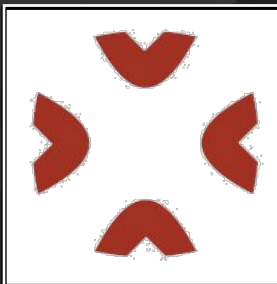


**HEALTHCARE
DATA SECURITY:
REPORT FROM
THE DARK WEB**

**24th NATIONAL
HIPAA SUMMIT
WASHINGTON D.C.**



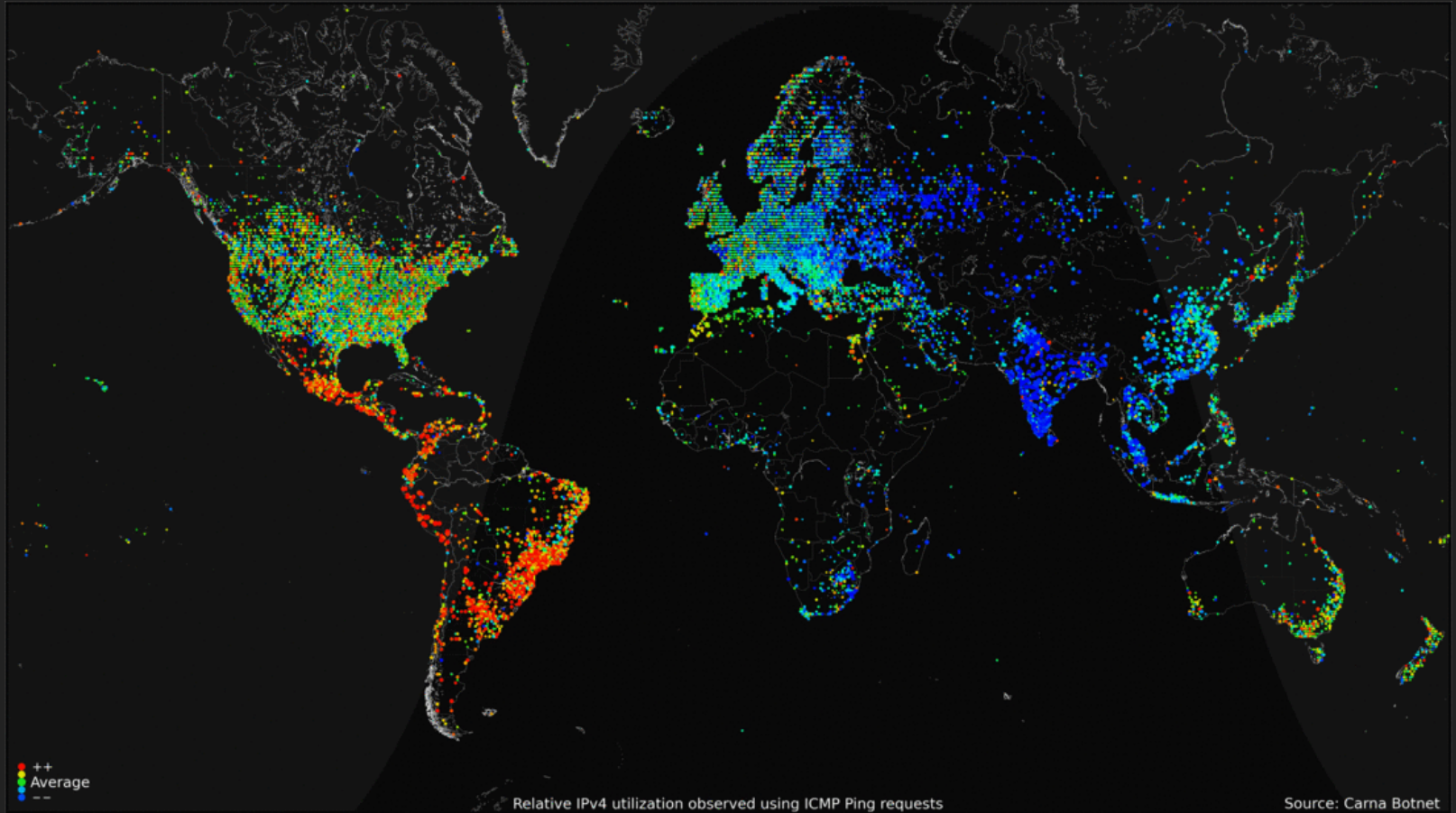


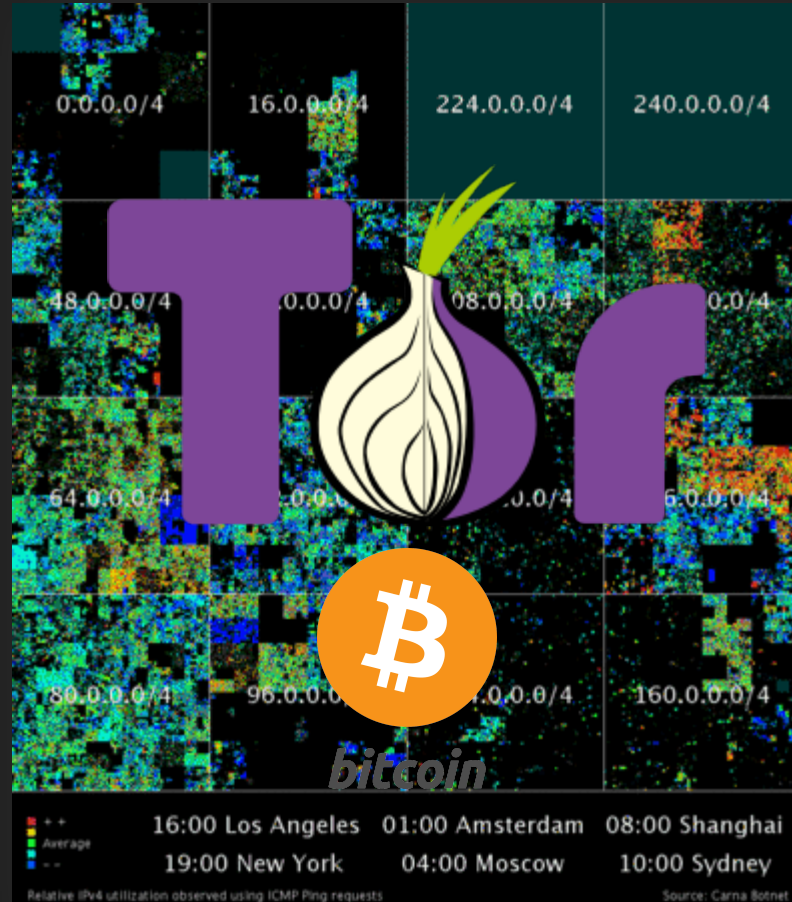
BEN GOODMAN

4A Security & Compliance



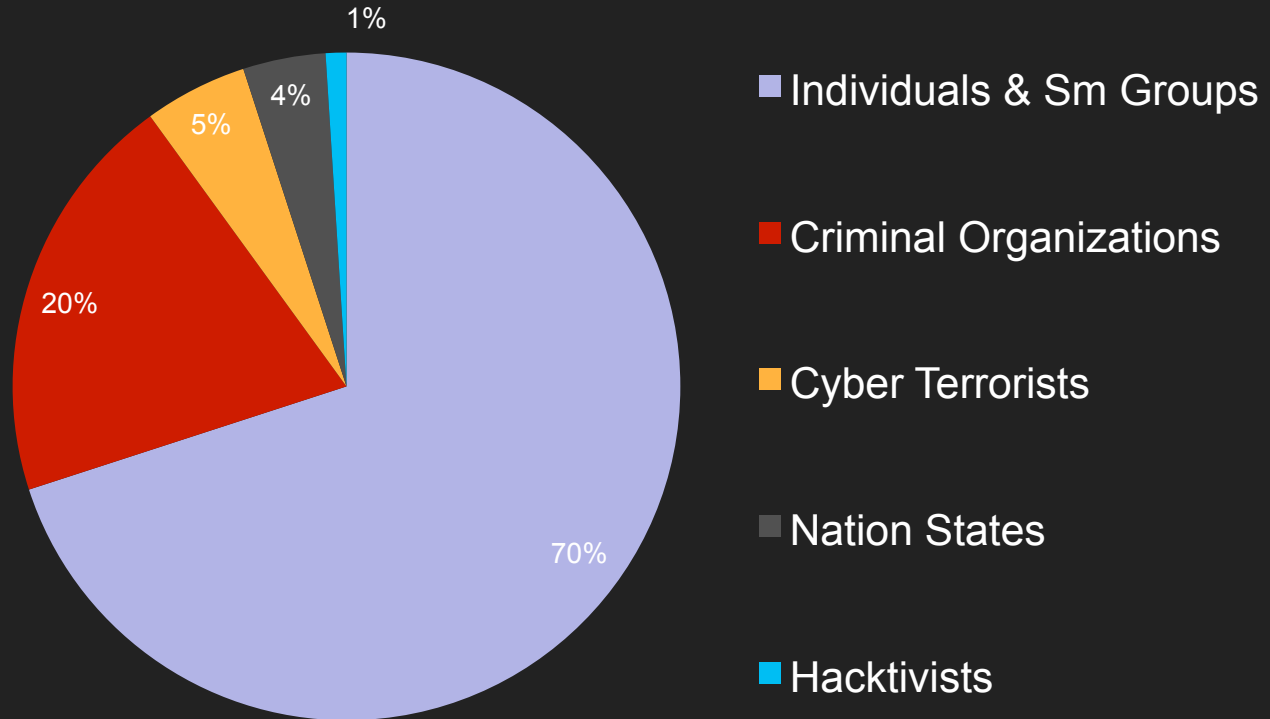
**WE ARE DEDICATED TO HELPING
HEALTHCARE ORGANIZATIONS
SECURE THEIR DATA,
MAINTAIN COMPLIANCE,
EDUCATE THEIR PEOPLE,
AND MANAGE CYBER RISK.**



