Unintended Consequences
Obfuscated Attacks on TLDs

Eberhard W Lisse & Alejandra Reynoso

Namibian Network Information Center & Universidad del Valle de Guatemala

2017-06-26
NA-NIC.COM.NA

**Infrastructure Domain**

- 2017-06-03: Email Received
- 3 of 4 Name Servers lame
  - (free) Service Provider
- Possibility of Man in the Middle Attack
- DNSSEC not considered
- .NA was *not* compromised
.NA ccTLD Admin and Technical Contacts

- dns-admin@na-nic.com.NA
- dns-tech@na-nic.com.NA

IANA Root Zone Management

- Requests confirmation by email from AC and TC
- Access to RZM
  - Web Interface
  - Email Template
Theoretical Scenario
- Register with Service Provider
  - re-list na-nic.com.NA
  - different Master
  - propagation to the 3 Name Servers
  - 3 of 4 MX hosts under control
- Attempt modification of .NA
  - RZM (Email Template)

Would not Have Worked
- na-nic.com.NA is DNSSEC signed
- IANA validates DNSSEC

Credible Threat
Mitigation

What Did We Do?

- Fixed within minutes
  - removed lame delegations
  - added 2 new servers (with TSIG)
- Propagated within the hour
  - Register Portal
- Reviewed all Infrastructure Zones
  - ZoneMaster
  - Fixed all Warnings (no Errors found)
- Contacted IANA
  - moved Tech Contact email out of Bailiwick
  - dns-admin@na-nic.COM
Who is a TLD Manager?
What’s (in) a MNAME?

Show of Hands

- Who is a TLD Manager?
- Who knows what the MNAME is?
What’s (in) a MNAME?

Show of Hands

- Who is a TLD Manager?
- Who knows what the MNAME is?
- Who knows the requirements?
Who is a TLD Manager?

Who knows what the MNAME is?

Who knows the requirements?

- RFC 1035
- RFC 2181
- RFC 2136
What’s (in) a MNAME?

Show of Hands

- Who is a TLD Manager?
- Who knows what the MNAME is?
- Who knows the requirements?
  - RFC 1035
  - RFC 2181
  - RFC 2136
- Who has recently checked?
What’s (in) a MNAME?

SOA 1dom.TLD

@ IN SOA MNAME.1dom.TLD. E.1dom.TLD.(2017061101 ; serial YYYYMMDDnn 86400 ; refresh (24 hours) 7200 ; retry (2 hours) 360000 ; expire (1000 hours) 3600 ; neg result ttl (1 hour))

This is an example only...
@ IN SOA MNAME.1dom.TLD. E.1dom.TLD. 
(2017061101 86400 7200 360000 3600)

IN NS NS.2dom.TLD. ; Secondary

IN NS NS.3dom.TLD. ; Secondary

IN NS MNAME.1dom.TLD. ; MNAME = PRIMARY

MNAME IN A 127.0.0.1 ; Glue

This is an example only...
Possible MNAME Failures

And Possible Consequences

- MNAME does not have IP Address (glue)
  - Some DNS Traffic may get lost
- MNAME’s Domain Name does not exist
  - As above
  - Domain Name can be registered
  - Man-In-the-Middle Attack becomes possible
    - MNAME can get (false) IP Address
    - (Lost) DNS Traffic can be redirected
- DNSSEC will protect
  - If Resolvers validate
June 2016: Migration of .GT’s services

2017-01-31 Email received

MNAME didn’t resolve

MNAME’s domain not registered

Possibility of Active Directory Vulnerability

Dynamic Update

.GT was **not** compromised
A Short Diversion
Windows Active Directory and Dynamic Update

- AD Domain Services
  - Manages a number of services

- Dynamic Update
  - Takes care of changing IP Addresses
    - DHCP
  - Uses MNAME to find (internal) Primary
  - Updates A Record(s) on (internal) Primary

- Internal traffic should remain internal
(Subtle) Misconfigurations can cause Leaks
  - Name Collision

DNS queries reach External Name Servers

External MNAME is returned
  - DNS UPDATE can be captured/exploited
Mitigation
Within the Hour

- Issue was rectified immediately
- MNAME was changed
  - Within a registered domain
- MNAME does not resolve
  - To avoid receiving DNS UPDATE traffic
What Needs To be Done?

Prevention and/or Cure

- RTFM
  - Again and again...
- Diversify
  - Infrastructure
- Manual Review of all Infrastructure Zones
  - Inefficient
- Tool Supported Review
  - https://www.zonemaster.net
- We are unaware of fully automated tools
  - https://github.com/dotse/zonemaster
- DNSSEC
Thank you very much!