DARKOWL

UNDERSTANDING DARKNET INTELLIGENCE (DARKINT)

DARKINT™ is a term, trademarked by DarkOwl, that combines two concepts: darknet and intelligence.

Intro

The darknet (or "dark web") is a thriving ecosystem within the global internet infrastructure that many organizations struggle to incorporate into security posture, but is becoming an increasingly vital component. In certain cases, that is because taking raw data and turning it into actionable security intelligence requires leveraging DARKINT – or data points sourced from the darknet and other OSINT sources that together form a risk and/or investigative portfolio.

Darknet 101

The darknet is a layer of the internet that was designed specifically for anonymity. It is more difficult to access than the surface web, and is accessible with only via special tools and software – specifically browsers and other protocols. You cannot access the darknet by simply typing a dark web address into your web browser. There are also darknet-adjacent networks, such as instant messaging platforms like Telegram, the deep web, some high-risk surface websites.

Quick Definitions

darknet: Also referred to as the "dark web." A layer of the internet that cannot be accessed by traditional browsers, but requires anonymous proxy networks or infrastructure for access. Tor is the most common.

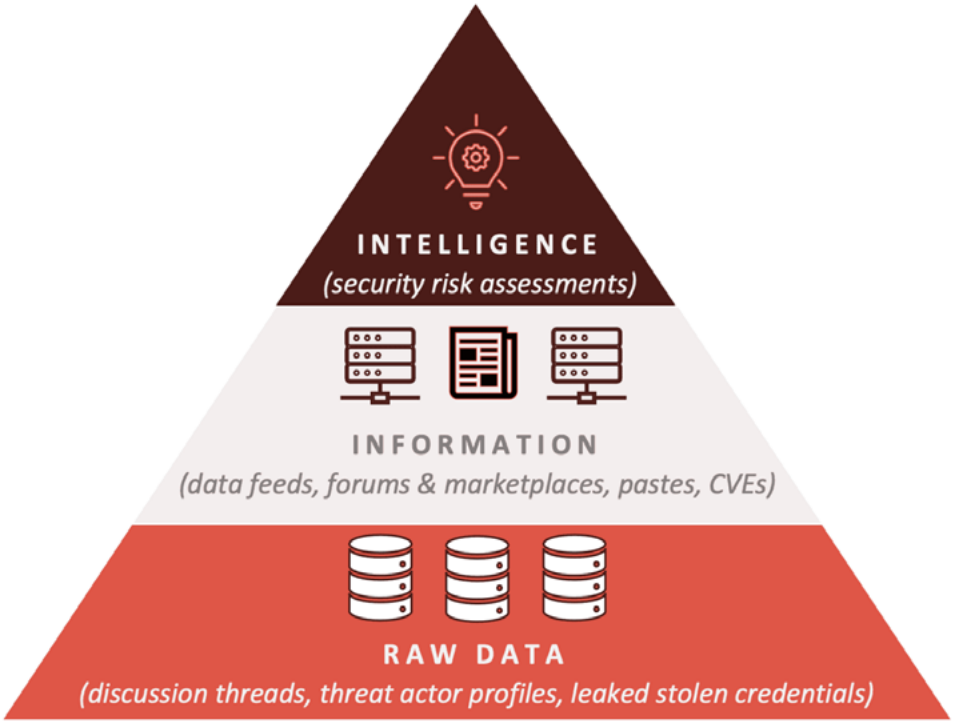
deep web: Online content that is not indexed by search engines, such as authentication required protected and paste sites and can be best described as any content with a surface web site that requires authentication.

high-risk surface web: consists of areas of the surface web (or "regular" internet) that have a high degree of overlap with the darknet community. This includes some chan-type imageboards, paste sites, and other select forums.

For a full list of darknet terms, check out our Glossary of Darknet Terms >>

The darknet is home to a diverse group of users with complex lexicons that often overlap with the hacking, gaming, software development, law enforcement communities, and more. DarkOwl's Glossary of Darknet Terms is a continually evolving resource that defines the common vernacular, slang terms, and acronyms that our analysts find in places like underground forums, instant messaging platforms (such as Telegram), as well as in information security research pertaining to the darknet.

What is Darknet Intelligene (DARKINT)?



DARKINT™ is a term, trademarked by DarkOwl, that combines two concepts: **darknet and intelligence.**

The darknet, also referred to as the dark web, is a segment of the Internet, hidden by the novice user, that is only accessible by using specialized software or network proxies. Due to the inherently anonymous and privacy-centric nature of the darknet, it facilitates a complex ecosystem of cybercrime and illicit goods and services trade.

