Analysis of DNS in cybersecurity

Patrik Hudák *Advisor: Mgr. Vít Bukač, Ph.D.*

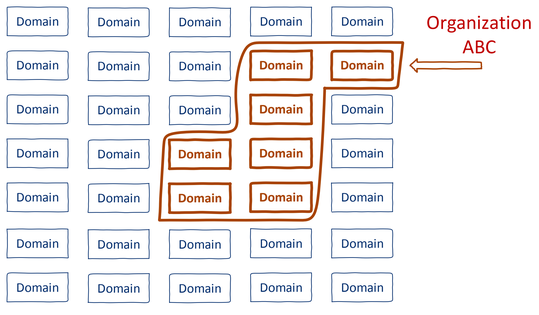
Faculty of Informatics, Masaryk University

Motivation

With companies slowly moving their infrastructures to the cloud, DNS is becoming more and more critical in the cybersecurity context. Although there are many types of research around DNS in cybersecurity, some of the modern methods and techniques are described only in informal blogs and articles on the Internet. This thesis provides in-depth technical details, practical techniques, and its results on two primary topics related to DNS and cybersecurity: **Domain Correlation** and **Subdomain Takeovers**.

Domain Correlation

The goal of domain correlation is to find all domains that are related to some organization. If we look at Internet domains as a big pool of independent domains, domain correlation aims to find (or cluster) those domains, which are owned by the same organization:

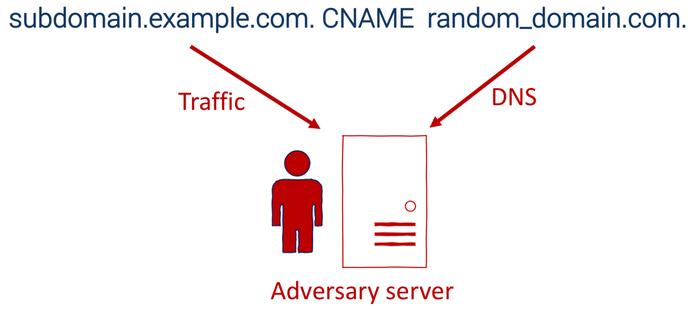


This process is mainly used in penetration testing, network audits, and bug bounty hunting. Its primary purpose is to find out, what domains are visible from the Internet. Our research showed that companies are often unaware of many domains they are exposing to the Internet. Some of these domains host unpatched applications which are commonly used as initial attack vectors for cyber adversaries.

Subdomain Takeovers

Put simply; subdomain takeover is a process of taking control over other, **legitimate** (sub)domain. When the domain has CNAME record set in its DNS zone, a cyber adversary can, under some circumstances have full control over the legitimate website.

This issue is becoming more and more prevalent with cloud providers (such as AWS or Heroku) requesting its customers to set CNAME records for proper functionality.



The biggest problem is, that subdomain takeover is **transparent to a web browser**. A web browser considers values returned from its DNS resolver as *trustworthy*. In case of subdomain takeover, this value is not legitimate, and potential cyber adversary has thus control over the content on the domain. Implications of successful subdomain takeover can be pretty severe:

- Phishing/Spear phishing attacks
- Cross-site scripting
- Brand damage
- Malware distribution
- ... *and much more!*

Contribution & Results

Domain Correlation

- Documentation of domain correlation process and techniques
- **New approach** into doing domain correlation using public DNS dataset (*nameserver clustering*)
- Scripts for domain correlation using public DNS dataset
- Benchmark: open source tools vs. our newly published approach

Subdomain Takeovers

- One of the first in-depth researches in this area
- Awareness to cybersecurity community and cloud providers about these issues
- Creation of automation tool which is able to scan 23 different cloud providers

The automation tool was used for an *Internet-wide scan* that revealed thousands of subdomain takeover possibilities. These results led to:

- Reports to **major organizations** (e.g., *NASA* or *IEEE*) describing the problem with their subdomain and providing actionable mitigation strategy.
- Reports to public **bug bounty programs** (e.g., *Microsoft* or *Starbucks*) that resulted into monetary compensation and appearance in *"Hall of Fame"*.