Router (telnet) botnety

slashing them for lot of fun and no profit (yet)

lexik

=====

CTJB 2015

=====

honeypotíme

- Telnet v chrootu vs. sbírání trafficu-only
- Logující iptables
  - Fancy statistiky (nemám)
- Připojujeme se zpátky (*wink* *wink*)
  - admin:admin
- ~~Děláme si vlastní botnet~~

Reverzíme, analyzujeme

- Strings, hexdump, objdump … hardcore
- ARM v qemu (scratchbox)
  - Risky yet fun
  - Strace
- lightaidra and rare ones
  - DDoSítko, klikátko na reklamy, těžítko (BTC, DOGE)
    - Řečnická otázka: kolik to vydělává?
    - Řečnická odpověď: né dost.

C&C slashing (DIY CERT)

- IRC based
  - Někdy hostováno (IRC a/nebo binárky) na pwnutých webserverech
    - Pwn them too / kontaktovat majitele
  - Kontaktujeme providera VPSky
    - Response se liší kus od kusu
  - Kontaktujeme autora na IRC channelu (͡° ͜ʖ ͡°)
    - Autoři si neradi povídají (͡° ʖ̯ ͡°)
  - Botnet overtake
    - Strings is you friend
    - Illegal ofc
- exploitace SMB, RPC
  - Proč to tam vůbec běží?

HACK EM'

```
cat /var/log/syslog | grep "New" | awk {'print $12'} |
grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}" | uniq
```

- **lexik.kybersquat.cz/hackem.txt**

```
cat telnet-honeypot/telnetlog.txt | grep -E -o "([0-9]
{1,3}[\.]){3}[0-9]{1,3}" | sort | uniq
```

- **lexik.kybersquat.cz/hackem2.txt**

EOF

- Dotazy, diskuze, free hacking, party, zabití zbývajících minut