Sabancı Üniversitesi

Internet-wide Scanning and Notifications to Prevent Cybercrime

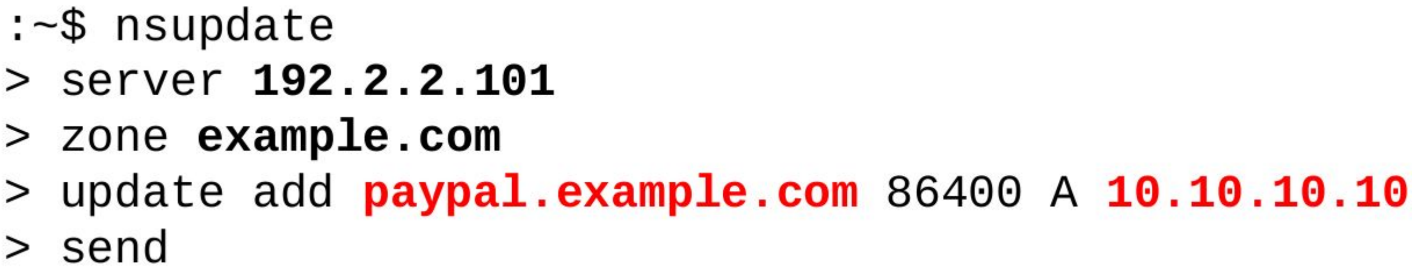
Orçun Çetin
Orcun.Cetin@sabanciuniv.edu

Internet-wide Scanning

- Scanning :
    - Vulnerabilities
        - DNS
    - Malicious behaviour or malware
        - Cryptojacking, hacked websites
    - Honeypots
        - Elastichoney 193.110.211.14 -> Genel Kurmay Baskanligi

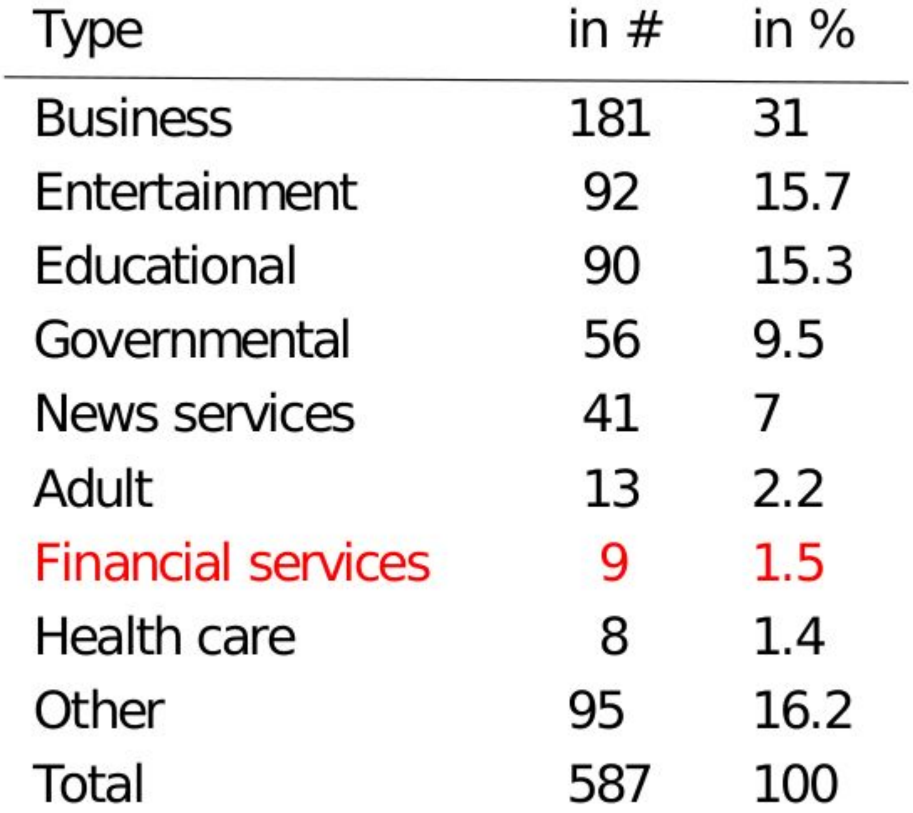
Zone Poisoning Vulnerability

- Cause: nameservers configured to allow non-secure dynamic updates.
- Anyone can manipulate DNS entries with single packet.
- Consequences: running **fake website/mail server** for phishing or espionage purposes.



```
:~$ nsupdate
> server 192.2.2.101
> zone example.com
> update add paypal.example.com 86400 A 10.10.10.10
> send
```

