Testimony

Data Thieves

The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data

Lillian Ablon

CT-490

Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, on March 15, 2018.

RAND CORPORATION

Published by the RAND Corporation, Santa Monica, Calif.

www.rand.org

Data Thieves:

The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data

Testimony of Lillian Ablon[1]
The RAND Corporation[2]

Before the Committee on Financial Services
Subcommittee on Terrorism and Illicit Finance
United States House of Representatives

March 15, 2018

Good afternoon, Chairman Pearce, Ranking Member Perlmutter, and distinguished members of the subcommittee. Thank you for the invitation to testify at this important hearing, "After the Breach: the Monetization and Illicit Use of Stolen Data."

Cybersecurity is a constant and growing challenge. Although software is gradually becoming more secure and developers are creating novel approaches to cybersecurity, attackers are becoming more adept and better equipped.[3] And as the world embraces more digital and hyperconnected components, the paths become more numerous for attackers to gain access to our most sensitive information.

Data breaches have become commonplace in the United States. In 2017, more than 1,000 data breaches exposed over a billion records of sensitive data.[4] From banking to retail, health care to entertainment, and even government, no sector is immune. Some of that information has been monetized by threat actors in flourishing underground markets. These cyber black markets offer the computer-hacking tools and services to carry out cybercrime attacks and sell the by-products stolen in those attacks: credit cards, personal data, and intellectual property. In other

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

[3] Martin C. Libicki, Lillian Ablon, and Tim Webb, *Defender's Dilemma: Charting a Course Toward Cybersecurity*, Santa Monica, Calif.: RAND Corporation, RR-1024-JNI, 2015 (http://www.rand.org/pubs/research_reports/RR1024.html).

[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, idtheftcenter.org, no date (https://www.idtheftcenter.org/2017-data-breaches).

cases, the attackers keep the data for their own espionage purposes or use stolen funds to facilitate future operations.

To get an understanding of what the attackers are doing with the stolen data, and how they are monetizing the data, we need to understand who they are and what motivates them.

Attackers, or *cyber threat actors*, can be grouped by their set of goals, motivation, and capabilities. Four groups of note are *cyberterrorists*, *hacktivists*, *state-sponsored actors*, and *cybercriminals*.[5] It is important to understand the full environment of threat actors, so I will briefly review these four, but I will focus my testimony largely on state-sponsored actors and cybercriminals, as they are of greatest concern to businesses and the government and merit the most note for this hearing.

Today I will give a brief overview of these four types of cyber threat actors, followed by a discussion of the landscape of the black markets for cybercriminal tools and stolen data, and then finish with some of the ways that state-sponsored actors and cybercriminals use and monetize the stolen data.

Different Cyber Threat Actors Have Different Motivations

Cyberterrorists

Cyberterrorism unites two significant modern concerns: attacks via technology in cyberspace and traditional terrorism. While there is no single or globally accepted definition of *cyberterrorism*, in theory, it consists of a politically motivated extremist group or nonstate actor using cyber techniques to intimidate, coerce, or influence an audience; force a political change; or cause fear or physical harm.[6]

To date, there have been no publicly reported cases of terrorists using the internet to carry out cyberattacks; what has been done that has been attributed to cyberterrorism is more akin to hacktivism. Many terrorists, or nonstate actors, do employ cyber to further their goals. They use the internet in many ways: for information gathering, e.g., learn how to build a bomb; to recruit, meet, and connect with like-minded individuals; and to spread propaganda.[7] But just “being” in cyberspace does not make a terrorist a cyberterrorist. Cyberspace must be used somehow to

[5] Robinson and colleagues have documented other categories, such as script kiddies, cyber researchers, and internal actors. Neil Robinson, Luke Gribbon, Veronika Horvath, and Kate Cox, *Cyber-Security Threat Characterization: A Rapid Comparative Analysis*, Santa Monica, Calif.: RAND Corporation, 2013 (https://www.rand.org/pubs/research_reports/RR235.html).

[6] B. Hoffman, *Inside Terrorism*, New York: Columbia University Press, 2006; R. Ahmad and Z. Yunos, “A Dynamic Cyber Terrorism Framework,” *International Journal of Computer Science and Information Security*, Vol. 10, No. 2012, pp. 149–158.

[7] Robert S. Mueller III, “Combatting Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies,” prepared remarks at RSA Cyber Security Conference, San Francisco, Calif., March 1, 2012 (http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies); and Ines, von Behr, Anais Reding, Charlie Edwards, and Luke Gribbon, *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism*, Santa Monica, Calif.: RAND Corporation, 2013 (https://www.rand.org/pubs/research_reports/RR453.html).

commit a terrorist act.[8] The movies and media portray what cyberterrorism could be: terrorists crafting digital attacks to take down traffic lights, make trains stop on a dime, and water pipes burst. But to date, no such dramatic events have occurred.

