I Pwnie Award 2018

I premi Pwnie (https://pwnies.com), fondati nel 2007 da Alexander Sotirov e Dino Dai Zovi, vengono assegnati ogni anno al meglio e al peggio della sicurezza informatica. La premiazione si svolge durante la conferenza Black Hat, le nomination vengono direttamente dalla comunità, mentre i vincitori vengono scelti da alcuni dei migliori professionisti dell'industria della sicurezza.

Una curiosità: il nome si basa sul termine "pwn", che nello slang hacker sta per "own", inoltre *Pwnie Award* ricalca/ricorda, nella pronuncia, i *Tony Award* che premiano le migliori opere del teatro di Broadway.

Chi ha vinto quest'anno

Pwnie for Best Server-Side Bug: Intel AMT Remote Vulnerability

La vulnerabilità sta nel fatto che c'è stato un errore nell'utilizzo della funzione *strncmp()*, funzione che confronta due stringhe di testo tra di loro. L'errore, di per sé banale, è tanto più grave perché è stato commesso da un gigante come **Intel** e si trova in una parte di codice altamente rischiosa, ovvero il codice che si occupa dell'autenticazione dell'interfaccia Web di Intel ATM. Qui tutti i dettagli dell'attacco:
https://thehackernews.com/2017/05/intel-amt-vulnerability.html

Pwnie for Best Client-Side Bug: The 12 Logic Bug Gifts of Christmas

Il premio come miglior bug lato client è andato al progetto **Chainspotting**. Nelle slide *Chainspotting: Building Exploit Chains with Logic Bugs*, presentate al CanSecWest e disponibili

all’indirizzo https://labs.mwrinfosecurity.com/publications/chainspotting-building-exploit-chains-with-logic-bugs/, sono stati illustrati undici *bug logici* in sei differenti applicazioni di Android, agli undici bug ne va aggiunto un dodicesimo (un DoS remoto) anch’esso parte della catena finale di exploit.

Pwnie for Best Privilege Escalation Bug e Pwnie for Most Innovative Research: Meltdown and Spectre

Il premio come ricerca più innovativa e quello per il bug con escalation di privilegi più devastante non poteva non essere assegnato a **Meltdown and Spectre** (https://meltdownattack.com). In breve e semplificando, queste vulnerabilità garantiscono l’accesso diretto alla memoria dei processori e ai dati attualmente processati. Per maggiori dettagli rimando all’articolo “Meltdown e Spectre, i super bug del 2018” (https://www.ictsecuritymagazine.com/articoli/meltdown-e-spectre-i-super-bug-del-2018-possono-essere-sfruttati-in-un-vero-attacco/).

Pwnie for Best Cryptographic Attack: Return Of Bleichenbacher’s Oracle Threat

Questo premio va ad un attacco crittografico applicabile nel mondo reale, quindi, non sono prese in considerazione tutte quelle ricerche accademiche che hanno effetto solo in linea teorica. Quest’anno il premio è andato all’attacco **Return Of Bleichenbacher’s Oracle Threat** (ROBOT, https://robotattack.org). L’attacco è una leggera variazione di uno già visto nel 1998 contro il protocollo TLS usato con RSA, da qui il nome. L’anomalia sta nel fatto che una piccola variazione ad un attacco di venti anni fa sia ancora efficace contro sistemi moderni.

Pwnie for Lamest Vendor Response: Bitfi

Bitfi (https://bitfi.com), produttore di un wallet per criptovalute, ce l'ha messa tutta per vincere questo premio. Prima il termine *Unhackable*, le dichiarazioni di John McAfee e la sfida. Poi il fatto che il prodotto in questione non è altro che un normale tablet Android senza meccanismi di sicurezza aggiuntivi quindi facilmente attaccabile. Ed infine la pubblicazione di un imbarazzante tweet (https://twitter.com/bitfi6/status/1024917066862796800). Qui tutti i dettagli della storia: https://www.theregister.co.uk/2018/08/01/unhackable_bitfi_wallet/.

Pwnie for Most Over-hyped Bug: Holey Beep

Questo premio va a chi ha fatto parlare (inutilmente) più di sé online. Inutilmente perché in genere si tratta di un bug difficilmente sfruttabile in pratica o di un bug scarsamente rilevante. Quest'anno il premio è andato al bug **Holey Beep** (https://holeybeep.ninja/) con tanto di webpage (molto divertente) e logo come accade per le vulnerabilità *branded*.

Lifetime Achievement Award: Michał Zalewski

Il premio alla persona che meglio incarna lo spirito hacker è stato assegnato a Michał Zalewski meglio conosciuto come **lcamtuf**. Autore di un libro fondamentale per la sicurezza (*Silence on the Wire*) e di alcuni tool tra i quali lo scanner *p0f* e il fuzzer *AFL*.

A cura di **Gianluigi Spagnuolo**

L'articolo I Pwnie Award 2018 proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/notizie/i-pwnie-award-2018/