SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- CISO Forum

Security Experts:

WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- CISO Forum
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
- Security Architecture

  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- SCADA / ICS
- IoT Security

Home › Risk Management

Demystifying the Dark Web and Mitigating Risks

By Alastair Paterson on June 28, 2018

Share G+ Tweet Recommend 0 RSS

Monitoring a Variety of Data Dources is Important to Understand Threats, Vulnerabilities and How to Manage Risk

The dark web is a hot topic right now, particularly given the speculation and discussion about the future of dark web marketplaces. But for all the notoriety of these marketplaces, it is also important to remember that criminal activity isn't limited to the dark web. It is an Internet-wide problem, and we may even see an uptick in activity on the open and deep web since Operation Bayonet and the takedowns of AlphaBay and Hansa. To fully appreciate this, let's step back for a moment and consider the topography of the Internet.

When most of us think of the Internet we think of the surface or open web, the portion of the web indexed by search engines. Yet this portion of the web only accounts for only a tiny level of the activity online. In reality, much of the activity on the Internet happens below the surface in an area called the deep web. This is where most online databases and other information reside, like the "private" portions of social media accounts, financial records, scientific reports, medical records, government resources, academic journals, etc. These assets are accessible through gateways that we know, all too often, are breached.

The final and smallest percent of the web is the dark web. These are the sites that are deliberately concealed from the rest of the web and Internet traffic. While we usually focus on the criminal activity happening on the dark web, there are also legitimate reasons to use dark web tools. For example, people living under oppressive regimes may use these tools to access information that is freely available to others, and journalists may frequent the dark web to communicate privately with sources. However, the fact remains, there is a large, digital, underground economy on the dark web that consists of illicit goods, compromised data, malicious software and cybercrime as a service tools, as well as knowledge and best practices for executing cyberattacks.

The dark web isn't only a place for illegal, online trade, it's a valuable resource to understand how cybercriminals do what they do. We've seen law enforcement use this information to great success, bringing down dark web markets and creating a ripple effect of mistrust and fear that has hampered other markets from taking their place and new markets from emerging. This is leading to cybercriminals using alternative methods, many of which are legitimate tools, to conduct their business. For example, mainstream communication channels like Jabber, Internet Relay Chat (IRC), Skype, Discord and Telegram, along with forums dedicated to hacking and security, including paste sites and code repositories. If your digital assets and data have been compromised, they are just as likely to end up on the surface web or in deep web forums as they are on dark web markets.

While it may be tempting for organizations to take it upon themselves to determine the extent of their information exposed in the underground digital economy and seek attribution, engaging in such activity can present even more risk if not done with extreme caution. A better investment of your time is to establish a trusted relationship with law enforcement and leave that work to highly trained professionals. Instead, focus more of your resources on creating a threat model that will allow you to better understand the threats your organization faces.

Threat modeling is an iterative process that needs to be updated whenever there are substantial changes to either assets or threats. Typically, the process consists of:

1. **Defining an organization's assets** – critical business processes, high-value systems, intellectual property (IP), etc.

2. **Identifying which systems comprise those assets** – for example, databases, Enterprise Resource Planning (ERP) systems, and more.

3. **Creating a security profile for each system** – this includes which security controls are currently used to protect the identified software applications, such as, firewalls, Endpoint Detection and Response (EDR) systems, web proxies, etc. and which known vulnerabilities are present.

4. **Identifying potential threats** – hacktivists, cyber criminals, freelancers, nation states, a disgruntled employee, etc.

5. **Prioritizing potential threats and documenting adverse events and the actions taken in each case** – this is accomplished by working from known examples of documented attacks and internal risk concerns, and attempting to foresee what the organizational impact of particular threats could be.

With a threat model in place, you can match the highest severity risks to appropriate tactics, techniques and procedures (TTPs) of threat actors. This helps to target security controls and hardening measures – used for mitigation and remediation – that you need to put in place in your organization.

Criminal forums exist everywhere, so focusing exclusively on the dark web won't give you a comprehensive view of your digital risk. And now with the trend among cybercriminals to use alternative methods to conduct illegal, online trade, monitoring a variety of data sources across the Internet is even more important as you strive to understand the threats, vulnerabilities and how to manage risk.

Share G+ Tweet Recommend 0 RSS

Alastair Paterson is CEO and Co-Founder of Digital Shadows. Alastair has worked for over a decade advising secure government and FTSE 100 clients on large-scale data analytics for risk and intelligence. Before founding Digital Shadows in 2011, Alastair was International Propositions Manager at BAE Systems Detica working with clients in the Gulf, Europe and Australasia. He holds a first class MEng in Computer Science from the University of Bristol.
Previous Columns by Alastair Paterson:

[Mitigate Risk From Malicious and Accidental Insiders](#)
[How Cybercriminals Are Using Blockchain to Their Advantage](#)
[Four Ways to Mitigate Cyber Risks for ERP Applications](#)
[Financial Industry Insiders Put the Keys to the Kingdom at Risk](#)
[Demystifying the Dark Web and Mitigating Risks](#)

Tags:
INDUSTRY INSIGHTS Risk Management

Search

SecurityWeek Daily Briefing

BRIEFING

Business Email Address Subscribe

ICS
CYBER SECURITY CONFERENCE
THE ORIGINAL SCADA/ICS CYBERSECURITY CONFERENCE
October 22-25, 2018 | Atlanta
Register Now »

Most Recent Most Read

- Exaramel Malware Reinforces Link Between Industroyer and NotPetya

- Juniper Patches Serious Flaws in Junos OS
- Triangulating Beyond the Hack: Stolen Records Just One Tool in a Comprehensive Kit
- MuddyWater Threat Actor Expands Targets List
- KeyBoy Abuses Popular Office Exploits for Malware Delivery
- Imperva to be Acquired for $2.1 Billion by Thoma Bravo
- Magecart Attack Hits 'Shopper Approved'
- SAP Patches Critical Vulnerability in BusinessObjects
- First GDPR Enforcement is Followed by First GDPR Appeal
- Cyberspy Group 'Gallmaker' Targets Military, Government Organizations

Popular Topics

- Information Security News
- IT Security News
- Risk Management
- Cybercrime
- Cloud Security
- Application Security
- Smart Device Security

Security Community

- IT Security Newsletters
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us