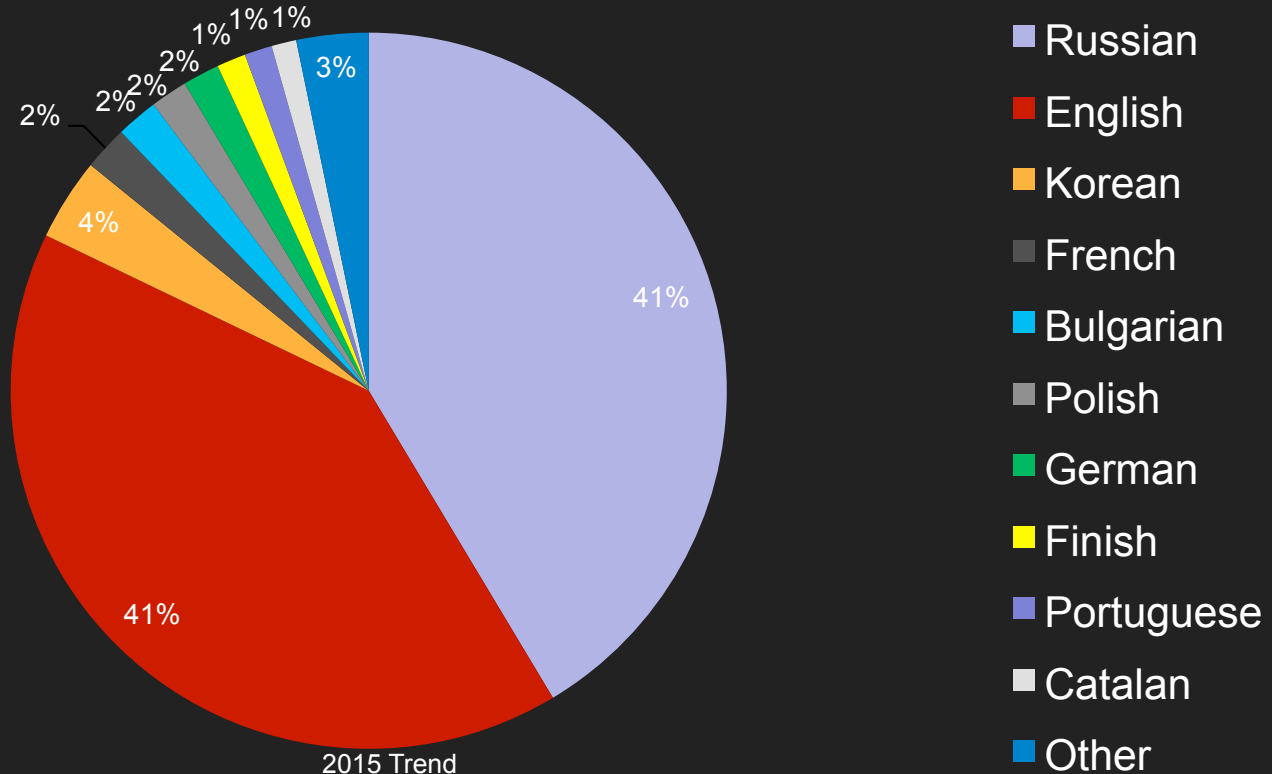




DARK NET ACTORS

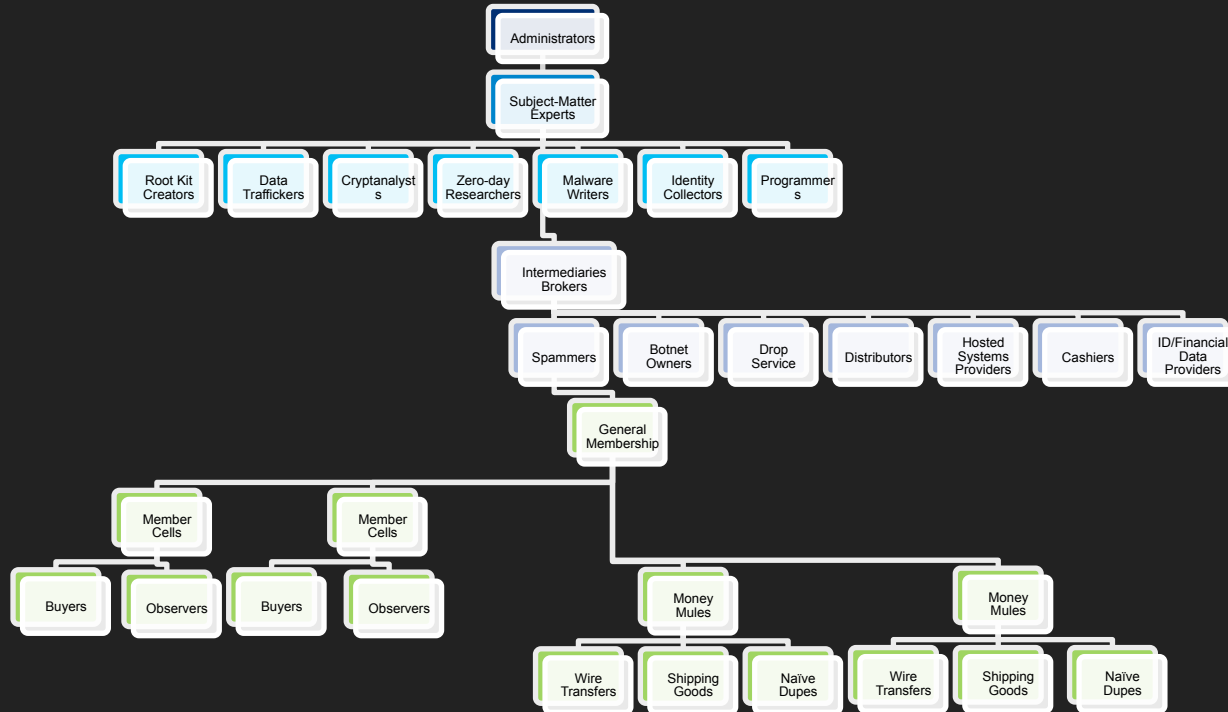


➔ DARK NET LANGUAGE DISTRIBUTION

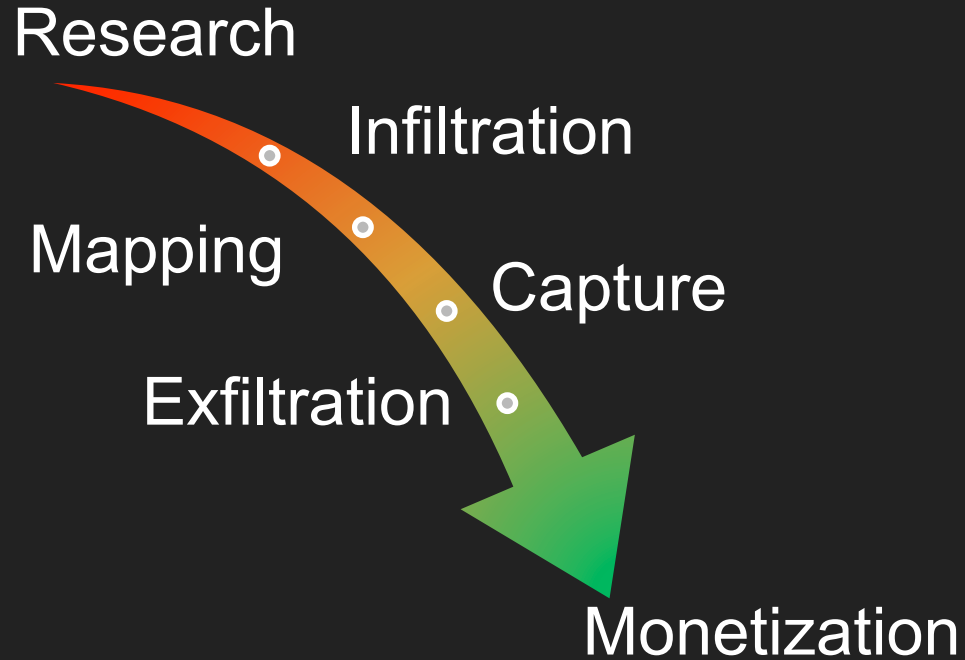




CYBER CRIMINAL ECOSYSTEM

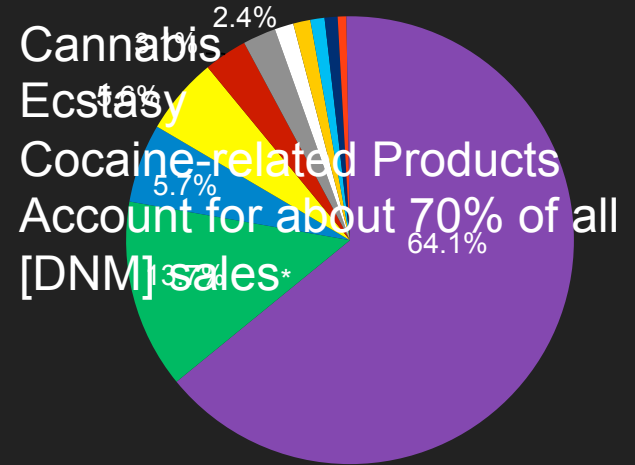
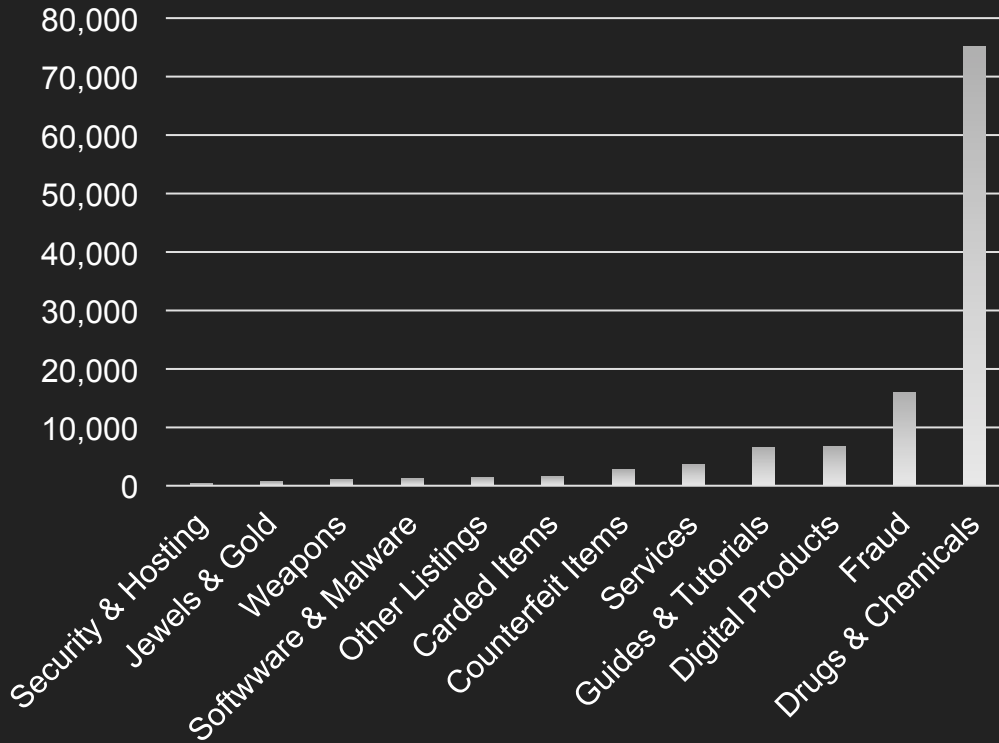


