Introducción

Conociéndonos y alineando expectativas

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*

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 infra-estructura 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 operacional: Windows o Linux
    - ❑ Vmware Player 4.0 o superior, o Vmware Workstation 7.0 o superior.
  - Distribución de imágenes (MVs y Vmware Player)

Presentación

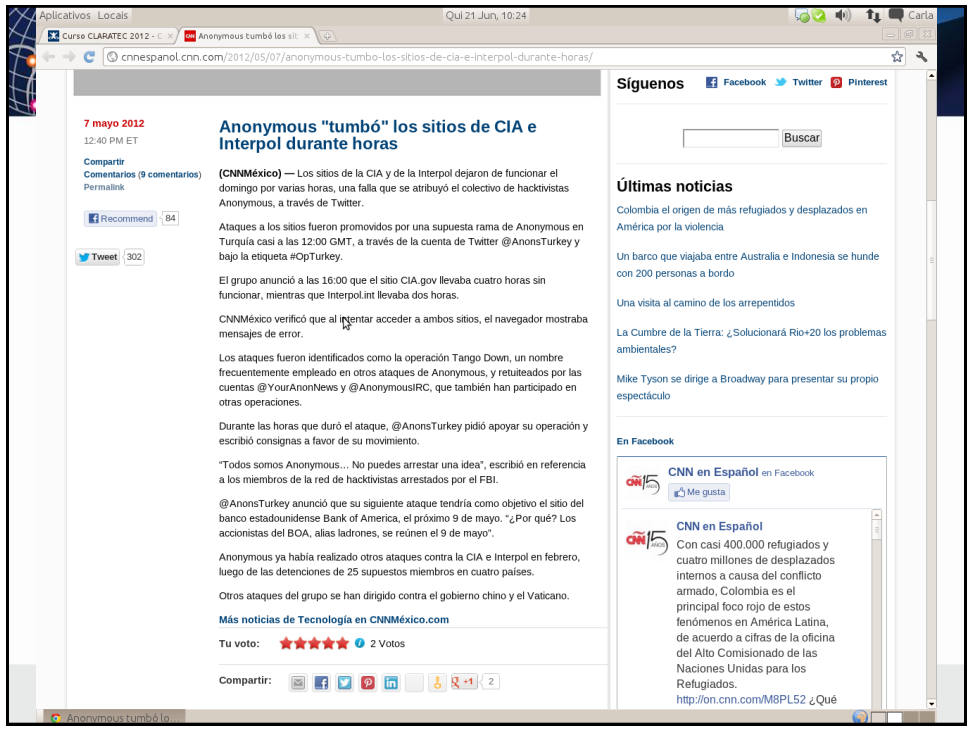
- Nombre
- Función
- Organización
- ¿Tiene CSIRT?
- ¿Tiene experiencia en el tratamiento de incidentes?
- ¿Fue designado como responsable por seguridad?
- Expectativas del curso

Preguntas

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

Contextualización

Por que estamos aquí?


Aplicativos Locais
Qui 21 Jun, 10:24
Carla
Curso CLARATEC 2012 -
Anonymous tumbó los sit
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 84
Tweet 302
Anonymous "tumbó" los sitios de CIA e Interpol durante horas
(CNNMéxico) — Los sitios de la CIA y de la Interpol dejaron de funcionar el domingo por varias horas, una falla que se atribuyó el 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.
CNNMéxico 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 CNNMéxico.com
Tu voto: 2 Votos
Compartir:
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 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
Anonymous tumbó lo...


Aplicativos Locais
Qui 21 Jun, 10:24
Carla
Curso CLARATEC 2012 -
Anonymous tumbó los sit
Anonymous dice haber tu
cnnespanol.cnn.com/2012/03/07/anonymous-dice-haber-tumbado-el-sitio-de-internet-del-vaticano-2/
We will donate US$2 to a charity of your choice
Click Here
CNN
GO BEYOND BORDERS
ADVERTISEMENT
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) –Vatican.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 operativa" 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.
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 Rio+20 los problemas ambientales?
Mike Tyson se dirige a Broadway para presentar su propio espectáculo
En Facebook
Anonymous dice hab...

Datos de incidentes en el mundo

Cada día, se identifican 9.500 sites maliciosos nuevos

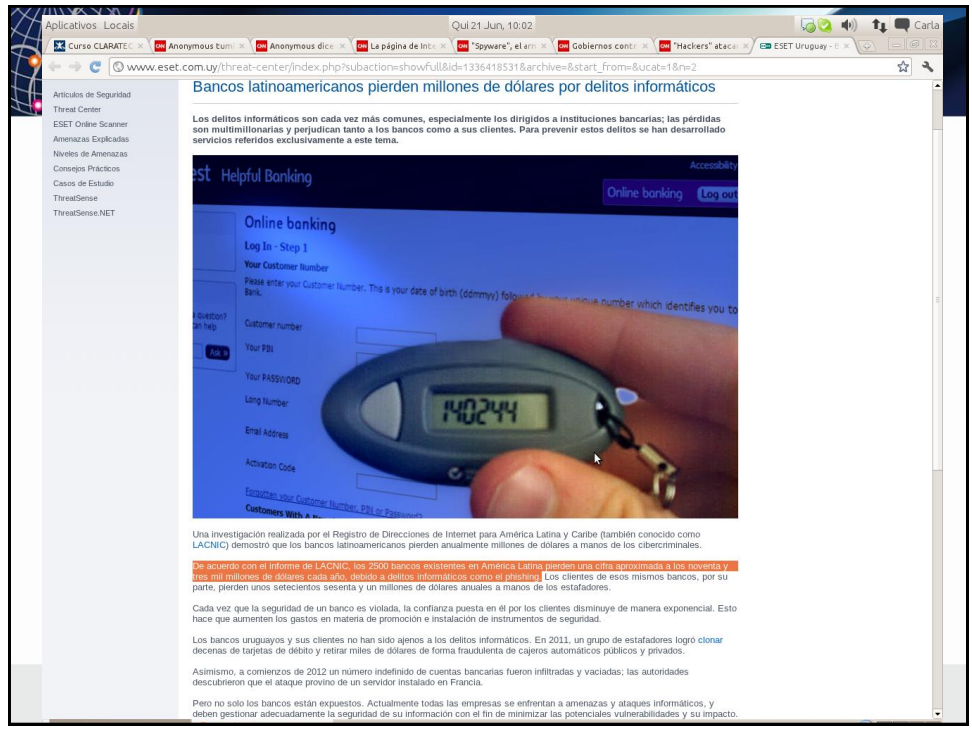
Diariamente, entre 12 y 14 millones de las búsquedas realizadas entran a sites maliciosos

Al día, hay 300 mil alertas de download de malware

Fuente: Google

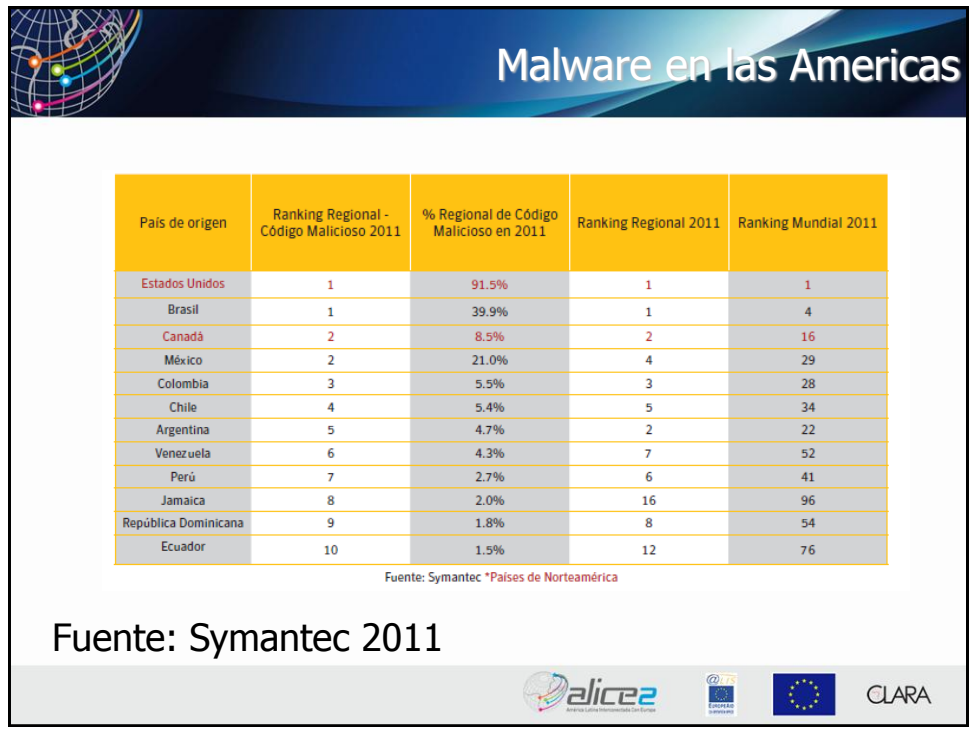
"Pero eso sólo ocurre en los EUA y Europa! Nosotros no somos objeto de este tipo de ataques."

