



GT-CSIRT: Grupo de Trabajo de RedCLARA CSIRT

Tratamiento de Incidentes de Seguridad: Una visión práctica

Apoyo: Centro de Atendimento a Incidentes de Segurança (CAIS/RNP)

Carla Freitas
Frederico Costa
Rildo Souza
Liliana Solha

16a Reunión Técnica de RedCLARA
04-06 de Julio, 2012
Lima, Perú




CLARA

This project is funded by the European Union A project implemented by CLARA



Derechos de autor© 2009 CAIS/RNP - Centro de Atención a los Incidentes de Seguridad de la Red Nacional de Enseñanza e Investigación de Brasil – RNP. Todos los derechos reservados.

La reproducción total o parcial de este material está totalmente prohibida, así como su uso para cualquier propósito, comercial u otro.





CLARA



Introducción

Conociéndonos y alineando expectativas





CLARA



GT-CSIRT: Propuesta

- GT-CSIRT
 - Establecido en agosto de 2011, duración de 2 años
 - Consolida acciones del GT-Seg
 - Misión:

Promover la implantación de CSIRTs (Equipo de Respuesta a Incidentes de Seguridad) en cada red académica nacional (NREN), y acciones colaborativas entre los CSIRTs existentes
- Propuesta focalizada en tres líneas de acción (LA):
 - LA-1: Monitoreo de actividad maliciosa
 - LA-2: Tratamiento de incidentes de seguridad
 - LA-3: Apoyo a la creación de CSIRTs
- Categoría del GT: *Despliegue de un piloto de nueva tecnología/servicio*





CLARA

GT-CSIRT: Cronograma

# tarea	Nombre de la tarea	Periodo de ejecución de la tarea	Relación de dependencia
T-1	Estructuración del ambiente de monitoreo de actividad maliciosa	Ago/2011 – May/2012	Ninguna
T-2	Estructuración del ambiente de tratamiento a incidentes de seguridad	Ago2011 – May2012	Ninguna
T-3	Entrenamiento sobre Monitoreo y Tratamiento de Incidentes de Seguridad	May/2012– Jun/2012 (1a Reunión CLARA-TEC 2012)	T-1 y T-2 finalizadas
T-4	Implantación de la solución de monitoreo en las NREns	Jul/2012 – Jun/2013	T-3 finalizada
T-5	Implantación del ambiente de tratamiento de incidentes en las NREns.	Jul/2012 – Jun/2013	T-3 finalizada
T-6	Apoyo al establecimiento de un CSIRT	Ago/2011 – Dic/2012	Ninguna






Sobre el curso

- **Objetivos**
 - Informar sobre los ataques y amenazas más diversos y comunes.
 - Capacitar en la implementación de una infraestructura de monitoreo de actividad maliciosa y de respuesta a incidentes de seguridad
 - Apoyar en el proceso de establecimiento de un CSIRT
 - Ejecutar los modelos de monitoreo y tratamiento desarrollados en el ámbito del GT-CSIRT.








Sobre el curso

- Metodología
 - Presentaciones, ejercicios, P&R, discusiones.
- Material
 - Presentaciones
 - Versiones digitales
 - Prácticas
 - Individuales y en grupo
 - Versiones impresas
 - Informaciones complementares

Servidor Índico: <http://www.redclara.net/indico/evento/150>



Sobre el curso

- Horario del curso e intervalos
 - Mañana: 08:30 – 13:00
 - coffee-break: 10:30 – 11:00
 - Almuerzo: 13:00 – 14:00
 - Tarde: 14:00 – 18:00
 - coffee-break: 16:00 – 16:30

Contamos con la puntualidad de todos!





Agenda – 1er día

- Contextualización
 - Algunos Conceptos
- Equipo de Respuesta a Incidentes de Seguridad
 - ¿Qué es un CSIRT?
 - Proceso de establecimiento del CSIRT
- Estudio de caso: UTPL, CAIS/RNP, PeCERT



Agenda – 2do día

- SurfIDS: Monitoreo de actividad maliciosa
 - Sistemas de alerta temprana (EWS)
 - Presentación de la herramienta SurfIDS
 - Operación del SurfIDS
 - Uso de la interface web
- GENICs: Notificación de incidentes de seguridad
 - Presentación de la herramienta GENICs
 - Funcionamiento de la herramienta GENICs
- Integración de las herramientas SurfIDS y GENICs





Agenda – 3er día

- El día a día de un “Incident Handler”
 - Qué es un incidente de seguridad?
 - Qué es un “incident handler”?
 - Proceso de tratamiento de incidentes de seguridad
 - Vivenciando este día!








Requisitos técnicos

- Laptops provistos por los propios alumnos
- Serán ejecutadas 03 máquinas virtuales
- Configuración recomendada:
 - Procesador: Intel Core2duo 2.5GHz o superior
 - Memoria: 4GB o superior
 - Hard Disk: 100GB o superior
 - Placa de red 10/100 o Gigabit Ethernet
 - Drive de lectora de DVD
 - Mínimo de dos puertas USB 2.0
 - Sistema operativo: Windows o Linux
 - Vmware Player 4.0 o superior, o Vmware Workstation 7.0 o superior.
- Distribución de imágenes (MVs y Vmware Player)






Presentación

- Nombre
- Función
- Organización
- ¿Tiene CSIRT?
- ¿Tiene experiencia en el tratamiento de incidentes?
- ¿Fue designado como responsable por seguridad?
- Expectativas del curso



Preguntas



GT-CSIRT gt-csirt@listas.redclara.net
Liliana Solha nina@cais.rnp.br





Contextualización

Por que estamos aquí?



Aplicativos Locals Qui 21 Jun, 10:08

«Hackers» atacaron gasoductos de Estados Unidos

Una vez que el blanco abre el archivo un paquete de material malicioso se descarga fácilmente o permite monitorear los sistemas.

9 mayo 2012
07:31 PM ET

Compartir
Comentarios (Comentar)
Permalink

Recommend 0

Tweet 49

"Hackers" atacaron gasoductos de Estados Unidos

Por Suzanne Kelly

(CNN) — Una serie de compañías de gasoductos del sector del gas natural en Estados Unidos son el objeto de un ataque cibernético que aparentemente fue lanzado desde diciembre, de acuerdo con una nota del Departamento de Seguridad Nacional de ese país (DHS, por sus siglas en inglés).

La amenaza fue revelada en un reporte mensual publicado por el equipo del Industrial Control Systems Cyber Emergency Response (ICS-CERT por sus siglas en inglés), una división de DHS dedicada a la seguridad cibernética.

El equipo del DHS, ICS-CERT "ha estado trabajando desde marzo de 2012 con los dueños y operadores de la infraestructura crítica del sector petrolero y de gas natural para afrontar una serie de intrusiones cibernéticas que cuyos blancos son las compañías de gasoductos para gas natural", dijo el vocero del DHS, Peter Boogaard.

