Advanced Notification of Cyber Threats against DNS Hijacking Activity

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory	ADV-19-02	**Criticality**	High	
Advisory Released On	04 February 2019			

Impact

DNS hijacking intercepts, records and forwards network traffic of affected domains

Solution

Adhere the advices written under the recommendations section.

Affected Platforms

DNS

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT would like to follow up on the DNS Hijacking Activity. The attack is targeting countries in the region. DNS hijacking leverages three different methods to intercept, record and forward network traffic of affected domains. This permits capturing the contents of web traffic to access, harvest, and store sensitive information.

Threat Details

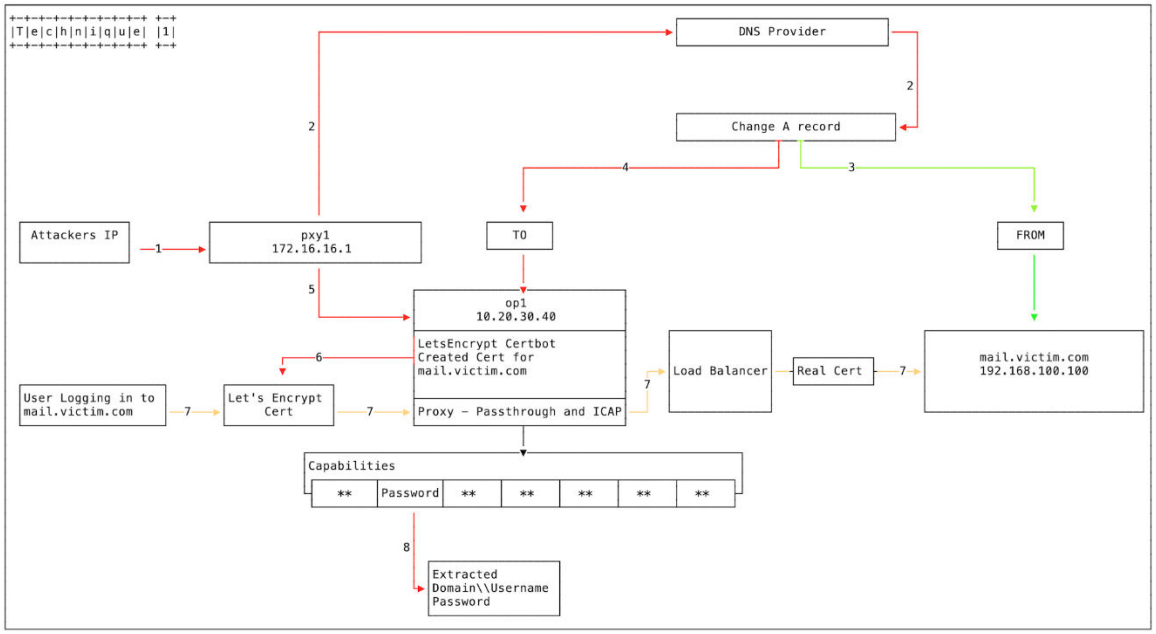
DNS hijacking is an attack targeting UAE and other countries in the region. It is leveraged through manipulating the DNS records for initial compromising of victims. DNS hijacking is the foothold that is later escalated to enable additional exploits which permits capturing the contents of the affected domains web traffic. Resulting in the attackers to access, harvest, and store sensitive information. While the objective of DNS hijacking is unclear, it enables intelligence collection operation towards the affected.

This is detailed further below, as capturing web traffic may enable:

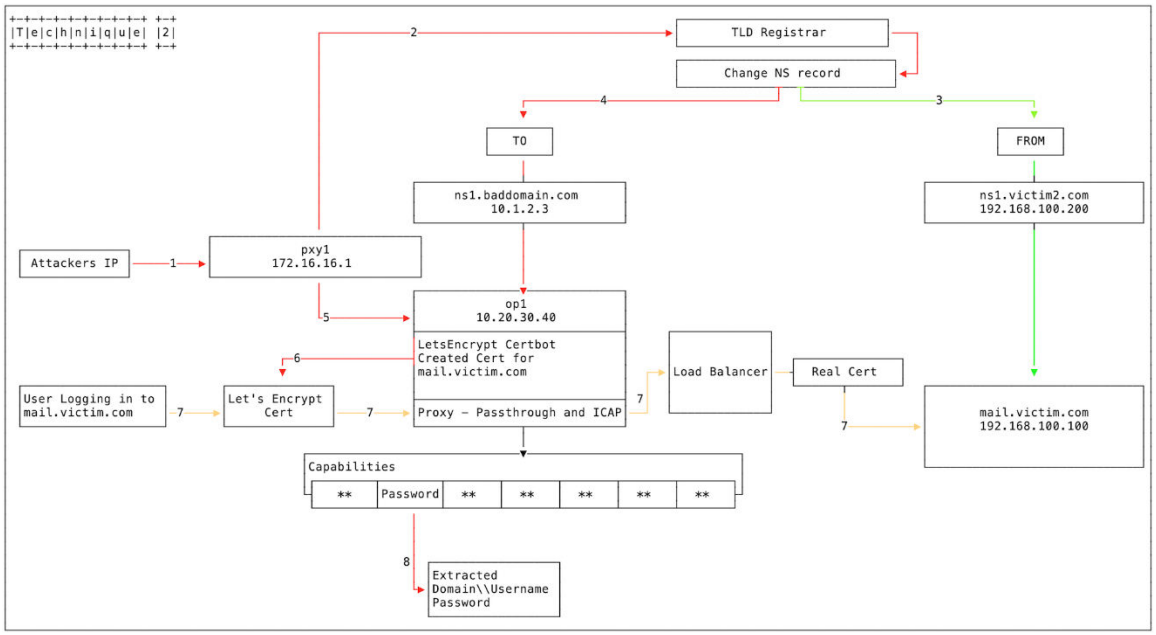
1. Direct data collection from web traffic of the affected domains
2. Collection of credentials from captured traffic to access the target's network
3. Distribution of malware to the target's infrastructure

Below are techniques used to initiate DNS hijacking

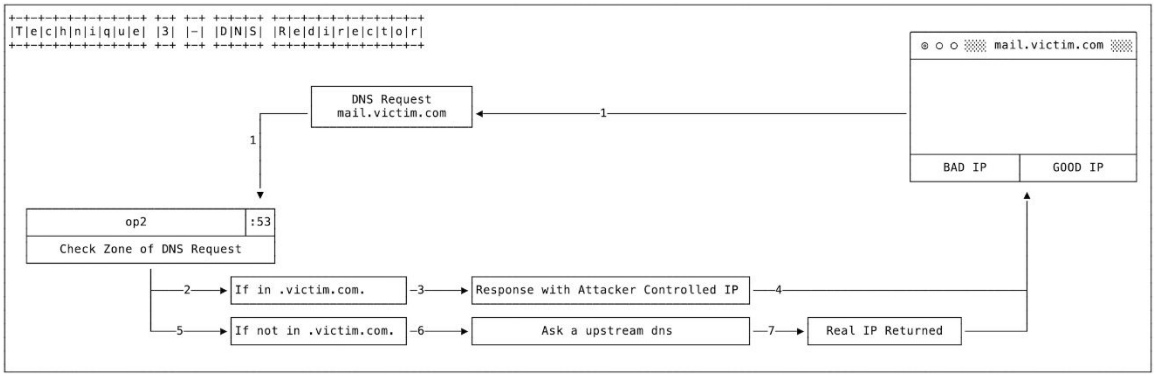
Technique 1 – DNS A Records



Technique 2 – DNS NS Records



Technique 3 – DNS Redirector



IOCs

Malicious IP Addresses

- 142.54.179.69
- 89.163.206.26
- 185.15.247.140
- 146.185.143.158
- 128.199.50.175
- 185.20.187.8
- 82.196.8.43
- 188.166.119.57
- 206.221.184.133
- 37.139.11.155
- 199.247.3.191
- 185.161.209.147
- 139.162.144.139
- 37.139.11.155
- 178.62.218.244
- 139.59.134.216
- 82.196.11.127
- 46.101.250.202

Recommendations

To harden the security against the attack, entities are recommended with the following:

1. Implement multi-factor authentication on domain's administration portal.
2. Internally investigate to assess if attackers gained access to the environment
3. Validate source IPs in OWA/Exchange logs.
4. Validate A and NS record changes.
5. Search for SSL certificates related to the domain and revoke malicious certificates.

References

FireEye

CrowdStrike

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae