Tendencias en Ataques Informáticos

Iván Arce

Core Security Technologies
Florida 141 7mo Piso
Buenos Aires, Argentina
(+54-11) 5032-2673
www.coresecurity.com

AGENDA DE HOY

- Prólogo
- Esos raros ataques nuevos (?)
- Futurología y otras disgresiones
- Epílogo

PROLOGO

Presentación del disertante

Quién es este tipo?? De donde salio? Por qué habla de esto?

- **CTO y co-fundador de Core Security Technologies (1996)**
- **Core Security Technologies es una empresa que:**

- **Esta involucrada con la investigación de vulnerabilidades de software desde su fundación**
  - Alrededor de 50 reportes de seguridad (*advisories*) publicados
  - Cientos de vulnerabilidades descubiertas y reportadas
  - Coordinación con Microsoft, Cisco, Sun, SGI, IBM, Digital, HP, Linux, Novell,.
  - Pioneros del proceso de “disclosure” (…de algún tipo…)

- **Desarrolla y comercializa un producto de software para realizar pruebas de intrusión (*penetration tests*) que incluye código de explotación**
  - CORE IMPACT

- **Comercializa servicios de auditoría de código, pruebas de intrusión y capacitación en temas relacionados.**
  - Empresas de software, de seguridad, grandes empresas

Queremos ver las cosas desde la perspectiva del atacante

De donde salió este tipo?

- **Pensamos que para tener una estrategia de seguridad efectiva hace falta defensa y ataque**
- **Inspirados por algo que escribieron Wietse Venema y Dan Farmer…**

  ***Improving the Security of Your Site by Breaking Into it* (1994)**

- **Convertimos esta filosofía en parte de nuestro trabajo diario**

… y nos divertimos bastante…

La perspectiva del atacante

Atacantes y ataques

- **Principio del menor esfuerzo**
- **Desafio al ingenio**
- **Superación técnica**
- **Reconocimiento de los pares**
- **Científicos, tecnólogos y hombres de negocios**
- **Fama y dinero**
- **Bien común**

...pero antes de seguir convengamos algunos términos...

TERMINOLOGÍA

- **Explotar**

  "Utilizar en provecho propio, por lo general de un modo abusivo, las cualidades o sentimientos de una persona, de un suceso o de una circunstancia cualquiera." (RAE)

- **Falla**

  "*Defecto material de una cosa que merma su resistencia.*" (RAE)

- **Vulnerabilidad**

  "Falla en un sistema que, de ser explotada, causa un efecto negativo en la seguridad de dicho sistema"

Vulnerabilidad, expuesto, falla, agujero, ***bug*** (bicho?)

Que es el código de explotación?

CODIGO DE EXPLOTACION

- **Código de explotación (*exploit*)**

  "Algoritmo, programa o herramienta desarrollada para explotar una vulnerabilidad y lograr un objetivo específico"

- **Prueba de concepto del código de explotación (PoC)**

  "Código de explotación cuyo unico objectivo es demostrar la existencia de una vulnerabilidad"

- **Vulnerabilidad de día cero** *(0-day vulnerability)*

  "Vulnerabilidad para la que el conocimiento de su existencia no es de accesso público"

