

Allaple

Tarko Tikan (Starman)

Anto Veldre (Sampo Pank)

2007-12-13

Latimeeria



(C) Miksike

Allaple

- W32/Allaple
- RAhack
- Trojan.Starman

Allaple

- MS04-012
- ICMP “Babcdefghijklmnopqrstuvwxyz”
- HTTP GET
- TCP SYN
- NetBIOS137/139?
- No Command & Control Centre
- Polymorphic (manual)

MS04-012

- 0,00, 000,0000,00000,000000,0000000,00000000,000000000,
1,12,123,1234,12345,123456,1234567,12345678,1234567
89,abc123,access,adm,Admin.alpha,anon,anonymous,asdf
gh backdoor,backup,beta,bin, coffee,computer,crew,
database,debug,default,demo go,guest hello install,internet,
login,mail,manager,money,monitor,network,new,newpass,
nick,nobody,nopass,oracle,pass,passwd,password,poiuytre,
private,public qwerty, random,real,remote,root,ruler secret,
secure, security, server, setup, shadow, shit, sql, super, sys,
system,telnet, temp, test, test1, test2, visitor,
windows,www, X

Lõpp ikka hea?

- *Latimeria chalumnae*