"La intrusión cibernética incluye sofisticadas acciones de phishing (un enlace, aparentemente de una fuente legítima, que te lleva a un sitio web falso para que introduzcas información confidencial, como tu contraseña de banco en línea) que tienen como objetivo atacar al personal de estas empresas privadas", dijo Boogaard.

Un comunicado de la ICS-CERT dice: "El análisis demuestra que los intentos de actividades de phishing han tenido como blanco a varios miembros del personal de estas organizaciones. Sin embargo, el número de personas que representan un verdadero objetivo parece ser un grupo altamente enfocado. Además, los correos electrónicos fueron elaborados de forma muy convincente para que aparenten haber sido enviados desde el correo de un empleado de confianza dentro de la empresa".

Algunos atacantes se han vuelto tan sofisticados en los esfuerzos de phishing, que realizan que llevan a cabo una investigación de los empleados conocidos en las redes sociales para después elaborar un correo electrónico que parezca que fue escrito por una persona conocida por el receptor.

Una vez que el blanco abre el archivo adjunto que acompaña el correo electrónico,

Síguenos Facebook Twitter Pinterest

Buscar

Últimas noticias

Colombia el origen de más refugiados y desplazados en América por la violencia

Un barco que viajaba entre Australia e Indonesia se hunde con 200 personas a bordo

Una visita al camino de los arrepentidos

La Cumbre de la Tierra: ¿Solucionará Río+20 los problemas ambientales?

Mike Tyson se dirige a Broadway para presentar su propio espectáculo

En Facebook

CNN en Español en Facebook

Me gusta

CNN en Español

Con casi 400,000 refugiados y cuatro millones de desplazados internos a causa del conflicto armado, Colombia es el principal foco rojo de estos fenómenos en América Latina, de acuerdo a cifras de la oficina del Alto Comisionado de las Naciones Unidas para los Refugiados.

<http://on.cnn.com/M8PL5Z> ¿Qué

Gobiernos contratan... «Hackers» atacaron g...

Aplicativos Locals Qui 21 Jun, 10:24

Curso CLARATEC 2012 - C x Anonymous tumbó los sit... x

cnnespanol.cnn.com/2012/05/07/anonymous-tumbo-los-sitios-de-cia-e-interpol-durante-horas/

7 mayo 2012
12:40 PM ET

Compartir
Comentarios (9 comentarios)
Permalink

Recommend 94

Tweet 302

Anonymous "tumbó" los sitios de CIA e Interpol durante horas

(CNMéxico) — Los sitios de la CIA y de la Interpol dejaron de funcionar el domingo por varias horas, una falla que se atribuyó al colectivo de hacktivistas Anonymous, a través de Twitter.

Ataques a los sitios fueron promovidos por una supuesta rama de Anonymous en Turquía casi a las 12:00 GMT, a través de la cuenta de Twitter @AnonsTurkey y bajo la etiqueta #OpTurkey.

El grupo anunció a las 16:00 que el sitio CIA.gov llevaba cuatro horas sin funcionar, mientras que Interpol.int llevaba dos horas.

CNMéxico verificó que al intentar acceder a ambos sitios, el navegador mostraba mensajes de error.

Los ataques fueron identificados como la operación Tango Down, un nombre frecuentemente empleado en otros ataques de Anonymous, y retuiteados por las cuentas @YourAnonNews y @AnonymousIRC, que también han participado en otras operaciones.

Durante las horas que duró el ataque, @AnonsTurkey pidió apoyar su operación y escribió consignas a favor de su movimiento.

"Todos somos Anonymous... No puedes arrestar una idea", escribió en referencia a los miembros de la red de hacktivistas arrestados por el FBI.

@AnonsTurkey anunció que su siguiente ataque tendría como objetivo el sitio del banco estadounidense Bank of America, el próximo 9 de mayo. "¿Por qué? Los accionistas del BOA, alias ladrones, se reúnen el 9 de mayo".

Anonymous ya había realizado otros ataques contra la CIA e Interpol en febrero, luego de las detenciones de 25 supuestos miembros en cuatro países.

Otros ataques del grupo se han dirigido contra el gobierno chino y el Vaticano.

Más noticias de Tecnología en CNMéxico.com

Tu voto: ★★★★★ 2 Votos

Compartir: [Email] [Facebook] [Twitter] [Pinterest] [LinkedIn] [Print] [RSS] [1] [2]

Anonymous tumbó lo...

Siguenos Facebook Twitter Pinterest

Buscar

Últimas noticias

Colombia el origen de más refugiados y desplazados en América por la violencia

Un barco que viajaba entre Australia e Indonesia se hunde con 200 personas a bordo

Una visita al camino de los arrepentidos

La Cumbre de la Tierra: ¿Solucionará Rio+20 los problemas ambientales?

Mike Tyson se dirige a Broadway para presentar su propio espectáculo

En Facebook

CNN en Español en Facebook

Me gusta

CNN en Español

Con casi 400.000 refugiados y cuatro millones de desplazados internos a causa del conflicto armado, Colombia es el principal foco rojo de estos fenómenos en América Latina, de acuerdo a cifras de la oficina del Alto Comisionado de las Naciones Unidas para los Refugiados.
<http://on.cnn.com/M8PL52> ¿Qué

Aplicativos Locals Qui 21 Jun, 10:24

Curso CLARATEC 2012 - C x Anonymous tumbó los sit... x Anonymous dice haber tu... x

cnnespanol.cnn.com/2012/03/07/anonymous-dice-haber-tumbado-el-sitio-de-internet-del-vaticano-2/



7 marzo 2012
05:30 PM ET

Compartir
Comentarios (22 comentarios)
Permalink

Recommend 50

Tweet 50

Anonymous dice haber tumbado el sitio de Internet del Vaticano

Por Amber Lyon, Eric Marrapodi y Hada Messia

Roma (CNN) —Vaticano.va, el sitio web oficial de la Santa Sede, no estaba en funcionamiento la tarde de este miércoles.

El portavoz del Vaticano, el padre Federico Lombardi, confirmó a CNN que el sitio fue atacado, pero dijo que se encontrará "plenamente operativo" de nuevo en breve.

Anonymous, un grupo internacional de piratas informáticos, se atribuyó la responsabilidad por el cierre de sitio web de la iglesia.

"Anonymous ha decidido sitiar a su web en respuesta a las doctrinas, liturgias y los preceptos, absurdos y anacrónicos, de su organización con fines de lucro propaga en todo el mundo", se lee en un comunicado subido al blog "ufficiale di Anonymous Italia".

