Dark Web Scraper

Introduction

Whether you are protecting a bank or the local grocery store, certain common sense security rules apply. These days this is not enough. Cyber criminals are still able to get all your sensitive data. Most of the time the will place it on the dark web before they release it on the normal web. This can take months before you will notices this. If the stolen data contains personal data, you have to report a data leak.

Most of the dark web scraper work on the cloud solution, so you never sure who is seeing your information. In addition, the information that can be found over you or your customer can, and most of the time it is, is private or company sensitive.

The developers will try to prevent that other people can see your information. By using, the solution in your own environment will reduce the risk that others see your information.

Index

History of the Dark web

As with the early Internet, the dark web has also gained a reputation as a haven for illegal activities. The dark web, like the web before it, is frequently blamed for horrible crimes, such as child abuse, child pornography and murder for hire. The dark web makes it harder to enforce both just and unjust laws.

What is the Dark web

The dark web is a place where cyber criminals will hide. The dark web is so large finding them is not easy. If you take the normal web and the dark web as 100%, the dark web takes 96% of the capacity.

The dark web you can only visit with a tor browser. To seek the complete dark web takes a lot of time and the change you are missing information is big.

Disadvantages of the Dark Web

The dark web empowers ordinary people, but some people will inevitably abuse that power. The dark web can make it easier to commit some of the worst crimes. For example, the combination of the dark web and cryptocurrencies theoretically makes it much easier to hire someone to commit a murder. While the dark web promises privacy to its users, it can also be used to violate the privacy of others. Private photos, medical records, and financial information have all been stolen and shared on the dark web.

What content can be found

The content on the dark web is large and you cannot find the content on the normal web. Index services like Google, Bing, Yahoo do not index this part of the web. The on the dark web content can be category i n the following:

Botnets
Botnet is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam or distribute ransomware.

Cryptocurrencies services
Cryptocurrency, altcoins, and crypto tokens are often used to interchangeably in the virtual currency world. However, on the dark web cryptocurrencies are also used for money laundering or funding of illegal activities like ISIS.

Dark net markets
Dark net markets are commercial website on the dark web. Most of the time they are used for selling drugs, cyber-arms, weapons, counterfeit currency, stolen credit card, personal information etc.

Hacking groups and services
Many hackers sell their services on the dark web. They do this either as individually or as groups. Many groups do this. Like xDedic, hackforum, Trojanforge, Mazafaka and dark0de. Cybercrimes and hacking services against financial institutions and banks have also been attacked over the dark web. However, there are more services at the dark web, like hitman, assassination and crowdfunded

Fraud services
There are numerous carding forums, PayPal and Crypto coins trading websites as well as fraud and counterfeiting services like fake passports and ID's.

Hoaxes and unverified content

The term "*Red Room*" has been coined based on the Japanese animation and urban legend of the same name. However, the evidence points toward all reported instances being hoaxes. However, there is also a lot of unverified content. This content can contain a Command and Control or someone who is experimenting on the dark web.

Phishing and scams

Phishing via cloned websites and other scam sites are numerous, with dark net markets often advertised with fraudulent URLs.

Illegal pornography

There is regular law enforcement action against sites distributing illegal pornography. This is different for each country. In the most counties, it is illegal to possess child pornography, but it is not in every country illegal to possess content of bestiality. Other content includes sexualized torture and killing of animals and revenge porn may be illegal to possess.

Terrorism

There are at least some real and fraudulent websites be used by ISIS. This allows the terrorism groups to attack the weaknesses of the technology. An actual such site was hacked by an Anonymous-affiliated hacker group. Terrorism groups also use the dark web to distribute propaganda movies and text, but they use it also for fundraising to support their actions.

Social media

There are social media platforms similar to Facebook, Twitter and pastbin on the dark web. They look and function the same as the traditional social media platforms.

Dark web tool

The developers have many years of experience in searching and investigation of the dark web. They have develop a tool that is able to search the dark web for you. All devices will be delivered as VM image. It can also be delivered as hardware appliance, but that will be custom.

AIO

There is an AIO (All In One) version. This contains a manager, database and one agent. It is able to look for you on the dark web. But can work only with one agent
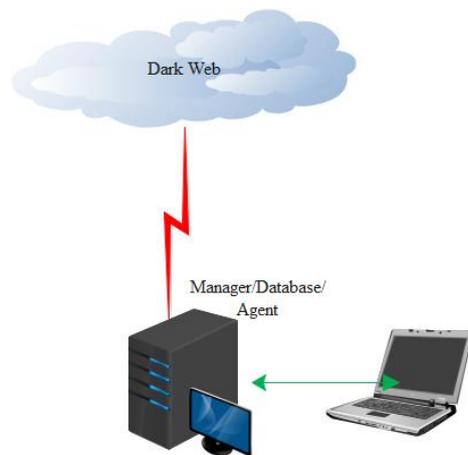
Multi agent