¿Será verdad?



“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.”


TARINGA!
Identificarme
REGISTRATE YA!
Buscar...
Posts
Comunidades
Música
Juegos
TOPs
Global
Inicio
Novatos
Destacados
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
595
47
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
País 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
CLARA

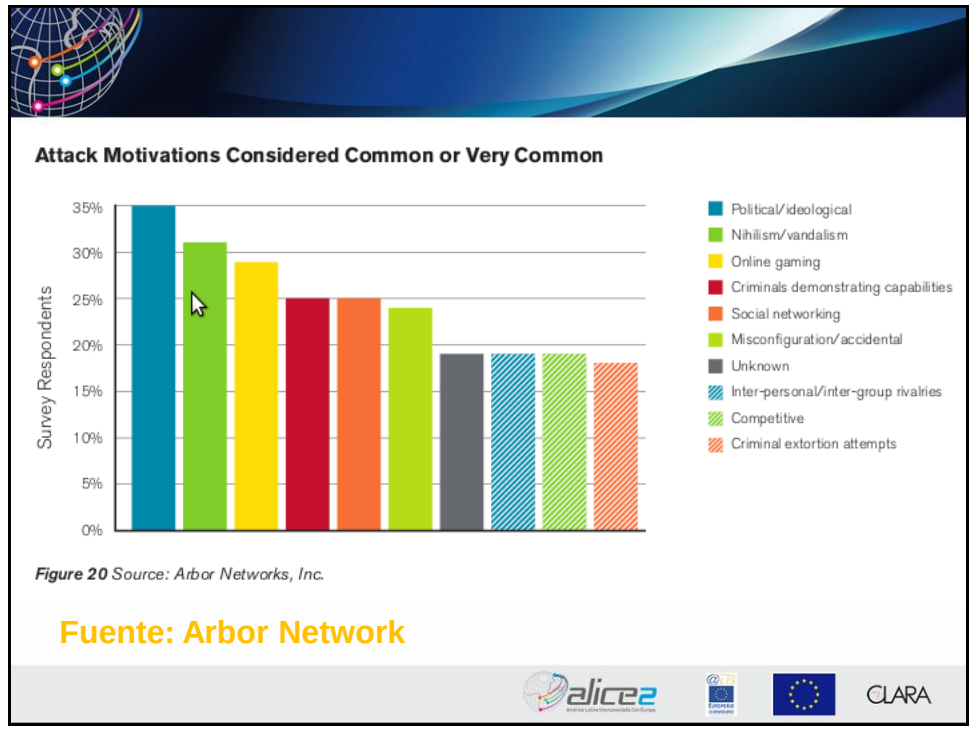
"¿Cuál es la motivación para estos ataques?"


Aplicativos Locais
Qui 21 Jun, 09:46
Carla
idgnow.uol.com.br/internet/2012/06/08/falha-usada-pelo-virus-flame-valeria-us-1-milhao-no-mercado-negro/
IDGNOW!
tecnologia em primeiro lugar
TÓPICOS
ÚLTIMAS NOTÍCIAS
INTERNET
MOBILIDADE
TI CORPORATIVA
TI PESSOAL
BLOGS
IT Verticals
Segurança
Falha usada pelo vírus Flame valeria US$ 1 milhão no mercado negro
Tim Greene, Network World (US)
08 de junho - 17h49 - Atualizada em 09 de junho - 03h20
Malware explorou brecha na autoridade de certificação do Microsoft Terminal Services, e gerou falsas assinaturas para se fazer passar por atualizações legítimas
Notícias Relacionadas
Certificados falsos da Microsoft foram usados no 'supervírus' Flame
Entenda tudo sobre o 'supervírus' Flame
'Supervírus' espião é o mais complexo já descoberto
Antes de ser descoberto, a parte do código do supervírus Flame que explora uma brecha no Microsoft Update poderia ter sido vendida por US$ 1 milhão no mercado negro de malware, diz um pesquisador de segurança.
"Essa descoberta vale muito dinheiro", diz Marcus Carey, pesquisador de segurança da empresa Rapid7, "pelo menos seis dígitos e provavelmente mais - o que mostra o quão sofisticado é".
Desde que o Flame e seus componentes foram desmascarados, porém, que tudo mudou. "Ninguém vai pagar isso agora", diz.
A vulnerabilidade rara foi descoberta no domingo, quando a Microsoft lançou um raro update de segurança para consertá-la. É uma parte obscura de uma plataforma complexa e furtiva que ficou sem ser detectada por mais de quatro anos.
Em particular, o Flame explorou uma brecha na autoridade de certificação do Microsoft Terminal Services, e gerou falsas assinaturas digitais que o malware usou para se fazer passar por atualizações legítimas da Microsoft. Isto permitiu que os atacantes alterassem e atualizassem o código à vontade.
Mas isso foi apenas um recurso da arquitetura. Outros elementos sofisticados incluem a capacidade de apagar todas ou algumas partes de si mesmo nas máquinas infectadas e depois eliminar qualquer vestígio.
Ele também tinha uma infra-estrutura de comando e controle "diferente de tudo que já vimos antes", de acordo com pesquisadores da Kaspersky Lab. Ele operava a partir de 80 domínios, e os servidores envolvidos foram aparentemente equipamentos
Publicidade
Microsoft
Teste o Windows Azure por 90 dias grátis.
A plataforma na Nuvem para construção, hospedagem e escalabilidade de aplicações.
Windows Azure
+ Notícias
Internet
Nova geração de vírus bancários faz transferências invisíveis
As 10 coisas mais irritantes do Facebook
Usuária entra com ação coletiva contra o LinkedIn após vazamento
Parque do Ibirapuera e Mercadão lideram acessos ao Facebook em SP
Escolas só usam computadores nas aulas de informática
+ Lidas
+ Comentadas
As 10 coisas mais irritantes do Facebook
Usuária entra com ação coletiva contra o LinkedIn após vazamento
Quase 10 mil sites maliciosos surgem por dia, diz Google
Opinião: Por que o Google+ ainda pode derrotar o Facebook
Falso antivírus para Android usa tecnologia do temido vírus Zeus
Vídeo Recente
Ver todos »
Microsoft apresenta a família de
Anonymous tumbó l...
Falha usada pelo víru...


Ideológicos
alice2
CLARA

Políticos

Represalias



Fuente: Arbor Network

SPAM

SPAM

~ 80% de los mensajes de correo electrónico son SPAM

Fonte: CelloPoint Security, Maio 2012

SPAM

Un
cue
ecibe
l día.

40GB de espacio ocupado con SPAM al día!

Y al mes?

disco

Phishing

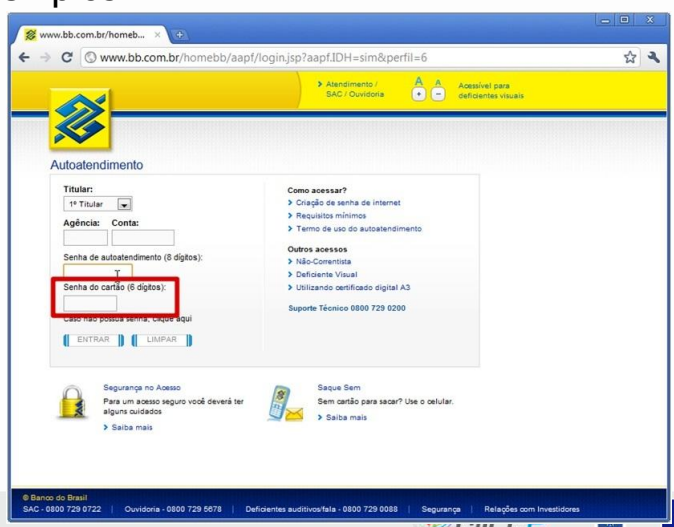
- Principal tipo de SPAM
- Uso de un tipo de ingeniería social para intentar adquirir información confidencial, como: contraseñas, datos bancarios, etc.
- El estafador se hace pasar por una persona o empresa de confianza
- Principales medios utilizados:
  - E-mail
  - IM
  - Web-Site

