THE DARK WEB AND HOW IT AFFECTS YOUR INDUSTRY

Jason H. Rivera
Manager – Cyber Threat Intelligence
Deloitte & Touche LLP
Twitter Handle: @Jason_JHR
How well do we understand the Dark Web?

We know that the Dark Web is filled with marketplaces that are often frequented by those with malicious intent – but how much do we know about these marketplaces’ impact on our industries?

More importantly, as security leaders within our various industries, how can we better understand the Dark Web and how can we prepare ourselves to deal with potential Dark Web threats?
The Dark Web is only one piece of the puzzle

We should seek to understand the Dark Web in the context of the larger strategic situation and understand its place alongside other intel collection sources.

**Strategic Considerations**

- **“What am I trying to Protect?”**
- **“What matters most?”**
- **“Who are my adversaries and how should I prepare for them?”**
- **“How determined are my adversaries and how likely are they to focus their efforts against us?”**
- **“How can my organization be held at risk both now and in the future?”**

**The Threat Intelligence Puzzle**

Threat intelligence is a puzzle that is comprised of many pieces.
A framework for understanding the challenge

Illicit products on the dark web

- Online Sale of PII
- Online Sale of credit card data
- Dark Web Malware Distribution
- Hacking for Hire Services
- Sale of hacked accounts
- Sale of Pirated Electronic Goods & Software

Every industry is affected

- Consumer & Industrial Products
- Energy & Resources
- Financial Services
- Life Sciences & Healthcare
- Public Sector
- Technology, Media, & Telecommunications

We must quantify both the tactical & strategic threats

The Tactical Threat

Day-to-day threats posed to an organization’s IT systems.

The Strategic Threat

Overarching, long-term threats posed to an organization’s operating model.
#RSAC

How the Dark Web affects the Consumer & Industrial Products Industry

**Overview**

Producers of consumer and commercial goods as well as hospitality & leisure services.

**Potential Threats**

| Commodity Malware | Insider Coordination | Counterfeit Products |

**Insider Coordination**

Counterfeit Products

**Key Considerations**

<table>
<thead>
<tr>
<th>Tactical Dark Web Cyber Threats</th>
<th>Strategic Dark Web Cyber Threats</th>
<th>Solutions that Leaders Should Consider</th>
</tr>
</thead>
</table>
| • The sale of counterfeit products  
• Increasing amounts of low-sophistication commodity style malware attacks  | • The large-scale theft and monetization of member rewards programs  
• The black market trading and weaponization of industrial components  | • Market deception and disruption techniques  
• Threat intel collection in Dark Web marketplaces |
How the Dark Web affects the Energy & Resources Industry

Overview
Companies specializing in the extraction and delivery of energy and other raw resources

Potential Threats
- Commodity Malware
- Black Market Trading
- ICS/SCADA Systems

Tactical Dark Web Cyber Threats
- Increasing amounts of low-sophistication commodity style malware attacks

Strategic Dark Web Cyber Threats
- Disruptive targeting against Industrial Control Systems (ICS)
- The use of anonymous marketplaces by insiders

Solutions that Leaders Should Consider
- Insider threat programs
- Threat intel collection in Dark Web markets

Key Considerations
How the Dark Web affects the Financial Services Industry

Overview
Financial service management and banking service providers

Potential Threats
- Money Laundering
- Brand Damage
- Financial Fraud

Key Considerations

<table>
<thead>
<tr>
<th>Tactical Dark Web Cyber Threats</th>
<th>Strategic Dark Web Cyber Threats</th>
<th>Solutions that Leaders Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Money laundering operations</td>
<td>• The continued growth of the black market for fraud products</td>
<td>• Threat intel collection in Dark Web marketplaces</td>
</tr>
<tr>
<td>• Potential for significant brand damage</td>
<td>• Dark Web insider trading forums</td>
<td>• Market deception and disruption techniques</td>
</tr>
</tbody>
</table>

Deloitte
How the Dark Web affects the Life Sciences & Healthcare Industry

Overview
Companies specializing in the production and distribution of pharmaceuticals, medical devices, and medical services

Potential Threats
- Commodity Malware
- Device Sabotage
- PII Theft

Key Considerations

<table>
<thead>
<tr>
<th>Tactical Dark Web Cyber Threats</th>
<th>Strategic Dark Web Cyber Threats</th>
<th>Solutions that Leaders Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The theft and monetization of PII/PHI</td>
<td>• The black market pharmaceuticals industry</td>
<td>• Threat intel collection in Dark Web markets</td>
</tr>
<tr>
<td>• Increasing amounts of low-sophistication commodity style malware attacks</td>
<td>• Disruptive targeting against medical devices</td>
<td>• Intelligence collection against TTPs that could be modified to impact medical devices</td>
</tr>
</tbody>
</table>
How the Dark Web affects the Public Sector

**Overview**

Government entities to include federal, state, and local governments

**Potential Threats**

- Weapons Trafficking
- Narcotics Trafficking
- Intelligence Collection

**Key Considerations**

<table>
<thead>
<tr>
<th>Tactical Dark Web Cyber Threats</th>
<th>Strategic Dark Web Cyber Threats</th>
<th>Solutions that Leaders Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Increasing amounts of low-sophistication commodity style malware attacks</td>
<td>• The proliferation of WMD and military grade weaponry</td>
<td>• Prioritizing and risk ranking black market threats</td>
</tr>
<tr>
<td>• Hacktivist efforts against US gov websites</td>
<td>• Intel collection against US interests</td>
<td>• Think through the Dark Web as an intelligence collection vehicle</td>
</tr>
<tr>
<td>• An uphill battle against a growing global narcotics industry</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Deloitte.

RSAConference2018
How the Dark Web affects the Technology, Media & Telecommunications Industry

Overview
Companies that specialize in the development of technology and communications products

Potential Threats
- IP Theft
- Pirated Products & Stolen Accounts
- Brand Damage

Key Considerations

<table>
<thead>
<tr>
<th>Tactical Dark Web Cyber Threats</th>
<th>Strategic Dark Web Cyber Threats</th>
<th>Solutions that Leaders Should Consider</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The sale of pirated technologies and software</td>
<td>• Breaches that lead to the large-scale theft of intellectual property (IP)</td>
<td>• Key word searches in the Dark Web for IP related issues</td>
</tr>
<tr>
<td>• Increasing amounts of low-sophistication commodity style malware attacks</td>
<td>• Strategic brand damage</td>
<td>• Threat intel collection in Dark Web markets</td>
</tr>
</tbody>
</table>
THANK YOU FOR YOUR TIME!

Jason Rivera
Manager – Cyber Threat Intelligence
Deloitte & Touche LLP
Email: jasrivera@deloitte.com