MitM Attack by Name Collision:

Cause Analysis and Vulnerability Assessment in the New gTLD Era

PI: Z. Morley Mao, University of Michigan (zmao@umich.edu)

Our work: Identified and systematically studied a newly-exposed MitM attack vector in the new gTLD era, called *WPAD name collision attack*.

- Uncovered the likely problem cause
- Proposed an attack surface definition to quantify the vulnerability status in the wild
  - *Illustrated real threat, provided a strong and urgent message to deploy proactive protection*
- Proposed remediation strategies at the DNS ecosystem level

Impact:

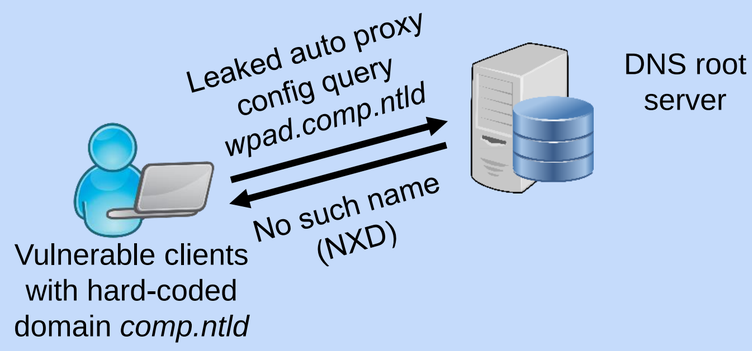
U.S. Department of Homeland Security: US-CERT alert (TA16-144A) based on our work to notify major enterprise & campus networks

New gTLD operators: Contacted us to get the highly vulnerable domain list

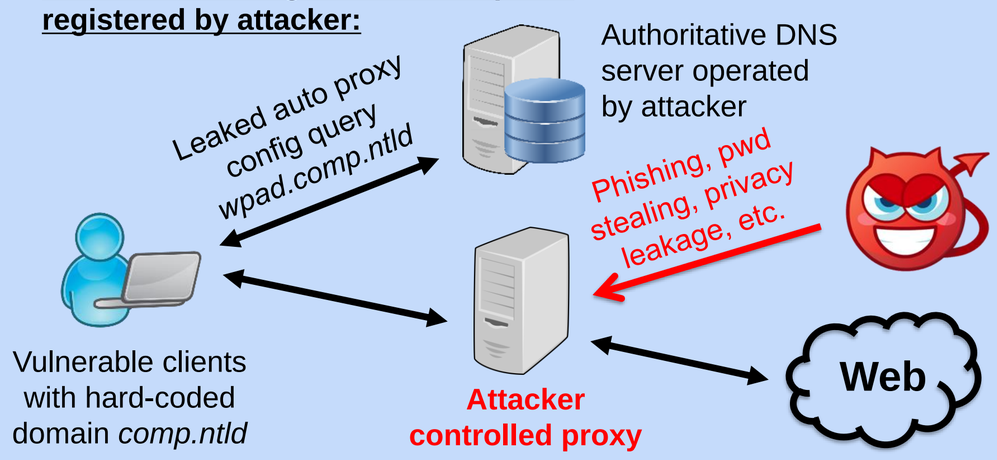
Domain name industry: Verisign published a white paper to guide remediation for enterprises based on our work

WPAD Name Collision Attack

- **Before the new gTLD era:**



- **After .ntld is delegated and comp.ntld registered by attacker:**



Systematic Problem Analysis

Vulnerability cause analysis

- Leakage traffic characterization
  - Leaked query source AS measurement
  - Leaked query domain suffix analysis
- Local testbed experiments
  - Concrete cause hypothesis test

Vulnerability status analysis

- Measurable attack surface definition
  - Highly-vulnerable domains (HVD): domains persistently exposing large numbers of victims
  - Quantification method development
- HVD registration status characterization

WPAD Query Leakage Characterization

- Dominate leak sources: Home network ASes
- Domain suffixes: Mostly corporate names
- **A very likely cause**: Individuals using corporate devices outside of the corporate internal networks, e.g., at home
  - Reproduced the problem in local testbed

Attack Surface Quantification

- HVD = high persistence + high volume
- Persistence: Leaked in every p-day period for at least n days
- Next, find high query volume domain
- **Evaluation**: Effective in finding HVDs in the victim ASes

Vulnerability Status Characterization

- HVD registration ratio: 7-13% overall
- Trend estimation: 60% TLDs' attack surface are likely to be fully registered in 2 years
  - Attack window is opening quickly
- ***Now is a good time for proactive mitigation!***

Remediation Strategies

- New gTLD registries: Scrutinize HVD registration
- Victim ASes: Drop leaked WPAD queries to the HVD domains
- End users: Turn off WPAD when not needed

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD