Securing threats of the Dark Web for Data Centers

Nov 2022

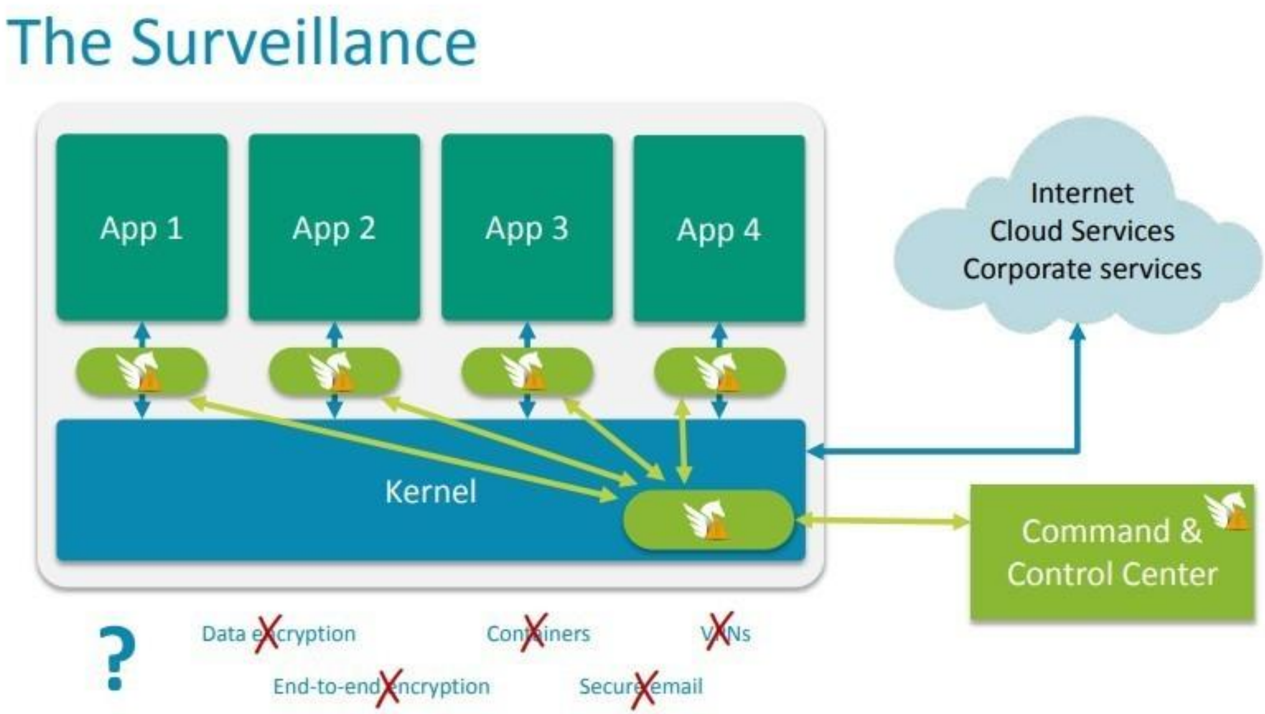
Case study- Pegasus

Pegasus is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device.

A. What can Pegasus do

- Intercept communications sent to and from a device, including communications over WhatsApp etc.
- Remotely turn on phone's camera and microphone to capture activity in phone's vicinity
- Use GPS functions to track a target's location and movements

B. How Pegasus Exploits ?



C. Who has Pegasus targeted?

- NSO had supplied spyware products to UAE, Saudi Arabia and Mexico
- Hacked the phone of human rights activist Ahmed Mansoor in the United Arab Emirates.
- NSO exploit links may have been sent to Mexican scientists and public health campaigners

45 NSO Pegasus infections associated in more than 45 countries

Case study- Pegasus- WatsApp

Impact on India

Pegasus was quietly eating into some Indians' data during this **year's election season**

