Instituto Politécnico
de Castelo Branco

DNS Firewall

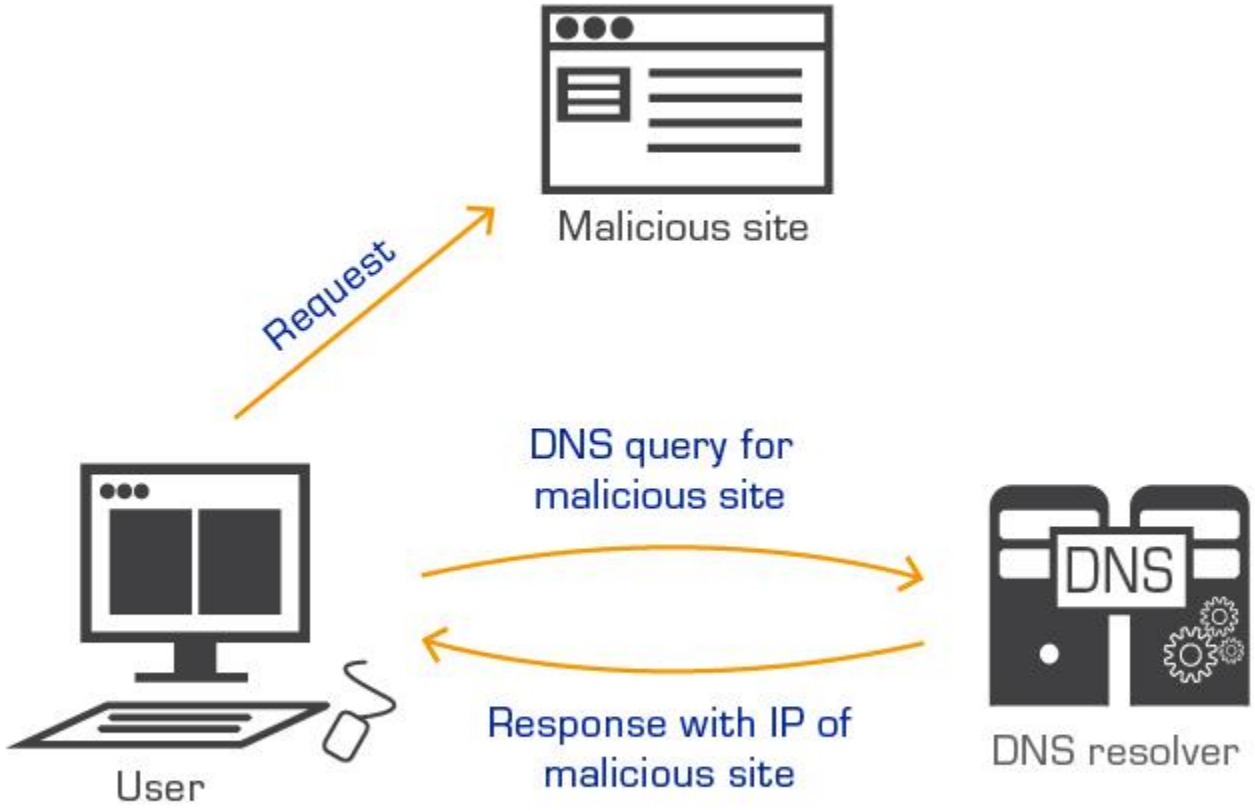
2ª Reunião da Rede Académica CSIRTs (RAC)|28.11.2017

Fernando Reis | Instituto Politécnico de Castelo Branco

O que é?