Hacktivists

Hacktivists are typically motivated by a cause—political, economic, or social: from embarrassing celebrities, to highlighting human rights, to waking up a corporation to its vulnerabilities, to going after groups whose ideologies they do not agree with.[9]

Hacktivists may steal and disseminate sensitive, proprietary, or, sometimes, classified data in the name of free speech. Other times, they aim to deny access to a particular service or website by conducting a distributed denial-of-service (DDoS) attack, essentially denying legitimate access by flooding a website with more traffic than it can handle, causing the site to crash.[10]

State-Sponsored Actors

State-sponsored actors receive direction, funding, or technical assistance from a nation-state to advance that nation's particular interests. State-sponsored actors have stolen and exfiltrated intellectual property, sensitive personally identifying information (PII), and money to fund or further espionage and exploitation causes. In rare cases, these data appear for sale on underground black markets. Instead, these data are usually kept by the actors for their own purposes. Although the data taken from data breaches might not always appear on underground markets, what *can* appear are the tools and guides for how to take advantage of the vulnerabilities that allowed access to the vulnerable systems in the first place. As an example, a researcher published the flaw that was used to penetrate Equifax, and within 24 hours the information was published to hacking websites and included in hacking toolkits.[11] Note, however, that there has not been official attribution of who conducted the intrusion into Equifax.

[8] Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday*, November 4, 2002 (http://firstmonday.org/ojs/index.php/fm/article/view/1001/922); and Maura Conway, "Cyberterrorism: Hype and Reality," in Leigh Armistead, ed., *Information Warfare: Separating Hype from Reality*, Washington, D.C.: Potomac Books, 2007, pp. 73–93.

[9] As a few examples, see Paolo Passeri, "List of Hacked Celebrities Who Had (Nude) Photos Leaked," Hackmageddon, August 7, 2012 (http://www.hackmageddon.com/2012/08/07/list-of-hacked-celebrities-who-had-nude-photos-leaked/); Lillian Ablon, "Hackerazzi: How Naked Celebrities Might Make the Cloud Safer," *The RAND Blog*, September 8, 2014 (https://www.rand.org/blog/2014/09/hackerazzi-how-naked-celebrities-might-make-the-cloud.html); "HBGary Federal Hacked by Anonymous," *Krebs on Security*, February 7, 2011 (https://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/); Paula Cohen, "Anonymous Hackers' Group Declares War on ISIS," *CBS News*, November 16, 2015 (https://www.cbsnews.com/news/anonymous-hackers-declare-war-on-isis/); "Anonymous Hacks Pro-ISIS Twitter Accounts, Fills Them with Gay Pride," *CBS News*, June 15, 2016 (https://www.cbsnews.com/news/anonymous-hacks-pro-isis-twitter-accounts-fills-them-with-gay-pride/).

[10] An example is Operation Payback, which targeted websites of large corporations to shut them down temporarily.

[11] Michael Riley, Jordan Roberston, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros," *Bloomberg*, September 29, 2017 (https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros).

In a few cases, state-sponsored actors have conducted cyberattacks—which deny, degrade, disrupt, or destroy computing systems—to send a political message. An example of this is the 2014 attack on Sony Pictures Entertainment, where North Korea wanted to advance its political agenda and, in part, to stop the release of the movie *The Interview*.[12]

Rather than viewing what they do as breaking laws, state-sponsored actors maintain that they are acting in accordance with their own laws, and most have accepted that cyberespionage is a legitimate state activity. Deterrence—diplomatic, financial, and economic consequences—is thought by some to play a role in preventing these types of attacks from happening or escalating.[13]

Cybercriminals

Cybercriminals are motivated by financial gain—they care about making money.[14] They want access to our personal, financial, or health data—in order to monetize them on underground black markets. For the retail sector in particular, the stolen data from these hacks appeared within days on black market sites.

These markets are dispersed, diverse, and segmented—rapidly growing, constantly changing, and innovating to keep pace with consumer trends and prevent law enforcement and security vendors from understanding them. They come in many forms. Some are dedicated to one product or a specialized service. Others offer a range of goods and services for a full life cycle of an attack—from the tools needed to exploit a system, all the way through to the cyberlaundering of the stolen goods. These markets are easy for almost anyone to get involved in—at least at the most basic levels.

Cybercriminals operate behind anonymous and peer-to-peer networks (such as Tor and OpenBazaar, respectively) and use encryption technologies and digital currencies (such as Bitcoin) to hide their communications and transactions.

Table 1 gives a summary of the various cyber threat actors, their main motivations, and use of stolen data.

[12] FBI, "Update on Sony Investigation," press release, December 19, 2014 (https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation).

