

BugCON v0.1  
Hacking & (IN)Security



17 de Mayo  
Ciudad de México

# One Shot Phishing On Local Area Networks

BugCON v0.1  
Hacking & Insecurity

Hector Leal Morales

Los ejemplo realizados en esta presentación son con fines educativos,  
el mal uso de la información no es responsabilidad del ponente de esta platica.

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)



17 de Mayo  
Ciudad de México

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

# ¿ Phishing ?

- Es la contracción de "**P**assword **H**arvesting **F**ishing" (cosecha y pesca de contraseñas).
- Diseñado con la finalidad de robar la identidad de alguien.
- Es una realidad de la hostilidad actual en los medios de comunicación y es altamente efectiva para todos aquellos que no son técnicos computacionales y para los que si lo son.



17 de Mayo  
Ciudad de México

# Lo mas común del Phishing

- Robo de identidades bancarias.
- Robo de cuentas de correo.
- Falsificación de sitios con ánimos de lucro.
- Falsificación para propagación de virus.
- Robo de identidades para pagos en línea.
- Falsificación de sitios para inmigrantes.
- Robo de identidades para sitios de descarga de software de pago.



17 de Mayo  
Ciudad de México

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

# Análisis

- El 25% de las visitas a un sitio de phishing se produce durante la primera hora del lanzamiento del fraude.
- Durante las 6 primeras horas del ataque se llegarían a concentrar el 51.6% de las visitas, entre las 6 y 12 horas aumenta un 10.7%, entre las 12 y 24 horas se suma un 13%, y el 24.6% de las visitas restantes se suceden transcurridas las primeras 24 horas.



17 de Mayo  
Ciudad de México

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

# Análisis continuación...

- Los servicios anti phishing reactivos mantienen medias superiores a las 6 horas para el cierre de un ataque.
- Un informe de la empresa de investigación de mercado Gartner habla de unas pérdidas de 3,200 millones de dólares por culpa del phishing en 2007.
- De agosto del 06 a agosto del 07 son 3.6 millones de usuarios los que han perdido los más de 3,000 millones de dólares en 2006.



17 de Mayo  
Ciudad de México

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

# ¿ Pharming ?

- Consiste en suplantar el sistema de resolución de nombres de dominio.
- También puede ser la explotación de vulnerabilidades en el software de los servidores DNS.
- Es otra muestra de la hostilidad real de los medios de comunicación.
- Muy buena modalidad para ataques y si se combina con phishing pueden ser en la mayoría de casos de tipo **One Shot.**



17 de Mayo  
Ciudad de México

# De lo famoso del Pharming

- La vulnerabilidad de los routers ADSL en 2wire modelos 1701HG, 1800HW y 2701.
- La combinación con Phishing de Banamex.
- El ataque a través de postales de Gusanito.



# ARP SPOOFING

- Suplantación de identidad por falsificación de tabla ARP.
- También conocido como ARP Poisoning o ARP Poison Routing.



# DNS SPOOFING

- Suplantación de identidad por nombre de dominio.
- También conocido como caché Poisoning.



# Demostración Sencilla

- Preparación
  1. Seleccionar el objetivo
  2. Instalar el Software Necesario
  3. Suplantar lo necesario
  4. Codear los scripts de captura
  5. Pruebas necesarias
  6. Justificar errores
  7. Mejoras de funcionamiento
  8. Realización del ataque (pidan permiso)



# 1. Seleccionar el objetivo

**Ejemplo en red local  
www.hi5.com**

**Razones:  
Sencillo  
Rápido  
Muy utilizado**



## 2. Instalar el Software Necesario

- **apt-get install**
  - Apache
  - Php
  - Mysql
  - Ettercap



**3. Suplantar lo necesario**

**4. Codear los scripts de  
captura**

**5. Pruebas necesarias**

**Video Numero 1**



17 de Mayo  
Ciudad de México

## 6. Justificar errores

- Utilizar de manera real todos los otros links.
- En caso de no poderse, poner pagina de disculpa.
- Inventar causas externas al mal funcionamiento.
- Proporcionar todos los datos de contacto para reportar fallos.



17 de Mayo  
Ciudad de México

# 7. Mejoras de funcionamiento

- Utilizar herramientas de diseño o recibir ayuda de un diseñador.
- Crear actualizaciones de las paginas o cosas suplantadas.
- Mejorar los servicios de nuestro objetivo.
- Utilizar servicios de correo electrónico.
- Utilizar alianzas.



17 de Mayo  
Ciudad de México

# 8. Ataque real

## Video 3 Linux

## Video 4 Windows



17 de Mayo  
Ciudad de México

# ¿ Que podemos hacer ?

- Uso de routers con anuncios constantes.
- Tablas de ARP estáticas.
- Uso de herramientas de monitoreo como arpwatch u otros.
- Administración y monitoreo de la red.
- Ejemplo con ettercap.



17 de Mayo  
Ciudad de México

# Otro ejemplo con ettercap

## Video de arp\_cop

**BugCON v0.1**  
Hacking & (IN)Security



**17 de Mayo**  
**Ciudad de México**

# Muchas Gracias

# Hector Leal Morales

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)

[www.zonartm.org/BugCON](http://www.zonartm.org/BugCON)