	DOMAIN NAMING SYSTEM (DNS) HIJACKING NOTICE

1.0. Introduction

Tanzania Computer Emergency Team (TZ-CERT) is informed of a large scale and global campaign involving DNS Infrastructure hijacking targeting domains belonging to Government, Internet Service Providers (ISPs), Telecommunications, Internet infrastructure and sensitive commercial entities.

This compromise is reported to affect numerous institutions across the Middle East and North Africa, Europe and North America.

2.0. Means of executing the attack

It has been reported that there are three techniques employed by *threat actors* to manipulate DNS records of the victim. The scenarios presented here use **"victim[.]com"** to stand in for the victim domain, and private Internet Protocol (IP) addresses to stand in for the actor controlled Internet Protocol (IP) addresses. Detailed descriptions of the scenarios are demonstrated below: -

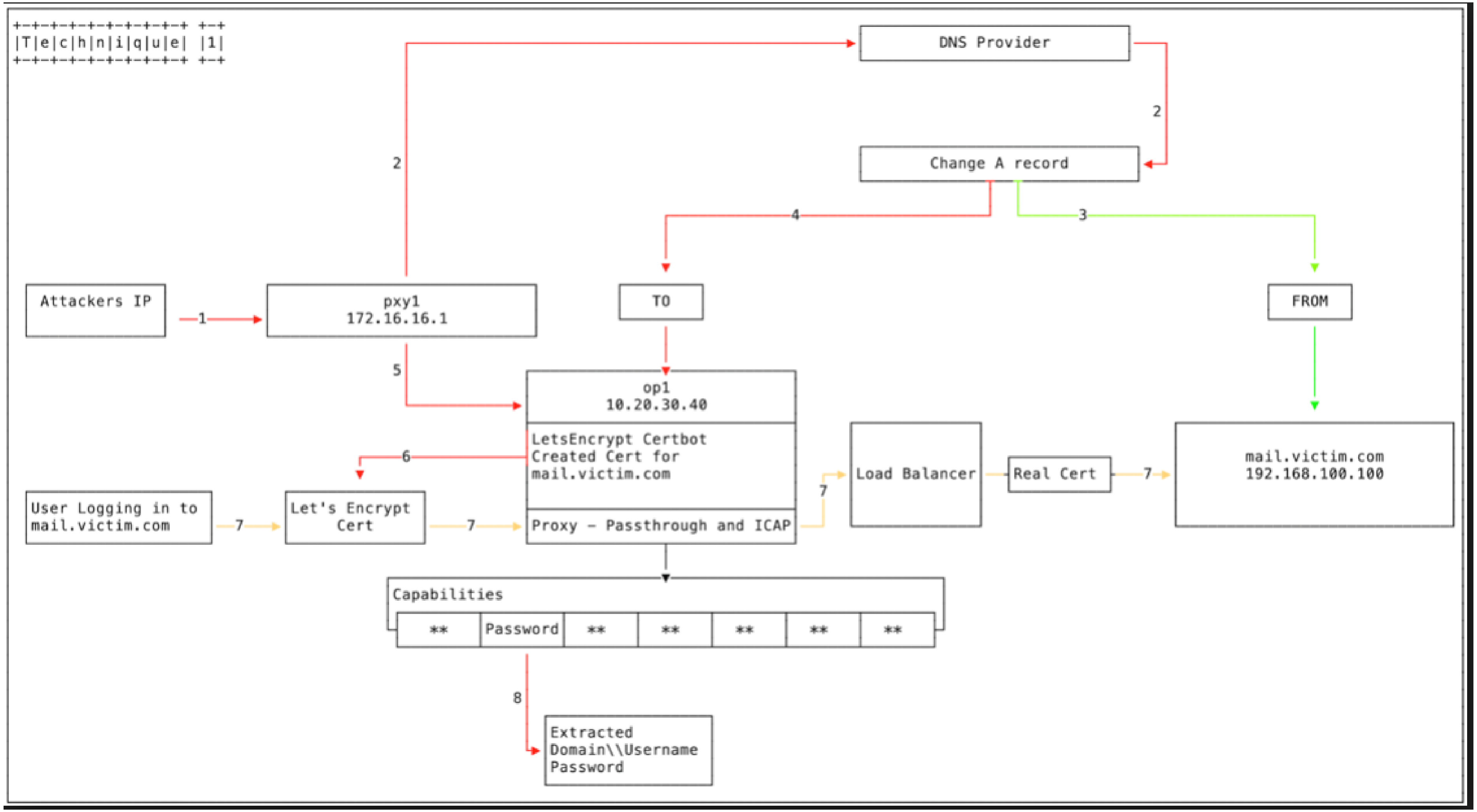
2.1. **Scenario 1:** Altering DNS "A" Records

In this scenario, the attackers attempt to alter the DNS "A" records that are used for mapping domain names to Internet Protocol (IP) addresses, so that traffic bound for one domain gets redirected through one controlled by the attackers as described in **Figure 1**.