[13] Martin C. Libicki, *It Takes More Than Offensive Capability to Have an Effective Cyberdeterrence Posture*, Santa Monica, Calif.: RAND Corporation, CT-465, 2017 (https://www.rand.org/pubs/testimonies/CT465.html).

[14] To be sure, there may be some sense of "nobility" of, for example, Russian actors victimizing Americans.

Table 1. Characteristics, Techniques, and Targets of Cyber Threat Actors

Cyber Threat Actors	Description	Motivator	Technique	Types of Targets	Use of Stolen Data
Cyberterrorists (theoretical)	Extremist groups or nonstate actors using cyber techniques to intimidate, coerce, or influence an audience; force a political change; cause fear or physical harm	Gain support for and deter opposition to a cause; carry out dictates of an ideology	Cause kinetic damage: destroy or disrupt critical infrastructure or systems; loss of life	Determined by actors' ideology	Disrupt critical infrastructure via cyberattack; Change prescription or allergy information, switch or delete medical record; further a campaign on a particular target
Hacktivists	Bring awareness to a cause (political, economic, social); exercise free speech (e.g., "lulz")	Ideological activism; disruption of services or access	Steal and leak sensitive, proprietary, or classified information; conduct DDoS on websites or services	No one type of target	Gather personal information of a specific target; publicize a breach to highlight how vulnerable a particular organization is
State-sponsored actors	Receive direction, funding, or technical assistance from nation-states; highly sophisticated and often use the most-sophisticated methods (e.g., zero-day vulnerabilities); targeted and persistent	Advance interests of their nation-state; further political agenda	Conduct intelligence, surveillance, reconnaissance, espionage; employ watering-hole attacks; exfiltrate data (e.g., intellectual property); degrade or destroy technical components; conduct targeted attacks	Other nation-states, defense contractors, technology sector, and critical infrastructure; (rare) banks or cryptocurrency wallets	Build profiles of possible targets for follow-on targeting, exploitation, or espionage campaigns; use personal, financial, or medical information as leverage to gain other types of intelligence
Cybercriminals	Access personal, financial, or health data to monetize it	Financial gain; power	Use crimeware (e.g., exploit kits, "script-kiddy" tools); rely on already known vulnerabilities, phishing, and spearphishing; smash-and-grab	Data repositories (e.g., banks, retail companies, health care) that can be monetized; cryptocurrency wallets	Use credentials (username/password combinations) and harvest contact lists for phishing attacks; exploit password reuse; conduct identity theft, tax, or medical fraud

The Challenge of Attribution

Attribution after a data breach is difficult. Often there is not enough digital evidence left behind to identify the attackers or their country of origin. That said, there are cases where various commercial security firms and threat analysis groups involved in the aftermath of a breach have found similarities in the malware used in various attacks. In particular, similar malware was used in the 2014 cyberattack on Sony Pictures Entertainment and the 2015–2016 SWIFT data breach (i.e., from North Korea). And many note the strong possibility that the malware for the data breaches of the Office of Personnel Management (OPM), Anthem, and United Airlines originate from the same place (China).[15]

There Is Overlap Between These Various Cyber Threat Actors

Although there are distinctions and differences in motivation between each of the cyber threat actors, there is some degree of fluidity between the groups. In many cases, the same tools and techniques are used by different groups, sometimes because those are the only tools available, and other times because that helps with plausible deniability and shifting the blame to a different group. In some countries, state-sponsored actors may work with "citizen hackers" or their country's cybercriminal elements to carry out an attack.[16]

Table 2 provides some more detail about the overlap between the various cyber threat actors.

The Hackers' Bazaar: How Stolen Information Gets Monetized

Turning to the cybercrime black markets, I will outline four aspects: *people*, *products*, *places* for communicating and conducting business transactions, and *prices*.[17]

[15] SANS Institute InfoSec Reading Room, *United Airlines May 2015 Data Breach: Suggested Near, Mid and Long-Term Mitigating Actions Using the 20 Critical Security Controls*, November 2015 (https://www.sans.org/reading-room/whitepapers/breaches/united-airlines-2015-data-breach-suggested-near-mid-long-term-mitigating-actions-th-36452); Threatconnect Intelligence Research Team, (2015, February 27). The Anthem Hack: All Roads Lead to China," February 27, 2015 (http://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/).

[16] The attack on Yahoo! is an example of this.

[17] Most of the language and analysis in this section are drawn from Lillian Ablon, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, Calif.: RAND Corporation, 2014 (https://www.rand.org/pubs/research_reports/RR610.html).

