THE GROWING CYBERSECURITY THREATS IN TELEMEDICINE

Stanley Louissaint
Principal and Founder of Fluid Designs

Industry Accomplishments

ChannelPro 20/20 VISIONARIES 2016

FLUID DESIGNS

What is Hacking?

- Hacking
  - Method in which one bypasses or modifies the normal operation of a system
    - Exploits
    - Vulnerabilities

FLUID DESIGNS

The Business of Hacking

- Purpose in the early day's
  - Pride
  - Glory
- Today's purpose
  - Profits
  - Espionage
  - Hacktivism

FLUID DESIGNS

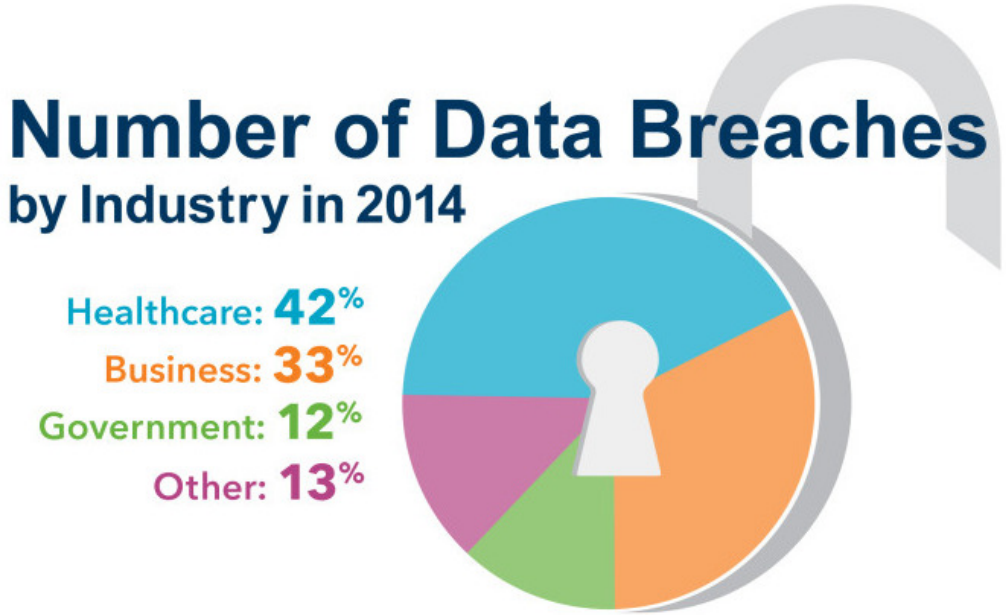
Types of Cybersecurity Attacks

- Attack vectors
  - Phishing
  - Social Engineering
  - Malware/Ransomware
  - Denials of Service (DoS)
  - Session Hijacking & Man-in-the-Middle

FLUID DESIGNS

Where Does Healthcare Fit?

- #1
  - Highest number of data breaches



Source:
idtheftcenter.org

FLUID DESIGNS

Reasons to Attack Healthcare

- 2016 Healthcare Information and Management Systems Society (HIMSS) Study
  - Medical Identity Theft
    - #1 Concern
      - 77% of respondents
  - Black Market/Organized Crime
- Over 113.2 million healthcare records stolen in 2015

FLUID DESIGNS

Health Records

- Where is the value?
  - Electronic Health Record
    - Demographics
    - Insurance Information
    - Mailing Address
    - Social Security Number
    - Birthdate
    - Medication
    - Billing Information
      - Credit Card Numbers

FLUID DESIGNS

Value in Health Records

- EHR = PII + Medical History + Insurance + Financial
  - This unique combination differentiates healthcare hacks from other industries

FLUID DESIGNS

Value in Health Records

- Personal Identifiable Information (PII)
  - No Expiration Date = Greater Value
    - Name
    - Date of Birth
    - Social Security Number

FLUID DESIGNS

Value in Health Records

- Uses
  - Obtain pharmaceuticals
  - Commit insurance fraud
  - Obtain medical care
    - Medicare
    - Medicaid

