Team: Team 3

Inject Number: 52

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 16:14:17 -0500

From: Chief Information Security Officer

To: Infrastructure Team

Subject: [F-200] DNS Cache Poisoning Concerns and Remediation

Our IT Director read a recent security article about DNS Cache Poisoning that contained the following information:

The Domain Name Service underpins our use of the Internet, but it has been proven to be flawed and open to attack. If an attacker can poison the DNS (introduce invalid information) then the user (relying party) may unknowingly connect to the attacker's service, rather than the correct one. The user may then be exposed to confidentiality, integrity and availability issues.

My own research found three common mitigations:
1) The most basic defense against this attack is use of latest version of DNS. Latest DNS uses port randomization with transaction ID so it's hard for attacker to guess for the port. DNS based on BIND 9.5.0 or above perform these checks. Transaction ID is also cryptographically secure which reduce the probability of attack. But BIND version must be hidden within the query packets.

2) Remove unnecessary services running on the DNS servers. Attackers can use these unnecessary services to attack on DNS.

3) Recursive queries should be limited and DNS should only store information about the domain it has requested. It must be configured not to add additional domains information in a query response.

The Director is concerned that we are vulnerable to this attack. Evaluate our DNS and reply with a management memo as to our status in this regard and outline the steps you took to determine whether we are vulnerable. Describe the prioritized list of remediations (the three above as well as any others, minimum of two additional, that you recommend based off of industry best practice). If we are vulnerable, institute the protective measures immediately that can be implemented and show evidence of those changes. Finally, enable bind query logging if not already enabled and push it to Splunk. Show evidence of the logging to Splunk.

Thank you.

Chief Information Security Officer