SOCCRATES

SOCCRATES Webinar series:
1. AI-based Attack Detection

13th October 2020

LIVE DEMO: DNS NINJA

SOCCRATES

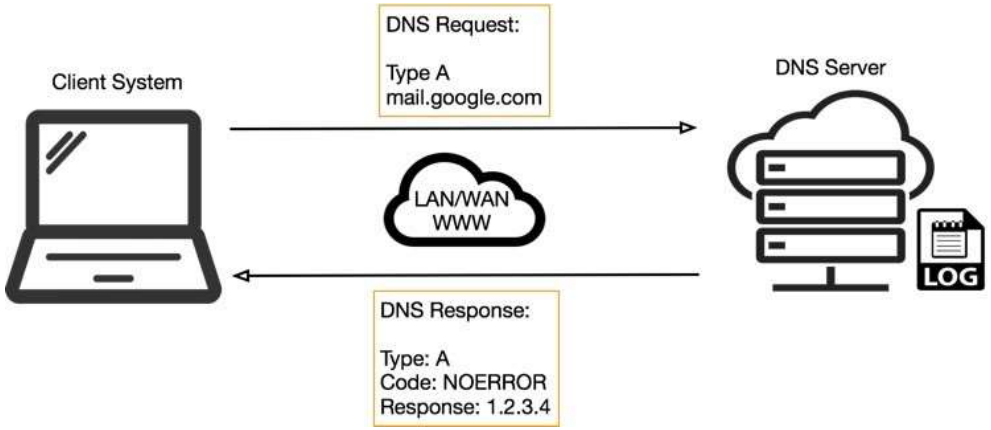
- We use DNS Ninja to find an exfiltration attack!

- Situation:
  - One of the computers in the network has been compromised by an attacker, whose goal is to extract sensitive information from the organization.
  - The data is exchanged through DNS protocol without any direct connection.

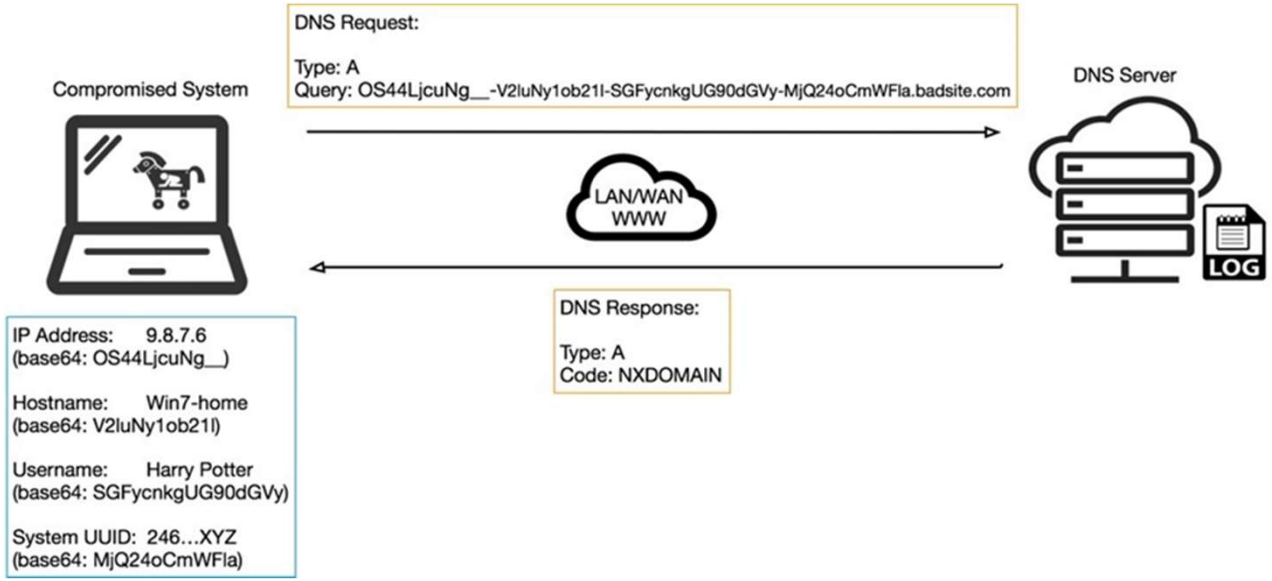
DNS TUNNELING

SOCCRATES

Normal



Exfiltration



CLUES

SOCCRATES

- Goal: Find the exfiltration attack on March 14 between 10:00 and 20:00.

- Patterns to look for:
  - 1. High volume of DNS queries from infected computer(s);
  - 2. NXDOMAIN responses to queries
  - 3. Short intervals between the queries (to reach a high volume);
  - 4. DGA-like or HGA-like queries because the exfiltrated data is within the DNS queries;

THANK YOU!

Liked this demo? Go try a few challenges yourself!
(info is in your email)

We will publish the answers tomorrow.

INTERESTED IN MORE?

https://www.soccrates.eu/

info@soccrates.eu

https://www.linkedin.com/groups/13786643/