"Esto no tiene la intención de atacar a la religión cristiana o a los fieles en todo el mundo, sino a la corrupta Iglesia Apostólica Romana y todas sus acciones," agregó el comunicado.

Anonymous dice hab...

Siguenos Facebook Twitter Pinterest

Buscar

Últimas noticias

Colombia el origen de más refugiados y desplazados en América por la violencia

Un barco que viajaba entre Australia e Indonesia se hunde con 200 personas a bordo

Una visita al camino de los arrepentidos

La Cumbre de la Tierra: ¿Solucionará Rio+20 los problemas ambientales?

Mike Tyson se dirige a Broadway para presentar su propio espectáculo

En Facebook

We will donate US\$2 to a charity of your choice

Click Here

CNN GO BEYOND BORDERS



Datos de incidentes en el mundo

Cada día, se identifican 9.500 sites maliciosos nuevos

Diariamente, entre 12 y 14 millones de las búsquedas realizadas entran a sites maliciosos

Al día, hay 300 mil alertas de download de malware

Fuente: Google





CLARA



**“Pero eso sólo ocurre en los EUA y Europa!
Nosotros no somos objeto de este tipo de ataques.”**

¿Será verdad?





CLARA

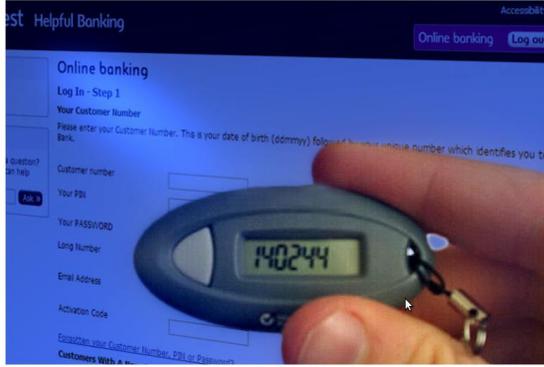
Aplicativos Locais

Qui 21 Jun, 10:02

www.eset.com.uy/threat-center/index.php?subaction=showfull&id=1336418531&archive=&start_from=&cat=1&n=2

Bancos latinoamericanos pierden millones de dólares por delitos informáticos

Los delitos informáticos son cada vez más comunes, especialmente los dirigidos a instituciones bancarias; las pérdidas son multimillonarias y perjudican tanto a los bancos como a sus clientes. Para prevenir estos delitos se han desarrollado servicios referidos exclusivamente a este tema.



Una investigación realizada por el Registro de Direcciones de Internet para América Latina y Caribe (también conocido como LACNIC) demostró que los bancos latinoamericanos pierden anualmente millones de dólares a manos de los cibercriminales.

De acuerdo con el informe de LACNIC, los 2500 bancos existentes en América Latina perdieron una cifra aproximada a los noventa y tres mil millones de dólares cada año, debido a delitos informáticos como el phishing. Los clientes de esos mismos bancos, por su parte, pierden unos setecientos sesenta y un millones de dólares anuales a manos de los estafadores.

Cada vez que la seguridad de un banco es violada, la confianza puesta en él por los clientes disminuye de manera exponencial. Esto hace que aumenten los gastos en materia de promoción e instalación de instrumentos de seguridad.

Los bancos uruguayos y sus clientes no han sido ajenos a los delitos informáticos. En 2011, un grupo de estafadores logró clonar decenas de tarjetas de débito y retirar miles de dólares de forma fraudulenta de cajeros automáticos públicos y privados.

Asimismo, a comienzos de 2012 un número indefinido de cuentas bancarias fueron infiltradas y vaciadas; las autoridades descubrieron que el ataque provino de un servidor instalado en Francia.

Pero no solo los bancos están expuestos. Actualmente todas las empresas se enfrentan a amenazas y ataques informáticos, y deben gestionar adecuadamente la seguridad de su información con el fin de minimizar las potenciales vulnerabilidades y su impacto.



“De acuerdo con el informe de LACNIC, en suma, los 2.500 bancos que existen en América Latina pierden una cifra aproximada a los noventa y tres mil millones de dólares cada año, debido a delitos informáticos como el phishing.”

alice2
Banco Latinoamericano del Caribe

EUROPEAN UNION

CLARA

Aplicativos Locals Qui 21 Jun, 15:06

HackerAnonymous amen... www.taringa.net/posts/info/11979812/Hacker_Anonymous-amenaza-con-ataques-al-gobierno-de-Ecuador.html

TARINGA! Identificarme REGISTRATE YA! Buscar...

Inicio Novatos Destacados

INFO | HACE MÁS DE 10 MESES Like 6 Taringa! 1 1 1 Twitter 2

Hacker: Anonymous amenaza con ataques al gobierno de Ecuador

Anuncios Google

[Gafisa - Zona Oeste](#)
Gafisa.com.br/ZonaOeste - Imóveis com Condições Especiais. Fale agora com nossos consultores!

[Crédito Fácil e Imediato](#)
ShopCredit.com.br/Credito-Bradesco - Com Até 24 Meses para Pagar. Exclusivo para Clientes Bradesco.

[Imóveis no Brooklin](#)
www.ZAP.com.br/Brooklin - O Imóvel que você procura está aqui Confira agora mesmo no ZAP Imóveis.

[Cyrela|Encontre seu Apto](#)
Cyrela.com.br/SaoPaulo - Veja outros Imóveis na Z.Oeste - SP Cyrela tem a opção ideal p/ Você!

La red de piratas informáticos o hackers Anonymous amenazó con realizar ataques al gobierno del Ecuador por el supuesto acoso de este a los medios de comunicación y las limitaciones a la libertad de expresión, destacando la demanda al diario El Universo y a varios periodistas y directivos de medios de comunicación; también rechaza la incautación de varios medios de comunicación privados y el uso de estos con fines políticos.

Dos videos subidos a Youtube, a nombre del grupo de hackers o piratas informáticos conocidos como Anonymous a nivel mundial, se refieren a la última sentencia emitida contra diario El Universo, la cual rechazan por considerarla un ataque a la libertad de prensa por parte del gobierno ecuatoriano. Y proponen el inicio de la Operación Cóndor Libre, "para luchar contra la censura a los medios informativos en el Ecuador". También hacen una enumeración de los medios de comunicación que pasaron a control del Estado durante esta

Jack Blacker
59 Seguidores
595 Puntos
47 Posts
Experto

Ver más del autor =

APTOS. CYRELA NOS MELHORES BAIRROS DA REGIÃO
CLIQUE E VEJA OPÇÕES

Tags
Gobierno medios
comunicacion tambien
grupo anonymous

Malware en las Americas

Pais de origen	Ranking Regional - Código Malicioso 2011	% Regional de Código Malicioso en 2011	Ranking Regional 2011	Ranking Mundial 2011
Estados Unidos	1	91.5%	1	1
Brasil	1	39.9%	1	4
Canadá	2	8.5%	2	16
México	2	21.0%	4	29
Colombia	3	5.5%	3	28
Chile	4	5.4%	5	34
Argentina	5	4.7%	2	22
Venezuela	6	4.3%	7	52
Perú	7	2.7%	6	41
Jamaica	8	2.0%	16	96
República Dominicana	9	1.8%	8	54
Ecuador	10	1.5%	12	76

Fuente: Symantec *Países de Norteamérica

Fuente: Symantec 2011

alice2
European Union
CLARA



“¿Cuál es la motivación para estos ataques?”





Políticos

25 abril 2012 08:40 AM ET

Gobiernos contratan a cibercybermercenarios para atacar sistemas

(CNN) — El 27 de abril de 2007, la pequeña nación báltica de Estonia —uno de los países más conectados del mundo— fue golpeada con un ataque cibernético masivo. Los sitios web de los bancos, de ministerios de gobierno, del Parlamento, periódicos y otros medios de comunicación fueron paralizados, estuados por una ataque de denegación de servicio.

"Estábamos francamente sorprendidos cuando esto pasó", dijo el presidente de Estonia, Toomas Hendrik Iivies. "Los botnets (robots informáticos) atacaron a todos los aspectos de la sociedad".

Hendrik sostiene que fue un "acto político" en el que Rusia, enajada sobre la decisión de Estonia de mover una estatua de la era soviética dedicada al soldado ruso de la Segunda Guerra Mundial, trató de "apagar" al país. Rusia siempre ha negado la acusación.

Pero la nueva generación de ataques cibernéticos puede ser mucho peor que el de Estonia, dijo Iivies en un discurso este mes en la conferencia E-Governance and Cyber Security (E-Gobernanza electrónica y seguridad cibernética) en el Centro nort...

CNN donará US\$2 a una caridad de su elección

Haga clic aquí

Síguenos Facebook Twitter Pinterest

Últimas noticias

Colombia el origen de más refugiados y desplazados en América por la violencia

Un barco que viajaba entre Australia e Indonesia se hunde con 200 personas a bordo

Una visita al camino de los arquetipos

La Cumbre de la Tierra: ¿Solucionará Rio+20 los problemas ambientales?

Mike Tyson se dirige a Broadway para presentar su propio espectáculo

alice2 América Latina Miembros de la Unión Europea

CLARA

Aplicativos Locales Sex 22 Jun, 09:54

www.wired.com/game/2011/05/sony-psn-hack-losses/

Sony Estimates \$171 Million Loss From PSN Hack

By Jason Schreier May 23, 2011 | 5:03 pm | Categories: Business Matters, Game/Death

Follow @jasonschreier

Like Send 82 people like this. Be the first of your friends.

Represalias

PLAYSTATION®Network

Sony will lose approximately 14 billion yen (\$171 million) following the PlayStation Network outage, it said Monday.

This loss includes expenses for security improvements, "Welcome Back" packages and an estimate of the impact on future profits of the security breach and resultant outage. Sony says it has still not confirmed any reports of credit card fraud or identity theft, both of which could change the company's estimated losses.

The PlayStation manufacturer said it had lost around 260 billion yen (\$3.18 billion) during the fiscal year that ended in March 2011. Sony said this loss was the result of "a non-cash charge to establish a valuation allowance ... against certain deferred tax assets in Japan." It blamed this partially on the "adverse impact" of the Japan earthquake earlier this year.

Sony's PlayStation Network services are still not fully operational following a devastating security breach in late April that may have compromised personal information, including credit card data, for its 70 million users. Though the company has restored some of the network's functionality, including online play, other services are still unavailable.

Notably, its PlayStation Store service through which it sells downloadable games for PSP and

AMP RE THINK ENERGY

SUBSCRIBE TO WIRED MAGAZINE

EDITORIAL TEAM

Editor: Chris Kohler | E-mail | Twitter
 Contributor: Ryan Rigney | E-mail | Twitter
 Contributor: John Mox Meyer | E-mail | Twitter
 Contributor: Daniel Fierl | E-mail | Twitter
 Wired Mag: Chris Baker, Peter Rubin

RECENT POSTS

Judge Declares iOS 'Teens Clone' 'Infringing'

Japan Passes Jail-for-Downloaders Anti-Piracy Law

Review: Bend Your Brain (And Thumbs) Around Quantum Continuum

Portal Designer Kim Swift Won't Let You Take Her Toys Away

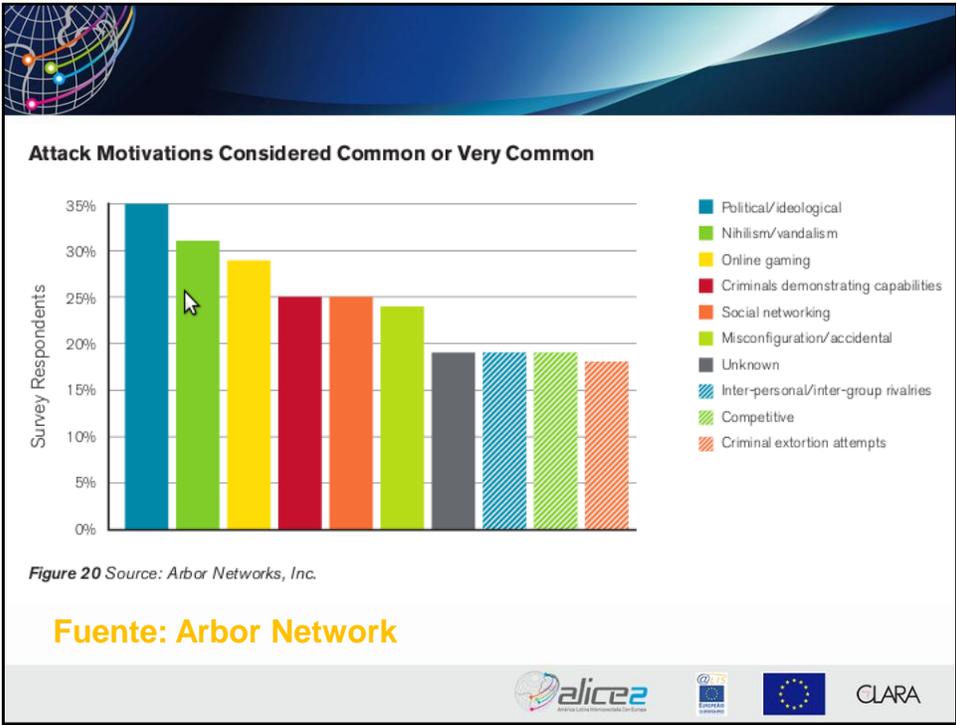
GameLife Video: We Find Your Lack of 3DS Games Disturbing

