ACIS XI Jornada de Seguridad Informática
Seguridad de la Información:
Una nueva década para avanzar

De Artefactos Sofisticados Persistentes y Otros Demonios

Julio Alvarez
MSc Autonomous Systems,CISSP, PMP

16 Junio de 2011

Que no es esta presentación:

- Definición estudio análisis de APTs
- Charla técnica
- Resumen de tendencias
- Una bola de cristal o Walter Mercado de lo que viene

Que tiene esta presentación:

- Reflexión / Percepción a la luz del entorno actual
- Exorcismo
- Compartir preocupaciones
- Llamado a esfuerzos comunes

Palabras claves

- Escenario amenazas actual
- Hechos relevantes 2011
- Complejidad
- Personas, Procesos, Tecnología
- Paranoia colectiva
- Necesidades reales Vs inventadas: Volver a lo básico, es posible decir que no

De donde el nombre

- Complejidad
- De aquello que no entendemos…

Agenda

- Parte I
  - De lo que sabemos
  - De lo que enfrentamos
  - De lo que ha pasado
  - De lo que sentimos
- Parte II
  - Referencias del ahora
  - Puntos de encuentro y mitos
- Parte III Conclusiones

Lo que Sabemos: Algunos términos de uso común

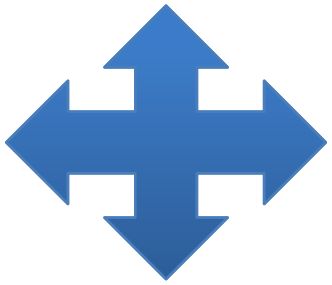
Risk Xploit Rootkit Bootnet Honeypot
Trojan Zombie Boot APT Backdoor Scanning
Control Vulnerabilities Low and Slow
PortKnocking Metasploit Nmap IDS/IPS WAF
FW HIPS Payload Rainbowtables CIS NIST
Privilege escalation Targetng Recon Probing Finger
and Footprinting Buffer Overflow Cracking Sniffing
Poisoning Switching DMZ SQL Patching CIA
Malware and Fraud as A Service UserMgmt
Injection DDOS XsiteScripting ...APT...

Lo que enfrentamos: Historia reciente: 2008-2010

Mas Instalado

Financiero

StuxNet

Zeus  **Aurora**

Mpack

Google, Yahoo ...

Usuario Comun
Comercio
Multi Exploit
Muchos compromisos Europa

Lo que enfrentamos: Aquí y Ahora: 2011

xxxxxxxxxxxxxxxxxxxx **PSN**

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxx**Anonymous**xxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxx**SonyPictures**xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxx 3 Incidentes Malware nuevo por Semana xxxxxxxxxxxxxxxxxxxxx**LookheadMartin**

xxxxxxxxxxxxxxxxxxxx **Google** xxxxxxxxxxxxxxxxxxxxxxxxxxx

Ataques contra gobierno Britanico

xxxxxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxxxxxxxxxx **abuso EC**

Amazon xxxxxxx xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx **2 Puesto Latinoamerica Troyanos Bancarios**

xxxxxxxxxxxxxxxxxxxx **RSA** xxxxxxxxxx xxxxxxxxxxx

Lo que enfrentamos: Aquí y Ahora: 2011

- Gran oleada de ataques “Avanzados Persistentes y Sofisticados” sin precedentes en la historia reciente durante las últimas semanas.

- Compañías de alto perfil:
  - Sony PSN & Sony Pictures
  - Citigroup
  - Google
  - PBS
  - Nintendo
  - Epsilon
  - RSA

- Alcance: Gobiernos, Corporaciones, Mundial, Regional, y Local.

- Local
  - DDOS
  - Defacements
  - Incremento malware dirigido a bancos locales (4 puesto -> 2 en LA)

- Hasta 3 tipos de malware “nuevo” o al menos no reconocido por AV tradicionales por semana.

Fuentes varias: Encuesta ESET, noticias varias y experiencia personal.