Table 2. Overlap Between the Various Cyber Threat Actors

	Hacktivists	State-Sponsored	Cyberterrorists
Cybercriminals	May use some of the same "script-kiddy" tools for things like DDoS May have some of the same targets Can be difficult to tell them apart	Cybercriminals often have close ties (perhaps funding) to nation-states For sophisticated cybercriminals, often the groups are confused with each other, especially by the media Most of the time, they do not want attribution, though some criminal groups have taken credit for state-sponsored actions	Cybercriminals do not want recognition or attribution Cyberterrorists do typically want attribution
Hacktivists		"Citizen hackers" may have hacktivists connected with state-sponsored actors Some hacktivist groups take credit for state-sponsored actions	May in fact be the same thing: "one man's terrorist is another man's freedom fighter" Both typically want attribution Often use similar low-level attacks (e.g., website defacements, taking over Twitter accounts)
State-Sponsored			May have same goals (e.g., to intimidate, coerce, or influence an audience or force a political change)—but one is in political power and the other is not

People: Who Participates In Cybercrime Markets?

Participants in cybercrime black markets come from all over the world, range across all skill levels, and occupy different roles depending on their technical abilities and reputation.

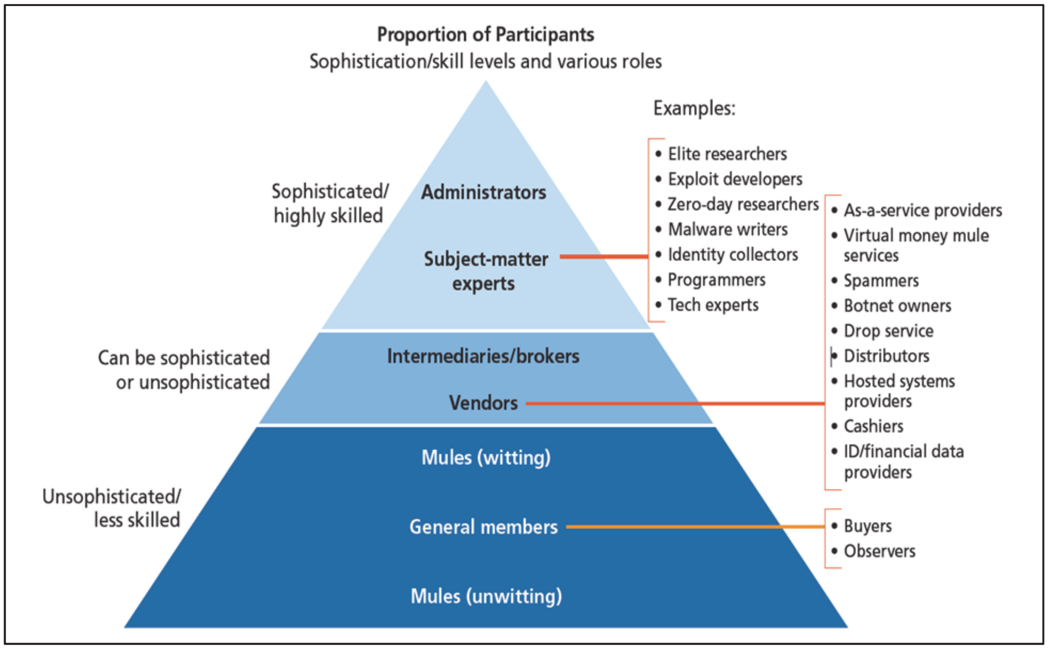
Within these markets, there are often hierarchies and specialized roles: *administrators* sit at the top, followed by *subject-matter experts*, who have sophisticated knowledge of particular areas (e.g., exploit-kit creators, data traffickers, cryptanalysts, those who vet). Next are *intermediaries*, *brokers*, and *vendors* and then the *general membership*.

At the bottom of the hierarchy is where the market meets the consumer. This is where *mules* and virtual money mule services come into play—the final level of participation in the market. Mules use multiple methods to turn the stolen credit card or ecommerce accounts into usable money—for example, by completing wire transfers or shipping goods overseas bought with stolen funds. Mules can be witting participants (well-informed and organized operations) or unwitting (naïve individuals duped into involvement).[18]

The number of participants in these black markets has increased as barriers to entry diminish. Barriers today to enter and participate in these markets are negligible—essentially all that is needed is an internet connection and a device. This is due to the greater proliferation of websites, forums, and chat channels where goods can be bought and sold. The greater availability of as-a-service models, point-and-click tools, and easy-to-find online tutorials makes it easier for technical novices to use what these markets offer or to just hire someone to carry out an attack for them. An increase in the number of tutorials, manuals, YouTube videos, and Google guides for "how to use exploit kit *X*" or "where to buy credit cards" also facilitates entry into the lower tiers of these markets, especially for those who wish to be buyers.

Figure 1 depicts the different participant levels in the underground market, proportionally. It also shows the sophistication and technical skill levels and gives examples of various roles.

