LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Intelligence Briefing Update
Dark Web PHI Marketplace

OVERALL CLASSIFICATION IS

UNCLASSIFIED

TLP:WHITE

4/11/2019

Agenda

Dark web PHI Marketplace

- Overview
- Dark Web Access
- Stolen Data Worth
- Healthcare Data
- Medical Data Uses
- Stolen PHI Data Path
- Vulnerable Groups
- TheDarkOverlord
- Mitigation
- Conclusions

Image: threatpost.com

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- The dark web enables malicious actors to buy and sell protected health information (PHI) taken from healthcare data breaches.
  - These markets further encourage cyber criminals to attack healthcare organizations for profit.
- Healthcare data is currently one of the most profitable types of data sold on the dark web.
- Using a variety of technologies, criminals are able to access the dark web to anonymously commit illicit activities without fear of repercussions.
- Criminals can support a variety of fraudulent scams and cyber crimes using PHI data purchased from the dark web.
- Hackers on the dark web are interested in countless aspects of a individual's PII, including: health data, (social) media accounts, birth records, financial data, education records, and more.
- Due to the profitable nature of selling PHI data, many sophisticated cyber criminals have focused their efforts on the healthcare industry.
- Organizations must exercise due care in protecting user PHI data, while individuals practice awareness in regards to their personal information.

Layers of the Web

Source: Darkwebnews; CISO

- The internet is divided into three distinct layers
- 90% of the entire internet is composed of the deep web.
- The deep Web and dark Web are often mistakenly used interchangeably.
- The dark web is used for illegitimate activity due to it's obscure nature

Surface Web

- Readily available to the general public
- Searchable with standard web search engines

Deep Web

- Not indexed by standard search engines
- Accessed by direct URL or IP address
- May require authentication for access

Dark Web

- Accessed through "Overlay Networks"
- Mostly encrypted
- Requires special software to access

Dark Web Access

TLP:WHITE

Tor Browser
The backbone of dark web browsing; software encrypts user traffic, allowing anonymous communication.

Tails
Operating system bootable from removable media allows users to browse with a clean OS every session

VPN Services
Mask user IP addresses and make so they appear registered to a different location.

Tools

Dark Web Market

Drugs

Stolen Information

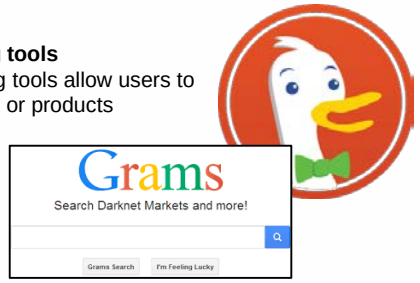
Malware, ransomware and hacking services

Weapons

Hitman-for-hire services

Images: darkwebnews.com

Dark Web Browsing tools
Anonymous Browsing tools allow users to find specific websites or products



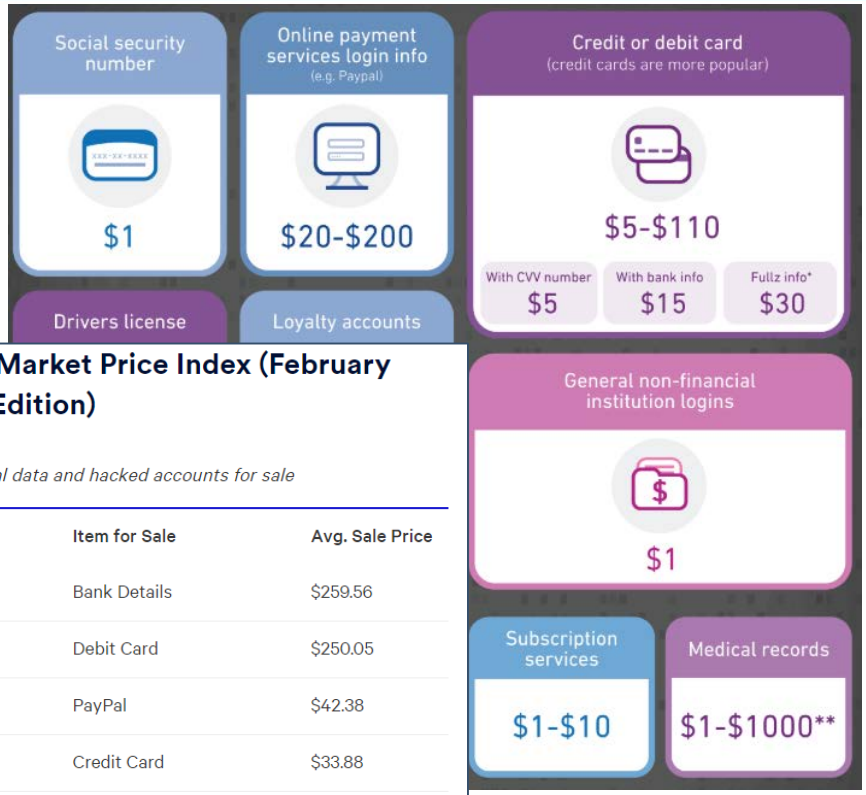
Encryption programs
Allows dark web users to safely communicate and exchange with each other.

Cryptocurrency Exchanges
Allow for the anonymous purchase of dark web services/products.

Source: CSO Online

Stolen Data Worth

- The average person's identity is "worth" $1,170 on the dark web.
  - Includes basic proof of identity, credit and debit information, online banking information, and logins for various social media accounts.
  - "Fullz" Information: full packages of a individuals' identifying information.
- Like a regular market economy, darkweb products/services fluctuate in prices.
- Cyber criminals consider PII a cheap, tradable commodity.
- Other types of sought out info include: Loyalty accounts, diplomas, passports, and any type of login credentials to websites.



Source: Experian, 2017

Dark Web Market Price Index (February 2019 – US Edition)

Stolen ID, personal data and hacked accounts for sale

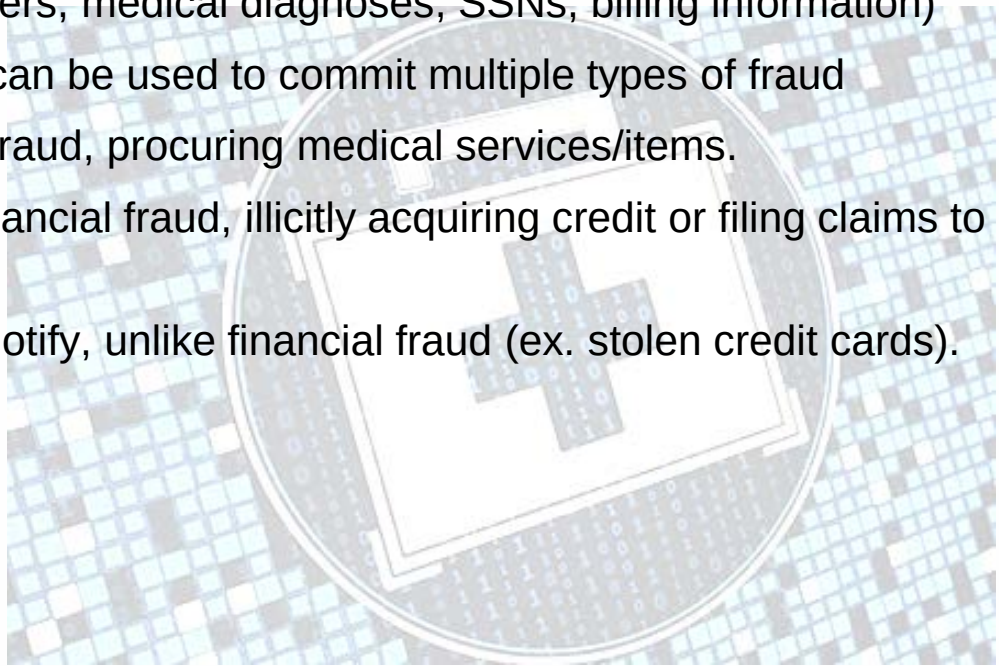
Item Category	Item for Sale	Avg. Sale Price
Personal Finance	Bank Details	$259.56
	Debit Card	$250.05
	PayPal	$42.38
	Credit Card	$33.88
	Western Union	$29.44
	Moneygram	$21.59
Proof of Identity	Driving License	$27.62
	Passport	$18.45
	Proof of Identity	$16.52

