MAKING OUR WORLD
SAFER
TOGETHER

EXCELLIUM

EYEDEEP

DeepWeb is a common name for parts of the World Wide Web where contents are not indexed by standard web search engines for any reason. Part of this Deep Web is known as pasties website.

These websites like “pastebin.com”, “quickleak.se”, “slexy.org” etc... are commonly used for exchanging information about compromised credentials.

Excellium offers a comprehensive service for monitoring the DeepWeb for your domains or any given keyword. This service is called EyeDeep and is operated by the CSIRT of Excellium services.

How do you seek for dataleaks in the wild?

Pasties are by default ephemeral, therefore the traditional monitoring based on search engines does not apply.

These websites could be used also for exchanging snippet of code that may include credentials and information about your infrastructure.

Excellium Services S.A
5 rue de Goell
L-5326 Contern

+352 26 20 39 64

contact@excellium-services.com

WHY EYEDEEP?

Credit photo by Freepik

Monitoring the DeepWeb is not a simple task. Due to the ephemeral nature of the data and the restrictions for accessing it, detection should be performed continuously and any potential findings should be kept. Therefore, detection needs dedicated infrastructure and resources for harvesting, qualifying and perform the triage of the findings.

EyeDeep is a service operated by Excellium CERT-XLM to address this effort for you. By using EyeDeep, you will be able to cover an extra surface in terms of security. This product will allow you to early detect publicly released data leaks that can directly affect your entities. Whether these leaks come from your assets or possibly other compromised website that may contains some of your data, EyeDeep will extend the coverage of your security perimeter.

ACTIVITY

Excellium will perform the following monitoring:

- Continuous scan of pasties websites:
  - Detection of custom keywords and customer domains;
  - Archivals of the matching pasties;
  - Detection of IP ranges.

- Manual triage of detected alerts:
  - Instant notification for credential leak and security related data.

- Comprehensive monthly report for all related findings during the last month.

ACTIVITY DETAILS

Scan of legitimate domains

Based on the list of domains provided by the client, EyeDeep engine scans pasties websites to find such strings. It allows you to be early notified when a collaborator account is compromised or when a data leak occurs.

Active scan for custom keywords.

Based on the list of words or regular expressions you will provide (Vip users, Solutions, Names…). You will be notified when our engine find a match.

Reporting

Excellium will provide immediate alerts through email on newly detected credentials or sensitive information. To avoid false positive and assess potential risks, Excellium manually reviews these alerts (24/7 via SOC).

Excellium will provide a monthly report will include details of all alerts.