Data scientists define intelligence as a continuum of increasing data complexity. At the foundation of the pyramid is "raw data." In statistics, raw data refers to data that has been collected directly from a primary source and has not been processed in any way.[1]

Assembled collections of raw, unverified data across multiple sources with context forms the basis of "information."

Intelligence is the consequence of combining analyzed, interpreted, and validated information with informed perceptions and personal experience to drive decisions.

DARKINT™ is intelligence derived from pure darknet, deep web, and associated adjacent underground cyber information sources.

Some key features of intelligence:

- Intelligence is created and shaped by humans. Machines can compile information but cannot produce intelligence.
- Intelligence is based on multiple, trusted and verified sources.
- Data intelligence is also sometimes referred to as 'insights.'
- Intelligence utilized by national security or geopolitical decision makers is often accompanied by a numerical confidence value, calculated using the history, veracity, and perceptions of the information available.

Darknet Intellligence and DarkInt™

DarkOwl's product suite facilitates the formation of actionable, DARKINT because its Vision platform collates darknet data from multiple sources including the deep web, high-risk surface web, and darknet-adjacent networks, such as instant messaging platforms like Telegram and IRC.

In the framework of underground criminal activity and darknet(s), the continuum of data, information, and intelligence follows the example:

- a sample of raw data could be a leaked credential for ABC software company;
- information consists of a document in DarkOwl Vision collected from a darknet forum where a threat actor shares a database containing the leaked credentials from ABC software company in conjunction with a known vulnerability against Microsoft Exchange server;
- a security analyst receives an alert of this document and analyzes this information to find the threat actor's social media account touting they will carry out a 'special' cyber-attack next weekend, coupled with a scan of the software company's network indicating they haven't installed multi-factor authentication on their employee accounts. Using this analysis and their intuition, the analyst produces a security risk intelligence assessment stating they believe with high confidence the threat actor is very likely to attack ABC software company as early as next weekend and alerts ABC's IT department to deploy multi-factor authentication and immediately patch all potential points of network entry.

The information in DarkOwl Vision, combined with open-source intelligence (OSINT) resources such as social media, port scanning, and network data, facilitate comprehensive business decisions across a numerous diverse set of use cases: **threat intelligence, fraud detection and mitigation, cyber insurance, supply chain and vendor risks, digital identity protection, national security, critical infrastructure protection, and law enforcement investigations.**

An Overview: DarkOwl Vision App

Search and Monitor the most comprehensive Darknet Dataset

The Vision app is the industry leading platform for Analysts to simply, safely, and comprehensively search the largest commercially available source of Darknet data. Vision provides a user friendly interface with powerful querying capabilities to search, monitor, and create alerts for critical information.

Common Types of Raw Data and Information Circulated on the Darknet

Personally Identifiable Information (PII)

Personally Identifiable Information, or PII, is any information used to identify an individual. This type of data is incredibly valuable on the darknet, especially when combined with credential information. Examples include full name, billing address with the zip code, date of birth, email address, passport numbers, national identification numbers, and phone numbers. It also includes anything associated with one's online presence such as a social media profile. Even information like a leaked mobile phone number can be leveraged by threat actors for social engineering activities like SIM swapping, which is used by criminals to bypass multi-factor authentication and gain unauthorized access to online accounts.

Banking and Transaction Data

Debit and credit card numbers are a common type of raw data available on the darknet. Some criminals specialize in the trade of the cardholder's sensitive PII associated with associated details for debit and credit card numbers, e.g. CVV, expiration date, and personal pin code. Criminals use card numbers to make fraudulent purchases online and deliver them to a different address, make a series of low-cost purchases the victim won't notice, or buy expensive goods in person.

There are numerous forums and marketplaces specializing in banking, carding, and financial fraud on the darknet and in DarkOwl Vision.

Critical Corporate Data

Critical corporate data consists of mentions of company names, domain names, IP addresses and other corporate identifying markers on the darknet. Sometimes raw corporate data like the domain name, subdomains, or IP addresses for a company are shared in the darknet or deep web temporary paste sites for threat actors to collaborate ahead of a concerted cyberattack against the company.

A darknet database brokerage service advertising a company's stolen competitive intellectual property, product design schematics, and sensitive financial or contracts packages for sale is information, not intelligence.

