Business Email Compromise

Or, why “you” may not be “you”

Andy Green

Lecturer of Information Security and Assurance

Kennesaw State University

Coles College of Business

Department of Information Systems

agreen57@kennesaw.edu

Kennesaw State University

Think about this scenario

- Your company A/P clerk receives an email from a vendor (ACME INC.), requesting a change to banking details for future payments
- The email appears to come from a name and domain that makes sense – frank.smith@acmeinc.info
- A/P clerk updates vendor records, cuts check for $566k next day
- Two days later, vendor contacts you when payment not received

Or, how about this scenario…

- Your company A/P clerk receives an email from the company CFO authorizing payment for the attached invoice
- A/P clerk processes payment and releases
- Days later, CFO asks why this payment was sent out

But, this never happens?!?

- Sedgwick County, Kansas - October 2016
- Attack carried out by a Brookhaven resident
- Attacker bought domain name and set up email server
- Approximate time to stage – 2 hours
- Approximate cost to attacker - $100
- BTW, dude was totally busted by the FBI…

Seriously, this happens…

- Ubiquiti Networks (2015) - $46.7M
- Ameriforge Group (2014) - $480K
- Socular (2015) - $17.2M

What are we talking about?

- Business email compromise, or BEC
- Organization, and specific employees, are carefully selected targets
- This is not a simple “phishing” attack
- Attackers study their targets, learn their operating methods
- Use OSINT to time attacks

How big is this problem?

- May 4, 2017 - FBI released a PSA regarding BEC
- October 2013-December 2016
  - Global
    - 40,203 incidents, $5.3B loss
  - U.S. only
    - 22,292 victims, $1.5B loss

https://imgflip.com/memegenerator/53373986/Macaulay-Culkin

Your adversaries are:

- Smart
- Organized
- Patient
- Intelligent
- Based in multiple countries

4GIFs
.com

So, what can you do?

- Operational controls
  - Out-of-band verification
  - Two-person authorization
  - Organizational policy
    - Operations and social media
  - Security Education and Awareness Training (SETA)

But wait, you can do more…

- IT controls
  - Sender Policy Framework (SFP)
  - Domain Message Authentication Reporting & Conformance (DMARC)
  - Buy "adjacent" domains
    - acme.info; acme.us; acme.org
  - Buy "fat fingered" domains

And still, there is more…

- Examine your organizational culture
  - Do you “shame” when mistakes are made
  - Do you encourage admission of mistakes
  - Encourage “healthy skepticism”

And with that…

Thank you for having me speak!

Andy Green
Lecturer of Information Security, KSU
agreen57@kennesaw.edu