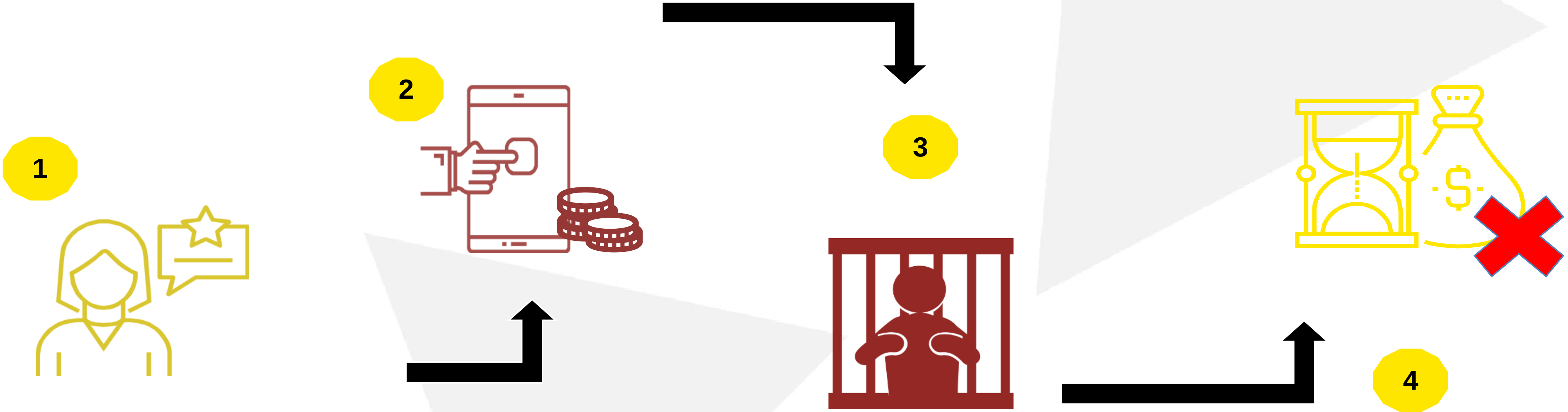
At least two dozen journalists, lawyers and activists in the country were targeted for surveillance in the weeks before May 2019 **via messaging platform WhatsApp**.

Targeted users include Nagpur-based Human Rights lawyer, Adivasi activists and former BBC journalists, amongst others.

Recent Buzz!!

- ✓ On October 29,2019, WhatsApp sued NSO Group for exploiting a since-then fixed vulnerability that **targeted 1,400 people**, about 100 of whom were human rights defenders, journalists, political dissenters, and lawyers in **at least 20 countries**.
- ✓ WhatsApp had informed the Ministry of Electronics and IT (MeitY) in early September 2019 that **121 Indians** had been affected by this

Case study- Pegasus- on dark web



- In July 2018, a lead programmer working for NSO Group, the Israeli cybersecurity firm behind the notorious Pegasus iPhone malware has been arrested after a failed attempt to illegally sell the top-secret spyware to an unauthorized party via the dark web in exchange for **$50 million worth of cryptocurrency**

- Although the attempted **$50 million sale was unsuccessful**, the incident raises a number of questions about
  - The internal security processes of NSO
  - Other private cybersecurity firms whose products like Pegasus could have potentially disastrous and far-reaching consequences if they fall into the wrong hands

Dark Web...................

