THE BLACK MARKET REPORT

Mar. 2018

A LOOK INSIDE THE DARK WEB

THE HACKER UNDERGROUND EXPOSED BY ARMOR'S THREAT RESISTANCE UNIT (TRU) RESEARCH TEAM

INTRODUCTION

Every day, behind closed digital doors, money and stolen data are changing hands. No one knows how much, but some studies from the past few years have placed cybercrime's cost to businesses globally as high as hundreds of billions of dollars annually.

Supporting this burgeoning industry is a global community of hackers, malware writers, money mules and others, all of whom are getting their piece of the action. Credit card data is sold for $10 USD. Personally identifiable information (PII) that could include everything from a name and address to an SSN or even a credit report is selling for $40 - $200. Even social media accounts have value, with one vendor selling 1,000 brute-forced Instagram accounts for $15.

TRY AS CRIMINALS MIGHT TO STAY IN THE SHADOWS, ARMOR'S THREAT RESISTANCE UNIT (TRU) RESEARCH TEAM REGULARLY MONITORS THREAT ACTORS AND THEIR ACTIVITY TO PROTECT OUR CLIENTS.

In this report, our experts pulled data from dozens of dark web and underground markets and forums during the fourth quarter of 2017 to provide readers with a snapshot of the type of activity threat actors are participating in every day, as well as valuable insights into how these forums work. More than just places for selling stolen credit cards, the underground offers hacker-for-hire services, hacking tools, tutorials and more.

Use this report to gain insight into what types of tools and services are popular among criminals, what types of data are the most valuable to thieves and what you can do to better protect your organization. Effective security takes more than technology; it requires real-time knowledge of the threat landscape and risks to your data. So, buckle up, and join us in a trip into the cyber underground.

The Armor Threat Resistance Unit's **(TRU)** mission is to stay one step ahead of threat actors, acting as Armor's forward eyes and ears to emerging cyber threats and activities in the Dark Web that may affect Armor customers. Part of the Armor Security Operations Center, TRU is a force multiplier providing advance notice and intelligence on emerging threats while enabling our SOC teams with tactics and methods—intelligence applied—that strengthen their ability to see and respond to even the most sophisticated threats.

DEN OF THIEVES

Every market has rules, and the black market is no different. Many of the sites where malware, stolen data and cybercrime services are sold exist on the Dark Web and can only be accessed using anonymization software/services such as Tor or I2P. Others exist in the Deep Web, which is the part of the Internet not indexed by search engines such as Google. Accessing these communities is not always easy. It is not uncommon for them to have several rounds of verification, even at times requiring an invitation to ensure bots and unwanted outsiders don't gain entry. If someone comes off as suspicious or seems more interested in window shopping than buying, they may be ejected from the forum.

On the other hand, sellers who are highly regarded are often rewarded with positive reviews. Like any other vendor, the reputation of the seller matters. Bad reviews are bad for business and being outed as a scammer or unreliable source of data can bring the career of a would-be cybercriminal to a screeching halt.

Some sellers will offer samples of personal information or credit card data to prove the validity of their products, and others go as far as providing replacements in the event data turns out to be inaccurate. Additionally, many will provide basic levels of support in the form of code updates for malware, troubleshooting or configuration and implementation advice. Often, this support comes at a higher cost, allowing malware developers to create new income streams without having to take the risk of being caught using the malware themselves. Those same developers often lower their risk even further by making support available through anonymized channels to prevent anyone who has gotten caught from identifying them.

CYBERCRIME-AS-A-SERVICE

So just how are attackers getting their hands on all this data? This brings us to the backbone of the business – the tools, tactics and services that make the world of cybercrime go round and round. As one can imagine, the forums are replete with offers for everything from a $50 password stealer to exploit kits such as Stegano – which has been linked in the past to malvertising and the exploitation of vulnerabilities in Adobe Flash Player.

The movers and shakers of this market have various models for generating income, one of the most profitable of which is selling cybercrime-as-a-service.

ARMOR TRU RESEARCHERS SPOTTED SEVERAL SERVICES BEING OFFERED TO AID ASPIRING CYBERCRIMINALS, FROM DDOS SERVICES TO SPAMMERS FOR HIRE.

The service offerings were very flexible. Want to DDoS an organization for an hour? $10. A day? $200. What about remote access to a machine via Remote Desktop Protocol (RDP) for three months? $35.