2.1.1. Explanations

1. The attacker logs into **PXY1**, a Proxy box used to conduct non-attributed browsing as a jumpbox to other infrastructure;
2. The attacker logs into the DNS provider's administration panel, utilising previously compromised credentials;
3. The A record (e.g. **mail[.]victim[.]com**) is currently pointing to **192.168.100.100**;
4. The attacker changes the A record and points it to **10.20.30.40 (OP1)**;

Figure 1: Alteration of DNS “A” Records



5. The attacker logs in from **PXY1** to **OP1**;
   - A proxy is implemented to listen on all open ports, mirroring **mail[.]victim[.]com**; and
   - A load balancer points to **192.168.100.100 [mail[.]victim[.]com]** to pass through user traffic.
6. Certbot is used to create the Let’s encrypt certificate for **mail[.]victim[.]com**. It has been observed that multiple Domain Control Validation providers being utilised as part of this campaign.
7. A user now visits **mail[.]victim[.]com** and is directed to **OP1**. The Let’s Encrypt certificate allows the browsers to establish a connection without any certificate errors as Let's Encrypt Authority X3 is trusted. The connection is forwarded to the load balancer which establishes the connection with the real **mail[.]victim[.]com**. The user is not aware of any changes and may only notice a slight delay;
8. The username, password and domain credentials are harvested and stored.

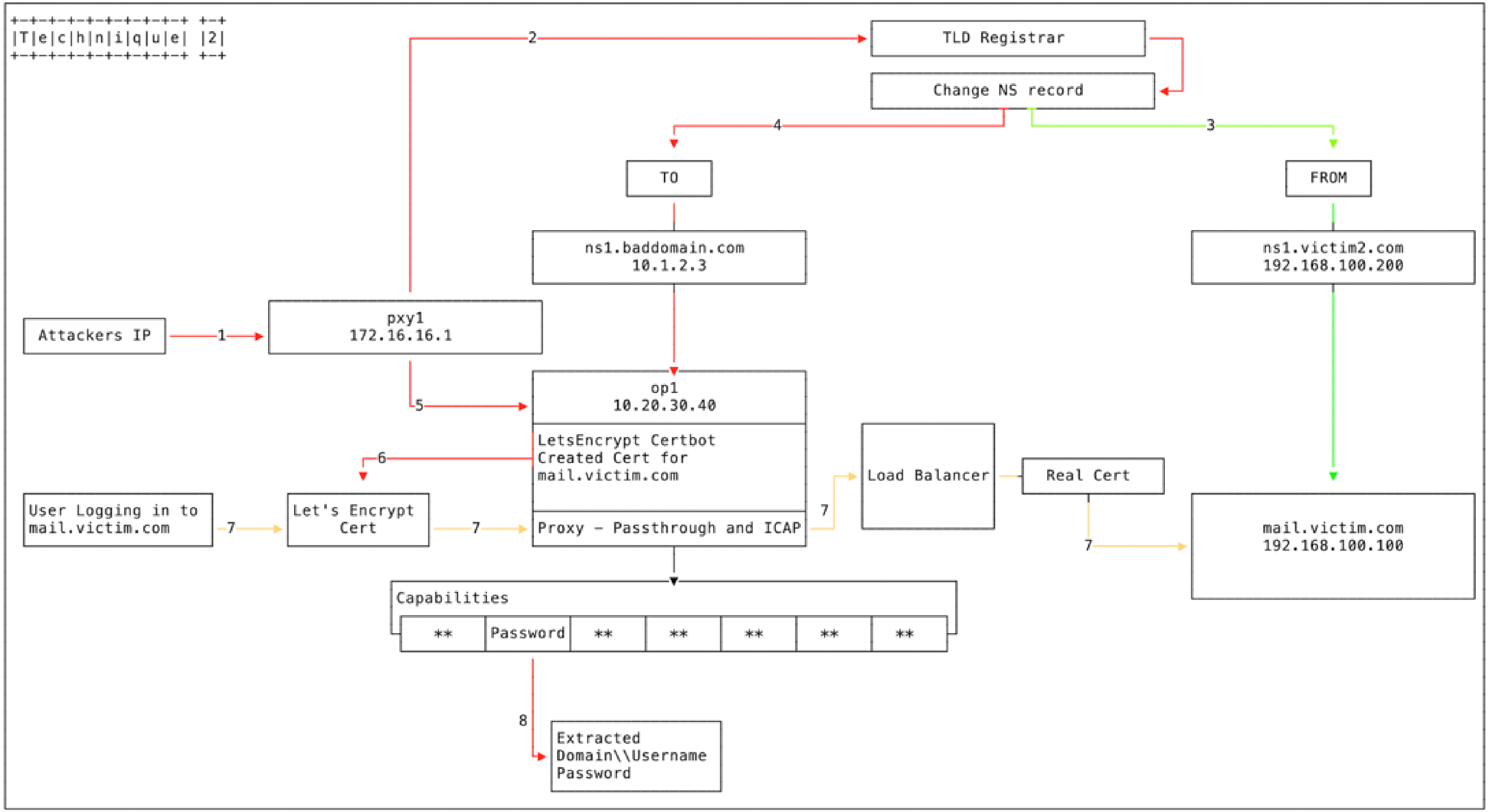
2.2. **Scenario 2:** Altering DNS “NS” Records