1 What is Dark Web

Introduction to Dark Web and its time line

2 How it works

How to access Dar Web and why

3 Threats and Risks

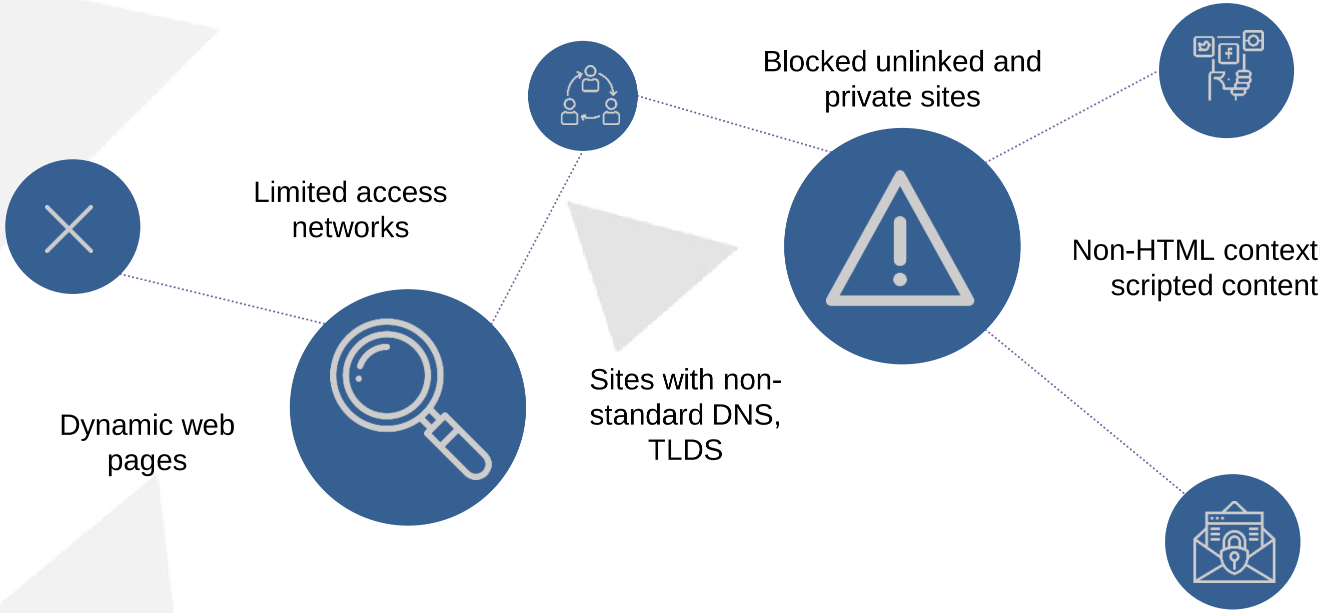
Why should you be concerned

4 What you need to do?

Actions businesses need to take to not be caught on wrong-foot

5 Case- studies

Work performed by EY



Limited access networks

Dynamic web pages

Blocked unlinked and private sites

Sites with non-standard DNS, TLDS

Non-HTML contextual scripted content

DARK WEB – *the hidden internet*

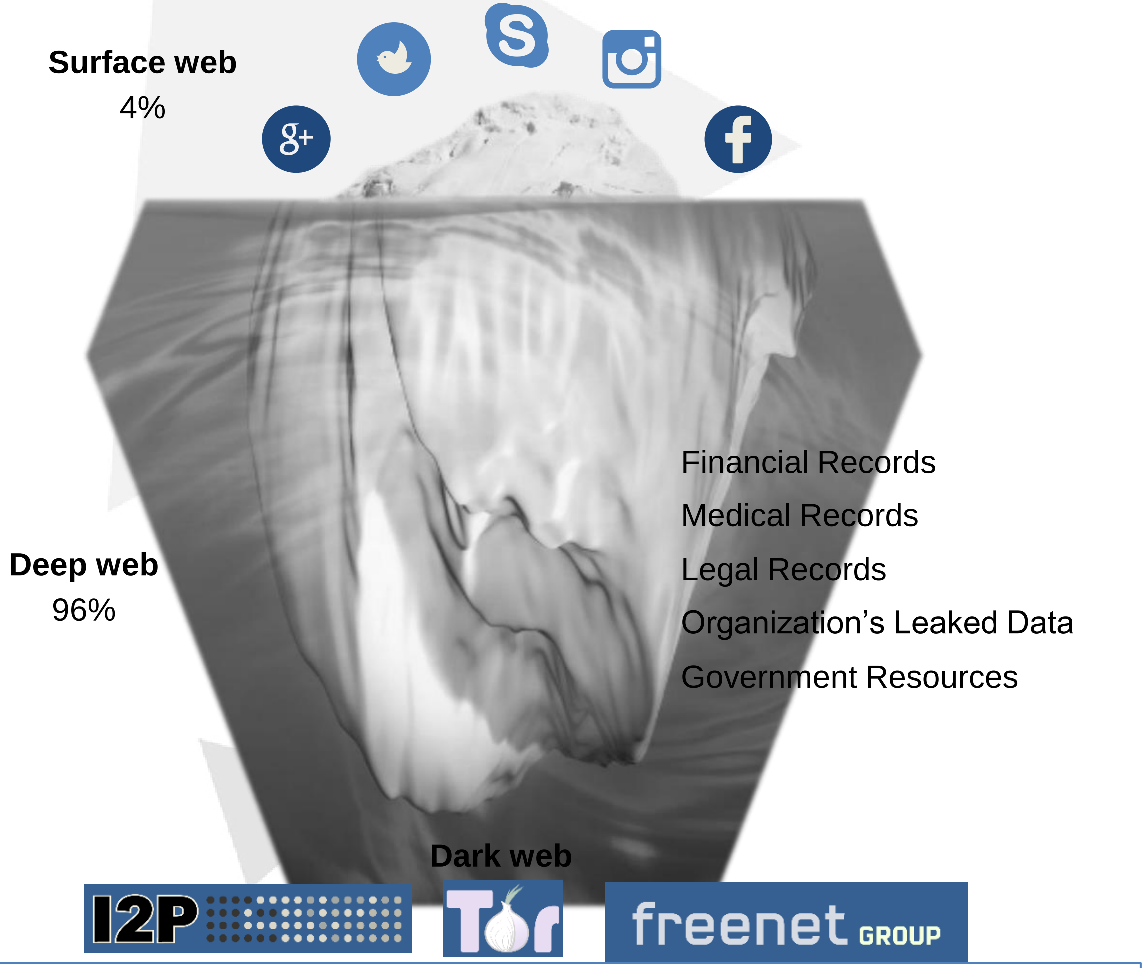
What is it?

Introduction

- Also known as the deep internet, deep net, or the invisible web, a Dark Web (or dark net) is any overlay network that can be accessed only with specific software, configurations, or authorization, often using non-standard communications protocols and ports.
- Dark web comprises web pages and data that are beyond the reach of search engines. Some of what makes up the Deep Web includes abandoned and inactive web pages, but the bulk of data that lies within has been crafted to deliberately avoid detection in order to remain anonymous.

