Beware the Internet's Dark Side: What HIM Professionals and Patients Should Know About the.Dark.Web

By David Gibbs, PhD, CPHI, CHPS, CPHIMS, CISSP; Alexander McLeod, PhD; and Karima Lalani, MBA, RHIA

As the conversation continues among health information management (HIM) professionals about information governance (IG), discussions about privacy and security have been in the spotlight lately. Much of that attention is focused on the "Dark Web," an online marketplace for hackers to sell and buy illegal goods like stolen data, including healthcare records.[1] A scan of literature for information on how the Dark Web impacts HIM professionals showed surprisingly few results and inspired a deeper review.

This article is intended to raise awareness among HIM professionals about risks associated with the Dark Web, such as medical identity theft, ransomware, and medical device hacking. HIM professionals need to be aware that health information is the target of sophisticated cyberattacks from hackers, who then use the Dark Web to profit from their breaches. However, there have also been innovations that have emerged from the Dark Web that could become mainstream solutions for addressing challenges faced by HIM professionals.

What to Know about the Deep Web

It has been known for some time that Internet search results are vastly underrepresented when using traditional search engines. A metaphor some have used for this phenomenon is that of a boat crawling across the surface of the ocean dragging a net, gathering items within the net's shallow reach.[2] While objects are collected near the surface, the ocean is much deeper and most of its contents are outside the reach of the surface-skimming net. The Internet is a virtual ocean, with content distributed through layers, ranging from the illuminated surface to the darkness below. The portion of the Internet that remains out of reach of traditional search engines has been appropriately termed the Deep Web.[3]

Since the early days of the World Wide Web, traditional search engines have provided search-related information based on a process of discovery created by crawling from site to site, collecting and following hyperlinks.[4] This method of indexing links between web pages fails to completely represent the Internet because much of the deep content is dynamically generated or password protected and not readily available to web crawlers.

The Deep Web is intriguing but not necessarily a threat. Being aware of its existence and well-informed about the evolving Internet should be adequate for most people working in the healthcare field. One section of the Deep Web, however, contains a high concentration of threats to healthcare information, healthcare professionals, and patients.

Beware the Dark Web

The dynamic and protected area of the Deep Web enables a darker side of web usage. The Dark Web refers to a subset of Deep Web content that intentionally conceals activities and anti-social information from traditional search engines.[5] Criminal activities take place in this space including markets for child pornography, credit card fraud, identity theft, drug sales, money laundering, digital media piracy, and the sale of stolen medical records. Criminals use tools available from the Dark Web to hide communications and control resources.[6] It is worth highlighting that law enforcement officials, intelligence agents, activists, and journalists use those same tools to protect their identities and transmit data.[7] The Dark Web provides tools that may be used for good or evil, depending on intentions. Without specific instructions, Dark Web content is difficult to discover because it is not accessible via direct queries by traditional search engines or browsers. It can only be queried using secret keywords or passwords and so cannot be indexed.

One of the earliest and most infamous communities of illegal activities on the Dark Web is the Silk Road website, which began operating in 2011 as a one-stop market for illicit drugs.[8] Psychoactive substances are freely discussed and traded in this online marketplace with auctions, ratings, and payment systems easily accessed using anonymous browsers. While the original Silk Road site was shut down by authorities, additional Dark Web sites such as Silk Road 2.0, and later 3.0, emerged to fill the void.[9] To discretely access Dark Web sites such as the Silk Road, special browsers providing anonymity were created.

The illicit portion of the Internet where the exchange of drugs, child pornography, weapons, and stolen medical records take place should be on the radar of healthcare professionals. Being knowledgeable about hacking activities includes being aware that stolen health records are easily traded on the Dark Web and are more valuable than financial records. HIM professionals should vigorously protect their organization's data stores, proactively inform colleagues of best practices for health information privacy and security, train other employees about threats and vulnerabilities, and ensure healthcare systems are hardened to prevent hacking. After all, protecting the confidentiality and integrity of health information is a core element of information governance.

What to Know about Tor and Onion Routing

One of the technologies commonly associated with the Dark Web is Tor, the name of a network of servers and an open source web browser originally developed by the US Naval Research Laboratory to enable secure, anonymous online communications.[10] Although initially named to show its association with onion routing, Tor is now the proper name and is not an acronym.[11] Onion routing is a way for data to be transmitted across the Internet anonymously, meaning the data cannot be traced back to its source. Rather than traditional direct connections between source and target servers, which are traceable, onion routing uses multiple layers of encryption and encapsulation that are "peeled" away as the data is routed through multiple intermediary servers called onion routers. Imagine peeling away the layers of an onion as it passes hand-to-hand among a series of people. The person at the end of the line will not know the identity of the person who initially introduced the onion and there will be no "fingerprints" from that first person remaining.

