Castellum Labs

WHITE PAPER 2022

Dark Web.
Scanning vs Monitoring

Dark Web scanning, is being pushed by a lot of people and lot of vendors who either have a background in big data analytics or else in traditional log management technologies, such as SIEM.

Though I am a big supporter of dark web monitoring, dark web scanning vendors and techs pushing their offerings (products & platforms) as a potential monitoring solution for threats and stolen data on Dark web is something I don't agree with. I see a lot of vendors providing dark web monitoring services using basic technologies and components which is capable of large scale crawl, collection, search and filter capabilities.

Their claim is to be able to scan the darkweb & locate the stolen data or credentials or other stuff on darkweb and/or deep web, is often misplaced, misquoted and misrepresented. Let us understand a few things about darkweb and what it takes to monitor it meaningfully and use the information and intelligence collected from it.

What is dark web scanning?

Dark web scanning is mostly facilitated by basic crawl, search and match technologies. Use of the analytic components and technologies enables orgs to analyze the collected darkweb data and present the basic findings. This is what is mostly perpetuated by a lot of people as darkweb monitoring. Such technologies, platforms and products have a problem.

They presume an easy availability of dark web assets (servers & resources on them). And, they also presumes the unhindered crawling option to be available to get to those darkweb servers and repositories. And then either scrap for information or else look for information specific to a particular customer/domain. This is mostly not true.

Why such basic web data scrapping and analysis does not work, needs to be understood.

But, before, we get there, lets understand what is dark web monitoring.

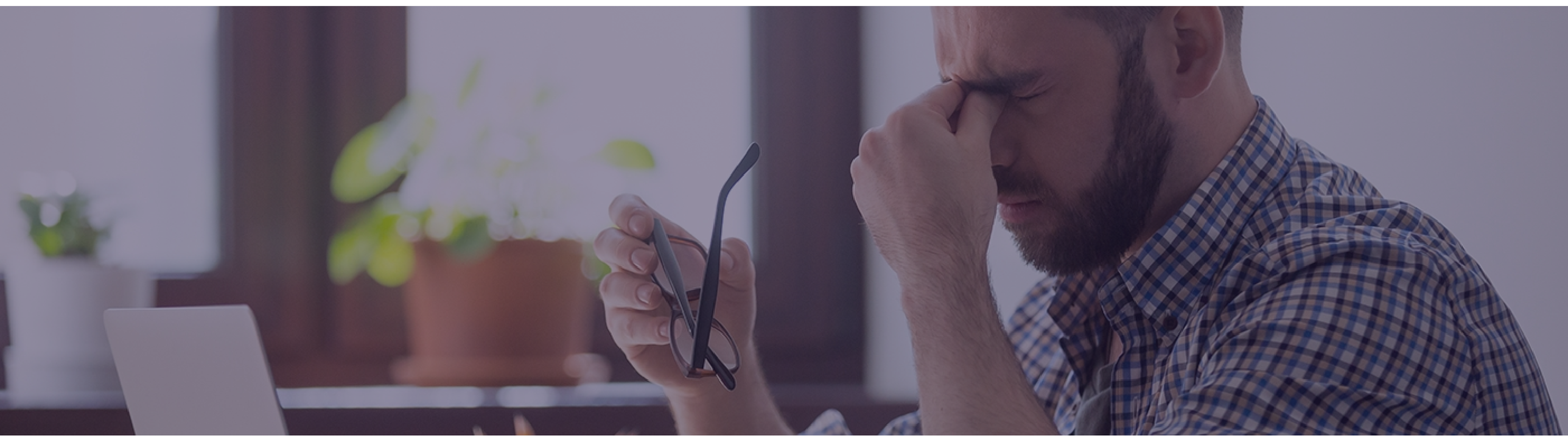
Castellum Labs

WHITE PAPER 2022

What is dark web monitoring?

Dark web monitoring is a large scale hunt operations for a given customer, to discover and unearth data belonging to that customer. Range of techniques are used to infiltrate through dark sites, dark forums, clandestine chat forums and more places to find the stolen data or else locate sensitive information about a particular customer.

A dozen odd techniques are used to facilitate an entry into hidden corners of dark web and know, locate and get stolen data. Crawling of the dark web servers & resources on them is, one and very small part of darkweb monitoring.



Presumption of Availability of Sites

Quite a many of onion sites, on darkweb, specifically the ones, which, may indeed contain stolen data, disruptive and harmful conversations or marketplaces will generally not be up and running most of the time.

Majority of the time, these sites come up for a brief duration, through a secondary channel coordination, to conduct specific transaction or else to do specific conversation, and, then they are taken off the grid.

Lack of Indicators

The real stolen and sold data or indicators on dark web sites, which, may really contain one which belongs to an enterprise, is mostly very obfuscated. And, in some cases it is not placed online at all. While you may be able to scan a specific set of nodes on dark web, you may still not bump into any specific indicators through tags or keyword searches.

Castellum Labs

WHITE PAPER 2022

Mutation of Locations

Quite many cyber criminal operators, groups & malicious actors will keep both, their digital infra and conversation on darkweb in mutated form. The data and other info on dark web, by these malicious actors will not be kept on static set of hosts and static set of trails.

So, even if you locate an asset on dark web which indicates compromised data, keeping on trail of that will be difficult if not impossible, using search and scrapping based technology.

How is Dark web Monitoring, Different?

Dark web monitoring should use a range of techniques, and, many of them are not as tech savvy or technology dependent, as one would think.

These methods will depend on how monitoring has been modeled but here are general list.

- Using pseudo identities to infiltrate forums/marketplaces/data dumps
- Indicative purchases on marketplaces which show your interest in stolen data
- Creating multi-set identities to explore market places which claim to sell data
- Avatars which posture themselves as employees & show interest in selling data
- And, many more

Overall monitoring ops for darkweb has very limited dependency on search techniques. It is largely dependent on active engagement and reverse espionage.

Quite a many times, it takes more than three to six months, to seed the players, into darkweb eco system, who can get their hands on specific customer's stolen data. Any claims that they can keep an eye on all and any stuff on darkweb and locate the sensitive or stolen stuff right away, using a web scrapping tech, is doubtful.

Castellum Labs

WHITE PAPER 2022

Dark web Scanning vs Darkweb Monitoring

- Dark web scanning does not yield results, most of the time (save your investment)
- Dark web scanning is passive in nature and hopes to find stuff
- Dark web monitoring is complicated and time taking process
- It takes a team of experts & quite a bit of understanding of darkweb, to locate data
- And, dark web monitoring is a continuous process, which builds up over time

Dark web Scanning may be a "good to have tool" from baseline search and satisfaction point of view. But, it does not yield any meaningful and effective results, from threat management point of view.

> ***Dark web monitoring is for companies, which are committed to get preemptive about their security, and, engage, look and act on stolen data, credentials and more which can be used against them.***

Key Services Areas

Application Security

Managed AppSec Programs

Cloud Security

Cloud Security Design & Governance

SOC Monitoring

Managed Detection and Response

Threat Intelligence

Contextual Threat Intel & Hunting

Our Technology Platforms

appFORT

Continuous Application Security

watchOUT

Darkweb Monitoring

threatNIXD

Next Gen SOC Monitoring

Continuous Unified View of your Cyber Security

Get in touch with us to know more on our Cyber Security offerings

2022

WHITE PAPER

Castellum Labs

+91 97009 70397

info@castellumlabs.com

www.castellumlabs.com