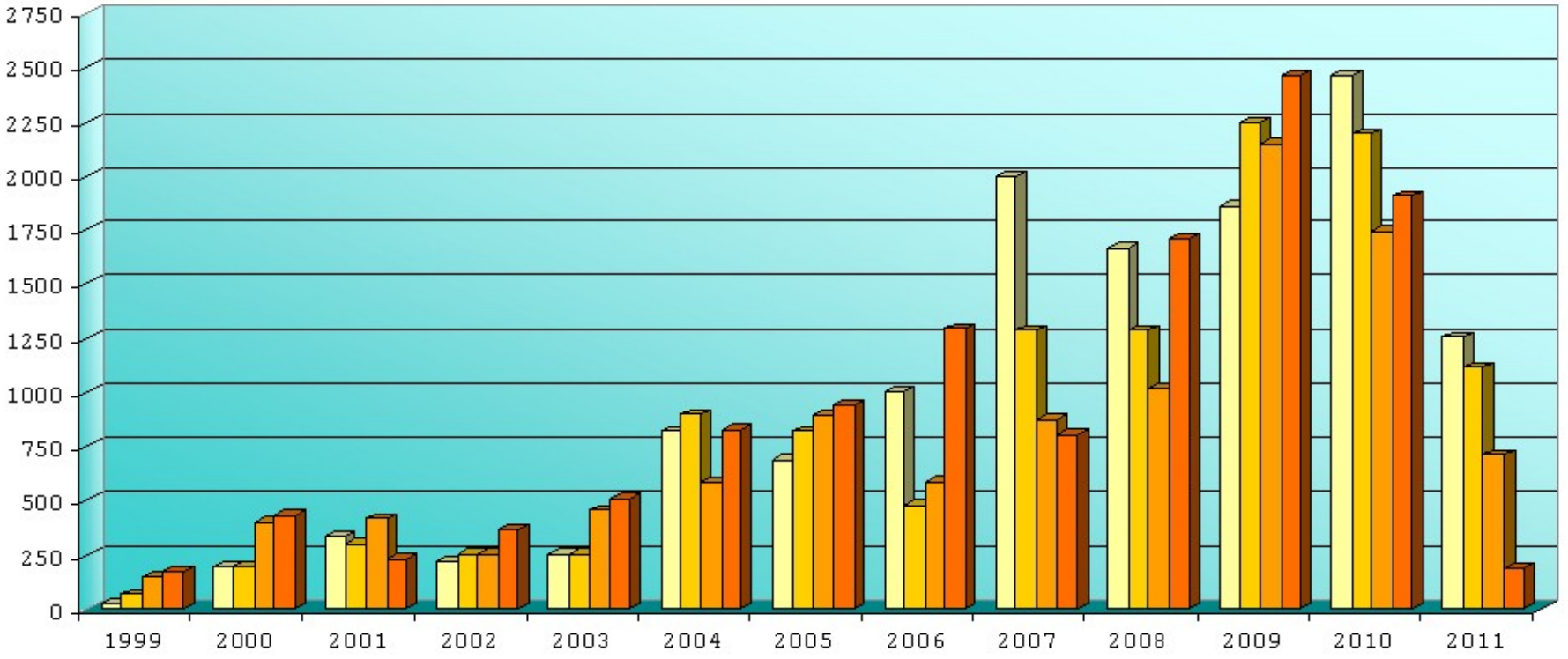
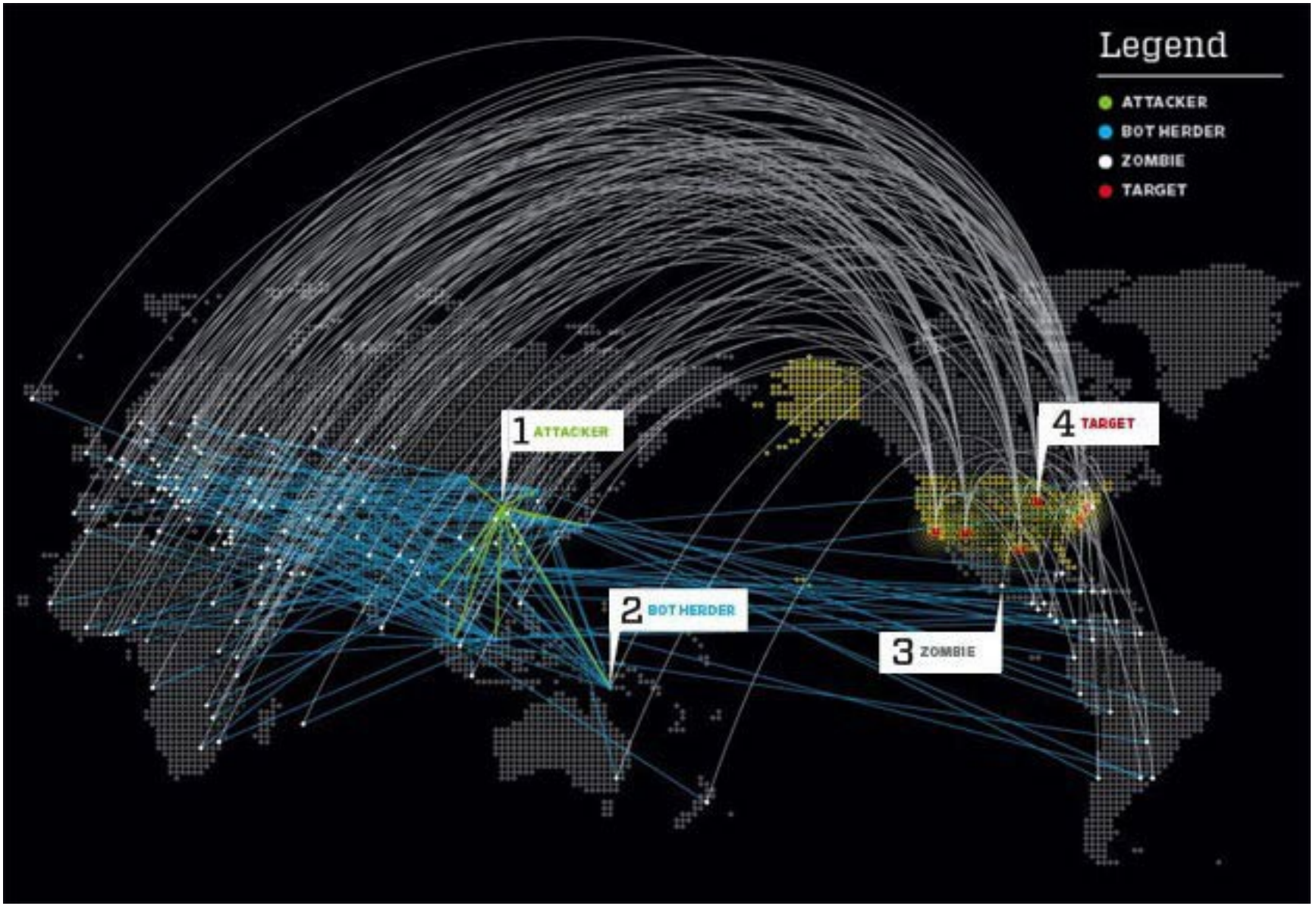