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"

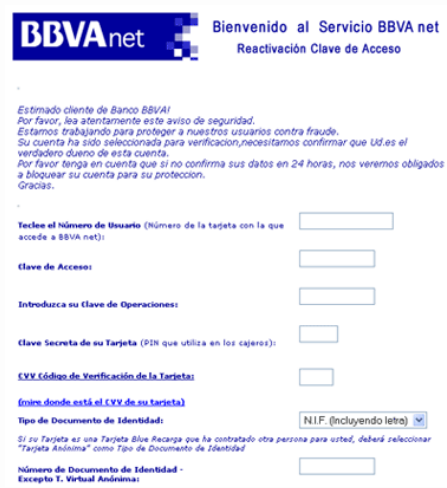
Phishing

- Ejemplos:



Phishing

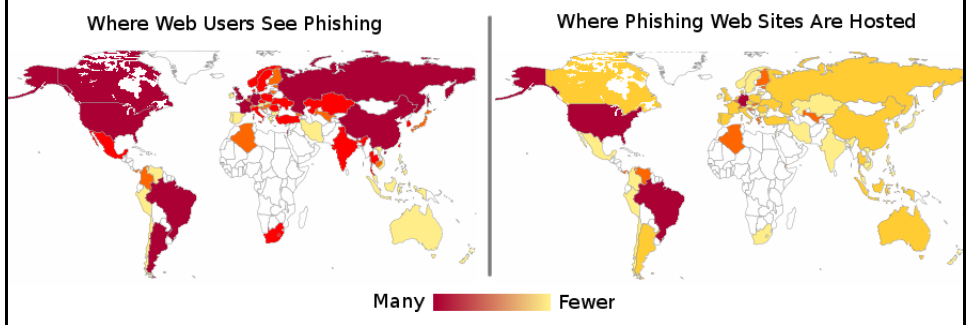
- Ejemplos:



Phishing

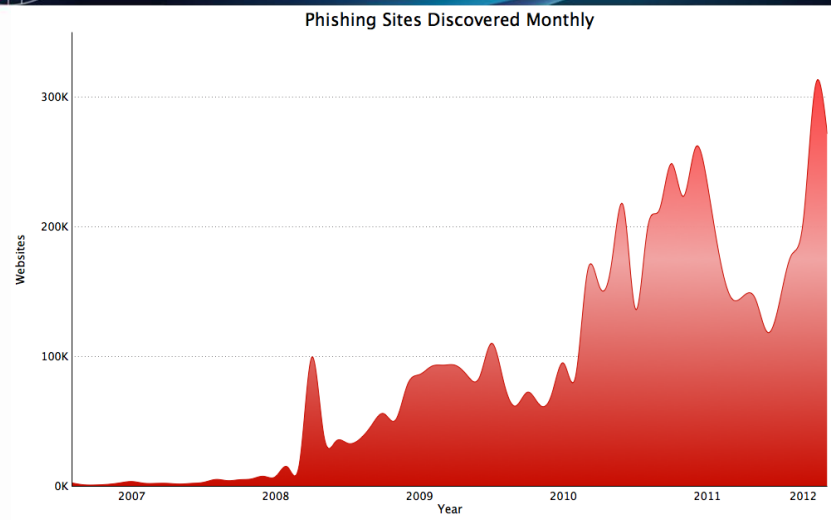
- Ejemplos:

Estadísticas de phishing



Fuente: Google

Estadísticas de phishing



Fuente: Google

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
  - Alojan información ilegal, como pornografía infantil
  - Roban informaciones personales y financieras
  - Obtienen información para fines publicitarios

