Increasingly, organizations' most sensitive and confidential information is winding up for sale on the Dark Web. No industry is immune. A quick online search for "database for sale on the dark web" returns with regular media reports publishing the headlines of another data breach.

Data Exposure Investigation, under Proactive Incident Response (IR) Readiness Services at Trustwave, can help close gaps in security environments by scouring the internet for data that was potentially made available during a breach. The breach could have occurred before security systems were put in place, or when data may have been compromised because of user actions outside of the security teams' control. Using a mix of automated tooling and manual review, the renowned Trustwave SpiderLabs researchers gain access to sites off the traditional radar and ensure any findings are relevant. We use a mix of automated and manual searching to ensure results are valid, to vet false positives, to optimize search profiles, and to cover all corners of the dark and surface web.

Data Exposure Investigation Services

Trustwave SpiderLabs offers two types of data exposure investigation services under the Digital Forensics and Incident Response (DFIR) consulting category:

- **Data Exposure Services** Search dark web & public sources for sensitive company data
- **Executive Exposure Profiling** Narrow the search to executive data to create executive dossiers and provide employee education

**Threats, Risks and Services**

Your company and your personnel may have been compromised…and you may not even know it. The Data Exposure Investigation Services are designed to identify unauthorized company & personnel data exposed on the Internet, including legitimate and underground darknet and dark web servers. Since executives are frequently the target of social engineering attacks, organizations should educate personnel to understand what information can be collected by adversaries and the risks they can pose, such as blackmail or loss of company reputation.
Threats

1. Data for sale posted on websites
   - Stolen email accounts & passwords
   - Chat sessions
   - Cloud services

2. Threat actors using to
   - Impersonate
   - Steal data

3. Compromised data

4. Social engineering attacks

Risks

1. Loss of customer loyalty
2. Loss of revenue
3. Business downtime
4. Litigation & business costs
5. Stock price devaluation
6. Stolen Intellectual Property (IP)
7. Employee attrition
8. Harm to brand reputation
9. Lack of response plan
10. Preventative data protection

Services

1. Uncover TOR websites & browsers
2. Expose IRC (Internet Relay Channels)
3. Search deep & dark web
4. Investigate surface websites
5. Explore public forums
6. Use covert access to underground sites
7. Expose & eliminate false positives

1. Technical malware deployment
2. Exposing compromised executives
   - Online executive dossiers for sale
   - Impersonating executive access
3. Social engineering attacks

1. Blackmail
2. Company reputation
3. Personal reputation
4. Loss of employment
5. Stolen strategic data
6. Inadvertently leaked information
7. Intentional leakage on dark web
8. Lack of preventative training knowledge

Service Delivery

The investigation starts with a collaborative effort between the Trustwave SpiderLabs investigator and you. We will work together to establish an in-depth understanding of your business and profile data. This in turn enables us to search for and find anything that has been exposed across the surface and dark webs, ensuring that your time is not wasted. The initial searches are likely to return many false positives, at which point we may work with you to gain a better understanding of your business and refine our approach using key words provided by the client. Finally, the end deliverable is a comprehensive report with findings from the investigators inside the elite Trustwave SpiderLabs. Data Exposure Investigation services are available as one-time services or via annual subscriptions, either monthly or quarterly. If a subscription is purchased, a report will be delivered each time the investigation is conducted.

Why Trustwave SpiderLabs?

The Trustwave SpiderLabs team includes 250+ threat hunters, penetration testers (ethical hackers), investigators, malware reverse-engineers and threat intelligence analysts. Team members have a large depth and breadth of expertise in various security domains that adversaries use to leverage an attack against organizations of any size.

Expertise

Our team consists of many of the top security professionals in the world. With career experience ranging from corporate security executives to security research labs as well as federal and local law enforcement, our team has the expertise and dedication to stay ahead of the issues and threats affecting your organization’s security posture.

Experience

We have performed thousands of incident response and forensic investigations as well as application and network security penetration tests for customers around the globe — from startups to Fortune 50 companies.