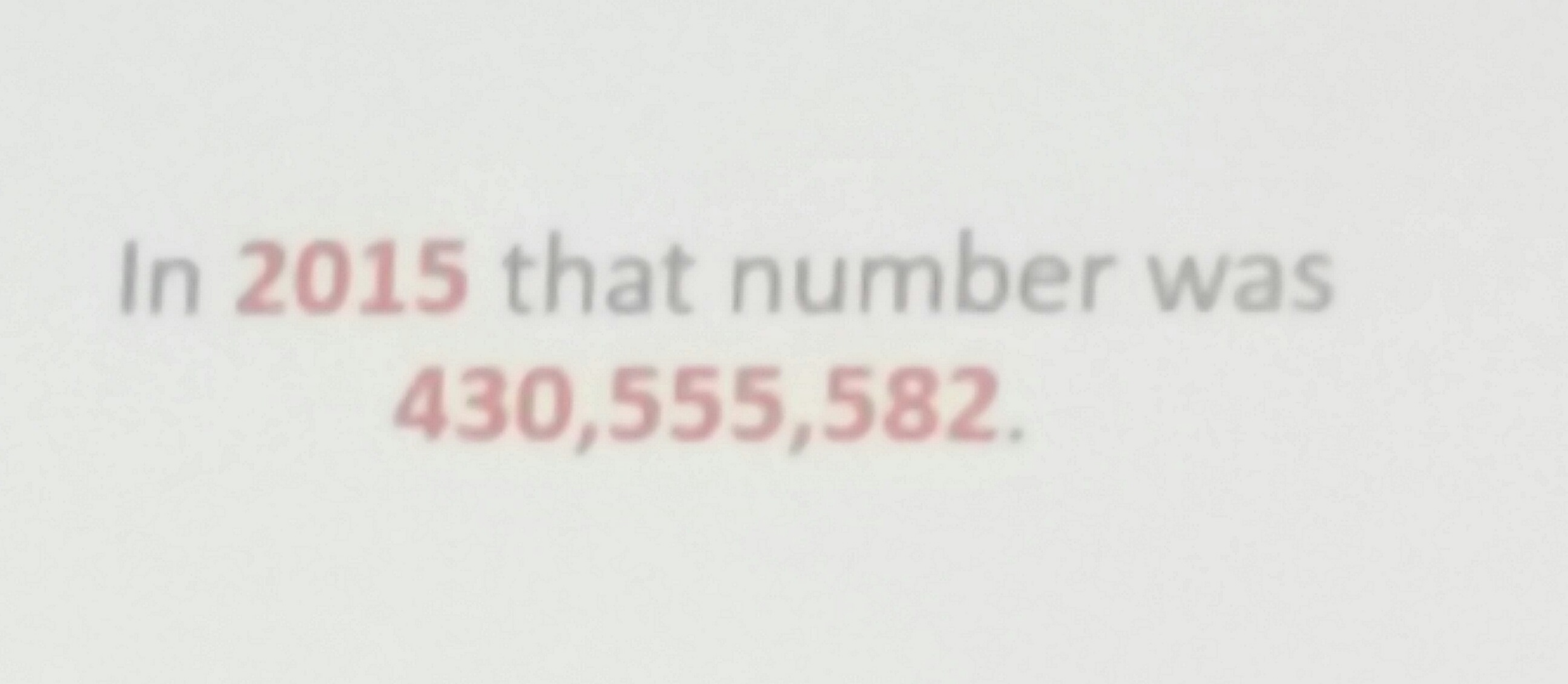
The Office of the National Coordinator for
Health Information Technology

Safeguarding Health Information: Building Assurance through HIPAA Security - 2016

ONC Update: Threat Sharing, Risk Assessment, APIs & Apps, and Block Chain: Yes, We’ve Been Busy

Lucia C. Savage, JD, Chief Privacy Officer, October 15, 2016

# of Pieces of Malware Created in 2015



In 2015 that number was

430,555,582.

Source: David S. Finn of Symantec

Agenda

- Information Sharing and Analysis Organization grant
- Security Risk Assessment Tool upgrade
- APIs, apps and security
- Thinking about blockchain

Sharing Identified Cyber Threats

- Last year: committed to supporting the development of an information sharing & analysis organization
  - To facilitate two-way communication about known cyber threats
    - To HPH from the U.S. Government, including what to do
      - Build a financial sustainable model that is available to all
        - Membership dues and size of business should not be barriers to better cyber threat response,
    - From HPH to U.S. Government
  - Grant Awarded to NH-ISAC: Press Release

Why Improve Threat sharing? Wont Sharing Threats Disclose PHI?