Figure 1. Different Levels of Participants in the Cyber Black Markets



SOURCE: Ablon, Libicki, and Golay, 2014.

Surprisingly, these markets are highly reliable—reputation matters a great deal, and, for the most part, products and participants are what they say they are and do what they say they do.

[18] Examples include some "work from home" scams where unwitting people are recruited to purchase goods (using the, unbeknownst to them, stolen credit cards) and then ship them overseas.

Reputation entails either having credentials and a good reputation with others or proving oneself (for example, getting good reviews on sales).

Because contracts in black markets cannot be legally enforced, the markets are constantly plagued by *rippers*, who do not provide the goods or services they advertise and are an exception to the high reliability of the markets. Rippers tend to get reported and then quickly removed by administrators (by, for example, suspending their accounts). Although they can easily access new channels under new names, it takes time to reestablish a reputation, which inhibits cheating.

Products: What Is For Sale?

Cybercrime markets offer a diverse slate of products, including both goods (hacking tools, digital assets) and services (hacking-as-a-service, digital asset handling, fake-identity creation) for all phases of the full cybercrime life cycle—from initial hack all the way through to monetizing the stolen data.

Examples include tools to help gain initial access onto a target (exploit kits), along with the payloads (malware) and the parts and features of those payloads, services to help scale or deliver a payload, support products to ensure that infrastructure is set up correctly or to provide cryptanalytic services, and considerations for how to manage the stolen goods. As-a-service offerings (setting up botnets or conducting ransomware attacks) are on the rise.

The product slate keeps evolving with the technology. Whatever is new or novel for the traditional consumer—mobile devices, cloud computing, social media platforms—offers new entries for attack and will thus elicit a counterpart exploit on the black market.

Table 3 describes the main categories of products available.

Table 3. Goods and Services on the Black Market

Category	Definition	Examples
Initial access tools	Enable a user to perform arbitrary operations on a machine to then deliver payloads; can automate the exploitation of client-side vulnerabilities	• Exploit kit (hosted or as-a-service) • Zero-day vulnerabilities (and weaponized exploits) • Point of sale (POS) skimmers
Payload parts and features	Goods or services that create, package, or enhance payloads to gain a foothold into a system	• Packers[a] • Crypters[b] • Binders[c] • Obfuscation or evasion
Payloads	Impart malicious behavior, including destruction, denial, degradation, deception, disruption, or data exfiltration	• Bots or botnets for sale • Malware (including that focused on targeting cryptocurrency wallets)
Enabling services	Assist in finding targets or driving targets to a desired destination to use an initial access tool or payload; attack vectors and scaling methods	• Spam services • Pay-per-install and affiliates • Phishing and spearphishing services • Services to drive or find traffic • Fake website design and development
Full services (as-a-service)	Package together initial access tools, payloads, and payload parts and features to conduct attacks on a customer's behalf; can provide full attack life cycle	• Hackers for hire • Botnets for rent • Doxing • DDoS as a service (including DDoS against cryptocurrencies) • Ransomware as a service
Enabling and operations support products	Ensure that initial access tools and hacking services (enabling or full service) work as needed, are set up correctly, and can overcome "speed bumps" or obstacles	• Infrastructure (e.g., leasing services, VPN services, bulletproof hosting, compromised sites and hosts) • Cryptanalytic services (e.g., password cracking, password hash cracking) • CAPTCHA breaking
Digital assets	Items obtained from the target or victim (i.e., the hacked or stolen information)	• Credit card information • Account information (e.g., ecommerce, social media, banking) • Email login and passwords • Online payment service accounts • Credentials • PII/protected health information (PHI)
Digital asset commerce and cyberlaundering	Facilitate turning digital assets into cash	• Mule services • Counterfeit goods and services (e.g., fake documents, IDs, currency) • Card cloners, fake ATMs • Credit card processor services

SOURCE: Ablon, Libicki, and Golay, 2014.

[a] The "outer shell" of some malware—e.g., Trojan horses—hides the malware and makes detection and analysis by antivirus software more difficult. Packers can also employ antidebugging, antiemulation, anti-VM techniques, and code obfuscation.

[b] Crypters are software that can encrypt executable (.exe) files. Crypters can be used to encrypt viruses, remote access Trojans, keyloggers, spyware, etc. to make them undetectable from antivirus systems.

[c] Binders are software used to bind or combine two or more files into one file under one name and extension. They are used for the evasion of anti-virus systems.

Places: How Do These Markets Communicate and Conduct Transactions?