Two typical dark web types are:

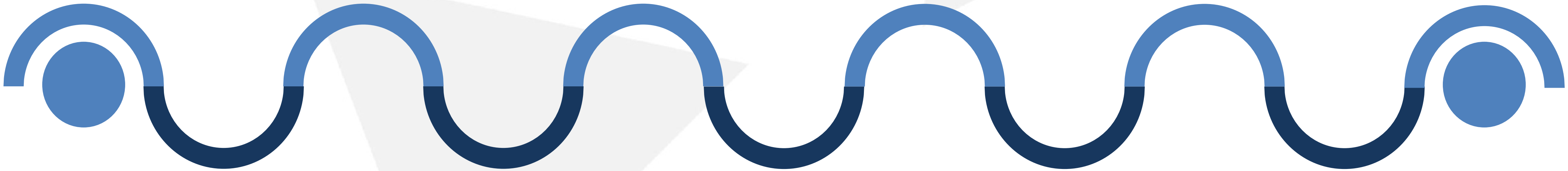
- friend-to-friend networks (usually used for file sharing with a peer-to-peer connection)
- Privacy networks such as The onion router (Tor)



Dark Web v/s Deep Web
Dark Web is only a part of the Deep Web. The Dark Web relies on darknets or networks where connections are made between trusted peers.
Dark Web are the deeper portions of the Deep Web that require highly specialized tools or equipment and configurations to access it. It lies deeper underground and site owners have more reasons to keep their content hidden.

DARK WEB – *the hidden internet*

Timeline



2000

The free net network started hosting static content

2002

Tor Network developed by US Naval Research Laboratory

2003

The I2P peer-to-peer network developed

2006

Tor becomes a non-profit organization

2009

“Satoshi Nakamoto” started Bitcoin digital currency

2011

Silk Road Market launch

2012

Carnegie-Mellon University researchers estimates Silk Road earnings to US$22M

2013

Silk Road shuts down (earnings > $1B) and relaunch of Silkboard 2.0

2014

Other dark web markets proliferate (Agora, Evolution)

2015

Ross Ulbricht sentenced to life; Evolution exit scan

2017

TradeRoute marketplace exits.
Huge scam with Bitcoins of $9 million value

DARK WEB – *the hidden internet*

How it works?

How to access darknet?

All darknets network require specific software installed or network configurations made to access them. To access the hidden web you need two things –

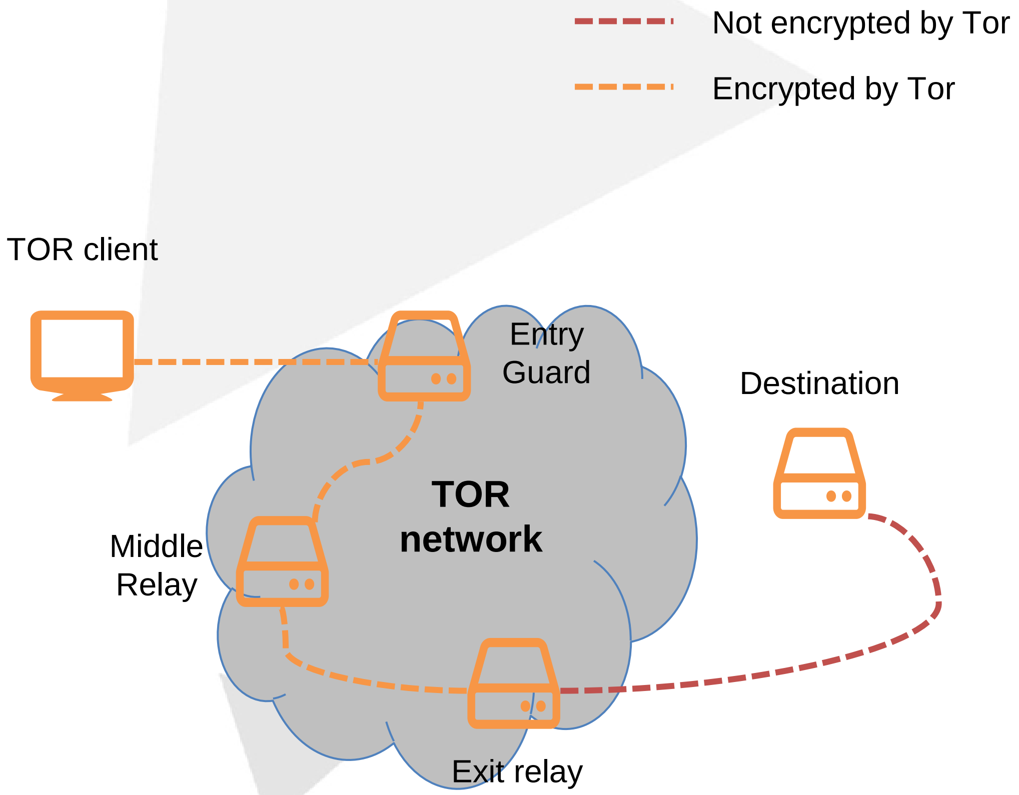
- The Onion Router (also known as Tor Browser) that can access dot onion pages
- A search engine or web page that can help you to search the dark web

Other Deep Web Technologies

- I2P – Anonymity network
- FAI (Free Anonymous Internet) – Based on blockchain technology
- ZeroNet – Based on torrent technology