Tipos de Malware

Spyware

Keylogger

Virus

Bot

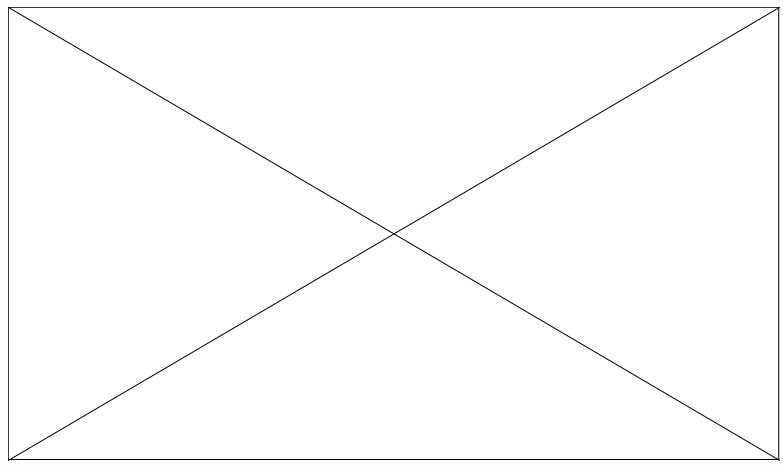
Worm

Trojan

Backdoor

¿En qué se diferencian?

Tipos de Malware

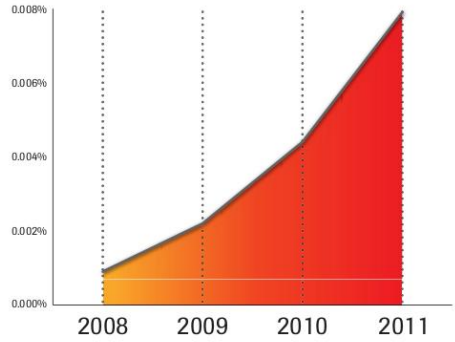


Malware

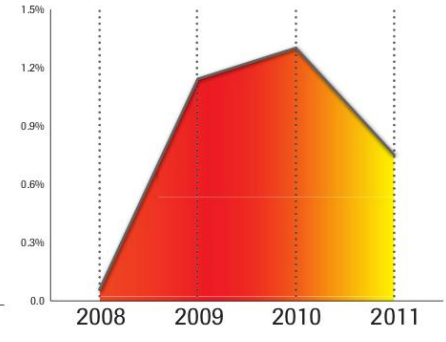
En 2011, diariamente fueron creados 73.000 nuevos ejemplares de malware (Fuente: Panda Security)

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

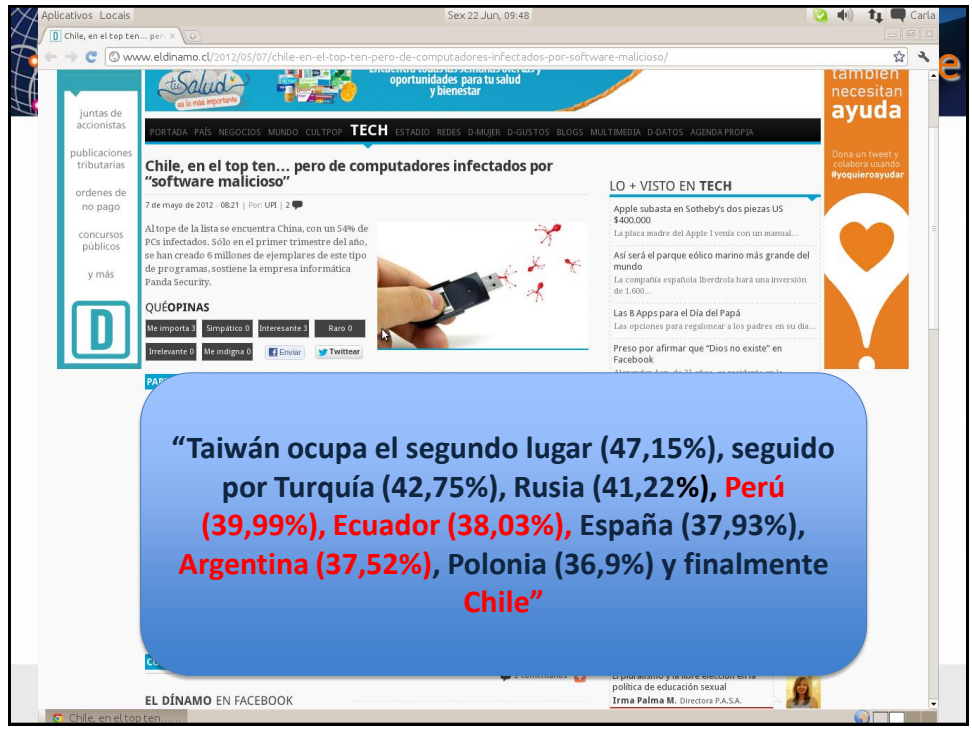
Malware



Percentage of Executable Attachments



Percentage of Viruses Detected


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

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.