Communications and transactions take place through a variety of channels that span multiple tiers. Channels can include online stores, bulletin board–style web forums, email, or instant messaging platforms (allowing for private one-on-one communications or open chat rooms). Some are easy to find, and others are by invitation only and only accessible after having gone through an extensive vetting process. The highest-access tiers are usually hidden in websites on the dark web, which offer anonymizing and secure features.[19]

Transactions can cut across multiple channels and access tiers. An advertisement might be posted on a forum openly available and easily accessed, with actual transactions taking place behind encrypted VPNs, private messaging, locked-down social media accounts (e.g., private Twitter accounts), a shared email (to exchange content through draft messages), or a private server spun up on Tor for just one transaction. As digital goods, payment systems, techniques, tools, and malware continue to evolve, forums with "how to" sections remain popular.

In recent years, there has been more gravitation toward methods of communicating and conducting business transactions that offer anonymity or make it harder for law enforcement to find. Tor—the onion router—is a service one can use to access websites on the dark web and is a way to browse the internet semi-anonymously, essentially masking the location where one is coming from. As law enforcement succeeds in finding and taking down cybercriminal sites, such as AlphaBay and Hansa (two popular dark web marketplaces), there has been more of a move toward decentralized peer-to-peer networks (such as OpenBazaar), where individual users connect with each other, making it difficult for outsiders, such as law enforcement, to track.

Prices: How Much Does Everything Cost?

Prices can range widely, depending on hardness of attack, freshness of data, sophistication of malware, or whether something is as-a-service or do-it-yourself.

Easily exchanged goods—such as PII, account credentials, and financial data—are prey to the normal microeconomic fluctuations of supply and demand. Often, there is too much of a product available to sell at normal prices. By contrast, stolen-to-order, nonfungible goods—such as new technology designs, details on R&D activities, mergers and acquisitions, and other sorts of intellectual property—can command a very high price, provided that the right buyer exists.

The yield of a product influences its price. For example, a stolen Twitter account costs more to purchase than a stolen credit card because the former's account credentials potentially have a greater yield: the username/password combination could unlock access to other accounts, as well as give access to the victim's contact list in order to carry out follow-on spam or phishing attacks. Immediately after a large breach, batches of credit cards get released in the markets: freshly acquired credit cards command a higher price—as there is greater possibility for the credit cards to still be active. Over time, prices fall because the market becomes flooded with more and more batches—leveling off as the data become stale or if there has been significant time since the last breach. High or no-limit cards (e.g., the American Express Black card) or

[19] A darknet or dark web is an anonymous or semianonymous private network that uses encryption and proxies to obfuscate who is communicating with whom. An example is the onion router (Tor).

cards with chip and PIN are more valuable and can command a higher price: While a U.S. "chip and signature" card might start off for $15 a number after a breach, a European "chip and pin" card will go for closer to $120—the higher price point stemming from these types of cards being more secure, often resulting in a higher credit limit. Over time, as banks and users discover the theft and shut down the cards, a card may be discounted to $12 a number, and then drop further to $10 a number. Eventually, the credit cards may go on clearance, and one can purchase a "grab bag" of 100 credit card numbers for $700. The thought here is that, even if only two of those credit card numbers are still open for fraud, one can purchase and then illegally sell electronics, yielding a profit of more than the $700.

Access to botnets and DDoS capabilities are cheaper because there are so many more options (same for exploit kits).

Although prices, in general, range widely (e.g., hacking into accounts can be anywhere from $16 to $325-plus, depending on the account type),[20] similar products tend to go for similar amounts. Medical records can be worth up to $50 per record. Brand-name recognition also plays a role. Services can involve leasing servers, finding traffic, creating a personalized payload (or "cleaning" or obfuscating an already existing payload to avoid antivirus signatures), and setting up infrastructure.

Table 4 summarizes stolen credit card prices and markets.

Table 4. Credit Card Prices Based on Market Circumstance

Card Price (per card)	Market Circumstance
$120	Freshly acquired (EU card)
$15	Freshly acquired (U.S. card)
$10–$12	Flooded
$0.75–$7	Clearance ("stale" data)
SOURCE: Updated from Ablon, Libicki, and Golay, **2014.**	

Although transactions can be completed with nondigital currency (e.g., Western Union, cash, PayPal), black market sites have moved toward accepting digital cryptocurrencies, given the appeal of anonymity and other security characteristics. Bitcoin is currently a popular choice, although with the volatility of the cryptocurrency markets, an increase in theft of digital currency wallets, and some notable takedowns by law enforcement of Bitcoin exchanges, it is by no means the only choice. Other, more reasonably priced digital currencies, such as like Ethereum, have become more popular. Further, the possibility that such countries as Russia and China will limit uses of Bitcoin has caused those doing transactions in that virtual currency to find ways to

[20] Max Goncharov, *Russian Underground 101*, Cupertino, Calif.: Trend Micro Incorporated, 2012 (https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf); Dell Technologies, *Securworks 2017 State of Cybercrime*, February 13, 2018 (https://www.delltechnologies.com/en-us/perspectives/secureworks-2017-state-of-cybercrime-executive-summary/); Dell Secureworks, *Underground Hacker Markets: Annual Report—April 2016*, April 2016 (http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf).

move those funds into other financial system or digital currencies to get their money out and usable. The uses of WebMoney and Perfect Money, online payment settlement systems, remain popular, although because they are not anonymous, users may send their digital currency through a "tumbler" or "washer" to virtually launder the wallet through several different accounts, making the funds difficult to trace.