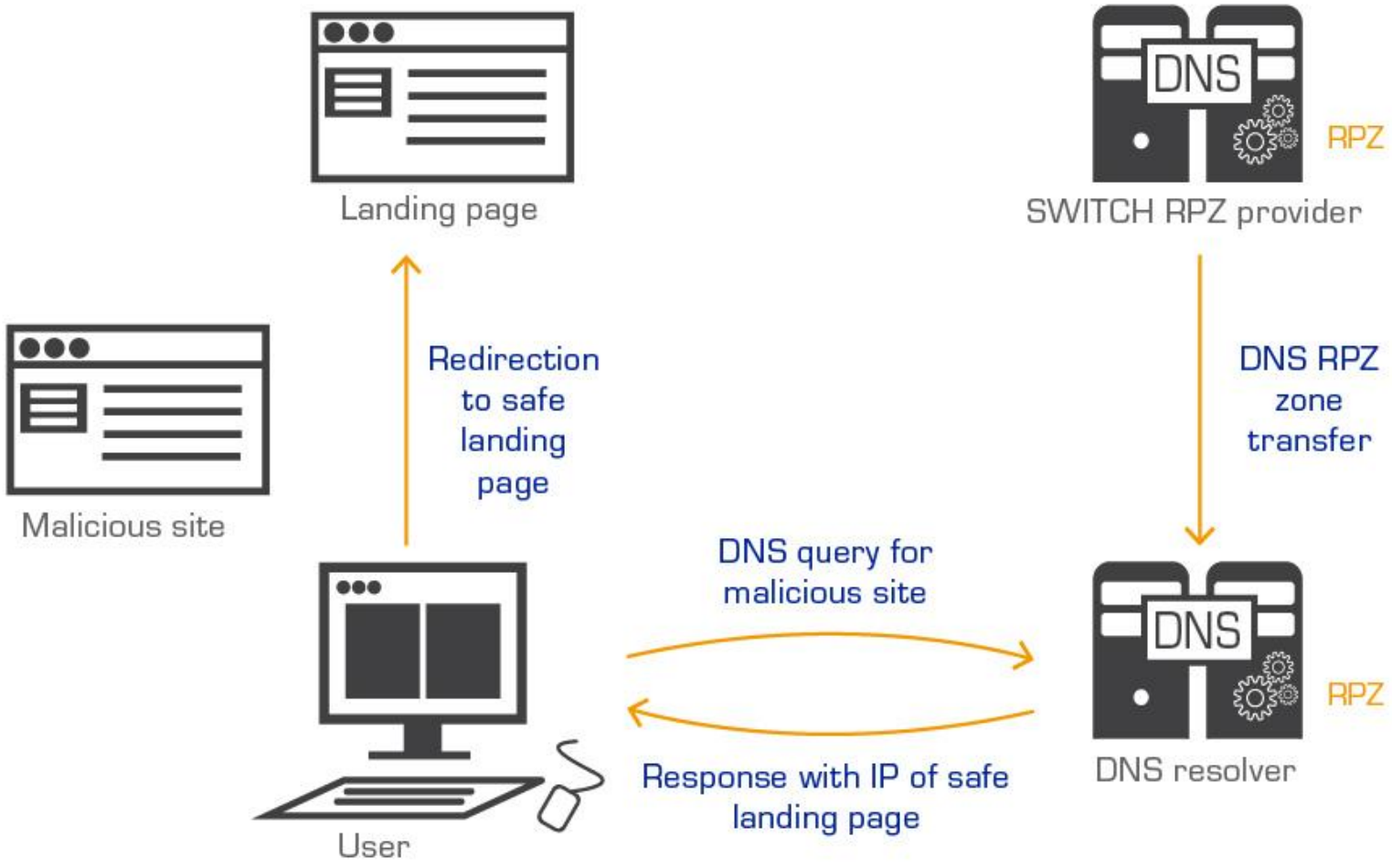
- Usar o DNS para proteger os utilizadores de ataques de malware, phishing e etc;
- Através de **D**omain **N**ame **S**ervice **R**esponse **P**olicy **Z**ones (DNS RPZ);
- Alterando as respostas do serviço de DNS global;
- Utilizando bases de dados de reputação existentes;
- Normalmente pagas…

