everbridge signal powered by NC4

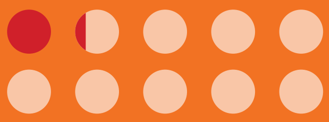
Dark Web Monitoring for Corporate Security

An Evolving Threat Landscape

The dark web is renowned for being where cyber criminals and terrorists go to plot and purchase resources for their next illicit activity. The media portrays it as some mysterious dark underworld of genius hackers, dark souled terrorists and nefarious merchants. As such, it has taken on a semi-mythical place in many people's minds which, whilst like every good story has roots in reality, does nothing much to illuminate the mechanics of the dark web.

According to Statista only an average of 12% of people have ever accessed the dark web. Among security professionals this number is higher but still numbers only 1 in 7 according to this study.

This lack of direct experience goes some way in explaining why there is so much fear and misunderstanding. It also suggests that many security professionals are missing out on a crucial source of highly-relevant information. A source of information which could help them protect their organization and gain a better understanding of the individuals behind the attacks in their company.



Only 12% of people have ever accessed the dark web*

Signal has been specifically developed for security teams to overcome the issues around dark web monitoring (which we explore further in this documents).

***Source:** Statista - Dark Web Access

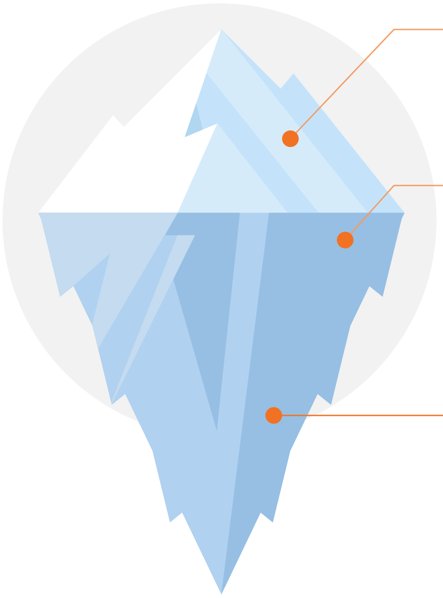
“Monitor hacker behavior and detect early warning signs of malicious activity.”

Customers around the world use our products to monitor hacker behavior and detect early warning signs of malicious activity which could evolve into a tangible threat. This forewarning helps them avoid costly physical and cyber attacks.

In this document, we use our knowledge to help break apart fact from fiction when it comes to the dark web, as well as outline how security professionals can efficiently leverage data from this ever expanding intelligence resource to better protect their organization.

About the Dark Web

When people describe the dark web they commonly use imagery of an iceberg outlining how the web is divided into three categories:



The surface web where all commonly accessible content is stored. This is the internet that is indexed by the likes of Google.

Then, just below the water is the deep web. This is where the majority of content is stored on unindexed pages. For example, Netflix content which is locked behind a paywall, or Dropbox where the content is locked behind a user login.

Finally, even deeper in the water, somewhere beyond where the light can penetrate is the dark web. This is where web content that is only accessible using particular technology such as a Tor browser is stored.

The dark web is infamous as being a hub of nefarious activity. But there’s nothing inherently evil or illegal about it. The dark web simply refers to a method of accessing and hosting web content which gives the user complete anonymity. This is done through the use of special software such as Tor (The Onion Router) I2P (Invisible internet Project).

My name is Lee Campbell & I'm a multi-disciplinary UX & UI Designer.
PROJECT A

Just like any other part of the internet the dark web can be and frequently is used for legitimate purposes. For example, journalists in countries operating under oppressive regimes might take to the dark web to express their right to political free speech without suffering consequences. However, like any other communications platform, the dark web can be accessed and used for less legitimate activity, such as selling drugs, guns, or stolen credit card data.

```
room_name_full FROM tbl_room WHERE room_checked='0'"
$uncheckedRoom["room_name_full"]."' class='list-gro
tbl_disposition.disposition_user = u.user_ID
```

Tor was in fact, developed in 2002 by the US Naval Research Laboratory as an anonymous communications tool for intelligence agencies and has since become the go to tool for both criminals, privacy researchers, academics, and law enforcement alike. The network is now maintained by the Tor Project, a non-profit organization based in Massachusetts. While funding is provided by a number of foundations, corporations, and individuals, the vast majority of the Tor Project's funding continues to come from the US Government.

"In the dark web, hosters don't want to be indexed."

Any website whose content has been intentionally hidden using a Tor type software is part of the "dark web". However, the very name of the dark web is slightly misleading. It suggests a web network existing, but the dark web is incredibly fragmented. The surface web is full of websites people and businesses are trying to get people to visit their site. Building backlinks is a vital part of building website authority in search engines like Google and as such building further links and interconnectivity is entirely necessary if a business wants to succeed. But in the dark web, hosters don't want to be indexed. They don't want to be found by the wrong people. It looks far less like a web, and more like independent repositories of content which very rarely, if ever, link to each other.

There are a number of technologies you can use to access the dark web including I2P and Freenet which are growing in popularity. Tor though, still represents the largest network with roughly 36 million users worldwide. It is worth noting though that only about 3.4% of their traffic is accessing hidden services.

A Brief Intro into How the Tor Browser Works

We aren't going to go into great detail explaining how a Tor browser works, but essentially the Tor browser provides anonymity to both host and users to explore the dark web by randomly routing user's encrypted traffic through a series of volunteer servers across the world. These volunteer systems are called relays, and ensure activity cannot be traced back to the end user. Tor users can then access special sites with .onion domains, which can only be accessed through Tor browsers.

The Tor network is supported by some 7,000 volunteer systems across the globe. These systems serve as relays, by which data on the network is pinged across in order to scramble and obfuscate the origin of traffic on the network.

Various Threats Encountered by Signal Users on the Dark Web2

Types of Malware and Exploit Kits

Postings requesting or selling information around newly discovered or created exploits or malware which is aimed at a specific company. Signal can alert users when this information is for sale on the dark web. The security team can then preemptively patch the potential vulnerability.

Credit Card Details

Stolen card credentials are big business. There are millions of accounts for sale on the dark web with some vendors even offering money back guarantees for those accounts which have been deactivated.

Having this information is especially valuable for banks as it allows them to better protect their customers from identity theft and fraud. The items for sale online could range from login credentials to a customers online banking account, card number date and csv, or full on clone cards with pin.

In 2018 hackers stole over half a billion personal records*

***Source:** Statista - Dark Web Access

Sensitive Information or Documents

In the wake of a data breach potentially sensitive documents relating to a company have been found online. The purpose of these documents for sale could be used in a variety of scams such as blackmailing employees, executing advanced phishing scams, or used in another way tp gain further access to sensitive information.

When this happens it could also represent a reputational threat to an organisation or, depending on the documents that are stolen, affect future cash flow.

Scam Tools

Scam tools are packages created by hackers and phishing experts that can be used to run phishing or other campaigns. These tools take on a variety of shapes, sizes, looks and feels. For example, a user of Signal found a convincing replication of their site online, however, the login button led to a data capture form that would have stolen the login credentials of their customers.

After quickly identifying this using Signal they were able to get the site removed, effectively removing the risk. However, they still need to constantly monitor the web for new threats and it’s always more effective to discover these scam tools before they go live.

Tutorials

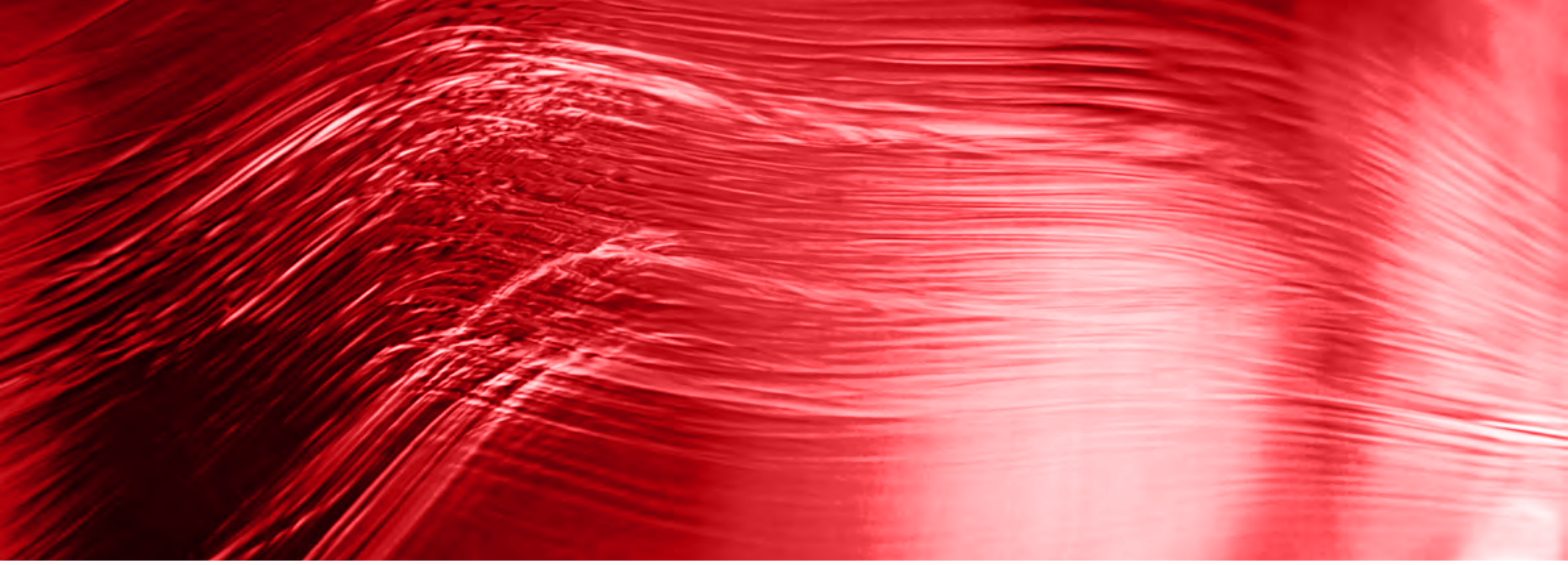
Educative materials may not be the top of everyone’s most threatening materials for sale on the dark web. But these tutorials are big business on the dark web. These how-to guides on the dark web can provide security professionals insight into the processes and techniques that both amateur and professional hackers are currently using.