 ATTACK LIFECYCLE



➔ DARK NET MARKET LISTINGS #

DARK NET MARKET SALES %






- Drugs & Chemicals
- Fraud
- Digital Products
- Guides & Tutorials
- Services
- Counterfeit Items
- Carded Items
- Other Listings
- Software & Malware
- Weapons

* "Measuring the Longitudinal Evolution of the Online Anonymouse Marketplace Ecosystem" Security & Hosting Soska & Christin 2015



DARK NET MARKET SIZE EXAMPLE



56,22		Members
465,22		Messages
61,29		Discussions



**DNMs ARE RESILIENT
TO LAW
ENFORCEMENT
TAKEDOWNS**



Sales volume rebounded quickly following Operation Omynous and Evolution, Pandora and Sheep, exit scams.*

** "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem", Soska & Christin 2015*



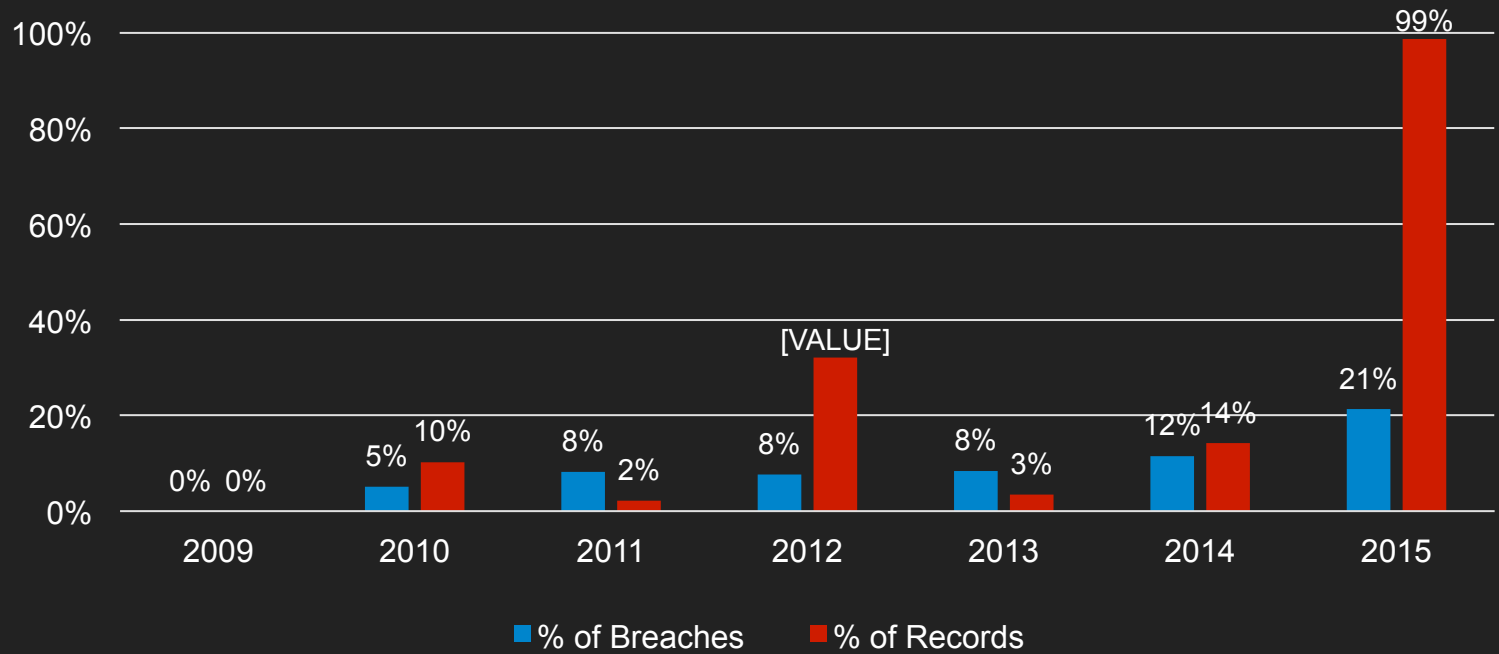
DARK NET MARKET LISTINGS

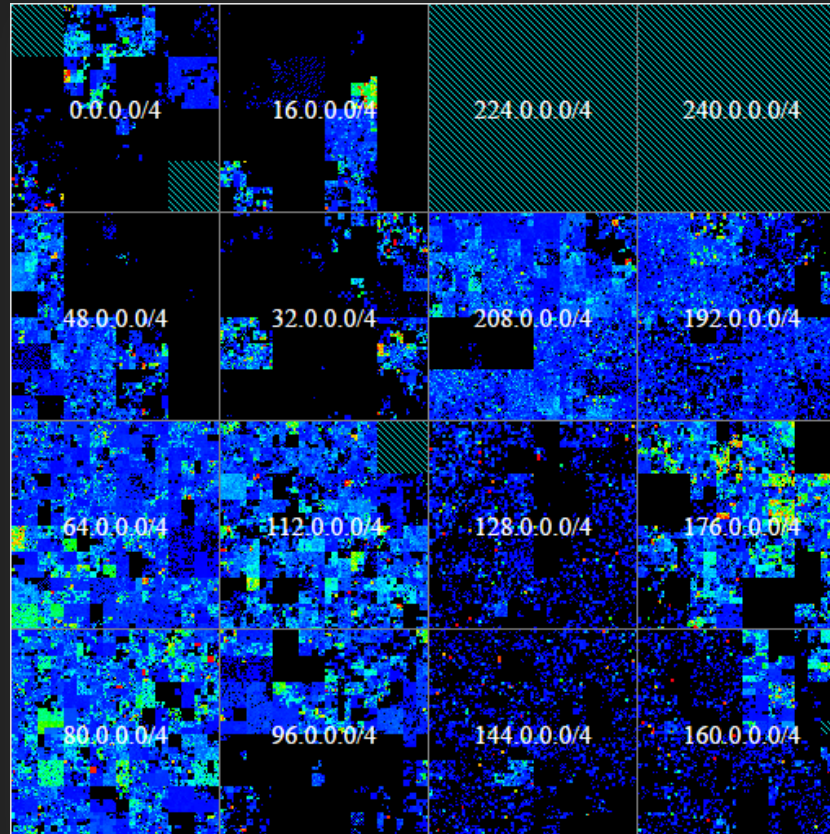
DEEP.DOT.WEB

Official Hidden service:
DeepDot35Wvmeyd5.onion

Market	Uptime Status	URL	Open registration?	Offers Multisig?	Had Security Issues?!	Active warnings	Commission	Vendor Bond	2FA	Forced Vendor PGP	FE Allowed?	Type	Ratings	Created
Alphabay	97.90% ↑	http://pwoah7foa6au2pul.onion/register.php?aff=41211	Open	✓	🟡	None	3.5%	200\$	✓	✓	Yes	Free Market	★★★☆☆ 3.02 (494 REVIEWS)	22-12-14
Dream Market	97.13% ↑	http://lchudifyeqm4ldjj.onion/?ai=1675	Open	✗	🟡	None	4%	0.25BTC	✗	✗	Yes	Market	★★★★☆ 3.93 (304 REVIEWS)	15-11-13
Valhalla (Silkkitle)	97.25% ↑	http://valhallaxmn3fydu.onion/register/E3we	Ref Only	✓	🟡	None	2-5%	1BTC	✓	✓	Yes	Market	★★★★☆ 3.76 (37 REVIEWS)	1-10-13
Hansa Market	98.60% ↑	http://hansamt2rr6nfg3.onion/affiliate/110	Open	✓	🟡	None	3%	0.3BTC	✓	✓	No	Market	★★★★☆ 4.23 (39 REVIEWS)	18-07-15
Outlaw Market	97.62% ↑	http://outfor6jwcztwbpd.onion/indxx1.php	Open	✓	🟡	None	3%	0.1 - 2BTC	✓	✓	Under Conditions	Market	★★★★☆ 3.81 (55 REVIEWS)	29-12-13
Python Market	98.79% ↑	http://25cs4ammearqrw4e.onion/market/task.php?register=1&ref=5164	Open	✓	🟡	None	3%	0.08BTC	✓	✗	With Permission	Market	★★★★☆ 3.99 (64 REVIEWS)	10-7-15
Acropolis Market	98.92% ↑	http://acropol4tl6ytzeh.onion/auth/register/BCBTNUERXY	Referral	✓	🟡	None	3.5%	100\$	✓	✓	Yes	Market	★★★★☆ 3.23 (13 REVIEWS)	6-11-15