Credentials and Compromised Accounts

Credentials are the secure information required to safely log in to network accounts. It is user-specific information that verifies the identity of the user attempting to access to the website or service. Some credentials are also considered PII. Credentials which include personal names such as usernames, are also considered PII. Email addresses and passwords are the most common type of credentials. More sophisticated credentials include PGP keys, AWS/Azure developer secret keys and security tokens. Credentials can also include user-verification and digital identity authentication tools.

Malware, Exploit Toolkits, and Ransomware

Malware is malicious software with harmful code designed to break into, infect, steal, surveil, compromise, or crash networked devices. It is used to get what a criminal wants from a target without their consent. There are many categories of malware like viruses, spyware, keyloggers, and ransomware.

Several types of malware, exploit toolkits, and ransomware are available for purchase on the darknet. High quality malware has detection-evasion, to bypass network security systems, and will establish persistence, meaning it will stay undetected and continue giving the cybercriminal access to the information on the compromised device for months or years.

Information consists of feeds and documents in DarkOwl Vision detailing the advertisements for such malware on offer or a ransomware Tor service publishing the identities of their victims along with the extorted sensitive corporate data and PII stolen from the victim.

Malware development and exploitation attack techniques are also openly discussed in darknet forums collected by DarkOwl Vision.

Example Darknet Sources Containing High-Consequence Information

Threat Actor Chatter from Instant Messaging Platforms

Conversations (also known as "chatter") directly from and associated with threat actors and their associated criminal communities on instant messaging platforms are an important aspect of information gathering to develop intelligence assessments based on DARKINT.

Instant Relay Chat (IRC) has been a historical, real-time chat environment for threat actors to plan, collaborate, and securely distribute stolen information related to cybercrime. Modern chat platforms like Telegram are an increasingly popular, high-frequency source of substantial darknet-adjacent information, despite not being directly connected to the darknet. These types instant messaging platforms are widely utilized by threat actors, who administrate both public and private servers and channels.

Chatter from instant messaging platforms coupled with darknet forum posts and OSINT aides in the translation of information into actionable, high-confidence DARKINT judgements.

Nation State Actors and Political Activity

Darknet intelligence concerning nation state actors and political activity is becoming increasingly relevant. Nation-states are typically on the darknet for intelligence gathering and espionage, campaigns to disrupt critical infrastructure of other nation-states, activism and propaganda, sharing and testing source code, exploits, and vulnerabilities, and for financial gain. Disinformation and misinformation are powerful tools some nation-states use to sway public perception and opinion.[2]

Even before the invasion of Ukraine, DarkOwl found evidence that nation-states were increasingly using the darknet as an information-based battlefield for a variety of key intelligence and cyber military campaigns.[3]

In just the last 90 days, Telegram has featured as a critical network for 24/7 disinformation campaigns and information operations spearheaded and sponsored by the governments of Russia and Ukraine. Channels regularly include interviews with prisoners of war (POWs), digitally altered videos to trigger false-flag operations or claim kinetic military success against critical infrastructure, and leaked data disseminated from successful cyber operations.

Conclusions

DARKINT is the byproduct of combining human-powered analysis of validated data derived from darknet sources with informed perceptions and personal experiences.

By actively monitoring for raw data points such as sensitive PII, compiled information advertised and discussed on forums and marketplace, along with darknet-adjacent chatter and associated OSINT signals, one can create concrete DARKINT, and quickly deploy remediation or defense mechanisms accordingly.

DARKINT is most effective when applied to drive complex decisions like quantifying supply chain and vendor risk, underwriting cyber insurance policies, fraud mitigation and digital identity protection efforts, or creating qualified, actionable threat intelligence products in matters of national security, critical infrastructure protection or law enforcement investigations.

DarkOwl's Vision-derived DARKINT helps international governments, local law enforcement, individuals, and companies create a more comprehensive security posture.

SOURCES

1 https://www.statology.org/raw-data/
2 https://www.darkowl.com/blog-content/nation-state-actors-on-the-darknet/
3 https://www.darkowl.com/blog-content/analysis-of-ukrainian-data-released-on-the-darknet-in-lead-up-to-russian-invasion/

DARKOWL DATA SOURCES

Tor, I2P, ZeroNet, authenticated forums, darknet marketplaces, IRC, high-risk paste sites, encrypted chat services, and open FTP servers.

ABOUT DARKOWL

DarkOwl uses machine learning to automatically, continuously, and anonymously collect, index and rank darknet, deep web, and high-risk surface net data that allows for simplicity in searching.

Our platform collects and stores data in near realtime, allowing darknet sites that frequently change location and availability, be queried in a safe and secure manner without having to access the darknet itself.

For more information, visit www.darkowl.com