Spotlight on South America

The data details basic counts HTTP bots over the past few weeks, for Brazil, Argentina and Chile.

Certainly Brazil has the largest share of infections, of course as well as the most computers. There are multiple factors that impact these statistics, but it's interesting that the relative proportions seem to fluctuate in tandem with each country.

TEAM CYMRU
WWW.CYMRU.COM
@teamcymru

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.

Violación de Copyright

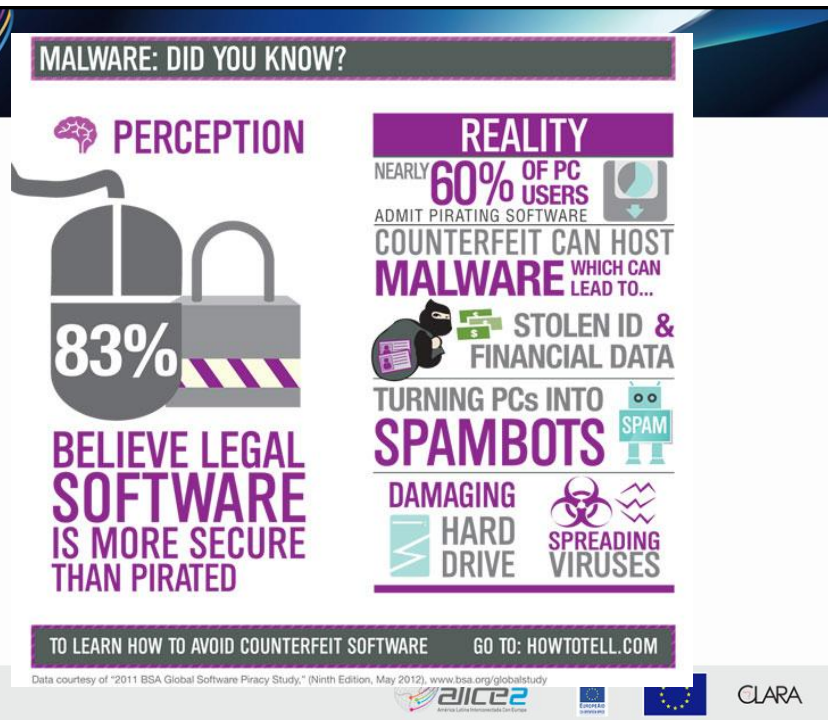
- Hacer download de material protegido por propiedad intelectual ilegalmente.
  - Películas, canciones, software, documentos
- Incidente común hoy en día
  - Especialmente en redes académicas devido a ancho de banda disponible
- Asociaciones como Irdeto, SafeNet, ESA monitoran y advierten este tipo de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

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
```

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)."



Violação de Copyright

URLs requested to be removed from Search per week

Copyright removal requests received for Search in the past month

1,246,713	URLs Requested to be Removed
24,129	Targeted Domains
1,296	Copyright Owners
1,087	Reporting Organizations

Top Reporting Organizations in the Past Month

	URLs
Marketly llc	461,851
BPI (British Record...	190,621
NBCUNIVERSAL	145,934
Takedown Piracy L...	104,936
DtecNet	96,242

Top Copyright Owners in the Past Month

	URLs
Microsoft Corporation	543,378
BPI (British Record...	162,601
NBCUNIVERSAL	145,934
Elegant Angel	39,990
RIAA member com...	33,462

Top Targeted Domains in the Past Month

	URLs	%
filestube.com	43,469	< 0.1%
torrentz.eu	23,131	< 0.1%
4shared.com	22,259	< 0.1%
zippyshare.com	19,420	< 0.1%
kat.ph	18,781	< 0.1%

Fuente: Google 2012

Papel del GT-CSIRT

- Aumentar la capacidad de respuesta a incidentes de seguridad en Latino América

¿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."

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!

Preguntas

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