Cyberdefense

Managed Cybercrime Monitoring [data]

Proactive identification of potential data exposure (whether accidental or malicious) across diverse sources, from paste sites and code repositories to Dark Web marketplaces and underground forums

What we do:

- Monitoring of several sources providing information about data leaks
- Identification of exposed credentials / data dumps
- Gather data via proprietary crawlers, our Threat Intelligence Datalake and strategic partnerships with enterprise Digital Risk Management platforms
- Triage of all alerts by Intelligence Analysts
- Assistance with takedown if required and possible

What you get with our standard service:

- Alert notification upon detection (PII, documents, credentials…)
- Full analysis, qualification and investigation of each case and criticality scoring
- Recommendations
- Optional Takedown service for exposed data

Advanced Capabilities with our Premium service:

- Discovers sensitive content on unsecured cloud applications such as Project Management tools, cloud connected storage drives, file sharing systems and cloud sharing platforms
- Looks for unsecured datasets on open databases exposed to the internet
- Finds exposed documents on connected storage including open RSYNC, SMB, FTP, HTTP/S Filesystems etc.

Cybercrime: stolen information sphere

The stolen information sphere is all about the stealing and selling of stolen information. This information can be sourced from many of the other spheres like phishing, malware and hacking.

Examples of what can be sold are sensitive information like credentials for VPN, ecommerce sites, social media, Windows domain and banking or payment card information.

Depending on the type of information, it can be monetised in different ways. Login credentials can be sold individually, but are usually sold in bulk and can include hashed passwords or passwords in plain text.

Banking details and payment card information can also be sold in bulk on carding forums, or cashed out using numerous methods.

Other popular information sold ranges from a single social security number, or ID number, to a full medical record.

Especially identity thieves like buying medical records as they usually contain a date of birth, place of birth, credit card details, social security numbers, addresses, and emails and health insurance details.