RSAC Studio

CHANGE

Challenge today's security thinking

Hack The Planet: Some Men Just Want to Watch the World Burn

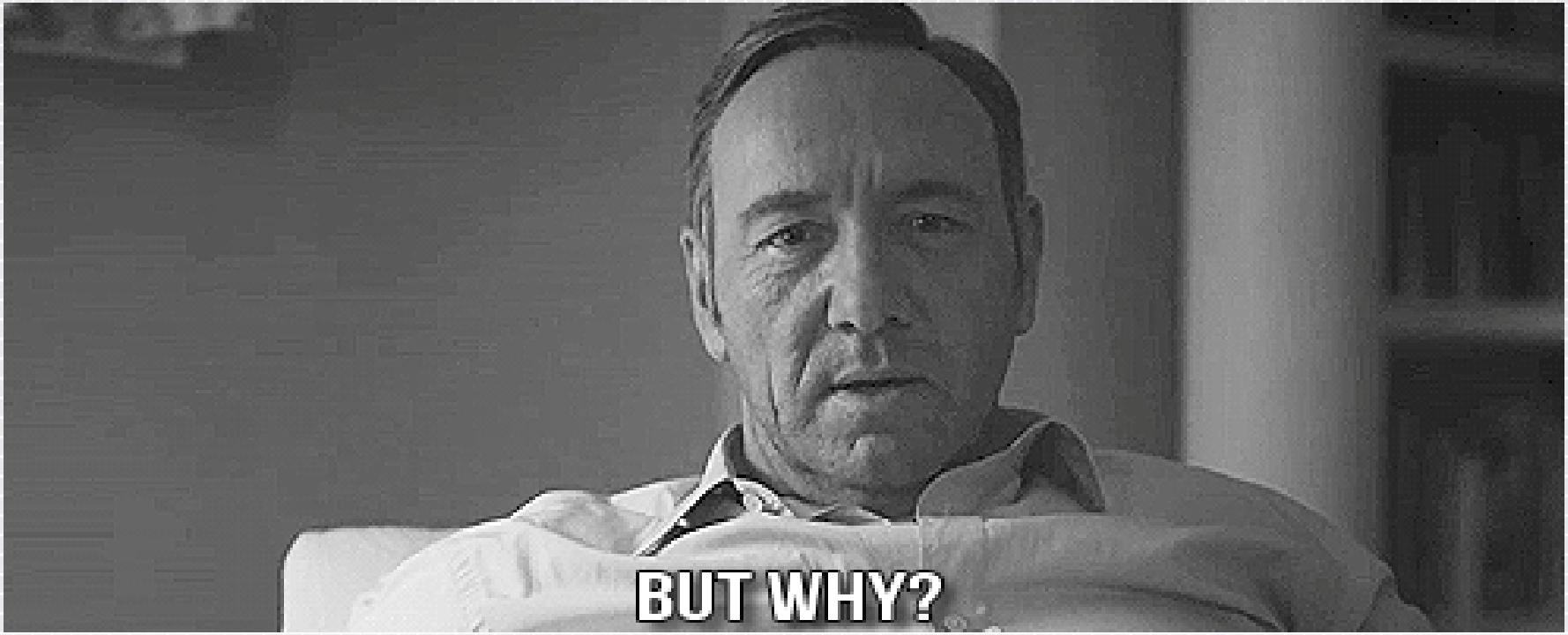
Mark Arena

Chief Executive Officer
Intel 471
@markarenaau

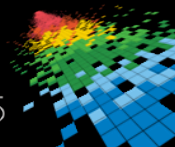

ARCHIVE
IN COMMONLY USED PASSWORDS WE TRUST


IN COMMONLY USED PASSWORDS WE TRUST

Lizard Squad


BUT WHY?

some.lizards.just.want.to.watch.the.world.burn



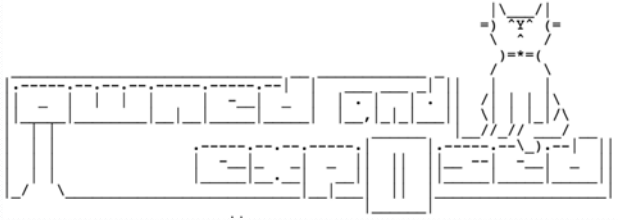
Origins

- Anti-sec movement first started in the late 1990s;
- Discouraged full disclosure of vulnerabilities and exploits;
- Promoted attacks against the security industry;
- pr0j3kt m4yh3m.

Beginnings

2010

- "Owned and Exposed"



2011

- Aug – Zine sent to Full Disclosure

Target: SwiftIRC

2013

- Early 2013 – Compromise of Linode

2013

Q1

- Windows trojan: “Zodiac”

Q2-Q3

- Web server botnet
  - Ruby on Rails vulnerability
- DNS amplification attacks (DDoS)

Lizard Squad: 2014 - 2015

Lizard Stresser

Targets

XBOX LIVE

PlayStation Network

malaysia airlines

webnic
accelerate your business

Google

lenovo

Other activity – 2014 - 2015

Wikileaks Support

- Seeking information on govt intelligence programs

Botnet

- Likely building web server botnet
  - Joomla exploitation

Targeted attacks TTPs

- Password re-use/brute forcing of commonly used passwords;
- Likely hold 0day exploits for some web applications;
- SQLmap;
- Fuhosin;
- **Chippy1337**


Uname: Linux barmen2 3.4.91-ih #1 SMP Sun May 18 15:37:26 CEST 2014 x86_64
User: uid=81(apache) gid=81(apache) groups=81(apache)
Time: 2014- Server IP: Client IP:
Cwd: /var/www/ drwxr-xr-x [home]
Currently logged in:
[Files] [Console] [Python] [Network] [SQL]
Network tools
Bind port to /bin/sh
Port: 2048 >>
Back-connect shell:
Server: Port: 443 >>
Chippy1337 enhanced back-connect shell (requires socat):
Server: Port: 443 >>
Change dir: >>
Make dir: >>
[Writeable]
Execute: >>
Read file: >>
Make file: >>
[Writeable]
Upload file:
Browse... No file selected. >>
[Writeable]

Attribution

We assess with **high confidence** that members of Lizard Squad are not in fact lizards who communicate with push ups.

Lizard Squad retweeted

UberFacts @UberFacts · Feb 10

Some lizards communicate through push ups.

Take aways

- Next week you should:
  - Evaluate your weakest links: domain registrars, server/service providers, lawyers, accountants etc.

- In the first three months following this presentation you should:
  - Evaluate threat actors that could target you or your sector: “Don’t judge a book by its cover”

Source materials

Email **rsaconference@intel471.com**
from your corporate email address