GO3

World Wide Web

CYBERSECURITY BULLETIN

ISSUE 10

MAY 2021

WELCOME

Welcome to the tenth edition of GDS Cybersecurity bulletin.

Through the growth of affordable hacking and exploitation tools, the fraudsters are becoming more tempted to gain access to highly secure networks, steal valuable data and sell it online. This easy and quick way to illegally access private information and networks allowed them to build a business market on the dark web, their home internet, and to gain large profits.

Despite all stakeholders' efforts to maintain top tier cybersecurity, data is still compromised and leveraged by malicious actors through the dark web, leading to reputational loss of the concerned organization and negative financial impact.

So, what could be done be more proactive? And how data on the dark web be monitored?

CONTENTS

SUMMARY

The key to any dark web monitoring solution is the ability to reach vital threat data and map it to the risk register of the organization in order to take appropriate actions.

Information about the dark web along with monitoring and analysis processes are detailed in the next pages.

DARK WEB

Nowadays, the dark web is becoming a crucial concern for organizations of all kinds. Apart from the growing list of attack techniques and data breaches, the malicious actors are publishing their illicit activities on the dark web, which increase the impact to victims, or concerned persons and harm their reputation.
Having said that, the enterprises should continuously scan the dark side and put an actionable remediation plan if needed.

Dark web definition
The dark web is a small part of the deep web which itself represents around 99% of the Internet that is not indexed by search engines. The dark web is composed of domains that usually end with ".onion" and require the use of an anonymising browser such asTor to access it. The latter routes the dark web requests through a series of proxy servers operated by thousands of volunteers around the globe rendering the source IP difficult to trace and identify. Another aspect of the dark web is the reliance on Bitcoin to perform anonymous payment: transactions are conducted using bitcoin between two parties without them knowing each other's identity.
In addition, the dark web sites use a scrambled naming structure to make it impossible to remember addresses; for example, the now defunct commerce site, "Dream Market", opens using the address "eajwlvm3z2lcca76.onion."
Since most of the dark web sites are set up by scammers, who constantly change addresses to hide their activities and avoid DDoS, the quality of search on the dark webvaries widely as a lot of material becomes outdated in a short period of time.

Monitor your data on the dark web.
Once the access is available on the dark web node, it will be possible to start acquiring its data using human efforts combined with automated tools. The steps involved in this process are summarized below:

1- Categorize the valuable and sensitive data that could be of interest for malicious actors, such as:
   - User credentials and privileged access
   - Personal Identifiable Information (PII)
   - Source code, customers list, products roadmaps
   - Legal documents, patent information
   - Others

Figure 1: Statistics about the data exposed on the internet- by Terbium Labs.

2- Search for the footprint of the leaked data that could be posted on social media, file sharing sites and black market using several techniques:
   - Simplistic through direct search for the exact data or files, but this could increase your attack surface since the data will be spread outside the organizations to be able to match with leaked data.
   - Search for Indicating tokens related to internal application or code used within the organization.
   - Search for hash files. This step could lead to successful results in some specific cases.

3- Parse the gathered data through automated tools then normalize it for processing, including integration with other systems (SIEM, threat intelligence databases) and deletion of irrelevant records, others...
   Several challenges are addressed at this level:
   - Complexities related to the prioritization of the leaked data and avoidance of false positives.
   - Number of records and fields to match with the real data, in case the data is structured.
   - Overlapping information and difficulties faced in case the data is unstructured.

4- Validate the data.

Based on above, searching for data on the "dark side" requires sophistication to detect real leaks, avoid false positives and not create new risks.
So, it is important to rely on dark web monitoring tools that include as a minimum the below capabilities:
- Perform risk mapping in corelation with the data and provide actionable recommendations.
- Find exact part of exposed data or hashing of data on the dark web.

