

CYBERCRIME, INC: THE BUSINESS OF THE DARK WEB

MICHAEL MAYES

Senior Writer & Researcher

THE ARMOR 2019 BLACK MARKET REPORT | A LOOK INSIDE THE DARK WEB

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's 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 go on to

become a pseudo-anonymous way of making digital purchases, with a form of money that was encrypted, faster than wire transfers, and not tied to any government monetary system or central bank. From 2011-2013, dark markets created a niche market for Bitcoin on a website called the Silk Road. The 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 there is no way to tie a specific transaction to a specific person. Thus, when it comes to "laundering the money," Bitcoin transactions make law enforcement's job very difficult. Once collected, Bitcoin can be sold to a developer or "burned" through a variety of mechanisms to further obscure the money trail.

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.



Illustration credit: © J. D. Smith for ARMOR

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 44% 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, XMR, SploitCoin (ransomware), Bitcoin Cash (Thantatos ransomware), Etherium (HCT (ransomware), and Dash (Mafate 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.

ARMOR.COM | 800-7-ARMOR (727-662-7768) | 1-800-744-ARMOR (2767)

\$0,000 email
\$35,561

SEC: 5.19
ATC:

SEC: 5.50
ATC:

imple, one
\$1 offer to
\$1)

SEC: 54.98
ATC:

ARMOR

ABOUT THE SPEAKER

MICHAEL MAYES

- Serves as a senior writer and researcher
- His career in technology communications includes work with the Human Genome Project, handheld software during the Palm and Pocket PC era, blockchain development, and cybersecurity
- Began research in black markets in 2013 during a PhD year in professional and technical writing at the University of Memphis – where he wrote on the early days of Bitcoin and its defining proof of concept, the Silk Road.



AGENDA

1

The Business of the Dark Web

2

Cybercrime-as-a-Service

3

Constant Vigilance

4

Q & A



THE BUSINESS OF THE DARK WEB



BENEATH THE SURFACE

An iceberg diagram illustrating the layers of the web. The tip of the iceberg is labeled 'SURFACE WEB'. The submerged part is divided into two sections: the upper submerged part is labeled 'DEEP WEB' and 'INVISIBLE TO STANDARD SEARCH ENGINES', and the lower submerged part is labeled 'DARK WEB' and 'SPECIAL ACCESS REQUIRED'.

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

INVISIBLE TO STANDARD SEARCH ENGINES

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. Most of this content is innocuous.

DARK WEB

SPECIAL ACCESS REQUIRED

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

OUR MESSAGE IS CLEAR FOR BUSINESS LEADERS

- 1 Cybercrime tools are highly developed, easy to acquire, and easy to use – even for the novice criminal.
- 2 The market to sell and buy illegally obtained data is well established, and all data has value in the underground black market. It's all for sale.
- 3 No matter your company size, location or industry, your organization is open for business to threat actors on a worldwide scale.

WHY THE BLACK MARKET MATTERS



Black markets impact clients and organizations of all types and sizes, they show the depth and breadth of data breach monetization and the lengths criminals will go to steal money.



Cybercrime-as-a-Service is rampant and evolving, making it easier for non-technical threat actors to get in the game.



There is a direct correlation between the sale of malware and hacker services online, and the need for security of networks and data—threat actors are hard at work, you should be, too.



Municipalities, Healthcare, Education & Financial Services are top targets.



Most SMBs don't have the budgets or staff to conduct 24/7/365 surveillance of networks and communications, but the need to do so is growing.

CRYPTOCURRENCY'S ROLE

- Bitcoin is a pseudo-anonymous digital currency that is not tied to any nation state or federal banking system; it is peer-to-peer, open source software
- Bitcoin's first proof of concept was the dark market Silk Road from 2011-2013
- In 10 years, Bitcoin code has not been broken or hacked, coins only stolen from 3rd party exchanges and wallet hacks
- Other cryptocurrencies such as Monero, Dash and ZCash have greater anonymity features.
- \$76 billion annually – or 46% of Bitcoin transactions – is involved in cybercrime
- Bitcoin's value, network strength and ability to obscure payments will continue to dominate (market cap of \$175 billion)