Insider Threat for Hire

A growing risk for enterprises posts from employees or partners offering to sell access or to steal information is becoming increasingly common. Seeing these posts can alert you to the presence of a malicious insider and pinpoint where in the organization they may sit. Effective monitoring of the dark web can enable you to identify attacks before they happen, track down insider threats, and know when your information or the information of key suppliers or partners has been compromised.

Credentials for Sale

Credential stuffing is a tactic growing in popularity that weaponises non-sensitive stolen credentials (eg. usernames and passwords) against websites and mobile applications. It takes advantage of the fact that many users use the same username and password across multiple sites.Large volumes of stolen account logins are tested against other website login pages to gain unauthorised access to accounts, in order to commit fraud.
By identifying stolen credentials for sale on the dark web you can mitigate the potential threat by informing your users that their login details of the data breach and encouraging them to take precautionary measures.



Physical Threats and Terrorist Attack

The big draw for criminals to the dark web is that all users need to use an encrypted browser to access the dark web which entirely anonymises their presence. This means, very simply, that criminals can and do talk about their activity, either to brag or as part of their preparations.

The dark web is also a place where terrorists go to communicate and organise. By monitoring the dark web then you can pick up on their conversation and use the data gathered to potentially predict and deter terrorist attacks aimed at the company.

Using software like Signal you can constantly monitor the dark web and when a criminal talks about or potentially threatens one of your staff or assets you can know instantly. Whilst they are anonymised and you won't know who is planning something, you will know that there is a very real potential threat that you can now guard against.

Impersonation

By impersonating an individual online, such as a doctor individuals can push through the sale of illegal goods. For example, the WHO estimates that 50% of the drugs for sale on the internet are fake. By impersonating a doctor - potentially using a details stolen from an attack on a medical institute - the criminal can take advantage of high medication prices and offer discounted fake versions masquerading as the real thing.

Establishing the capability to identify each of these threats as they emerge on the dark web with a tool like Signal will ensure your organisation stays ahead of threats.

