Recent DNS Hijacking Attacks

Overview, actions, and future options

John Crain

ThaiNOG
May 2019

ICANN

Background

There have been a number of recent reports describing attacks against Internet Infrastructure, e.g.:

- "A Deep Dive on the Recent Widespread DNS Hijacking Attacks"
- United States Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive 19-01: "Mitigate DNS Internet Tampering
- "Why CISA Issued our first Emergency Directive"
- "Global DNS Hijacking Campaign: DNS Record Manipulation at Scale"
- "Widespread DNS Hijacking Activity Targets Multiple Sectors"

Reports suggest nameservers for TLDs were changed, sometimes using compromised registrar credentials.

The attack was reported to have also targeted other infrastructure (IXPs, telephone companies, governments, etc.) and to have been mainly (not exclusively) focused on targets in the Middle East.

How we were informed

ICANN first became aware due to requests for Emergency Change Requests to nameservers for a ccTLD to IANA.

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 introduced to the individual who discovered and is investigating the attacks, who we refer to as "The Reporter" and informed of the situation.

Conversations remain ongoing.

Information Flood: Fact vs. Hearsay

In the midst of such events there is a lot information that arrives and it is important to distinguish what is know to be fact from what we have heard.

We heard from The Reporter that Twelve TLDs had potentially been affected.

- Confirmed: IANA received requests for changes from some ccTLDs who indicated that they were in response to the attacks. Other ccTLDs who we believe were affected (e.g., used the same infrastructure provider) made changes without such indication.

We heard from The Reporter that a large registrar that they had been compromised.

- Confirmed: in conversation with the registrar, they indicated the cause of compromise was found and that systems have since been secured.

We also asked RSSAC to confirm with the Root Server Operators that there was no indication of compromise of their root server related to the attacks.

- Eight root server operators responded.

What we know about the attacks – Methodology 1

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

1. Compromise DNS registration (Registrar or user) credentials
2. Register an X.509 Certificate for domain name (allows for HTTPS)
3. Set up proxy on attacker's server to pass through connections
4. Change A records for MX server (redirect to attacker's server)
5. Listen for email client login attempts and 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 – Methodology 2

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

1. Compromise DNS registration (Registrar or user) credentials
2. Register an X.509 Certificate for servers
3. Set up proxy on attackers server to pass through connections
4. Change NS Records for TLD (redirect to attacker's nameserver server)
5. Attacker's names server responds with A record of attacker's proxy machine.
6. Listen for any (proxied) login attempt and harvest credentials
7. Once you have credentials you can authenticate as the user and do pretty much anything.

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

What we know about the attacks – Methodology 3

Attack against Nameservers and use a redirector

1. Compromise DNS registration (Registrar or user) credentials
2. Register an X.509 Certificate for servers
3. Set up proxy on attacker's server to pass through connections
4. Change NS Records for TLD (redirect to attacker's nameserver server)
5. Attacker's name server responds with A record of attacker's proxy machine only for target machines. DNS queries for non-targeted domain names are passed through to authentic TLD nameservers.
6. Listen for any (proxied) login attempt and harvest credentials
7. Once you have credentials you can authenticate as the user and do pretty much anything.

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

ICANN Org’s Response

The response from ICANN was to initiate our Crisis Management Team:

Response can be broken into three main efforts:

1. Gain understanding of the ongoing situation

   Working with The Reporter and affected parties to understand the breadth of the the attacks.

2. Work with The Reporter and affected parties to take reparative action.

   This included name server changes for TLDs and working bring The Reporter and affected parties together for notification and remediation

3. Work to inform the community at large

   This comprised of a series of notification/publications related to the the attacked.

ICANN Announcements

“Alert Regarding Published Reports of Attacks on the Domain Name System”

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

Provided links to public reports of the attacks, a 12-point checklist to improve security, and pointers to 3 relevant SSAC advisories.

“ICANN Calls for Full DNSSEC Deployment, Promotes Community Collaboration to Protect the Internet”

https://www.icann.org/news/announcement-2019-02-22-en

Called “for full deployment of the Domain Name System Security Extensions (DNSSEC) across all unsecured domain names” and reaffirmed ICANN’s “commitment to engage in collaborative efforts to ensure the security, stability and resiliency of the Internet’s global identifier systems.”

ICANN's Role

DNS ecosystem is complex, with many participants, few wanting to spend money

There is a lack of understanding of the implications of the DNS hierarchy

- Compromise of a DNS node can impact **ALL** children, e.g., compromise of a TLD means **ALL** second level domains (and below) can be compromised.

ICANN Org tools are limited, despite Bylaw mandates on Security Stability and Resiliency

- Contractual obligations must be mutually agreed and only apply to contracted parties.
- DNSSEC solves a part of one problem, but has become a lightning rod.
- Some attack vectors are arguably not anywhere near our limited technical remit (e.g., "apply patches")

Not a new issue: SSAC has provided multiple advisories, going back to 2005:

- "SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle" (https://archive.icann.org/en/announcements/hijacking-report-12jul05.pdf)
- "Measures to Protect Domain Registration Services Against Exploitation or Misuse" (https://www.icann.org/en/system/files/files/sac-040-en.pdf)
- "A Registrant's Guide to Protecting Domain Name Registration Accounts" (https://www.icann.org/en/system/files/files/sac-044-en.pdf)
- "SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle" (https://www.icann.org/en/system/files/files/sac-074-en.pdf)

What do we know about the attackers?

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

Most of the attack mechanisms were not complex but were highly orchestrated and over a long period 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?

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”

Non-Prioritized Checklist

- ✓ Ensure all security patches have been reviewed and applied;
- ✓ Review log files for unauthorized access, especially administrator access;
- ✓ Review and limit internal controls over administrator (“root”) access;
- ✓ Enforce sufficient password complexity, especially length of password;
- ✓ Ensure that passwords are not shared with other users;
- ✓ Ensure that passwords are **never** stored or transmitted in clear text;
- ✓ Enforce regular and periodic password changes;
- ✓ Enforce a password lockout policy;
- ✓ Enable multi-factor authentication on all systems, especially for administrator access;
- ✓ Verify integrity of every DNS record, and the change history of those records;
- ✓ Ensure that DNS zone records are DNSSEC signed and your DNS resolvers are performing DNSSEC validation;
- ✓ Ensure your email domain has a DMARC policy with SPF and/or DKIM and that you enforce such policies provided by other domains on your email system.

Engage with ICANN

ICANN

Thank You and Questions

Visit us at **icann.org**
Email: john.crain@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann
- instagram.com/icannorg