

SEPTEMBER 2019

ARMOR



**THE ARMOR 2019 BLACK MARKET REPORT**

---

# A LOOK INSIDE THE DARK WEB

# CONTENT

---

## INTRODUCTION

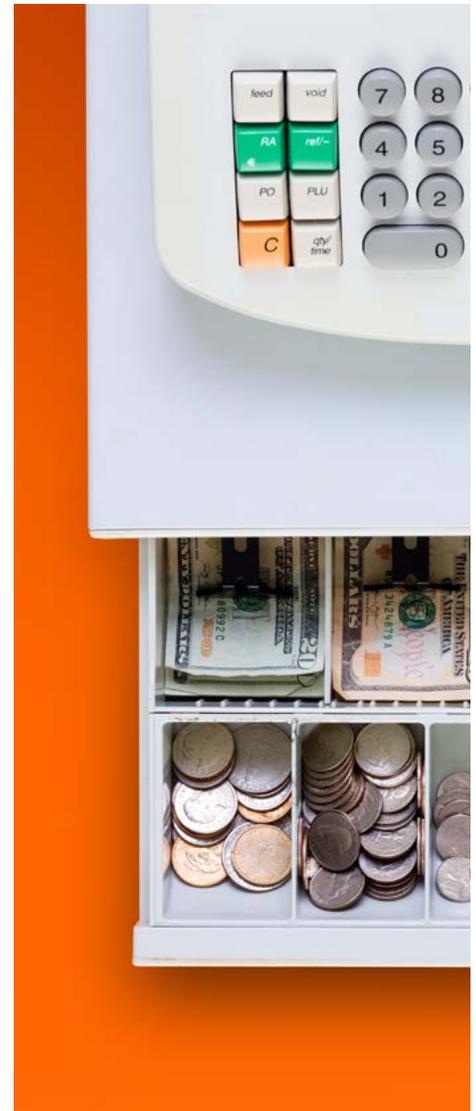
For all the money that is spent on cybersecurity, it is likely that at this very moment metaphorical cash registers are ringing throughout the cyber underground.

In the second-annual Armor Black Market Report, Armor's **Threat Resistance Unit (TRU)** research team once again dug deep into the underground economy for illicit goods and services. Not only can interested buyers purchase malware and stolen credit card data, but they can hire a fraudster to knock their competitor's website offline, upgrade their credit score, or steal a person's email credentials.

While examining approximately a dozen digital black markets and underground forums—both English- and Russian-speaking ones—the TRU team discovered several products and services that have risen in popularity since last year, as indicated by the numerous black markets now offering these items for sale.

The roster of products and services include “credentials to unhacked” Remote Desktop Protocol (RDP) servers for sale, and lucky buyers get to specify the server's location: London, Paris, Tokyo, New York, Sydney, you name it. The TRU team found cybercriminals offering to sell credentials to RDP Servers for a mere €18 to €22 a piece (\$20.29 to \$24.80).

What makes these RDP Servers so attractive to hackers? One of the ways cybercriminals are infecting organizations with ransomware is by targeting “open” RDP servers. Fraudsters then use the servers as their initial entry into the target's computer network.



First, the hackers scan the internet for “open” internet-facing servers running the RDP service. Once discovered, the attackers will attempt to use a brute-force, password-spray attack whereby they try logging into the server using common or default usernames such as “administrator” along with multiple commonly used passwords to gain access.

Once the threat actors have accessed the vulnerable RDP system, they simply use it as a steppingstone to the main area of the network and proceed to install ransomware onto target machines. From there they can encrypt files, including backups, and disable network protections.

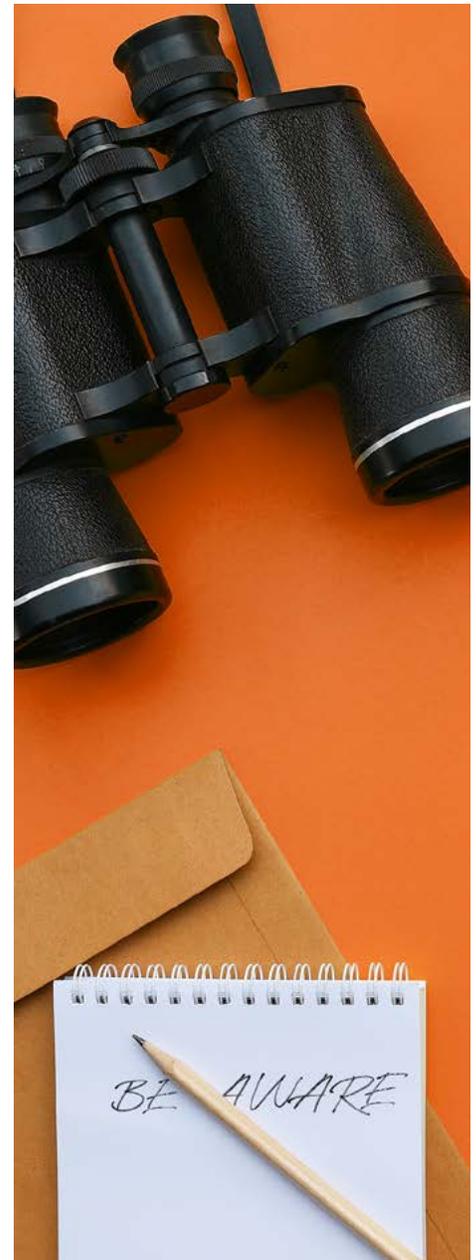
In 2019, as of Sept., Armor’s TRU team has identified 161 publicly reported ransomware attacks against organizations in the U.S. These include every type of entity, from municipalities and school systems to healthcare facilities and radio stations. Unfortunately, these are merely the victims that have been made public. The TRU team estimates there are thousands of other ransomware attacks that have resulted in the encryption of data belonging to public and private organizations around the globe, and these simply have not come to light. Thus, it makes sense that security researchers and cyber defenders would begin to see plenty of scammers selling access to unhacked RDP servers.

One of the most alarming trends the TRU team saw emerge this year was the number of cybercriminals selling cold, hard cash for only 10 cents to 12 cents on the dollar. Financial scammers are giving buyers the opportunity to purchase cash in various amounts—\$10,000, \$5,000, \$2,500—and all the buyer has to do is prepay the criminal their 10% to 12% fee in Bitcoin and provide them with a bank or Paypal account they would like the money transferred into. The buyer can also opt to have the money wired to them via Western Union. No longer do buyers have to purchase online bank account credentials, secure a money mule account to transfer the funds into, log into the stolen bank account, and conduct the money transfer themselves; they simply have to collect the money. It is a turn-key service for fraudsters who are not technically savvy.

Additionally, this arrangement works well for the cybercriminal selling the stolen funds because, ultimately, he or she is not taking possession of the funds but merely transferring them, which puts the majority of risk on the scammer buying the money. With the glut of online bank credentials and credit cards (which can be used to wire money via Western Union) for sale on the underground markets, it came as no surprise to the TRU team that the cybercriminals would figure out additional ways to monetize these illicit goods.

Other items that gained popularity this year were articles of incorporation and sole proprietorship papers. For those scammers who want to become high-end money mules, these documents are like gold because they come with an Employer Identification Number (EIN), which in turn enables a fraudster to open a business bank account. For money mules, larger amounts of money moving in and out of business bank accounts, as opposed to personal accounts, are less likely to flag a financial institution's fraud alerts. And being that money mules' bank accounts are so integral to the success of online financial fraud, it only makes sense that several key tools of their trade—articles of incorporation and sole proprietorship papers—would become a hot commodity.

The TRU team is confident that, like this year, it will see new and different trends emerge in 2020. And although the black markets and forums might change from year to year, one thing remains the same—cybercriminals are chasing profit. In fact, an early 2019 study from **Accenture** predicted cyberattacks worldwide could cost companies approximately \$5.2 trillion over the next five years. Therefore, every organization, no matter how big or how small, whether public or private, is at risk for becoming a victim of cybercrime. As a result, the risk extends to their customers, their employees, their business partners, and the list goes on. Thus, it is critical that businesses, as well as individuals, are aware of the current cyber threats, how the criminals are pulling off these digital crimes, and how best to protect one's organization and oneself against these cyber assaults. It will take every entity and every individual working together to ensure that the internet remains a safe place for good people and good organizations to thrive.