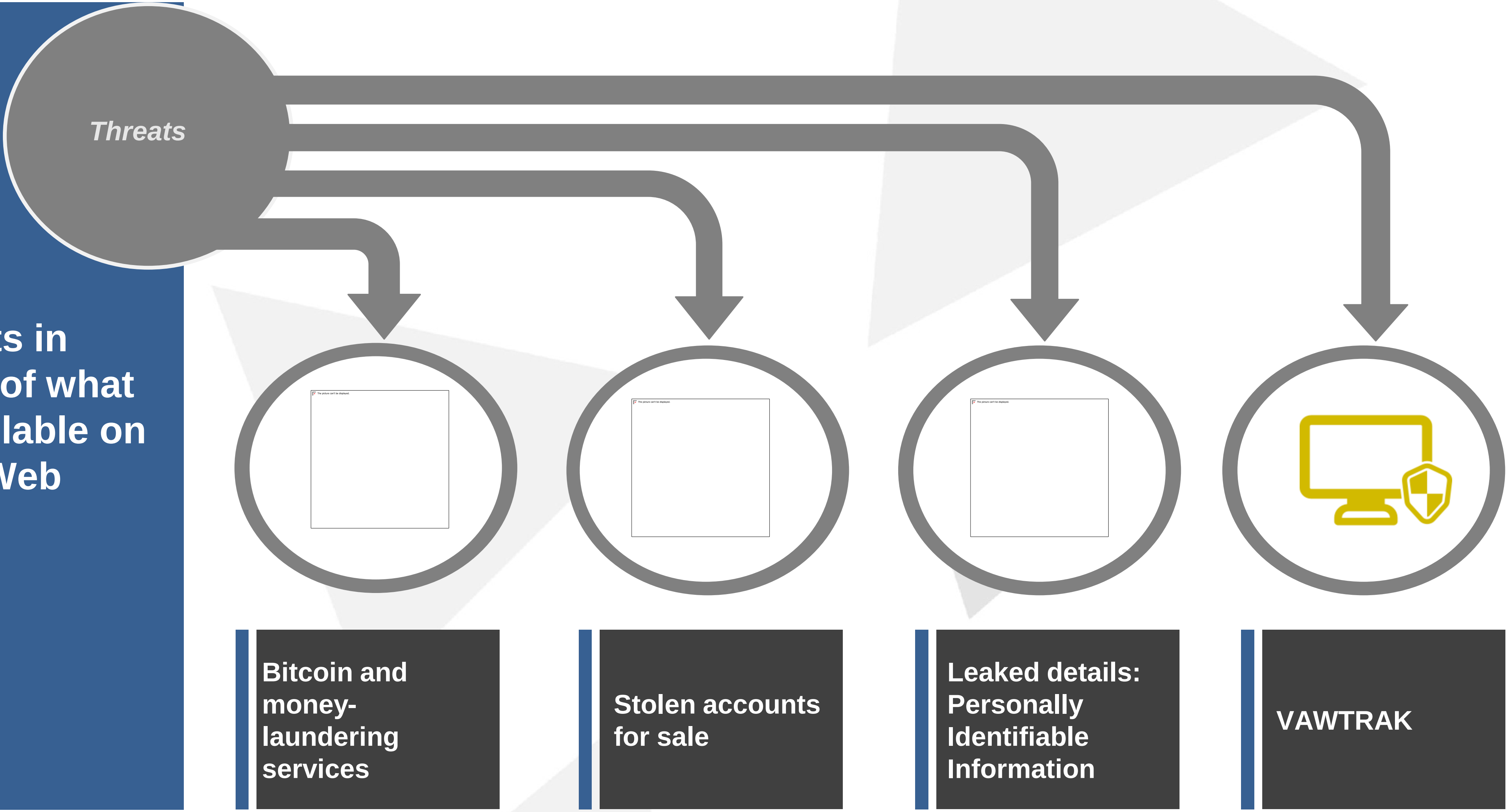
Darkweb benefits to Hacker?

- **Anonymity**
- **Privacy**



DARK WEB – *the hidden internet*

Threats in terms of what is available on Dark Web


Threats
The picture can't be displayed.
The picture can't be displayed.
The picture can't be displayed.

Bitcoin and money-laundering services

Stolen accounts for sale

Leaked details: Personally Identifiable Information

VAWTRAK

DARK WEB – *the hidden internet*

Risks

External - Reconnaissance using TOR; pre-attack planning; Attacks using TOR to hide originating IPs (DDoS, C&C, Hacking – Application and Network level); Infection; browsing the dark web is not safe, drive-by downloads, exploit kits, etc.

Circumventing IT Controls - TOR from USB or using TAILS Live CD and Private Proxy.