- **Código de explotación de día cero** *(0-day exploit)*

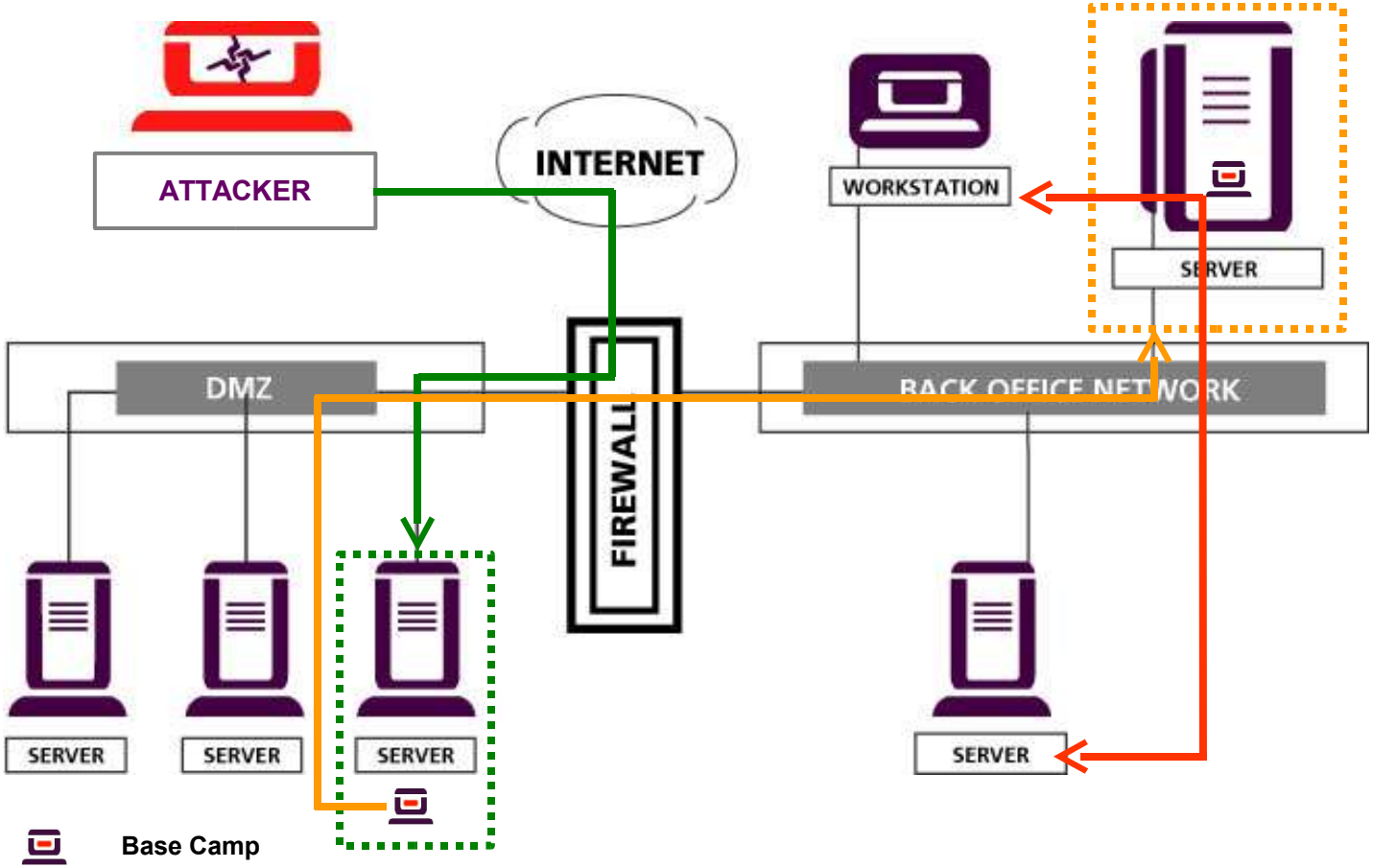
  "Código de explotación para una vulnerabiliad de día cero"

ESOS RAROS ATAQUES NUEVOS

Tendencias de ataque “recientes”

