ATTIVITÀ MANUTENTIVA REMOTA

PROJECT OVERVIEW

Feedback

FEEDBACK ITALIA OVERVIEW

Fondata nel 2000, **Feedback Italia**

è specializzata nel design e sviluppo

di soluzioni software e hardware per

la comunicazioni sicura audio, video e dati,

I TREND DEL 2016

- ✓ **Ransomware:** +752% (247 famiglie), con ampio uso di open-source Ransomwares e RaaS (Ransomware as a Service)
  - **Giro di affari mondiale stimato in 1Billion USD**
- ✓ **Vulnerabilità:** +7.1% (765 casi), inclusi 60 zero days.
  - Targets: Advantech WebAccess (SCADA) 109, **Apple OS-X 52, Android 52**, Internet Explorer 33, Windows OS 26, Microsoft Edge 22
- ✓ **Utilizzo crescent di SCADA ed IOT per guadagnare l'accesso alle reti**

Vendor	Prodotto	2015 vs 2016
Microsoft		- 47%
	Internet Explorer	- 73%
	Office	- 53%
	Windows	- 26%
Android		+ 206%
Apple		+ 145%
	IOS	+ 275%
	OS X	+ 189%
SCADA		+ 421%

2016 Totale/ Impatto	765
Alto:	37,12%
Medio:	61,44%
Basso:	1,05%

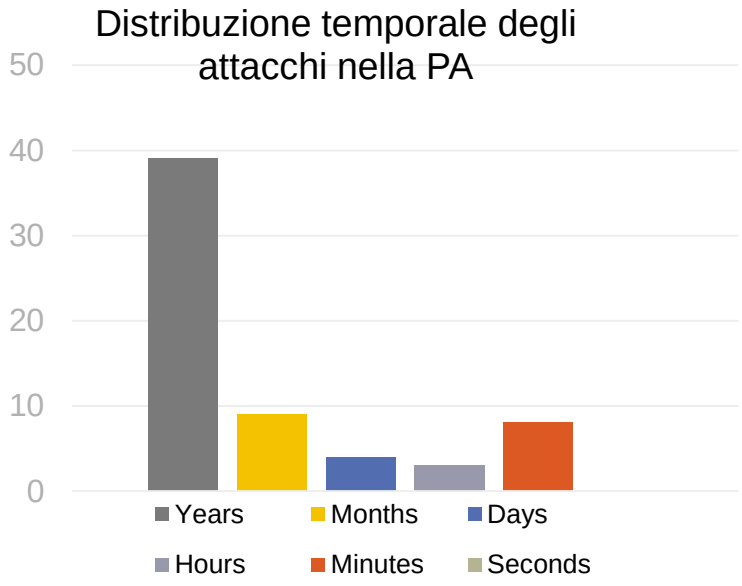
[Sorgente: 2016 TrendLabs Annual Security Roundup by TrendMicro]

I TREND DEL 2016: ANALISI

- ✓ Gli attacchi sono principalmente focalizzati **all'estorsione di denaro o al furto di informazioni**
- ✓ **Gli attaccanti gestiscono il "business" come una vera e propria industria**, attaccando le nuove tecnologie non appena vengono utilizzate dagli utenti finali in maniera diffusa per consentire loro una customer-base accettabile
- ✓ **Android ha l'85% della quota di mercato, ma IOS e Android hanno tendenze simili in forte crescita**: si può spiegare perché Android è adatto per attacchi di massa, mentre IOS è più soggetto ad attacchi chirurgici (dal momento che Apple è utilizzato principalmente da persone benestanti e decision maker)
- ✓ **L'impatto è sempre alto**: gli attaccanti, se si muovono, si muovono solo per colpire e colpire duramente

IL CASO DELLA PUBBLICA AMMINISTRAZIONE

- ✓ <u>Attori principali:</u> 58% Esterni, **36% Interni**, 4% Entrambi, 2% Partners.
  - Circa metà degli attacchi sono dovuti a cause interne, **principalmente errori umani**
- ✓ Circa la metà degli attacchi (i.e. 239 incidenti) ricadono nella categoria degli attacchi a lungo termine:



- I client sono lenti nel reagire
- Alto numero di attacchi o di tecnologie coinvolte (che a volte non sono il core business del cliente)
- Mancanza di risorse

