NOTABLE CYBERSECURITY INCIDENT

Democratic National Committee 2016

By Alexander Turnsek, Laron Christian, Arielle Chapman

1 What was the event?

In 2016, the DNC was the target of two groups of Russian computer hackers who infiltrated the DNC Computer network leading to the release of ten of thousands of stolen emails.
Jul 27, 2015 - Apr 28, 2016

2 Impact of the breach

The emails and documents released damaged the reputation of the Clinton Campaign and it showed that the DNC favored Clinton over her rival Bernie. It has been assumed that this breach was the major factor why she lost the election.

3 How the breach occured

The breach occurred in 2015 when FBI agent Adrian Hawkins, called the Democratic National Committee in September 2015. The tech-support contractor at the D.N.C confused it for a prank call. The hackers stole various documents then moved on to other targets, John D. Podesta, whose private email account was hacked months later via a Phishing attack masquerading as google.

4 Attack Vectors, Attackers Approach

The group called Cozy bear used a powershell script to access a backdoor into the DNC servers, the other group called Fancy Bear used X-agent malware which enabled distant command execution, transmission of files and keylogging, They also used a phishing email sent to John D. Podesta, the campaign aide said the email was legitimate which caused an email to be hacked and leaked to wiki leaks

5 Mitigation Strategies

Some mitigation strategies against penetration attacks are to Update and Upgrade Software regularly, Defend Privileges and Accounts, and Ensure your network defenders implement cybersecurity best practices. For Phising attacks use Multifactor Authentication, Email filtering, and Domain Authentication.