➔ HACKERS' SHARE OF PHI BREACHES

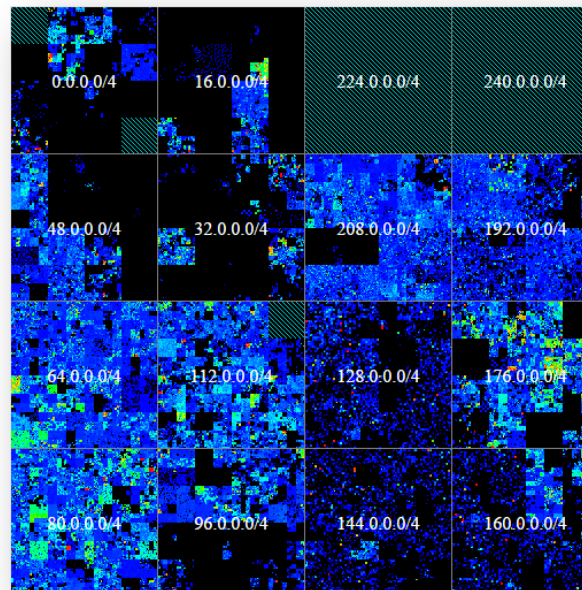




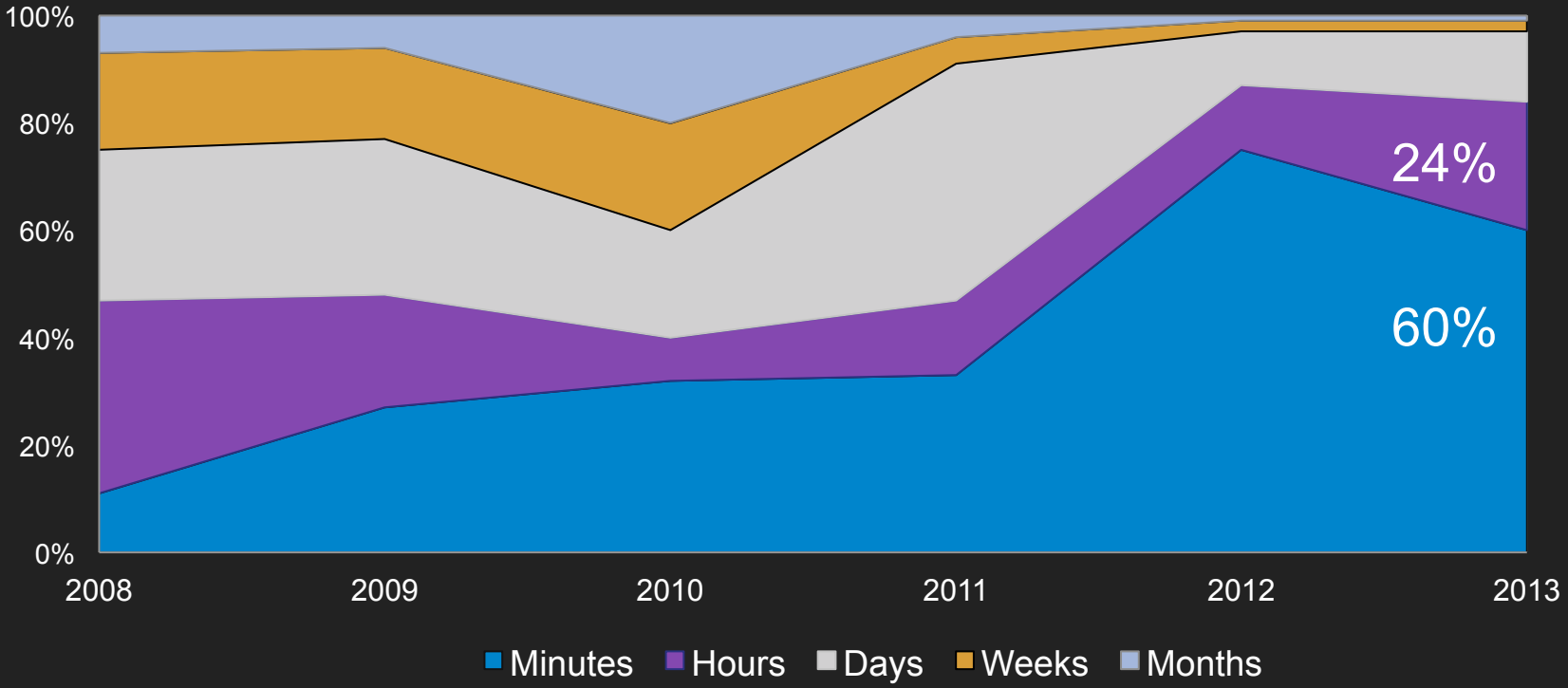
DATA AT RISK

420,000 ROOT:ROOT COMPROMISES
165 MILLION IPs WITH THE TOP 150 PORTS
OPEN & RETURNING DATA

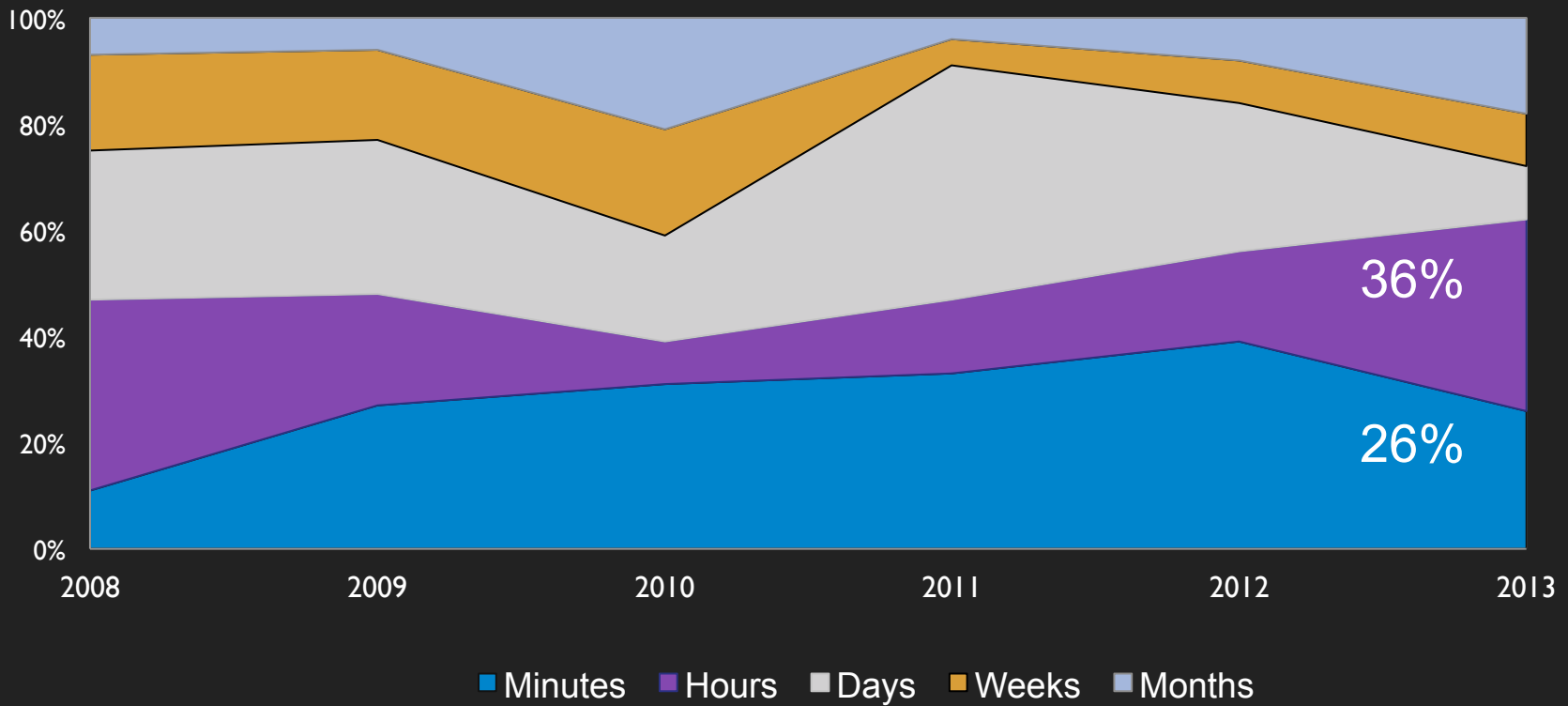
-
- Vulnerability Scans, Fingerprinting
-
- Buffer Overflows, Telnet Sessions
-
- NetBios Audits
-
- Extract Users, Groups, Permissions
