CURRENT ISSUES OF MALICIOUS DOMAINS BLOCKING

Tuesday 9th April, 2019

Stanislav Špaček
Martin Laštovička, Martin Horák and Tomáš Plesník

CSIRT-MU

Introduction

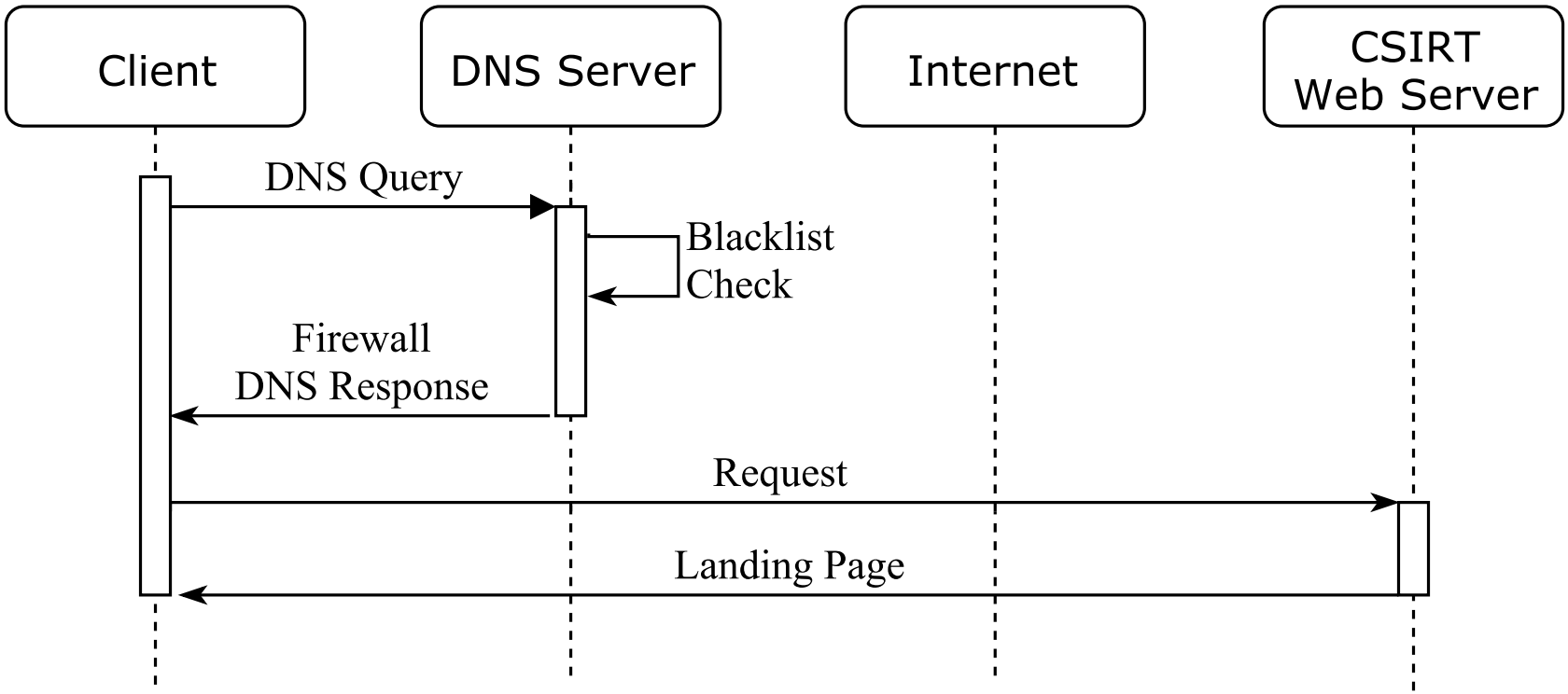
Malicious Domains

- Attackers may register their own domains
- May host phishing websites or distribute malware
- Using the DNS provides attackers with:
  - Trustworthy links
  - A way to avoid IP firewalls

DNS Firewall

- A "clever" resolver
- Checks its domain blacklist before forwarding DNS query

Basic DNS FW Model



CSIRT-MU

Technology

DNS Response Policy Zones

- The only open standard for DNS Fireall up-to-date
- Integrated into BIND and Windows Server 2016
- Provides only the resolver-side support

Proprietary Technologies

- Commercial application of the DNS Firewall, often as a service
- A lot of providers – Infoblox, FarsightSecurity, SpamHaus

CSIRT Requirements

1. Functions Integration
2. Logging
3. Blacklist Sharing
4. User Education

CSIRT-MU

CSIRT Requirements – Integration

1. Functions Integration

- Manage the DNS FW operation through a GUI
- Integrate the GUI along other cybersecurity tools

CSIRT Requirements – Logging

2. Logging

- User Data
  - Generated as the DNS queries hit the DNS FW blacklist
  - Analysis may point incident handlers to an infected device
- Management Data
  - Generated as incident handlers manage the DNS FW
  - Allows keeping track of blacklist history

CSIRT Requirements – Sharing

3. Blacklist Sharing

- Blocking a domain after or during an attack may be too late
- Sharing blacklists between CSIRTs and other institutions allows for proactive domain blocking