## PRICE LIST FOR HACKER GOODS & SERVICES

| CREDIT CARD DATA WITH CVV NUMBERS  |           |             | DOB +       | BIN +       |
|--|-----------|-------------|-------------|-------------|
| <br>    | U.S.      | \$5 - \$12  | \$15 - \$25 | \$15        |
|  | U.K.      | \$15 - \$20 | \$25 - \$30 | \$20 - \$30 |
|  | Canada    | \$10 - \$20 | \$15 - \$25 | \$20 - \$25 |
|  | Australia | \$5 - \$25  | \$13 - \$35 | \$8 - \$30  |
|  | EU        | \$14 - \$30 | \$20 - \$40 | \$30 - \$35 |
| <br> | U.S.      | \$5 - \$15  | \$15 - \$25 | \$15        |
|  | U.K.      | \$10 - \$25 | \$25 - \$30 | \$20 - \$30 |
|  | Canada    | \$15 - \$25 | \$15 - \$25 | \$20 - \$25 |
|  | Australia | \$8 - \$30  | \$13 - \$35 | \$8 - \$30  |
|  | EU        | \$18 - \$35 | \$20 - \$40 | \$30 - \$35 |

| CREDIT CARD DATA WITH TRACK 1 AND 2 DATA |               |
|--|---------------|
| U.S.                                     | \$85 - \$110  |
| U.K.                                     | \$100 - \$110 |
| Canada                                   | \$110 - \$120 |
| Australia                                | \$110 - \$120 |
| EU                                       | \$120 - \$150 |

| CLONE CREDIT & ATM CARDS |                   |
|--------------------------|-------------------|
| PRICE                    | CARD BALANCE      |
| \$100                    | \$2,000           |
| \$250                    | \$3,000           |
| \$350                    | \$4,000           |
| \$200 - \$400            | \$5,000           |
| \$600                    | \$7,000           |
| \$800                    | \$10,000          |
| \$900                    | \$12,000          |
| \$1,000                  | \$15,000          |
| € 150                    | € 2,000 / £ 2,000 |
| € 300                    | € 5,000 / £ 5,000 |
| € 450                    | € 8,000           |
| € 550                    | € 10,000          |

| PAYPAL ACCOUNTS |                    |
|-----------------|--------------------|
| AVERAGE PRICE   | BALANCE            |
| \$50            | \$500              |
| \$60            | \$600              |
| \$80            | \$800              |
| \$100           | \$1,000 - \$2,000  |
| \$200           | \$1,500 - \$4,500  |
| \$250 - \$300   | \$2,500 - \$8,500  |
| \$500 - \$550   | \$5,000 - \$13,000 |

| BANK CREDENTIALS   |                   |                   |
|--|-------------------|-------------------|
| TYPE   | AVERAGE PRICE     | ACCOUNT BALANCE   |
| <br><br>                                       | \$150 - \$300     | \$3,000           |
|  | \$250 - \$500     | \$5,000 - \$6,000 |
|  | \$400 - \$600     | \$8,000           |
|  | \$600 - \$800     | \$12,000          |
|  | \$800 - \$1,000   | \$15,000          |
|  | \$1,000 - \$1,200 | \$20,000          |
| <br>LLOYDS BANK<br><br>BARCLAYS<br><br>HSBC | \$300 - \$400     | £3,000 - £5,000   |
|  | \$600             | £6,000 - £12,000  |
|  | \$700 - \$800     | £10,000 - £16,000 |
|  | \$900 - \$1,000   | £12,000 - £20,000 |
|  | \$1,000 - \$1,200 | £16,000 - £30,000 |
|  | \$1,500           | £20,000           |

| FULLZ DATA |               |  |
|------------|---------------|--|
| ORIGIN     | AVERAGE PRICE | INCLUDES   |
| U.S.       | \$30 - \$40   | Full Name<br>Date of Birth<br>Address<br>City<br>Zip Code<br>State<br>Country<br>Phone Number<br>Mother's Maiden Name<br>Social Security Number<br>Driver's License Number |
| U.K.       | \$35 - \$50   |  |
| CANADA     | \$30 - \$45   |  |
| AUSTRALIA  | \$17 - \$50   |  |
| ITALY      | \$20 - \$25   |  |
| SPAIN      | \$20 - \$25   |  |
| DENMARK    | \$25 - \$30   |  |
| SWEDEN     | \$20 - \$25   |  |
| FRANCE     | \$20 - \$25   |  |
| GERMANY    | \$20 - \$25   |  |
| IRELAND    | \$20 - \$25   |  |
| MEXICO     | \$15 - \$20   |  |
| ASIA       | \$15 - \$20   |  |
| Other EU   | \$17 - \$60   |  |

| RANSOMWARE AND RANSOMWARE-AS-A-SERVICE (RaaS) |  |
|---|--|
| TYPE  | PRICE  |
| Generic Ransomware #1                         | \$225  |
| Generic Ransomware #2                         | \$660  |
| Inpivx  | Ransomware + Panel + Tutorial = \$500   Ransomware-only – \$300   Panel-only – \$200 |
| Ranion-(RaaS)                                 | 12 Months – \$900   6 Months – \$490   1 Month – \$120                               |
| Megacortex                                    | \$1,000 or €1,000 + 10% of Ransom  |

### UNHACKED REMOTE DESK PROTOCOL SERVERS

|  |                              |
|--|------------------------------|
| Japan, Sydney, Australia-Based RDPs  | €22 (\$24.64) per RDP Server |
| Unhacked RDP servers in multiple countries including the U.S. and many in Europe, including the U.K. | €18 (\$20.16) per RDP server |

### BANKING TROJANS/EXPLOIT KITS/MALWARE DROPPERS

| TYPE                                     | PRICE         |
|--|---------------|
| Emotet Trojan (spreader/malware dropper) | \$1,000       |
| Trickbot Banking Trojan                  | \$600         |
| TinyNuke                                 | \$6,000       |
| Parasite HTTP RAT                        | \$500         |
| Generic Exploit Kit                      | \$2,080/month |
| Fallout Web Exploit Kit                  | \$300/week    |
| Drupal RCE Exploit                       | €71           |
| Android Clipper (SMS stealer)            | \$150         |
| Chip POS                                 | \$700         |

### CORPORATE PAPERS

|   |            |         |
|---|------------|---------|
| Sole proprietorship papers complete with Employer Identification Number (EIN) | \$1,611.27 | €1,429  |
| EIN and Articles of Incorporation   | \$811.04   | €719.29 |

### AWS VIRTUAL PRIVATE SERVER

|         |                |
|---------|----------------|
| AWS VPS | \$25 per month |
|---------|----------------|

| GIFT CARDS  |         |       |
|---|---------|-------|
| TYPE  | BALANCE | PRICE |
| <br><br><br> | \$1,000 | \$100 |
|   | \$2,500 | \$200 |
|   | \$3,000 | \$300 |
|   | \$4,000 | \$500 |
|   | \$5,000 | \$650 |
|   | \$7,000 | \$800 |

| ATM AND POINT-OF-SALE (POS) SKIMMERS |         |
|--------------------------------------|---------|
| ATM SKIMMERS                         | PRICE   |
| Wincor with keypad                   | \$700   |
| Wincor Nixdorf                       | \$1,200 |
| Wincor                               | \$1,200 |
| Slimm                                | \$1,200 |
| NCR                                  | \$1,200 |
| Diebold Opteva                       | \$1,000 |
| Diebold                              | \$800   |
| Universal                            | \$1,500 |
| Small                                | \$1,200 |
| Chip POS                             | \$700   |

| COMPUTERS/PHONES |       |
|------------------|-------|
| ITEM             | PRICE |
| Apple laptop     | \$250 |
| Dell/HP laptop   | \$140 |
| Toshiba laptop   | \$140 |
| Samsung laptop   | \$140 |
| Vaio laptop      | \$200 |
| iPhone 3gs       | \$130 |
| iPhone 4g        | \$160 |
| iPhone 4gs       | \$190 |
| iPad 2gs         | \$180 |
| Blackberry       | \$150 |

| DDOS ATTACK          |
|----------------------|
| \$60/hour            |
| \$280/day            |
| \$479-\$659 per week |
| \$2,000 per month    |

| SPAMMING SERVICES |         |        |
|-------------------|---------|--------|
| 20,000 emails     | \$35.56 | €31.50 |
| 50,000 emails     | \$60.95 | €53.99 |

| MONEY TRANSFER SERVICES   |                   |                     |
|---|-------------------|---------------------|
| TYPE  | AVERAGE PRICE     | BALANCE             |
|    | \$150 - \$240     | \$1,800 - \$2,400   |
|   | \$300 - \$400     | \$3,500 - \$4,500   |
|   | \$500 - \$550     | \$6,000 - \$7,000   |
| BANK TRANSFERS  | \$150 - \$250     | \$1,800 - \$2,500   |
|   | \$250 - \$350     | \$3,000 - \$3,500   |
|   | \$350 - \$450     | \$4,500             |
|   | \$500             | \$5,000 - \$7,000   |
|   | \$700 - \$800     | \$9,000 - \$10,000  |
|   | \$1,000 - \$1,300 | \$15,000            |
|  | \$120 - \$200     | \$1,200 - \$1,500   |
|   | \$180 - \$250     | \$1,800 - \$2,500   |
|   | \$300 - \$350     | \$4,000 - \$4,500   |
|   | \$500 - \$550     | \$5,000 - \$7,000   |
|   | \$700             | \$9,000 - \$10,000  |
|   | \$800 - \$900     | \$10,000 - \$12,000 |
|   | \$1,000           | \$15,000            |
| Skrill  | \$150             | \$1,800             |
|   | \$250             | \$3,000             |
|   | \$350             | \$4,500             |
|   | \$500             | \$7,000             |
|   | \$700             | \$8,000 - \$9,000   |
|   | \$800             | \$10,000            |
|   | \$900             | \$12,000            |
|   | \$1,000           | \$15,000            |

| SOCIAL MEDIA  |                   |                 |
|---|-------------------|-----------------|
| TYPE  | SERVICES          | PRICE PER 1,000 |
|  TWITTER     | Likes             | \$10            |
|   | Retweets          | \$14            |
|   | Poll Votes        | \$3             |
|  FACEBOOK    | Post Likes        | \$2             |
|   | Events Interested | \$6             |
|  YOUTUBE   | Views             | \$1             |
|   | Subscribers       | \$20            |
|   | Likes/Dislikes    | \$17            |
|  INSTAGRAM | Followers-Male    | \$6             |
|   | Followers-Female  | \$6             |
|  TWITCH    | Channel Views     | \$4             |
|  LINKEDIN  | Network           | \$15            |
|  TELEGRAM  | Group Members     | \$10            |

| CREDIT CARD TOP-UP RATES |                  |
|--------------------------|------------------|
| PRICE                    | BALANCE INCREASE |
| \$150                    | \$1,800          |
| \$250                    | \$3,000          |
| \$500                    | \$7,000          |
| \$700                    | \$9,000          |

| CHANGES TO CREDIT HISTORY |          |         |
|---------------------------|----------|---------|
| Remove Negative Item      | \$152.39 | €134.98 |
| Add Item                  | \$304.78 | €269.96 |

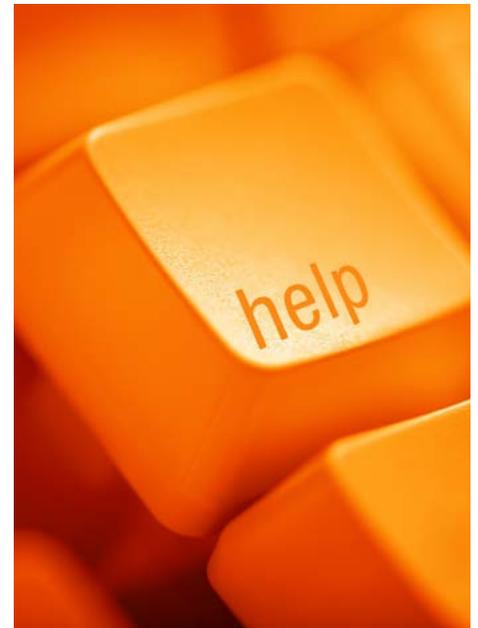
## CYBERCRIME INC.

---

The online black market for malware, stolen information, and illicit services functions with much of the same ebb and flow of the legitimate market. The laws of supply and demand still apply, and one's business reputation can make or break sales.

Some of these underground markets operate similarly to online stores such as Amazon, where users can have an account, message the seller, and write reviews about the products and services they receive. Many markets operate on escrow, and some sellers even offer money-back guarantees if the customer is not satisfied or the product does not meet the customer's needs.

Underground markets also are places where scammers exchange information, discussing tactics and sharing advice. When it comes time to do business, the cyber underground has no shortage of items lining its digital shelves. With the right amount of money, shoppers can buy everything from full identities to cloned ATM cards, stolen credit cards to malware.



## CRYPTOCURRENCY'S ROLE

---

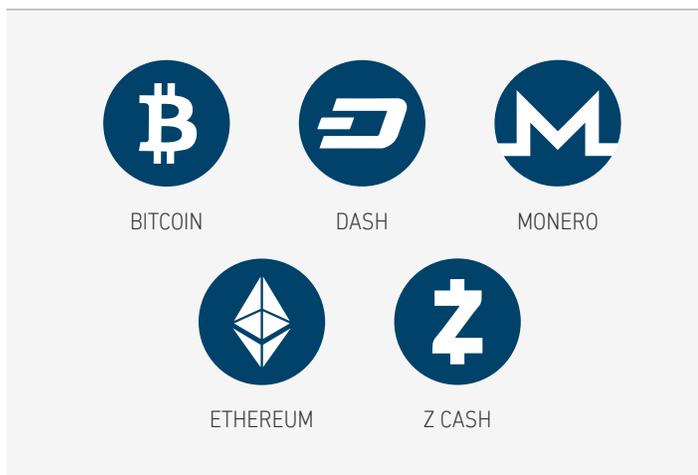
In October 2008, a white paper published online in an obscure email list introduced the world to a new form of money—one that included features attractive to cybercriminals. The paper, **“Bitcoin: A Peer-to-Peer Electronic Cash System,”** published under the name Satoshi Nakamoto, introduced the world to the first truly workable, global digital currency. While not intended for cybercrime, Bitcoin would find its proof of concept in dark markets.

Bitcoin ushered in a pseudo-anonymous way of making digital purchases, with a form of money that was encrypted, faster than wire transfers, and wasn't tied to any government monetary system or central bank. From 2011-2013, dark markets created a unique use case for Bitcoin on a website called the Silk Road. This website sold everything from drugs and firearms to stolen credit cards and passports.

While every Bitcoin transaction is posted and visible on an immutable, open ledger (and thus not completely anonymous), no other personal information is attached to transactions, and third parties such as banks or wire transfer companies are unnecessary. Thus, when it comes to "following the money," Bitcoin transactions make law enforcement tracking efforts very difficult. Once collected, Bitcoin can also be laundered or "tumbled" through a variety of techniques to further obscure the money trail.

Today, less than 1% of the world's population owns or transacts in Bitcoin. However, **one 2018 study** by the University of Sydney stated \$76 billion annually, or 46% of Bitcoin transactions, is involved in cybercrime. In 2019, Bitcoin continues to be the leading currency for transactions in the dark market. The Armor TRU team found that most vendors in 2019 almost exclusively accept Bitcoin as payment. Bitcoin is also used as the primary payment mechanism in the case of ransomware, although there have been instances of payments being required in Monero (Kirk, SpriteCoin ransomware), Bitcoin Cash (Thanatos ransomware), Ethereum (HC7 Planetary ransomware), and Dash (Anatova ransomware).

While a number of cryptocurrencies have been introduced with enhanced anonymity features such as Monero, Dash, and ZCash, Bitcoin remains the most trusted and most valuable choice in dark markets. In the case of ransomware, for example, asking for ransom in Monero or Dash would require a level of sophistication on the part of victims that simply does not commonly exist. With a current market cap of \$175 billion\*, Bitcoin's value, network strength, and ability to obscure payments for criminals will continue to dominate dark markets.



Bitcoin market cap as of July 26, 2019, at 9 a.m.

## CYBERCRIME-AS-A-SERVICE

In the **2018 edition of Armor's Black Market Report**, TRU researchers found that cybercrime-as-a-service activities were among the most popular items for sale.

Chief among these were Distributed Denial of Service (DDoS)-for-hire businesses, which at the time offered their services for as little as \$10 per hour or \$200 for a day. These services can cause significant disruption for businesses. In December 2018, the U.S. Department of Justice **announced** the seizure of 15 internet domains associated with DDoS-for-hire services as well as criminal charges against three defendants. According to the Department of Justice, these services have been linked to attacks on victims ranging from financial institutions to universities.

In this year's report, the TRU team found that many DDoS services did not publicly advertise their prices. However, Armor researchers did see one criminal selling their DDoS service for \$60 per hour, \$280 per day, \$479-\$659 per week, and \$2,000 per month.



Spamming-for-hire remains a profitable racket as well. In one case, a seller offered to spam 50,000 email addresses at a cost of just €53.99 (\$60.95). The cost for 20,000 spam messages was €31.50 (\$35.56).

|  |   |  |
|--|---|--|
|   | <p><b>EMAIL BOMBER 50,000 PIECES</b><br/>                     Item #36775 - Services / Other - ██████████ (9)<br/> <b>Views: 21 / Sales: 0</b><br/> <b>Quantity Left: Unlimited</b></p> | <p><b>BUY PRICE:</b><br/> <b>EUR €53.99</b><br/>                     (0.007876 BTC)<br/> </p>   |
|  | <p><b>EMAIL BOMBER 20,000 PIECES</b><br/>                     Item #36776 - Services / Other - ██████████ (9)<br/> <b>Views: 9 / Sales: 0</b><br/> <b>Quantity Left: Unlimited</b></p>  | <p><b>BUY PRICE:</b><br/> <b>EUR €31.50</b><br/>                     (0.004595 BTC)<br/> </p> |

Email spamming services being sold on the underground.

