hacking into the websites of several U.S. law enforcement agencies and releasing the personal information (names, addresses and phone numbers) of dozens of police officers. In this case, Ochoa's arrest was largely due to his own mistake, as he twitted a photo of his girlfriend's breasts with a sign attached to her belly that mentioned the hacker's online name ("w0rmer"). The picture was taken with an iPhone 4, which contains a GPS device that inserts GPS co-ordinates in all pictures taken. As a result, the police only had to use the GPS co-ordinates embedded in the photo to trace the exact street and house where the picture was taken. This served to identify the woman, who happened to be Ochoa's Australian girlfriend.

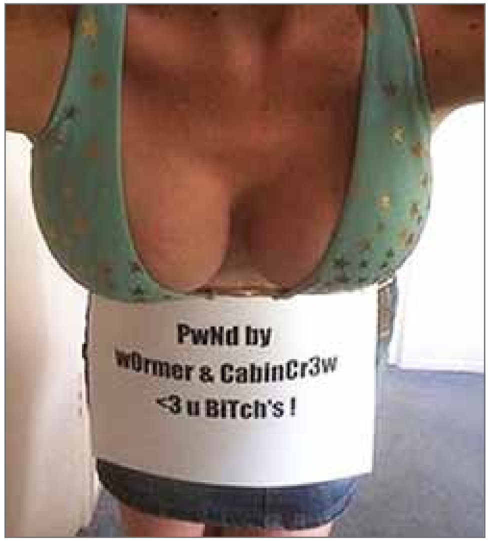


FIG.30. *PICTURED POSTED BY HIGINIO O. OCHOA III THAT LED TO HIS ARREST.*

In April, the FBI announced the arrest of John Anthony Borell III, another alleged member of Anonymous, in Ohio. On this occasion, the FBI found Twitter direct messages and tweets in which Borell admitted to taking down a number of websites.

Junaid Hussain of Birmingham, United Kingdom, the leader of the TeaMp0isoN collective, pleaded guilty to hacking into the Gmail account of former UK Prime Minister Tony Blair. A few weeks later he was sentenced to six months in prison.

FIG.31. *TONY BLAIR'S EMAIL ACCOUNT HACKED BY GROUP TEAMPOISON.*

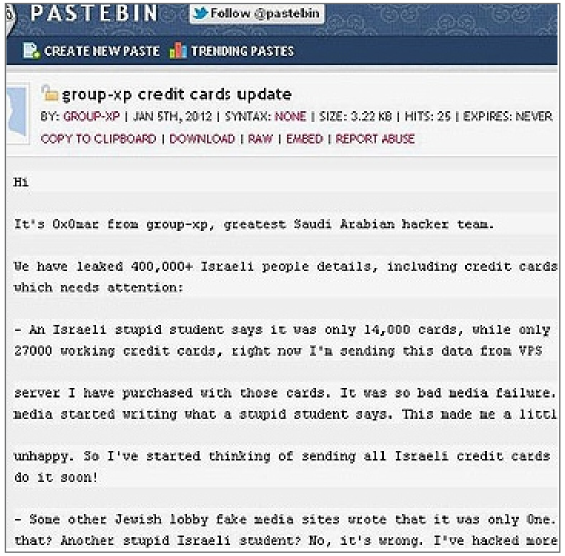
Hacker Joshua Schichtel, of Phoenix, United States, received a 30-months prison sentence for hijacking 72,000 computers. More precisely, he was paid to install or have installed malware on those computers. In one case, a customer paid him $ 1,500 to install a Trojan on every computer on his botnet.

Christopher Chaney, who made headlines by hacking into the personal online accounts of such stars as Scarlett Johansson or Mila Kunis, was sentenced to 10 years in jail for illegally accessing the email accounts of more than 50 people in the entertainment industry.

All of these stories provide clear examples of the way the fight against cyber-crime is changing. For example, Japan's National Police Agency (Japan's equivalent to the American FBI) offered its first-ever monetary reward (US$36,000) for a wanted hacker. Up until now, this type of reward was reserved for cases involving crime like murder and arson, never for cyber-criminals.

Cyber-war

The year 2012 has seen some remarkable events in the cyber-war arena. On January 2, thousands of credit card numbers belonging to Israeli citizens were stolen. A Saudi hacker, calling himself 0x0mar, took credit for the hack attack, although further investigation revealed the hacker's real identity: 19-year-old computer science student Omar Habib, born in the United Arab Emirates, but currently living in Mexico. Later on, 0x0mar denied the allegations



group-xp credit cards update

BY: GROUP-XP | JAN 5TH, 2012 | SYNTAX: NONE | SIZE: 3.22 KB | HITS: 25 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
Hi

It's 0x0mar from group-xp, greatest Saudi Arabian hacker team.

We have leaked 400,000+ Israeli people details, including credit cards
which needs attention:

- An Israeli stupid student says it was only 14,000 cards, while only
27000 working credit cards, right now I'm sending this data from VPS

server I have purchased with those cards. It was so bad media failure.
media started writing what a stupid student says. This made me a littl

unhappy. So I've started thinking of sending all Israeli credit cards
do it soon!

- Some other Jewish lobby fake media sites wrote that it was only One.
that? Another stupid Israeli student? No, it's wrong. I've hacked more
```

32. *SCREENSHOT FROM 0X0MAR'S ONLINE CLAIM OF AN ISRAELI HACK ATTACK.*

Soon after, a war began to brew between the hackers of Israel and Saudi Arabia: Arab hackers paralyzed the websites of the Tel Aviv Stock Exchange, El Al Airlines and several Israeli banks, whereas Israeli hackers brought down the websites of both the Saudi Stock Exchange (Tadawul) and the Abu Dhabi Securities Exchange (ADX) in retaliation, claiming to act on behalf of the Israeli Defense Forces and vowing to strike Arab countries' websites related to their economies unless attacks on Israeli sites were halted.

To make matters worse, Tariq al-Suwaidan, one of Kuwait's most famous TV preachers, called for a cyber-war against Israel. He used his Twitter account to call on all Muslim hackers to unite against Israel in a "cyber-jihad against Zionist enemy, which will be rewarded by God".
Also in the Middle East, thousands of emails received and sent by Syrian president Bashar al-Assad were stolen by Saudi hackers.

In the Far East, it was reported that Japan's Defense Ministry had commissioned Fujitsu to develop a cyber-weapon virus capable of tracing and disabling computers being used in cyber-attacks against the country. The information is a bit confusing, and it looks like a bad idea anyway as, even if created with the best of intentions, there may be adverse effects that turn the weapon against its creators or the entire world. In any event, users of Panda Security's solutions can set their mind at ease, as we will detect every virus created, either by public or private writers.

Let's look now at two of the countries that usually take the spotlight in this section: China and the United States. In January, it was revealed that Chinese hackers had deployed a Trojan targeting smart card readers used by the U.S. Department of Homeland Security. These cards are a standard means of granting users access to intranets, networks and physical locations. Had the hackers actually managed to crack the smart cards, they could easily access lots of confidential information.