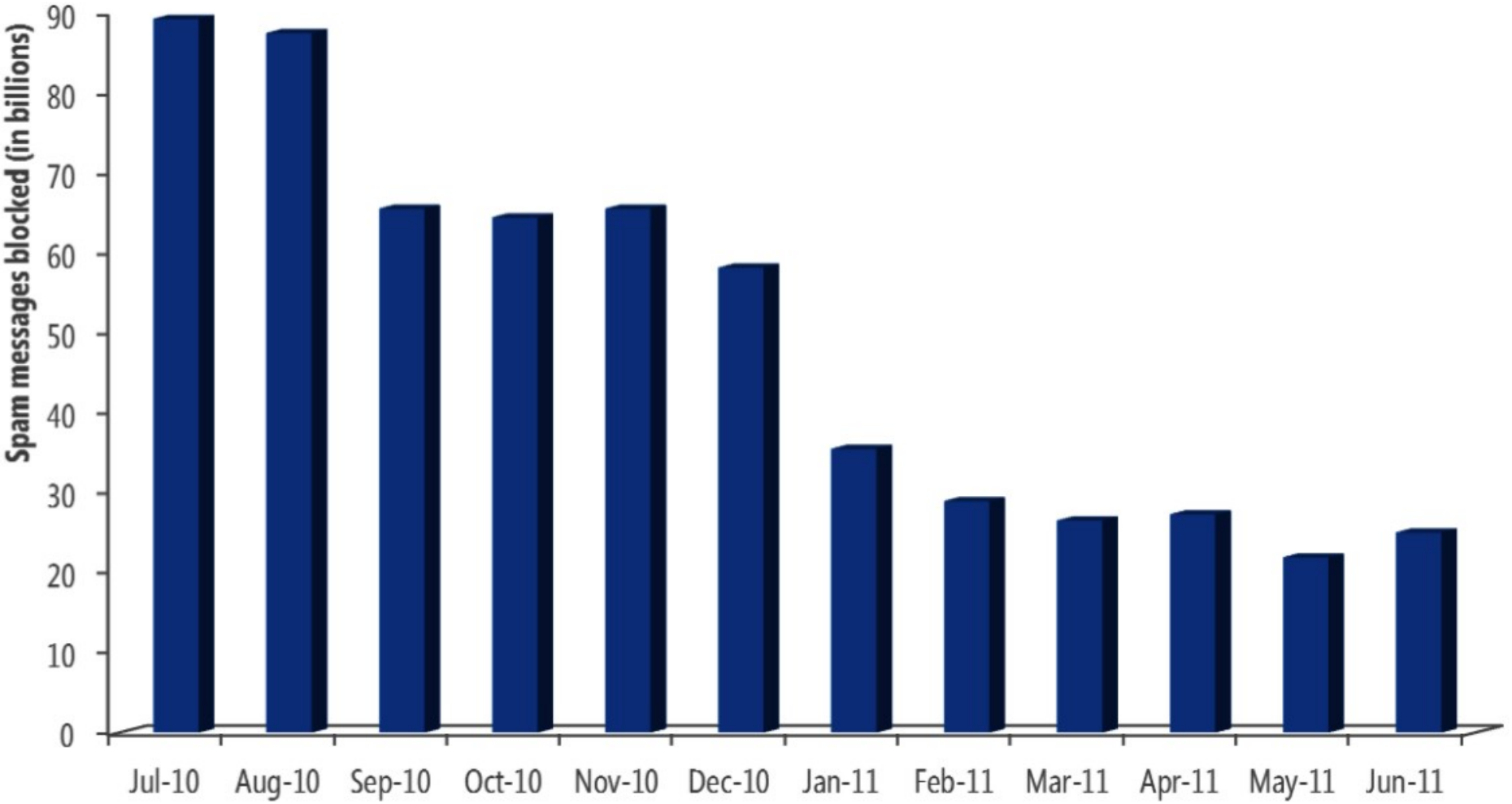

