PRESS REVIEW ARCHIVE

Digital Media Monitoring & Documentation Service

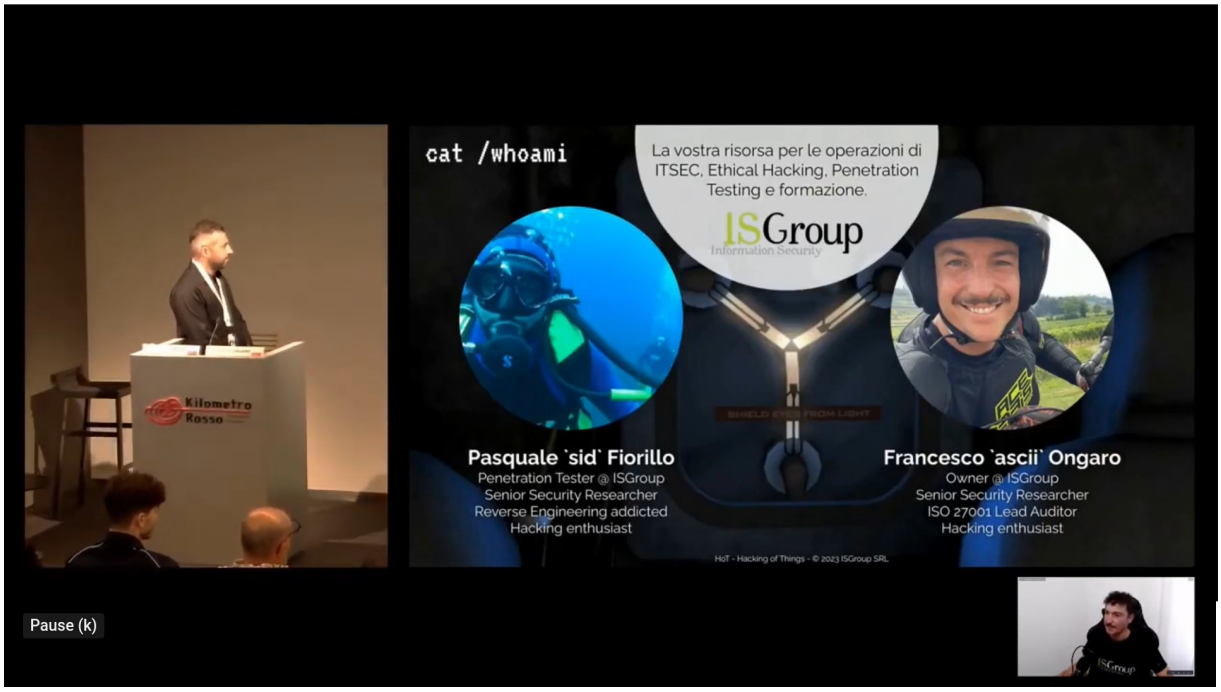
Source URL: https://www.youtube.com/watch?v=47Sq5jmJ38c

Archived Date: August 15, 2025 at 15:16

Document Type: Web Page Archive

Wayback Machine: https://web.archive.org/web/*/https://www.youtube.com/watch?v=47Sq5jmJ38c

Page Screenshot



Abbiamo due ospiti, uno in locale e uno da remoto: **Francesco Ongaro** e **Pasquale Fiorillo**, sono ricercatori.
Pasquale, aggiungimi così ti presento alla platea. Sono ricercatori.

Ciao, siamo ricercatori di **ISGroup**. Con loro abbiamo creato e stiamo lavorando in questa partnership di ricerca congiunta nell'ambito intrusion detection, hacking etico e dell'analisi. Appunto perché non è che una persona o un'azienda può fare tutto, ma innanzitutto certi processi bisogna certificarli e gestirli adeguatamente.

Francesco ci sei?
— Eccolo qua.
— Ciao Francesco.
— Vi sento, voi mi sentite correttamente?
— Perfetto.
— Francesco, fantastico. Vi lascio la platea e ci salutiamo tra un attimo.

Grazie Alessandro. Buongiorno a tutti, è un piacere essere con voi al **Kilometro Rosso**. Ciao Pasquale, ti vedo che sei sul podio, benissimo. Perfetto.

Nella presentazione di oggi: **Hacking of Things**, ovvero ottenere controllo degli oggetti connessi. Vedremo cosa si intende per dispositivo IoT, com'è fatto a livello macro e come lo si può attaccare, quindi come un attaccante reale lo attaccherebbe. Poi andiamo a vedere anche qual è lo stato attuale dell'arte dal punto di vista della sicurezza informatica e delle informazioni.

Allora, in **ISGroup** ci occupiamo di sicurezza delle informazioni. ISGroup è un laboratorio indipendente: siamo una risorsa per le operazioni di IT security, ethical hacking, penetration testing, formazione.

Questa presentazione è stata realizzata dal collega **Pasquale Fiorillo**, penetration tester presso ISGroup, senior security researcher e appassionato di reverse engineering e hacking. Piacere, sono **Francesco Ongaro**, socio ISGroup. Il mio scopo oggi è quello di introdurre i contenuti divulgativi che poi vi presenterà Pasquale.

Siamo molto contenti della nostra partnership con **Phoenix Informatica**, con cui lavoriamo in una logica di open innovation per avere processi e prodotti più sicuri.

