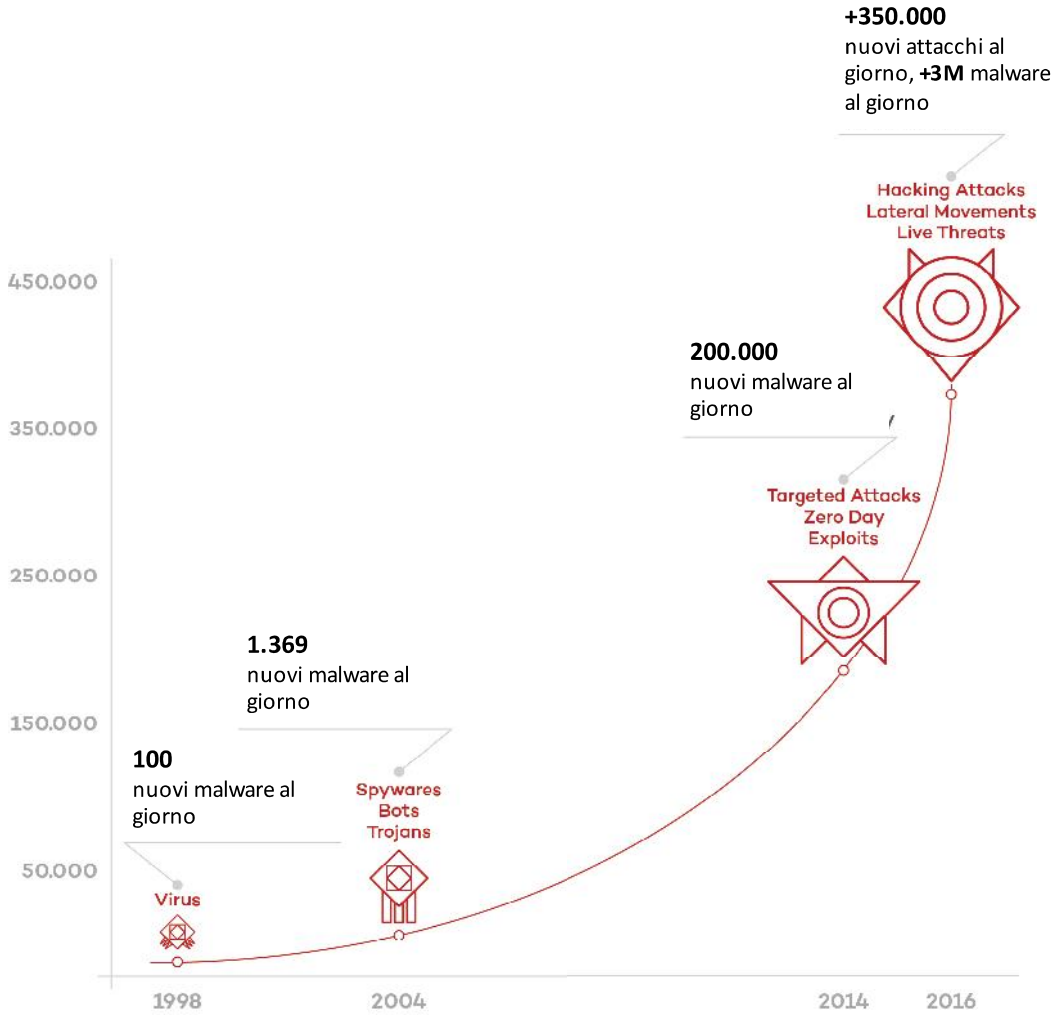
TMC
Top Management Consulting

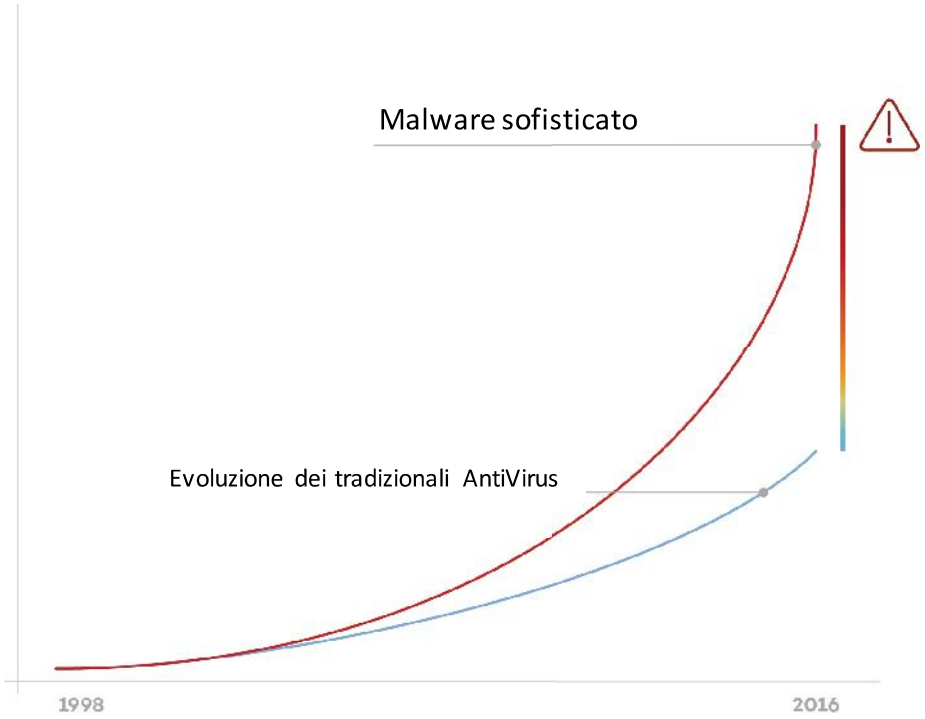
DATA RISK

Come tutelare i propri dati di business nel rispetto del nuovo Regolamento Europeo sulla protezione dei dati (GDPR - Reg. UE 679/2016 *)*

Ordini ODCEC e CdL Verona, 19 Marzo 2018

Evoluzione degli attacchi e fattore di successo





Fonte Panda Software

Alcuni dati del 2017

- ***Il 31,9% dei computer degli utenti ha subito, nell'anno, almeno un attacco web riconducibile alla classe dei malware***
- *Le soluzioni KL hanno respinto 758.044.650 attacchi lanciati attraverso siti Internet dislocati in ogni parte del mondo*
- *Sono stati riconosciuti come dannosi, da parte del modulo Anti-Virus Web, 261.774.932 URL unici*
- *Il 29,1% degli attacchi web neutralizzati è stato condotto attraverso risorse web malevole situate negli Stati Uniti*
- *Il modulo Anti-Virus Web ha rilevato 69.277.289 oggetti nocivi unici*
- *Gli encryptor hanno preso di mira 1.445.434 computer di utenti unici*
- *Le soluzioni KL hanno bloccato tentativi di lanciare malware capace di sottrarre denaro tramite il banking online su 2.871.965 dispositivi*
- *Il modulo Anti-Virus File ha rilevato, in totale, 4.071.588 programmi dannosi o potenzialmente indesiderabili*