VIAGRA
C20

Incidenti aperti da GARR-CERT (fino al 28/10/2011)

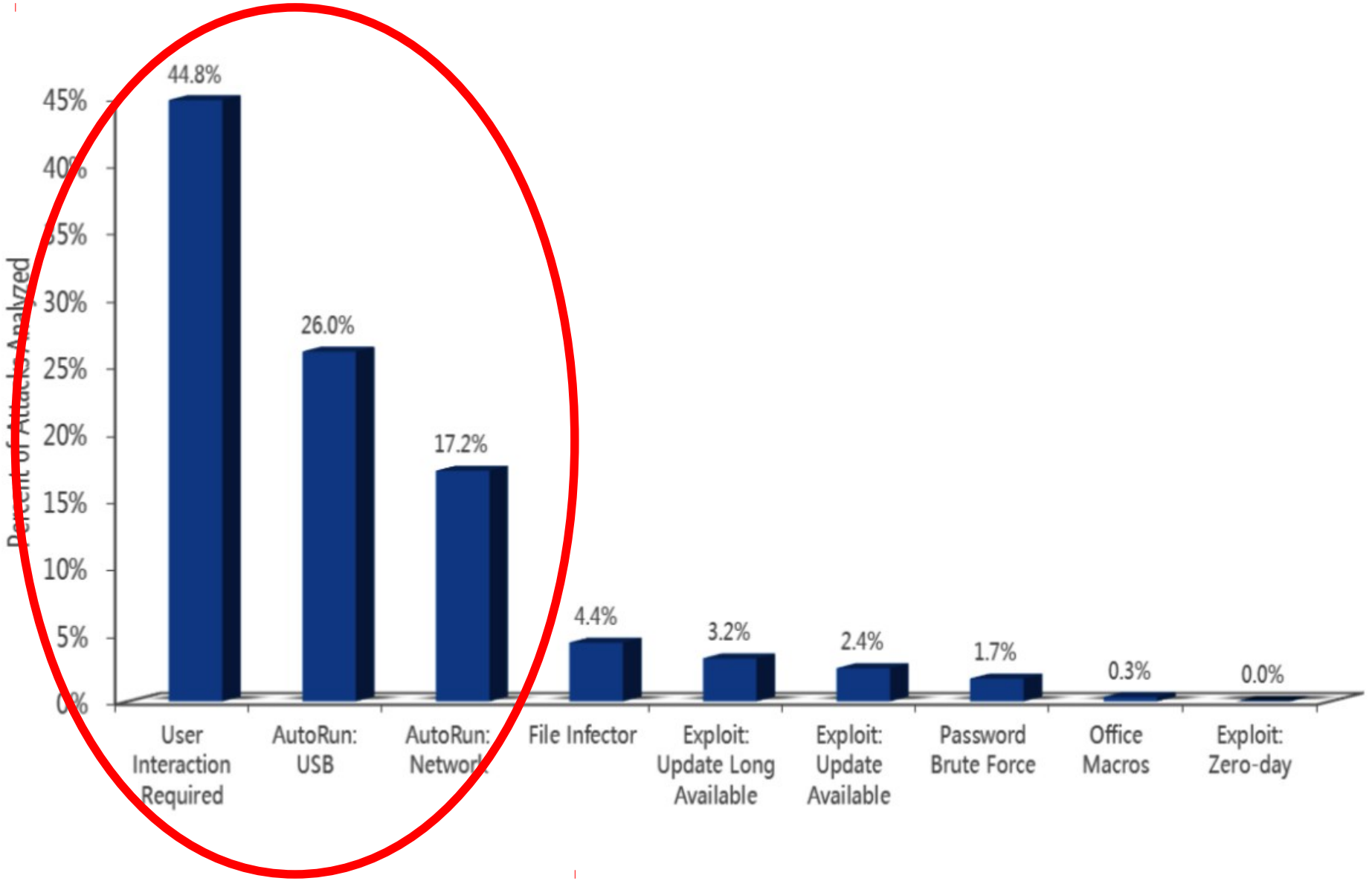


In diminuzione???


Legend
ATTACKER
BOT HERDER
ZOMBIE
TARGET
1 ATTACKER
2 BOT HERDER
3 ZOMBIE
4 TARGET



Microsoft Security Intelligence Report, Vol. 11



Microsoft Security Intelligence Report, Vol. 11


SPAM®
Lite
50% LESS FAT
33% FEWER CALORIES
25% LESS SODIUM
THAN SPAM® CLASSIC
Crazy Tasty
SIGNATURE RECIPE COLLECTION
Hormel foods

BOTNET

Utenti ”ingenui”…

Chiudete quella porta!

Autenticate i client!

Limitate i flussi!

Limitate i destinatari!

Alcune risposte caratteristiche di gestori di NAT (giuro che non le ho inventate!):

- ”mi servirebbe il MAC address del nodo origine”;
- ”nell’intervallo temporale indicato non vi sono registrazioni dell’attività segnalata”;
- ”non sono in grado di risalire al sistema origine”;
- ”ho mandato una mail di alert a tutti gli utenti perché controllino le proprie macchine”;
- ”sono portatili di studenti connessi in wireless: non si può fare niente”.