A multi agent version contains of one manager, one database and can have multiple agents. The advances of having multiple agents is the speed of searching the dark web. Depending on the internet connection and the number of agents the speed of searching.
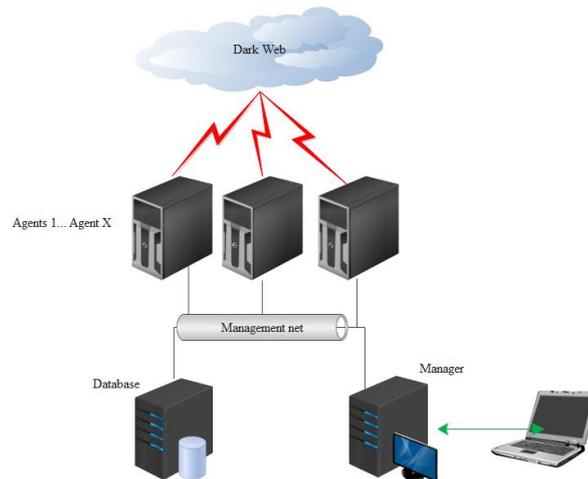
MSSP

A MSSP version contains of one manager, one database and can have multiple agents. The advances of having multiple agents is the speed of searching the dark web. Depending on the internet connection and the number of agents the speed of searching. In addition, a MSSP version is able to let users to login and see only their own hits and keywords.
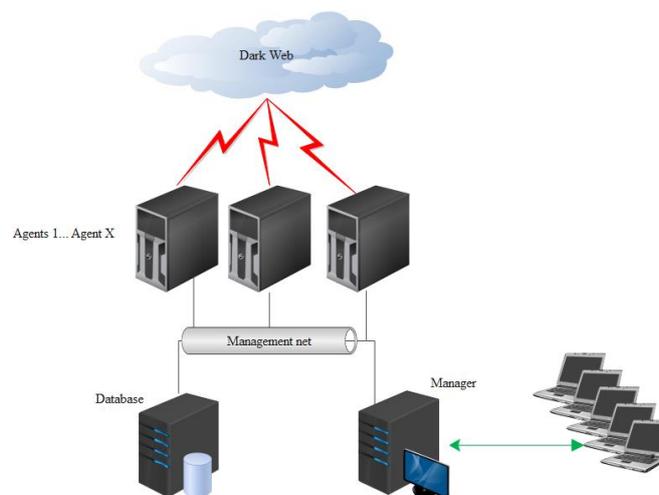
Agent

The agent is the tool that is looking for you information on the dark
web. The agent is the one who is searching the dark web for you. The search is
based on the keywords you have to provide to the system. This keyword can
be for example the name of one of your customers. When there is, a hit found.
The agent will take a screen shot of the page. After that, the image is saves.
The screenshot will be taken in a way that you are **not** in possession of illegal
content. There are several agents available.

- AIO: This agent works on the AIO server and is not able to balance the
  speed.
- Multi agent: This agent is able to work with other agents. This has
  advance the load is even spread over the agents. This will increase the
  speed.
- MSSP agent: This agent works the same as the Multi agent. The
  difference between the Multi agent and the MSSP version is that a hit
  on a keyword is stored only for that specific customer.

Manager

The manager controls the database and agents. If a hit is found a mail
will be send to the persons of your choice. In addition, with the manager you
configure and control the environment.

Database

This is where all the information is stored. The data is encrypted in the database.
On this way privacy can be guaranteed. The database can grow big depending on
The number of domains, links and keywords.

Proxy

The proxy server is used to connect to the dark web. It is possible to have this as a
cluster solution. This way the agents can connect to the dark web immediately

Intelligent

The agents is the one that contains the intelligent.
It is able to read information from a dark web site, but also from
PDF file and hidden information in images. The agent is able to read around 5000
pages a minute. This is based and tested on an internet connection of 1 MB.

Protection

The dark web tool will skip illegal content. It will read the information
on the site. However, if it finds a hit, it will only take a screen shot of
the text of the page and not the images.

Disable protection

There is a possibility to disable this protection.
The developers can do this for you. However,
The developers has to receive a permission from an official
law enforcement agency that you allowed to see and have
this illegal content.

Forensic logging

All the information that is found about you or your customer is
logged on a forensic way. This way it is possible to use the data as
evidence if you or your customer need to go to court,

Customization

It is possible to customize tools and reports. The developers are
able and willing to do this for you.

Add-ons

The following add-ons possible.

Malware analyze

The Dark Web scraper has the option to add a malware analyze tool. This
way you are able to analyze your own malware. The results will be added to
the Dark Web Scraper. The Dark Web Scraper use the Domain to search if
there is more.

Sniffing

There is an option to add a network sniffer to the Dark Web Scraper. This
sniffer will look if there is any connection to the dark web. If there is a
connection to the dark web, it will send a message. In combination with the
malware analyze tool it can also look if there is any connection to the domain
that is contains the malware.

Dark web proxy cluster

There is an option to add a proxy for the dark web scraper. This cluster works
as load balancer for the agents. This will speed up the search