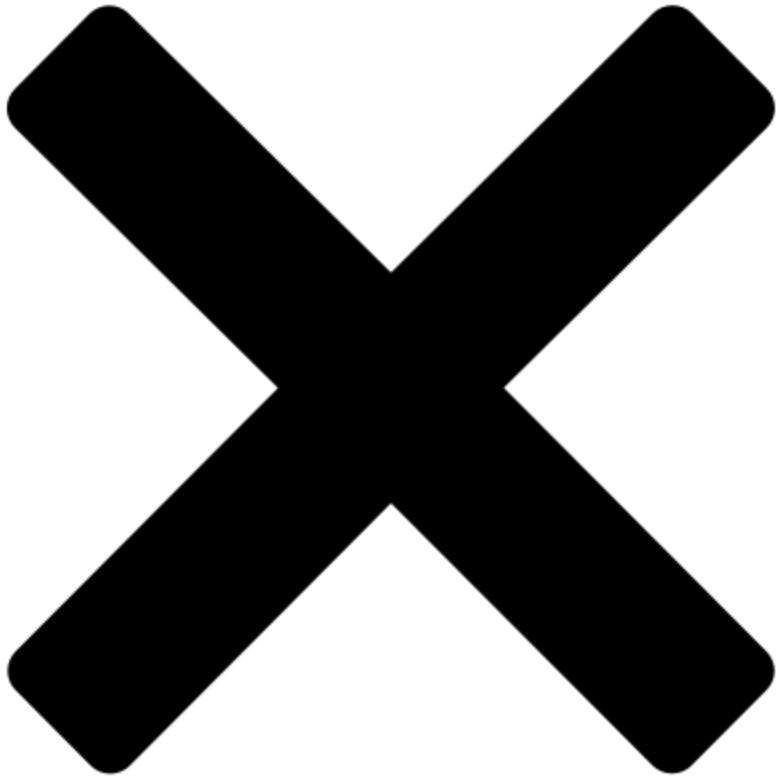
Global DNS Hijacking Campaign: DNS Record Manipulation at Scale

mandiant.com/resources/blog/global-dns-hijacking-campaign-dns-record-manipulation-at-scale



Threat Research

Muks Hirani, Sarah Jones, Ben Read

Jan 09, 2019

6 min read

| Last updated: Aug 23, 2022

Threat Research

Introduction

FireEye's Mandiant Incident Response and Intelligence teams have identified a wave of DNS hijacking that has affected dozens of domains belonging to government, telecommunications and internet infrastructure entities across the Middle East and North Africa, Europe and North America. While we do not currently link this activity to any tracked group, initial research suggests the actor or actors responsible have a nexus to Iran. This campaign has targeted victims across the globe on an almost unprecedented scale, with a high degree of success. We have been tracking this activity for several months, mapping and understanding the innovative tactics, techniques and procedures (TTPs) deployed by the attacker. We have also worked closely with victims, security organizations, and law enforcement agencies where possible to reduce the impact of the attacks and/or prevent further compromises.

While this campaign employs some traditional tactics, it is differentiated from other Iranian activity we have seen by leveraging DNS hijacking at scale. The attacker uses this technique for their initial foothold, which can then be exploited in a variety of ways. In this blog post, we detail the three different ways we have seen DNS records be manipulated to enable victim compromises. Technique 1, involving the creation of a Let's Encrypt certificate and changing the A record, was previously documented by Cisco's TALOS team. The activity described in their blog post is a subset of the activity we have observed.

Initial Research Suggests Iranian Sponsorship

Attribution analysis for this activity is ongoing. While the DNS record manipulations described in this post are noteworthy and sophisticated, they may not be exclusive to a single threat actor as the activity spans disparate timeframes, infrastructure, and service providers.

- Multiple clusters of this activity have been active from January 2017 to January 2019.
- There are multiple, nonoverlapping clusters of actor-controlled domains and IPs used in this activity.
- A wide range of providers were chosen for encryption certificates and VPS hosts.

Preliminary technical evidence allows us to assess with moderate confidence that this activity is conducted by persons based in Iran and that the activity aligns with Iranian government interests.

- FireEye Intelligence identified access from Iranian IPs to machines used to intercept, record and forward network traffic. While geolocation of an IP address is a weak indicator, these IP addresses were previously observed during the response to an intrusion attributed to Iranian cyber espionage actors.
- The entities targeted by this group include Middle Eastern governments whose confidential information would be of interest to the Iranian government and have relatively little financial value.

Details

The following examples use victim[.]com to stand in for the victim domain, and private IP addresses to stand in for the actor controlled IP addresses.

Technique 1 – DNS A Records

The first method exploited by the attacker is altering DNS A Records, as seen in Figure 1.