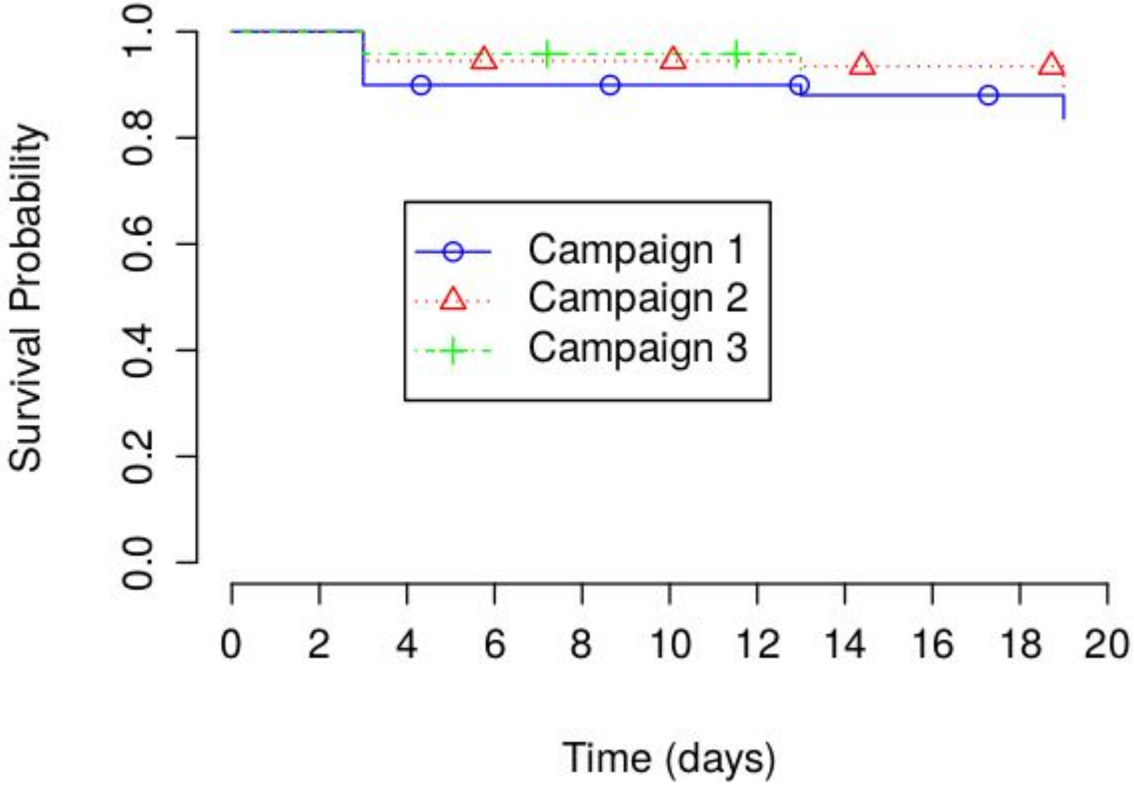
Zone Poisoning Vulnerability



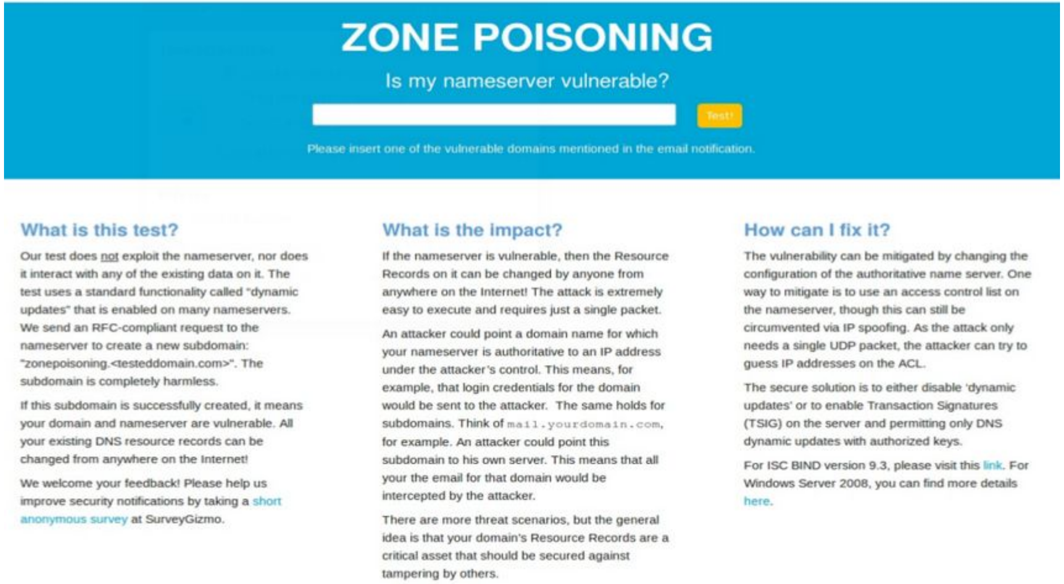
Type	in #	in %
Business	181	31
Entertainment	92	15.7
Educational	90	15.3
Governmental	56	9.5
News services	41	7
Adult	13	2.2
Financial services	9	1.5
Health care	8	1.4
Other	95	16.2
Total	587	100

Notifications

- All notified groups did better than the control group.
- Still, overall remediation rates were low.



Does it help to demonstrate the vulnerability?



ZONE POISONING

Is my nameserver vulnerable?

Please insert one of the vulnerable domains mentioned in the email notification.

What is this test?

Our test does not exploit the nameserver, nor does it interact with any of the existing data on it. The test uses a standard functionality called "dynamic updates" that is enabled on many nameservers. We send an RFC-compliant request to the nameserver to create a new subdomain: "zonepoisoning.<testeddomain.com>". The subdomain is completely harmless.

If this subdomain is successfully created, it means your domain and nameserver are vulnerable. All your existing DNS resource records can be changed from anywhere on the Internet!

We welcome your feedback! Please help us improve security notifications by taking a short anonymous survey at SurveyGizmo.

What is the impact?

If the nameserver is vulnerable, then the Resource Records on it can be changed by anyone from anywhere on the Internet! The attack is extremely easy to execute and requires just a single packet.

An attacker could point a domain name for which your nameserver is authoritative to an IP address under the attacker's control. This means, for example, that login credentials for the domain would be sent to the attacker. The same holds for subdomains. Think of `mail.yourdomain.com`, for example. An attacker could point this subdomain to his own server. This means that all your the email for that domain would be intercepted by the attacker.

There are more threat scenarios, but the general idea is that your domain's Resource Records are a critical asset that should be secured against tampering by others.

How can I fix it?

The vulnerability can be mitigated by changing the configuration of the authoritative name server. One way to mitigate is to use an access control list on the nameserver, though this can still be circumvented via IP spoofing. As the attack only needs a single UDP packet, the attacker can try to guess IP addresses on the ACL.

The secure solution is to either disable 'dynamic updates' or to enable Transaction Signatures (TSIG) on the server and permitting only DNS dynamic updates with authorized keys.

For ISC BIND version 9.3, please visit this link. For Windows Server 2008, you can find more details here.

- Short answer: no.

Thank you for listening!

- More info : Orcun.Cetin@sabanciuniv.edu
- More info on underlying study:
  - Cetin, O., Ganan, C., Korczynski, M., & van Eeten, M. (2017, June). Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning. In *Workshop on the Economy of Information Security*.