Bitcoin



Ethereum



Dash



Monero



ZCash



CRYPTOCURRENCY'S ROLE

- Cybercrime marketplaces offer straight money deposits to bank accounts, PayPal, or delivered to Western Union
- Prices are typically 10 cents on the dollar: get \$10,000 for \$800 in Bitcoin
- Money Mules are often deployed to pick up and launder cash; criminals offering 10-20% of the take in exchange for their services
- Use of shell corporations – there is no shortage of scammers on the underground offering to sell sole proprietorship papers complete with an Employer Identification Number



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)



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)



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)



CYBERCRIME- AS-A-SERVICE



CYBERCRIME-AS-A-SERVICE

Cybercriminal groups offer a variety of hacker tools and services, making it easy for fraudsters who lack the technical skills to get into the game.



Affiliate programs and subscription models.



Customer service including live chat, video tutorials and customer service.



Ready-to-exploit servers, accessed through Remote Desktop Protocol vulnerabilities, are packaged and sold.



Plug-n-play ransomware campaigns need little more than a secure email address.

CYBERCRIME-AS-A-SERVICE

- **Distributed Denial of Services (DDoS)**
\$60/hour, \$280/day, \$479-659/week or \$2000/month
- **Spamming**
\$32 for 20,000 messages or \$54 for 50,000 messages
- **Exploit Kits**
Ranges from \$80-\$1000 pending on the extensiveness of the exploit and malware
- **Remote Administrative Tools (RATs)**
Highly sophisticated offered for \$500, while others offered as low as \$10
- **Customizable**
Ranging from hacking bank accounts, applications, popular accounts like Skype, Yahoo!, Gmail; spying on competitors; criminal record removal, credit score upgrade, passports, and much more.



EMAIL BOMBER 50,000 PIECES

Item #36775 - Services / Other - (9)

Views: 21 / Sales: 0
Quantity Left: Unlimited

BUY PRICE:
EUR €53.99

(0.007876 BTC)



EMAIL BOMBER 20,000 PIECES

Item #36776 - Services / Other - (9)

Views: 9 / Sales: 0
Quantity Left: Unlimited

BUY PRICE:
EUR €31.50

(0.004595 BTC)



Set Up Remote Administration Tool Zeus BotNET (RAT) INSTANT DELIVERY
Item #19974-Software & Malware/Botnets & Malware - (3654)

Views: 258 / Sales: 5
Quantity Left: Unlimited (Unlimited Automatic Items)

BUY PRICE:
EUR €2.28

(0.000316 BTC)



DIAMONDFOX BOTNET ! ULTIMATE SNIFFER, STEALER, RAT
Item #28629-Software & Malware/Botnets & Malware - (56)

Views: 154 / Sales: 5
Quantity Left: Unlimited (Unlimited Automatic Items)

BUY PRICE:
EUR €6.17

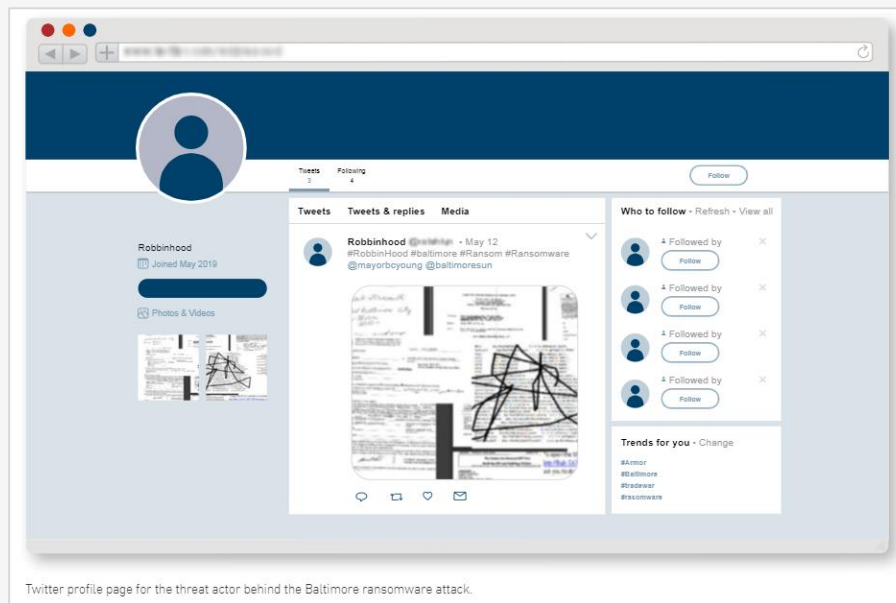
(0.000316 BTC)