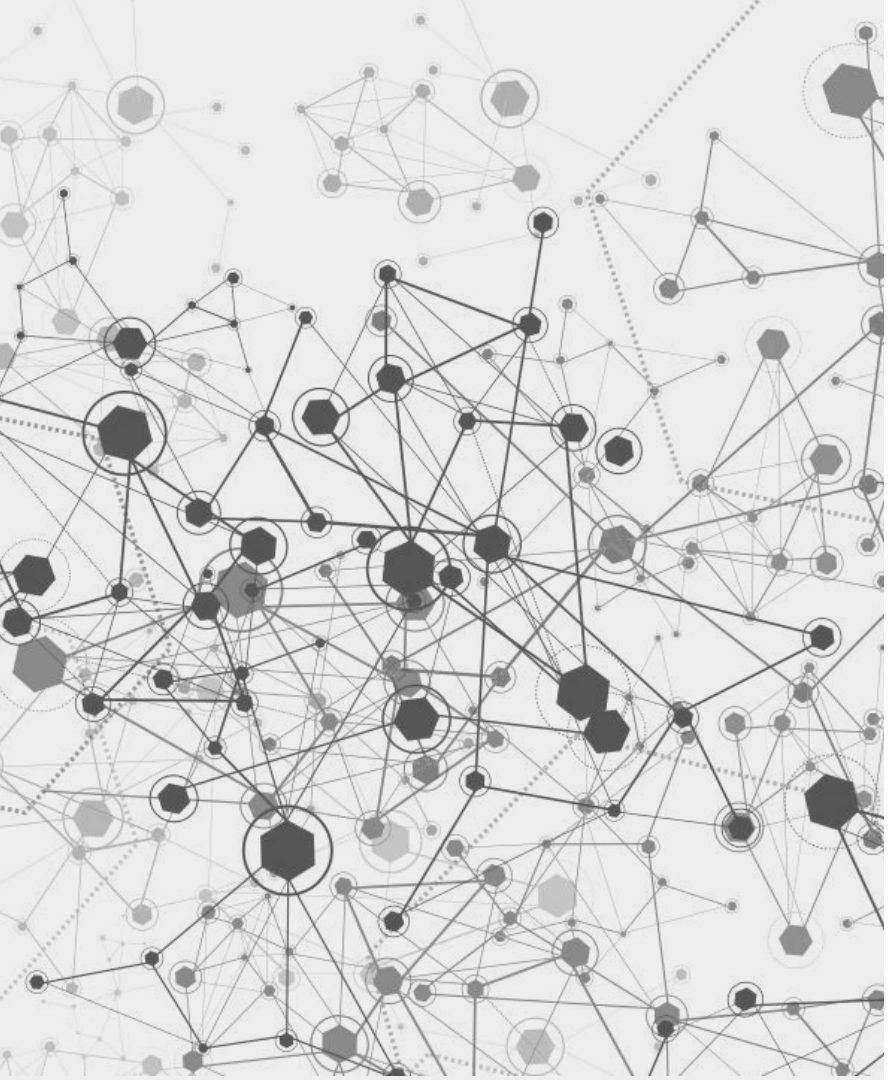
✓ I pattern tipici di attacco:

- Privilege Misuse
- Insieme di errori
- **Eventi sconosciuti**

[Sorgente: 2017 Data Breach Investigations Report by Verizon – 10th Edition]