Lo que nos piden:

- Virtualization & Cloud
- IT Consumerization (Hw &Sw)
- Threat Landscape
- Consolidation
- Data Security
- Web 2.0 and Social media
  - Facebook 3th Country,
  - Twitter 7th,
  - 7% tráfico facebook,
  - 44% videos online)
  - 23% laboral en Web
  - 45% top 100 sites permite contenido de usuariosy 60% malware
- GRC

HBGary
Wikileaks
RSA SecurID data breach
Hacktivism
Stuxnet/Zeus/Aurora
Mpack
Cyber Crimeware

Criminal Networks

Komodo certificates

- No perímetro
- Amenaza interna
- Privacidad
- Seguridad basada en datos (Shell-176K-E, Apple 100K-C, Facebook 170M-S, MacDonnalds Undisclosed-C)

Lo que ha pasado:

FASE I	***FASE II***	***FASE III***
Fama	Poder computo	APT
Grandes marcas	Target Vs Random	Anonimato
Mucho ruido	Poco conocimiento necesario /herramientas	Hacktivism
No crimen organizado	Europa del este & China	Cyberwarefare
	Cybercrime	APT
	Bootnets	Slow and Down
		Redes crimen organizado
		Alquiler y venta
		Malware an Fraud as a Service

Perimeter Security (Era I),

Mobile Security (Era II),

Application Security (Era III),

Collaboration Security (Era IV).

Securing the Borderless Network: Security for the Web 2.0 World (Tom Gillis)

Clasificación del Autor.

Lo que sentimos!!! (algunas veces…)

Inevitabilidad?

Imagen tomada de: Pirates of the Caribbean: Dead Man's Chest

Referencias situación actual.

- IT: "is that problems and questions seemingly always come before solutions and answers, …answers oftentimes prove quite elusive. It's like playing a game of chess where strategy, tactics, …This intellectual challenge of move/counter-move is energizing and exhausting,…"

- "Today, we are seeing signs that existing practices are fragile. Antivirus vendors are overwhelmed with malware, …patching is nearly …. Our online world is viral, with more than 1.5 billion people around the world connecting, …increasingly brittle, fragile, and vulnerable to disruption, corruption, and exploitation"

- "On the other hand, malware is getting more sophisticated, more malicious, and more difficult to detect than ever before."

- "Wouldn't it be nice if the IT team could say, "Yes—use your iPhone," instead of always saying no? After all, everyone wants to be loved, even the poor IT team"

Securing the Borderless Network: Security for the Web 2.0 World (Tom Gillis)

Referencias situación actual.

- “Over the past week, the White House has announced two big plans for improving Internet security. One is an international policy that seeks to promote Internet freedom while cracking down on the theft of intellectual property. The other is a domestic legislative proposal whose key features include tightening data-breach notification laws…One would have required the White House to generate detailed reports on the extent of cybercrime emanating from each nation. …to work with counterparts abroad to forge partnerships in crime fighting…recommends establishing Internet security standards and imposing some penalties on countries that don't comply with them… "We want nation states to be unified behind a vision like this so we can send a clear message to bad actors that there's going to be no place for them to operate in the international sphere.”citing industry estimates, said the toll of such theft was $1 trillion in 2008..”

Technology Review
Mayo 18 de 2011
The U.S. Cyber Policy Blitz
Computing

Referencias situación actual.

- "We are Legion. We do not forget. We do not forgive. Expect us."
- "splinter faction took control of a critical communications hub, and released information that could be used to track down other members of the secretive organization."
- "how hard it is to peer behind the …more importantly who, Anonymous really is."
- "Internet Relay Chat network called AnonOps, and it was this hub that was highjacked last weekend in what the network's abruptly shut-out"
- "counterblow: The infiltration of an 800,000-computer botnet with which the rogue group (…AnonOps admin called Ryan, age 19, …) had threatened to overrun any new Anonymous sites with DDoS attacks."

Technology Review
Mayo 16 de 2011
Is Anonymous Less Anonymous Now?
Computing

Referencias situación actual.

- "Chancellor says UK Treasury is under malicious software attacks led by foreign intelligence agencies"
- "target of up to 20,000 malicious emails every month"
- "2010 "hostile intelligence agencies made hundreds of to break…".
- "Some analysts have suggested that the French attacks were done by Chinese hackers seeking an advantage …during the G20 summit"
- Spending Review last year that it would invest £650m in a national cyber security programme to enhance online security.

The Guardian
Mayo 16 de 2011
Main Section
Osborne: Treasuty Under Sustained Attack

Referencias situación actual.

- "Biggest advantage hackers over their targets is that they work together… odds appear in their favour …able to use the benefits of Internet…"
  - "...Massive multiplication through botnets…"
  - "… Shift operations very quickly to avoid detection and attribution…"
  - "…forces for good often appear one or two steps behind…"

- **"The key is collaboration. And, like our adversaries, this collaboration needs to break new ground, involve a wider community — of public and private sector bodies — and operate at internet"**

- "Commercial pressures …significant obstacle to achieving better security… descoping of security over functional requirements."

CIO, UK
Hopkinson, Do hackers have the advantage in cyber space?
Mayo 11 de 2011
Main Section
Osborne: Treasuty Under Sustained Attack

Referencias situación actual:

- **Last month's attack was a "very carefully planned, very professional, highly sophisticated criminal cyber attack," Sony said**.

- "…rent computing power for pennies from Amazon EC2…"

- Abuso de tecnología: EC2 para DDOS y para ataques fuerza bruta (passwords, hashes, llaves.

- "very sophisticated and aggressive techniques to obtain unauthorized access, hide their presence from system administrators and escalate privileges inside the servers."

Security Watch
Mayo 19, 011
Sony PSN Hackers Used Amazon EC2 In Attack

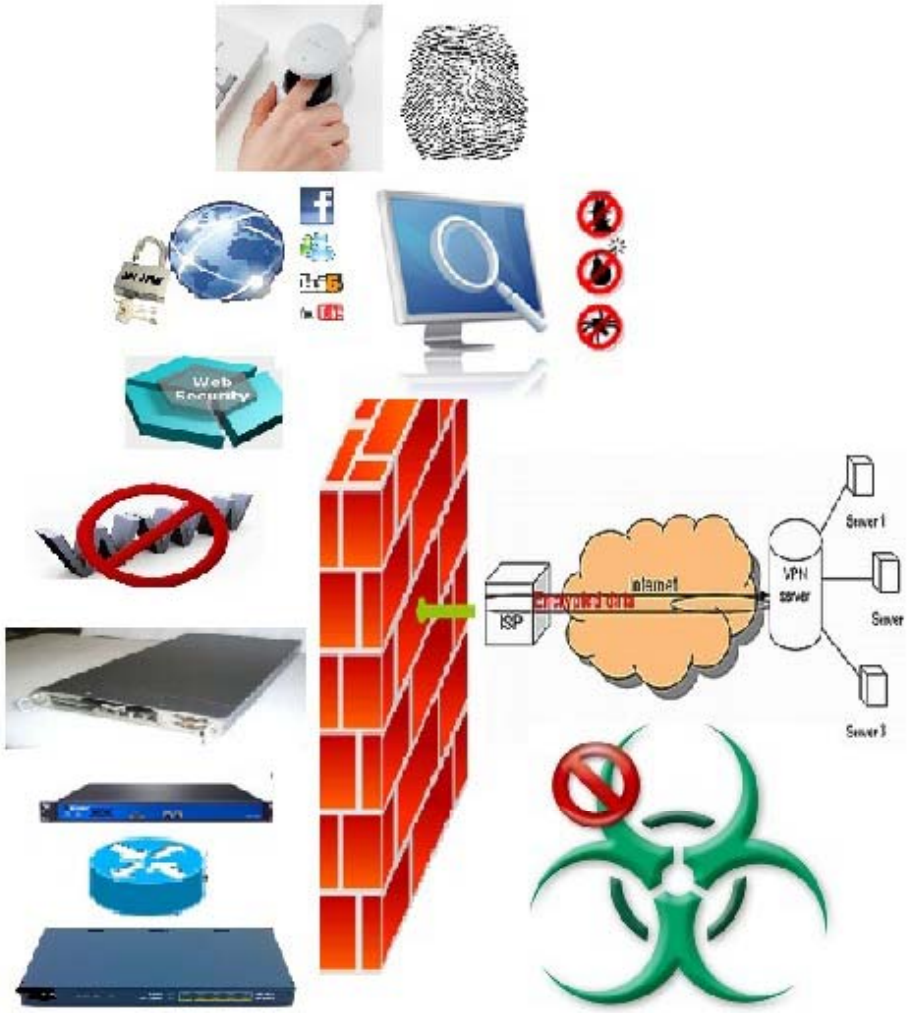
Referencias situación actual.