DNS sem RPZ



Imagens: https://www.switch.ch/security/services/dns-firewall/

DNS com RPZ



Imagens: https://www.switch.ch/security/services/dns-firewall/

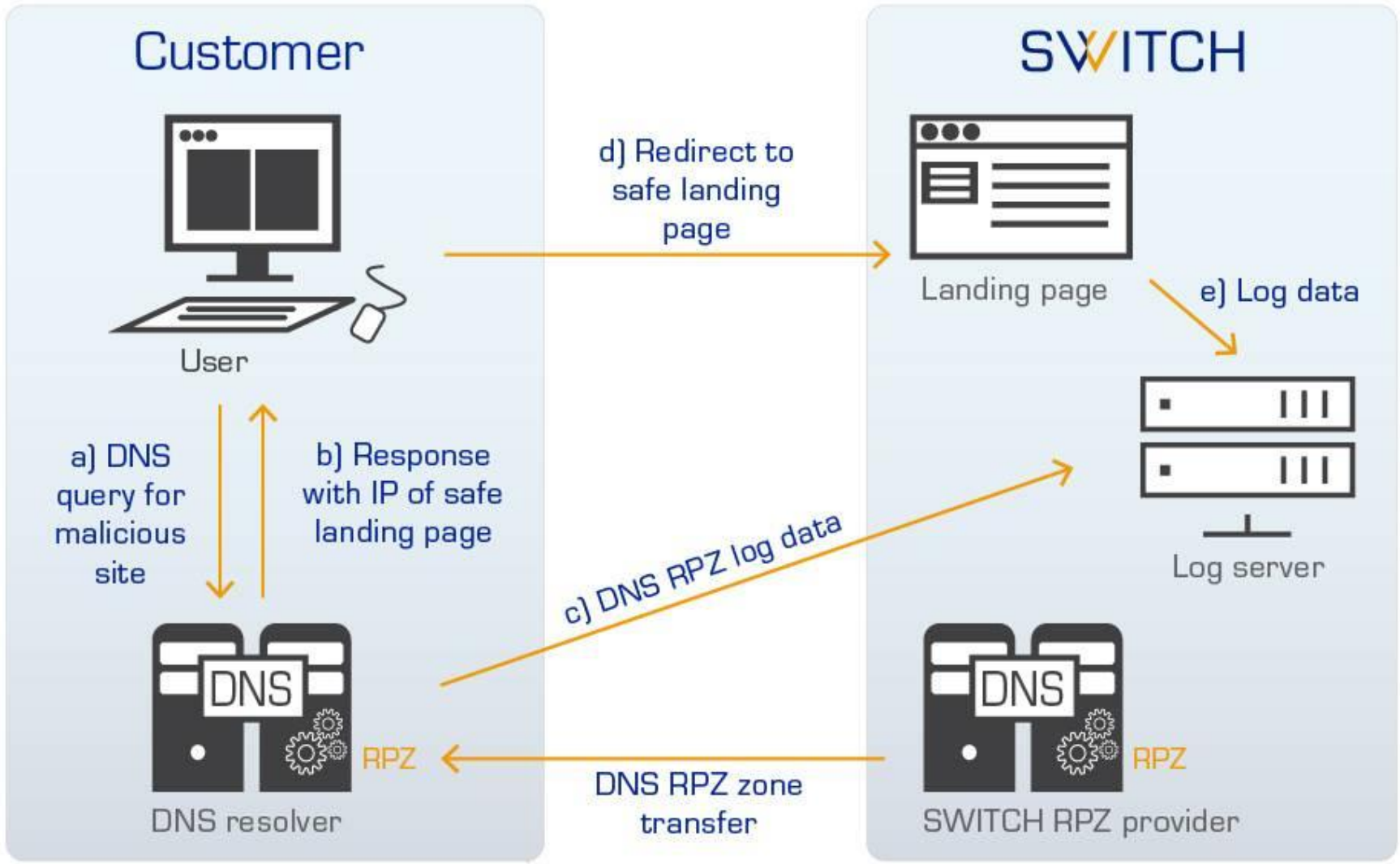
Reputation data providers

Provider	Service
DissectCyber	rpzone.us
FarsightSecurity	Newly Observed Domains and example
InfoBlox	DNS firewall
SpamHaus	Several of their popular blocklists are available via RPZ. Article Pricing
SURBL	Data Feed
SWITCH	SWITCH DNS Firewall
ThreatStop	DNS firewall and announcement

Fonte: https://dnsrpz.info/

Reputation data providers utilizados

SWITCH DNS Firewall baseada em DNS RPZ



Imagens: https://www.switch.ch/security/services/dns-firewall/

SWITCH

Warning: Malicious site

Warning

The website you've tried to visit is marked as malicious. This could be a Drive-by or other threats.

Your institution is using a filter and therefore the harmful requests are redirected to this landing page.

For further information and support, please contact the IT support of your institution. For general information about Drive-by and Internet Threats, consult the SWITCH Safer Internet website.

SWITCH has two roles in this process. Firstly, in providing information to the institutions about domains that are involved in malicious activities. Secondly, is providing this landingpage.