In second possible technique, attackers change DNS NS records via a TLD (domain name) provider account i.e. Altering DNS NS records and point a victim organization's nameserver record to an attacker-controlled domain as seen in **Figure 2**.

2.2.1. Explanations:

1. The attacker again logs into **PXY1**;
2. This time, however, the attacker exploits a previously compromised registrar or country code Top-level Domain (ccTLD);
3. The nameserver record **ns1[.]victim[.]com** is currently set to 192.168.100.200. The attacker changes the **NS record** and points it to **ns1[.]baddomain[.]com [10.1.2.3].** That nameserver will respond with the IP **10.20.30.40 (OP1)** when **mail[.]victim[.]com** is requested, but with the original **IP 192.168.100.100** if it is **www[.]victim[.]com;**
4. The attacker logs in from **PXY1** to **OP1**;
   - A proxy is implemented to listen on all open ports, mirroring **mail[.]victim[.]com**; and
   - A load balancer points to **192.168.100.100 [mail[.]victim[.]com]** to pass through user traffic.

Figure 2: Alteration of DNS “NS” Records



5. **Certbot** is used to create a Let’s Encrypt certificate for **mail[.]victim[.]com**. It has been observed that multiple Domain Control Validation providers being utilised during this campaign.
6. A user visits **mail[.]victim[.]com** and is directed to **OP1**. The Let’s Encrypt certificate allows browsers to establish a connection without any certificate errors as Let's Encrypt Authority X3 is trusted. The connection is forwarded to the load balancer which establishes the connection with the real **mail[.]victim[.]com.** The user is not aware of any changes and may only notice a slight delay.
7. The username, password and domain credentials are harvested and stored.

