Is Your Data Safe?
The Challenge of Client-side Security

Seth Hallem
CEO & Co-founder, Mobile Helix
ndElevate, NetDocuments® Executive Summit
May 23, 2017

mobile:helix™

Hacking is relevant to you

March 1, 2017
[6 major law firm hacks in recent history]

6 major law firm hacks in recent history

POSTED MAR 01, 2017 11:54 AM CST

BY JULIE SOBOWALE

Law firms have been victims of some of the most damaging hacks in recent history. Here's a list of the major law firm hacks in the past five years:

1. PANAMA CITY

Panama Papers—More than 11.5 million documents from the Panama-based law firm Mossack Fonseca were leaked to the public.

The information leaked was 2.6 terabytes of data, which is more than the contents of the Edward Snowden National Security Agency leaks and the 2010 WikiLeaks documents combined.

Law firms are a ***lucrative*** target

Bloomberg

December 27, 2016
[Chinese Hackers Charged With Trading on Stolen Law Firm Data]

- Three allegedly made $4 million trading on inside information
- U.S. says top deals lawyers targeted in computer intrusions

"This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world," Manhattan U.S. Attorney Preet Bharara said in the statement.

CRAIN'S CHICAGO BUSINESS.

March 29, 2016
[Russian cyber criminal targets elite Chicago law firms]

"I've always been surprised, frankly, that the law firms have not been more aggressively targeted in the past," he said. "If you've got confidential information about a merger or a patent, it's going to be very valuable."

A good attack vector is

- Inexpensive to execute in high volumes
- Hard to trace to its origin
- Hands off (at least for the master mind of the operation)
- Effective – lots of bang for the buck

A perfect example of a ***perfect*** attack

August 24, 2016
[The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender]

"On August 10 and 11, 2016, [Ahmed] Mansoor received SMS text messages on his iPhone promising "new secrets" about detainees tortured in UAE jails if he clicked on an included link."

"… the ensuing investigation … determined that the links led to a chain of zero-day exploits ("zero-days") that would have remotely jailbroken Mansoor's stock iPhone 6"

"… Once infected, Mansoor's phone would have become a digital spy in his pocket, capable of employing his iPhone's camera and microphone to snoop on activity in the vicinity of the device, recording his WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking his movements. "

Mobile devices are ripe targets

- They have a broad attack surface for launching remote attacks
- They are constantly changing, with version fragmentation even in iOS
- They are easy to steal, and stealing a device does not require a sophisticated criminal

Protect your data

The device *is not* in your control

Step 1: Authenticate and authorize

- Access to sensitive firm data should follow the same authentication and authorization best practices that you apply to a firm laptop
  - Secure, rotating passwords
  - Multi-factor authentication
  - Single sign-on

Step 2: Limit exposure

- Allow attorneys to download and manipulate the data they need on a mobile device, but retain control of how long and how much of that data resides on the device.
  - Do not allow sensitive data to be accumulated on the device – including emails and documents
  - Consider that hackers will often take stolen devices offline to prevent remote wipe – can you control what data is available online vs. offline?

Step 3: Protect your data

- Once data leaves your network, it should be:
  - Transmitted over TLS using strong keys and a secure cipher
  - Transmitted to authorized devices only using bi-directional certificate authentication to prevent man-in-the-middle attacks
  - Encrypted independently from the underlying device's pincode-based encryption mechanism, which ensures that your data is immune to a generic SpyWare attack

Summary: protect your data

- Hacking is a lucrative industry, and law firms are a ripe target
- Client devices are one of many ways that attackers can steal data – mobile devices are particularly ripe for attack
- Enable your users to accomplish work on a mobile device
- Protect your data by:
  - Ensuring data access is authenticated and authorized
  - Limiting data exposure
  - Protecting your data

Thank you

http://www.mobilehelix.com

contact@mobilehelix.com