Source: Top 10 VPN

Source: Knowbe4

Healthcare Data

- Research indicates healthcare records attract some of the highest prices on the dark web
  - Estimated mean value of healthcare record on criminal markets: **$250** (up to $1000)
  - Patient data is seen as a good source of PII, as so many attributes are stored and the data is more likely to be accurate.
  - Healthcare records often contain information that is harder to cancel and/or recover once stolen (PII, insurance, policy numbers, medical diagnoses, SSNs, billing information)
  - The data found on health records can be used to commit multiple types of fraud
    - Criminals can commit medical fraud, procuring medical services/items.
    - Malicious actors can commit financial fraud, illicitly acquiring credit or filing claims to financial institutions.
- Medical fraud is slower to detect and notify, unlike financial fraud (ex. stolen credit cards).



Source: Duo, Trustwave

Medical Data Uses

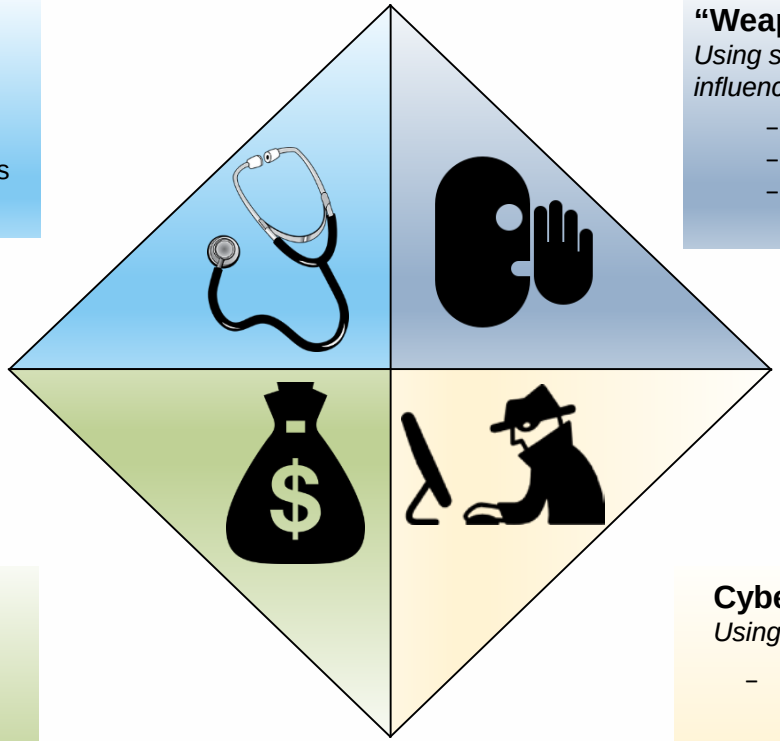
- Medical records purchased on the dark web can be used in a variety of malicious ways

Medical Identity Theft
Utilizing someone else's personal medical information to obtain medical services

- Prescriptions for drugs
- Surgeries and medical procedures
- False medical insurance claims

"Weaponizing" healthcare data
Using sensitive healthcare data to threaten, extort, or influence individuals

- leverage for ransom payments
- Can be real or doctored data
- Public figures and VIPs highly susceptible



Financial Fraud
Using PII in medical records to establish credit/banking profiles for financial gain.

- Healthcare organizations often carry financial data of individuals
- Loans and lines of credit often require data found in medical records
- False tax return claims