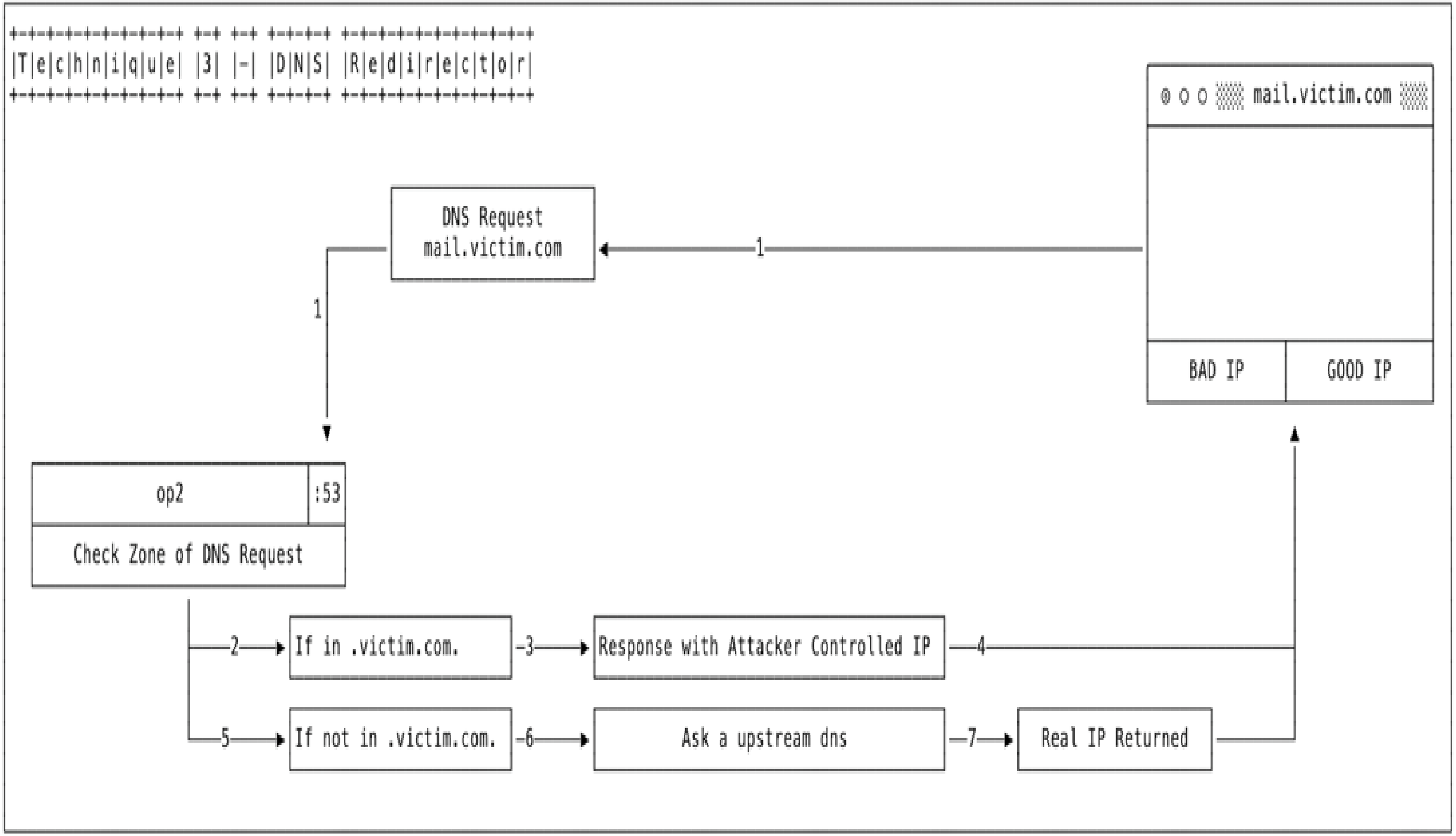
2.3. **Scenario 3:** A DNS Redirector

The attacker has also been observed using a third technique in conjunction with either Figure 1 or Figure 2. This involves a DNS Redirector, that is designed to respond with an attacker-controlled IP address to DNS requests for victim domains as described in **Figure 3**.

2.3.1. Explanations

1. A DNS request for **mail[.]victim[.]com** is sent to **OP2** (based on previously altered **A Record** or **NS Record**);
2. If the domain is part of **victim[.]com** zone, **OP2** responds with an attacker-controlled IP address, and the user is re-directed to the attacker-controlled infrastructure; and
3. If the domain is not part of the victim.com zone (e.g. **google[.]com**), **OP2** makes a **DNS request** to a legitimate DNS to get the IP address and the legitimate IP address is returned to user.

Figure 3: DNS Redirect



3.0. Root Cause

Until now the root of the attack is not yet established as the threat actors are exploiting multiple techniques to gain an initial foothold into each of the targets described in section 2.0 of this notice. However, it has been reported that the following attack vectors are being employed by actors to conducts DNS hijacking;

a) Phishing scams where the target site is replaced with an entirely different website that looks and acts like the original;

b) Data scraping sites that mimic banking or online shopping sites and try to get login details;

c) So-called "soft" hijacking where an Internet Service Provider (ISP) redirects traffic to gain adverts revenue. These can be innocent redirects in the case of mistyped URLs, or they can be malicious;

d) DNS spoofing by governments to censor data by blocking or redirecting DNS requests; and

e) Pharming efforts that replace common websites with sites covered in advertisements.

4.0. Mitigation Measures

Users and system administrators are urged to implement below control measures to mitigate the attack.

a) **Verify their DNS records** to ensure they're resolving as intended and not redirected elsewhere. This will help spot any active DNS hijacks;

b) **Update DNS account passwords** to disrupt access to accounts which an unauthorized actor might currently have;

c) **Add multi-factor authentication** to the accounts that manage DNS records. This will also disrupt access and harden accounts to prevent future attacks;

d) **Monitor Certificate Transparency logs** for certificates issued that the agency did not request. This will help defenders impersonation attempts or act of spying;

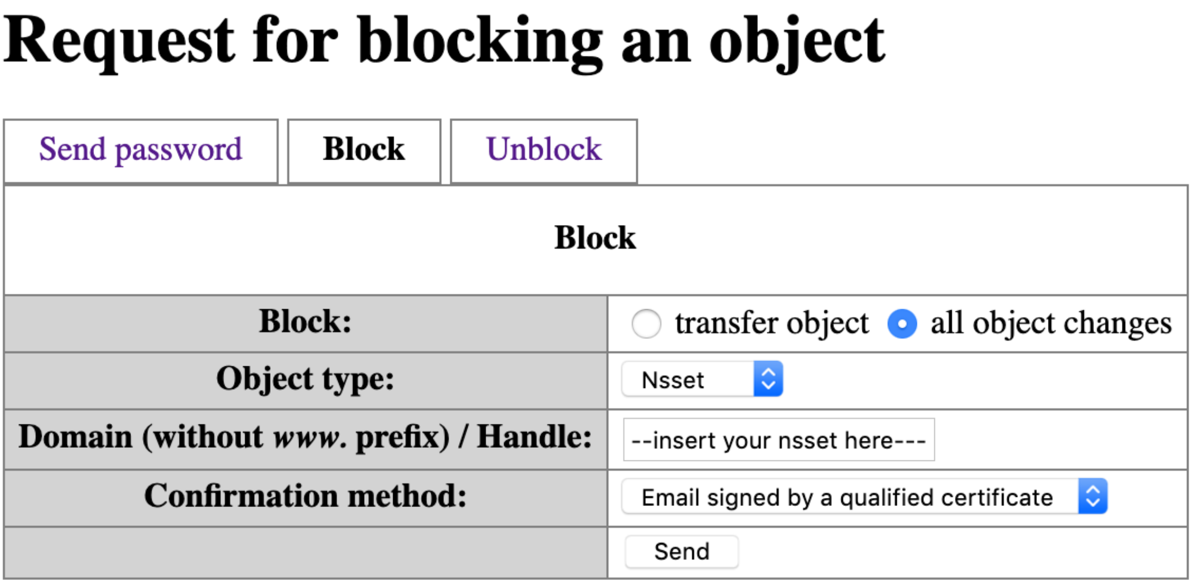
e) Ensure all system security patches are reviewed and applied;

f) Ensure that passwords are never stored or transmitted in clear text;

g) Ensure that DNS zone records are **DNSSEC signed** and DNS resolvers are performing DNSSEC validation; and

h) Ideally ensure email domain has a **Domain-based Message Authentication, Reporting and Conformance** (DMARC) policy with **Sender Policy Framework** (SPF) and/or **DomainKeys Identified Mail** (DKIM) and have measures to enforce policies provided by other domains on your email system.

i) Request domain lock services for your domain at the registry. Registry lock offers protection against EPP changes of objects in the registry. In this case NSSET for your nameservers is locked for changes. To lock your NSSET for .TZ domains access https://whois.tznic.or.tz/whois/block-object/ and enter your details as per sample below:-



Request for blocking an object

Block	
Block:	○ transfer object ● all object changes
Object type:	Nsset
Domain (without *www.* prefix) / Handle:	--insert your nsset here---
Confirmation method:	Email signed by a qualified certificate
	Send

NOTE: To obtain your NSSET, search from https://whois.tznic.or.tz/whois and copy your NSSET handle.

5.0. Reference:

a) https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

b) https://www.icann.org/news/announcement-2019-02-15-en

c) https://cyber.dhs.gov/blog/#why-cisa-issued-our-first-emergency-directive