FLUID DESIGNS

Health Records Sold on Darkweb

DARK Reading

Stolen Health Record Databases Sell For $500,000 In The Deep Web

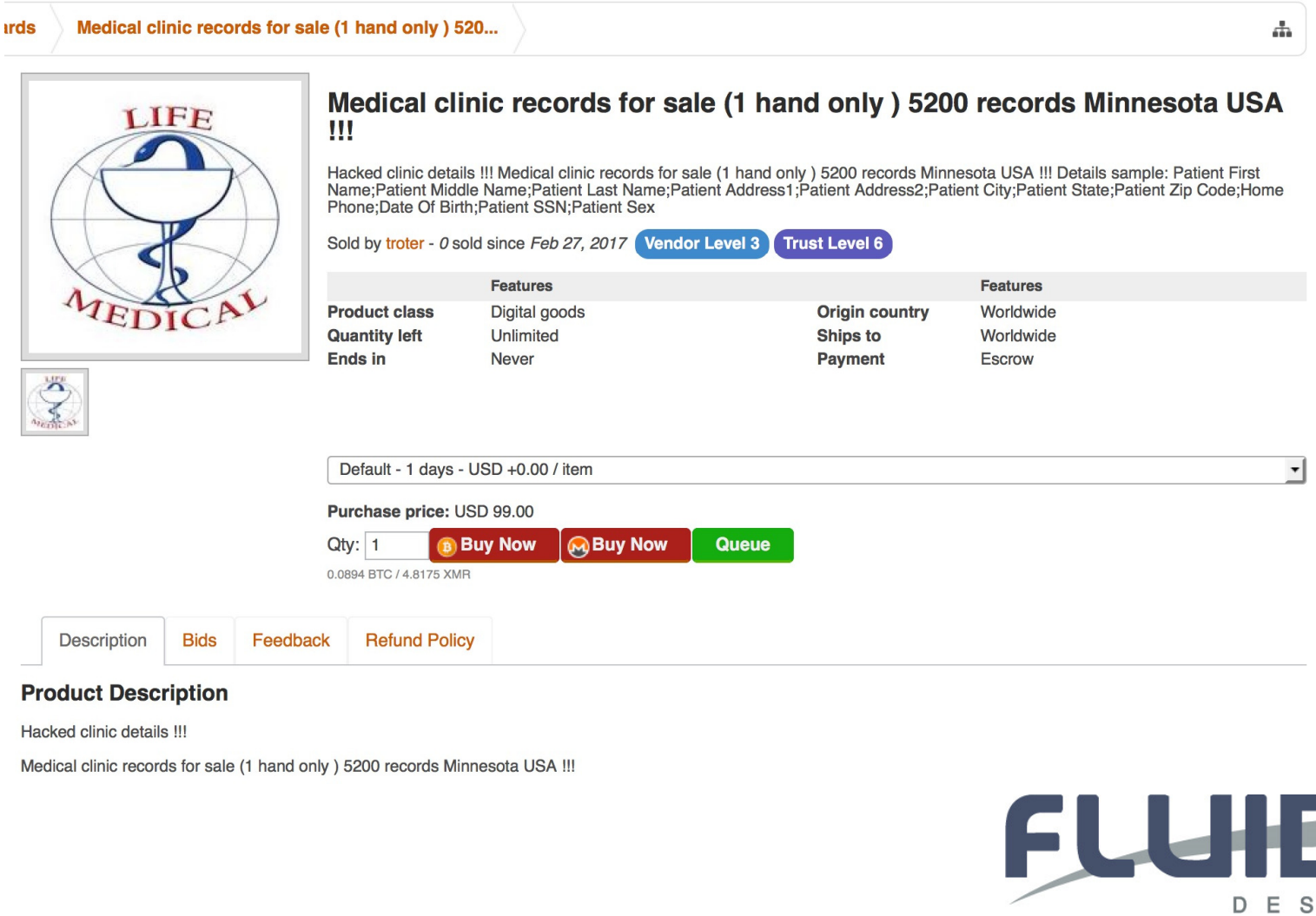
Electronic health record databases proving to be some of the most lucrative stolen data sets in cybercrime underground.