- **"…**large technology companies (biggest banks, SAP large technology) rushed Tuesday to accept RSA offer to replace tokens…"

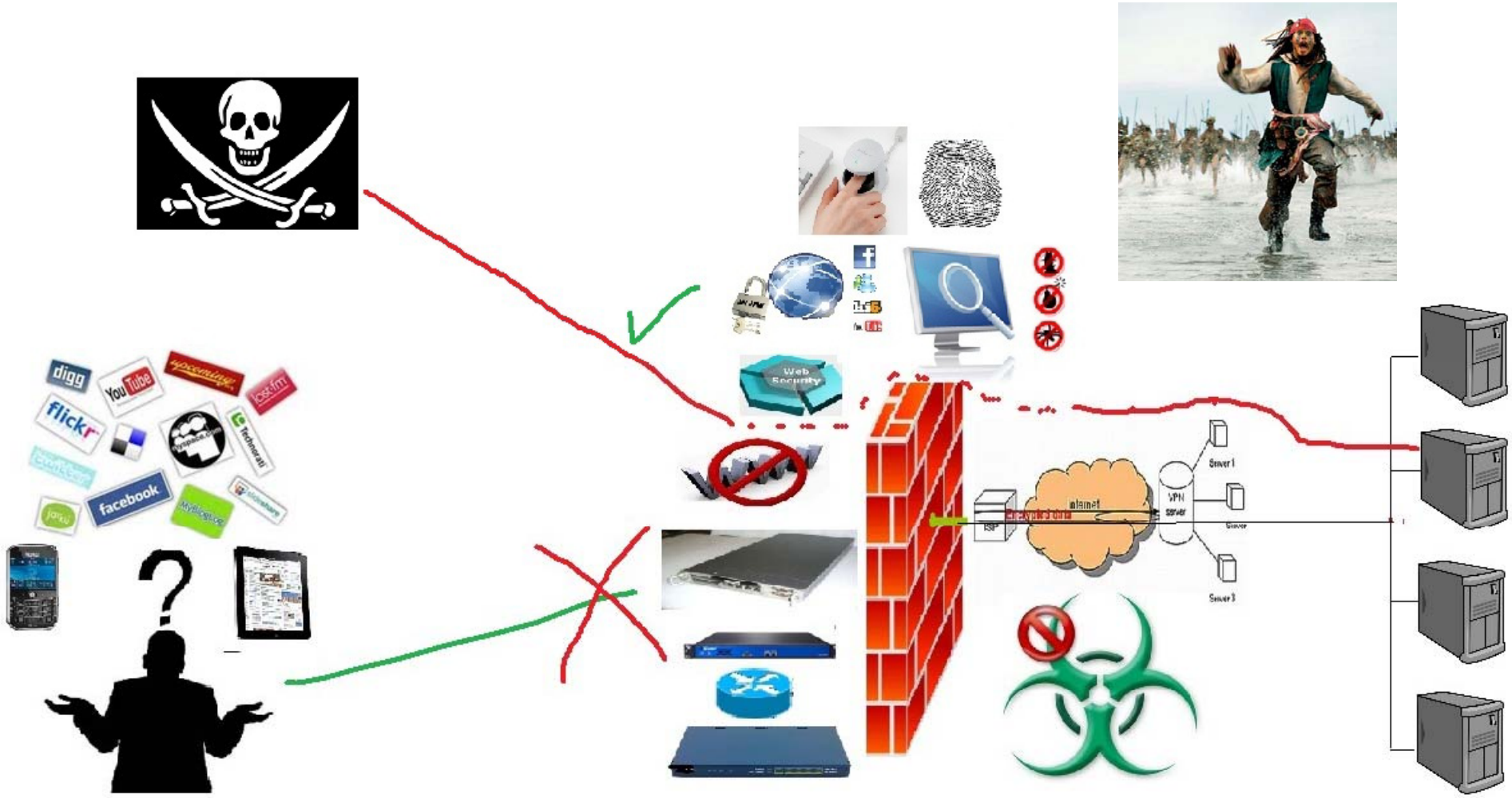
- "The companyís admissions were too little, too late, industry experts said."
  - Shock to customers
  - So long after hacking attack on RSA
  - Lockheed Martin Episode