Also in China, we learned that a group of hackers managed to penetrate the corporate network of Nortel, using passwords stolen from seven top Nortel executives, including the CEO. Apparently, they had been spying on the company from as far back as 2000.

In most cyber-war or cyber-espionage operations all you can do is speculate about who is behind the attack. It is extremely unlikely that a country openly admits to being responsible for carrying out this type of action. However, things might be c websites being
used by Al Qaeda's affiliate in Yemen.

More specifically, the U.S. cyber experts hacked into Jihadist Web pages and substituted material that bragged about killing Americans with information about Muslim civilians killed in terrorist strikes.

Meanwhile, in South Korea, intelligence sources accused North Korea of running a special unit of elite hackers to steal military secrets and sabotage information systems of Seoul.

Flame

The Flame computer virus has been the highlight of the year without any doubts. Flame is a complex piece of malware used for information gathering and espionage in Middle East countries.

This malicious code is most likely created by a government or intelligence agency, and is clearly tied to the infamous Stuxnet malware (a Trojan reportedly designed and launched by the U.S. and Israeli governments in an attempt to sabotage Iran's nuclear program). Targeted attacks are generally carried out using Trojans, but in this case we are talking about a worm, which introduces a new factor: Worms can replicate themselves automatically, so virus authors could eventually lose control of who or whose computers their creations are infecting. That is really not advisable if you have a specific target to attack and want to stay under the radar in order to avoid detection. How did Flame resolve this? Well, the worm has a very curious and somewhat innovative feature: its ability to turn its spreading functionality on and off, something extremely handy when you want to go unnoticed.

One of the most striking features of Flame is that it can steal all kinds of data in multiple ways, even by turning on victims' microphones to record conversations.

As previously mentioned, this was undoubtedly a targeted attack aimed at specific individuals and organizations in the Middle East. And it seems that the cyber-espionage worm might have been active for many years without being detected by security companies, which has produced a number of conspiracy theories claiming that governments pressed antivirus vendors to not detect the worm. Obviously, this is completely false, and as soon as the worm has been discovered, it has been detected by all of them.

