



# RANSOMWARE: STRATEGIE DI DIFESA

# RANSOMWARE: LA TECNICA DI ATTACCO PIÙ DIFFUSA

## Due principali tipi di attacco



Distributed  
DoS  
(DDoS)

Invia **enormi quantità di dati** per rendere **inaccessibile** una risorsa o un'intera rete

La richiesta di **riscatto** viene inviata **durante** l'attacco per farlo **cessare**

Attacco **estremamente violento** e brutale



Crypto-  
locker

**Cifra** tutti i dati aziendali e li rende **inutilizzabili** senza la chiave di accesso

La richiesta di **riscatto** avviene dopo la **cifratura**

Attacco **"chirurgico"** - hacker possono **studiare** l'azienda dall'interno



## DDOS – CONTROMISURE POSSIBILI

Obiettivo:  
**Assorbire  
l'aumento  
di traffico  
generato  
dall'attacco**

Verifica su fornitore  
servizi di TLC

Rete protetta da anti-  
DDoS

Tipo di protezione  
(always-on, automatica,  
manuale)

Protezione customizzabile

Verifiche "buona  
salute" della rete  
aziendale

SW aggiornato

Verifica vulnerabilità

Verifica traffico anomalo



## CRYPTOLOCKER – CONTROMISURE POSSIBILI

Obiettivo:  
**Rendere  
sempre  
disponibili  
le risorse  
chiave**

### Sicurezza perimetrale

Firewall,  
antivirus, policy  
comportamento

VAPT periodici

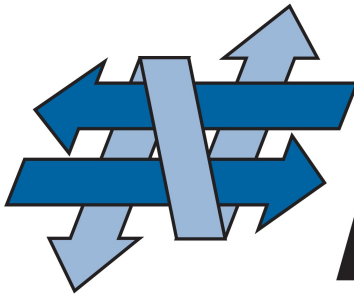
### Backup Delocalizzati

Dati chiave  
isolati

Agent  
(automatizzati)

Regola 3-2-1





*NET & CLOUD PROVIDER*

***FASTNET***<sup>®</sup> Spa