Le statistiche sulle minacce mobile possono essere consultate nel report "Evoluzione del malware mobile nel 2016"

Rapporto Clusit 2017

Dilaga il cybercrime che colpisce il 100% delle aziende

Secondo il rapporto Clusit 2017, l'anno scorso gli attacchi gravi compiuti per finalità di cybercrime sono aumentati del 9,8%, con un incremento esponenziale soprattutto degli attacchi di phishing, cresciuti nell'ordine del 1.166%. I settori più colpiti? La sanità (+102%), seguita dalla grande distribuzione (+70%) e dalle banche (+64%).

L'evidenza principale dell'edizione 2017 del Rapporto è che ormai ***tutte le aziende sono sotto attacco, indipendentemente dalla dimensione o dal settore merceologico di appartenenza****.* ***"La probabilità di essere attaccati è pari a uno, ormai, basta che i malintenzionati abbiano il tempo sufficiente per agire*** *– commenta* ***A.Z.M., membro del Consiglio Direttivo del Clusit****. La definitiva consacrazione delle logiche di crime-as-a-service, infatti, permette anche ai criminali comuni di allargare il perimetro delle proprie attività illecite al web semplicemente affittando infrastrutture e strumenti di attacco dai produttori solo per il periodo strettamente necessario, a fronte del versamento di una percentuale dei proventi illeciti".*