A modified version of the open source Firefox browser, Tor Browser is compatible with Windows, Macintosh, Android, and Linux operating systems. Other developers have created similar browsers for iOS. These browsers were designed to provide anonymity when traversing the Internet. This high level of obscurity is not necessary or appropriate for most HIM work settings and introduces complexity and slower performance. HIM professionals should be aware of Tor and similar browsers and work with information technology professionals to guide appropriate policies for browser use in their organization. In many environments, information technology teams have network administration tools that control or monitor software installed on each workstation. Administrators can also monitor facility networks for connections to questionable Internet systems. HIM professionals should validate that any installations of Tor or similar browsers are justified and not used to compromise protected health information (PHI).

What to Know about Bitcoin Digital Currency

While Tor and comparable tools effectively enable private Internet communications, financial transactions using traditional methods such as credit cards or wire transfers are not anonymous. Dark Web users desiring anonymity in financial transactions were among the drivers for the development of Bitcoin.

Bitcoin is a digital currency created in 2009 that avoids traditional banking institutions to transfer funds using real or assumed identities, enabling anonymity for financial transactions.[12] The majority of Bitcoin users are law abiding people desiring anonymity or simply curious about using the digital currency.[13] However, Bitcoin is also the currency of choice for criminal activity on the Dark Web. Use of Bitcoin, like cash, is not an indicator of criminal activity, but is popular with criminals due to its anonymity. For example, Silk Road enthusiasts avoid law enforcement by using hidden Dark Web services and Bitcoin to side-step government monitoring and create serious challenges to drug control policies.[14]

The use of Bitcoin for payments on the Dark Web also extends to stolen medical records. In 2016, a hacker known as "thedarkoverlord" offered for sale 655,000 stolen health records, complete with victims' Social Security numbers, names, addresses, birth dates, medical diagnoses, family history, surgical history, vital statistics, and more.[15,16] Three US-based healthcare organizations were targeted to acquire this data by exploiting software vulnerabilities on computers connected to the Internet. The asking price for these stolen records was $716,000 in US dollars and the payment method specified was

Bitcoin. This offer was openly advertised on the website DeepDotWeb.com, with screenshots of data to demonstrate possession of the records. Using an unpublished vulnerability in remote desktop software, the hacker located and copied the electronic health records (EHRs) from the three healthcare organizations. Two days later, the same hacker offered for sale 9.3 million healthcare records stolen from an insurance database.

According to Clearwater Compliance, a cybersecurity vendor, the market pricing for medical records on the Dark Web in 2016 was $60 per complete medical record, much more than stolen financial information.[17] Cybersecurity professionals believe that creation of this type of criminal market for patient medical records will continue to expand.

The Dark Web marketplace for stolen medical records adds another level of complexity to the cybersecurity threats facing healthcare organizations. Healthcare is especially susceptible to cyberattack because employees deal directly with the public and because some healthcare organizations are lagging behind with implementing stringent cybersecurity measures.[18] The Dark Web provides a marketplace for those with the intention to sell illegal materials, and HIM professionals need to understand that criminals create markets to sell information contained in healthcare records. HIM professionals have a responsibility to protect the identities and data of patients. Dark Web activities should continue to motivate HIM professionals to maintain high information privacy and security standards in their organizations. For example, HIM professionals should work with cybersecurity experts to ensure software patches are current, risk assessments are performed routinely, and any vulnerabilities are addressed swiftly and effectively.

What to Know about Ransomware

While stealing medical records and selling them to criminals is lucrative, another growing scheme is holding electronic health records hostage and selling access to the records back to their legitimate custodian. Known as ransomware, this form of cybercrime is enabled by the anonymity of the Dark Web. Ransomware attacks are often carried out via phishing e-mails originating from automated Dark Web sources. E-mails that appear legitimate entice users to click on a link or an image that secretly installs malicious software on their computer. The malicious software encrypts data using secret keys known only by the hackers, rendering the data unavailable. A window will then appear on the affected computer demanding payment, often in Bitcoin, to regain access to the data which has been held at ransom. Ransomware attacks on healthcare organizations put lives as well as reputations in jeopardy. The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) provided clear guidance in July 2016 that having ransomware or any malicious software on a computer of a covered entity or a business associate is a security incident according to the HIPAA Security Rule.[19] Having healthcare information unavailable for even a few hours could harm both patients and the healthcare organization.[20] Ransomware is on the rise and specifically targets healthcare workers due to the high financial impact and perceived weakness of security and training across the healthcare industry.[21] HIM professionals are especially at risk of being targeted due to having extensive access to PHI.