New York Times Business Day
RSA Faces Angry Users After Breach
By NELSON D. SCHWARTZ and CHRISTOPHER DREW
Published: June 7, 2011

Puntos de encuentro



Puntos de encuentro

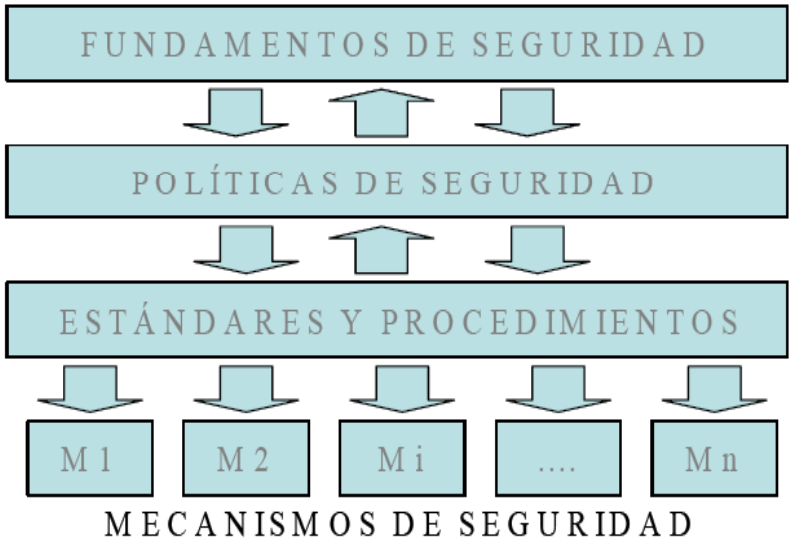


Puntos de encuentro fáciles…

- Mas cajas?, Mas es mejor?
- Se acabo el perímetro?
- APTs como respuesta suficiente?
- Solo podemos decir si?

Conclusiones: Volver a lo básico

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Autenticación
5. Control de acceso
6. No Repudio
7. Observancia



Conclusiones: Volver a lo básico

1. Entorno viral complejo
2. Amenazas sofisticadas corresponden con complejidad de nuestra tecnología actual
3. El tema de cambio de paradigma es puramente de forma
4. Sigue habiendo perimetro, solo que este se debe ir con los datos

Conclusiones: Volver a lo básico

5. Es necesario Compartir
6. Es necesario Sensibilizar
    1. Ciudadano de a pie
    2. Corporación
    3. Organismos judiciales y de control
7. Necesitamos Etica no maleable
8. Es posible decir que no!
9. Paranoia controlada

Gracias,