Attaccanti competenti che usano tutte le armi

1. Intelligence (su persona e azienda)

– Sorgenti aperte

– Sorgenti chiuse

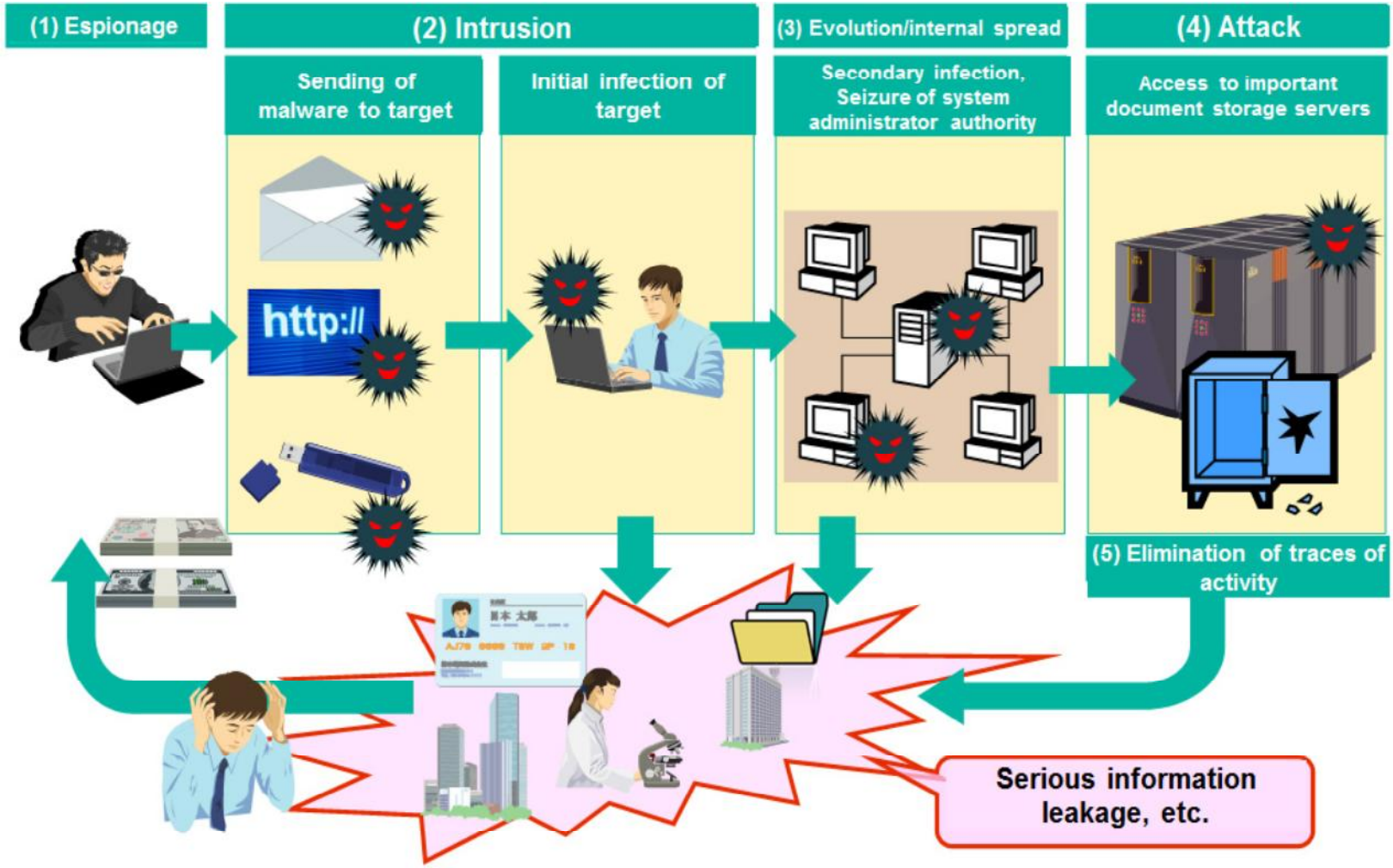
2. Psicologia

– spear phishing che sfrutta fiducia, scarsa osservanza delle regole, abitudini, ideologia, timori, bramosia di guadagni, insoddisfazione, narcisismo, ecc.