CyberhoodWatch
We immediately report all suspicious activities to our Healthcare Neighbors

- In an ***interoperable, interconnected health system***, an intrusion in one system could allow intrusions in multiple other systems.

- ***volume, timeliness, and quality***

- ***Better information yields better prevention***.

- Dept of Homeland Security guidance on sharing threats, for every sector

- OCR also helps explain how to do this right Help from OCR: guidance on sharing threats, not PHI

Security Risk Assessment

- What: evaluating what are the security risks in your environment that are not reasonable.

  (assessment is NOT remediation)

- Should be regularly assessing security risks for
  - Good hygiene
  - Security Rule Compliance
  - If required under CMS programs such as Meaningful Use, MACRA, or other payment programs.
- ONC can help
  - Security Risk Assessment Tool updated September, 2014

APIs, Apps, and mobile health

- “Open API” required for Certified Electronic Health Information technology effective January 1, 2018
  - What, exactly does this mean?
- Why: so a patient can use an app of their choosing, as specified in CMS rules, to obtain their health information and help with their own care.
- An “open” API is a new concept for EHRs and especially for providers
  - API Task Force December 2015-May 2016
  - Recommendations
  - Security Engineering and APIs
    - API Task Force concluded that security issues for read-only, open-specification API in healthcare are *the same* as security issues for existing read-only, open-specification APIs, such as made available in other sectors: Internet commerce, banking, energy

Any App the patient chooses

- **In 2016, people using apps can**
  - Get a mortgage
  - Sell stock
  - Apply for jobs.
- **Apps are where people are.**
- **In interpreting 45 CFR 164.524, OCR has said that an individual may assert these rights through an app they choose, and the discloser can only reject the app when it poses a security threat to the discloser's system.**

- **App developers need to "do the right thing".**

Thanks Wikipedia for Spike Lee poster!

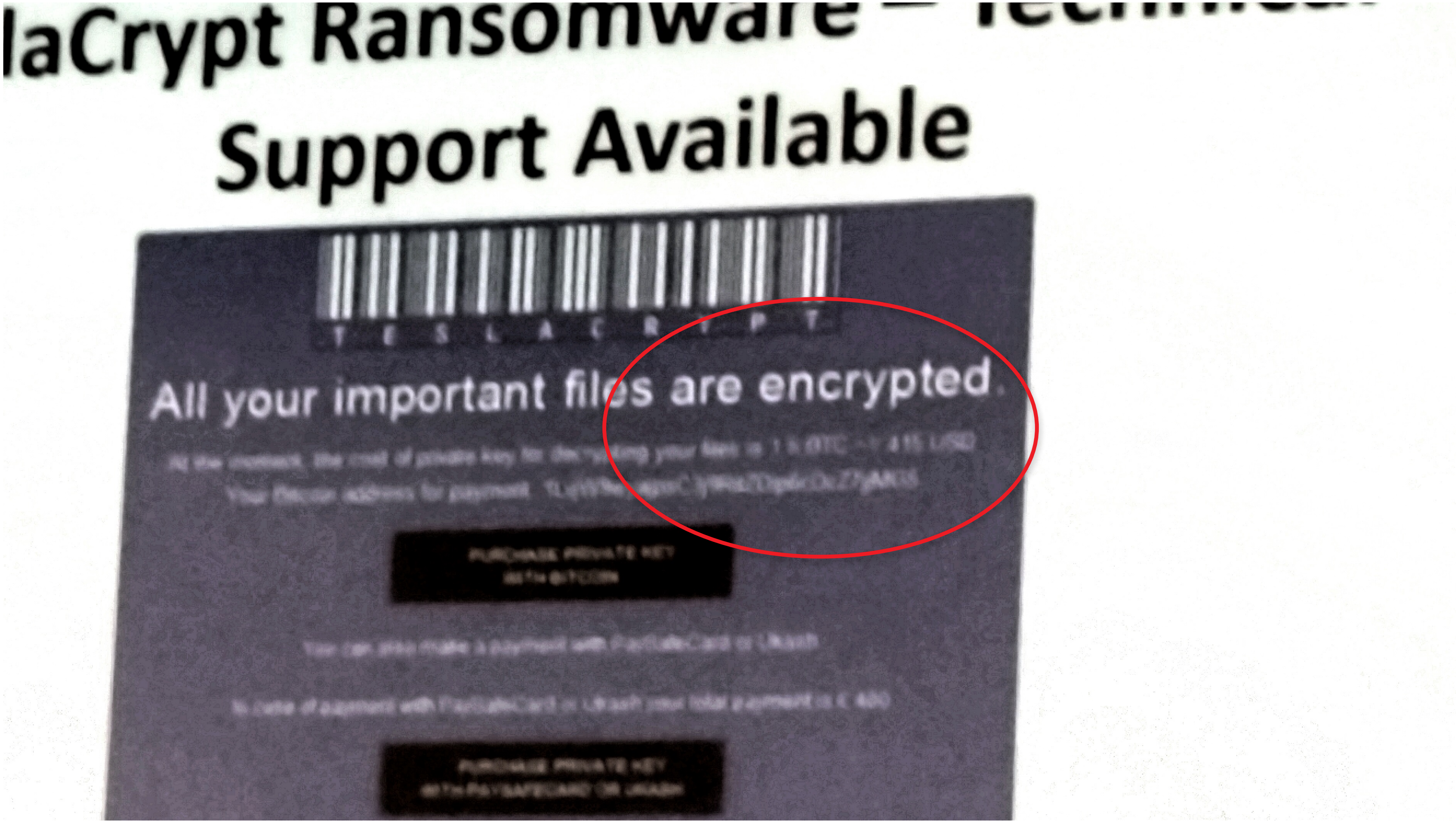
Mobile Health (speaking of doing the right thing)

