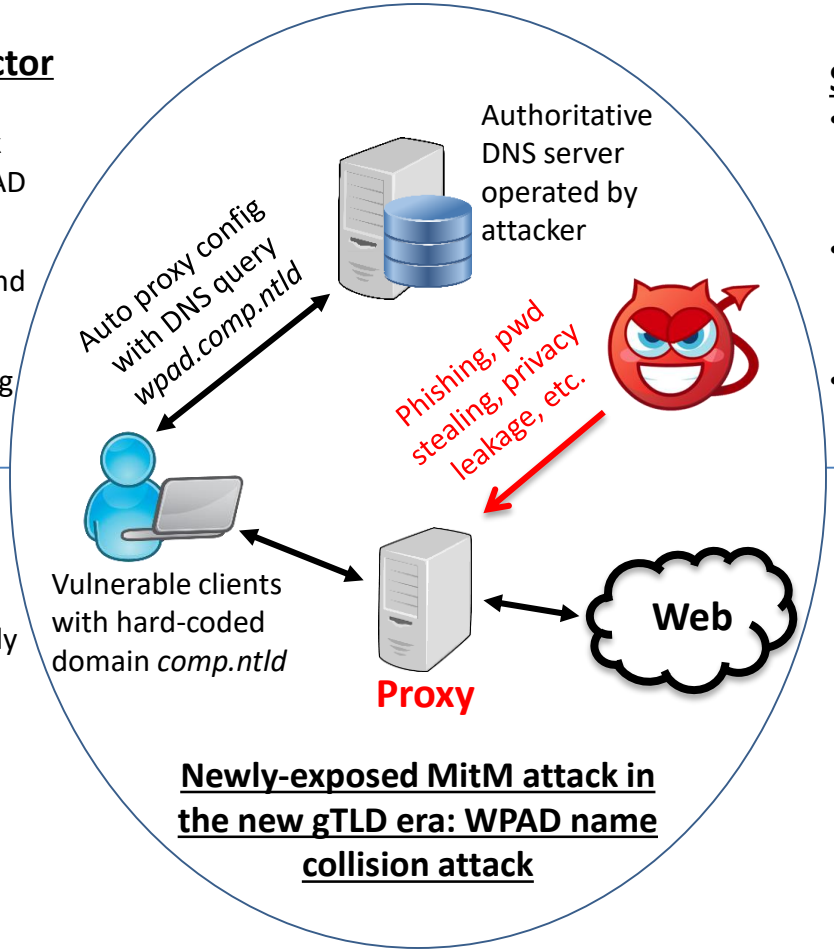
MitM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era

Newly-exposed Attack Vector in the New gTLD Era

- WPAD name collision attack
  - Name collision + WPAD query leakage
- Intercept user's web traffic with a vulnerable domain and a proxy server
- Security implications: sensitive data theft, phishing attacks, malicious code injection, etc.

Systematic Problem Analysis:

- Quantified the problem severity, uncovered the likely problem cause
- Defined attack surface, and quantified the vulnerability status in the wild
- Proposed defenses, and estimated the effectiveness and deployment challenges



Newly-exposed MitM attack in the new gTLD era: WPAD name collision attack

Scientific Impact:

- Systematically studied the newly-exposed WPAD name collision attack in the new gTLD era
- Illustrated real threat to Internet users in the wild, provided a strong and urgent message to deploy proactive protection
- Proposed remediation strategies at multiple parties in the DNS ecosystem level

Broader Impact:

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

Award #: CNS-1318306, CNS-1526455
Institution: University of Michigan
PI: Zhuoqing Mao