Mkit | Security Solutions

# Medical Records on the black market

Matias Katz
@MatiasKatz
katz@mkit.com

Who here had a Pentest

done in the last 6 months?

Who corrected what the auditing company found?

# What do we

# try to protect?

# What is really lost in an attack?

# What does it all come to?

$$$$$

- Hack stuff
- Hack some more
- ???
- Profit

Mkit

Let’s talk about the

– ???

# The value of an owned server:

- Web Server
- Email
- Data
- Reputation
- Zombie
- Credentials
- Financial
- Hostage

http://krebsonsecurity.com/2013/01/you-are-a-target-poster-builds-on-hacked-pc-graphic/

# Web Server

- Phishing
- Ilegal Software
- Child Porn
- Viagra

# Email

- SPAM
- Access to corporate Emails
- Identity Theft
- Account Harvesting

# Data

- Trade secrets
- Licenses
- Databases
- Personal Content

# Reputation

- Defacement
- Emails
- Public Trust
- Social Networks

## Zombie

- SPAM
- DDoS
- Proxy
- CPU Power

# Credentials

- Users/Passwords
- Private keys/Certificates
- Traffic Capture
- E-commerce Apps

## Financial

- Banking Data
- Credit Cards
- Stock Trading
- Payroll

## Hostage

- Fake Antivirus
- Ransomware
- Remote Disk Encryption
- Capture of Email Accounts

Mkit

1 owned server can make **AT LEAST**

# USD 500,000 per year

in profits for the attackers

# Recent Examples

Mkit

# Equifax (Sept. 2017)

Damage: 143 MM records

What happened?

WebApp vulnerability

Cause: Poor AppSec Procedures

# Deloitte (Sept. 2017)

Damage: Clients trade secrets

What happened?

Privileged Account Takeover

Cause: Weak Auth Policies

# Australia Military (Oct. 2017)

Damage: Top Secret Info Disclosure

What happened?

12-month-old vulnerability

Cause: Absent Patching Strategy

# Accenture (Oct. 2017)

*(The problem was reported before anything happened)*

Potential Damage:
Passwords & Private Keys exposure

Cause: Failed Monitoring Process

What about us?

Which one is our “server”?

Just 1 electronic Health Record (EHR) has a black market value of between

USD 40 and 1000

A credit card is between USD 2 and 5

http://hipaahealthlaw.foxrothschild.com/2015/03/articles/privacy/hacked-health-records-prized-for-their-black-market-value/

In September 2014, 4.5 MM medical records were stolen from Community Health Systems Inc.

http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

In January 2015, at

Anthem Health Insurance,

80 MM records were stolen

http://www.npr.org/sections/alltechconsidered/2015/02/05/384099135/anthem-hack-renews-calls-for-laws-to-better-prevent-breaches

# Comparison:

## Ashley Madison (July 2015)

- Only 39 MM records

- Only Full Name/Email

# Comparison:

## Anthem Health Insurance

- 80 MM records
- Full Name/email
- Social Security number
- Medical Records
- History of illnesses
- History of procedures

The theft of medical records

has increased 40% since 2013

because of how easy it is to achieve

and its high market value

# For What?

- Health Insurance Fraud

- Prescription Medication

- Identity theft

- Extortion

# Why?

- Lack of Protection

- Noncompliance with Standards

- Obsolete ID verification processes

- Unprotected comms between entities

- Failing chains of custody

# How?

- Intrusion
- Social Engineering
- Malware
- Espionage

Mkit

1 owned server can make **AT LEAST**

USD 500,000

per year

in profits for the attackers

Mkit

What if it contains medical records?

Mkit | Security Solutions

# Medical Records on the black market

Matias Katz
@MatiasKatz
katz@mkit.com