This all fits into a general trend where vendors offered services and access as opposed to source code for their malware. Threat actors are increasingly monetizing their wares by leasing access to botnets, exploit kits, hacked accounts or other items that they now want to make a regular income from. An example of this would be the Disdain exploit kit, which could be rented for $80 a day, $500 a week or $1,400 a month.

In some cases, vendors create an additional income stream by providing support for an additional cost. For example, a seller offered to rent out the Blow-bot botnet, which includes webinject and other capabilities, for either $750 or $1,200 a month depending on whether the renter wanted a fully-featured version. Support was an extra $100 or $150 a month, respectively.

When source code is offered, there is a trend toward offloading risk by selling malware or exploit code to someone else and then selling support as well.

In the spirit of helping others, some sellers have taken to hawking hacker tutorials and known exploits in bundles at relatively low cost, most likely to low-skill hackers known as script kiddies.

Making crime easier of course is part of what the markets are about. A Microsoft Office exploit builder that targets CVE-2017-1099 was selling for as much as $1,000. Meanwhile, a banking trojan license could be purchased for $3,000 to $5,000, and a remote access trojan was seen selling for $200. The barrier to entry for cybercrime remains perilously low, making it that much more important that organizations and individuals focus on security.

YOU CAN DDoS AN ORGANIZATION FOR

$10 HOUR

$200 DAY

84% of 1,010 organizations surveyed in a 2017 report had experienced at least one DDoS attack in the previous 12 months, and 86% of those attacked dealt with more than one during that period.

HACKING TOOLS & SERVICES	
Account Hacking Program	**$12.99** (See more details on page 10)
Hacked Instagram Accounts in Bulk	1,000 - 10,000 accounts **$15 - $60**
Botnet: Blow-Bot Banking Botnet	Monthly Basic Rental **$750** | Monthly Full Rental **$1,200** | Monthly Support **$150**
Disdain Exploit Kit	Day **$80**, Week **$500**, Month **$1,400**
Stegano Exploit Kit: Chrome , FireFox, Internet Explorer, Opera, Edge	Unlimited Traffic, Day **$2,000** Unlimited Traffic, Month **$15,000**
Microsoft Office Exploit Builder	Lite exploit builder **$650** Full Version **$1,000**
WordPress Exploit	**$100**
Password Stealer	**$50**
Android Malware Loader	**$1,500**
Western Union Hacking Bug For World Wide Transfer	**$300**
DDoS Attacks	Week long attack **$500 - $1,200**
ATM Skimmers: Wincor, Slimm, NCR, Diebold	**$700 - $1,500**
Hacking Tutorials	Multiple Tutorials **$5 - $50**

The more sophisticated criminals were not left wanting, however. Code-signing certificates, which can allow malware to slip by security defenses undetected, were selling for between a few hundred dollars to thousands. Code-signing certificates are meant to provide assurance that a piece of software is from a legitimate, trusted creator and has not been tampered with. By abusing that trust, malware can use those types of certificates to compromise unsuspecting victims. One vendor offered a Class 3 code-signing certificate for $400. Another offered an Extended Validation (EV) certificate for $2,500.

Not all cybercrime begins with software, however. Credit card skimmers and magnetic stripe readers sell for as little as $700 and $450, respectively. To scammers, they are worth their weight in gold.

THE FINANCIAL LOSS FROM CYBERCRIME

THE U.S.  EXCEEDED

1.3 BILLION

in 2016, a rise of 24% from 2015.

Figure 1. P. 4. DDoS Attacks. According to the Worldwide DDoS Attacks & Cyber Insights Research Report, May 2017, Neustar. **Figure 2.** P. 5. Hacking Tools and Services. **Figure 3.** P. 5. Financial Loss from Cybercrime. According to the report issued by the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3).

THE TREASURE TROVE

There is a mountain of data in every organization. Some of it is customer data, some of it is employee data, but all of it has value to cybercriminals. **Social security numbers, bank account information and even hotel and airline rewards points can all be turned into money on the black market.**

Still, stolen credit card data remains arguably the most common staple of this market. The cyber underground is awash with it. Major brands such as Master Card, Visa and American Express all make regular appearances, and as shown in the tables, the stolen card information can come from a variety of countries.