CYBERCRIME-AS-A-SERVICE

Ransomware-as-a-Service

- Ransomware variants and services available from online vendors cheap!
- Includes customizable source code, customer service chat functions, video tutorials
- Business models vary, some provide only tools while others provide full service and take %



CONSTANT VIGILANCE



TIPS FOR YOUR SECURITY/IT TEAMS

1

Train your employees on how to identify suspicious activity, phishing emails, etc.

3

Deploy patches as promptly as possible to shorten the vulnerability window.

5

Monitor cloud usage, manage access to cloud services, and secure any data or applications you migrate.

7

Implement multi-factor authentication when providing access to your most critical systems. This provides an extra layer of security to prevent unauthorized access.

2

Find, classify, and protect your most sensitive data, particularly information impacted by compliance regulations such as PCI-DSS and HIPAA.

4

Employ data encryption to protect sensitive data in transit and at rest.

6

Use security technologies such as firewalls, anti-malware software, and intrusion detection and prevention systems to build a shield around your environment.

8

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.

ARMOR'S SECURITY OPERATIONS CENTER



Data-focused, cloud agnostic protection



24/7/365 detections and response against all threats to your environment



+6000 security incidents managed yearly

A FEW WAYS WE HELP:

1. CONTINUOUS THREAT HUNTING

Proactive, not reactive. We perform continuous threat hunting to ferret out potential threats that might have gotten past our strong preventative and detective controls and/or new threats discovered in the Dark Web that may affect customers.

2. NEAR REAL-TIME DETECTION & RESPONSE

We go above and beyond what traditional managed security providers do. We detect and respond to threats, resulting in an average dwell time of less than 1 day compared to an industry average of 100+ days.

3. SELF-LEARNING

Insights and intelligence gleaned from monitoring customer environments are continually adapted into countermeasures, further automation, orchestration and playbooks, enhancing the effectiveness of our SOC.

KEY TAKEAWAYS AND FINDINGS

- **Cybercriminals are continuing to make money from every little piece of data a consumer or business has, and massive data breaches have given them millions of victims to exploit.**
- **The hackers are making it easier for novices to commit cybercrimes.**
 - **Laundering of Banking and Credit Card Credentials**
Instead of just selling threat actors a person's online credentials (where the buyer would need the technical skills to transfer the money out of the victim's bank account into their account), hackers are simply doing it for the buyers.
 - **Hacking, harassing and data kidnapping-as-a-service**
Threat actors offer crime-as-a-service models where a scammer can buy a subscription and become an affiliate member. It is a plug and play system for the buyers making it easier for non-technical fraudsters to commit cybercrime.
 - **Selling Fraudsters a Network of Infected Computers (Bots)**
Fraudsters only have to tell the owner of the Botnet what type of malicious software they want downloaded onto the hijacked computers or bots.
 - **Selling Step by Step Print Tutorials and Videos on How to Commit All Kinds of Fraud**
Examples include "how to use someone's identity to apply for a big bank loan."

KEY TAKEAWAYS AND FINDINGS

- **As cyber defenders figure out how to protect against threat actors, threat actors produce new ways to get around those protections every day.**
- **Your own people continue to be one of the biggest vulnerabilities to any organization.**
 - Using the same passwords for lots of different systems
 - Clicking on links and attachments in emails
 - Being tricked into providing credentials to key systems or accounts
 - Not patching or running computer system updates
- **Invest in proactive security measures and 24/7 monitoring**