Medical insurance identification, medical profiles, and even complete electronic health record (EHR) databases have attracted the eyes of enterprising black hats, who increasingly see EHR-related documents as some of the hottest commodities peddled in the criminal underground. A new report today shows that complete EHR databases can fetch as much as $500,000 on the Deep Web, and attackers are also making their money off of smaller caches of farmed medical identities, medical insurance ID card information, and personal medical profiles.

The data comes by way of a report from Trend Micro's TrendLabs Forward-Looking Threat Research (FTR) Team, which took a comprehensive look at how attackers are taking advantage of healthcare organizations' weaknesses to devastating effect. Cybercriminals always have their eyes open for new profitable revenue streams, and the poor security around increasingly data-rich EHR systems pose a huge opportunity for the bad guys.

FLUID DESIGNS

Health Records Sold on Darkweb



ırds › Medical clinic records for sale (1 hand only) 520...

LIFE MEDICAL

Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!!

Hacked clinic details !!! Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!! Details sample: Patient First Name;Patient Middle Name;Patient Last Name;Patient Address1;Patient Address2;Patient City;Patient State;Patient Zip Code;Home Phone;Date Of Birth;Patient SSN;Patient Sex

Sold by troter - *0* sold since *Feb 27, 2017* Vendor Level 3 Trust Level 6

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 99.00

Qty: 1 Buy Now Buy Now Queue

0.0894 BTC / 4.8175 XMR

Description | Bids | Feedback | Refund Policy

Product Description

Hacked clinic details !!!

Medical clinic records for sale (1 hand only) 5200 records Minnesota USA !!!

FLUID DESIGNS

How Prevalent?

- Bitglass' Healthcare Breach Report
  - 1 in 3 Americans victims of healthcare data breaches

FLUID DESIGNS

Consequences for You

- Department of Health and Human Services' Office for Civil Rights (OCR)
  - Fines
- Loss of consumer trust
- Loss of consumer confidence
- Loss of patient to competing provider
- Reporting, analysis, review and remediation costs

FLUID DESIGNS

HIPAA

- Department of Health and Human Services' OCR
  - Enforcing rules
  - 2016
    - 13 settlements
    - $22.8 million in payments

FLUID DESIGNS

Cost of HIPAA Violations

Covered Entity	Amount	Date	Breach that triggered OCR investigation
University Medical Center	$650,000	11/2016	Malware infection
Health System	$2,140,500	10/2016	PHI made available through search engines
Health System	$400,000	9/2016	Loss of two unencrypted backup tapes
Health System	$5,550,000	8/2016	Theft of desktop computers, loss of laptop, improper access of data at business associate
University Medical Center	$2,750,000	7/2016	Unprotected network drive

FLUID DESIGNS

Cost of HIPAA Violations

Covered Entity	Amount	Date	Breach that triggered OCR investigation
Business Associate	$650,000	6/2016	Theft of mobile device
Hospital	$2,200,000	5/2016	Filming of patients by TV crew
Physician Group	$750,000	4/2016	Improper disclosure to business associate
Medical Research Institute	$3,900,000	3/2016	Improper disclosure of research participants' PHI
Health System	$1,550,000	3/2016	Theft of laptop computer / Improper disclosure to business associate (discovered during investigation)

FLUID DESIGNS

Cost of HIPAA Violations

Covered Entity	Amount	Date	Breach that triggered OCR investigation
Physical Therapy Provider	$25,000	2/2016	Improper disclosure of PHI (website testimonials)
Infusion and Equipment Provider	$239,800	2/2016	Improper disclosure (unprotected documents)

*Data Source: U.S. Department of Health and Human Services Office for Civil Rights

FLUID DESIGNS

Protecting Patient Data

- Protecting patient data = protecting yourself

FLUID DESIGNS

Protecting Patient Data

- Third Party Audits
- Vulnerability Testing
- Penetration Testing
- Hardware Solutions
  - Firewalls
    - Unified Threat Management (UTM) Firewalls
    - Next-Gen Firewalls (NGFW)

FLUID DESIGNS

Protecting Patient Data

- Software Based Solutions
  - Encryption
  - Antivirus
  - Antimalware
  - E-mail Spam Filtering
  - Application Containerization
    - Work Container
    - Personal Container
  - Data Backup