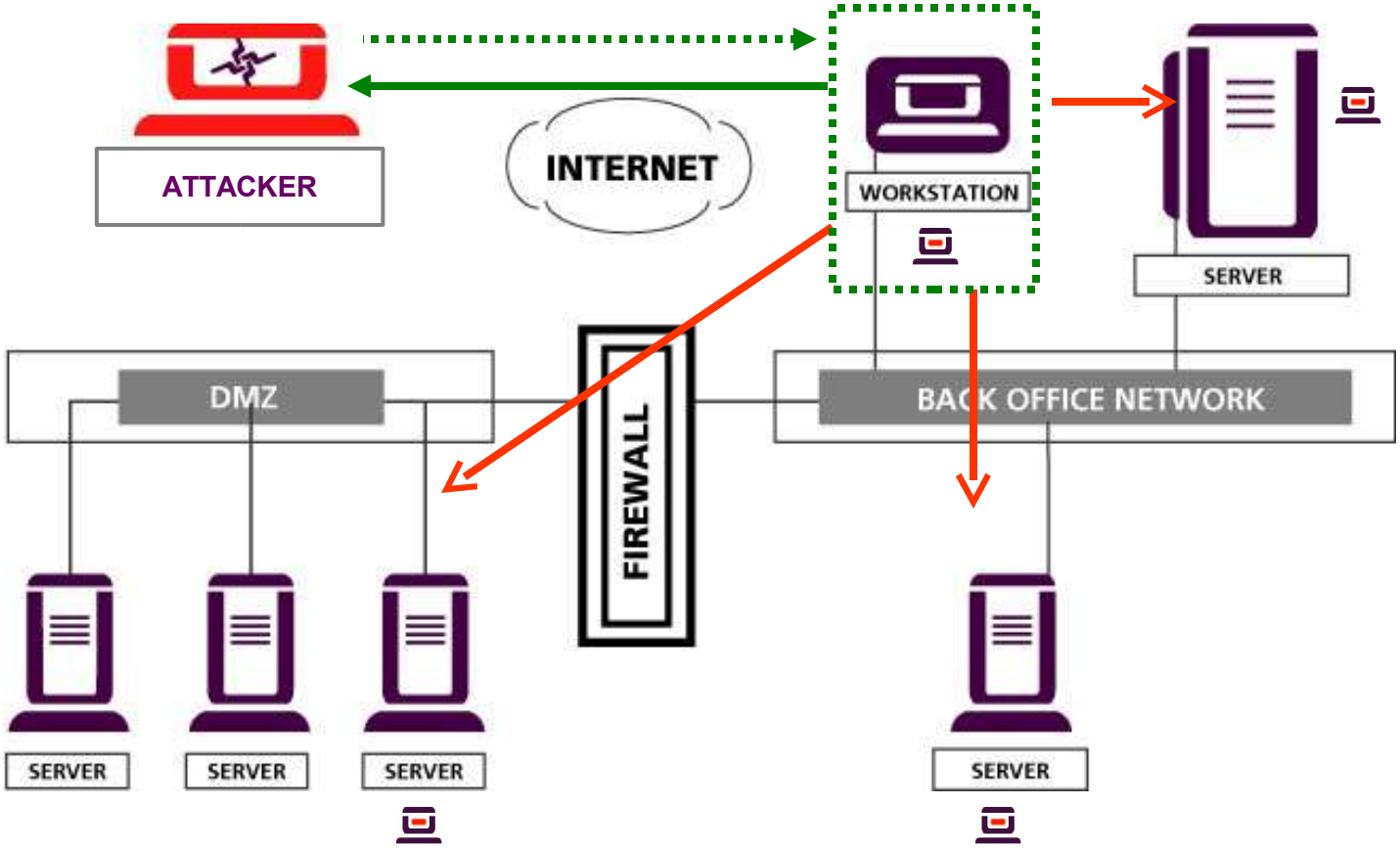
El escenario clásico de un ataque externo: Servers en la DMZ

ANATOMIA DE UN ATAQUE CLASICO



Hoy el eslabón mas débil es la estación de trabajo

ATAQUE A LA ESTACION DE TRABAJO



Por qué atacar una estación de trabajo?