But, why did it take so long to detect Flame? Well, no antivirus solution has a 100-percent success rate at catching new, unknown threats. This is quite simple to understand: professional cybercriminals make sure their malicious creations will go undetected before spreading them. They test them against all popular antivirus engines to make sure they cannot be detected by signature files or any other protection systems (behavioral and heuristic scanning, etc.). If you have the necessary resources at your disposal, you can set up a Quality Assurance process that eliminates the possibility of the malware being found, at least at the start. The threat will be eventually detected by antivirus solutions, but making it go unnoticed for as long as possible is the key to success. For example, by infecting a small number of targeted computers instead of triggering a massive infection.

Throughout the year we have seen a number of cyber-espionage attacks aimed at journalists in different parts of the world. For example, in Morocco, a group of independent journalists who received an award from Google for their efforts during the Arab Spring revolution, was infected with a Mac Trojan. In China, a group of foreign correspondents was targeted by two malware attacks via email a few weeks before the Congress of the Chinese Communist Party.

FIG.33. *SAUDI ARAMCO.*

This year we have also seen a couple of malware infections in companies operating in the energy sector in the Middle East. It is still not known if these incidents are related or are due to some type of cyber-attack, but all the evidence seems to indicate so. The Saudi Arabian Oil Company (Saudi Aramco) was hit by a malware infection that led the company to severe its connections to the Internet as a preventive measure.

FIG.34. *RASGAS.*

In addition to this, a virus infected Qatari natural gas company RasGas. However, neither RasGas nor Saudi Aramco saw their production halted due to these incidents.

03| 2012 in figures

Approximately, 27 million new strains of malware were created in 2012, 74,000 every day. As a result, PandaLabs has now a total of 125 million classified malware samples. And the number keeps growing, aided by cyber-crooks eager to bypass antivirus protections to increase their profits. Trojans continued to account for most of the new threats, as three out of every four new malware strains created were Trojans. Here are the details:

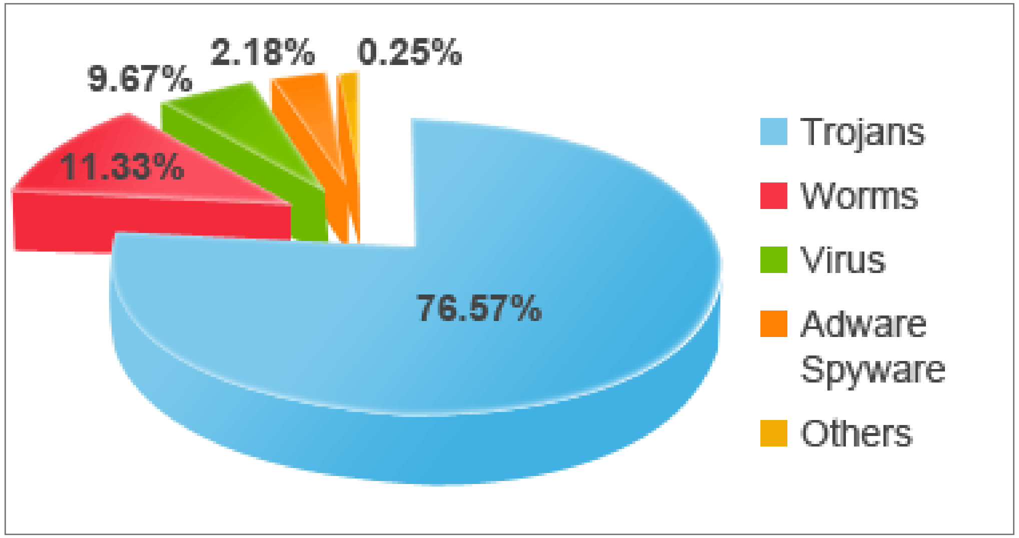


FIG.35. *NEW MALWARE CREATED IN 2012, BY TYPE.*

Over the last few years, the number of Trojans in circulation has been constantly increasing. In 2010 they accounted for more than half of all malware created (56 percent), in 2011 they rose spectacularly to 73.31 percent, whereas in 2012 they reached 76.57 percent. Worms came second (11.33 percent compared to 8.13 percent in 2011), whereas viruses dropped to third place at 9.67 percent compared to 14.24 percent in 2011.

When it comes to the number of infections caused by each malware category, as recorded by our Collective Intelligence technologies, Trojans once again dominated the ranking at 76.56 percent, almost the same percentage as that of Trojans in circulation. It seems that cyber-criminals have managed to infect more computers with Trojans this year than in previous years. In 2011, the percentage of Trojan-infected computers was 66.18 percents, so there has been a 10 point rise in this respect. One of the reasons for this growth is the increased use of exploit kits such as Black Hole, which are capable of exploiting multiple system vulnerabilities to infect computers automatically without user intervention. Here are visuals depicting these trends:

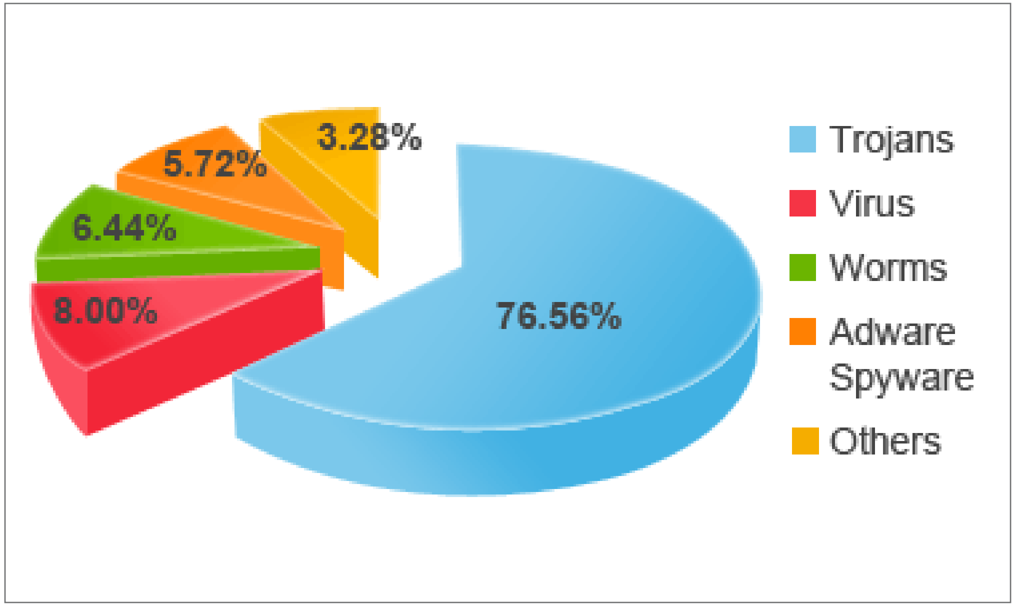


FIG.36. *MALWARE INFECTIONS BY TYPE IN 2012.*

However, not everything was good news for cyber-criminals. The proportion of infected computers worldwide decreased significantly from 38.49 percent in 2011 to 31.98 percent in 2012.

Let's now look at the geographic distribution of infections. Which countries were most infected? Which countries were best protected? China was once again top of the list of countries with most infections with more than 50 percent of infected PCs (54.89 percent), followed by South Korea (54.15 percent), and Taiwan at a distant third (42.14 percent).

Here is a graph representing the countries with most malware-infected computers:

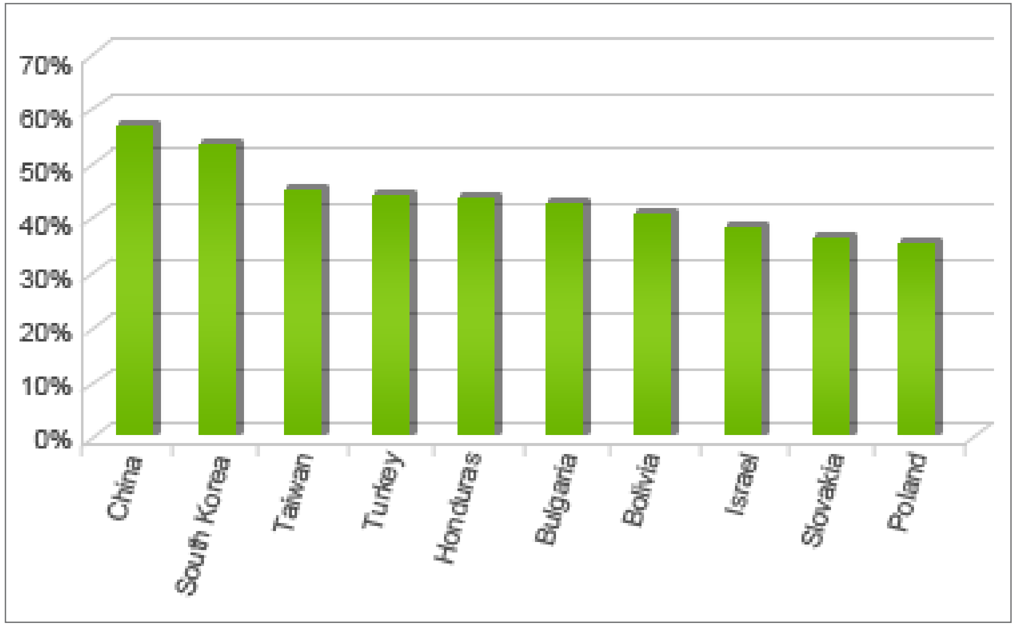


FIG.37. *MOST MALWARE-INFECTED COUNTRIES IN 2012.*

The list of top ten most infected countries is made up of nations from almost every part of the world: Asia, Europe, Central America and South America. Other countries whose number of malware infections was above the global average are: Lithuania (35.46 percent), Thailand (35.37 percent), Peru (35.05 percent), Argentina (34.79 percent), Spain (34.06 percent), Nicaragua (34.03 percent), Guatemala (33.89 percent), Ecuador (33.68 percent), El Salvador (32.86 percent), Brazil (32.09 percent) and Chile (31.98 percent).

Nine of the ten least infected countries are in Europe with the only exception being Canada. The country with the fewest infections is Sweden (20.25 percent of infected PCs), followed by Switzerland (20.35 percent), and Norway (21.03 percent).

Here's a graph representing the countries with the fewest infections in 2012:

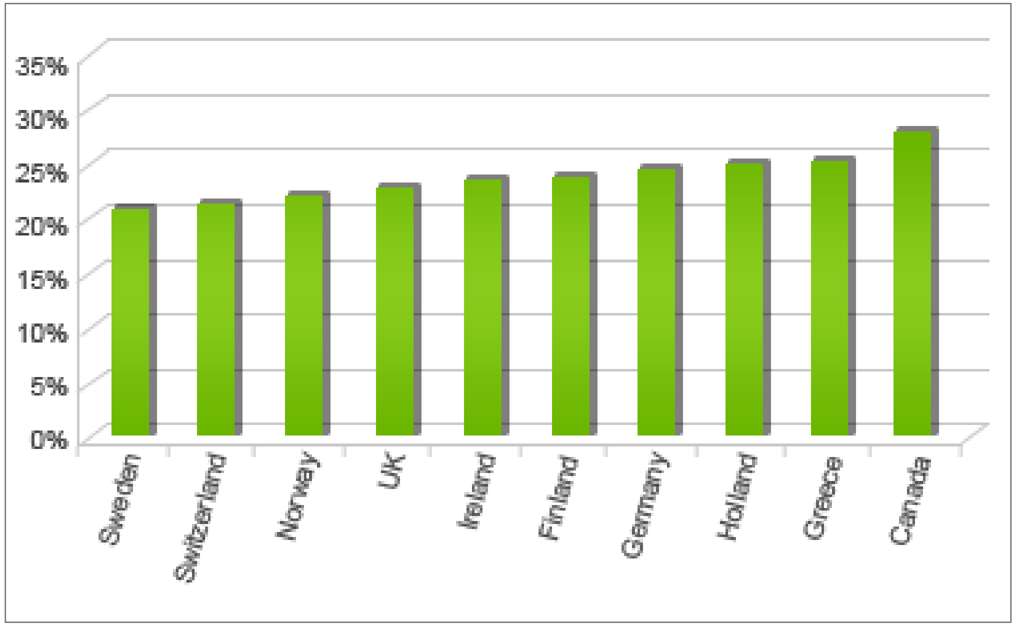


FIG.38. *LEAST MALWARE-INFECTED COUNTRIES.*

Other countries whose number of malware infections was below the global average are: Czech Republic (31.84 percent), Romania (31.54 percent), Colombia (31.49 percent), Estonia (31.33 percent), United States (30.52 percent), Slovenia (30.37 percent), Italy (30.25 percent), Venezuela (29.81 percent), Mexico (29.81 percent), Costa Rica (29.73 percent), Panama (29.61 percent), France (29.19 percent), Paraguay (28.57 percent), South Africa (27.94 percent), Denmark (27.65 percent), Hungary (27.37 percent), Uruguay (27.23 percent), Austria (27.03 percent), Belgium (27.02 percent), Portugal (26.78 percent), Australia (26.60 percent), Latvia (26.06 percent), Japan (26.00 percent) and New Zealand (25.76 percent).

04| 2013 Security Trends

We have seen what has happened in 2012: attacks in social networks and cyber-war everywhere. What do we have to expect for the next 12 months?

Vulnerabilities

Software vulnerabilities will be the main target of cyber-criminals next year. It is undoubtedly the preferred method of infection for compromising systems transparently, used by both cyber-criminals and intelligence agencies in countries around the world. In 2012, we saw how Java, which is installed on hundreds of millions of devices, was repeatedly compromised and used to actively infect millions of users. In second place is Adobe, as given the popularity of its applications (Acrobat Reader, Flash, etc.) and its multiple security flaws, it is one of the favorite tools for massively infecting users as well as for targeted attacks.