Ransomware incidents vary from simple scareware, to malware removable by virus scanners, to complex variants that are extremely difficult to resolve. Scareware involves a threat to encrypt data or a false claim to have already done so. HIM professionals should work with their information technology professionals to provide training to users concerning backups and proper e-mail use to avoid ransomware problems. Also, users should be provided policies and procedures on how to react to ransomware.

Risks to Medical Devices

The reach of cyberthreats began to extend into the physical world in June 2010 with the emergence of the Stuxnet computer worm. Prior to Stuxnet, the cyber world was generally considered separate from the physical world. Stuxnet forever bridged cyberspace and the physical world by demonstrating that malicious software can cause physical harm. Designed to replicate itself onto every Microsoft Windows computer it encounters on a network, Stuxnet also can infect isolated computers via USB memory sticks, meaning that computers on networks not connected to the Internet can be compromised. When the original Stuxnet found its target systems, it reconfigured the operating parameters of mechanical equipment causing physical damage and destruction.[22] The cyber and physical worlds are no longer separate.

Computers are embedded in and control today's implanted and wearable medical devices. For example, insulin pumps and cardioverter defibrillators are controlled by software, and therefore are vulnerable to attack.[23] In 2011, a security researcher demonstrated his ability to hack an insulin pump via a wireless network and alter the insulin dosage to levels that could be

lethal.[24] A real-world breach occurred targeting laboratory systems at a hospital, demonstrating the potential to alter or corrupt lab results.[25] Implanted medical devices commonly use wireless communication for configuration information. An attacker with knowledge of how devices communicate could accelerate the battery drain forcing surgical replacement, or worse.[26] These examples are provided to show how cybercriminals and their tools lurking on the Dark Web have a direct impact on patients and healthcare professionals.

Over the last 50 years there has been an increase in the use of computers in medical devices, such as cardiac defibrillators, cardiac pacemakers, and insulin pumps. And with the growth of wireless technology, the use of these devices is expected to expand in the coming years.[27] The benefits and conveniences associated with medical devices also comes with risks of hackers accessing these systems to steal patient information or cause harm to patients. As risks continue to evolve, more concerted efforts to secure medical devices will continue to be warranted among device manufacturers, medical researchers, medical providers, and computer security experts. HIM professionals involved in information governance are well positioned to bring attention to these risks among their healthcare colleagues.

One of the first steps HIM professionals can take with regard to medical devices is to ensure all devices have default passwords changed. Default passwords assigned by manufacturers of devices are published online and easily obtained by hackers. The Internet of Things (IoT) provides opportunities for hackers to exploit vulnerabilities in those organizations that have not changed default passwords. HIM professionals should also educate colleagues about these threats.

What to Know about Blockchain

Since one of the objectives of Bitcoin was to avoid traditional banking infrastructure, the creators had to develop their own highly reliable and secure system for tracking transactions. Bitcoin introduced an innovative supporting technology called blockchain to manage its own distributed financial ledger using decentralized computing resources.[28] It turns out the way blockchain works to secure financial transactions may also be useful for securely maintaining and sharing electronic health records. Timing and sequencing of transactions are critical to finance. For example, funds must first be deposited into an account before being transferred out. One of blockchain's strengths is maintaining integrity and sequence of transactions to avoid fraud.

Electronic health records have a similar need for integrity and time sensitivity. One way to think about the longitudinal continuum of care for an individual patient is a series of transactions including birth, diagnoses, laboratory tests, administration of medicine, clinical procedures, etc. Maintaining a secure and accurate history of transactions is precisely what blockchain was designed to do. It seems natural to explore how blockchain could be used as a platform for storage and exchange of electronic health records. In fact, HHS saw sufficient potential that it sponsored a blockchain challenge competition in 2016 to encourage vendors to propose ways to apply blockchain for health IT and health research. The competition resulted in fifteen winners with some very promising proposals.[29] HIM professionals should continue to explore blockchain.

Dark Web Creates and Solves Risk

The Dark Web refers to regions of the Internet which are not illuminated by mapping or indexing, and therefore are not exposed by traditional search engines. These regions contain a variety of information services and tools used by people on both sides of the law desiring to maintain privacy. While the Dark Web remains a source of high risk for patients and HIM professionals, it has also provided innovations and tools that may be useful to HIM professionals working to enable secure storage and exchange of electronic health records. Blockchain is a prime example as it has strong potential application for healthcare and deserves deeper understanding by HIM professionals. Knowing the potential the Dark Web holds to potentially hurt HIM is the first step in being proactive to protect against it.

Notes

[1] Reeves, Mary. "Create a Learning Environment for Information Governance." *Journal of AHIMA* website. July 28, 2016.