TOR Relay Hosting - TOR relays set up in your own network leading to potentially illegal material, non-authorised users of your network resources and the legal knock-on effects. Possibility of the relay host being compromised (hacked) acting as a pivot point for attackers

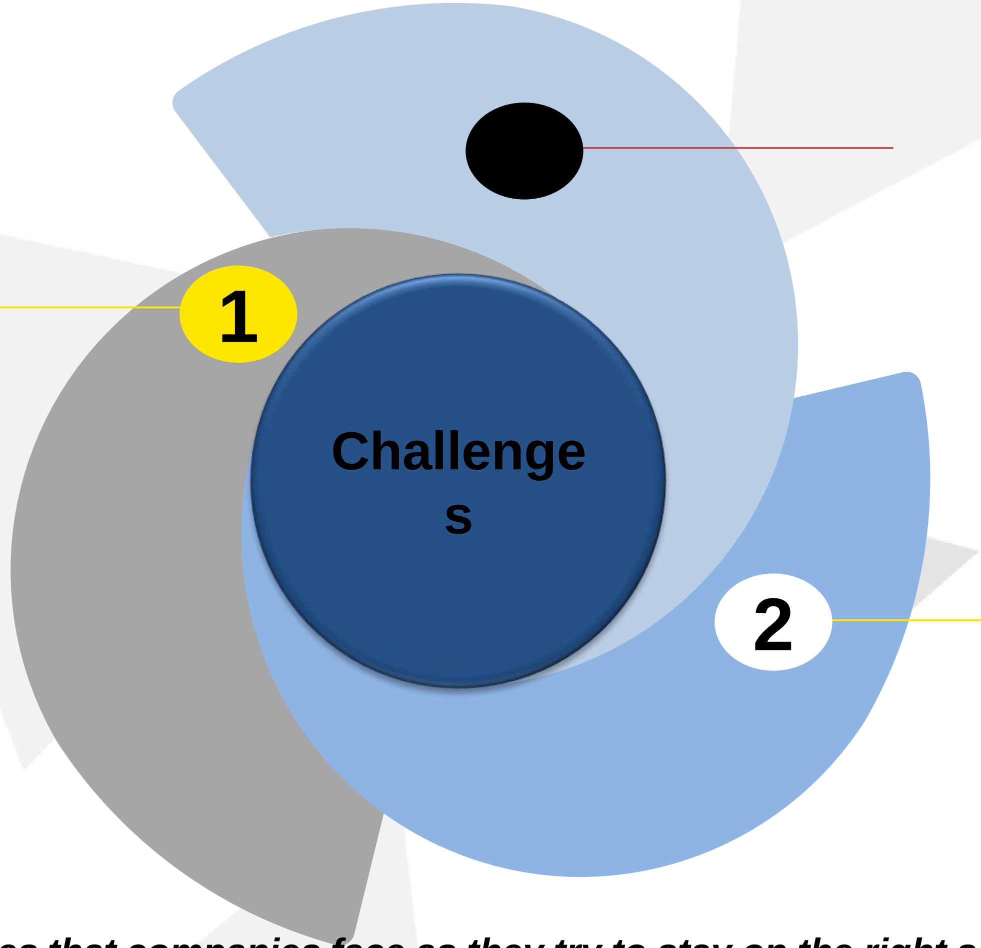
Bitcoin Mining - Data centre and other powerful systems being used without the knowledge or approval of the asset owner.

Reputation – Brand Risk - Market Place, Search Engines, Email, Social Media, Search Engine Ads; Whistle-blowers may want to share vast amounts of insider information to journalists without any paper trail.

DARK WEB – *the hidden internet*

Challenges posed to law enforcement agencies and corporates

Law enforcement agencies already face several existing challenges when it comes to international crime on the Surface Web. With regard to the Deep Web, three additional aspects can make law enforcement even more problematic.



Encryption

Everything in the Deep or Dark Web is encrypted. This makes user information hidden. In the dark web, users can communicate and transact with each other anonymously.

Attribution

It's extremely difficult to determine attribution. Everything happens on .onion domains. The dark web sites have no common names, only sixteen digit strings of alphanumeric characters, which are traded personally among users.

Fluctuation

The Deep Web is a very dynamic place. An online forum can be at a specific URL one day and gone the next. The naming and address schemes in the Deep Web often change.

The dark web is one of the major challenges that companies face as they try to stay on the right side of the lines drawn by Privacy regulations

DARK WEB – *the hidden internet*

Way forward-The solution to the pertinent challenges

Prepare - If you prepare for a data breach, you can create more effective safeguards to make your data harder to interpret.

Monitor - Ensure that you or your Managed Service Provider have the capabilities to scan the dark web and identify your company data.

Secure - Use of Deep Web Analysers, Threat intelligence and Web Application Firewalls (WAF).

Manage Risk - Evaluate risks specific to your business and create a step-by-step plan to ensure you don't lose time trying to figure out what to do next.

