RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: TV-T05

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?"

"Who are my adversaries and how should I prepare for them?"

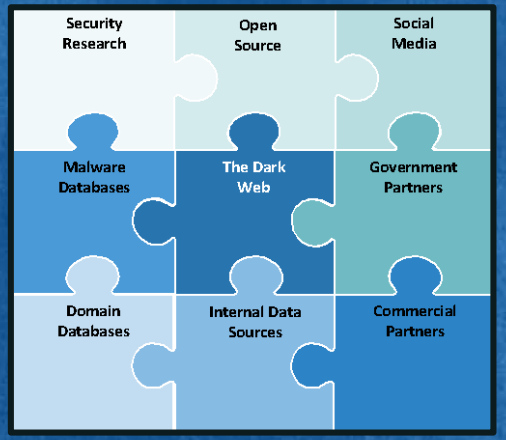
"What matters most?"

"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

#RSAC

Illicit products on the dark web

- Online Sale of PII
- Online sale of credit card data
- Dark Web Malware Distribution
- Hacking for Hire Services
- Online Weapons Trafficking
- Online Counterfeit Goods
- 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	*The Strategic Threat*
Day-to-day threats posed to an organization's IT systems.	Overarching, long-term threats posed to an organization's operating model.

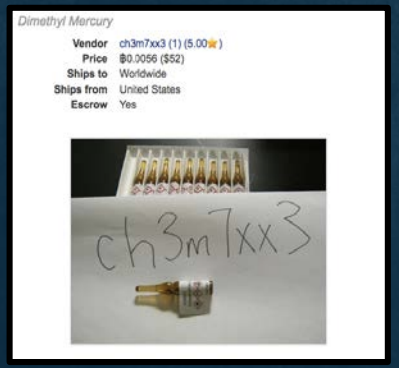
How the Dark Web affects the Consumer & Industrial Products Industry

Overview

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

Potential Threats

- **Commodity Malware**
- **Insider Coordination**
- **Counterfeit Products**



Key Considerations

Tactical Dark Web Cyber Threats	Strategic Dark Web Cyber Threats	Solutions that Leaders Should Consider
• 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

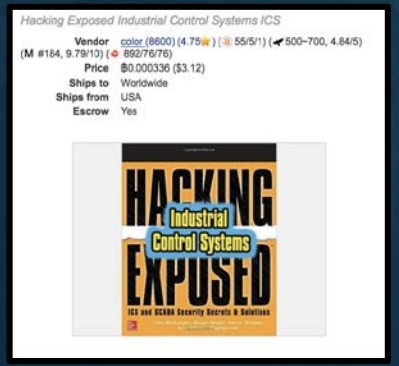
#RSAC

Overview

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

Potential Threats

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



Key Considerations

Tactical Dark Web Cyber Threats	Strategic Dark Web Cyber Threats	Solutions that Leaders Should Consider
• Increasing amounts of low-sophistication commodity style malware attacks	• Disruptive targeting against Industrial Control Systems (ICS) • The use of anonymous marketplaces by insiders	• Insider threat programs • Threat intel collection in Dark Web markets

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

Tactical Dark Web Cyber Threats	Strategic Dark Web Cyber Threats	Solutions that Leaders Should Consider
• Money laundering operations • Potential for significant brand damage	• The continued growth of the black market for fraud products • Dark Web insider trading forums	• Threat intel collection in Dark Web marketplaces • Market deception and disruption techniques • Counter-intelligence activities

How the Dark Web affects the Life Sciences & Healthcare Industry

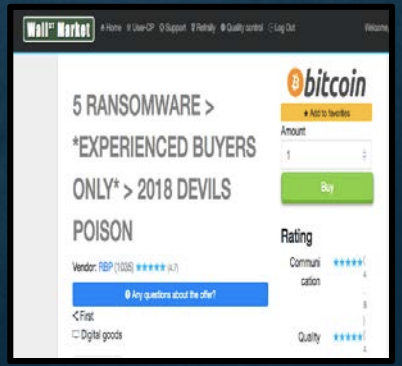
#RSAC

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

Tactical Dark Web Cyber Threats	Strategic Dark Web Cyber Threats	Solutions that Leaders Should Consider
• The theft and monetization of PII/PHI • Increasing amounts of low-sophistication commodity style malware attacks	• The black market pharmaceuticals industry • Disruptive targeting against medical devices	• Threat intel collection in Dark Web markets • Intelligence collection against TTPs that could be modified to impact medical devices

How the Dark Web affects the Public Sector

#RSAC

Overview

Government entities to include federal, state, and local governments

Potential Threats

Weapons Trafficking

Narcotics Trafficking

Intelligence Collection

Key Considerations

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

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

Tactical Dark Web Cyber Threats	Strategic Dark Web Cyber Threats	Solutions that Leaders Should Consider
• The sale of pirated technologies and software • Increasing amounts of low-sophistication commodity style malware attacks	• Breaches that lead to the large-scale theft of intellectual property (IP) • Strategic brand damage	• Key word searches in the Dark Web for IP related issues • Threat intel collection in Dark Web markets

THANK YOU FOR YOUR TIME!

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