

ccn-cert

IX JORNADAS STIC CCN-CERT

DETECCIÓN E INTERCAMBIO, FACTORES CLAVE

Madrid, 10 y 11 de diciembre 2015

Defensa Activa



CENTRO CRIPTOLÓGICO NACIONAL



www.ccn-cert.cni.es



David Barroso **@lostinsecurity**

CounterCraft

dbarroso@lostinsecurity.com

Defensa activa es:

1. conseguir que al atacante le sean más **costosos** sus **esfuerzos**
2. **aprovechar** su **momentum** en nuestro beneficio

Defensa activa es:

- 3. obtener la máxima información del atacante**
- 4. alertar de forma temprana compromisos o fases iniciales de un ataque**

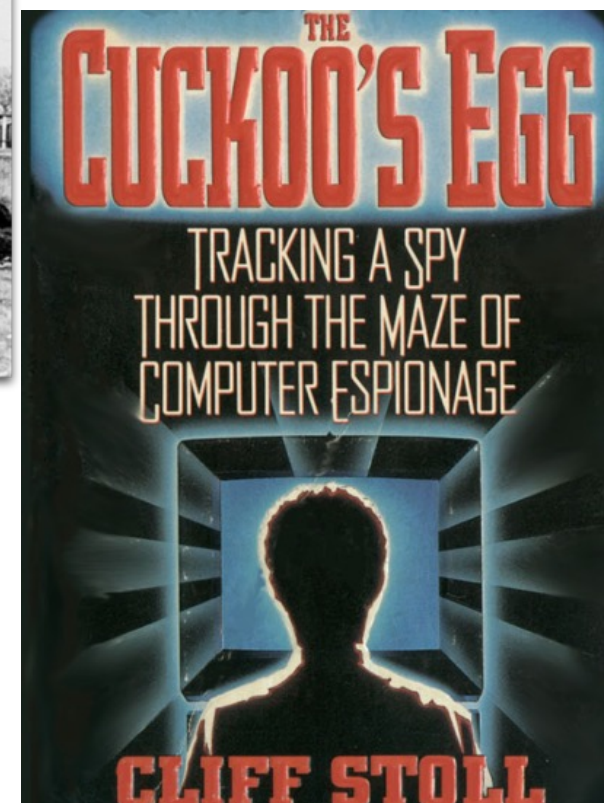
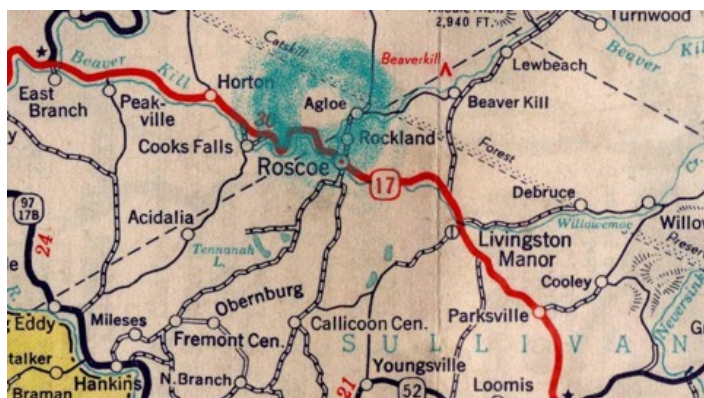
Defensa activa







Un poco de historia

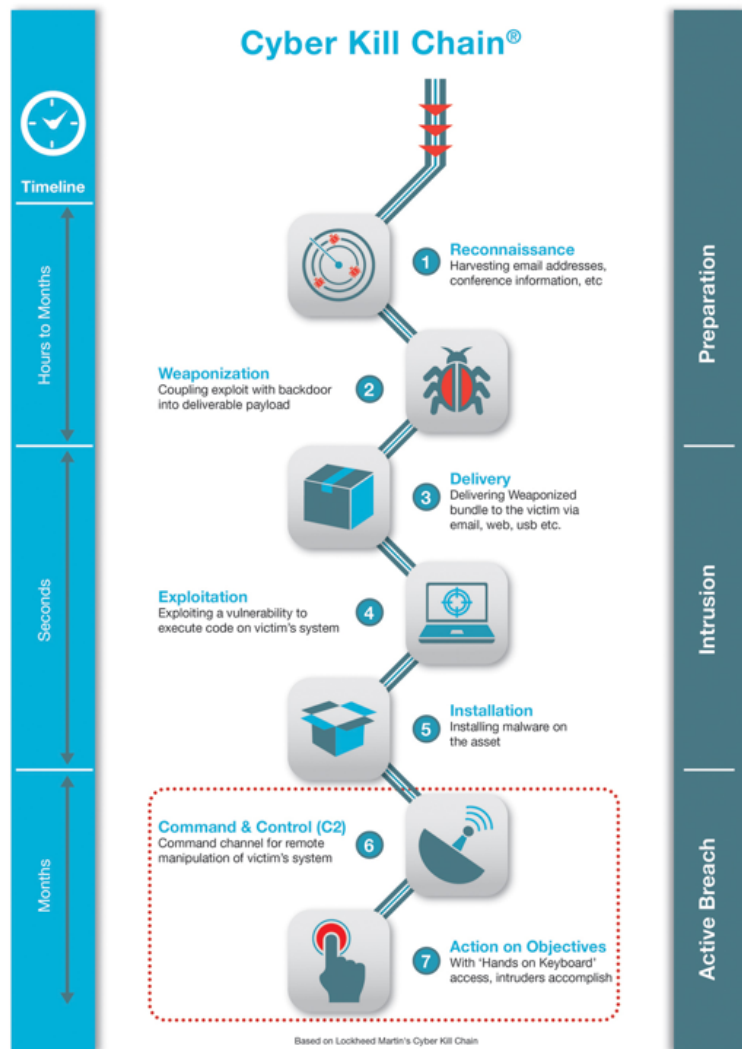


Consideraciones

- Nivel de habilidad
- Recursos
 - Financieros
 - Humanos
 - Técnicos
 - Inteligencia
 - **Experiencia**
- Predictabilidad
- Atribución
- Legalidad

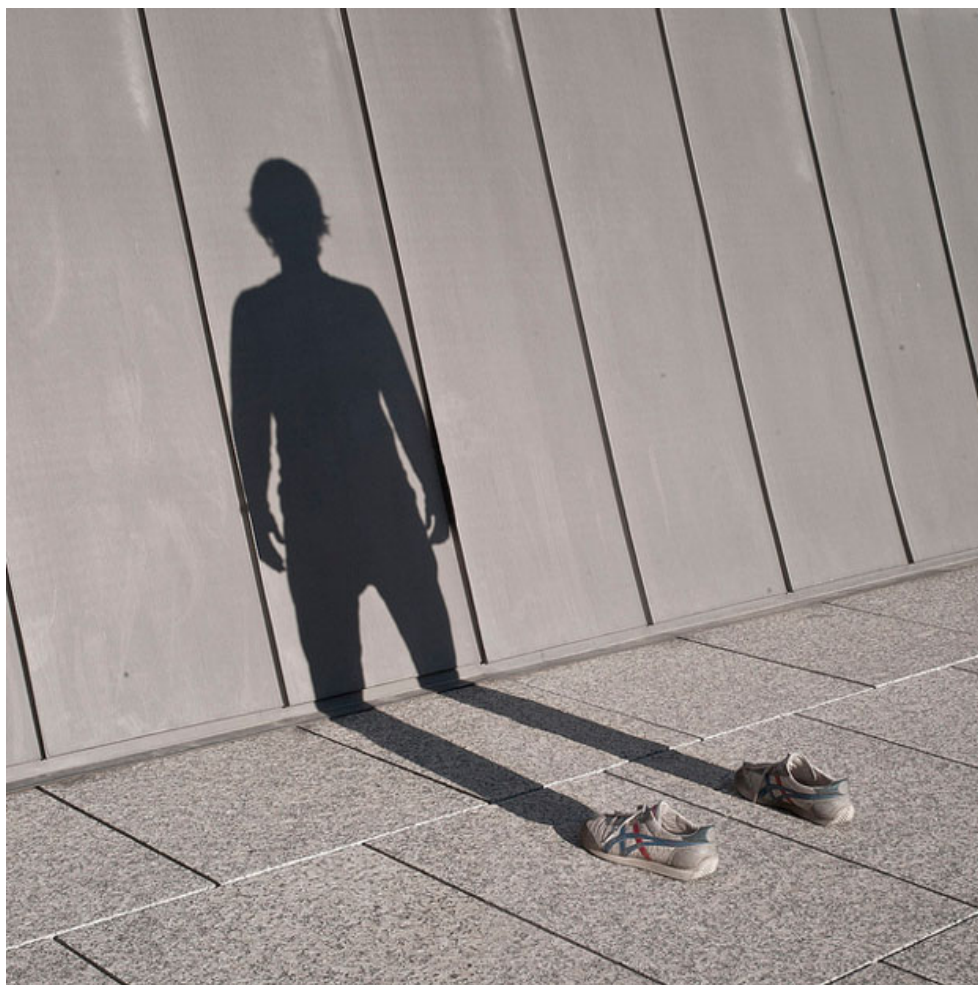
“Aunque el engaño sea detestable en otras actividades, su empleo en la guerra es laudable y glorioso, y el que vence a un enemigo por medio del engaño merece tantas alabanzas como el que lo logra por la fuerza.”

