Dettagli sul fenomeno in Corso
I principali Vettori di attacco

1) **Sfruttamento Vulnerabilità:** In cybersecurity, una vulnerabilità è una criticità che può essere sfruttata dai Criminal Hacker per ottenere un accesso non autorizzato a un sistema informatico. Dopo aver sfruttato una vulnerabilità, un criminale informatico può eseguire codice dannoso, installare malware e persino rubare dati sensibili;

2) **Social Engineering:** Nel contesto della sicurezza informatica, il social engineering è l'uso dell'inganno per manipolare le persone nel divulgare informazioni riservate o personali che possono essere utilizzate a fini fraudolenti. In altre parole, le persone possono essere ingannate nel condividere informazioni che altrimenti non divulgherebbero. La variante più comune è il Phishing, mail costruite ad hoc per ingannare il destinatario e costringerlo a rivelare dati o informazioni sensibili;

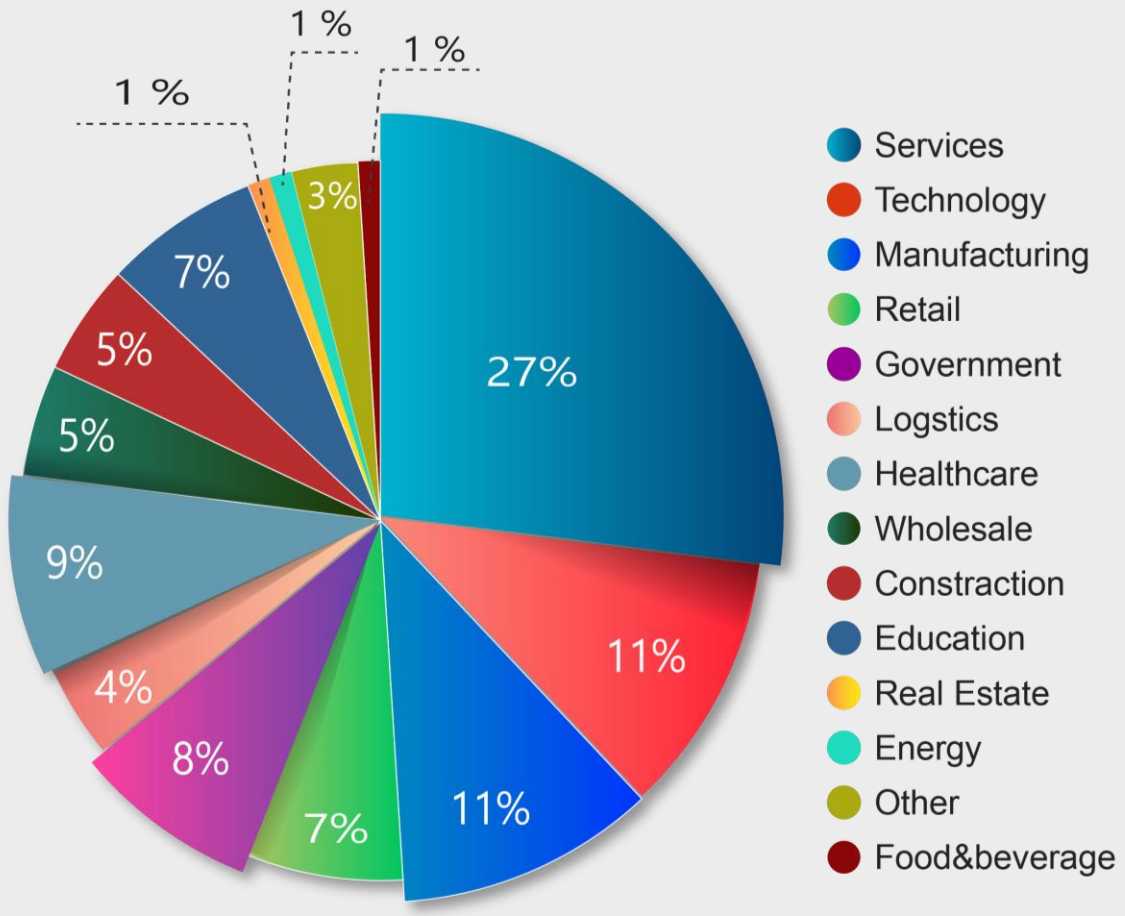
3) **Botnet:** Le botnet sono grandi reti di computer compromessi, la cui potenza di elaborazione viene utilizzata all'insaputa dell'utente per svolgere attività criminali. Questo può includere la distribuzione di spam o e-mail di phishing, così come l'esecuzione di attacchi DDoS, ma anche il furto di credenziali di accesso a servizi aziendali e non solo;

4) **Supply Chain attack:** Ogni azienda o infrastruttura non è più oramai monolitica, ma si appoggia su una lunga e complessa supply chain digitale. I Criminal Hacker possono colpire il proprio target proprio andando a compromettere un fornitore a monte;