-
- FTP - Get and Put Files, Execute Malicious Scripts, etc.



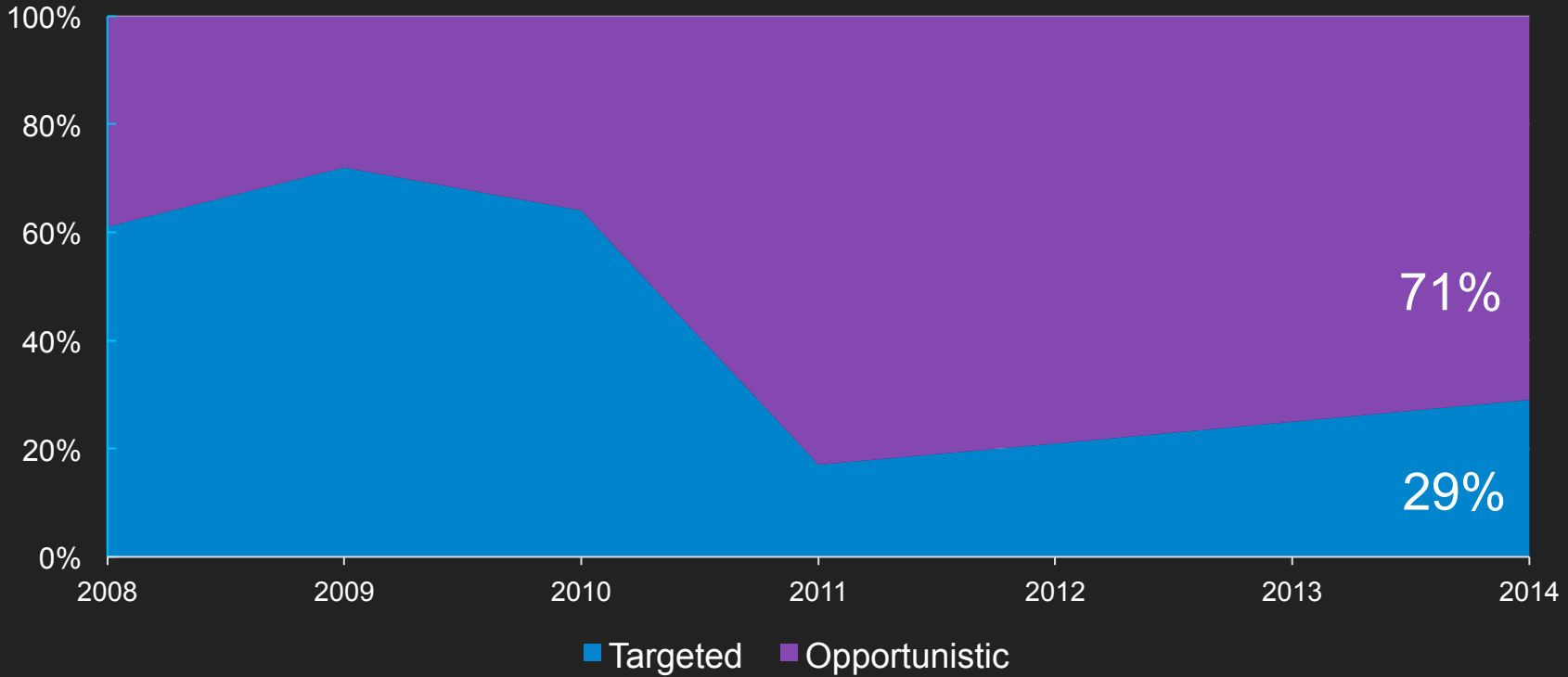
→ TIME FROM ENTRY TO COMPROMISE



→ TIME FROM COMPROMISE TO EXFILTRATION



→ ATTACK TYPE: OPPORTUNISTIC VS. TARGETED





ATTACK TYPE: TRENDING TOWARD MORE TARGETED ATTACKS

Malware searching Hostnames, IPs, etc. for strings:

- Pediatric
- Orthoped
- Nurse
- Hospital, etc.