- *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA. Published July 19, found, as to Security:*
- **Health information collected in more places without consistent security standards may pose a cybersecurity threat (of which individuals may be unaware):**
  - As more and more data is stored electronically, and as information is stored in multiple locations, the new locations for storage and new collection points make the data increasingly vulnerable to cybersecurity attacks.
  - While HIPAA imposes security standards for individually identifiable health information held by covered entities and business associates, such legal standards do not necessarily apply to NCEs
  - FTC consumer protection authority provides some protections.

How to Know What the Right Thing Is?

- ONC resources
  - » Developer Tool
  - » Mobile Device Roundtable
  - » Mobile Security for Providers
  - » Model Privacy Notice (coming soon).
- FTC Resources
  - » For consumers
  - » For business:
- Other Resources
  - » Consumer Technology Assn
  - » Future of Privacy Forum

What about blockchain?



laCrypt Ransomware – Technical
Support Available

TESLACRYPT

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD

Your Bitcoin address for payment: [illegible]

PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is € 400

PURCHASE PRIVATE KEY
WITH PAYSAFECARD OR UKASH

Concepts of How Blockchain Could be Used in Healthcare (ONC Blockchain Challenge Winners)

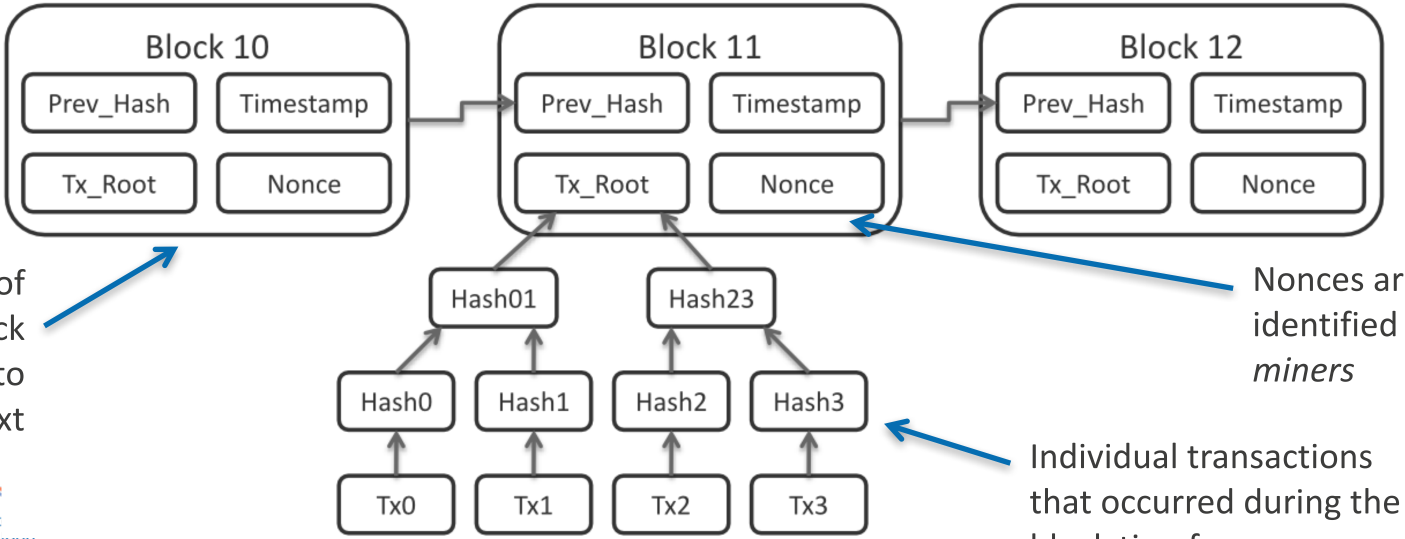
- Handing off data for claims processing
- Patient record storage
- Identity management
- Precision Medicine
- Alternate payment models
- HIE & accountable care
- Clinical research

Check out all the winners at:

https://www.hhs.gov/about/news/2016/08/29/onc-announces-blockchain-challenge-winners.html

Blockchain Basics

- Blockchain is a distributed ledger for recording the type and nature of a transactions
  - » E.g., the Bitcoin blockchain maintains copy of every Bitcoin transaction ever made
- Every 10 minutes, a new block is added to the blockchain
- The blockchain is secured using complex cryptographic functions computed by *miners*
- Distributed nature makes tampering difficult



Hash of each block is input to the next

Nonces are identified by *miners*

Individual transactions that occurred during the block timeframe

Limits of Blockchain

- Nearly impossible to change the blockchain itself
  - So, how to correct errors in health data?