THE TRU RESEARCH TEAM NOTED SIMILARITIES BETWEEN THE CREDIT CARD OFFERINGS WITHIN, AND SOMETIMES ACROSS, THE DIFFERENT UNDERGROUND MARKETS.

These similarities suggest that there are likely only a handful of major credit card data farmers doing the majority of the data theft. It appears these wholesalers are, directly or via a middleman, distributing the data and guidance on the most effective ways to sell it to retailers or sales people that post advertisements to the underground markets and forums. Doing business in this manner creates a separation between the theft and sale of the data that reduces the risk for the thieves and the sellers. This business model not only has the smell of a pyramid scheme, it reminds us that this is nothing new, that organized crime has simply moved into the digital age.

Credit card data can be stolen in a number of ways, including via credit card skimmers and infected point-of-sale systems. There is some variance in the prices from vendor to vendor. Overall, the cost of credit card data from the U.S. is consistently lower than that of other countries. This is likely due to a classic supply and demand situation, meaning there is just more of certain credit card data on the underground market. Often, card numbers are sold with additional identifying information, known as "Fullz", which amount to everything the buyer needs to prove they are the card owner if they are challenged, increasing the price.

CREDIT CARD DATA		
VISA / MasterCard	U.S.	$7 - $10
	UK	$15 - $25
	Canada	$15 - $25
	Australia	$25 - $27
	EU *(Italy, Spain, France, Germany, Denmark, Sweden, Ireland)*	$15 - $30
AMERICAN EXPRESS / DISCOVER	U.S.	$10 - $12
	UK	$25 - $27
	Canada	$25 - $30
	Australia	$18 - $35
	EU *(Italy, Spain, France, Germany, Denmark, Sweden, Ireland)*	$15 - $35

For instance, one a seller offered U.S. credit card numbers for $10-$12. However, the TRU team spotted a vendor selling a U.S. credit card number with fullz for $18. That same seller also offered a U.K. credit card number with fullz for $30.

Cybercriminals also sometimes charged more to verify the bank information number (BIN). For example, while a Visa card number on its own may sell for $10, the seller may charge $15 in exchange for verifying the BIN number. In the case of one vendor Armor spotted, the price of an American Express and Discover card number was selling for $12 to $17 with BIN verification.

The credit limit on the card can impact the cost as well. One person with a variety of cloned cards for sale offered one with a $5,000 limit for $450. A card with a $10,000 limit was being offered for $800, while another with a $15,000 limit was being hawked for $1,000.

In some cases, card information was also sold in large bundles. For example, one vendor offered 30 U.S. credit card numbers, BIN numbers and the owner's date of birth for $450. That seller offered the same package of information for 30 U.K. credit card numbers at a cost of $500.

Track data is also worth its weight in gold. Written on a credit card's magnetic stripe is not only information associated with the card's legitimate owner, but also service codes and security mechanisms that indicate how and where the card should be used, pin numbers, and unique codes that make any card created with that data appear to be legitimate. Having this data allows a buyer with the right equipment to create a cloned card and use the card with less risk of getting caught.

LIKE IT OR NOT, CYBERCRIME - AT LEAST IN THE SHORT TERM - DOES PAY.

CREDIT CARD TRACK DATA DUMPS			
VISA Classic / MasterCard Standard	U.S.	Track 1 & 2 Data	$25 - $45
	Canada & Australia		$25 - $45
	EU & UK		$50 - $60
	Asia		$30-$50
VISA Gold, Platinum & Business / MasterCard Gold & Platinum	U.S.	Track 1 & 2 Data	$35 - $50
	Canada & Australia		$40-$80
	EU & UK		$70 - $100
	Asia		$50-$70
AMERICAN EXPRESS Premium	U.S.	Track 1 & 2 Data	$35
DISCOVER	U.S.	Track 1 & 2 Data	$25-$50

Figure 4. P. 6. Banking & Online Payment Account Credentials. Prices in USD.
Figure 5. P. 7. Credit Card Track Data Dumps. Prices in USD.

BANK HEIST

Since they are easy to monetize, credit card numbers will always be fixtures of the underground market. The same can be said of ATM cards and bank account information. The bigger the balance, the bigger the payoff for the seller.

In one case, one vendor offered access to accounts with a balance of $3,000 from Bank of America, JPMorgan Chase and Wells Fargo - three of the largest banks in the U.S. - for $300. Another seller offered bank login information – including username, passwords and email address – for prices ranging from $200 to $1,000 for accounts at Wells Fargo, JPMorgan Chase and Bank of America. The accounts were advertised as having balances between $3,000 and $15,000.