ADVERTISEMENT

Gafisa - Zona Oeste
 Invoiveis com Condições Especiais. Fale agora com nossos consultores! - Gafisa.com.br/ZonaOeste

MBA Contabilidade
 Faça seu MBA USP-Fundace Investa em Você - www.fundace.org.br

Apto 1 e 2 Dorms
 Em Alhaurilla À Sua Medida. Moderno Funcional A



Conceptos Básicos

alice2
European Union
CLARA



SPAM

alice2
Associação Latino-Americana de Segurança

ES
European Security

EUROPEAN UNION

CLARA



SPAM

**~ 80% de los mensajes
de correo electrónico
son SPAM**

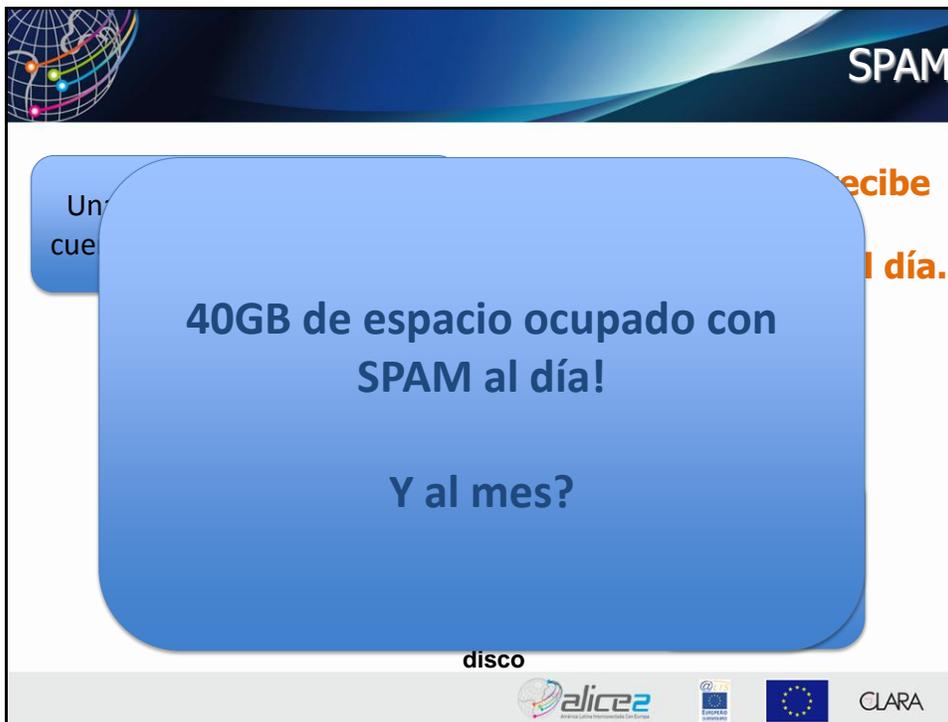
Fonte: CelloPoint Security, Maio 2012

alice2
Associação Latino-Americana de Segurança

ES
European Security

EUROPEAN UNION

CLARA



Un
cua

recibe
el día.

40GB de espacio ocupado con SPAM al día!

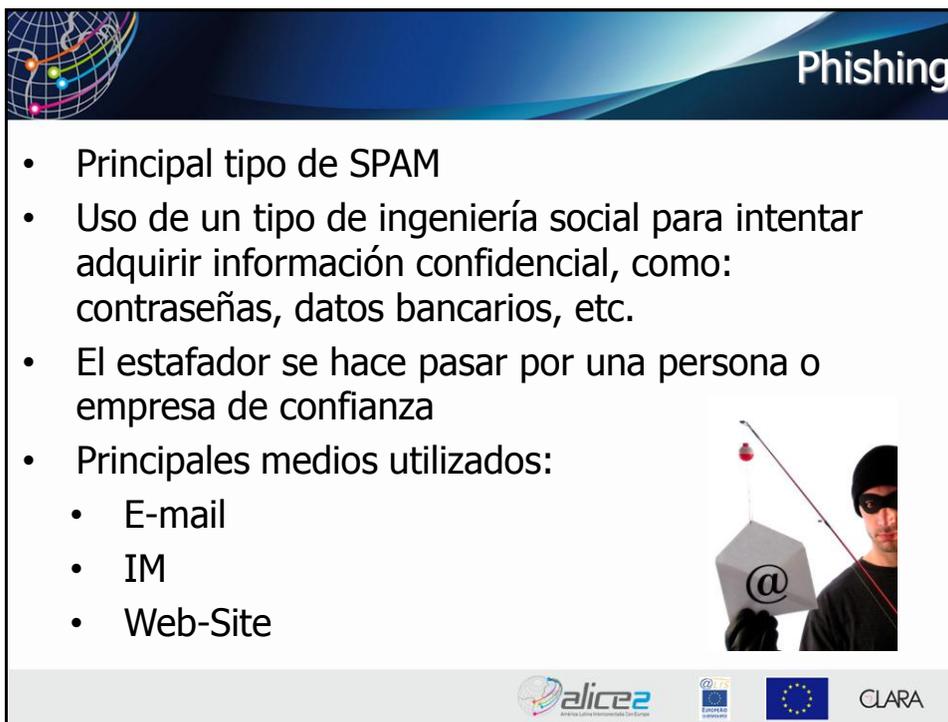
Y al mes?

disco

alice2
Redes de Alta Velocidad en Europa

ETN
EUROPEAN
TECHNOLOGY
NETWORK

CLARA



Phishing

- Principal tipo de SPAM
- Uso de un tipo de ingeniería social para intentar adquirir información confidencial, como: contraseñas, datos bancarios, etc.
- El estafador se hace pasar por una persona o empresa de confianza
- Principales medios utilizados:
 - E-mail
 - IM
 - Web-Site



alice2
Redes de Alta Velocidad en Europa

ETN
EUROPEAN
TECHNOLOGY
NETWORK

CLARA

Phishing

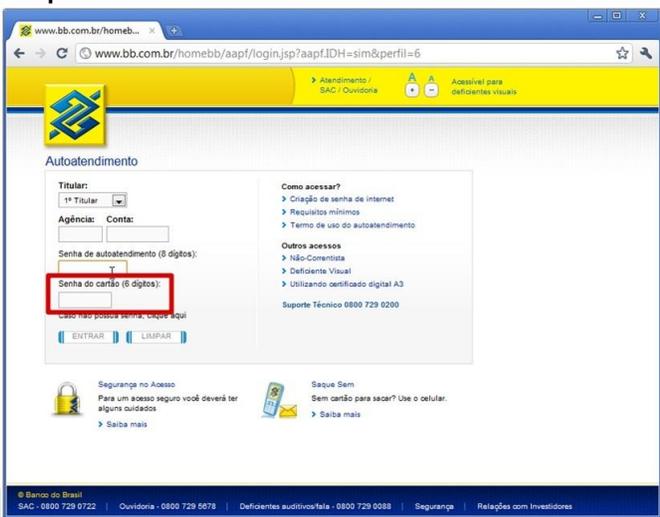
- Objetivo: \$\$\$\$
- Muy utilizado para robar informaciones bancarias, tarjetas de crédito, cuentas en *paypal*, etc.
 - Utilizado para realizar compras
 - Transferencias no autorizadas de efectivo
 - Ventas en el mercado negro
- Robo de información personal
 - Creación de cuentas falsas para fraudes
- Robo de las cuentas de e-mails, redes sociales
 - Pedido de "rescate"