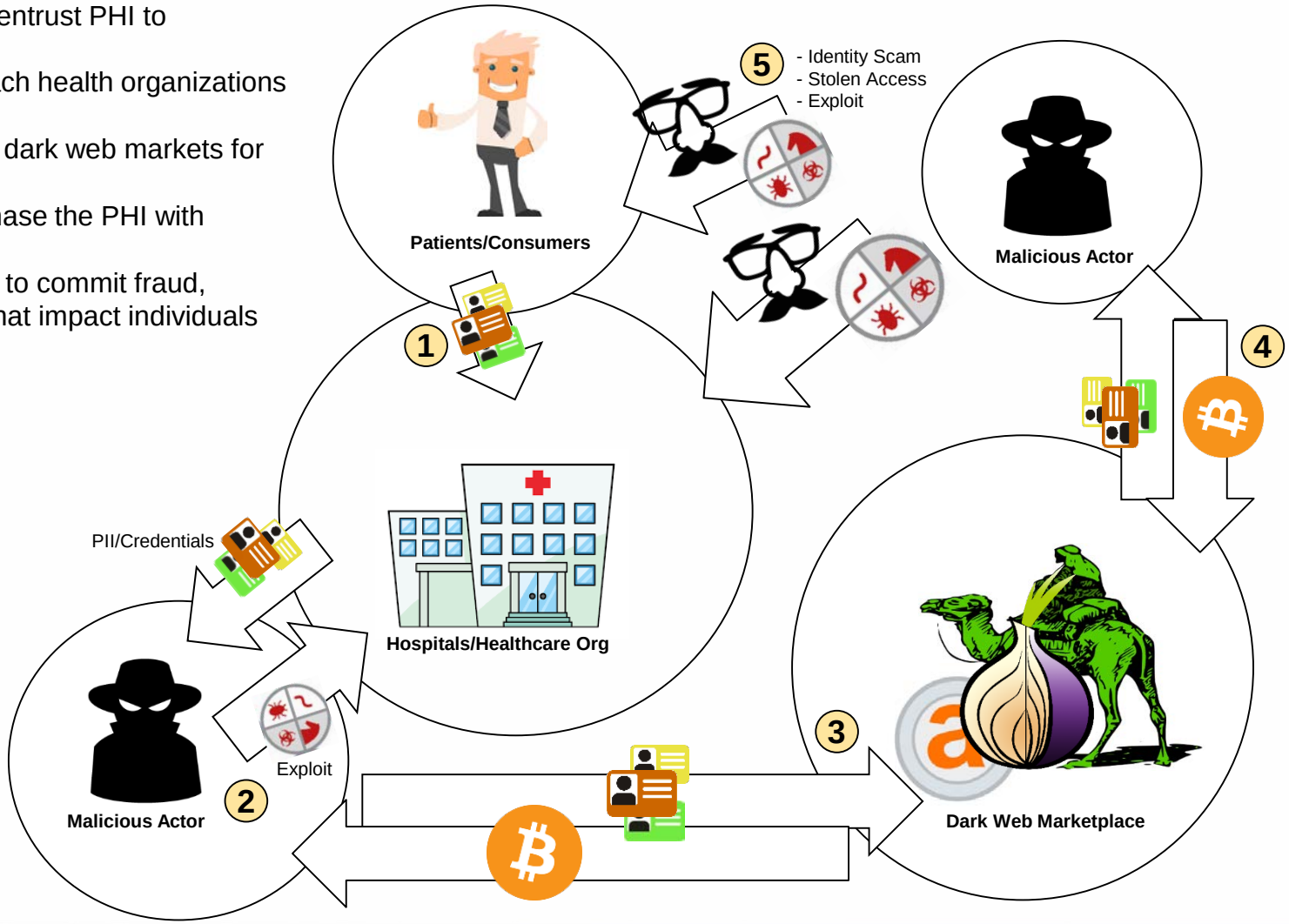
Cyber Campaigns
Using healthcare data to support hacking campaigns

- Contact information can be targeted for phishing and scams
- Credential/authentication information can be used for access/privilege escalation

Source: Mcafee, creditkarma, creditinfocenter

Stolen PHI Data Path

1. Patients/Consumers entrust PHI to organizations
2. Malicious actors breach health organizations to obtain the PHI
3. The PHI is placed on dark web markets for sale
4. Other criminals purchase the PHI with cryptocurrency
5. The PHI data is used to commit fraud, attacks, and scams that impact individuals and organizations



Vulnerable Groups

Malicious actors continue to look for vulnerable groups to exploit for profit on the dark web.

- In dark web markets, the “freshness” of data is an important selling point. (i.e. Data hasn’t been exploited before).
  - Child data is “fresh” by default.
- Lines of credit, loans, and large purchases can be made using child data, unaware to the victim.
- The crime will often not be discovered for 10, 15, even 20 years after.
- Starting with a low-level credit applications, a profile can be established through time, resulting in a massive lines of credit.
- Checks are not in place to stop a child identity from using/establishing credit.

