message from the board

Mid-Columbia Members,

Happy Holidays!

November has come and gone and we are already in our last month of the year! We hope you enjoyed last month’s topic on conflicts of interest. It is always a good idea to refresh on those sometimes broad or grey area topics.

Although the Fraud article below is long, it is a good one; highlighting the different parts of the internet and how it could relate to your life both at home and at work. With the constant rise in technology it is always a good idea to be aware of how fraudsters can and will compromise information.

See you back at the Richland Public Library for this month’s luncheon.

Have a great month and happy auditing!

Mid-Columbia Chapter Board Members

JOIN US - SAVE THE DATE:

Excel – Supercharge Your Spreadsheet Abilities by Steve Hunt

When: April 7, 2020
Time: 7:30am to 4:00pm
Upcoming Luncheon

“Auditing in a Safe Work Environment – An Active Shooter Training”

Captain Sam Hernandez

Thursday, December 19, 2019

11:30 – 1:00 (lunch provided)

Location: Richland Public Library
955 Northgate Drive
Doris Roberts Gallery

CPE: 1.0

RSVP to Susan Rodabaugh

CPE Fee: Free CPE for IIA Members! $15/ea. for Non-Members; first time attendance by a Non-Member is free. Members and Non-Members that RSVP and do not attend will be charged a $15.00 fee. The CPE fee will be collected at the door upon arrival.

About the Speaker

Captain Sam Hernandez has 32 years with Hanford Patrol and is Nationally Certified as an Active Shooter Instructor.

Page Content

WHAT’S IN THE NEWS?

THE TRUTH ABOUT THE DARK WEB FRAUD TRADE

By: Emily Wilson, CFE

In February 2016, someone with the username “dogdaygod” approached a site on the dark web ostensibly run by Albanian gangsters looking for a hitman. The site, Besa Mafia, said the hit would cost $6,000. According to a Vice article by Joseph Cox, dogdaygod told Besa Mafia where the target would be traveling. After some back and forth, Besa Mafia said their hitman was caught and in police custody, which would delay the job. The group asked for another $12,000. (See A Fake Dark Web Hitman Site is Linked to a Real Murder, Vice, Feb. 23, 2017.)

But in May 2017, a hacker published Besa Mafia’s customer hit list and revealed the site as a fraud. Dogdaygod never got what he paid for from Besa Mafia because it was an elaborate scam designed to extort the money of potential clients with enough leverage from their hit requests to stop them from going to the police over the lost funds.

The dark web, often inaccurately portrayed as a playground for hitmen and human traffickers, is a place where fraudsters leverage tools, tactics and technology to build scalable business models, collect and co-opt sensitive data, and exploit organizations around the clock.

Internet divided into thirds

To understand the dark web, consider internet content existing in three segments: the clear web (or surface web), the deep web and the dark web. The clear web is the traditional, easily navigated internet content accessible through all standard browsers and technology. When someone visits The New York Times homepage or looks for movie show times, they’re engaging with the clear web. Search engines, like Google, crawl (or index) the clear web to smooth users’ navigation.
The deep web consists of content search engines can’t index — this includes material that’s accessible only behind login pages or on websites that have restricted or blocked search engines from indexing their contents. When we log into bank or social media accounts, for example, the content available to us as registered users is the deep web. Pages or sites that request not to be indexed or are designed so a crawler can’t navigate their contents (e.g., a page that might require extended user interaction to access materials) are also part of the deep web.

The dark web’s content on the internet isn’t accessible through traditional browsers or standard browsing technology. Content on the dark web is designed to be hidden from search engines and from casual users — we can’t simply stumble across dark web sites by accident.

The dark web, compared to the billions of sites available on the clear and deep web, comprises just tens of thousands of sites, and only a limited number of those sites are available at any given moment.

Peeling back layers of an onion
When a user visits a website on the clear web or the deep web, the user’s browser will send a request from their IP (Internet Protocol) address to the website asking for the content. The content is delivered back to the user, and the website stores a record of the request from that IP address. IP addresses are tied to location information, so the website now can see where the user is accessing the website (e.g. Austin, Texas).

This information exchange allows website tracking services (like Google Analytics) to measure volume and traffic frequency from different locations. Traditional browsing also creates records of site visits with internet service providers and digital advertising agencies, which they can use for marketing campaigns. That’s why we see ads on social media for items we’ve previously viewed on other sites.

Dark web browsing technology, like the Tor network, prevents this type of user tracking. The Tor network, accessible through the Tor browser, allows users to access the dark web with encrypted routing technology. Users also can employ the Tor browser to travel the clear and deep web anonymously with the same dark web routing technology — it anonymizes traffic and location information for each of its users.

So, if a user visits a website with the Tor network, the request won’t come directly from Austin, Texas, but will instead route through a series of “nodes” — traffic might go through Switzerland, Canada, Germany and France before being finally routing to the site. Traffic isn’t only routed through a number of sites, but the request to visit the website is also encrypted several times over — like layers of an onion, which is where the Tor (the onion router) gets its name. The nodes operate independently so no one can know where traffic originated or where it’s going. Only the final node knows that it needs to make a request to visit the website. Once the website’s been accessed, the encrypted routing process happens all over in reverse.