CLARA

Phishing

- Ejemplos:



CLARA

Phishing

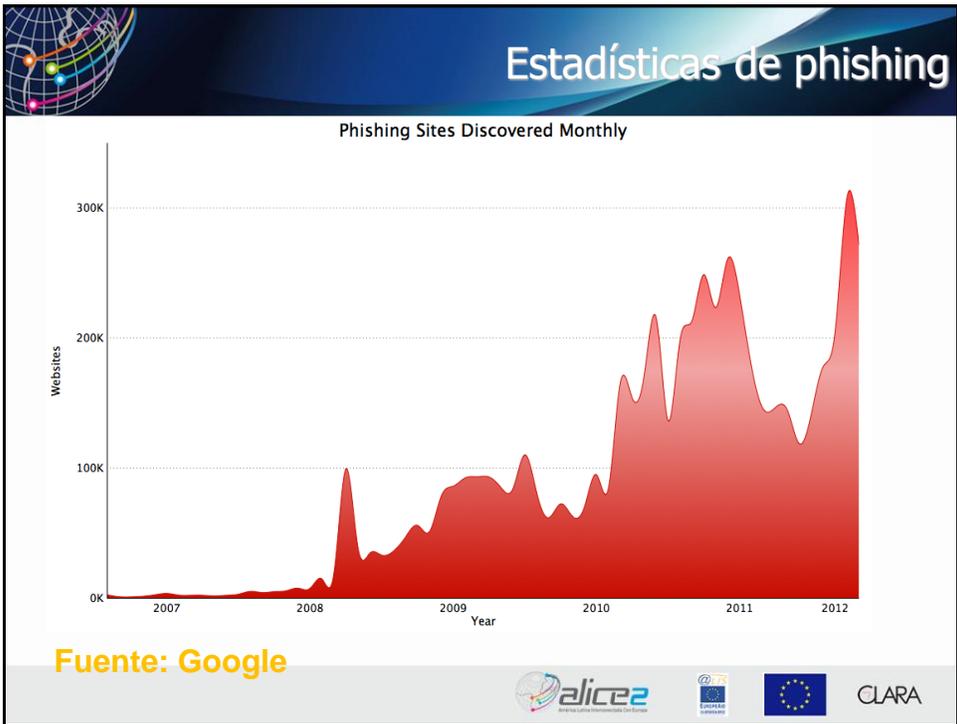
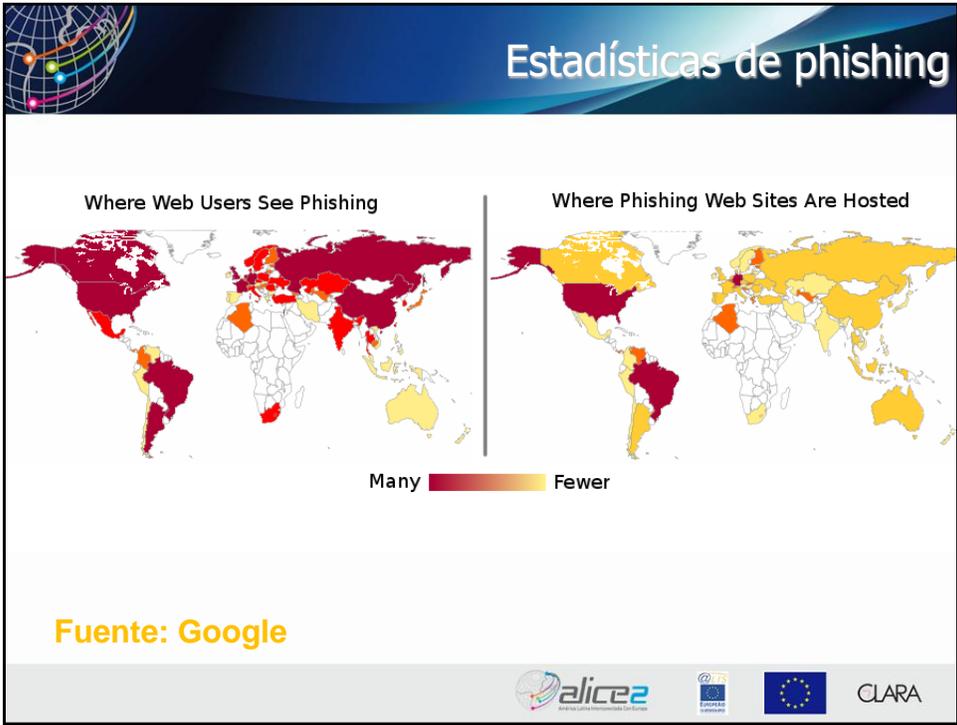
- Ejemplos:**




Phishing

- Ejemplos:**



Malware

- Malware = Archivo malicioso
- Tiene como objetivo infiltrarse a una computadora, o dañarla, sin el consentimiento de su propietario
- El software se considera malware en función de los efectos que provoque en una computadora
- Un Bug no es un malware!
 - Bug es un software defectuoso
- Se aprovechan de las vulnerabilidades de los sistemas o de la ingeniería social para infectar las computadoras








Malware - Propósitos

- En los 80 y 90, los malware eran creados como una forma de vandalismo o travesura
- En los últimos años, la mayoría de malware es creada con fines económicos
- Algunos usos de los malware:
 - Causan daños o pérdidas de datos
 - Toman control de las computadoras para utilizarlas en el mercado negro
 - Envían mensaje de Spam
 - Se unen a ataques DoS
 - Alojando información ilegal, como pornografía infantil
 - Roban informaciones personales y financieras
 - Obtienen información para fines publicitarios