Reporting a false positive

If you think a request to a website is wrongfully restricted, please inform SWITCH-CERT. To do that, add the technical information which is shown below to a email, add a short description why the domain should not be on the list anymore and send it to cert@switch.ch

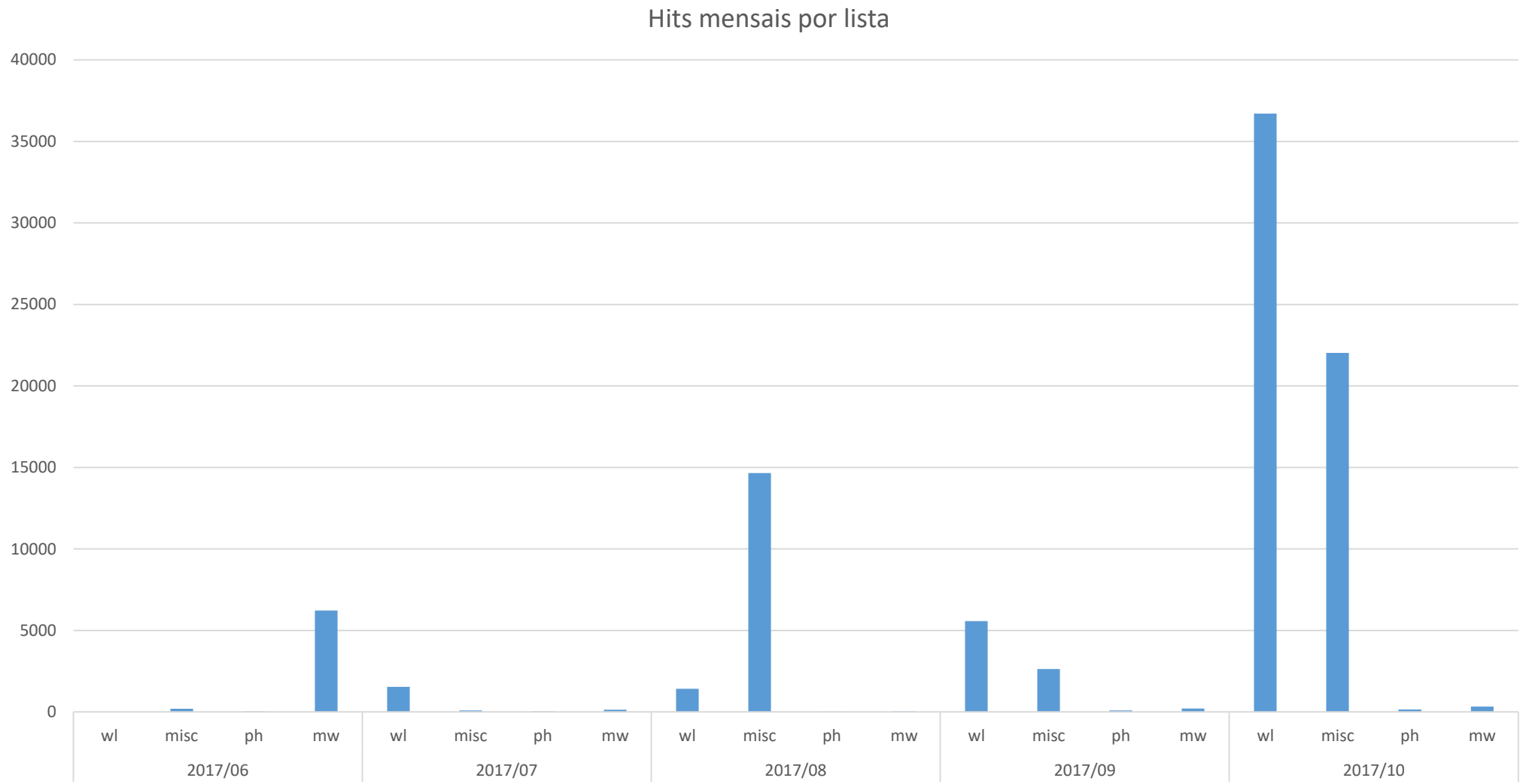
Client:	2001:690:2260:107:7477:1cf1:2617:46fd
Queried domain:	test.mw.rpz.switch.ch
Queried port:	80
URL:	test.mw.rpz.switch.ch/
Time of access(UTC):	2017-11-27 17:08:06.607
Landingpage:	SWITCH malware

Contact

For further information and support, please contact the IT support of your institution.

: informatica@ipcb.pt

Estatísticas



Ideias

- Implementar uma solução DNS-RPZ académica:
  - Instalar um servidor de DNS;
  - Criar as zonas;
  - Alimentar as zonas:
    - Criar uma página para que os administradores de cada instituição de ensino adicionem entradas;
    - Criar um procedimento de revogação/*timeout* das entradas;
    - Adquirir dados de *reputation data providers*:
      - SURBL;
      - SWITCH;
      - Etc.
  - Partilhar as zonas.

Fim...