Tor technology also provides access to dark web sites, known as Tor hidden services. These sites are hosted within the Tor network and are accessible only via the Tor browser. Because these sites are hosted within the Tor network, they’re difficult to locate unless a user already knows the address, and are even more difficult to investigate or take down. They’re colloquially called “onion sites” — instead of ending in .com or .org, the addresses end in .onion, as a nod to the Tor Project’s original namesake.

What and why of the dark web
The dark web is home to a hundreds of different communities and hosts a wide variety of site types — medical forums, political parties, graphic design firms, anime fan gatherings and more. It contains mirrors of clear websites, like The New York Times and Facebook, each with their own .onion address. It’s a place of anonymity, but that doesn’t immediately equate to criminality. The dark web is a privacy tool, designed with user security and anonymity in mind. Security and privacy are neutral goals — they’re as beneficial to legal communities looking for protection as they are to criminal communities looking for a way to hide.

Research conducted by Terbium Labs in 2017 showed that 47.7% of site content across Tor hidden services is legal — other numbers in the industry closely match this stat. (See Separating Fact From Fiction: Legal Content on the Dark Web, Terbium Labs.)

The dark web can provide safety for whistleblowers or for those who want or need access to information that’s blocked in their home countries. This can range from media content, work by the international free press, and medical services or community groups that are illegal or highly charged in their home countries (e.g., abortion or mental health services, women’s rights, LGBTQ communities).

However, the anonymous setup of the dark web does allow for thriving criminal enterprises that deal in drugs, fraudulent materials, weapons and child exploitation.

Criminal enterprises that trade in fraudulent materials tend to focus on personally identifiable information (PII), customer or employee data, counterfeits and templates, access guides, credentials and financial details. The criminal portions of the dark web operate on a stable and standardized economy, which makes the trade in fraudulent information easy and accessible. Unlike some portions of the dark web that go out
of their way to stay hidden, criminal enterprises often operate to turn a profit, which necessitates a slightly more open operation to ensure that buyers can locate the markets.

**Dark web fraud trade**

Previously, dark web transactions relied on payment processors like PayPal and Western Union to pay for goods and services. Those services required a certain level of user information to transact, and law enforcement leveraged those user details to arrest buyers and vendors. This isn't a sustainable system for building a large-scale criminal economy. Cryptocurrency changed everything.

Within the criminal communities on the dark web, fraudsters have built entire e-commerce platforms designed to trade in illicit goods and services. The infamous Silk Road marketplace, launched in 2011, was the first market to combine the anonymizing dark web technology with the power of anonymous cryptocurrency transactions. (See *Silk Road: A Cautionary Tale about Online Anonymity*, by Marcell Nimfuer, Aug. 18, 2018, Medium.)

Silk Road became a model for all future dark web marketplaces. At any given time, a handful of large-scale criminal marketplaces operate on the dark web, each with thousands to tens of thousands of listings for illicit goods and services. These marketplaces use familiar site structures, akin to the user experience of browsing on Amazon or eBay. On these markets, users can browse listings by category, navigate vendor advertisements, filter their search options by price, location or vendor reviews, and message the vendors or market administrators with questions.

These marketplaces — like Empire and Berlusconi — rely on mutual anonymity and reputation. Vendors encourage positive reviews for their products and prioritize customer service, offering to troubleshoot software or to replace defunct digital goods. In exchange for these efforts, vendors receive reviews and “vendor trust level” rankings, which helps them capture more market share for their particular good or service.

Established platforms allow vendors — particularly fraud vendors dealing in digital goods — to automate and scale their operations. Many fraud vendors use an auto-delivery mechanism for their listings, which ensures buyers receive the volume of data purchased immediately after checkout. In this way, vendors can continue to turn profits and move inventory around the clock.

Additionally, criminals have created a wide range of fraud forums and independent shops. Many independent fraud shops are dedicated entirely to the sale of compromised payment cards (like the famous release of payment cards from the Target breach). Buyers can filter listings on a range of card-specific attributes (e.g., issuing bank, expiration date) and receive discounts for buying data in wholesale quantities. Forums provide a marketing and networking platform where vendors can promote links to their goods and services, and interface with customers. Forums also give fraudsters a platform to request specific goods and services, whether they’re seeking access to specific types of financial data or are looking for partners to assist in money laundering.

The dark web fraud economy follows the same economic patterns as traditional commerce: New vendors enter the scene promising differentiated value from their competitors, established shops announce holiday sales and new inventory, and buyers — determined to destroy the reputation of the responsible vendors — take to the platform expounding negative experiences and scams.

These established platforms and economic flows speak to the maturity and resilience of the dark web fraud economy. Media often paints dark web interactions as code-based interfaces in darkened rooms where transactions occur through the digital equivalent of back-alley trades. However, the reality is far more mundane and familiar — and all the more concerning for its practicality.