Niccolo Machiavelli, 1469-1527



Objetivo: entorpedecer Cyber Kill Chain





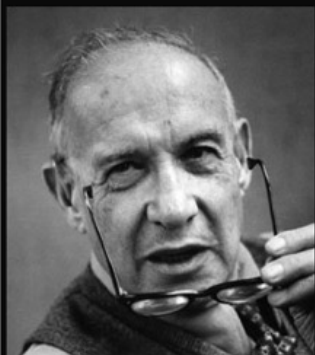
Sensación

No vemos la totalidad del escenario

Haroon Meer hace una analogía interesante con el juego del ajedrez

Asimetría: los defensores tienen que defender siempre, y los atacantes ganar una sola vez

No es verdad. Los atacantes también pierden.



Todo el mundo comete errores. La clave es
cometerlos cuando nadie nos ve

(Peter Drucker)

akifrases.com



Todo el mundo comete errores. La diferencia es
que los míos los publican todos los días

(Miley Cyrus)

akifrases.com

Objetivo

Los atacantes cometen errores

Queremos elevar **su** coste del
ataque (el famoso ROI)

Queremos que tengan que
esforzarse más

Cuidado: nuestra defensa activa
no nos puede costar más que su
coste de evadir nuestras
estrategias.

Defensa activa

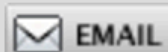
NO es hacking back

Legalizing "Hacking Back": A Comedy of Errors

Fighting software piracy

M Edwards | Windows IT Pro

Jun 24, 2003



EMAIL



LinkedIn



Tweet



Tweet



Like

COMMENTS 0

Security UPDATE, Web exclusive, June 25, 2003

Georgia outs Russian hacker, takes photo with his own webcam

News

By Sam Cook Oct. 31, 2012 4:28 pm

Follow @geekdotcom



www.ccn-cert.cni.es

Defensa activa

NO es hacking back (¿o algo así? – la polémica)



Defensa activa

Pero sí hay otras opciones

“The Active Response Continuum comprises a variety of different tactics for responding to unauthorized digital intrusions...[including] a variety of reactive, non-cooperative responses to digital intrusion that are typically calculated to affect remote systems and are intended to investigate, defend, repel, or punish the intrusion. Such measures range from benign measures that implicate the legitimate interests of innocent persons without impacting remote systems to aggressive measures that are intended to inflict harm or damage on the intended targets.”

David Dittrich, Kenneth Einar Himma, 2005

Defensa activa

Pero sí hay otras opciones

Figure 1 – Levels of Intrusion Response

Level	Victim Posture	Characteristic Actions
0	Unaware	None: Passive reliance on inherent software capabilities
1	Involved	Uses and maintains anti-virus software and personal firewalls
2	Interactive	Modifies software and hardware in response to detected threats
3	Cooperative	Implements joint tracebacks with other affected parties
4	Non-cooperative (Active Response)	Invasive tracebacks, cease-and-desist measures, and retaliatory counterstrikes

Figure 2 – Levels of Force

Level	Causal Impacts	Characteristic Actions
Benign	Limited to victim's own systems	Sniffing, scanning, readdressing hosts, honeypots
Intermediate	Impacts on remote systems but not calculated to produce damage	Invasive tracebacks, remote evidence collection
Aggressive	Impacts calculated to produce damage in remote systems	Remote exploitation, corruption of data, denial of service