[2] Bergman, Michael K. "White Paper: The Deep Web: Surfacing Hidden Value." *The Journal of Electronic Publishing* 7, no. 1 (2001): 1-35.

[3] He, Bin; Mitesh Patel; Zhen Zhang; and Kevin Chen-Chuan Chang. "Accessing the Deep Web." *Communications of the ACM* 50, no. 5 (2007): 94-101.

[4] Bergman, Michael K. "White Paper: The Deep Web..."

[5] Weimann, Gabriel. "Going Dark: Terrorism on the Dark Web." *Studies in Conflict and Terrorism* 39, no. 3 (2016): 195-206.

[6] Weimann, Gabriel. "Terrorist Migration to the Dark Web." *Perspectives on Terrorism* 10, no. 3 (2016): 40-44.

[7] Ibid.

[8] Van Hout, Marie Claire and Tim Bingham. "'Silk Road', the Virtual Drug Marketplace: A Single Case Study of User Experiences." *International Journal of Drug Policy* 24, no. 5 (2013): 385-391.

[9] Chaudhry, Peggy E. "The Looming Shadow of Illicit Trade on the Internet." *Business Horizons* 60, no. 1 (2017): 77-89.

[10] Weimann, Gabriel. "Terrorist Migration to the Dark Web."

[11] The Tor Project. "Tor."

[12] Carmona, Anais. "The Bitcoin: The Currency of the Future, Fuel of Terror." *Evolution of Cyber Technologies and Operations to 2035*. Switzerland: Springer, 2015: 127-135.

[13] Bohannon, John. "Why Criminals Can't Hide Behind Bitcoin." Science. March 9, 2016.

[14] Barratt, Monica J.; Simon Lenton; and Matthew Allen. "Internet Content Regulation, Public Drug Websites and the Growth in Hidden Internet Services." *Drugs: education, prevention and policy* 20, no. 3 (2013): 195-202.

[15] Reeves, Mary. "Create a Learning Environment for Information Governance."

[16] Dyer, Owen. "Medical Data of 655,000 Americans Put Up for Sale by Hacker." *BMJ: British Medical Journal* 353, no. 1 (2016): 1.

[17] Goedert, Joseph. "Active Market for Healthcare Records Looms as Newest Cyber Threat." *Information Management*. July 12, 2016.

[18] Solander, Adam C.; Adam S. Forman; and Nathaniel M. Glasser. "Ransomware—Give Me Back My Files!" *Employee Relations Law Journal* 42, no. 2 (2016): 53-55.

[19] Department of Health and Human Services. *Fact Sheet: Ransomware and HIPAA*. 2016.

[20] Solander, Adam C. "Ransomware—Give Me Back My Files!"

[21] Butler, Mary. "Ransomware and Hacking Attempts against Healthcare Expected to Increase in Severity, Scope." *Journal of AHIMA* website. November 21, 2016.

[22] Kushner, David. "The Real Story of Stuxnet." *IEEE Spectrum* 50, no. 3 (2013): 48-53.

[23] Zhang, M.; A. Raghunathan; and N. K. Jha. "Trustworthiness of Medical Devices and Body Area Networks." *Proceedings of the IEEE* 102, no. 8 (2014): 1,174-1,188.

[24] Radcliffe, Jerome. "Hacking Medical Devices for Fun and Insulin: Breaking the Human Scada System." Black Hat Conference presentation slides, Las Vegas, NV, July 30 to August 4, 2011.

[25] Butler, Mary. "Ransomware and Hacking Attempts..."

[26] Zhang, M. "Trustworthiness of Medical Devices and Body Area Networks."

[27] Leavitt, Neal. "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers." *Computer* 43, no. 8 (2010): 11-14.

[28] Azaria, A., A. Ekblaw, T. Vieira, and A. Lippman. "MedRec: Using Blockchain for Medical Data Access and Permission Management." *International Conference on Open and Big Data (OBD)*, Vienna, Austria, August 22 to August 24, 2016.

[29] Department of Health and Human Services. "Use of Blockchain in Health IT and Health-related Research Challenge."

David Gibbs (dgibbs@txstate.edu) is an assistant professor, department of health information management, and Alexander McLeod (am@txstate.edu) is an assistant professor, department of health information management, at Texas State University. Karima Lalani (KL32@txstate.edu) is a lecturer in the health information management department at Texas State University and a PhD student at the UTHealth School of Public Health.

Article citation:
Gibbs, David; McLeod, Alexander; Lalani, Karima. "Beware the Internet's Dark Side: What HIM Professionals and Patients Should Know About the.Dark.Web" *Journal of AHIMA* 88, no.8 (August 2017): 30-33,52.