Although we may think that home users are exposed to the highest risk, remember that updating applications, which is essential for protecting against these types of attacks, is a very complex process in companies, where updating all computers must be coordinated. At the same time, it is essential to ensure that all the applications used in a company work correctly. This makes the update processes slow, which opens a window that is exploited to steal information in general and launch targeted attacks in search of confidential data.

Social networks

The second most widely used technique is social engineering. Tricking users into collaborating to infect their computers and steal their data is an easy task, as there are no security applications to protect users from themselves. In this context, use of social networks (Facebook, Twitter, etc.), places where hundreds of millions of users exchange information, on many occasions personal data, makes them the preferred hunting ground for tricking users.

Particular attention should be paid to Skype, which after replacing Messenger, could become a target for cyber-criminals.

Malware for mobile devices

Android has become the dominant mobile operating system. In September 2012, Google announced that it had reached the incredible figure of 700 million Android activations. Although it is mainly used on smartphones and tablets, its flexibility and the fact that you do not have to buy a license to use it are going to result in new devices opting to use Google's operating system. Its use is going to become increasingly widespread, from televisions to all types of home appliances, which opens up a world of possible attacks as yet unknown.

Cyber-warfare / Cyber-espionage

Throughout 2012, different types of attacks have been launched against nations. The Middle East is worth mentioning, where the conflict is also present in cyber-space. In fact, many of these attacks are not even carried out by national governments but by citizens, who feel that they should defend their nation by attacking their neighbors using any means available. Furthermore, the governments of the world's leading nations are creating cyber commandos to prepare both defense and attack and therefore, the cyber-arms race will escalate.

Growth of malware

For two decades, the amount of malware has been growing dramatically. The figures are stratospheric, with tens of thousands of new malware strains appearing every day and therefore, this sustained growth seems very far from coming to an end.

Despite security forces being better prepared to combat this type of crime, they are still handicapped by the absence of borders on the internet. A police force can only act within its jurisdiction, whereas a cyber-crook can launch an attack from country A, steal data from citizens of country B, send the stolen data to a server situated in country C and could be living in country D. This can be done in just a few clicks, whereas coordinated action of security forces across various countries could take months. For this reason, cyber-criminals are still living their own golden era.

Malware for Mac