ATAQUES A LA ESTACION DE TRABAJO

- **Ley del menor esfuerzo**
- **Cúmulo de aplicaciones vulnerables (*client-side exploits*)**
  Web browser, lector de email, Media players, Instant Messaging
  Aplicaciones de negocios, adminitrativas y de oficina, file viewers, utilitarios, agentes de resguardo (backup) y seguridad (PF,AV,IDS)
  Componentes re-usables y de terceros
- **Díficil control de Inventorio y Cambios**
  Que estaciones hay en la red, direcciones IP, software instalado, usuarios
- **Díficil control instalación de contra-medidas**
  Patches, politicas de accesso, etc
- **Operada por usuarios despreocupados y/o novatos**
- **Cuestión de escala y probabilidad de éxito**
- **Es la puerta principal a la red**
  "The Weakest Link revisited" - IEEE S&P magazine vol.1 no.1

El código de explotación evolucionó

CODIGO DE EXPLOTACION

- **Código de explotación separado en componentes**
  - Shellcode monolítico (1989-1994-2000)
  - Aislación funcional: ***Vector de ataque, adquisición del control de flujo, código-objectivo***

- **Componentes re-usables**
  - Técnica de de explotación
  - Método de conexión
  - Funcionalidad final
  - “Stagers”
- **Implementación de “técnicas” de explotación**
  - Sobre-escritura de pila (*stack*), *heap*, *exception handler*,
  - Signal handlers, GOT, PLT, vpointers, protección de la pila, DEP, etc, etc, etc.
  - etcétera
- **Técnicas anti-detección y prevención**
  - Polimorfismo, metamorfismo, encoding, fragmentación (red)
  - Syscall proxying, agentes multi-proposito, volatilidad, *rootkits (host)*

- **Una nueva generación de atacantes**

  "The Shellcode Generation" - IEEE S&P magazine vol.2 no.5

Hay nuevos vectores de ataque

LOS NUEVOS VECTORES DE ATAQUE

- **Redes inálambricas**
  - 802.11
  - Bluetooth
- **Nuevas interfases para periféricos**
  - Firewire
  - USB
  - SCSI, PCMCIA, etc.
- **Nuevos dispositivos “conectados”**
  - PDA, teléfono celular, cámara de fotos, consola de juegos
  - Electrodomesticos
  - Automobiles (?!)
- **La superficie de ataque se amplió**

"The Rise of the Gadgets" - IEEE S&P magazine vol.1 no.5

“Bad Peripherals" - IEEE S&P magazine vol.3 no.1

Los dispositivos de red son una amenaza?

LOS DISPOSITIVOS DE RED

- **La separación entre hardware y software es difusa**
  - Visión hermética del hardware (obscuridad)
  - Existe un dispositivo de red SIN software?
  - Routers, switches, load-balancers, centrales de teléfono privadas (y públicas!)
  - Impresoras, teléfono VoIP, sistemas de almacenamiento
- **Uso de sistemas operativos embebidos**
  - Cisco IOS
  - VxWorks
  - JavaVM
  - Linux
  - Windows CE
  - Symbian OS
- **Implementaciones nuevas de software de base**
  - Estado de seguridad inmaduro
  - Repetición de viejos errores
  - Proceso de desarrollo desligado de la seguridad
  - Denegación de servicio es un síntoma, no necesariamente un objetivo
- **La potencial fuente de origen de ataques se amplió**

A todo ello se suman una serie de ”nuevos problemas”

LOS OTROS ATAQUES

- **Aplicaciones Web**
- **SPAM**
- **Malware**
  - Virus
  - Spyware, adware, dialers
  - Worms
  - Rootkits, Bots, caballos de toya, zombies
- **Phising**
- **Ataques “semánticos”**
- **<u>El destinatario del ataque es una persona física</u>**

FUTUROLOGIA Y OTRAS DISGRESIONES

Algunas “predicciones”