**What are criminals buying?**

After drugs, fraud materials are the most popular listings on dark web markets. Fraud materials fall into five main categories: personal data, financial data, guides and templates, software and fraud services.

**Personal data**

The dark web fraud economy is built on compromised data, and the steady stream of breaches and exposures have contributed to the proliferation of personal data on the markets. Vendors sell everything from music-streaming accounts to credit reports, health records to full identity kits containing complete sets of personal and financial information.

Some fraudsters also openly leak PII — free for anyone to use or exploit. Long lists of usernames and passwords, email addresses or contact information float freely around the dark web. Users repackage and remarket data from different sources over time; fraudsters might sell or leak the same data set hundreds of times over, and each new leak or sale increases the risk to the individuals or organizations involved.

**Financial data**
Financial data on the dark web typically appears as payment card information, banking information or payment processor accounts. Unlike personal data, financial details aren’t leaked quite as frequently. PII allows fraudsters to carry out a wider range of fraud schemes over time, but financial information offers immediate cash-out opportunities — financial accounts are typically shut down as soon as an unauthorized transaction takes place. Vendors typically safeguard full card numbers until after buyers make a purchase, and any fraudster in possession of financial data would extract all monetary value from the accounts before sharing remaining details with the broader fraud community.

Payment processor accounts and other financial data, like gift cards or money orders, allow fraudsters to launder money and pay mules through alternative networks.

Guides and templates

Dark web markets go beyond simply offering personal and financial details for sale. Vendors also offer guides and templates to better facilitate fraudulent activity. Guides contain detailed instructional kits for fraudsters that offer step-by-step tutorials on popular fraud schemes, including phishing, account takeover, business email compromise, tax fraud and how to cash out on stolen payment cards.

These guides are effectively recipes for the fraud community that provide lists of raw materials, sets of instructions and authors’ guidance for specific tips and tricks to achieve the best possible results. Some guides offer exclusively technical information, but many also provide recommendations for the social engineering aspects of fraud, such as how to speak to customer service representatives, managers, bank tellers and other associates they might need to interact with over the course of their fraud scheme.

Guides range from general information on how to execute fraud schemes to specific, targeted recommendations on how to defraud a given financial institution, retailer or other organization. These guides represent institutional knowledge developed within the fraud community over the last several decades. They’re another example of the maturity and development of the digital fraud economy. Schemes have become so practiced and sufficiently standardized that vendors can record their tactics and profit from the sale of that knowledge.

Software and fraud service

Vendors also offer software and fraud services on the dark web. Software can be legal, mass-market tools (like Adobe Photoshop, which is used to edit or manufacture fraudulent documentation) to makeshift programs or custom scripts from vendors.

Phishing schemers buy pre-made scam pages to convince users they’re visiting a legitimate website. These scam pages come loaded with the technology needed to capture account details when unsuspecting users interact with the page.

Some vendors offer fraud services as a compliment to their existing data listings. One vendor selling PII offered an additional look-up service, for a fee, if users wanted to track down the drivers’ license numbers for stolen identities they’d purchased. These value-add services expand a vendor’s potential profit.

Other vendors offer unrelated services, including one-off fraud services or physical documentation copies — most users purchasing fraudulent documentation seek out digital versions, but some vendors still process the traditional forgeries.

Data valuation

All goods and services traded on these criminal platforms reinforce the growth and stability of the dark web fraud economy. The fraud economy runs on compromised data, and these compromised data sets are raw materials to cybercriminals. Treating compromised information like raw materials changes the way fraudsters view and value data. Fraudsters value data based on its potential for monetization, whether because of intrinsic value (like a payment card) or its ubiquity across multiple platforms or targets (like a Social Security number), which allow fraudsters to carry out a wide range of schemes with a single data point.

Organizations typically worry about securing financial projections, research and development details, or merger and acquisition activity, but fraudsters work most effectively with the standard data types that an organization has amassed over time — employee details, customer information, executive profiles and financial accounts.

The future of fraud

Fraudsters have always used technological advancements as a means to build faster, and more efficient and damaging fraud schemes. The dark web’s no different. The dark web is just another part of the internet, and the internet is a tool that creates wider access and broader impact for users’ goals. Data is the most valuable commodity in modern commercial economies, and that same data is being traded every day, at scale, on established criminal marketplaces.
While these marketplaces are unfamiliar territory for many, results of these data sales and fraud schemes are familiar: Fraudsters still want to gain access to accounts and services, pretend to be someone else and, above all, profit. They have a wider set of resources and the means to operate their criminal enterprises at scale, but their goals are still the same — and many of their methods are simply updated versions of age-old classics. Fraud examiners need not start from scratch. These cyber-enabled frauds are a far more familiar beast than we might expect.

Emily Wilson, CFE, is vice president of research at Terbium Labs. Contact her at LinkedIn.com/in/emily-e-wilson.

DID YOU KNOW?

- Months that start on a Sunday will always have a Friday the 13th, December starts on a Sunday this year.
- December 19, 1997 the movie Titanic was released and was the largest grossing movie for over 12 years.