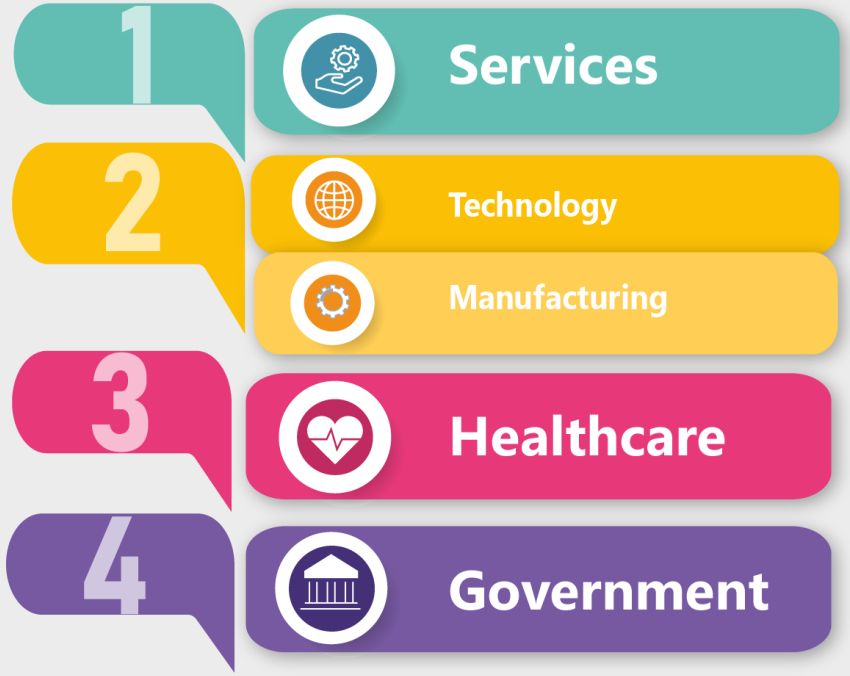
5) **0 – Day:** Questa è l'insidia maggiore per ogni organizzazione, gli zero-day sono così noti perché lasciano appunto – zero giorni di tempo – agli sviluppatori per correggere una vulnerabilità prima che venga sfruttata. In essenza sono criticità che vengono scoperte solo nel momento in cui un attacco è già in corso.

I settori di riferimento. Perchè ?

Attacchi per settore in percentuale

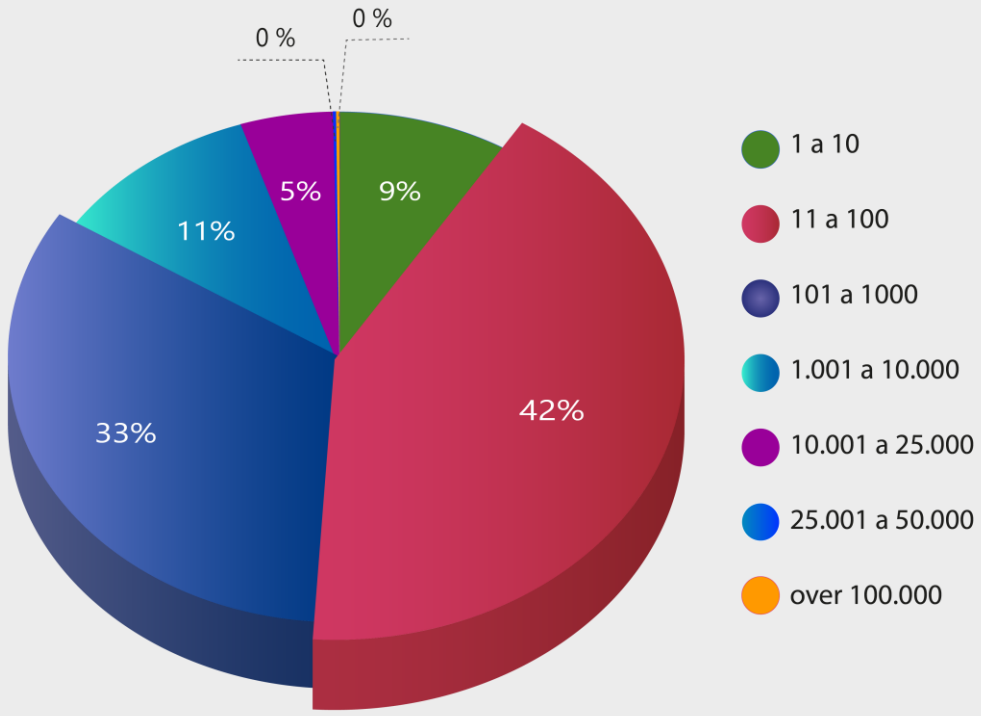


I Settori più Colpiti

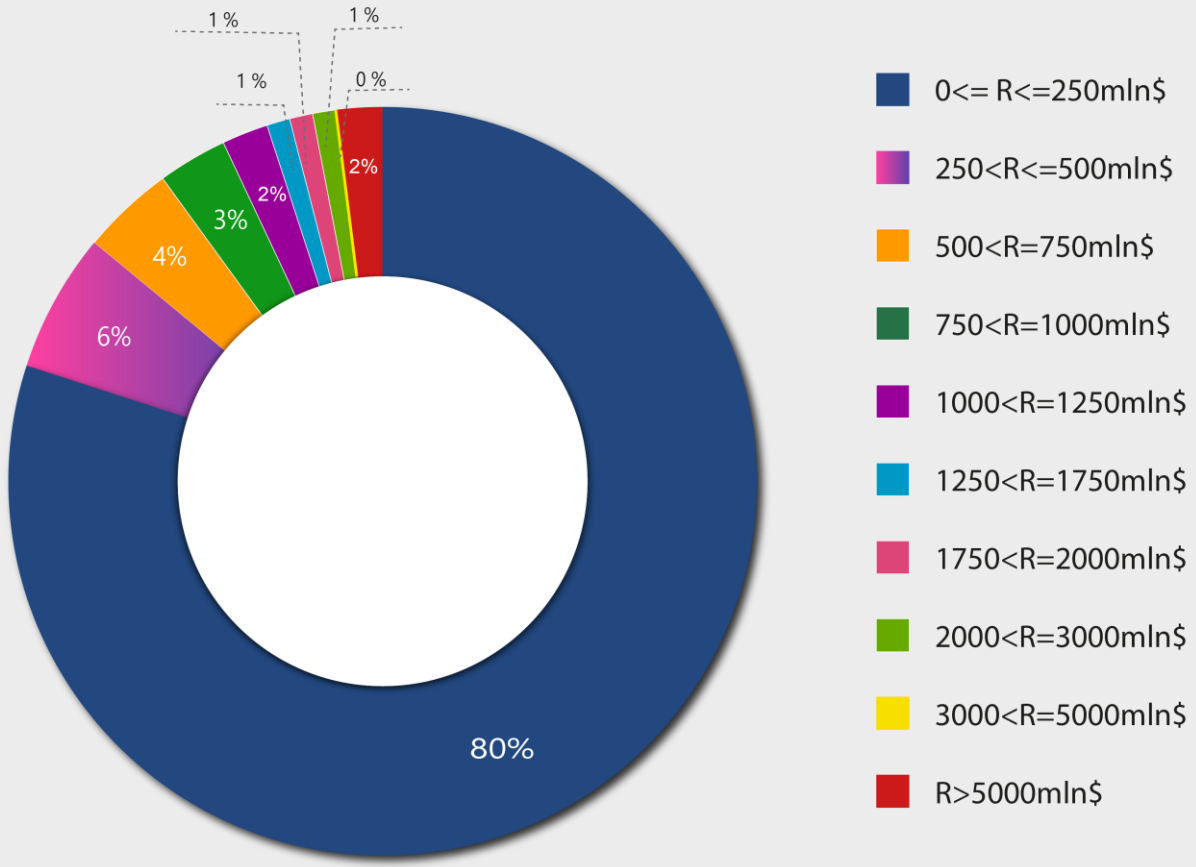


Dipendenti e fatturato

Numero Dipendenti Aziende Colpite



Spaccato Aziende Colpite In Base A Fatturato



Le modalità di attacco

Attacco DDOS

DDoS: Un attacco DDoS (Distributed Denial-of-service) è una tecnica di cyber attack utilizzata al fine di interrompere il normale funzionamento di server, servizi o reti tramite un flusso di traffico internet anomalo e oltre la capacità del target.

Social engineering

Social Engineering: Nel contesto della sicurezza informatica, il social engineering è l'uso dell'inganno per manipolare le persone nel divulgare informazioni riservate o personali che possono essere utilizzate a fini fraudolenti. In altre parole, le persone possono essere ingannate nel condividere informazioni che altrimenti non divulgherebbero. La variante più comune è il Phishing, mail costruite ad hoc per ingannare il destinatario e costringerlo a rivelare dati o informazioni sensibili;

Sfruttamento delle Vulnerabilità

Sfruttamento Vulnerabilità: In cybersecurity, una vulnerabilità è una criticità che può essere sfruttata dai Criminal Hacker per ottenere un accesso non autorizzato a un sistema informatico. Dopo aver sfruttato una vulnerabilità, un criminale informatico può eseguire codice dannoso, installare malware e persino rubare dati sensibili.

Botnet

Botnet: Le botnet sono grandi reti di computer compromessi, la cui potenza di elaborazione viene utilizzata all'insaputa dell'utente per svolgere attività criminali. Questo può includere la distribuzione di spam o e-mail di phishing, così come l'esecuzione di attacchi DDoS, ma anche il furto di credenziali di accesso a servizi aziendali e non solo.

Zero Day

0 – Day: Questa è l'insidia maggiore per ogni organizzazione, gli zero-day sono così noti perché lasciano appunto – zero giorni di tempo – agli sviluppatori per correggere una vulnerabilità prima che venga sfruttata. In essenza sono criticità che vengono scoperte solo nel momento in cui un attacco è già in corso.

Supply Chain Attack

Supply Chain Attack: ogni azienda o infrastruttura non è più oramai monolitica, ma si appoggia su una lunga e complessa supply chain digitale. I Criminal Hacker possono colpire il proprio target, andando a compromettere un fornitore a monte.