LA NATURA DEGLI ATTACCHI: ANALISI

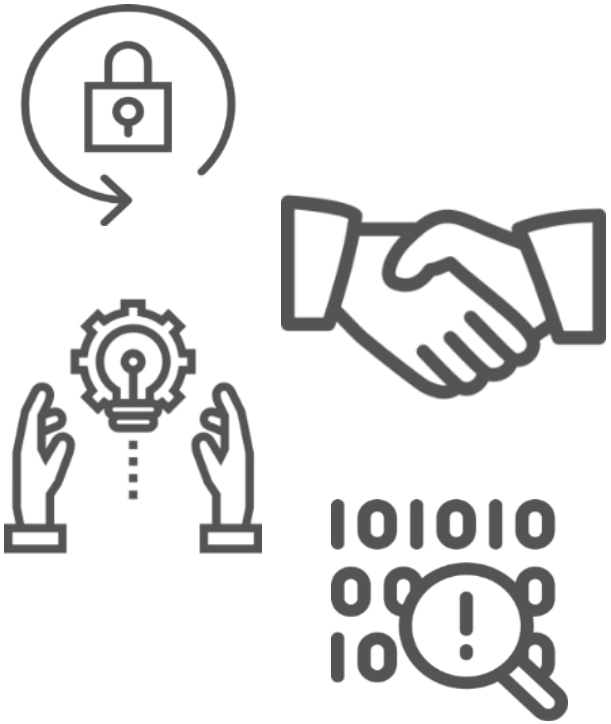
- ✓ **La maggior parte degli attacchi è dovuta a una non corretta implementazione delle politiche di sicurezza**, o perché le soluzioni sono troppo complesse per essere facilmente adottate dagli utenti finali
- ✓ **Quando viene rilevato un attacco, è SEMPRE troppo tardi**
- ✓ **La maggior parte degli attacchi sono sconosciuti (ca 40%)**, probabilmente perché sono stati progettati specificamente per quel particolare obiettivo. Significa:
  - ✓ **Più il know-how da proteggere è specifico, più l'attacco è mirato e più le aziende IT mainstream non sono adatte a proteggere le infrastrutture** (i.e. producono soluzioni per prevenire attacchi che colpiscono un gran numero di utenti, non attacchi chirurgici ad hoc ...)
  - ✓ **Gli attacchi sono simili ad azioni militari** (cioè ricognizione, profilazione, finto attacco per testare una reazione, attacco reale)
  - ✓ **Oggi è importante un approccio proattivo** (principalmente, **sicurezza in fase di progettazione**)



CASO REALE APPLICATIVO

ESIGENZE DA SODDISFARE

- ✓ **Gestione di attività manutentive in modo interattivo e remoto,** tramite l'uso di reti pubbliche
- ✓ **Protezione dei dati veicolati** (contro malware, trojan, attacchi di rete, attacchi hardware, etc..)
- ✓ **Riduzione costi per operazioni in campo,** a supporto di attività remote e su strutture distribuite sul territorio
- ✓ **Riduzione tempi di intervento:** possibilità di dispiegare velocemente personale sul territorio con supporto del solo competence centre relativo in remoto
- ✓ **Tracciabilità,** per quality assurance
- ✓ **Security by design** (OWASP, LPT,…)



PROGETTO PROPOSTO

Stazione di tele-diagnosi (fotocamera, scheda di acquisizione, postazione di comunicazione e collaborazione)

Dispositivo indossabile securizzato (Smartglass o dispositivo wearable dotato di casco, fotocamera, microfono, PC autoalimentato incorporato, modem Wifi e 4G). Il tecnico può essere istruito in tempo reale, mostrare ciò che sta vedendo e ricevere dati e documenti in modo sicuro

Altri tecnici possono **prendere parte ad un'attività remota** tramite laptop, tablet, smartphone (cioè in mobilità) o i dispositivi securizzati (computer portatili e smartphone) ed **interagire**

Tutte le attività possono essere registrate in maniera sicura a fini di audit e raccolte all'interno di **un portale interno per addestrare il personale**

Il portale ha **politiche di controllo accesso ed è protetto**, per evitare perdite di informazioni

SERVIZI PROPOSTI AL CLIENTE

- **Training del cliente per la gestione autonoma della soluzione** e la corretta implementazione delle misure di sicurezza necessarie:
  - ✓ **Penetration testing congiunto**, in modo da verificare la bontà della soluzione proposta
  - ✓ **Trasferimento di know-how** in modo da consentire al cliente di gestire autonomamente la soluzione, le sue configurazioni, le backdoor
  - ✓ Corsi di formazione sui pericoli informatici per il personale del cliente

- **Servizi consulenziali legali e tecnici** per la corretta applicazione copertura delle norme vigenti, principalmente:
  - ✓ **Il decreto Privacy GDPR** - Regolamento UE 2016/679
  - ✓ **Il decreto legislativo 8 giugno 2001/231** in fatto di tutela delle responsabilità amministrative delle persone giuridiche e delle associazioni in rapporto ai delitti informatici
  - ✓ Misure di sicurezza ICT per le PA – **Direttiva AGID del 1 agosto 2015**

CONTATTI

For more information, visit www. Feedbackitalia.com

mailto: demo@feedbackitalia.it
hushmeeting@feedbackitalia.it

Mirko Auro Minuzzo – Country Manager MENA
Mail: minuzzo@feedbackitalia.it
Phone: +39 335 60 34 879