Foundations of Information Security

Introduction

Attacks

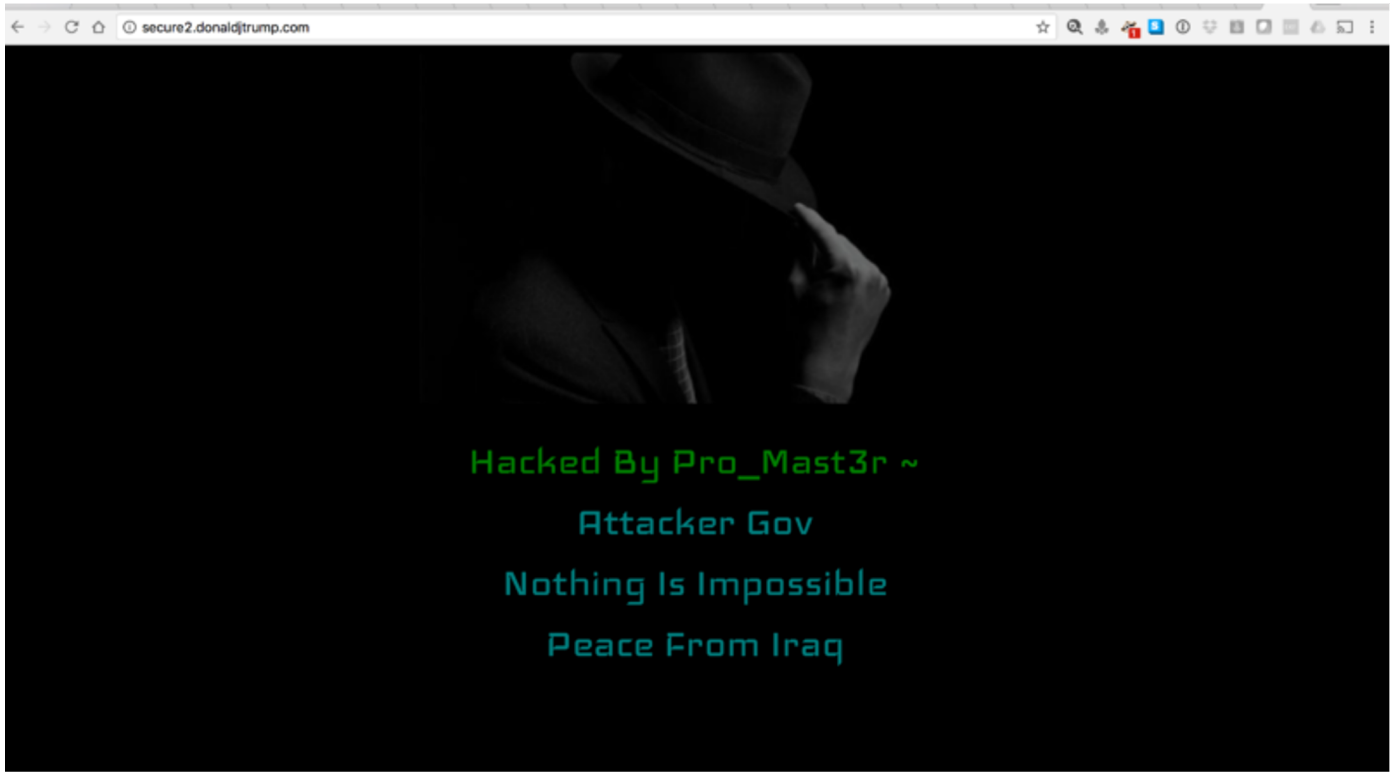
Stanford Advanced Cybersecurity

Stanford | ONLINE

Defacement

Online Vandalism, attackers replace legitimate pages with illegitimate ones; often targeted towards political web sites

Ex: Old Donald Trump Campaign Web Site Hacked by Iraqi attacker (2017)



Phishing & Spear phishing

Attacker sets up spoofed site that looks real

- Lures users to enter login credentials and stores them
- Usually sent through an e-mail with link to spoofed site asking users to "verify" their account info
- The links might be disguised through the click texts
- Wary users can see actual URL if they hover over link
- Spear phishing targets individuals in particular

```
<a href="http://www.evil-site.com">
        Legitimate Site
</a>
```

Malware

Malware = malicious software

Lots of variations -- spyware, ransomware, clickbots, etc.

Forms of distribution:

- Email attachment
- Trojan / trick to download
- Drive-by-download (e.g, Gumblar, The Ghost in the Browser)
- Link to drive-by in phishing email ()
- Worm (e.g, WannaCry, Code Red, Nimbda)

Cyber Security & Executive Strategy

Important Questions and Principles of Board Management

Stanford Advanced Cybersecurity

Stanford | ONLINE

Security and the Board: Important Questions

Why is it important to talk about security with your board of directors?

Who is on the board of directors? Who does the board and the CEO hold accountable for security?

Does your board have an audit and/or risk committee?

Security and the Board: Important Questions

Does your company have a CSO (Chief Security Officer) or CISO (Chief Information Security Officer)? Who does the CSO / CISO report to?

How technical or non-technical is your board of directors? What are their expectations in hearing about security?

Is there an executive-level “dashboard” for security?

Important Questions for Middle Management

Where is security on the corporate agenda? If not already high on the agenda, how can you help promote importance and awareness?

How can you help build the security program and/or report metrics on security that can flow into the executive-level dashboard on security?

Principles

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

Principles

3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.

4. Directors should set an expectation that management establish an enterprise-wide cyber-risk management framework with adequate staffing and budget.