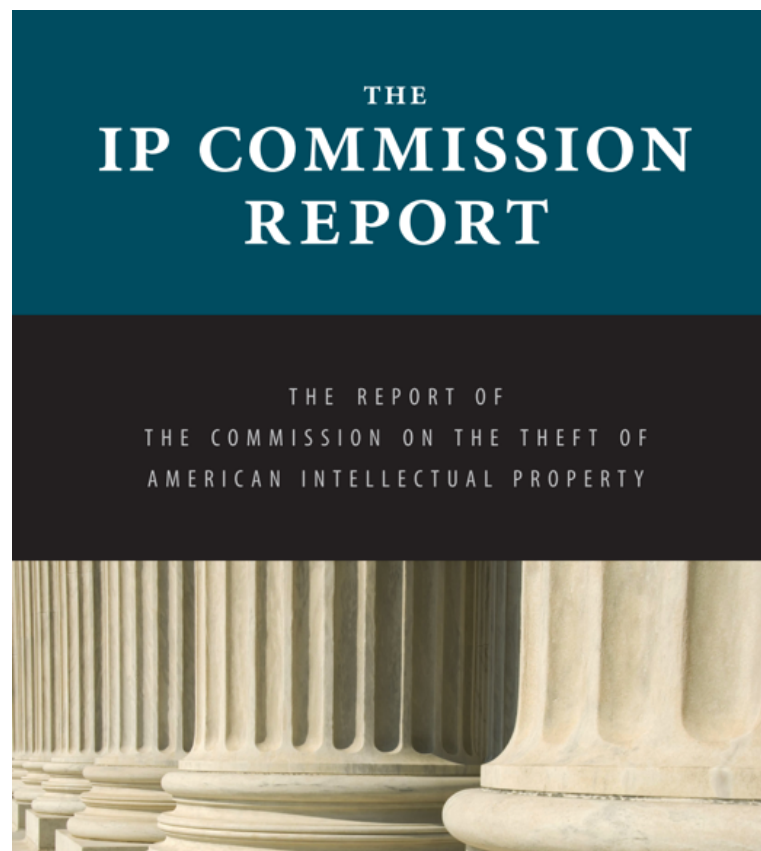
Defensa activa

Pero sí hay otras opciones

3. **Flexibility of response actions** that include traditional passive defense options such as prevention and alerting, but also deception, containment, tying up adversary resources, and creating doubt and confusion while denying them the benefits of their operations. This furthers the goal of increasing attacker's costs and empowers defenders to collect additional intelligence on the adversaries and their tradecraft, while simultaneously preventing damage to their networks

<http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/>

Cyber Counter Strikes



Cyber Counter Strikes

The Commission recommends the following measures to address cybersecurity:

- *Implement prudent vulnerability-mitigation measures.* This recommendation provides a summary of the security activities that ought to be undertaken by companies. Activities such as network surveillance, sequestering of critical information, and the use of redundant firewalls are proven and effective vulnerability-mitigation measures.
- *Support American companies and technology that can both identify and recover IP stolen through cyber means.* Without damaging the intruder's own network, companies that experience cyber theft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information.
- *Reconcile necessary changes in the law with a changing technical environment.* Both technology and law must be developed to implement a range of more aggressive measures that identify and penalize illegal intruders into proprietary networks, but do not cause damage to third parties. Only when the danger of hacking into a company's network and exfiltrating trade secrets exceeds the rewards will such theft be reduced from a threat to a nuisance.

Cyber Counter Strikes



From the Selected Works of Jan Kallberg

February 2015

A Right to Cyber Counter Strikes - The Risks of Legalizing Hack Back

Suposiciones en Cyber Counter Strikes (Hacking Back)

- Es posible una **atribución certera**
- Es posible **enfrentarse a una nación**
- No existe **escalado incontrolado**
- El atacante inicial no tiene **segunda oportunidad de ataque**
- Es algo entre los **dos actores**
- La empresa no tiene **intereses en ese país**
- La **información robada se** elimina del atacante



Los 10 Principios de la Defensa Activa

- **Engaño:** hacer pensar que algo es verdadero
- **Degradación:** reducción de la efectividad
- **Retraso:** ralentizar la actividad
- **Negación:** ocultar nuestras capacidades
- **Disrupción:** interrumpir o impedir sus capacidades
- **Desvío:** forzar al cambio de rumbo
- **Neutralización:** hacer al adversario incapaz de interferir
- **Supresión:** degradar temporalmente
- **Exploit:** ganar acceso a sus sistemas
- **Destrucción:** eliminación de las capacidades del adversario