- Malicious actors target elderly demographics due to a vulnerability coined “Age-associated Financial Vulnerability”.
- FTC states that 35% of fraud complaints and 18.9% of ID theft complaints impacted seniors
- Senior living facilities are known to store a plethora of both financial and health information on individuals.
- Elder abuse victims, including those who suffer financial exploitation, die at a rate 3x faster

“I knew these crimes were killing people”
– Elizabeth Loewy, Manhattan District Crimes Attorney’s Office

- Researchers have found many health records listings on the dark web included a death date.
- The deceased have become a safer target as consumer awareness grows
  - The records will rarely be changed and the victims will not file any complaints.
- Deceased identities can be still be used to open credit card accounts, apply for loans, commit tax fraud and purchase large items.
  - Medical identity fraud can still be accomplished with deceased identities as well.

Source: Becker Hospital Review, Zdnet, Bloomberg

TheDarkOverlord

TLP:WHITE

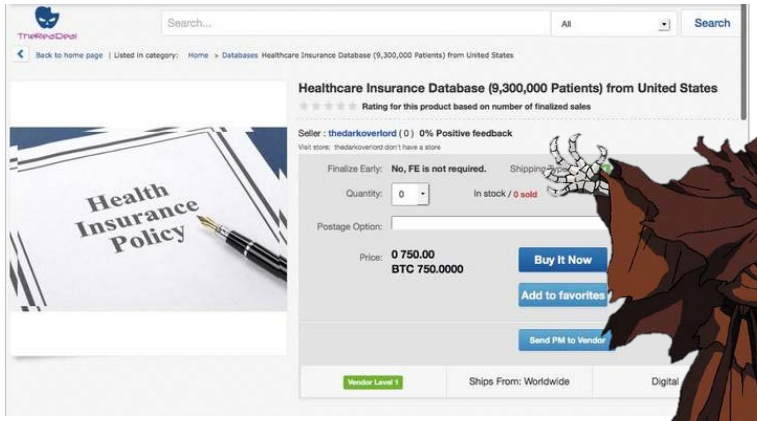
Source: bleeping computer, Bank Info Security

- International cybercriminal group that has often focused on healthcare.
  - Has contributed to hundreds of millions of stolen health records from data base breaches.
  - Known to be very “loud” and active on social media with brags, claims and threats.
  - Sells breached information for profit on the dark web or holds stolen data for ransom.
    - Will send ransom data samples to news-outlets to validate their authenticity.

A member in Serbia was in May 2018

  - TDO continues to recruit on internet job boards: offering salaries up to $762k

- Also known to target education and entertainment organizations



Notable Breaches + Healthcare Organization

SMART Physical Therapy – 16,428 records +
Peachtree Orthopedics – 531k records +
Atlanta Healthcare Database – 396k records +
OrangeCounty Gastrocare – 34k records +
Unnamed MO Healthcare facility – 48k records +
Netflix - $67,000 Ransom demand
Unnamed Central/Midwest Healthcare organization – 210k records +
Cancer Services of East Central Indiana-Little Red Door - $44,800 Ransom demand +
Adult Internal Medicine of North Scottsdale – 11,798 records +
Gorilla Glue – Undisclosed Ransom Demand

Mitigation

- In order to safeguard user PHI from exploitation and comply with HIPAA standards, healthcare enterprises must adopt a defense in depth approach:
  - Deployment of proper network security controls such as firewalls and content filtering software.
  - Utilizing endpoint security software such as antivirus suites and disk encryption
  - Ensuring proper training and awareness procedures are in place for personnel.

- Individual users should monitor sensitive information such as credit, financial information, insurance information, etc.
  - Fraud monitoring services can be beneficial
- Many individuals underestimate the importance of securing PHI data versus financial related data.
  - One should treat medical bills, prescription drug labels and insurance statements as you would any other sensitive information
  - Users should periodically check the accuracy of their medical records.
    - You can have medical records corrected if you find false information

Source: Bankrate

Conclusion

Upcoming Briefs

- LockerGoga Ransomware

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide their feedback to **HC3@HHS.GOV**.

Requests for Information

Do you need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV.**