3. Tecnologia

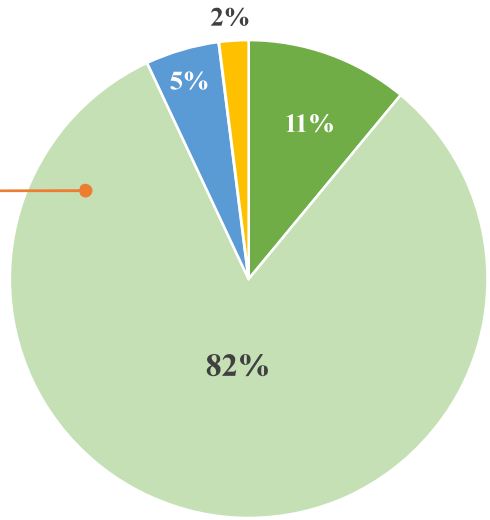
– malware inviato attraverso multipli canali di comunicazioni e sfruttando (multiple) vulnerabilità del software

Analisi di un tipo di attacco e dei suoi effetti



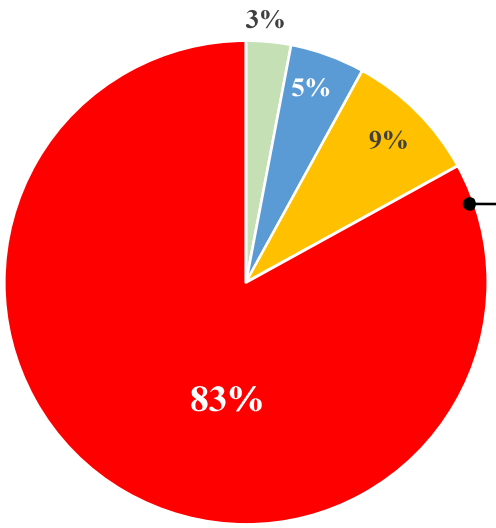
Due differenti velocità ed il gap aumenta sempre

Tempo di compromissione



I Cyber-criminali sono più efficienti che mai.

Tempo di rilevamento



Rilevare una compromissione richiede tempo,

spesso troppo tempo!

secondi minuti ore giorni settimane

TMC
Top Management Consulting

Possibili conseguenze di un attacco

- I documenti presenti sul computer vengono **cifrati**
- I documenti diventano **illeggibili**
- I **nostri** dati vengono **rubati** e messi in rete o venduti a terze parti
- I dati dei **Clienti** vengono rubati e messi in rete o rivenduti
- I **dati personali o particolari** vengono venduti o manipolati
- I server o i mobile dovranno essere riformattati con potenziali perdite di dati
- Tutto il lavoro presente sul computer non esiste più
- Il **backup**, per chi ne è dotato, a quale data risale? E i backup sono stati a loro volta compromessi?
- Formule, disegni, progetti, brevetti vengono rubati e rivenduti
- Mail e documenti possono essere messi in rete con danno di immagine o reputazione dell'azienda e/o personale

Possibili costi di un attacco (data breach)

Costi di ripristino

Riprogettazione e aggiornamento sistemi informatici e di sicurezza, Lavoro straordinario, Riqualificazione del personale, Recupero e ridigitazione dati esterni

Interruzione di attività

Fermo di produzione, Impossibiità di erogare I servizi, Perdita di fatturato, Pagamento di penali per mancata consegna…

Responsabilità civile

Contenzioso legale (class action), Rivalsa di Clienti o dipendenti

Costi di notifica

Esame informatico forense, Stampa, spedizione e altre comunicazioni, Servizio di monitoraggio del credito

Sanzioni amministrative

Per la nuova privacy dal 2% al 4% del fatturato

Danno reputazionale

Danno all'immagine, Perdita di credibilità e di fiducia, Deprezzamento delle azioni

Costi per tutelare il brand e la reputazione

Legale, Pubbliche relazioni, Pubblicità e relative comunicazioni

TMC
Top Management Consulting

Chi viene colpito e perché?

Chiunque …per gioco ….o per soldi!!!

TMC
Top Management Consulting

QUINDI LA DOMANDA NON E' SE ……. MA QUANDO?!!