Ejemplo

	Atacante	Defensor
Negación	Evitar que descubran el ataque	Evitar que descubran su objetivo
Engaño	Engañar para que nos dejen entrar	Engañar para que nos revelen su presencia
Desvío	Llamar la atención del defensor en algo no relacionado	Llamar la atención del atacante en el objetivo equivocado
Engaño	Hacer pensar al defensor que el ataque es no sofisticado o no dirigido	Hacer pensar al atacante que lo que están buscando no está aquí
Engaño	Hacer pensar al defensor que el ataque está controlado o finalizado	Hacer pensar al atacante que ya han conseguido su objetivo
Desvío	Hacer pensar que el atacante es otro	Hacer que el atacante ataque a otro o que piensen que se han equivocado de objetivo

Ejemplos concretos de Defensa Activa

- Generación de **logs** falsos
- Generación de **documentación** falsa
- Concepto clásico de **honeypots** (máquinas, redes, etc.)
- Generación de **tráfico** falso (ARP, CDP, DHCP, SIP, mDNS, etc.)
- Cambios de 'foco' en el **análisis** de incidentes
- **Cebos** en foros, phishing, pastebin, etc.
- Hacer creer que su ataque ha tenido **éxito** (spear phishing, infecciones ,etc.)
- Generación de **canaries**: tablas, usuarios en AD, dominios, cuentas de correo, perfiles en redes sociales, teléfonos, puntos de acceso Wifi, documentos, etc.

Herramientas para la Defensa Activa

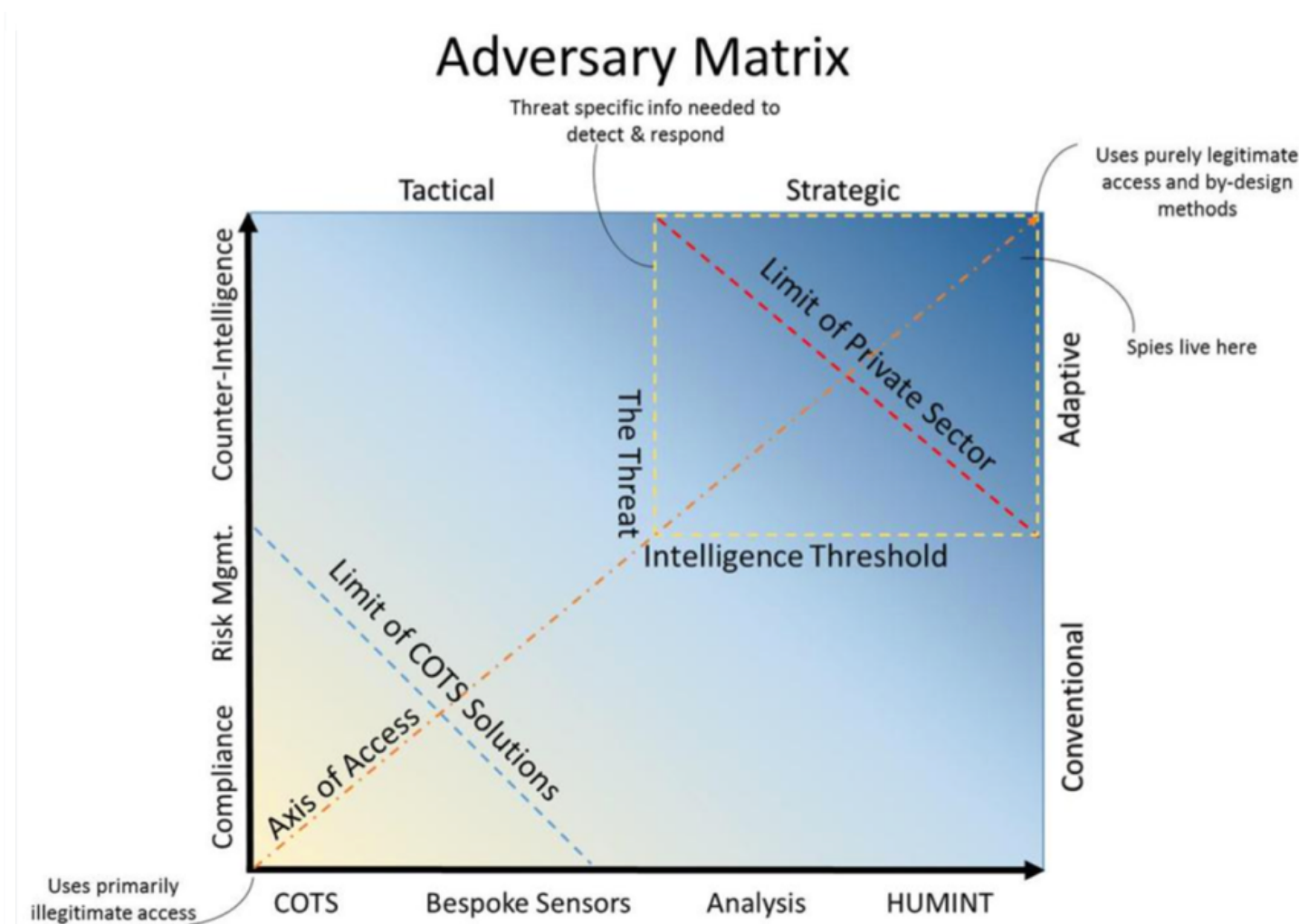
- **Múltiples formas de engaño:** tamaño, actividad, tiempo, habilidades
- **Ambigüedad** (muchos aleatorios) **vs Falsa atribución**
- **Confirmación de información:** mejor establecer nuestra estrategia en algo ya establecido que forzar a cambiar el pensamiento de nuestros atacantes (Magruder's principle)
- Límites en el procesamiento de información:
 - Ley de números pequeños
 - Fácil de condicionar (Pedro y el lobo)
 - No existen cisnes negros
 - Ejemplo: muchos servidores sin datos; Alerta + Retraso + Condicionamiento