RESOURCES

The 2019 Black Market Report

armor.com/reports

SEPTEMBER 2019



THE ARMOR 2019 BLACK MARKET REPORT

A LOOK INSIDE THE DARK WEB

Armor Threat Intelligence Reports

armor.com/threat-intelligence

THREAT INTELLIGENCE ARTICLES

- NEW THREAT INTELLIGENCE ARTICLES**
Ransomware Attack Against Reading, Writing, and Payroll: New Attacks Greet Students
Update Tuesday September 3, 2019. To reflect new victims identified by Armor as of today, Armor's Threat Resistance Unit (TRU) security team has identified four new ransomware victims since Friday August 30 bringing the total to 17 new ransomware victims in the past 11 days. Ten of them are school systems. Education efforts across the U.S. ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
City of Borger, TX and Keene, TX Among 22 Local Texas Government Organizations Hit by Ransomware
Updated as of 10:30 am EST August 22, 2019. Armor Operations Seven New Victims in Spokewide Ransomware Attack After identifying the cities of Ames and Borger, Texas as victims of the multi-organism attack which hit Texas on August 14th, cloud security specialist provider Armor has identified seven new victim organizations. They include: Wilson, TX; Lubbock, TX. ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Ransomware Attack Against Baltimore: Tweet from Hacker or Malicious Frankster?
Last updated: 8/29/2019 Eric Sifford, Security Researcher with Armor's Threat Resistance Unit (TRU), found new tweets on Twitter, August 28, 2019. At 11:00 am on Tuesday, Aug 28, 2019 from a Twitter account, which appears to be connected to the IP of Baltimore ransomware attackers. Both tweets were directed openly at Baltimore's mayor, Brandon S. "Jack" L. ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Hackers Go After Payroll Departments and Payroll Services
It is no secret cybercriminals follow the money. But during the past several months, that edge has taken a very literal turn, as a series of cyberattacks targeting payroll departments and payroll services has transpired. Armor is leading global cloud security solutions provider, advised mention of one such cyberattacks in early April, whereby hackers targeted [...] ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Threat Alert - Armor Warns Online Retailers of Increased Attacks
Threat Alert - Armor has found what it believes to be the first Magento-style (e-commerce) cart stuffing attack tool to be openly offered for sale on the Dark Web. ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Armor Detects and Neutralizes 481 Million Cyberattacks Launched at its Cloud Customers in 2018
If you think that hackers aren't going after organizations (one being listed in the cloud), well then again, Armor, leading cloud security solutions provider which protects the international assets of 1,300 cloud clients globally, reported that during 2018 they detected and neutralized over 481 million cyber attacks being launched at its clients. Based on its report, ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Threat Intelligence Brief - Q1 2018
In April, we released the much-anticipated Black Market Report, based on three months worth of Dark Web research from Armor's Threat Resistance Unit. The report features some juicy information, like how much your periodic data is worth and how cheap operational-as-a-service is. ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)
- NEW THREAT INTELLIGENCE ARTICLES**
Threat Intelligence Brief - August 2017
TECH TALK With email phishing's constant popularity and effectiveness, it's important that we expand on our monthly reports with an overview of email header analysis. Analyzing email headers can help you determine if the email is spoofed, or manipulated so that the points of the email appear to be from a familiar source. Spoofed emails [...] ...
[VIEW THREAT INTELLIGENCE ARTICLES](#)

Armor's Security Operations Center


armor.com/extend-security-team

Meet Armor's Cybersecurity Experts

The Armor Security Operations Center (SOC) was formed with a keen understanding of the strategies and tactics threat actors employ against organizations around the world. We don't just stand as a SOC, we stand as a collection of counter-threat experts working in unison to keep even the most advanced threat actors and their ever-evolving cybercrime against our customers nearly impossible.

Our suitable approach to managed cloud security ensures that you're always supported by proven security talent capable of mitigating any sort of security incident. The certified security experts in our SOC have all been trained in the latest and most advanced cybercrime against our customers' critical data.

[MEET THE HEAD OF ARMOR'S THREAT RESISTANCE UNIT](#)




Security Operations Center in Action

Our Security Operations Center experts monitor, identify and protect your critical data, networks and applications, no matter where they're located. When you partner with Armor, our security experts extend your security program through 24x7x365 monitoring and protection.

Learn how they react to form a protection barrier against threat actors and their attempts to compromise your organization.

[VIEW THREAT](#)



TOTALLY SECURE IN ACTION

Why Use Armor

[CHECK OUT WHY CUSTOMERS TRUST ARMOR FOR THREAT DETECTION, INCIDENT RESPONSE, AND COMPLIANCE MANAGEMENT.](#)

[FIND GAPS IN YOUR SECURITY](#) [FIXING](#)

Q & A

MICHAEL MAYES

Senior Writer & Researcher



ARMOR

THANK YOU.

WWW.ARMOR.COM