Making The Stolen Goods Useful: How Data Get Used or Monetized by Cyber Threat Actors

The cybercrime black markets can be more profitable than traditional markets for illicit goods: The links to end users are more direct, and worldwide distribution, being electronic, is a relatively trivial task. This is because a majority of players, goods, and services are online-based and can be accessed, harnessed, or controlled remotely, instantaneously. "Shipping" digital goods may only require an email or download at worst—or a username and password to a locked site at best. This enables lower costs and possibly greater profitability.

Cybercriminals are always looking for exotic ways to use or monetize stolen data in ways that law enforcement and security vendors are not looking for or have not yet figured out. That said, because the main motivation of cybercriminals is to make money as quickly as possible, data, which require several steps before they can be monetized, are not as valuable as that which can be monetized quickly. As such, medical records and PHI, credit report information, and extraordinarily sensitive PII are likely more valuable to state-sponsored actors, who might use this information to build profiles to target for exploitation or espionage campaigns, as leverage to gain other types of information, or to help incubate innovative new strategies for using big data against an adversarial country.

In what follows, I describe various categories of stolen data and how each can be monetized or used by cybercriminals or state-sponsored actors. While I note examples of data breaches, unless explicitly stated, I do not intend to imply attribution of a particular cyber threat actor or imply that the data from those breaches have appeared on cybercrime markets for monetization. Instead, my intent is to provide real-world examples of data breaches involving the particular types of data and illustrate what might be done with those data.

Financial information, such as credit card data and bank account numbers, can get monetized by withdrawing cash, purchasing gift cards for resale, or harnessing a "money mule" (witting or unwitting) to make fraudulent orders to purchase goods, such as expensive electronics, which can then be sold on other black markets.

Credentials, such as usernames, passwords, account login information, and email addresses, enable an attacker to get access to the victim's contact list for further spam or phishing campaigns. The actor might also take advantage of password reuse and try to access a variety of banking and ecommerce sites. With access to business email addresses, an attacker can pose as a legitimate employee in the business and request a seemingly legitimate wire transfer, whose funds end up in the account of a money mule, who may then forward on the money or withdraw it and send it to the attacker through different means.

The breaches of Target (2013) and Home Depot (2014) are examples of data breaches where attackers collected credit and debit card numbers, as well as account information and email addresses (110 million from Target and 56 million from Home Depot).[21] The 2013 breach of Yahoo! compromised the accounts of between 500 million and 3 billion users.[22] And the 2014 data breach of JP Morgan Chase, where names, addresses, phone numbers, and email addresses of the holders of 76 million households and 7 million small business accounts were taken, was the largest theft of customer data from an American financial institution at the time.[23]

Medical records and PHI, such as the information accessed from Community Health Systems in 2014[24] or Anthem in 2015,[25] may be used for medical fraud—for example, filling out prescriptions in the victim's name—or combined with other PII to create a more detailed, comprehensive profile.

Financial reports on publicly traded companies, such as those accessed during the 2016 data breach of the Securities and Exchange Commission's EDGAR database, could provide the attackers information to make illegal trades.[26]

Credit report information, such as addresses, dates of birth, social security numbers, driver's license information, and other PII can be combined, creating a comprehensive profile of a victim to create a custom dictionary of possible passwords that can be used to attempt to crack a victim's bank or financial account or for identity theft—posing as the victim to open up new lines of credit or to add new authorized users to existing credit lines. In the 2017 data breach of Equifax, approximately 149 million users had this kind of information taken.[27]

Extraordinarily sensitive PII, akin to the kind of information taken from OPM in 2014,[28] can facilitate those building comprehensive profiles of victims.[29] Cybercriminals might use this information in the same way they use credit report information.

[21] Target, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," December 19, 2013 (https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car); Home Depot, "The Home Depot Report Findings in Payment Data Breach Investigation," November 6, 2014 (http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315)

[22] Yahoo! Help, "Yahoo 2013 Account Security Update FAQs," webpage, no date (https://help.yahoo.com/kb/account/SLN28451.html).

[23] United States Securities and Exchange Commission, "Form 8-K: JPMorgan Chase & Co.," Shareholder.com, October 2, 2014 (http://investor.shareholder.com/jpmorganchase/secfiling.cfm?filingID=1193125-14-362173).