In addition to these services, buyers can also purchase other services related to fraud. For example, one seller offered to remove negative items from the buyer's credit history for €134.98 (\$152.39). An offer to add information to a credit report was also available, with the activity costing €269.96 (\$304.78).

|   |  |   |
|---|--|---|
|  | <p><b>REMOVE ALL NEGATIVE ITEMS FROM YOUR CREDIT REPORT</b><br/>                     Item #26746 - Services / Other - ██████████ (1)<br/> <b>Views: 79 / Sales: 0</b><br/> <b>Quantity Left: Unlimited</b> (Unlimited automatic items)</p> | <p><b>BUY PRICE:</b><br/> <b>EUR €134.98</b><br/>                     (0.007876 BTC)<br/> </p> |
|---|--|---|

A threat actor offering to remove negative items from your credit report.

Offering fraudulent social media “Likes” and “Followers” is a profitable service as well. With “social media influencers” becoming more like business owners, the prospect of purchasing “Likes” and “Followers” has become more attractive. In Armor’s examination of the underground, there was no shortage of sellers offering “Followers” and “Likes” to customers at a price.

One seller offered 1,000 “Likes” on Twitter for €9 (\$10). One thousand retweets can be purchased for €12.59 (\$14). Facebook “Likes” were even less, coming in at a price of €1.80 (\$2) for 1,000 “Likes.” For LinkedIn users, 1,000 “Followers” (network connections) can be purchased for €12.49 (\$15).

Buyers can purchase Twitter “Likes,” “Retweets,” and LinkedIn “Followers” for a song.

|   |  |  |
|---|--|--|
|    | <b>TWITTER LIKES   1,000 FOR \$10</b><br><small>Item #18567-Services/Other - (536)</small><br><b>Views: 105 / Sales: 0</b><br><b>Quantity Left: Unlimited</b>              | <b>BUY PRICE:</b><br><b>EUR €9.00</b><br><small>(0.001310 BTC)</small><br>    |
|    | <b>TWITTER RETWEETS   1,000 FOR \$14</b><br><small>Item #18562-Services/Other - (536)</small><br><b>Views: 105 / Sales: 0</b><br><b>Quantity Left: Unlimited</b>           | <b>BUY PRICE:</b><br><b>EUR €12.59</b><br><small>(0.001435 BTC)</small><br>   |
|  | <b>TWITTER POLL VOTES   1,000 FOR \$3</b><br><small>Item #18564-Services/Other - (536)</small><br><b>Views: 104 / Sales: 0</b><br><b>Quantity Left: Unlimited</b>          | <b>BUY PRICE:</b><br><b>EUR €2.70</b><br><small>(0.000393 BTC)</small><br>  |
|  | <b>LINKEDIN FOLLOWERS   1,000 FOR \$15</b><br><small>Item #18565 - Services / Other - (536)</small><br><b>Views: 91 / Sales: 0</b><br><b>Quantity Left: Unlimited</b>      | <b>BUY PRICE:</b><br><b>EUR €12.49</b><br><small>(0.001966 BTC)</small><br> |
|  | <b>TELEGRAM GROUP MEMBERS   1,000 FOR \$10</b><br><small>Item #18567 - Services / Other - (536)</small><br><b>Views: 104 / Sales: 0</b><br><b>Quantity Left: Unlimited</b> | <b>BUY PRICE:</b><br><b>EUR €9.00</b><br><small>(0.001310 BTC)</small><br>  |
|  | <b>TELEGRAM POST VIEWS   1,000 FOR \$4</b><br><small>Item #15568 - Services / Other - (536)</small><br><b>Views: 115 / Sales: 0</b><br><b>Quantity Left: Unlimited</b>     | <b>BUY PRICE:</b><br><b>EUR €3.60</b><br><small>(0.000524 BTC)</small><br>  |

Another hacker advertised the following services:



**\*\*\*\*WEBSITE HACK & SECURITY \*\*\*\***

Hey, we can Unlock computer systems for you and do the following: for example

- Spy for you on (competitors, employees, children, lovers)
- Credit score upgrade
- Driving under influence / Criminal records removal
- Derogatory Remark Removal
- Charge-off Negotiation/Removal
- Fix your collection account
- Retrieve lost files/documents
- Content removal
- Test score upgrade
- Source for test/exam questions and answers
- Get your account Verified on Twitter/Instagram
- Any Kinds of Countries Passport worldwide
- Upgrade University Grades
- Delete unwanted online Pictures and Videos on any website
- Tracing peoples background
- Hack bank accounts
- Apps hacking
- Loading all MasterCard, Bank Accounts, PayPal, Bitcoin, WU,

---

**We also hack:**

Facebook, Twitter, Instagram, Line, Skype, Yahoo, Gmail passwords etc.

Do you need to keep an eye on your spouse by gaining access to their emails?

As a parent do you want to know what your kids do on a daily basis on social networks?

**\*\*\*\*Tutorials and e-books & more**

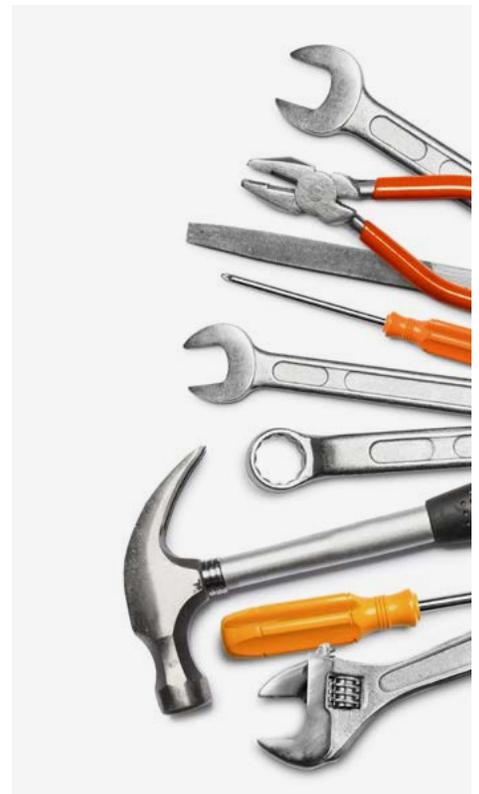
## MALWARE: A STAPLE OF THE UNDERGROUND MARKET

### EXPLOIT KITS, REMOTE ADMINISTRATION TOOLS (RATS), AND RANSOMWARE

Just as a handyman needs his tools, so too does a criminal hacker. For the hacker, this means exploit kits, remote administration tools (RATs) and other types of malware, such as ransomware. An exploit kit is essentially an all-in-one package used to identify and exploit software vulnerabilities on targeted computers so that hackers can download their choice of malicious software on the targeted computer. This could be anything from banking malware to DDoS code to a crypto miner. Exploit kits are typically designed to be modular and are updated to add newer exploits to replace older ones.

The TRU team spotted one exploit kit, aptly titled “Fallout Web Exploit Kit,” being rented for \$300 a week, while another fraud group offered to lease their exploit kit for \$2,080 a month. These same fraudsters went on to promise their customers that as long as the website or websites they chose to exploit had high traffic, they would deliver an exploit rate of approximately 1% of the website’s traffic, explaining: “if you have 40k unique visitors per day, you can get approximately 400 High Quality Bots per day, and if the GEO of the traffic is good then this can be very valuable.” The scammers bragged further about their exploit kit, enumerating its “fine” qualities:

- Bots Last Longer
- Bots are High Quality and contain excellent logs
- Bots mostly clean, not containing other malware
- Bots not using outdated systems
- Bots using All browsers, not just Internet Explorer



In another case, a seller was seen offering an iOS exploit that claimed to “permanently crash iPhone versions 4 through 8 Plus.” The seller stated that only four copies of the malware would be sold, and the price would go up with each copy. The seller offered the first copy for \$1,000. Purchases could be made in Bitcoin, though trusted buyers could also purchase it directly via PayPal. The TRU team also saw the Drupal RCE Exploit Kit being offered for €71 (\$80).

|   |  |  |
|---|--|--|
|  | <p><b>[POWERFUL] DRUPAL RCE Exploit [Fully Weaponized] [88% BUILDS VULN]</b><br/>                 Item #52141-Software &amp; Malware/Exploits - ██████████ (45)<br/> <b>Views: 39 / Sales: 1</b><br/> <b>Quantity Left: 24</b> (674 Automatic Items)</p> | <p><b>BUY PRICE:</b><br/> <b>EUR €71.74</b><br/>                 (0.009937 BTC)<br/> </p> |
|---|--|--|

Threat actor offering the Drupal Exploit Kit on the underground for \$80.