Tipos de Malware

Spyware

Keylogger

Virus

Bot

Worm

Trojan

Backdoor

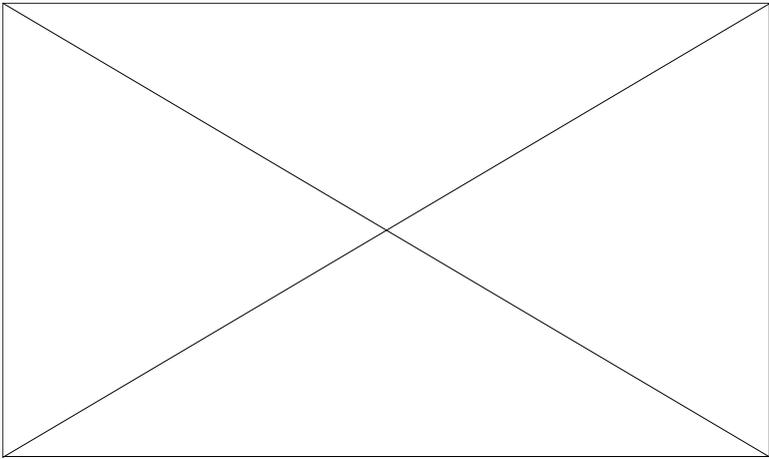
¿En qué se diferencian?



CLARA



Tipos de Malware



CLARA

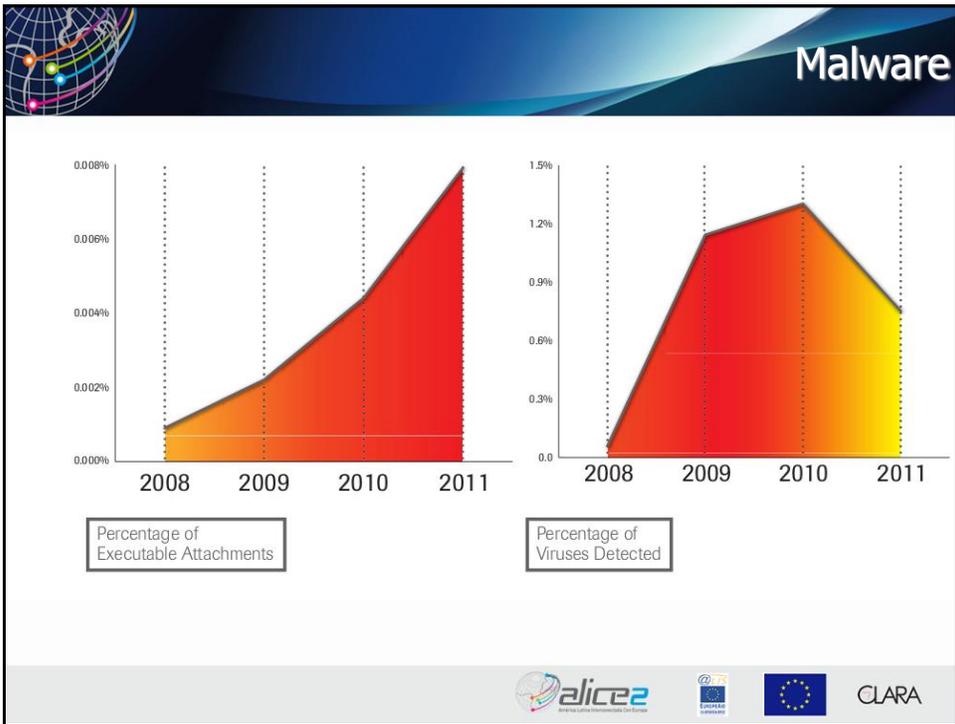
Malware

En 2011, diariamente fueron creados 73.000 nuevos ejemplares de malware
(Fuente: Panda Security)

Los software de anti-virus llegaron a detectar menos del 12% de los malware lanzados en 2011
(Fuente: Trustwave 2012 Global Report)





Chile, en el top ten... pero de computadores infectados por "software malicioso"

7 de mayo de 2012 08:21 | Por: UPI | 2

Al tope de la lista se encuentra China, con un 54% de PCs infectados. Solo en el primer trimestre del año, se han creado 6 millones de ejemplares de este tipo de programas, sostiene la empresa informática Panda Security.

QUEÓPINAS

Me importa 3 Simpatico 0 Interesante 3 Raro 0 Irrelevante 0 Me indigna 0 Enviar Twittear

LO + VISTO EN TECH

- Apple subasta en Sotheby's dos piezas US \$400.000
- La placa madre del Apple I venia con un manual...
- Así será el parque edico marino más grande del mundo
- La compañía española Iberdrola hará una inversión de 1.600...
- Las 8 Apps para el Día del Papá
- Las opciones para reglonaer a los padres en su día...
- Preso por afirmar que "Dios no existe" en Facebook

EL DÍNAMO EN FACEBOOK

Chile, en el top ten...

“Taiwán ocupa el segundo lugar (47,15%), seguido por Turquía (42,75%), Rusia (41,22%), Perú (39,99%), Ecuador (38,03%), España (37,93%), Argentina (37,52%), Polonia (36,9%) y finalmente Chile”

Botnet

alice2

IPTS

CLARA

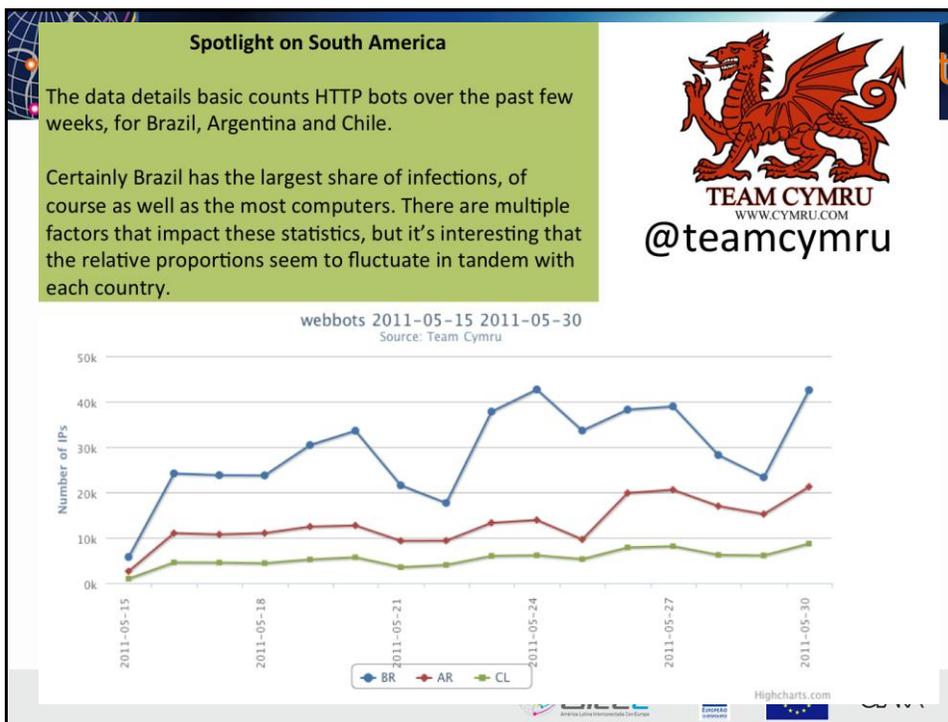
European Union

Botnet

- Conjunto de bots ejecutados de manera autónoma y automática.
- El artífice del botnet (controller) puede tener el control remoto de todas las computadoras/servidores infectados.
- Normalmente son controlados a través del IRC.
- Son propagados a través de los *cracks* de software, download de software pirata, mediante mensajes falsos; acceden a los sistemas con contraseñas débiles, etc.