FLUID DESIGNS

Protecting Patient Data

- User Education
  - Do not share passwords
  - Enable two-factor authentication
  - Do not use third party device
    - Ex: Free USB flash drive
  - Do not open e-mails and/or attachments from unidentified individuals
  - Do not allow a random person who calls access to your computer/device

FLUID DESIGNS

Remote Worker Protections

- Mobile Device Protection
  - Never leave devices unattended
  - Lock devices if unattended
  - Avoid logging to secure sites or portals around people
  - Do not use public wireless hotspots

FLUID DESIGNS

Breach

- What to do?
  - Follow protocol
  - Shutdown All Systems
  - Contact your IT provider or department

FLUID DESIGNS

Presenter

Stanley Louissaint

Principal and Founder, Fluid Designs

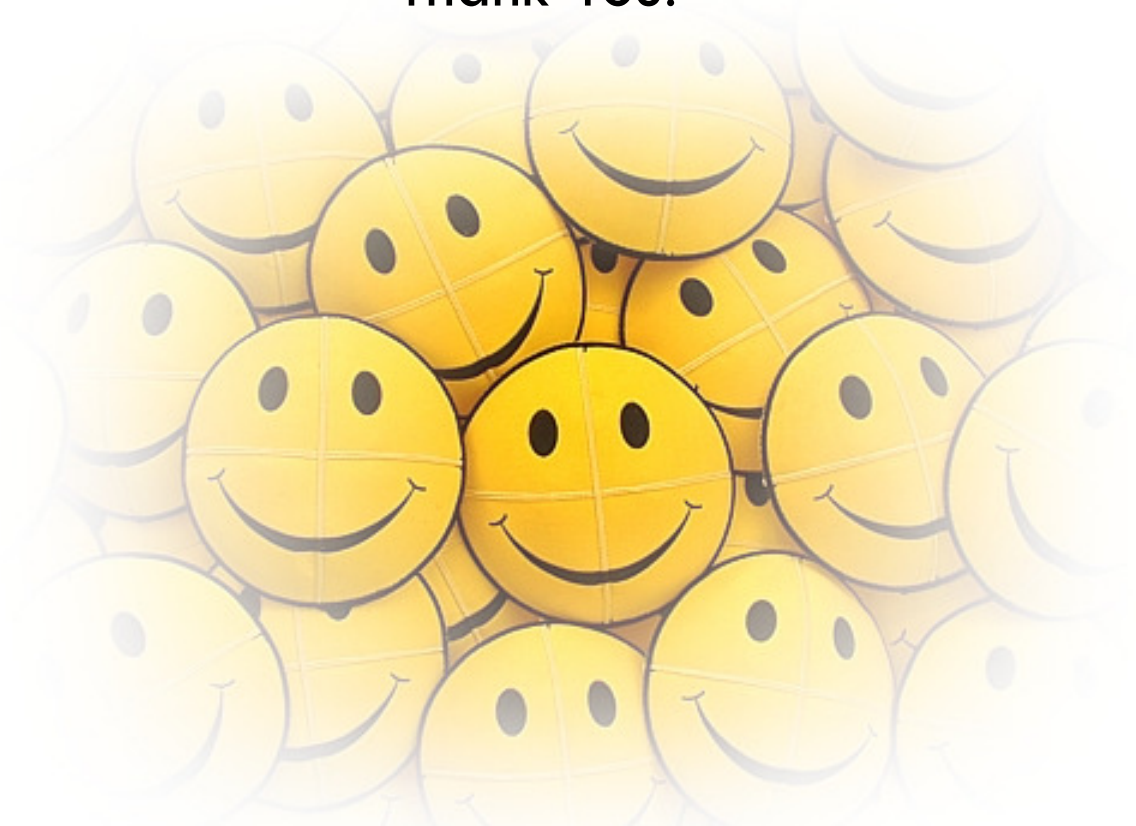
- Managed Service Provider
- Computer and Network Support/Consulting
- Cybersecurity Penetration Testing
- Business Continuity Solutions
- e-Discovery & Litigation Support

908-688-2444
www.FluidDesigns.com
www.LinkedIn.com/in/slouissaint
slouissaint@fluiddesigns.com

FLUID DESIGNS

Questions?

Thank You!



FLUID DESIGNS