Educate - Educating your workforce about the risks associated can help limit the likelihood that the Dark Web will create havoc in your own firm

Know your employees - sources on the Dark Web try to recruit "insiders" at companies to legitimately gain access to company information, which could then be misused

DARK WEB – *the hidden internet*

Threat Intelligence, Dark Analytics and Web Application Firewalls (WAF)

Threat Intelligence

- Leverage threat intelligence and mitigation platforms to monitor and analyse attacks.
- The intelligence gathered on the Dark Web allows organizations to defend against threats to their own assets and applications, and stay abreast of new vulnerabilities being sold in underground marketplaces.
- The data helps brands learn when they are mentioned in a negative context — as in a vulnerability, hack attempt or leaked information.

Dark Analytics

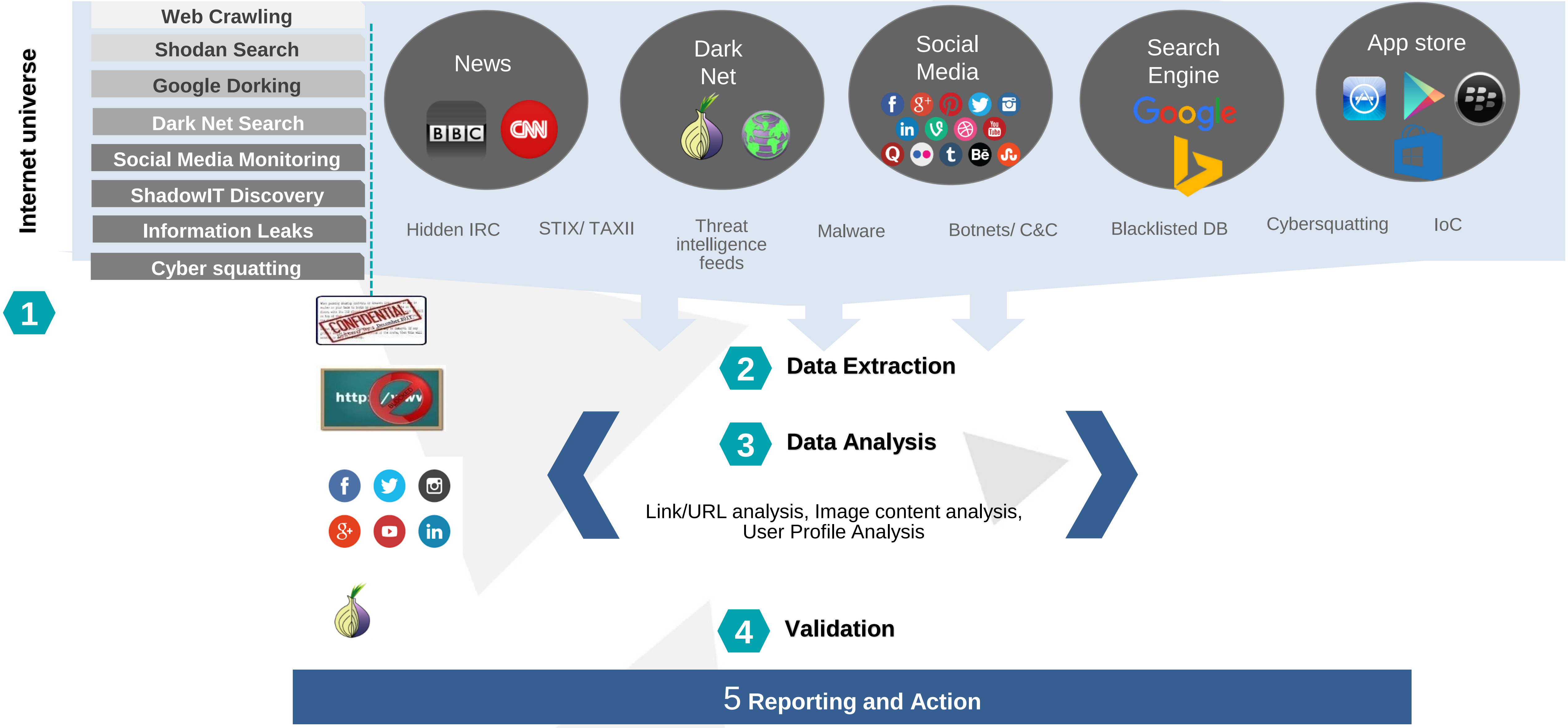
- While there are risks to enterprises attempting to garner unindexed data from the Dark Web, the benefits of anonymity allow them to extract previously untapped business, customer and operational insights by investigating unstructured and hidden or undigested data.
- Leverage new search tools designed to help users target scientific research, activist data or even hobbyist threads.

Web Application Firewalls (WAF)

- WAF models applications, including field type & length
- Signatures identify “suspicious” web requests
- Works on signature based algorithm
- Identifies attacks, like SQL injections command injection, XSS, by correlating a profile violation and signatures

DARK WEB – *the hidden internet*

Solution to the persistent issue of dark web- What should organizations do?



