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
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.

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. Most of this content is innocuous.

DARK WEB
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.
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.
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).
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.

CRYPTOCURRENCY’S ROLE
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.
**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

<table>
<thead>
<tr>
<th></th>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Train your employees on how to identify suspicious activity, phishing emails, etc.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Find, classify, and protect your most sensitive data, particularly information impacted by compliance regulations such as PCI-DSS and HIPAA.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Deploy patches as promptly as possible to shorten the vulnerability window.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Employ data encryption to protect sensitive data in transit and at rest.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Monitor cloud usage, manage access to cloud services, and secure any data or applications you migrate.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Use security technologies such as firewalls, anti-malware software, and intrusion detection and prevention systems to build a shield around your environment.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Implement multi-factor authentication when providing access to your most critical systems. This provides an extra layer of security to prevent unauthorized access.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
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
Q & A

MICHAEL MAYES
Senior Writer & Researcher
THANK YOU.