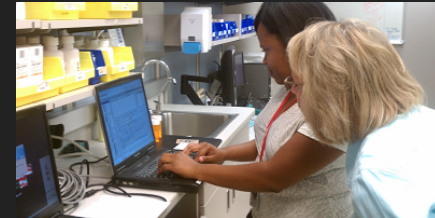
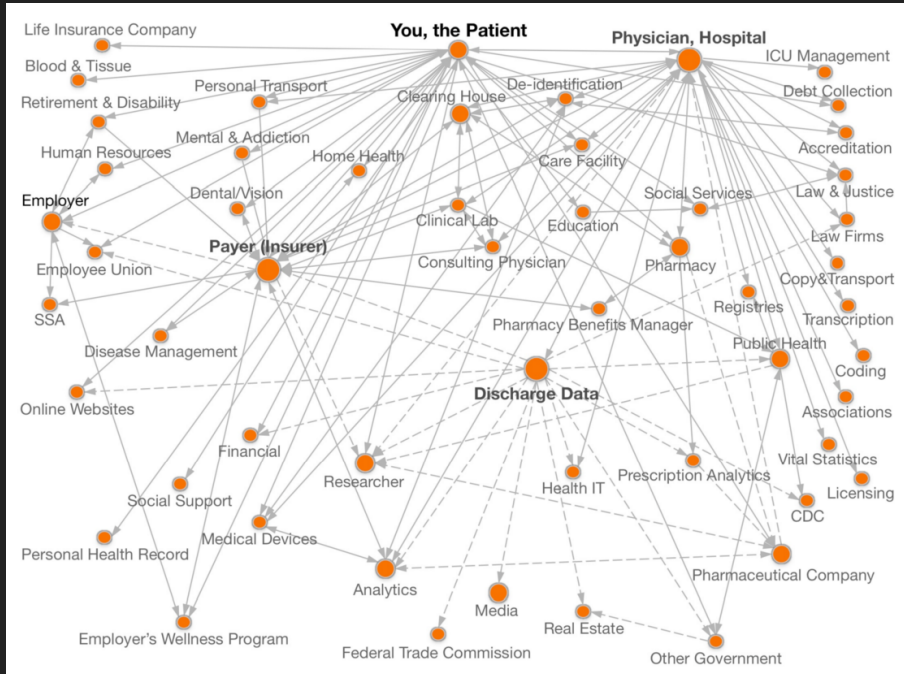
Malware phones home to report if it's a desirable target or not

Increasingly malware designed to use Tor & Hidden Services infrastructure



HEALTHCARE DATA SHARING ECOSYSTEM

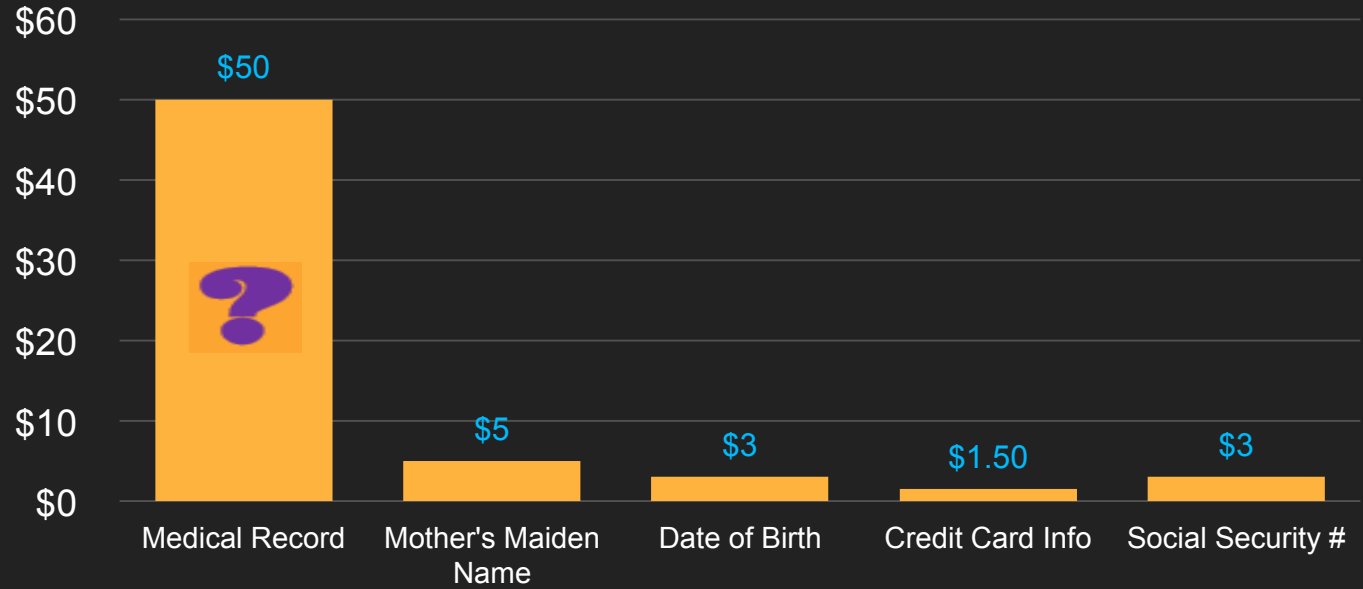
ATTACK SURFACE










MEDICAL IDENTITY THEFT: VALUE OF A MEDICAL RECORD ON THE DARK NET MARKET

Like any market, black market prices fluctuate. Medical records values on DNMs are consistently higher than other FULLZ.

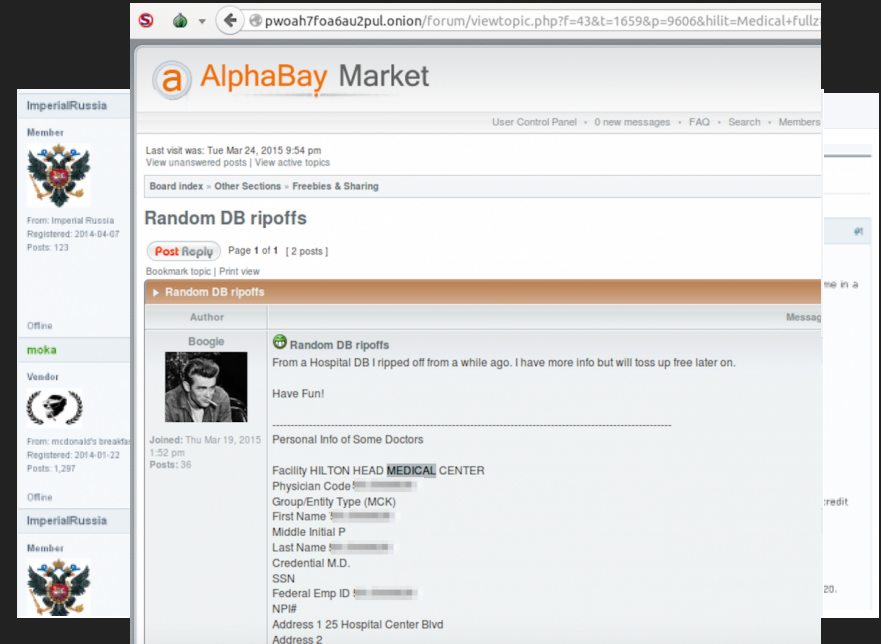


WHAT'S A MEDICAL RECORD REALLY WORTH ON A DNM?