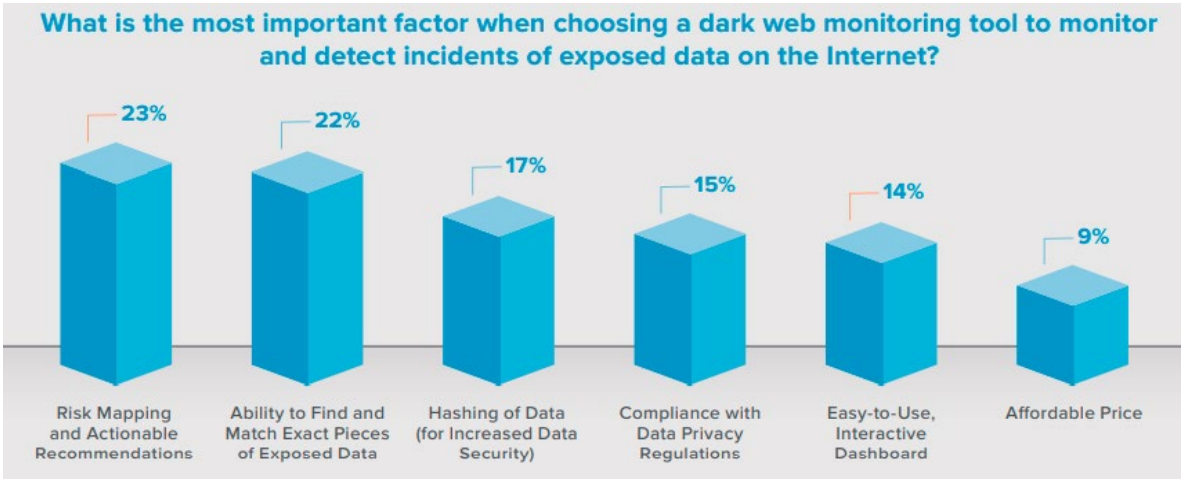

Figure 2: Statistics about the required features of dark web monitoring tools- by Terbium Labs.

Risks of data leaks and mitigation

There is a wide spectrum of risks resulting from data exposure on the internet, such as:
- Phishing, business email compromise
- Account takeover
- Brand damage, reduced revenue
- Doxing

- Physical risk
- Credential theft
- Identity theft
- Fraud
- Money Laundering
- Else

A mitigation process shall be developed and processed within your organization to reduce the impact of these risks, including the below steps:

- Refresh employee training including awareness of prevention steps from phishing attacks, and reminder about email and password policy (ex: set complex password, do not utilize work email for personal use...)
- Notify your customers to take proactive account protection steps, warn them about possible phishing attempts and how to identify them, communicate any data leakage to initiate an immediate mitigation process.
- Secure your systems through passwords reset and targets hardening .
- Increase the monitoring level for early detection of phishing attempts and spam, notify security teams and proactively monitor the dark side.
- Takedown leaked data whenever possible such as fake domains, imposter social media accounts, fake mobile application, personal information…
- Perform investigation in case it is a real data leak and try to understand how this occurred to take the appropriate security measures.

FACEBOOK DATA BREACH

More than 500 million Facebook users' details were published online on a website used by cyber criminals.
According to Insider, "The exposed data includes the personal information of over 533 million Facebook users from 106 countries, including over 32 million records on users in the US, 11 million on users in the UK, and 6 million on users in India. It includes their phone numbers, Facebook IDs, full names, locations, birthdates, bios, and, in some cases, email addresses." Lebanon is amongst the 106 affected countries.

The data breach is related to a vulnerability reported by Facebook and fixed in August 2019, that is related to the misuse of legitimate functions in the Facebook systems according to the reference: *https://www.bleepingcomputer.com/news/security/533-million-facebook-users-phone-numbers-leaked-on-hacker-forum/.*

One of the easiest ways to check if your data has been leaked, is to rely on popular and effective websites maintained by security researchers such as: https://haveibeenpwned.com/ created by Troy Hunt.

According to Hunt, only the leaked email addresses were published on the website for now, and he is still considering the risks of adding the leaked phone numbers to the website.

Figure 3: Troy Hunt Tweet about Facebook data leaks

So, in case your email was exposed, change immediately your password and set-up multi-factor authentication if possible (it is nevertheless a good idea to change your Facebook password anyway).
In addition, you can use password manager tools to generate complex passwords and store them in a database which avoids password-reuse and other types of attacks.

Finally, GDS SOC team performs continuous dark web monitoring and is ready to assist you in building a proactive monitoring of your data through the internet.

To learn more about GDS and our security portfolio, visit https://www.gds.com.lb/security.php

Globalcom Data Services sal
Holcom Bldg., 4th floor
Corniche Al Nahr - Beirut - LEBANON
Tel: +961 - 1 - 59 52 59
info@gds.com.lb

About Globalcom Data Services sal

Operating since 1996, GDS is widely regarded as being one of the first Data Service Providers in Lebanon to bring modern and fast connectivity to the country. Always leading the way to the future for individuals and businesses, GDS has been continuously supporting new technologies for more than 20 years.
Building on its extensive network and security expertise, GDS provides a comprehensive security services portfolio. A team of security experts is available to assist customers with facing the complex security threats and cyber-attacks that might affect their business.

GLOBALCOM DATA SERVICES