BANKING & ONLINE PAYMENT ACCOUNTS CREDENTIALS	
ACCOUNTS (U.S.) BANK OF AMERICA, JPMORGAN CHASE, WELLS FARGO...	
Balance $2,000 - $5,000	**$100 - $400**
Balance $12,000 - $15,000	**$600 - $1,000**
Balance $20,000 +	**$1,000 +**
ACCOUNTS (UK) LLOYDS BANK, BARCLAYS, HSBC...	
Balance 3,000 - 6,000 GBP	**$150-$600**
Balance 10,000 - 16,000 GBP	**$600 - $1,000**
Balance 20,000 GBP +	**$800-$1,500**
ATM CARDS WITH BALANCES AND PIN	
Balance $2,000 - $8,000	**$100-$500**
LARGE U.S. ONLINE PAYMENT ACCOUNT CREDENTIALS	
Verified Balance $1,500 - $5,000	**$100 - $450**

Those interested in U.K. bank accounts need not worry. There are items for sale that cater to them as well. For example, a vendor offered access to accounts at Lloyds Bank with balances of 3,000 GBP and 5,000 GBP for 300 and 400 GBP, respectively.

Thieves go where the money is, so it is not surprising that they continue to have PayPal in their sights as well. As with the other accounts, how much PayPal accounts were worth varied according to the balance. For example, one seller offered a verified PayPal account with a balance of $3,000 for $200. Another vendor advertised a PayPal account with a $4,000 balance for $200.

Buying access to an account, however, is only part of a successful heist. From there, the buyer needs to be able to get their hands on the money. To accomplish this, cybercriminals traditionally have turned to money mules. Money mules can be either knowing or unwitting accomplices. Their role is to receive the funds from the compromised account, after which, they will be often tasked with transferring that money to another account overseas in exchange for a commission. In other cases, the buyer may use other means such as gift cards to launder the money.

Just as with credit cards, U.S. bank account information appears to be the least expensive. This is likely due to the laws of supply and demand. U.S. banks may have more global access points to support international travel, increasing the potential points of attack. In addition, their customers may have higher or more stable balances in their accounts on average than others, making them more attractive targets and contributing to their larger presence on the black market.

IDENTITY THEFT

While credit card and bank account data represent direct access to cash, the digital shelves of the cyber underground market are full of other profitable items as well. Personally identifiable information (PII) and counterfeit documents are often as valuable, if not more valuable, than the cash in a bank account. **The uses for PII and forged/stolen documentation are limited only by imagination and initiative. For example, anyone seeking to move unnoticed across borders can purchase an entirely new identity and potentially go undetected. Most of the PII and fake documents seen by Armor were tied to the U.S., Canada and Europe, with the U.S. leading the way. One seller spotted by the Armor TRU research team offered "US green cards, driver's license, Insurance, and Passport Visas" for $2,000.**

For just $40, another seller offered what was termed "full profiles", a swath of information that included obviously sensitive data such as social security numbers, dates of birth and addresses, as well as less sensitive, but no less personal, data like phone numbers, education level and employment information. The same seller also offered a background check for an unspecified additional fee that included criminal history, address history and other information. All of this sensitive and personal data is potentially damaging on its own, but it can quickly escalate to devastating when combined with fake receipts, IDs, and government documents. Packets of document templates for creating everything from fake utility bills and bank statements to driver's licenses and social security cards were being offered for $50. While fake documents such as these might fail under heavy scrutiny by an expert or a government database search, they will easily pass the eyeball test for local government offices, schools and small businesses, sporting logos and letterheads from companies like Comcast, PECO, DTE Energy, Chase and Wells Fargo. It's the same with the official documents and IDs.

Having a fake identity opens the door to all kinds of fraud and can be very damaging for anyone who is victimized. Nevertheless, the market for fake and stolen documents is thriving.

IDENTITIES, SOCIAL SECURITY INFORMATION, PASSPORTS AND OTHER DOCUMENTS	
U.S. PII (name, address, phone number, SSN, DOB, bank account data, employment history, credit history, criminal history)	$40 - $200
U.S. green cards, driver's license, Insurance, and Passport Visas (bundled)	$2,000
PASSPORTS, DRIVER'S LICENSE AND ID'S	
Germany (EU Source)	€37.95
Canada	$400-$1,000
China	$600
Other (Including U.S.)	$500-$800
Diplomatic passports and paperwork	$2,000
U.S. Document Templates and Forgeries (utility bills, bank statements, passports, SSN cards, driver's license- 46 states)	$10-$50
Forged Prescriptions - Large U.S. Drug Stores	$50 - $100

Figure 6. P. 8. Banking & Online Payment Account Credentials. Prices in USD.
Figure 7. P. 9. Identities, Social Security information, Passports and other documents. Prices in USD.

It's easy to think that identity theft stops with the physical world where the biggest worry is that a stranger might have everything they need to walk into businesses and government offices and successfully assume your identity. There is another aspect to identity theft however that is less obvious and, often, more personal and insidious. In this digital age, a continually growing population is becoming inextricably linked to their online personas. Social media and other seemingly innocuous online accounts have more value than one might think. Compromising these accounts can allow an attacker to assume the victim's online persona and use the account for spam campaigns, malware distribution and other activity.

It should come as no surprise then, that these accounts are available for purchase in the underground. One vendor the TRU team spotted offered 1,000 Instagram accounts for a price of $15, 2,500 for $25, 5,000 for $40 and 10,000 for $60. Another seller offered budding cybercriminals a program the seller claimed could hack into accounts for Facebook, Netflix, Twitter and other services for $12.99.

Outside of the valuable PII and credit card data in online account profiles, there are other less obvious ways that perpetrators can use your accounts. For example, social media accounts are often used by attackers to conduct reconnaissance for other crimes. The people you communicate with, how you communicate with them, your personal preferences and other personal details are used to not only deepen identity theft, but also for targeted attacks via social engineering, such as phishing and spam campaigns.

Having hundreds or thousands of accounts in a particular service enables the perpetrator to engage in botnet-like activities. Examples of this type of activity range from artificially boosting "Likes" or views on social media to swaying public opinion and even election results. Stealing established accounts with histories associated with them makes these campaigns more effective and harder to detect.

VALUABLE SOCIAL MEDIA ACCOUNTS

$12.99

ACCOUNT HACKING PROGRAM
USED TO HACK SOCIAL MEDIA ACCOUNTS

HACKED ACCOUNTS ARE THEN USED TO:

Purchase Products | Broadcast | Verification | Cashouts and more.

MO' MONEY

Another seemingly unlikely piece of data attackers can turn into profits are airline and hotel rewards points. These points are meant of course to be redeemed by legitimate customers to obtain discounts on flights and hotel stays. But the idea of discounted travel and lodging is valuable to criminals as well. As a result, cybercriminals are using these stolen points to offer travel and hotel packages to willing buyers. These underground travel agencies can potentially offer significant discounts for travelers. In addition, there are services called mileage brokers that pay people to transfer points. The points can also be redeemed for gift cards through certain sites.

Other times, cybercriminals sell the points directly. In one case, a vendor offered access to a Southwest Airlines rewards account with at least 50,000 miles for $98.88. The same seller offered access to accounts with at least 100,000 miles for $148.88 and 150,000 miles or more for $198.88. The price for a Scandinavian Airlines rewards points account with a minimum of 150,000 miles was $99.99.

Whether it is airline rewards points or credit card information, attackers have their eyes on your data. As much as ever, it is critical both businesses and individuals don't lose sight of the risks they face.

AIRLINE REWARDS POINT ACCESS	
LARGE U.S. AIRLINE MILES ACCOUNT	
50,000 miles	**$98.88**
100,000 miles	**$148.88**
150,000 miles	**$198.88**
LARGE EUROPEAN AIRLINE MILES ACCOUNT	
25,000 miles	**$34.99**
100,000 miles	**$89.99**
200,000 miles	**$119.99**

HOTEL REWARDS POINT ACCESS	
LARGE INTERNATIONAL HOTEL CHAIN REWARDS POINTS ACCOUNT	
50,000 points	**$74.99**
150,000 points	**$139.99**

Figure 8. P.10. Account Hacking Programs and uses. Price in USD. **Figure 9.** P.11. Airline Rewards Point Access Prices in USD. **Figure 10.** P.11. Hotel Rewards Point Access. Prices in USD.

PROTECT YOUR DATA

Whether you are a small business owner, an enterprise executive or a private individual using a computer from the comfort of your home, there are attackers who are interested in your data. As long as these markets continue to thrive, cyberattacks will remain a constant threat, making it vital business leaders arm their security teams with the resources they need to keep information secure.

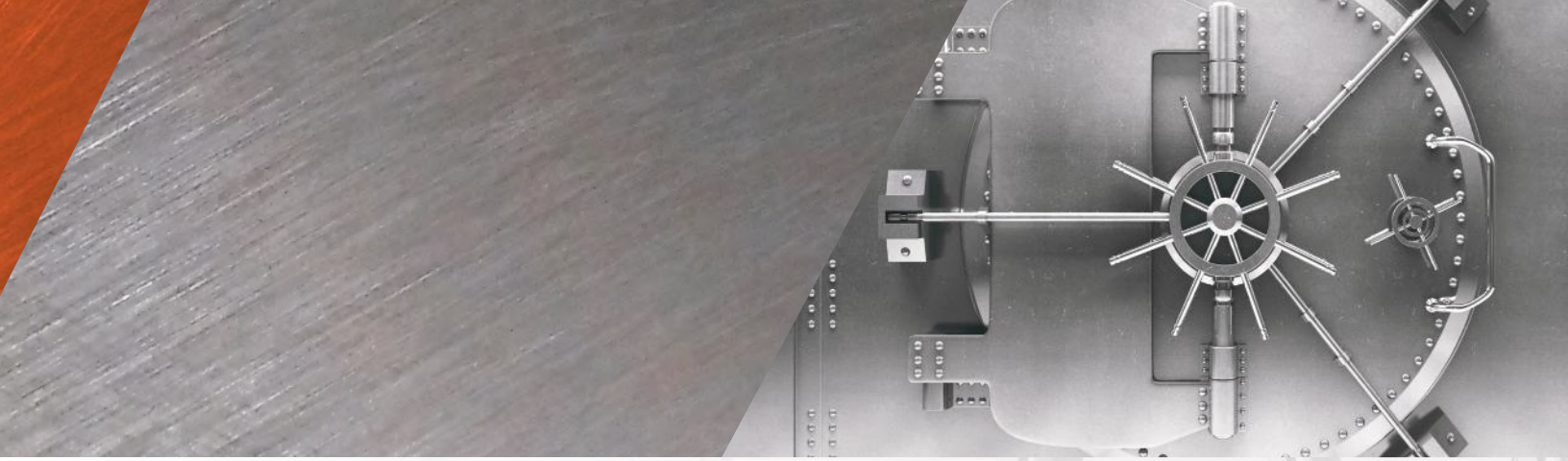
Our experts probe both the Dark Web and Deep Web to keep tabs on how the black market is evolving, what tools are emerging and their cost, what types of data is available and for how much, and what threat actors are actively saying and doing. All of this provides a sense of the machinery behind the risk to organizations and our customers worldwide.

THROUGH ALL OF THIS, OUR MESSAGE IS THREEFOLD FOR BUSINESS LEADERS:

1. TOOLS TO ENABLE PERSONS TO COMMIT CYBERCRIMES ARE HIGHLY DEVELOPED, EASY TO ACQUIRE AND EASY TO USE, EVEN FOR NOVICES.

2. THE MARKET TO SELL AND BUY ILLEGALLY OBTAINED DATA IS WELL ESTABLISHED, AND BASED ON OUR MONITORING, ALL DATA HAS VALUE IN THE UNDERGROUND BLACK MARKET. IT'S ALL FOR SALE.

3. NO MATTER WHERE YOUR BUSINESS IS BASED AND NO MATTER WHAT MARKET YOU MAY OPERATE IN, YOUR ORGANIZATION IS OPEN FOR BUSINESS TO THREAT ACTORS ON A WORLDWIDE SCALE. ENABLE YOUR SECURITY LEADERS WITH THE RESOURCES TO DO WHAT IS NECESSARY TO PROTECT YOUR ORGANIZATION.



TIPS FROM (TRU) TEAM

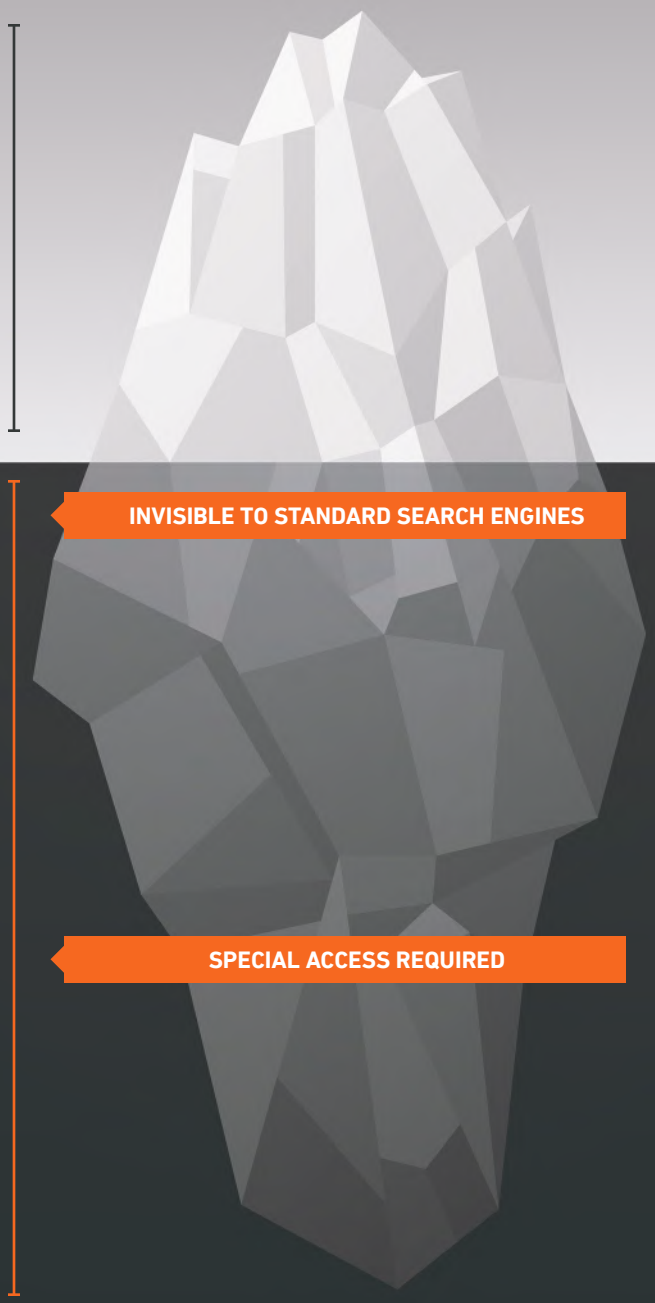
FOR IT AND SECURITY TEAMS:

- Train your employees on how to identify suspicious activity.
- Find, classify and protect your most sensitive data, particularly information impacted by compliance regulations such as PCI-DSS and HIPAA.
- Deploy patches as promptly as possible to shorten the vulnerability window.
- Employ data encryption to protect sensitive data in transit and at rest.
- Monitor cloud usage, manage access to cloud services, and secure any data or applications you migrate.
- Utilize security technologies such as firewalls, anti-malware software, and intrusion detection and prevent systems to build a shield around your environment.

FOR INDIVIDUALS:

- Do not click on suspicious links or open email attachments from unknown senders.
- Use anti-malware software.
- Update your software regularly for security patches.
- Be cautious accessing online banking sites, email or other sensitive sites when using public Wifi hotspots, as many lack strong security and can leave you susceptible to attacks.
- Do not use the same password for multiple websites or services and allow a single compromised account to turn into many.
- Consider using credit monitoring services to detect suspicious activity.

BENEATH THE SURFACE



SURFACE WEB

This represents everything on the Internet indexed by search engines such as Yahoo and Google, and is only a small portion of what is online.

