INTESA SANPAOLO
GROUP SERVICES

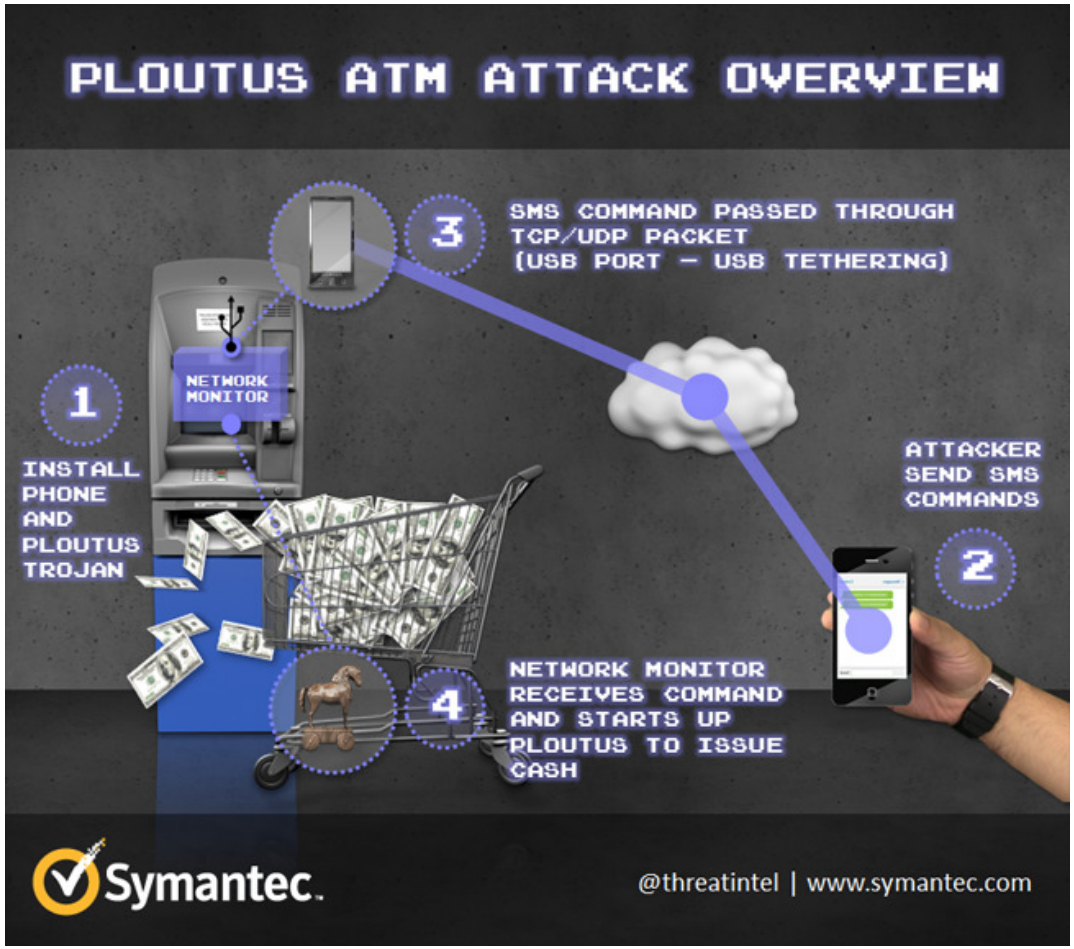
Nuove sfide per la sicurezza fisica
Alcune riflessioni

Claudio Ferioli
Responsabile Progettazione e Standard Sicurezza Fisica

Roma, 4 giugno 2015


Il mare è calmo.
Ma cosa emerge all’orizzonte?

Ploutus: sicurezza fisica o informatica?



Come avviene l'attacco

1. **Accesso fisico** al PC
2. Installazione malware con **un cd o una pendrive**
3. Collegamento **fisico** di un **cellulare** tramite porta USB
4. Quando il cellulare riceve uno specifico **SMS**, l'ATM eroga una somma definita di contante

Keylogger: sicurezza fisica o informatica?

Come avviene l'attacco

1. Si **collega fisicamente** al PC, in genere interposto tra le periferiche (tastiera, monitor) e la base
2. **Trasmette all'esterno** il traffico dati: tutto ciò che viene digitato a tastiera e visto a monitor
3. **Permette di operare** sul PC, ad esempio per trafugare informazioni oppure lanciare operazioni illegali.

Hacking video: sicurezza fisica o informatica?

Forbes

Researcher Reveals Flaws In Video Surveillance That Let Hackers Spy On You

BBC

Breached webcam and baby monitor site flagged by watchdogs

The public is being warned about a website containing thousands of live feeds to baby monitors, stand-alone webcams and CCTV systems.

Come avviene l'attacco

1. **Accesso remoto** alla telecamera
2. Violazione dei sistemi di protezione **software**
3. Accesso alle **immagini** registrate
4. Eventuale **modifica delle impostazioni** della telecamera

Hacktivism: sicurezza fisica o informatica?

WIRED

A CYBERATTACK HAS CAUSED CONFIRMED PHYSICAL DAMAGE FOR THE SECOND TIME EVER

Come avviene l'attacco

1. Accesso al sistema di controllo dell'impianto **da remoto**, attraverso **USB** oppure con tecniche di **social engineering**
2. Installazione **malware**
3. Modifica dei **parametri di configurazione** oppure **danneggiamento** del software operativo
4. Conseguente **modifica del funzionamento fisico**

Dove va la sicurezza fisica?

Emergono nuovi attacchi

- Attacchi **fisici** per violare i **sistemi informatici**

  …attraverso aree non protette dalla sicurezza fisica (es. porta USB dei PC) o con tecniche non considerate (es. insider)

- Attacchi **informatici** per violare **sistemi** (di sicurezza) **fisici**

  …attraverso sistemi non prioritari per la sicurezza informatica (es. sistemi di controllo fisico) o con tecniche non standard (es. violazione software proprietario di controllo industriale)

Emergono nuovi attacchi: una delle sfide del futuro?

…In addition, new challenges will emerge. Evolved threats to critical infrastructure and human implants ***will increasingly blur the distinction between cyber and physical attack****, resulting in offline destruction and physical injury…*

Emergono nuovi attacchi: una delle sfide del futuro?

I **trend** sottostanti sono di lungo periodo:

- i ***millennials*** nei ruoli di comando delle organizzazioni criminali, anche di quelle '*tradizionali*'
- diffusione di modelli ***crime as a service***
- disponibilità informazioni e know how sugli attacchi e sulle difese, ad esempio nel ***dark web***
- crescente pervasività dell'**ICT** nelle soluzioni di sicurezza fisica
- …

Come cambia il *mestiere* della sicurezza fisica

Competenze

- integrazione con competenze ICT security
- acquisizione competenze di *operational technology security*

Come cambia il *mestiere* della sicurezza fisica

Competenze

- integrazione con competenze ICT security
- acquisizione competenze di *operational technology security*

Approcci

- creare reti trasversali per affrontare il nuovo contesto (ICT security, real estate, organization)
- modificare focus e strumenti dell'analisi del rischio

Come cambia il *mestiere* della sicurezza fisica

Competenze

- integrazione con competenze ICT security
- acquisizione competenze di *operational technology security*

Approcci

- creare reti trasversali per affrontare il nuovo contesto (ICT security, real estate, organization)
- modificare focus e strumenti dell'analisi del rischio

Soluzioni

- scouting di soluzioni su mercati affini
- logiche open innovation e attenzione alle start up

INTESA SANPAOLO
GROUP SERVICES

claudio.ferioli@intesasanpaolo.com