- Distributed nature makes tampering with the transaction economy very difficult
  - Akin to manipulating traffic on the Internet → possible but only at a nation state level or collusion among ISPs
- Unique risk to blockchain: the 51% Attack
  - If a single entity controls 51% of mining power, they could manipulate blockchain by starting one block behind every other miner, then “catching up” to them with fraudulent blocks
  - In lay mans terms…if a miner can compute two blocks in the time it takes everyone else to compute one, they can manipulate the previous block when they publish the new block
- Other risks
  - Vulnerabilities in the blockchain/mining software itself
  - Yet undiscovered cryptographic weakness in blockchain or crypto protocols
  - Denial of service attacks

Blockchain is not a silver bullet. It addresses the problems of distributed, immutable storage only

Mining and Miners

- New York Times had an interesting story about the scope of block chain processing that now occurs in the People's Republic of China.
  - "At the time of the meeting [April 2015], over 70 percent of the transactions on the Bitcoin network were going through just four Chinese companies, known as Bitcoin mining pools — and most flowed through just two of those companies. That gives them what amounts to veto power over any changes to the Bitcoin software and technology. "
  - What does this mean for the 51% concept?
- Mining takes vast amount of computing power. Who pays for that in healthcare?
  - Mining is expensive (hardware, power, cooling)
  - ~200 quintillion crypto computations required for creating a new block
  - Bitcoin miners are paid in bitcoin, but who pays healthcare miners?

What Blockchain may not be able to do

- Establish the rules
- Adjudicate ambiguous rules
- Interpret rule
- Address the needs of
  - Those without computers
  - Work well where there is no broadband?

Key Challenges

- Hype vs reality
- Blockchains are large—who stores them and how do small practices access them?
- At it’s core, blockchain is simply a distributed transactional database model
  - All the complexity in the blockchain apparatus is to ensure transactions can be trusted & to prevent fraudulent activity
  - Confidentiality & access control come from other technology
  - Privacy established by rule everyone agrees to; technology merely enforces privacy. Where do the rules come from?
- Blockchain isn’t appropriate in all use cases—need to do a security risk assessment to determine what risks blockchain addresses