Recent DNS Hijacking attacks

Infrastructure attacks and general security issues

John Crain

LACTLD
Sept 2019

Background

There were a number of reports in early 2019 describing attacks against Internet Infrastructure.

Reports indicated that a number nameservers for TLDs were changed using compromised registrar credentials.

The attack were reported to have also target other infrastructure and to have been mainly focused on targets in the Middle East

How we were informed.

ICANN first became aware due to requests for emergency changes to nameservers for a CcTLD

ICANN's Chief SSR officer also received telephonic updates from one of the affected infrastructure providers.

As the events started to hit the press, ICANN's CTO and Chief SSR Officer were also introduced to the individual who discovered the attacks and informed more deeply of the situation.

What we know about the attacks

As always there was much speculation in the press etc.

However the techniques described in the fire eye report is a close representation of our understanding of the attacks.

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

This report is also reference by NetNod who were one of the affected parties.

https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod

Packet Clearing House (PCH) was another affected party.

https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Basics of attack

Attack against Mail by changing A records (Any other service is also feasible)

1. Compromise DNS registration (Registrar or user) credentials
2. Change A Records for MX server (Redirect to attackers server)
   (Do this for a short period of time to avoid detection)
3. Register a x509 Certificate for name (allows for HTTPs)
4. Set up proxy on attackers server to pass through connections
5. Harvest credentials

6. Once you have credentials you can read mail, gather intelligence for future attacks.

Not particularly sophisticated but effective and implementable with widely available tools

What we know about the attacks

Attack against Nameservers (Basically same attack with a new layer)

1. Compromise DNS registration (Registrar or user) credentials
2. Change NS Records for a TLD (Redirect to attackers nameserver server)
3. Attackers names server responds with attackers A record of attacker proxy machine.
4. Register a x509 Certificate for mail server
5. Set up proxy on attackers server to pass through connections
6. Harvest credentials

7. Once you have credentials you can read mail, gather intelligence for future attacks.

This potentially allows the attacker to target any name within a TLD.

What we know about the attacks

Attack against Nameservers and use a redirector

1. Compromise DNS registration (Registrar or user) credentials
2. Change NS Records for TLD (Redirect to attackers nameserver server)
3. Attackers names server responds with attackers A record of attacker proxy machine only for target machines
4. DNS queries for non targeted domain names are passed through to authentic TLD nameservers
5. Register a x509 Certificate for mail server
6. Set up proxy on attackers server to pass through connections
7. Harvest credentials

8. Once you have credentials you can read mail, gather intelligence for future attacks.

Because non victim related DNS queries are passed back to the original TLD nameservers there is little visible change in query volume.

What do we know about the attackers?

There is a lot of speculation about who was/is doing this.

Most of the attack mechanisms were not complex but were highly orchestrated and over long periods of time.

Timing of changes indicated that the attackers seemed to understand the inner workings of their victims.

Dare I use the word “professional”?

So whether this is nation state, organized crime or some other element there is an important message hear:

“Don’t underestimate the opponent”

Are there lessons we can learn?

Credential Management:

Many domain registrant accounts do NOT use multi-factor authentication.

Passwords are no longer enough. (And haven't been for some time)

DNSSEC:

Could help with detection of unauthorized changes. Certainly would have helped with the TLDs where there are manually checks on updates to DS records

It also only helps those that do DNS authentication.

(Can you turn on authentication on your resolvers?)

Are there lessons we can learn?

Other ways of securing DNS data changes:

Mechanisms, such as “Registry Lock”, that allow for tighter controls on changes to DNS data.

However they are not universally implemented, or even consistently implemented, and are only as strong as the processes behind them.

Do you provide this at your registry?

Basic Cyber Hygiene:

Some of the vectors used by these attackers include exploiting, unrelated, unpatched Software and used those systems as stepping stones.

We need to keep on top of our systems.

Are there lessons we can learn?

When operating infrastructure on the Internet we must remain vigilant!

Your data, or more importantly, your customers data is a prime target and has value you might not even realize.

“It’s not paranoia if they’re really out to get you!”

- Harold Finch, character in “Person of interest”