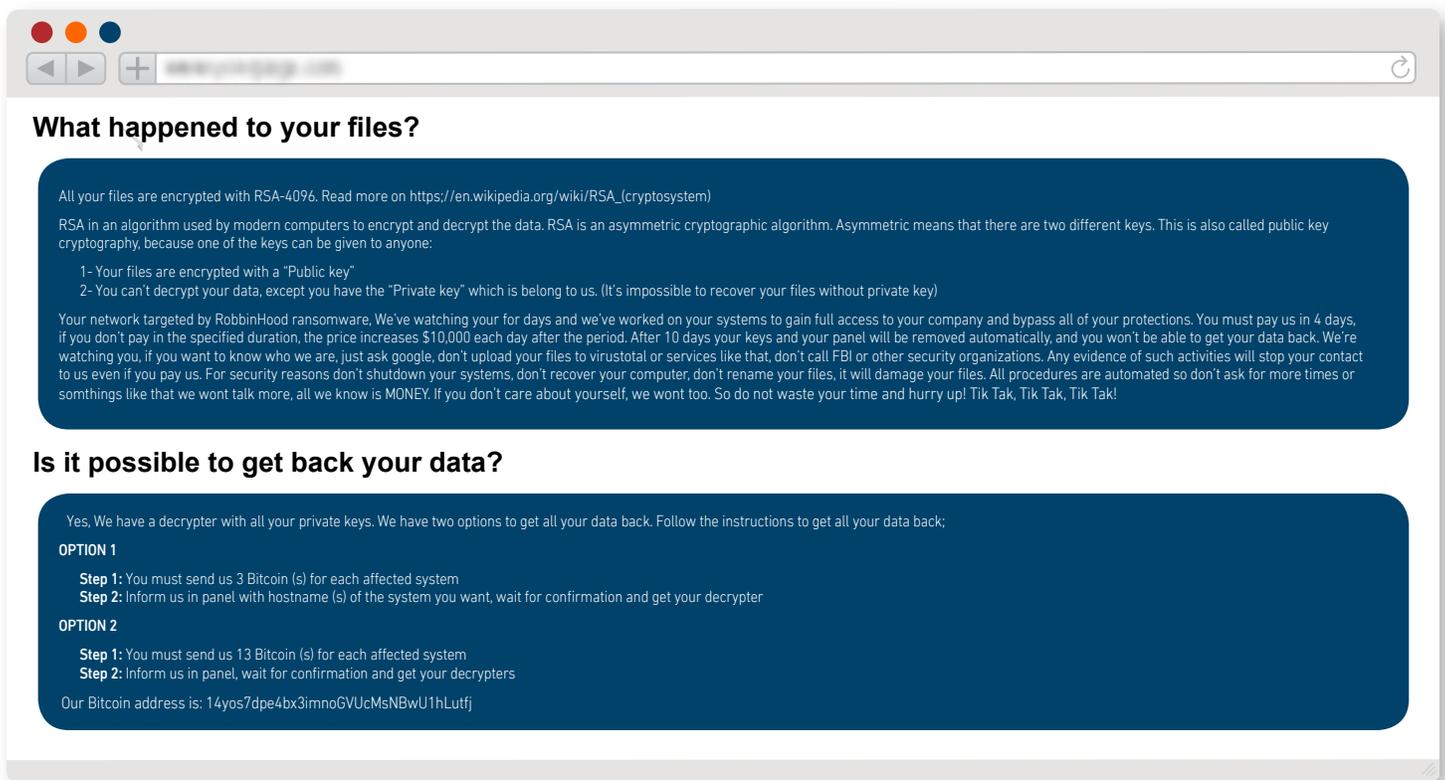
Just as prices for exploit kits can vary, so can prices for remote administration tools (RATs) and ransomware. Parasite HTTP, a highly sophisticated RAT, was observed being offered for \$500. A RAT is software that gives a person access to your computer system, just as if they had physical access to your device. With this access, the person can access your files, use your camera, and even turn on/off your device.

|   |  |   |
|---|--|---|
|  | <p><b>[MS] Set Up Remote Administration Tool Zeus BotNET (RAT) INSTANT DELIVERY</b><br/>                 Item #19974-Software &amp; Malware/Botnets &amp; Malware - ██████████ (3654)<br/> <b>Views: 258 / Sales: 5</b><br/> <b>Quantity Left: Unlimited</b> (Unlimited Automatic Items)</p> | <p><b>BUY PRICE:</b><br/> <b>EUR €2.28</b><br/>                 (0.000316 BTC)<br/> </p> |
|  | <p><b>DIAMONDFOX BOTNET ! ULTIMATE SNIFFER, STEALER, RAT</b><br/>                 Item #28629-Software &amp; Malware/Botnets &amp; Malware - ██████████ (56)<br/> <b>Views: 154 / Sales: 5</b><br/> <b>Quantity Left: Unlimited</b> (Unlimited Automatic Items)</p>                          | <p><b>BUY PRICE:</b><br/> <b>EUR €6.17</b><br/>                 (0.000855 BTC)<br/> </p> |

Zeus Botnet RAT and Diamondfox RAT for sale under \$10.

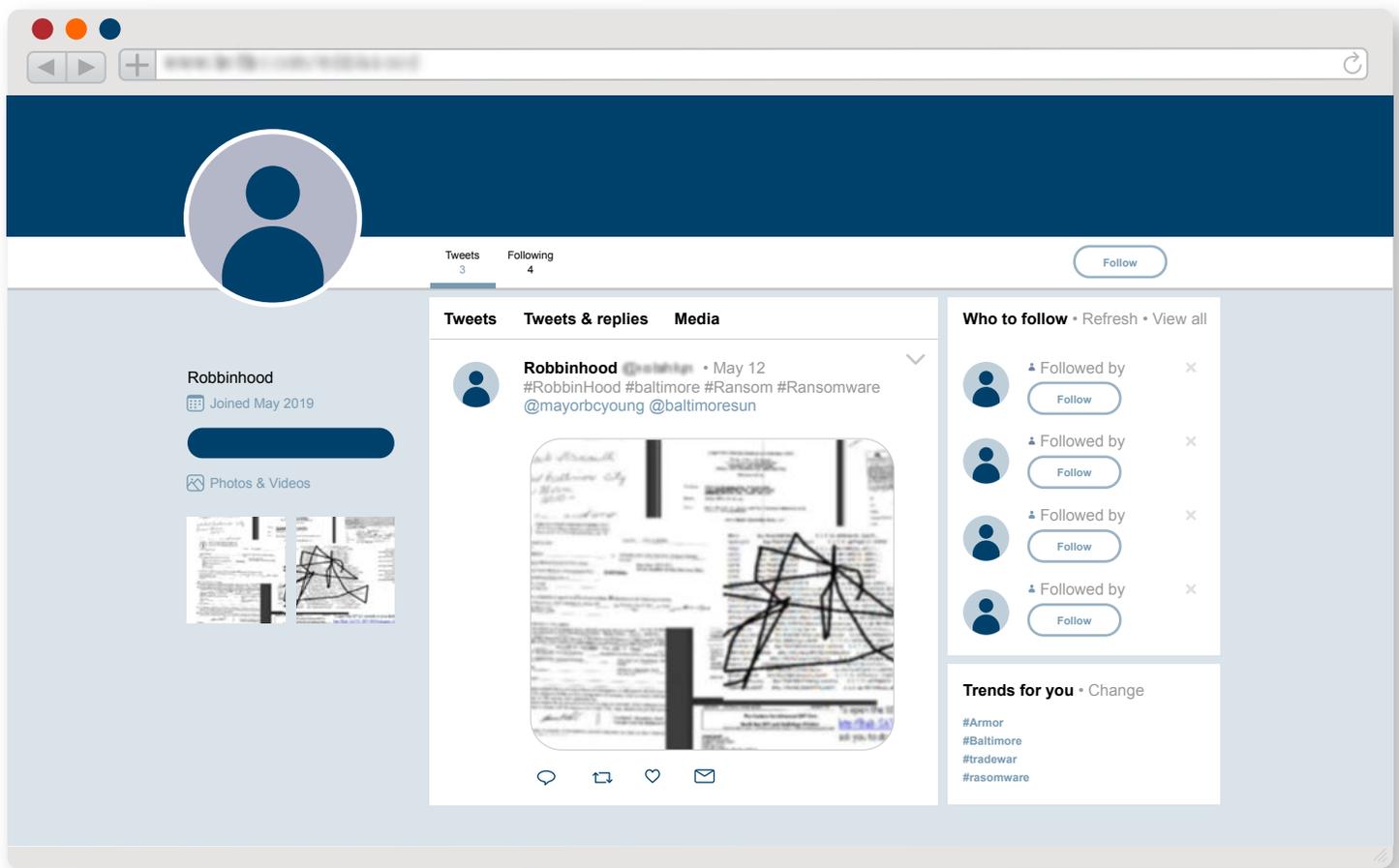
## RANSOMWARE IS ON A TEAR

Ransomware remains one of the most critical security threats facing organizations today. In May, Baltimore, Maryland, joined a list of over 60 municipalities hit by ransomware in 2019, according to the TRU team's **research**. The attack caused Baltimore to shut down most of its servers, though critical services such as EMS, police, and fire remained operational. In the case of Baltimore, the ransomware that was used was a new strain called Robbinhood.



Ransom message to the City of Baltimore.

Armor was able to track down the Robbinhood variant used against Baltimore and reverse engineer it. Armor's **analysis** revealed that the ransomware itself did not contain the NSA-created Eternal Blue exploit. However, it is possible that Eternal Blue was used by the ransomware criminals as a separate component to spread the Robbinhood ransomware. The TRU team also discovered that Robbinhood was structured as ransomware-as-a-service. As of August, it had not been spotted by the TRU team for sale on the underground, so the team believes that Robbinhood was a new ransomware service offering.



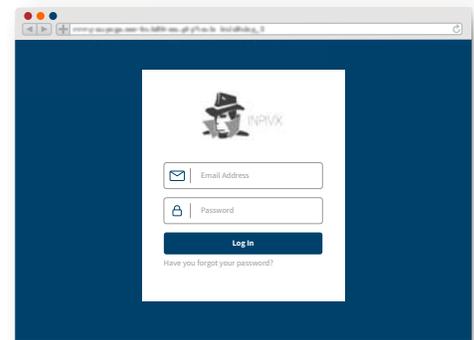
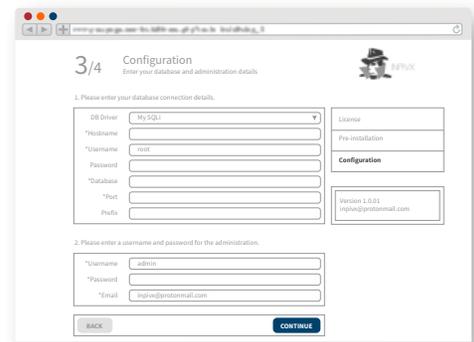
Twitter profile page for the threat actor behind the Baltimore ransomware attack.

On May 12, 2019, the TRU team spotted a member of a hacker forum who advertised that he or she was running a private, ransomware affiliate program. The person was looking to hire five threat actors, including spammers and fraudsters with access to Remote Desktop Protocol servers and network access, as well as owners of doorway pages. Doorway pages affect the index of a search engine by inserting results for particular phrases while sending visitors to a different page. The threat actor stated they had been in business for five years. They proposed a profit split of 40/60 with 60 percent going to affiliate members. After three successful operations, the profit split would change to 30/70. Interestingly, targeting the Commonwealth of Independent States (CIS) was prohibited by the hacker running the affiliate program. This may indicate that the CIS is the base of the threat actor's operation. (Note: The Commonwealth of Independent States is a **regional intergovernmental organization** of 10 **post-Soviet republics** in **Eurasia** formed following the **dissolution of the Soviet Union**.)

Interestingly, Brian Krebs referenced the same forum post in a July 19 story where he explored whether this new private ransomware affiliate program being recruited for is actually the Sodinokibi (also known as Sodin, REvil) ransomware program. Another interesting aspect of the Sodinokibi program is that several security research groups, including Cisco's Talos division and Dutch security firm Tesorian, have found clues of a possible link between Sodinokibi and the purportedly retired GandCrab ransomware, making some wonder if the same threat group is behind both GandCrab and the newer Sodinokibi ransomware program.

The TRU team also saw some ransomware malware being sold as a stand-alone product for \$225 and another ransomware family for \$650. However, the Inpivx ransomware tools were being offered as separate components or as a complete package:

- Inpivx Ransomware + Panel + Tutorial = \$500
- Inpivx Ransomware-only – \$300
- Inpivx Panel-only – \$200



Step 3 of a 4-step process, the Inpivx ransomware interface makes attacks easier for novices.

The TRU team noted that the Ranion ransomware service continues to be advertised on the underground, even though it was first spotted in 2017. The Ranion threat actors are peddling their 1.10 version of the service, which they list as publishing in January 2019. The current prices for the service are:

|   |                           |       |                |
|---|---------------------------|-------|----------------|
| The TRU team spotted the Ranion ransomware service being advertised for the following prices: | 1 month                   | _____ | <b>\$120</b>   |
|   | 6 months                  | _____ | <b>\$490</b>   |
|   | 12 months                 | _____ | <b>\$900</b>   |
|   | 12 months (Elite Service) | _____ | <b>\$1,900</b> |

**PACKAGES COMPARISON**

| DESCRIPTION  | PACKAGE #3     | PACKAGE #2     | PACKAGE #1     | PACKAGE #ELITE  |
|--|----------------|----------------|----------------|-----------------|
| Subscriptions  | 1 Month        | 6 Months       | 12 Months      | 12 Months       |
| Darknet C&C Dashboard  | Yes            | Yes            | Yes            | Yes             |
| Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer | Yes            | Yes            | Yes            | Yes             |
| Offline Encryption   | No             | Yes            | Yes            | Yes             |
| Support  | No             | Yes            | Yes            | Yes             |
| Real-Time Client Manager   | No             | Yes            | Yes            | Yes             |
| Dropper  | No             | Buy            | Yes            | Yes             |
| Clone  | No             | Buy            | Buy            | Yes             |
| FUD+Obfuscator   | Buy            | Buy            | Buy            | Yes             |
| Unkillable Process   | No             | Buy            | Buy            | Yes             |
| FUD Stub #   | 1              | 1              | 2              | 12              |
| <b>Price</b>   | <b>120 USD</b> | <b>490 USD</b> | <b>900 USD</b> | <b>1900 USD</b> |

**PACKAGE #1 - 12 MONTHS C&C DASHBOARD (RaaS) PRICE: 900 USD**

- C# FUD Ransomware (AES 256 Encryption with a 64 chars long uncrackable key)
- C# Decrypter
- Stub Size: 250kb (unique exe for each buyer)
- Stub #: 2 FUD exes (the second one after 6 months)
- Platform: Windows (both x86 and x64)
- Duration: 12 Months access to Darknet C&C Dashboard (to receive the AES keys from Clients)
- Fees: We take NO FEES from your Clients
- Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer
- IP Tracking: Yes
- Offline Encryption: Yes
- Support: Yes
- Real-Time Client Manager: Yes
- Paid Add-On (Dropper): Execute your own exe (backdoor, implant, etc.) (FREE)
- Paid Add-On (Clone): A fresh FUD RANION copy with the same setup information (+90 USD)
- Paid Add-On (Crypter): Additional Crypter/Obfuscator + unique onion address (+90 USD)
- Paid Add-On (Unkillable Process): Unkillable Process aka BSOD (+90 USD)
- Free Add-On: optional file types to encrypt (for all encrypted file types see FAQ)
- Free Add-On: optional Client's sub-banner in your language (already present en, ru, de, fr, es, it, nl, fas, za)

**HOW TO BUY**

Carefully read our FAQ and after use following procedure:

1. Send the Package's price to the following Bitcoin address:
  - Your price to receive from your Clients (ie. 0.20 btc)
  - Your email address to get contacted from your Clients (enabled by default)
  - If you want to keep track of IPs of your Clients (enabled by default)
2. Write us an email to [redacted]@[redacted].net using:
  - Chosen package
  - Your Bitcoin address used to send us money
  - Your own Bitcoin address to receive money from your Clients
3. We'll until we check your payment
4. You will receive an email with 2 links:
  - The first one with your files (Ransomware + Deployment)
  - The second one with your C&C Dashboard

Any setup information must be sent with payment email. No further customization can be put in place if your own RANION copy is in production.

Your satisfaction is important! Contact us for any need.  
Copyright (c) 2018-2019 - RANION (RaaS)

Ranion ransomware-as-a-service package offerings.

One of the ways ransomware infects computers besides using exploit kits and phishing emails is by exploiting open remote desktop protocol (RDP) servers. The TRU team found cybercriminals offering to sell credentials to open RDP servers for a mere €18 to €22 a piece (\$20.29 to \$24.80). On top of that, buyers are given the opportunity to purchase credentials to RDP servers in different parts of the world, including Paris, London, Tokyo, and Sydney.

|   |   |  |
|---|---|--|
|   | <p><b>London, UK-Non hacked RDP Service or VPS, RDP server</b><br/>                     Item #38605-Services/Carding - ██████████ (7)<br/> <b>Views: 24 / Sales: 0</b><br/> <b>Quantity Left: Unlimited</b></p>                             | <p><b>BUY PRICE:</b><br/> <b>EUR €22.49</b><br/>                     (0.003276 BTC)<br/> </p> |
|  | <p><b>Paris, FR-Non hacked RDP Service or VPS, RDP server</b><br/>                     Item #38606-Services/Carding - ██████████ (7)<br/> <b>Views: 5 / Sales: 0</b><br/> <b>Quantity Left: Unlimited</b></p>                               | <p><b>BUY PRICE:</b><br/> <b>EUR €22.49</b><br/>                     (0.003276 BTC)<br/> </p> |
|  | <p><b>[MS] RDPS/MULTIPLE COUNTRIES(BEST PRICE&amp;QUALITY)</b><br/>                     Item #32703-Software/Other - ██████████ (114)<br/> <b>Views: 28 / Sales: 0</b><br/> <b>Quantity Left: Unlimited (Unlimited Automatic Items)</b></p> | <p><b>BUY PRICE:</b><br/> <b>EUR €18.00</b><br/>                     (0.002625 BTC)<br/> </p> |

Credentials for Remote Desktop Protocol Servers for sale.