Cases like Flashback, which occurred in 2012, have demonstrated that not only is Mac susceptible to malware attacks but that there are also massive infections affecting hundreds of thousands of users. Although the number of malware strains for Mac is still relatively low compared to malware for PCs, we expect it to continue rising. A growing number of users added to security flaws and lack of user awareness (due to over-confidence),mean that the attraction of this platform for cyber-crooks will continue to increase next year.

Windows 8

Last but not least, Windows 8. Microsoft's latest operating system, along with all of its predecessors, will also suffer attacks. Cyber-criminals are not going to focus on this operating system only but they will also make sure that their creations work equally well on Windows XP to Windows 8, through Windows 7.

One of the attractions of Microsoft's new operating system is that it runs on PCs, as well as on tablets and smartphones. For this reason, if functional malware strains that allow information to be stolen regardless of the type of device used are developed, we could see a specific development of malware for Windows 8 that could take attacks to a new level.

05| Conclusion

The year 2013 presents itself full of challenges in the computer security world.

Android users will have to face a growing number of attacks from cyber-crooks wanting to steal private information.

Cyber-espionage and cyber-war will also be on the rise, as more and more countries are organizing their own cyber-commando units. There is growing concern for the information that could be compromised and the possibility of using malware to launch direct attacks on critical infrastructure.

Companies will have to tighten up security measures to avoid falling victim to the increasing number of cyber-attacks, while special care will have to be taken to protect networks against operating system and application vulnerabilities, with Java posing the biggest threat due to its multiple security flaws.

Visit the PandaLabs blog (http://www.pandalabs.com) to stay up to date with all the developments and discoveries made at the laboratory.

06| About PandaLabs

PandaLabs is Panda Security's anti-malware laboratory, and represents the company's nerve center for malware treatment:

- **PandaLabs** creates continually and in real-time the counter-measures necessary to protect Panda Security clients from all kind of malicious code on a global level.

- **PandaLabs** is in this way responsible for carrying out detailed scans of all kinds of malware, with the aim of improving the protection offered to Panda Security clients, as well as keeping the general public informed.

Likewise, PandaLabs maintains a constant state of vigilance, closely observing the various trends and developments taking place in the field of malware and security. Its aim is to warn and provide alerts on imminent dangers and threats, as well as to forecast future events.

- For further information about the last threats discovered, consult the PandaLabs blog at: **http://pandalabs.pandasecurity.com/**

Follow us on the Web

facebook
https://www.facebook.com/PandaUSA

twitter
https://twitter.com/Panda_Security

google+
http://www.gplus.to/pandasecurity

youtube
http://www.youtube.com/pandasecurity1