FUTUROLOGIA

- **La distinción entre ataques “tradicionales” y ataques “híbridos” desaparece**
- **La estación de trabajo se explota masivamente**
- **Las técnicas de explotación “sofisticadas” se vuelven masivas**
- **Las nuevas plataformas de ataque se explotan selectivamente**
- **Los nuevos vectores de ataque se explotan selectivamente**
- **La distinción entre HW y SW deja de tener sentido**
- **La distinción Red/Server/Estación de Trabajo deja de tener sentido**

DISGRESIONES PSEUDO-ALEATORIAS

- **La investigación y desarrollo “alternativo” se mueve hacia el Este**
  - EEUU
  - Europa
  - China

- **Las investigacion y desarollo “alternativo” se mueve hacia Afuera**
  - EEUU
  - Alemania, Francia, Rusia
  - China, Corea, Polonia, Rumania, Argentina, Brasil

- **El paradigma de ataque cambia**
  - Inyección de código
  - Ejecución de código
  - Ingeniería social
  - ??

EPILOGO

Y entonces…que hacer?

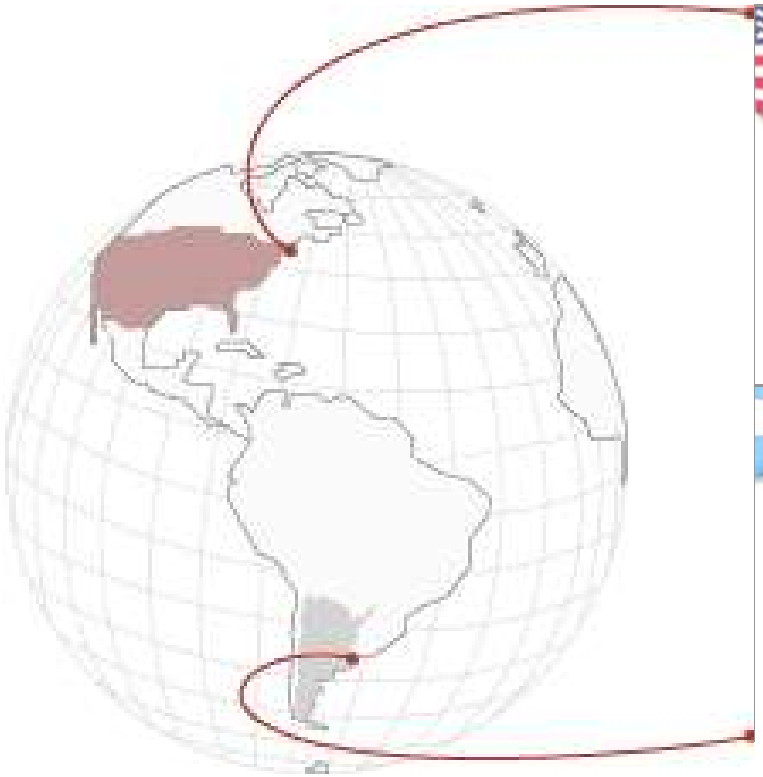
EPILOGO

- **Adoptar la visión del atacante**
  - Pensar y hacer
  - Ensuciarse las manos con código
- **Preparar defensas y herramientas**
  - Detección
  - Prevención
  - Vision contextual a escala local y global
  - Análisis forense
- **Evitar la exclusión y alienación**
- **Adoptar seguridad como un <u>proceso</u>**
  - Defensa y ataque se complementan

PREGUNTAS

GRACIAS!

CONTACT INFORMATION



Headquarters · Boston, MA
46 Farnsworth St
Boston, MA 02210 | USA
Ph: (617) 399-6980 | Fax: (617) 399-6987
info@coresecurity.com

Research and Development Center
Argentina (Latin America)
Florida 141 | 2º cuerpo | 7º piso
(C1005AAC) Buenos Aires | Argentina
Tel/Fax: (54 11) 5032-CORE (2673)
info.argentina@coresecurity.com

www.coresecurity.com