Zneužití linuxového serveru: útoky z honeynetu

CZ.NIC z.s.p.o.

Jiří Machálek / *jiri.machalek@nic.cz*
24. 11. 2012

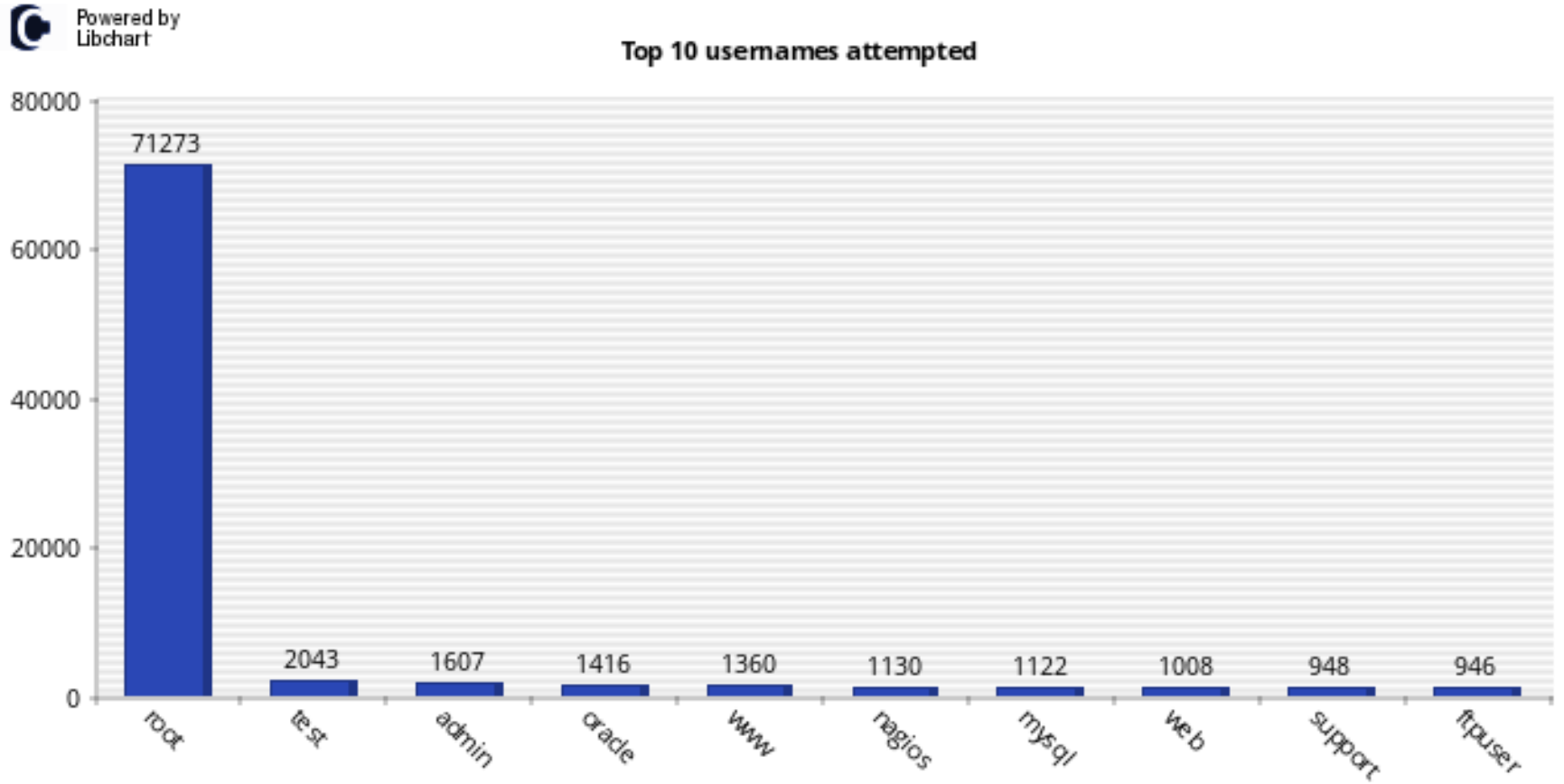
Honeynet CZ.NIC

- Monitorovaná síť záměrně zranitelných serverů
- Projekt Dionaea
  - http://dionaea.carnivore.it/
  - Replikuje známé zranitelnosti Windows
  - Čtvtletně statistiky na http://blog.nic.cz/
- Projekt Kippo
  - Simulace linuxového stroje se slabými přístupovými údaji
  - http://code.google.com/p/kippo/