Il nostro team viene dall'underground italiano, ovvero quella sottocultura degli anni '90 legata all'hacking, quando ancora non esisteva un mercato in Italia per questo tipo di servizi. Siamo attivi nella ricerca e nella pubblicazione di advisory ed exploit anche per prodotti di primaria importanza come, ad esempio, backup software come *CUP* e *BAM Backup*.

Vediamo cosa si intende per **IoT**.

Mentre prima i sistemi IoT, e prima ancora quelli di controllo industriale (SCADA), erano relegati agli ambienti produttivi, oggi — anche incentivati attraverso iniziative come quelle di *Industria 4.0* — è evidente come i dispositivi Internet of Things, ovvero la connessione tra un dispositivo hardware, il software su di esso installato e una infrastruttura accessibile attraverso Internet (che normalmente è un cloud), siano presenti e pervasivi nella nostra vita quotidiana.

Abbiamo quindi prodotti consumer come quelli appartenenti allo **smart home**, oppure alla gestione dell'energia e del comfort aziendale, o ancora **smart grid**. Ma anche l'evoluzione di appliance che precedentemente non erano intelligenti: frigoriferi che capiscono quando sono vuoti e ordinano la spesa per noi in autonomia, forni che iniziano a cucinare prima che torniamo a casa.

Pensate che in una **ECU** (unità di controllo elettronico) di una macchina moderna sono presenti circa **100 milioni di righe di codice**. Per confronto, in un Boeing 787 Dreamliner ce ne sono solamente 14 milioni.

Qual è il problema?
Con l'IoT, una determinata vulnerabilità — e in generale tutte le vulnerabilità cui è soggetto l'oggetto e la sua infrastruttura — affligge contemporaneamente tutti gli utenti. La compromissione del cloud può portare alla compromissione di tutti gli utenti. Questa è la differenza principale dell'architettura hardware-software-cloud dell'IoT rispetto al software tradizionale.

Grazie, passo la parola al collega **Pasquale Fiorillo**, che entrerà nel dettaglio della composizione di un sistema IoT e di come questo possa essere attaccato.

Grazie Francesco. Mi sentite anche così? Perfetto.

Dal punto di vista della sicurezza, abbiamo questo oggetto che si divide in due grandi parti: la parte fisica e la parte cloud. Oggi ci concentriamo sulla parte fisica.

Un dispositivo IoT è composto da:

- una **CPU**;
- delle interfacce (display, tastiera, microfono, altoparlante);
- uno **storage** per i dati;
- uno **storage protetto** per le credenziali di accesso a servizi esterni;
- connettività Internet diretta o tramite gateway;
- sensori vari (temperatura, qualità dell'aria, ecc.), a seconda del dispositivo.

Per quanto riguarda le CPU, abbiamo due famiglie principali:

1. dispositivi con **microcontrollori**, chip specifici che non eseguono un sistema operativo ma software scritto direttamente sul chip;

2. dispositivi più complessi, con una vera CPU e un sistema operativo a bordo, simili a smartphone o tablet, con più processi e ambienti complessi.

In questi casi incontriamo sistemi operativi basati su Linux, spesso Android, o WebOS (ad esempio nei televisori LG).

Come si analizzano dal punto di vista della sicurezza?

Per noi questi oggetti sono "black box". La prima operazione è **smontarli**, analizzare la board, identificare chip e componenti, consultare i datasheet dei produttori, e identificare tutte le porte e i connettori (anche nascosti). Queste possono diventare potenziali porte di accesso.

Una volta individuato il componente che conserva il software, si procede all'**estrazione del firmware**. Esistono tecniche non invasive e strumenti che non lasciano traccia del nostro passaggio.

Un'altra attività è l'analisi della **comunicazione interna tra i chip**, utile quando il firmware è crittografato. Si usano logic analyzer per catturare il flusso di bit (sequenze di 0 e 1) dai pin dei chip, ad esempio durante la fase di boot. Questo permette di ottenere informazioni preziose.

Estratto il firmware, si procede con l'analisi usando software standard, spesso open source, per ottenere il maggior numero di informazioni possibili. Poi si fa **reverse engineering** (ad esempio con **Ghidra**, open source rilasciato dalla NSA).

Per la parte cloud, invece, si applicano tecniche classiche di penetration testing, in particolare **web application penetration test**.

Negli anni 2000 abbiamo visto un grande incremento della sicurezza informatica nel mondo di computer e smartphone, grazie a mitigazioni architetturali. Il mondo IoT, invece, è molto indietro: la sicurezza dei dispositivi è relativamente bassa, paragonabile al livello pre-2000.

Lascio a Francesco l'ultima slide per i saluti.

Grazie Pasquale.
Proprio così: il livello di sicurezza dei dispositivi IoT è solitamente basso, ed è per questo che vi incoraggiamo a rivolgervi ad esperti per identificare i rischi e le opportune azioni correttive.

Grazie a Pasquale, grazie a Phoenix Informatica per averci invitato, grazie al Kilometro Rosso per l'ospitalità e grazie a tutti voi per l'attenzione. Speriamo di entrare in contatto con voi presto e vi auguriamo una piacevole prosecuzione di conferenza e di giornata.

— Grazie Francesco.
— Grazie di tutto, buongiorno.