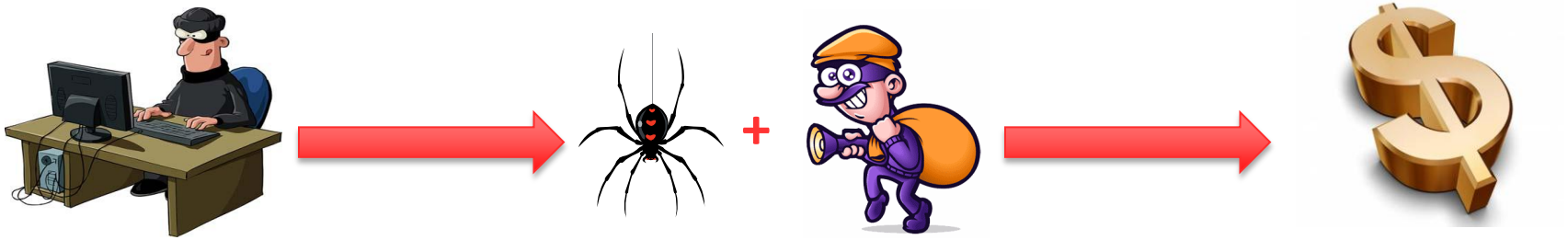
Protezione 0-Day…Anche da Cryptolocker

Gianluca Pucci
WatchGuard SE

Malware: Hai la corretta visione?

Malware ieri: Statico…..mirato al solo danno specifico…..

Malware oggi: Mutevole, avanzato…..mirato ad essere una fonte di guadagno



Ransomware: Overview

- Categoria di malware il cui scopo e' indurre l'utente a pagare una forma di riscatto al fine poter riutilizzare i dati resi inutilizzabili

- Possono agire per via intimidatoria, attraverso l'uso di Loghi importanti: (es FBI Moneypak)

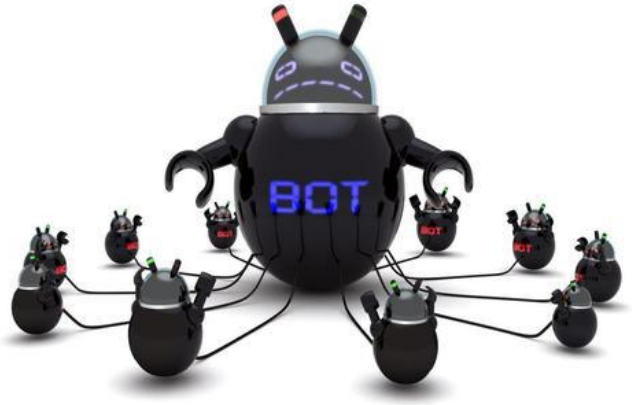
- Danni: Criptare dati personali, o rendere inaccessibile il sistema: In entrambi I casi un messaggio richiede un pagamento al fine di rendere il dato o l'intera macchina riutilizzabile

CryptoLocker: Come funziona

RSA-2048

C&C

DGA



CryptoLocker: L'effetto...

CryptoLocker: Perche' l'Antivirus non basta?

- CryptoLocker e' strutturalmente complesso "uscendo" quindi dagli schemi standard di analisi e riconoscimento.

- CryptoLocker e' mutevole: Contatti molto frequenti con I server C&C facilitano gli update modificando di volta in volta le componenti chiave del malware

- CryptoLocker e' mirato a generare denaro: Questo implica che si tratta e si trattera' sempre in tutte le sue evoluzioni, di un attacco PERSISTENTE con il solo scopo di raggiungere l'obbiettivo.

CryptoLocker: Soluzione……

- La soluzione DEVE essere preventiva: NON posso accontentarmi di rimozioni parziali quando ormai il danno e' procurato.

- La soluzione DEVE essere continuativa: Serve una tecnica che sia in grado di andare al di la del continuo inseguimento che il motore AV fa nei confronti della vulnerabilita'

CryptoLocker: Scegli di non pagare…

WatchGuard APT Blocker

Best-of-Breed….anche per il motore APT!

- **Partner tecnologico: Lastline**

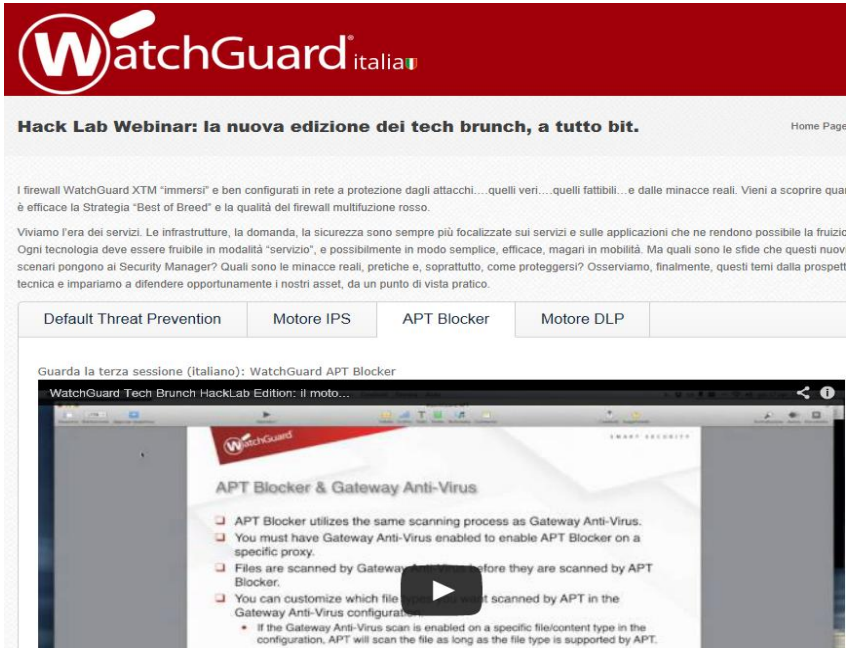
- **Servizio Cloud-Based: L'utilizzo della tecnica di Sandboxing fornisce una ottima soluzione alle minacce Zero-Day**

…..Vuoi saperne di piu'?…….

WatchGuard al tuo servizio!

..Guarda il Webinar interamente dedicato al Motore APT-Blocker..

https://www.watchguarditalia.com/hack-lab/



Grazie

Gianluca Pucci
WatchGuard Sales Engineer
prevendita-italia@watchguard.com