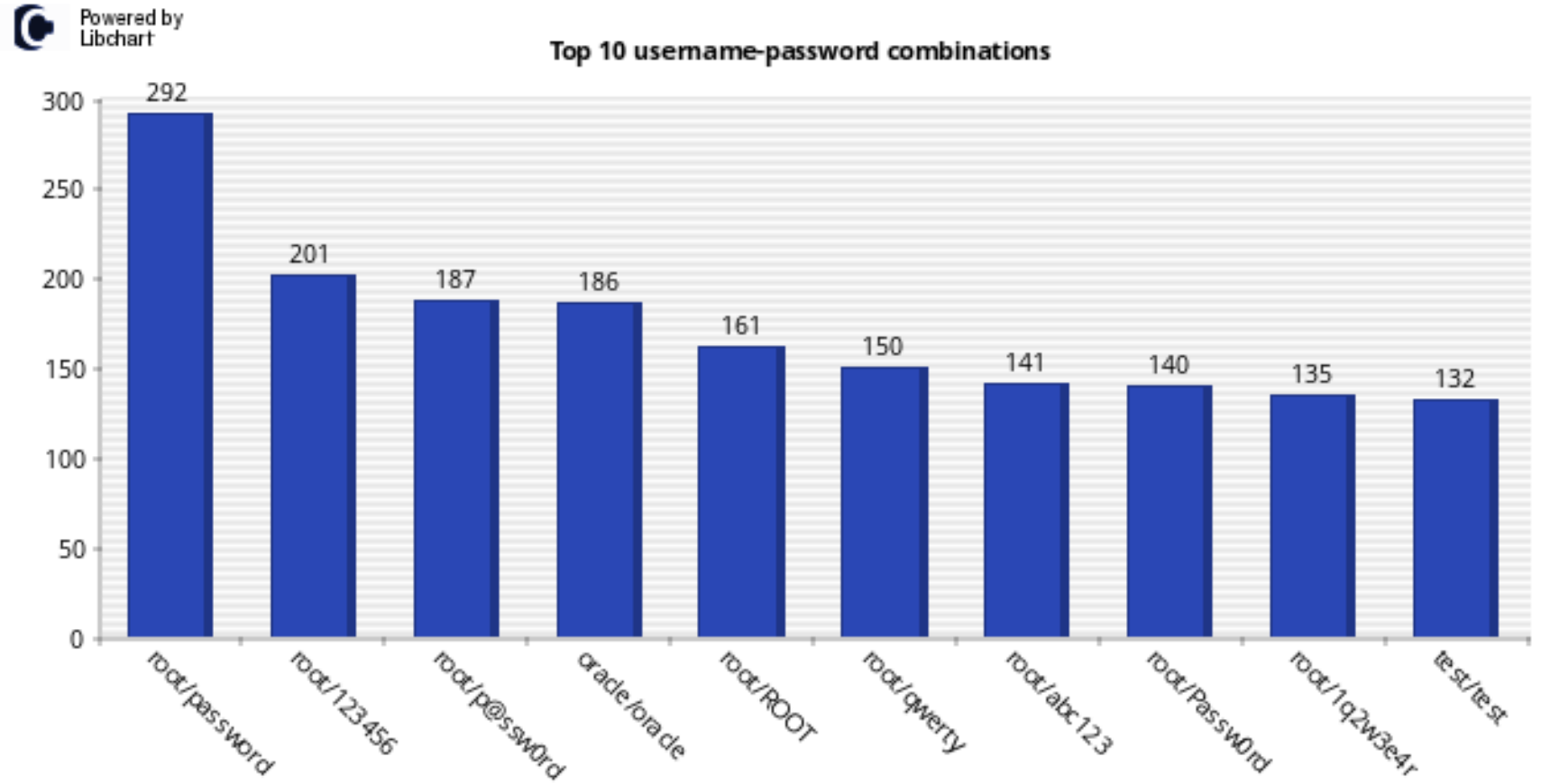
Kippo

- virtuální souborový systém
- implementované příkazy wget, tar, apt-get, passwd, shutdown, ping, adduser, ssh, aj.
- simulace spuštění známých typů malware
- náhodné chyby při spuštění neznámých skriptů

Pokusy o přihlášení: nečastější účty



Pokusy o přihlášení: kombinace login/heslo



CZ.NIC | SPRÁVCE DOMÉNY CZ

Chování útočníků

- Benchmarking – cat /proc/cpuinfo, kvalita připojení
- Zapojení do botnetu (řízení přes IRC)
- Scanování jiných strojů
- Zvýšení oprávnění
- Zajištění přístupu (passwd, authorized_keys)
- Skrývání stop (adresář “...”, “ “, history -c)

Ukázky

Děkuji Vám za pozornost

Jiří Machálek

jiri.machalek@nic.cz

Kde získat informace o dalších aktivitách sdružení CZ.NIC?

www.nic.cz

blog.nic.cz

Facebook CZ.NIC

Twitter CZ.NIC

CZ.NIC | SPRÁVCE DOMÉNY CZ