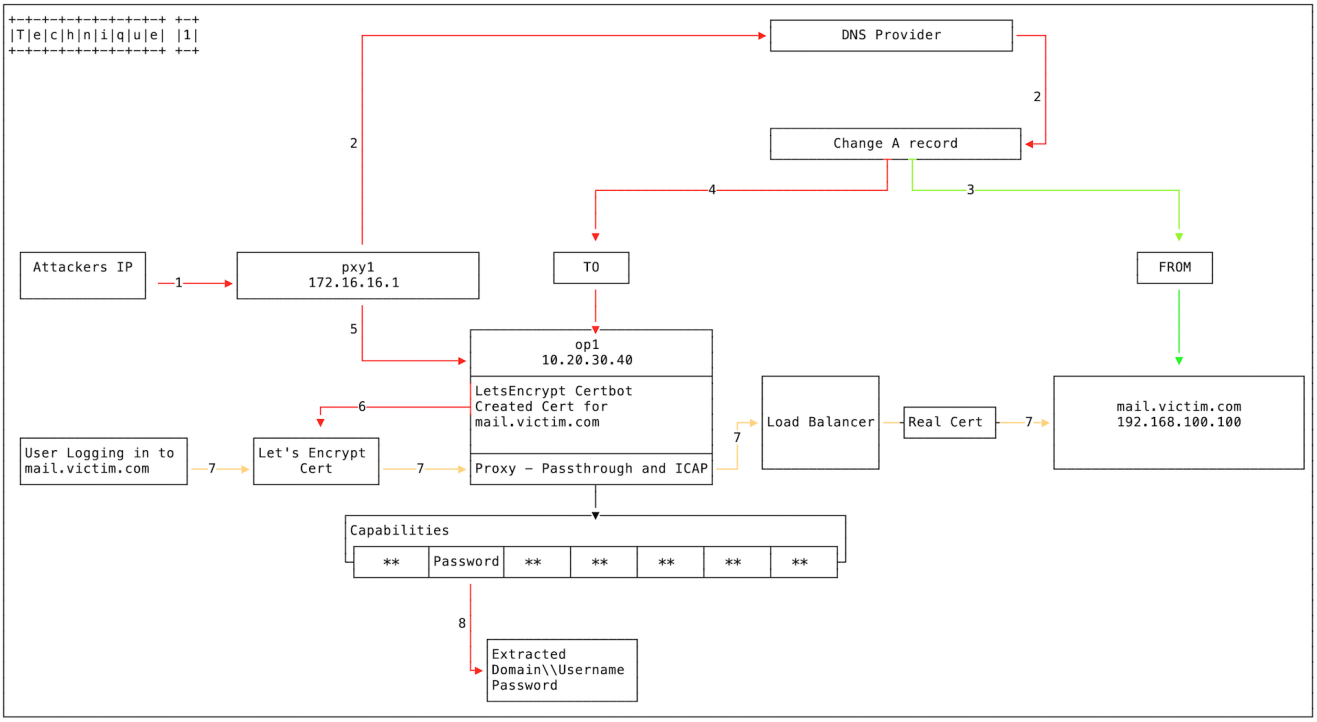


Figure 1: DNS A Record

1. The attacker logs into PXY1, a Proxy box used to conduct non-attributed browsing and 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).
5. The attacker logs in from PXY1 to OP1.
    - A proxy is implemented to listen on all open ports, mirroring mail[.]victim[.]com.
    - A load balancer points to 192.168.100.100 [mail[.]victim[.]com] to pass through user traffic.
6. certbot is used to create a Let's Encrypt certificate for mail[.]victim[.]com

    We have observed 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.

Technique 2 – DNS NS Records

The second method exploited by the attacker involved altering DNS NS Records, as seen in Figure 2.

