



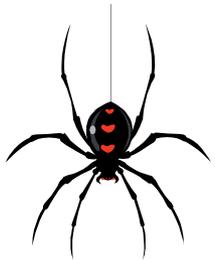
# **Protezione 0-Day...Anche da Cryptolocker**

**Gianluca Pucci  
WatchGuard SE**

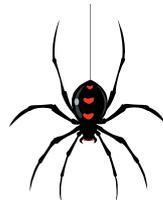
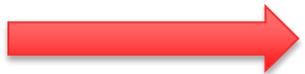


# Malware: Hai la corretta visione?

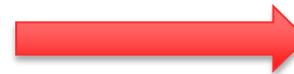
Malware ieri: Statico.....mirato al solo danno specifico.....



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



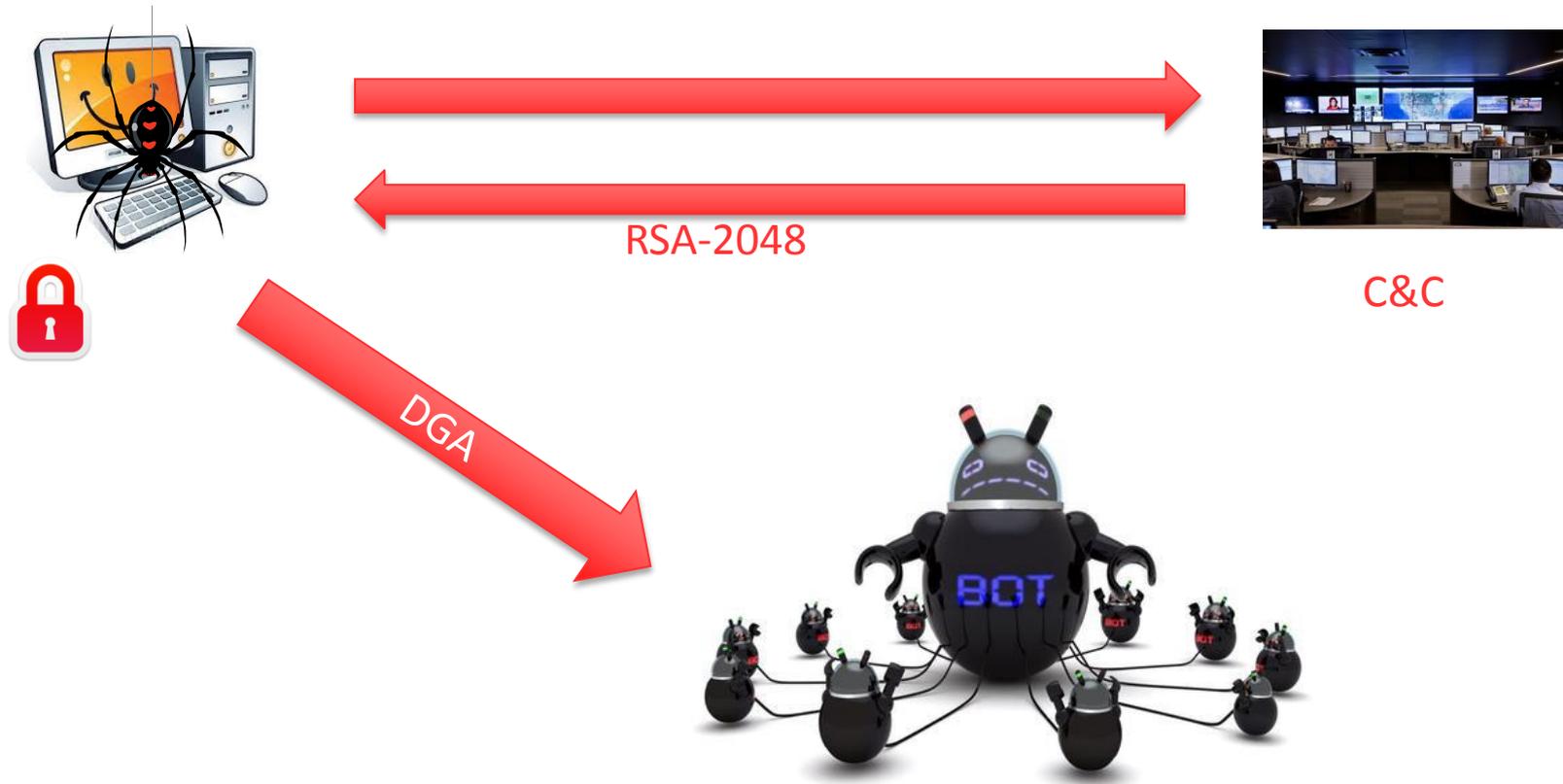
+



## 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



# CryptoLocker: L'effetto...



## YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

**To unlock the computer you are obliged to pay a fine of \$200.**

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted].  
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK

# **CryptoLocker: Perché l'Antivirus non basta?**

- CryptoLocker è strutturalmente complesso “uscendo” quindi dagli schemi standard di analisi e riconoscimento.**
- CryptoLocker è mutevole: Contatti molto frequenti con I server C&C facilitano gli update modificando di volta in volta le componenti chiave del malware**
- CryptoLocker è mirato a generare denaro: Questo implica che si tratta e si tratterà sempre in tutte le sue evoluzioni, di un attacco PERSISTENTE con il solo scopo di raggiungere l'obiettivo.**

## 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**



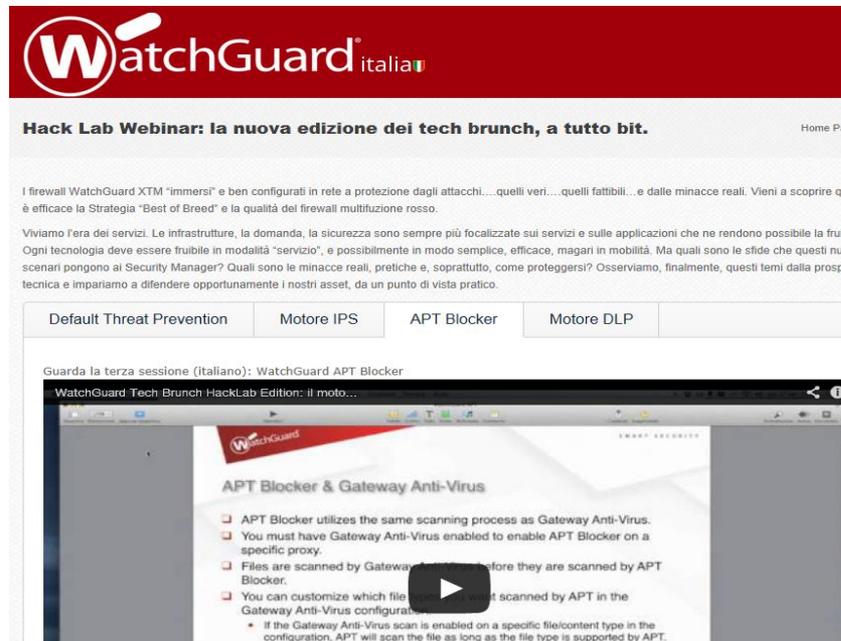
**- Servizio Cloud-Based: L'utilizzo della tecnica di Sandboxing fornisce una ottima soluzione alle minacce Zero-Day**

**.....Vuoi saperne di piu'?.....**

# WatchGuard al tuo servizio!

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

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



The screenshot shows the WatchGuard Italia website's Hack Lab Webinar page. At the top, the WatchGuard Italia logo is displayed. Below it, the heading reads "Hack Lab Webinar: la nuova edizione dei tech brunch, a tutto bit." with a "Home Page" link. The main content area contains two paragraphs of text. The first paragraph discusses the WatchGuard XTM "immersi" firewall and its "Best of Breed" strategy. The second paragraph talks about the shift to service-oriented security. Below the text is a navigation menu with buttons for "Default Threat Prevention", "Motore IPS", "APT Blocker", and "Motore DLP". The "APT Blocker" button is highlighted. Underneath the menu, there is a video player titled "Guarda la terza sessione (Italiano): WatchGuard APT Blocker". The video player shows a slide titled "APT Blocker & Gateway Anti-Virus" with a list of bullet points: "APT Blocker utilizes the same scanning process as Gateway Anti-Virus.", "You must have Gateway Anti-Virus enabled to enable APT Blocker on a specific proxy.", "Files are scanned by Gateway Anti-Virus before they are scanned by APT Blocker.", and "You can customize which file types are scanned by APT in the Gateway Anti-Virus configuration." with a sub-bullet: "If the Gateway Anti-Virus scan is enabled on a specific file/content type in the configuration, APT will scan the file as long as the file type is supported by APT."