DEEP WEB

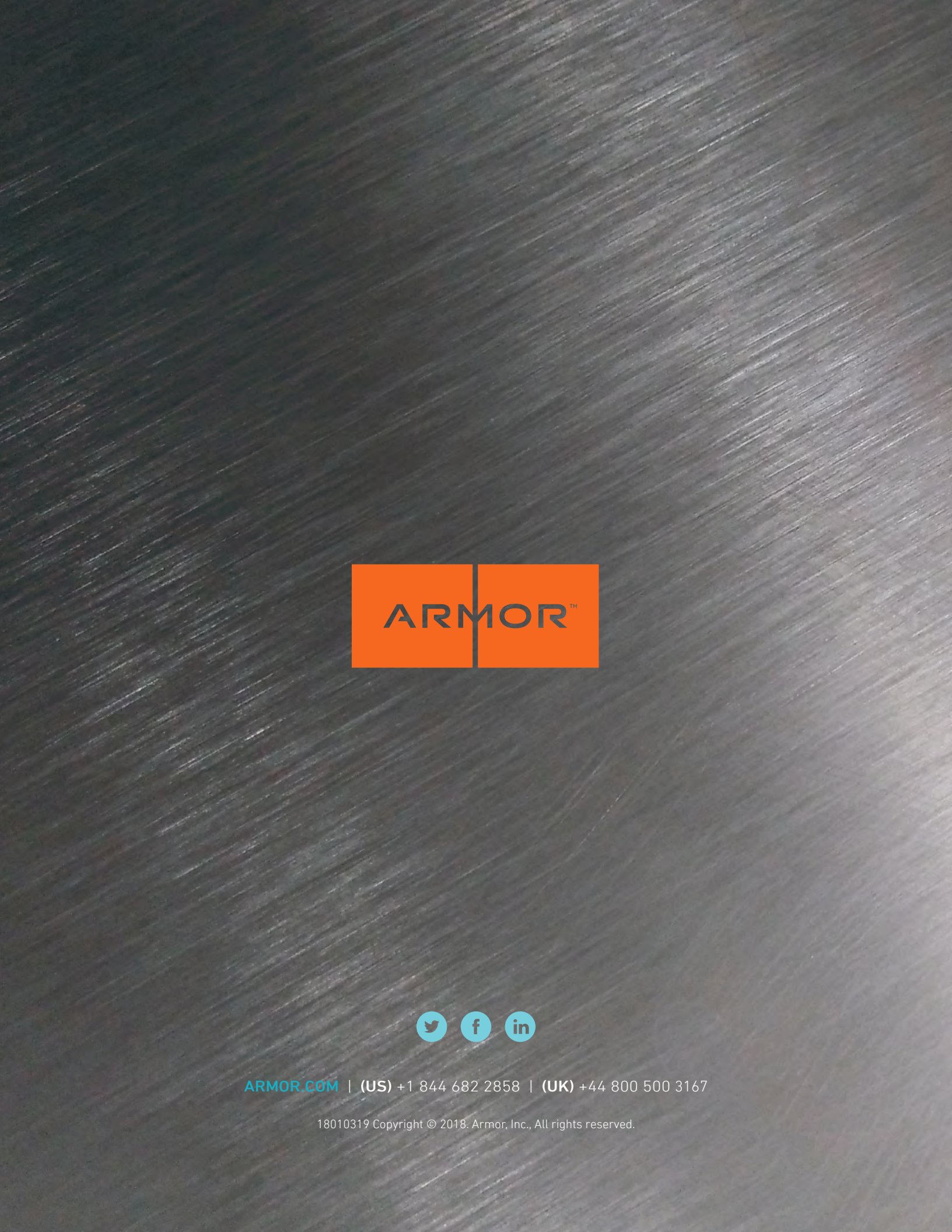
While sometimes confused with the term Dark Web, the Deep Web is the part of the Web not indexed by standard search engines, and represents the bulk of the content online. The vast majority of this content is innocuous.

DARK WEB

A subset of the Deep Web, the Dark Web refers to content on darknets and overlay networks that can only be accessed with specific software, configurations or authorization.

CONCLUSION

Unfortunately, cybercrime remains big business. Even with occasional law enforcement takedowns like the recent effort against the Infraud marketplace, the sophistication of market operators makes the illicit buying and selling of goods on the Web difficult to stop. From credit cards to social media accounts to social security numbers, all matter of data can be found in the corners of the Dark Web, and all of it can be turned into money. Imagine accessing your PayPal account only to find it's empty. Or discovering from a friend that your Facebook account is being used to send out links you didn't approve that are infecting others. While a password for an Instagram or an airline rewards program account may seem inconsequential next to a credit card number, as the report has shown, that information has value. With malware developers selling their wares to whoever will buy, the barrier for entry for cybercriminals remains low. The tools, documents and services threat actors need are readily available, which means big businesses, small organizations and home users alike need to follow security best practices and stay on guard to stay safe.



ARMOR.COM | **(US)** +1 844 682 2858 | **(UK)** +44 800 500 3167