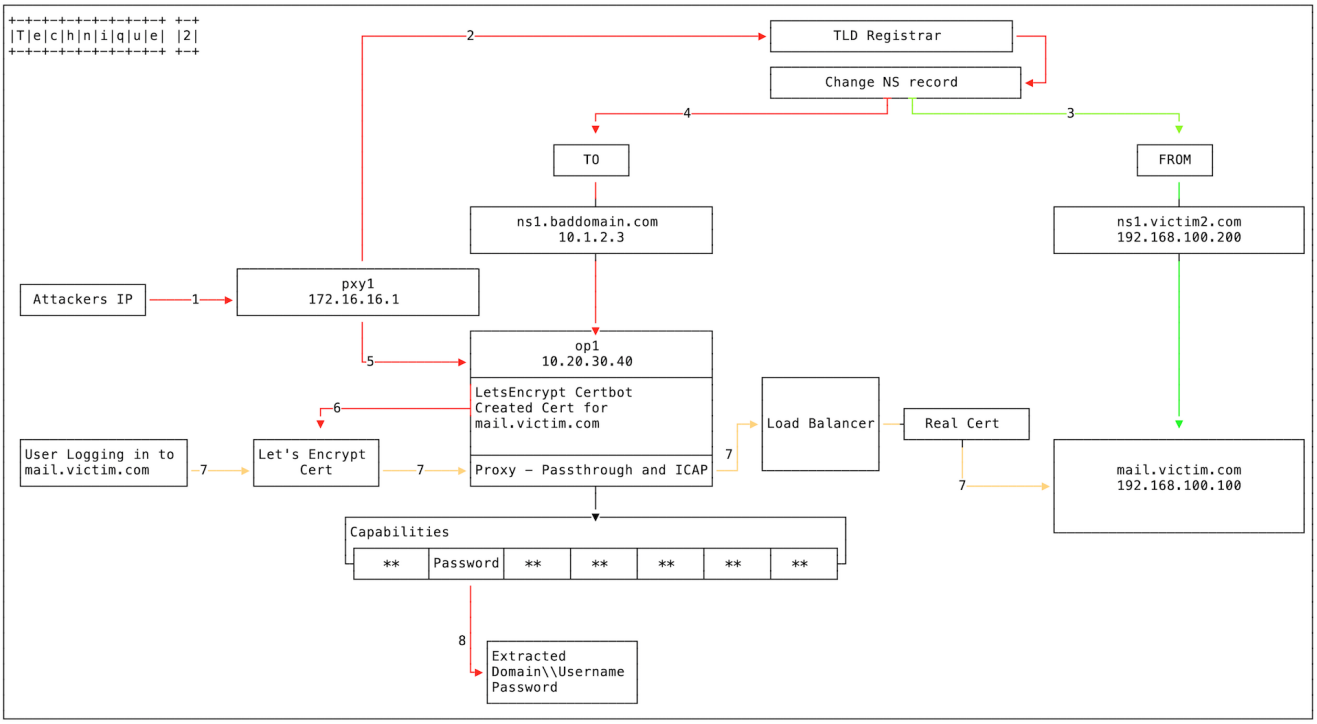


Figure 2: DNS NS Record

1. The attacker again logs into PXY1.
2. This time, however, the attacker exploits a previously compromised registrar or 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.
    - A load balancer points to 192.168.100.100 [mail[.]victim[.]com] to pass through user traffic.

5. certbot is used to create a Let's Encrypt certificate for mail[.]victim[.]com.
   We have observed 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.

Technique 3 – DNS Redirector

The attacker has also been observed using a third technique in conjunction with either Figure 1 or Figure 2 above. This involves a DNS Redirector, as seen in Figure 3.

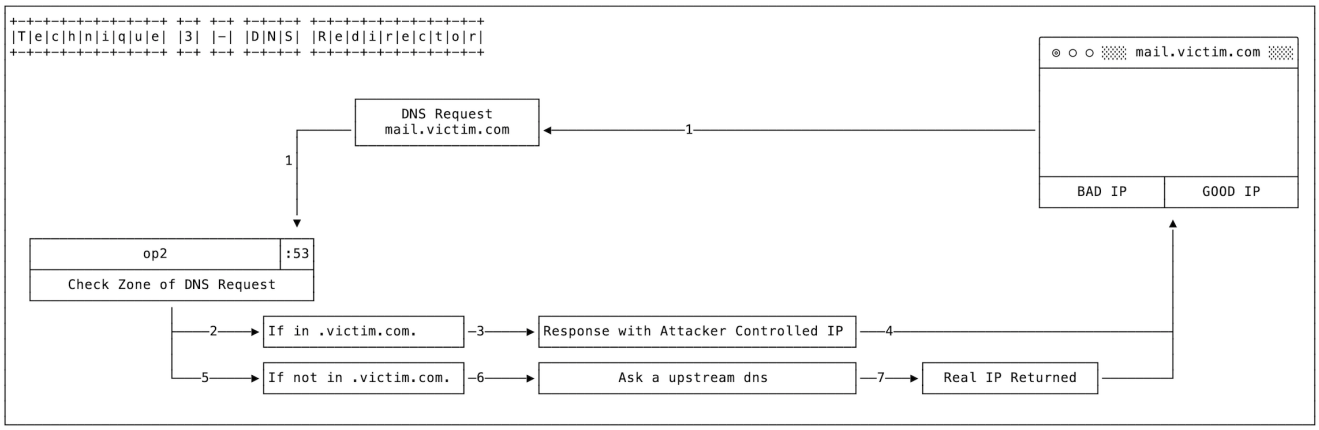


Figure 3: DNS Operational box

The DNS Redirector is an attacker operations box which responds to DNS requests.

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.
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 the user.

Targets

A large number of organizations have been affected by this pattern of DNS record manipulation and fraudulent SSL certificates. They include telecoms and ISP providers, internet infrastructure providers, government and sensitive commercial entities.

Root Cause Still Under Investigation

It is difficult to identify a single intrusion vector for each record change, and it is possible that the actor, or actors are using multiple techniques to gain an initial foothold into each of the targets described above. FireEye intelligence customers have received previous reports describing sophisticated phishing attacks used by one actor that also conducts DNS record manipulation. Additionally, while the precise mechanism by which the DNS records were changed is unknown, we believe that at least some records were changed by compromising a victim's domain registrar account.

Prevention Tactics

This type of attack is difficult to defend against, because valuable information can be stolen, even if an attacker is never able to get direct access to your organization's network. Some steps to harden your organization include:

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

Conclusion

This DNS hijacking, and the scale at which it has been exploited, showcases the continuing evolution in tactics from Iran-based actors. This is an overview of one set of TTPs that we recently observed affecting multiple entities. We are highlighting it now so that potential targets can take appropriate defensive action.

Have questions? Let's talk.

Mandiant experts are ready to answer your questions.

Contact Us