## STOLEN CREDIT CARDS, SKIMMERS, OH MY!

One of the most prevalent pieces of stolen information in black markets and forums is credit card data. Credit card information is often stolen in attacks on businesses accepting the credit card, not on the credit card issuer. Earlier this year, Earl Enterprises confirmed a breach impacting some of its restaurants—including Planet Hollywood, Chicken Guy!, and Buca di Beppo—which stretched on from May 23, 2018, to March 18, 2019, with different locations impacted at different times. In a public statement, the company admitted that cybercriminals had successfully swiped payment card data at numerous restaurants throughout the U.S. by installing malware on their point-of-sale systems. According to media [reports](#), more than 2 million credit card numbers were affected.

In many ways, it must seem like easy money. Stolen credit cards are easy to monetize, which makes them valuable commodities in the world of cybercrime. Just how valuable, however, depends on a number of factors. For example, prices for credit cards continue to vary depending on the country of origin. A Visa or Mastercard issued by a U.S. bank can cost between \$5 and \$12, while American Express cards were offered for \$5 to \$15. However, a U.K.-based Visa or Mastercard runs \$15 to \$20, while a U.K.-based American Express card runs between \$10 to \$25.



Point-of-Sale credit card skimmer for sale online.

Sellers that also include a BIN (bank identification number) with a U.S. card can expect to fetch an additional \$15. The date of birth of the cardholder will cost a buyer an additional \$13 to \$40, depending on the country in which the card was issued. The same is true as those cards being sold with a VBV (Verified by Visa) code.

In comparing the current market prices for stolen credit cards, bank accounts, and personal identities to the prices advertised in June 2018, the TRU team found similar rates. At that time, the average price for a U.S. Visa or Mastercard was \$9 and the current price averages out at \$8.50. However, the TRU team is seeing a drop in price for U.K. Visa and Mastercard credit cards. In June 2018, they were averaging \$22 a piece, whereas today they are averaging \$17 a piece. The TRU team wonders if this price drop is due to an influx of credit cards hitting the black markets, after a spate of card-skimming **attacks hit hundreds of e-commerce websites**, including organizations doing business in the U.K., such as British Airways, Marriott, Ticketmaster, and others.

Credit card data is often purchased by criminals looking to commit “card-not-present fraud.” This occurs when scammers do not physically present

a card but rather purchase items online. More sophisticated criminals may opt to physically clone credit cards. This requires obtaining track 1 and 2 data.

This information is encoded on the magnetic stripe on the back of the card and includes information associated with the account holder, as well as service codes and other data. This data is often stolen by placing skimming devices at gas pumps or other point-of-sale terminals.

In Armor’s previous report on the black market, track 1 and 2 data dumps sold for varying amounts, with some selling for \$25-\$45 per U.S. card and \$50-\$60 for cards from the EU or U.K. This year, data dumps for U.S. cards with track 1 and 2 data are running between \$85-\$110 per card, while track 1 and 2 data dumps for credit cards originating in the U.K. cost between \$100-\$120 per card.

## CLONED ATM CARDS, CLONED CREDIT CARDS, & SKIMMERS APLENTY

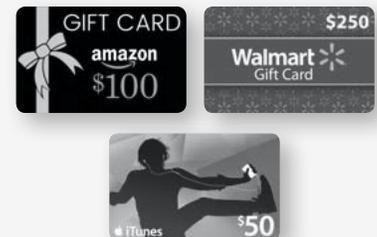
---

Credit card skimmers used to steal this information were on sale as well. Prices varied, with the most expensive fetching prices as high as \$1,500, while others were being offered for \$700. These skimmers can swipe debit and ATM cards, which can also be cloned. These cloned cards are worth their metaphorical weight in gold. Armor observed cloned cards with a \$3,000 limit selling for \$250. Cards with a \$15,000 limit were being offered for \$1,000.



Realistic-looking skimmer overlays for ATMs are sold online.

There is another type of card that is valuable in the cyber underground: gift cards. Cards loaded with money are being offered on the cheap. An iTunes gift card with \$1,000 on it was for sale for \$100; an Amazon card with \$4,000 on it was offered for \$500; and a Walmart gift card with a \$5,000 balance was on sale for just \$650. Gift cards come cheap on the underground.



Besides their value for shoppers, gift cards are also being used by cybercriminals as part of their schemes. In October 2018, the Internet Crime Complaint Center (IC3) reported an increase in the number of complaints related to Business Email Compromise (BEC) schemes whereby employees were conned into purchasing a **gift card**. In a typical scenario, a target receives a fake request, purportedly from their management, to buy a gift card for work-related reasons or as a present for a special occasion having to do with an employee. Once purchased, the gift cards are then used by the scammers to facilitate the purchase of goods and services. Sometimes these incidents are also combined with additional requests for wire transfer payments used in traditional BEC scams.

## MONEY SCHEMES & MONEY MULES

Nothing is more attractive to thieves than direct access to cash, and buying online bank account credentials gives criminals just that. Compromised online bank accounts from the U.S. were still the least expensive. This is most likely due to supply and demand. Many of these accounts are personal accounts at major banking institutions, such as Wells Fargo and Bank of America. Online account credentials (usernames and passwords) for accounts with balances of \$3,000 were offered for \$150-\$300; accounts with deposits of \$20,000 were offered for between \$1,000-\$1,200.

Banking customers in the U.K. were not spared. Compromised account credentials from customers at Lloyd's Bank, for example, were priced in one case at \$300 for an account containing £3,000 (\$3,386.77), and \$1,500 for an account with £20,000 (\$22,578.46). Online financial services such as PayPal are not safe either. One seller offered access to a PayPal account with a balance of \$500 for \$50. Another offered an account with an \$8,000 balance for \$600.



## CASH GRAB—MONEY LAUNDERING

If a fraudster doesn't have the skills or the nerve to purchase stolen bank account credentials and transfer the account's funds into an account under his or her control or into a prearranged money mule account, that is no longer a problem. There are plenty of hackers willing to simply transfer stolen funds to the bank account or PayPal account of your choice or send you the funds via Western Union.

The TRU Team began to notice this service in the past year, and it has quickly become one of the key offerings on the underground. These seamless transactions cost around 10 cents to 12 cents on the dollar, and the buyer doesn't have to steal the victim's money themselves. They simply pay the hackers to do it for them.



One cybercriminal advertised their money-laundering services using Western Union, a bank account, or a PayPal account:

"Are You looking for easy way to make money and you want to be a billionaire ? then simply stay connected with US. With Our stuff the first deal we give low rates to build trust with each other . We have big experience in Western Union Transfer, Bank Transfer, PayPal transfers . My rates are fixed so no negotiation in terms of prices. Please Never ask me for test transfers or etc. We don't sell CC , Dumps or fullz etc so don't add US to your contact list if you need those data..... First of all i want to be clear on one thing i don't work for percentage % , so please don't waste Our time and yours and don't ask % partnership , because we are happy with Our work and We don't want to lost my time in this kind of proposals!!!! CONTACT ID !!!! Gmail xxl; icq: xxxx;.

**Rules For Western Union Transfer: Info Needed:-** 1: First Name 2: Last Name 3: City 4: Country 5: Email for confirmation? Western Union Transferring Worldwide. You will get MTCN code + Sender info + amount and then you can pickup from any WU store office. Note: Only 1-time transfer on 1 name in a week, if you need daily transfers then you must use more names. Western Union Transfer Rates: For \$1000 Transfer = \$100 For \$2000 Transfer = \$250 For \$3000 Transfer = \$350 For \$4000 Transfer = \$500 For \$5000 Transfer = \$600 For \$7000 Transfer = \$700 For \$10000 Transfer = \$1000 <== MTCN split code into 2 parts - \$5000+\$5000 "

**Rules for Bank Transfer:** For bank transfer you will provide me your bank info and i will transfer funds into your account within time limit as we promised. I will only do one transfer in a week on one bank account. If you need more transfers then arrange more bank accounts. I'm Specially Trained in Transferring From These Countries: (US,UK,IN,GM,NL,AU,CA,DM,CH,BN,IT,MX,RU)? Bank Transfer Rates: For \$1500 transfer = \$200 For \$2000 Transfer = \$250 For \$3500 Transfer = \$450 For \$5000 Transfer = \$600 For \$7000 Transfer = \$700. Info needed for Bank transfers :- 1: Bank name 2: Bank address 3: Zip code 4: Account Holder 5: Account number 6: Account Type 7: Routing number Bank transfer will take maximum 8 hour for money to Reflect in your bank account.

**Rules for PayPal Transfer:** - Using hacked and verified PayPal accounts to transfer PayPal money into your PayPal account. I'm doing PayPal transfer to myself safety first and I want to Share my skills with buyers and customers On here too-- so that all of us here can make each other Rich here, So you don't have any headache to clean the money because its already clean when i transfer it into my account."