-  Database records from McKesson subsidiary, PST Services showing up on Dark Net Markets 1+ year after breach **\$1 ea**
-  Medical FULLZ **\$10 ea**
-  Medical FULLZ **\$10 – 20 ea**
-  Medicare IDs **\$470 ea**
-  Life Insurance **\$7 ea**



MEDICAL IDENTITY THEFT

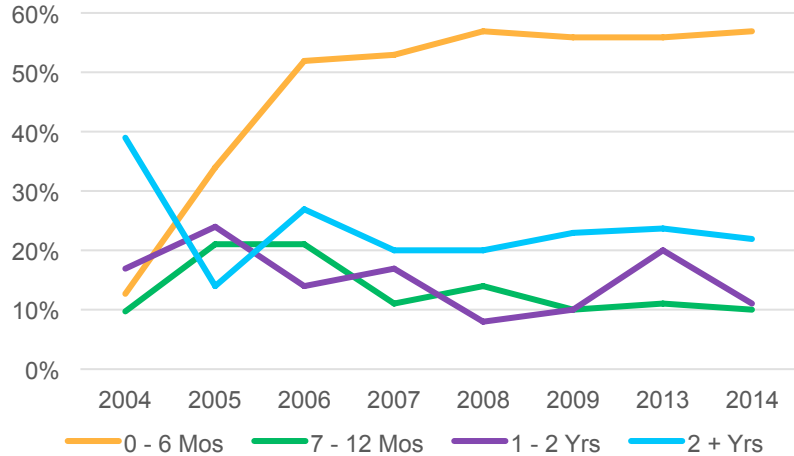


The screenshot shows a forum post on AlphaBay Market. The post title is "Random DB ripoffs" and it is on page 1 of 1. The author is "Boogle". The post content reads: "From a Hospital DB I ripped off from a while ago. I have more info but will toss up free later on. Have Fun!". Below the text, there is a section titled "Personal Info of Some Doctors" which lists details for a doctor at the "Facility HILTON HEAD MEDICAL CENTER". The listed information includes: Physician Code, Group/Entity Type (MCK), First Name, Middle Initial P, Last Name, Credential M.D., SSN, Federal Emp ID, NPI#, and Address (1 25 Hospital Center Blvd).

* KrebsSecurity, Sept. 18, 2014, "Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm"

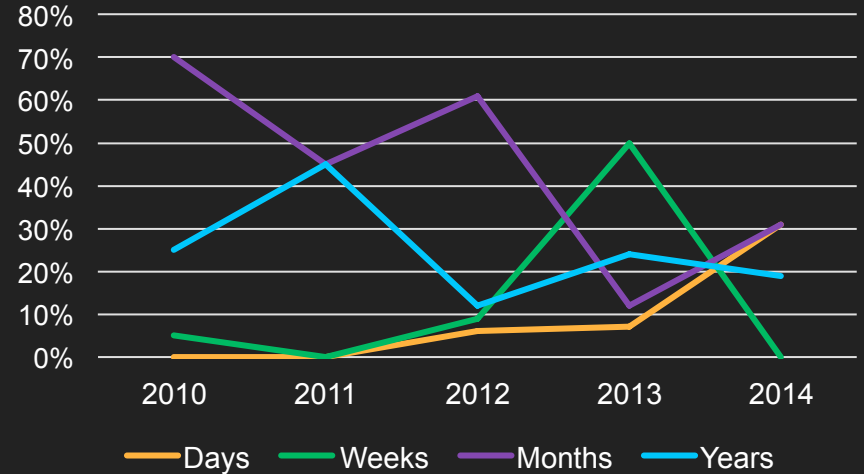
DETECTION LAG TIMES

IDENTITY THEFT - CRIME TO DISCOVERY*



MEDICAL DATA BREACH

COMPROMISE TO DISCOVERY*



* Identity Theft Resource Center, Aftermath Surveys 2003 - 2014

* Verizon, 2015 Protected Health Information Data Breach Report

MEDICAL IDENTITY THEFT (MIT)

- **7M PHI records breached in 2013***
- **12.7M PHI records breached in 2014***
- **2.32M adult MIT victims in U.S. as of 2014****
- **13% of 17.6M Identity Theft victims in 2014†**
- **500,000 MIT victims in 2014****

* U.S. Department of Health & Human Services, OCR "Wall of Shame"

** Ponemon Institute, "Fifth Annual Study on Medical Identity Theft"

† U.S. Department of Justice, Bureau of Justice Statistics, "Victims of Identity Theft, 2014"

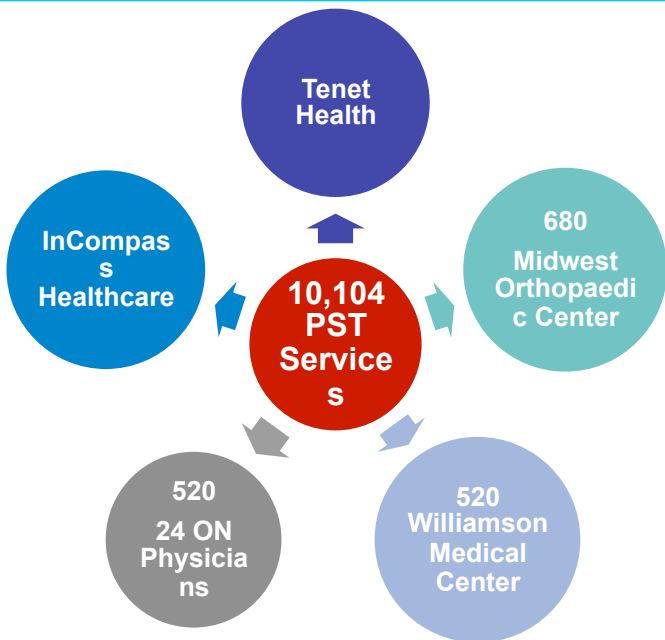
2015

113,258,966 INDIVIDUALS' PHI EXPOSED
268 REPORTED BREACHES

2016 MEDICAL IDENTITY THEFT ?



“To date, we have no knowledge that any of our patients’ information has been accessed or used improperly.”



BITGLASS HONEYPOT EXPERIMENT

- Day 1: 3 logins & 5 logins on portal
- Day 2: Files exfiltrated
- Day 30: 1,400 login attempts 30 countries 5 continents
- !!!: Credentials used on other accounts

ALIGNMENT OF SECURITY & COMPLIANCE

**Healthcare Data Systems are part
of a broader, interconnected
ecosystem**

- **Get to know how & where you
fit within the entire ecosystem**
- **Inform your risk analysis**
- **Align risk and compliance**



HEALTHCARE

DATA SECURITY

COMPLIANCE

EDUCATION

484.858.0427

info@4ASecurity.com