Internet universe

1

- Web Crawling
- Shodan Search
- Google Dorking
- Dark Net Search
- Social Media Monitoring
- ShadowIT Discovery
- Information Leaks
- Cyber squatting

News

Dark Net

Social Media

Search Engine

App store

Hidden IRC

STIX/ TAXII

Threat intelligence feeds

Malware

Botnets/ C&C

Blacklisted DB

Cybersquatting

IoC

2 **Data Extraction**

3 **Data Analysis**

Link/URL analysis, Image content analysis, User Profile Analysis

4 **Validation**

5 **Reporting and Action**

Performed digital footprint assessment through their CTI framework for a Auto-Manufacturing industry.

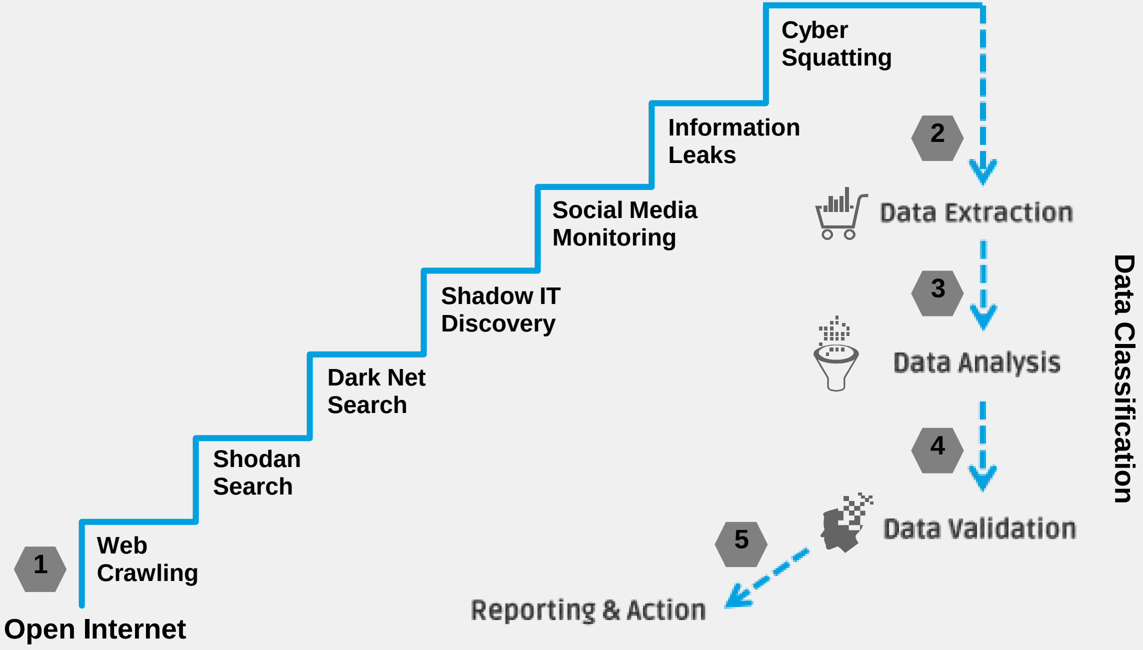
Offering Description

The Cyber Threat Intelligence tool gathers information about the client entity and brand from hundreds of different sources and delves deep into multiple different avenues where a client entity may be exposed, depending on the services provided by them

Modules

- **Digital Foot-Printing**
- **Document Search**
- **Rogue Mobile Applications**
- **Social Media Scanning**
- **Brand Monitoring**
- **Anti-Phishing**
- **Malware & Threat Advisory**
- **Credential Leaks**
- **Dark Web Monitoring**

Solution Overview



Client Issues Addressed

- What parts of the organization's tech infrastructure are visible from the open internet?
- Are there any phishing or malware campaigns associated with my organizational brand?
- Have any sensitive credentials or IP addresses been leaked-accidentally or intentionally?
- Is my brand reputation being tarnished by a social media campaign or a data breach?
- Are there any rogue mobile applications using my brand name to aide in nefarious agendas?
- Are there any threats or vulnerabilities in our network-facing systems that was overlooked, which could be leveraged in an attack against my organization.

Red Team program build for a large bank.

Phase I: External Cyber Kill-Chain

Phase II: Internal Cyber Kill-Chain

Phase III: Target Manipulation Kill-Chain

Methodologies Used

- **Dark Web Research**
- **Threat Intel analysis**
- **Cyber Threat Actor Scenarios**
- **Advanced Attack TTPs**
- **Command and Control Channel**
- **Red Team kill-chain Review**
- **Optimized counter measures**

Tasks Performed

- Company end point assessment
- Compromise of global payment process
- Compromise email systems

Provided a holistic approach to aligning the company's information security program to current threats and emerging technologies

Identified critical security issues within information systems and provided actionable remediation strategy

Helped the client to build process and procedure about how Red Team activities should operate

Identified critical security gaps existing between Red Team and blue team within the company's information security program

THANK YOU

The better the question. The better the answer. The better the world works.