Best practice - Rete

- Utilizzare servizi di "IP address reputation" che consentano il blocco selettivo di IP, siti e URL ritenuti pericolosi;

- Bloccare il traffico verso i Command-and-Control server, in quanto questo limita il meccanismo di comunicazione di molti malware;

- Permettere la navigazione web solamente verso siti categorizzati o preventivamente controllati (white list); usando usare un sistema a liste di web reputation, in maniera da evitare accessi a quei siti che possono essere pericolosi in quanto segnalati in varie "black-lists"

- Diffidare da email non attese, o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad aprire un allegato o cliccare su un link;

- Network Intrusion Detection System (NIDS): sono degli strumenti informatici, software o hardware, dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche. I più comuni NIDS sono composti da una o più sonde dislocate sulla rete, che comunicano con un server centralizzato, che in genere si appoggia ad un Database. Fra le attività anomale che possono presentarsi e venire rilevate da un NIDS vi sono: accessi non autorizzati, propagazione di software malevolo, acquisizione abusiva di privilegi appartenenti a soggetti autorizzati, intercettazione del traffico (sniffing), negazioni di servizio (DoS).