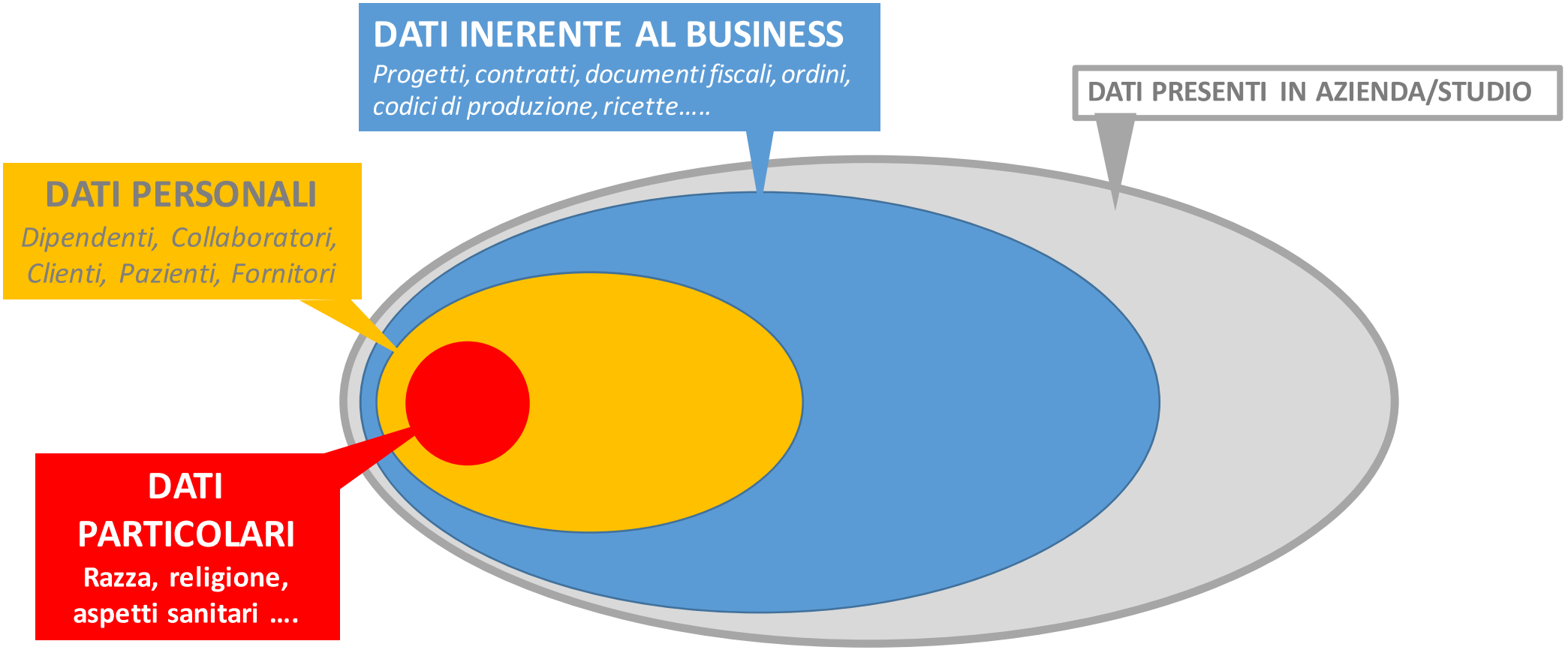
Ed avrò fatto tutto il possibile per difendermi?

Saprò reagire tempestivamente?

Avrò fatto tutto in regola per non essere sanzionato?

Avrò attivato una copertura assicurativa adeguata?

Ma quali sono i dati a rischio?



Ma qual'é il vero obiettivo di un attacco

Rubare i dati

- e metterli gratuitamente in rete (per sfregio, per gioco, per ragioni politiche, …)
- o rivenderli a terze parti (call center, ditte di profilazione, direct marketing,..)

Rubare Know-how

- Formule, disegni, progetti, brevetti, contratti, nomi di clienti, fatture vengono rubati e rivenduti

Rubare soldi

- Mediante richieste di riscatto dei dati (es. criptolock)
- Mediante il blocco dei servizi e la richiesta di un riscatto per il suo sblocco
- Mediante l'utilizzo improprio dei dati bancari