CSIRT-MU

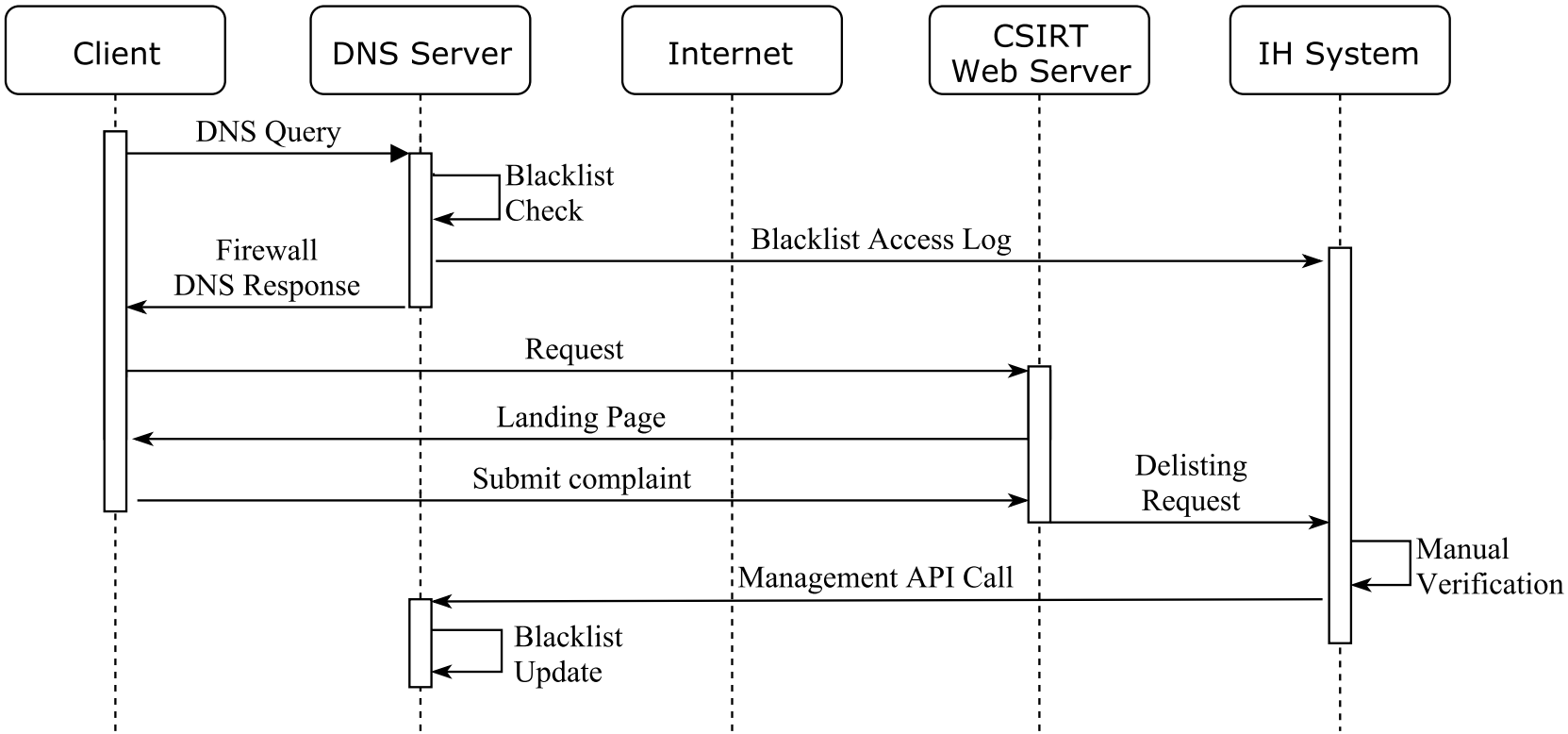
CSIRT Requirements – Education

4. User Education

- The DNS FW may redirect the connections instead of blocking them
- User is redirected on a safe landing page with the details about the incident
- It is a direct and immediate way to tell the user what just happened

CSIRT-MU

Advanced DNS FW Model



CSIRT-MU

Implementation

- Based on the DNS Response Policy Zones standard
- Contains other modules to meet the CSIRT requirements
  - Integration - GUI in the currently used incident handling software
  - Logging - database backend with a visualization plugin
  - Sharing - supported by the DNS RPZ itself
  - Education - landing page with a report form
- Several open issues prevent implementing the "ideal" model

Open Issues

- Transition to HTTPs
- Blacklist Sharing
- Few Open Implementations
- Easy to Bypass

Open Issues

Transition to HTTPs

- Certificate check of the browser makes redirection impossible
- Breaks the direct way to inform the user about the incident
- Users can be contacted outside of the DNS Firewall

CSIRT-MU

Open Issues

Blacklist Sharing

- Issue with the blacklist trustworthiness
- Blacklisting a harmless domain may cause severe disruption of institution's services
- A serious issue if the feedback from users is not possible

Open Issues

Few Open Implementations

- The DNS Response Policy Zones is the only open standard
- Every institution has to develop its own service backend

CSIRT-MU

Open Issues

Easy to Bypass

- The DNS resolver is easy to change in open network
- More significant issue if the firewall is used to enforce a policy
- In some cases may be mitigated by exerting more control over the network

Current Results

- DNS Firewall is active on a campus network with around **43 000 devices**
- The blacklist contains **135 domains** manually added and known to be malicious
- Since November 2018, **10 230 incidents** were detected, originating from **507 unique devices**

CSIRT-MU

Summary

- Our testing shows that DNS firewall is a concept that covers another possible hole in the security of a private network
- There exists at least one open source technology for DNS FW implementation - DNS RPZ
- The technology allows implementing the DNS FW itself, but cannot satisfy all the CSIRT requirements yet
  - Integration
  - Logging
  - Sharing
  - Education

THANK YOU FOR YOUR ATTENTION

csirt.muni.cz

@csirtmu

Stanislav Špaček

spaceks@ics.muni.cz