Aproximaciones actuales (y sus problemas)

- **Beaconing, tracking**
 - Depende del alcance, zona gris
- **Threat counter-intelligence (foros, etc.)**
 - Participación (pay-to-play), reputación, child abuse
- **Sinkholing**
 - Autorización judicial, información personal
- **Honeypots**
 - Entrapment, pasarela para otros ataques, atracción, daño a la imagen
- **Hacking back (¿me van a denunciar los criminales?)**
 - Escalado de la violencia, efectos colaterales, fallo en la atribución, legalidad

El modelado de amenazas es importante

1. Qué queremos proteger (activos)
2. Contra quién queremos protegerlo (adversarios)
3. Qué probabilidades hay de que tengamos que protegerlo
4. Cómo de malas son las consecuencias si fallamos
5. Cuánto esfuerzo quiero dedicar para protegerlo



John Lambert, Microsoft

Conclusiones

- Defensa activa es aumentar el coste del ataque (para los atacantes!)
- Realmente no es tan asimétrico (Ej: los informes de APT groups)
- Existe un espectro de respuestas (de benigna a agresiva)
- No estamos aprovechando la defensa activa hoy en día
- **Necesitamos establecer nuestra estrategia de defensa activa**
- La parte legal debe estar involucrada desde el principio
- Establece una estrategia que suma pero que no reste
- Imprescindible para mejorar enormemente en:
 - Detección tanto de compromisos como fases iniciales de un ataque
 - Ralentizar y neutralizar los ataques
 - Obtener información sobre los atacantes (IOCs)

Recursos

- <http://www.crowdstrike.com/blog/active-defense-time-new-security-strategy/>
- <http://www.geek.com/news/georgia-outs-russian-hacker-takes-photo-with-his-own-webcam-1525485/>
- Active Response to Computer Intrusions http://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585
- Active Defense and the A.R.T. Of War <https://www.rationalsurvivability.com/presentations/ARTofWAR-v2.pdf>
- IP Comission report <http://www.ipcommission.org/>
- A Right to Cyber Counter Strikes http://works.bepress.com/jan_kallberg/27/
- Bring back the Honeypots (BH 2015) <https://www.youtube.com/watch?v=W7U2u-qLAB8>
- Deception for the Cyber Defender <https://www.youtube.com/watch?v=iA7P-v-MpLY>
- Cyber Security Active Defense: Playing with Fire or Sound Risk Management? <http://jolt.richmond.edu/index.php/cyber-security-active-defense-playing-with-fire-or-sound-risk-management/>
- The Drawbacks and Dangers of Active Defense https://ccdcoe.org/cycon/2014/proceedings/d2r1s5_hathaway.pdf
- Framework and principles for active cyber defense <http://www.sciencedirect.com/science/article/pii/S0167404813001661>
- Active reponse for computer intrusions http://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in