Tutti gli utenti a cui vengono forniti accessi alla Rete GARR devono essere **riconosciuti** ed **identificabili**. Devono perciò essere attuate tutte le misure che impediscano l'accesso a utenti non identificati.

AUP GARR

Delle 14 blacklist più utilizzate, ABUSES Forum ne sconsiglia 7 (il 50%)!

- **APEWS**
- **FIVE-TEN**
- **MAPS-DUL**
- **MAPS-RBL**
- **SORBS SPAM DATABASE**
- **SPAMCANNIBAL**
- **UCEPROTECT**

E le whitelist?

Ma ce la fa?
Ma quanto mi costa?

Mi chiudo a cozza, ma il traffico interno?

Quanti protocolli non sono facilmente analizzabili ”al volo”?

Quanto è facile aprire un tunnel?

E l'encryption E2E?

E la roba tra le nuvole?

eduroam

Standard IPSec VPN: IP protocols 50 (ESP) & 51 (AH) both egress and ingress; UDP/500 (IKE) egress.

OpenVPN 2.0: UDP/1194.

IPv6 Tunnel Broker service: IP protocol 41 ingress and egress.

IPsec NAT-Traversal UDP/4500.

Cisco IPSec VPN over TCP: TCP/10000 egress.

PPTP VPN: IP protocol 47 (GRE) ingress and egress; TCP/1723 egress.

SSH: TCP/22 egress.

HTTP: TCP/80 & 443 egress

IMAP2,3,4: TCP/143, 220 & 993 egress.

POP: TCP/110 & 995 egress.

Passive (S)FTP: TCP/21 egress.

SMTP: TCP/465 & 587 egress.

RDP: TCP/3389 egress.