Russian Botnet Operator Busted For Infecting 6 Millions of Computers & Stealing £2.9 Million

POSTED BY VOUGH REPORTER ON 6/25/2012 10:26:00 PM

0 tweets 6

Russian Botnet Operator Busted For Infecting 6 Millions of Computers & Stealing £2.9 Million

6 Millions of Computers & Stealing £2.9 Million



Russian Police authorities have arrested a 22 year hacker from Southern Russia known as "Hermes" and "Arashi" in online communities. According to the reports the suspect was running a botnet which comprised more than 4.5 million computers while making it the largest publicly known botnet to date. It has been also found that the hacker used banking trojans to steal more than 150 million roubles, almost £2.9 million, from private individuals and organisations. According to the statement of Russian Interior Ministry the trojan is believed to have infected more than six million computers. On some days, more than 100,000 new computers were recruited. The authorities also confirmed that the arrest of "Hermes" and other members of his hacker group was carried out with the assistance of anti-virus company Dr. Web. Most of the accomplices lived in Moscow and St. Petersburg. We also like to give you reminder that couple of months ago another Russian hacker who was the creator of the **Bredolab botnet** received a four-year imprisonment by Armenian court.

Site search

We're on  Follow

+1  +174

Follow @voiceofgreyhat

Enter Your Email here.

RSS Feed  

Cyb3r-W4r #Unseen & #Uncut

VOICE OF GREY HAT

VOUCH RELEASE III

EVER-W4R

Download NOW

DoS – Denial of Service

- Este tipo de ataque está en crecimiento, por la cantidad de botnets existentes y lo fácil que es generarlos.
- En 2011, los principales motivos detrás de los ataques fueron de índole ideológica (35%) y vandalismo (31%)
 - Una gran parte fue generada por Anonymous
- La mayoría de los ataques llegan a 10Gbps
 - Hay reportes de ataques que indican la generación de un total de 60Gbps!
 - ¿Puedes imaginar que ésto pase en tu red?
- ¡El Firewall *stateful* y el IPS no son eficaces para este tipo de ataque!
 - **Agotamiento del cuadro de estado.**

alice2  CLARA

Violación de Copyright

- Hacer download de material protegido por propiedad intelectual ilegalmente.
 - Películas, canciones, software, documentos
- Incidente común hoy en día
 - Especialmente en redes académicas debido a ancho de banda disponible
- Asociaciones como Irdeto, SafeNet, ESA monitoran y advierten este tipo de actividad
 - Paramount, Zenimax, Actvision



42%
WORLDWIDE SOFTWARE
PIRACY RATE



Alice2 European Union CLARA

Violação de Copyright

Infringing Work: Harry Potter and the Chamber of Secrets

Filename:
John.Williams.Harry.Potter.and.the.Chamber.of.Secrets.pdf

First Found: 27 May 2009 15:01:13 EDT (GMT-4)

Last Found: 27 May 2009 15:01:13 EDT (GMT-4)

Filesize: 29,609k

IP Address: 200.200.200.200

IP Port: 21408

Protocol: eDonkey

Username: <http://emule-project.net>



Alice2 European Union CLARA

Violación de Copyright

“Through the Berne Convention and other international treaties covering intellectual property rights, ESA and ABES believe that their members' rights in such entertainment software products are entitled to the full protection of the Brazilian intellectual property laws, specifically **laws 9.609 and 9.610**, executed February 19, 1998. Moreover, we believe that the infringement(s) described below is(are) in violation of other Brazilian Laws, including Unfair Competition and Trade Marks Law (Law 9.279, of 14-05-96); Computer Programs copyrights law (Laws 9.609 and 9.610, of 19-02-98); Crimes against the Tributary Order Law (Law 8.137/90) and Tax Evasion Law (Law 4.729/65); and Crimes against the Consumer Protection Act (Law 8.078, of 11-09-90).”



MALWARE: DID YOU KNOW?

PERCEPTION



83%

BELIEVE LEGAL SOFTWARE IS MORE SECURE THAN PIRATED

REALITY

NEARLY **60%** OF PC USERS ADMIT PIRATING SOFTWARE

COUNTERFEIT CAN HOST MALWARE WHICH CAN LEAD TO...

-  **STOLEN ID & FINANCIAL DATA**
- TURNING PCs INTO SPAMBOTS**
-  **DAMAGING HARD DRIVE**
-  **SPREADING VIRUSES**

TO LEARN HOW TO AVOID COUNTERFEIT SOFTWARE GO TO: HOWTOTELL.COM







¿Qué preparación tiene su institución para tratar con incidentes de seguridad?

¿Qué hacer ante este escenario?




¿Qué hacer ante este escenario?

- Para fines organizacionales, una de las principales defensas es la creación de un CSIRT
- CSIRT = *Computer Security Incident Response Team*, o Equipo de Respuesta ante Incidentes de Seguridad

"Una organización o equipo que ofrece servicios y apoyo, a un grupo definido, para la prevención, manejo y respuesta a incidentes de seguridad informáticos" - CERT / CC





Reflexión

“El grupo Anonymous realizó un ataque DoS que está ocupando todo el link de la NREN. El ataque ya tiene dos horas, en horario de oficina. Es imposible navegar por internet y tener acceso a los servicios de los clientes. No se sabe cuándo terminará y el grupo anunció que realizará otras acciones en lo que queda del día.”





CLARA



Reflexión

- En el escenario actual de su organización, ¿Quién lidiaría con este incidente? ¿Hay personas o un equipo responsable por ello?
- ¿Quién debería participar en el equipo?
- ¿Cómo debe ser tratado este incidente?
- ¿Su organización está preparada para responder ante este tipo de incidente?
- ¿Qué debe cambiar en su organización para lidiar con este tipo de situación?

¡Esperamos que este curso le ayude a resolver estas preguntas!





CLARA



Preguntas



GT-CSIRT gt-csirt@listas.redclara.net
Carla Freitas carla@cais.rnp.br



CLARA