[24] Anthem, "2015 Cyber Attack Settlement Agreement Reached," (http://www.chs.net/media-notice/).

[25] "Anthem Cyber Attack Class Action Settlement Agreement," Anthemfacts.com, no date (https://www.anthemfacts.com/cyber-attack); "Anthem Data Breach: Frequently Asked Questions," Databreach-settlement.com, no date (http://www.databreach-settlement.com/Home/FAQ).

[26] Jay Clayton, "Statement on Cybersecurity," Sec.gov, September 20, 2017 (https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20).

[27] Equifax, "2017 Cybersecurity Incident and Important Consumer Information," website, Equifaxsecurity2017.com, no date (https://www.equifaxsecurity2017.com).

[28] OPM, "Cybersecurity Resource Center," webpage, no date (https://www.opm.gov/cybersecurity/cybersecurity-incidents/).

[29] Data taken from OPM include up to 21.5 million records of Social Security numbers, passport numbers, birthdates, birthplaces, and multiple modes of contact information; details about victims' residential, employment,

Aggregation from Different Data Breaches Can Build a Strong Targeting Profile

Aggregating data from multiple breaches makes the potential for harm much greater. For example, combining credit report information, health care information, and travel information of a person helps to build a comprehensive profile and ideas of how to exploit this person. In this way, if the same actor carried out the hacks on OPM, Anthem, and United Airlines, they would have information on some of the most sensitive personal and health information, which, combined with travel information, can give a fairly comprehensive picture of a potential target, along with locations of frequently traveled places in order to "bump" into them.

And, in some cases, competing groups are all looking for the same data: State-sponsored actors might use credit report information to help build a dossier on a potential counterintelligence target, understanding their weaknesses and vulnerabilities, whereas cybercriminals would use the same information to create the custom dictionary for password guessing.

What Can Be Done?

Each type of cyber threat actor brings its own concerns. With cybercriminals, systems do not need to be completely secure: As long as there are easier and cheaper targets nearby, your safety is much higher. That said, the most sophisticated and determined threat actor will get through no matter what—in this case, security is more about making it expensive for an attacker (in terms of resources, money, time, research, and so on). By adopting certain core technologies, organizations can prevent cybercriminals from targeting the "low-hanging fruit" and instead turn to others with more-lax controls. Cybersecurity solutions that make it harder for threat actors to successfully breach an organization include regular patching and updating systems, employing multifactor authentication, encrypting data (in transit and at rest), and implementing regular security awareness training for people to be more aware of the individual threat and the need to protect themselves.

Recent congressional hearings on Equifax and other data breaches have been useful, highlighting several issues, including potential measures for how to improve response in the wake of a breach. One policy measure would require the extension of identity theft and credit monitoring services for victims to ten years, keeping the requirement for private companies the same as what Congress required of the U.S. government (extended from three years) in the wake of the OPM data breach. From a consumer protection perspective, this makes a lot of sense, given the permanent, unchangeable personal information that was compromised. Other solutions raised included requiring notification following a breach of security of a system containing personal information and amending the Fair Credit Reporting Act to provide access to free credit freezes for all consumers. Although the data from these particular breaches (Equifax and OPM) may not appear on black markets, breach notifications could apply to retailers and other organizations where the data stolen often do appear on black markets. The faster consumers are

travel, educational, criminal, financial, addiction, and mental health history; detailed information on spouses, cohabitants, other family members, and foreign contacts; and as many as 5.6 million fingerprint records.

aware of compromises, the lower the prices fetched for this information on the black market, which could disincentive the thefts. Free credit freezes could make it harder for criminals to monetize the information.

While not a cybersecurity panacea, information sharing and international cooperation between the public and private sectors can help.[30] State and local law enforcement would benefit from knowing about these markets. Communications between law enforcement, banks, and commercial sectors (health care, retail, entertainment) could help to track down nefarious actors. Although digital currency exchanges are a weak link in attributing a cybercriminal to stolen money, they are often housed overseas. Getting international cooperation is key for law enforcement to successfully pursue the attackers.

Finally, cybercrime markets are highly reliable. Finding ways of tarnishing the reputations of the markets, by wasting a criminal's time or making an exploit tool purchased on the black market ineffective, can help to prevent the loss of information and cut the value chain early in the attack cycle. Solutions might include spreading misinformation or injecting false products into the markets to breed distrust among the actors and increase the number and quality of arrests.

Thank you for the opportunity to testify, and I look forward to your questions.

[30] Martin C. Libicki, *Sharing Information About Threats Is Not a Cybersecurity Panacea*, Santa Monica, Calif.: RAND Corporation, CT-425, 2015 (https://www.rand.org/pubs/testimonies/CT425.html).