**VERY FAST Western Union Transfers**

Item #50317-Services/Other - (2)

Views: 62 / Sales: 0  
Quantity Left: Unlimited

**BUY PRICE:**  
**EUR €629.91**

(0.091892 BTC)  
B



**PAYPAL TRANSFER SERVICE** \* \$500 Deposit \* CHEAPEST! \*

Item #50990-Services/Other - (35)

Views: 226 / Sales: 5  
Quantity Left: Unlimited

**BUY PRICE:**  
**EUR €134.98**

(0.019691 BTC)  
B

Western Union and PayPal transfers make for quick money-laundering schemes.

## MONEY MULES

Stealing online banking information is often the work of banking trojans such as **Gozi**, **Zeus**, and **Trickbot**. These pieces of malware are often distributed in malicious email campaigns and via drive-by download attacks. Cybercriminals also use phishing schemes to trick users into giving up their online banking credentials. Getting cash out of these accounts, more often than not, involves the use of money mules.

Money mules are persons who have a bank account or multiple bank accounts and who knowingly, or unknowingly, permit cybercriminals to transfer stolen funds into their bank account so it can later be withdrawn. The cybercriminal pays the mule a portion of the siphoned-off funds.

A well-established money mule, with a solid reputation and one who has multiple accounts in various top financial institutions, will command approximately 10% of the take. However, the payout can run up to 20% depending on the risk and the amount being stolen. Also, the hacker has to trust that the mule is going to remit the remainder of the stolen monies to them after the mule has taken their cut. It is for this reason that the threat actor will seek out a mule or a mule network operator with a solid reputation. They may pay a higher percentage, but it is critical to work with a mule that has established bank accounts and can be trusted to remit the funds.



## CORPORATE DOCUMENTS, PERSONAL IDENTITIES, FULLZ, & MEDICAL RECORDS

And just how do the money mules keep their bank accounts from being shut down, especially those being used to move large amounts of cash? One way is to establish a shell corporation. There is no shortage of scammers on the underground offering to sell sole proprietorship papers complete with an Employer Identification Number (EIN), also known as Tax Identification Number (TIN). An EIN is a unique, nine-digit number assigned by the IRS to business entities operating in the U.S. for the purposes of opening a bank account or filing tax returns.

One scammer offered to sell sole proprietorship papers and an EIN for €1,429 (\$1,611.27). Another criminal included an EIN number and articles of incorporation for €719.29 (\$811.04). With these documents in hand, money mules can open business bank accounts, enabling them to move larger amounts of money in and out of the account without drawing unwanted attention to their activities.



**GIVE YOU EIN AND ARTICLES OF INCORPORATION**  
Item #28682-Services/Other - (1)

**Views: 52 / Sales: 0**  
**Quantity Left: Unlimited**

**BUY PRICE:**  
**EUR €719.29**  
(0.000000 BTC)

Darknet vendor advertising EIN and articles of incorporation for sale.

## FULLZ

Compromised bank accounts, credit cards, and gift cards are not the only items cybercriminals are turning into money. Personally identifiable information (PII) and counterfeit documents remain valuable commodities as well. For the right price, a buyer can purchase fullz, the motherload of personal information on an individual. The packet of PII typically includes a person's full name, date of birth, social security number, phone number, address, mother's maiden name, driver's license number, etc. The TRU team also observed several cybercriminals who offered to sell additional data relating to a victim, if the buyer was willing to pay a bit more money. This information included such items as an individual's

credit card data, bank account data, bank security questions and answers, victim's employer, etc. This information can be used for identity theft and, if the victim has good credit, all manner of scams can be facilitated, such as securing hefty bank loans, high-limit credit cards, car loans, and other lines of credit.

The cost of the fullz depends on the identity victim's country of origin. For fullz from the U.S., the TRU Team saw that prices ran from \$30-\$40. For information on a victim from the U.K., the cost ranges from \$35-\$50. For fullz from European countries such as France, Italy, and Spain, the price falls between \$20 and \$25. For other EU countries, the price can fluctuate from \$17 to \$60.

The TRU Team observed one cybercriminal explaining how his fullz were so much more valuable than having a victim's online banking credentials:

"The bank usernames and passwords are not as important as the fullz and here is why. With a bank username and password by itself you can't do very much, but with fullz records you can CREATE NEW bank usernames and passwords that will match whatever IP/Browser Agent you are using. So think of the fullz as the master key to fraud. My fullz for example come in this format.

- Name/Address
- DOB
- SSN
- Tel#
- Driver's License#
- Workplace
- Bank Name
- Bank Location
- Bank Routing#
- Bank Account #
- Average Monthly Balance
- Account Opening Date

With all this info you can do each transfers of 10k or more, open brand new 15,000 USD and up credit cards, open up fresh bank accounts for quick internal transfers, and way more. Put your fullz to use. Tutorial How to get approved for a bank loans step by step and how to cash it out safely + Bank account takeover guide (VALUE 300\$) FREE."

Another cybercriminal advertising fullz recommended:

**"Hey if you need a victim's mother's maiden name, just go to Ancestry.com!"**

With the nominal cost of stolen identities, and therefore the barrier to identity theft remaining so low, protecting private information must remain a key priority for individuals and businesses alike.

## MEDICAL RECORDS

If you are looking for medical records on the underground, these can also be found. Although the number of digital storefronts selling them appear to be far fewer than those selling other illicit cyber goods and services. However, one has to wonder why this is, considering that in 2019 in the U.S. alone, 266 medical organizations have been hacked and 23,548,446 medical records have been stolen, according to the [Privacy Rights Clearinghouse](#).

Most medical records contain everything one needs for identity theft: full name, address, birthdate, phone number, email address, social security number, credit card number or checking account number, and emergency contact (which is often a family member). Thus, the TRU team wondered if one

reason they don't see stores of medical records being advertised on the underground markets is that the cybercriminals are culling out the PII data from the stolen medical records and selling this valuable information off separately. This data can be quickly monetized, as it contains everything for identity theft.

In studying several of the underground forum posts, it is quite evident that the cybercriminals stealing medical records are very aware of their value, especially as it relates to the fullz data contained in them. See two posts where the hackers brag about their success in hijacking thousands of medical records containing fullz.

**Cybercriminal 1**-- " My recent feat a health clinic portal that contains over 30,000+ medical records of people. I want to be here primary to help others and hopefully others can help me, I'm always interested in learning and taking note. and I'm also wiling to stand back and let someone else get some shine. The primary thing I'm bringing here is what i just stated above. I recently hacked in a USA health records database that contains 11 health clinics across 1 state. It took time and effort but it worked. I still don't have an exact number because the number is still rising!!!. I am going to offer my fullz to anyone since I'm new and i want more people to trust me. I am willing to give out the 1st 200 names free!!

**Cybercriminal 2**--"So I have access to over 500 SSN all of them have DOB, full name, address, copy of signature and medical records. I have no idea what to do, I have read several tutorials but don't know where to start or what i can accomplish with them. All i know is with SSN I can check credit. Any interest in the SSN or where I can start would be great. >> >>

**Respondent 1**---" price?"

**Respondent 2**---" i wanna use it too please."

## PROTECT YOUR DATA AND ENVIRONMENT

---

With the cyber black markets continuing to bustle, keeping data and systems safe requires effective security services and technology, but also sound security practices. The TRU research team recommends the following cybersecurity protections for organizations and individuals:

### FOR IT AND CYBERSECURITY TEAMS

- Train your employees on how to identify suspicious activity, phishing emails, etc.
- 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.
- Use security technologies such as firewalls, anti-malware software, and intrusion detection and prevention systems to build a shield around your environment.
- Implement multi-factor authentication when providing access to your most critical systems. This provides an extra layer of security to prevent unauthorized access.
- Use OFFLINE Backup Storage – Users must have backups of their data, which is air gapped from the internet. Ensure all critical data, applications, and application platforms are backed up and password-protected.

## 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 Wi-Fi hotspots. Many of them 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 and financial account monitoring services to detect suspicious activity.



## CONCLUSION

---

The digital shelves of the dark web are filled with everything from credit card details to online bank accounts. The economy of cybercrime is not in a downturn—far from it. The malware, cybercrime services, and other tools that threat actors need to perpetrate fraud are plentiful and profitable for sellers and buyers alike. As the underground markets bustle, security professionals, business leaders, and members of the public must stay vigilant in protecting their systems and data.

## ABOUT ARMOR

---

Armor is a cloud security company that takes the complexity out of protecting your data, whether it resides in a private, public, or hybrid cloud—or in an on-premise IT environment. We provide managed security solutions that give you a clear picture of threats facing your organization. This allows us to provide you with the people and security resources to stop attacks before they happen and react quickly and effectively when they do, keeping your data safe and compliant. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.



[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

19030909 Copyright © 2019. Armor, Inc., All rights reserved.