There is a hacker attack approximately every 39 seconds*

***Source:** Statista - Dark Web Access

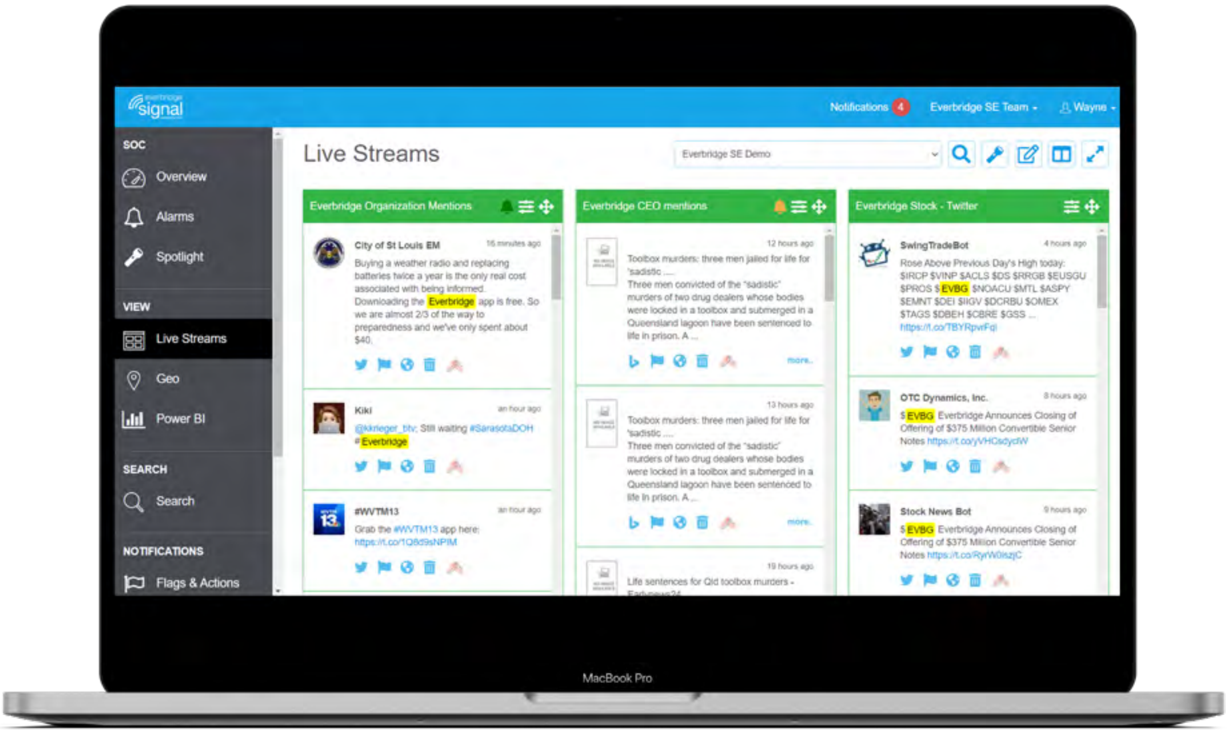
Signal, LERTR and the Dark Web

Signal and the Dark Web

Examples of activities that have been identified from dark web content using Signal.

Threat Intelligence software include;

- Online markets selling stolen and fake goods;
- Hackers selling non-sensitive data for use in credential stuffing attempts;
- Impersonation of individuals or organizations;
- Details in regard to hacking or incitement to hack;
- Reputational risk via fake news and impersonation;
- Illegal activities such as drugs and drug paraphernalia;
- Information regarding a previously undetected sensitive data breach;
- Data breaches and information leaks Counterfeit gift cards;
- Stolen customer credit card information is discovered online.



Live Streams

Everbridge Organization Mentions

City of St Louis EM 16 minutes ago
Buying a weather radio and replacing batteries twice a year is the only real cost associated with being informed. Downloading the Everbridge app is free. So we are almost 2/3 of the way to preparedness and we've only spent about $40.

Kiki an hour ago
@kkrieger_btv: Still waiting #SarasotaDOH #Everbridge

#WVTM13 an hour ago
Grab the #WVTM13 app here: https://t.co/1Q8d9sNPIM

Everbridge CEO mentions

12 hours ago
Toolbox murders: three men jailed for life for 'sadistic ....
Three men convicted of the "sadistic" murders of two drug dealers whose bodies were locked in a toolbox and submerged in a Queensland lagoon have been sentenced to life in prison. A ...

13 hours ago
Toolbox murders: three men jailed for life for 'sadistic ....
Three men convicted of the "sadistic" murders of two drug dealers whose bodies were locked in a toolbox and submerged in a Queensland lagoon have been sentenced to life in prison. A ...

19 hours ago
Life sentences for Qld toolbox murders - Earlynews24

Everbridge Stock - Twitter

SwingTradeBot 4 hours ago
Rose Above Previous Day's High today: $IRCP $VINP $ACLS $DS $RRGB $EUSGU $PROS $EVBG $NOACU $MTL $ASPY $EMNT $DEI $IIGV $DCRBU $OMEX $TAGS $DBEH $CBRE $GSS ... https://t.co/TBYRpvrFqi

OTC Dynamics, Inc. 8 hours ago
$EVBG Everbridge Announces Closing of Offering of $375 Million Convertible Senior Notes https://t.co/yVHCsdycIW

Stock News Bot 9 hours ago
$EVBG Everbridge Announces Closing of Offering of $375 Million Convertible Senior Notes https://t.co/RyrW0iszjC

3 Uses for Signal for Monitoring the Dark Web

1. Detecting Data Breaches

Our software has been used to identify stolen credentials and other personal information that is circulating on dark web networks and other channels.

To identify relevant data you are able to set up specific search queries within the software. These constantly monitor the open, dark and deep web and then filter these searches using our AI technology to determine what is and isn't relevant.

We then add a human touch to the remaining data to further filter using human intelligence to identify what is highly relevant.

The scan infiltrates private sites - many of which require membership within the cybercriminal community to enter.

When it comes to detecting data beaches it can quickly identify chat around data that is circulating online which has been gained by illegal hacking attempts. If data is detected from a particular company, whilst there is no way to retrieve that data organisations can take precautionary measures to mitigate the damage and threat of the data breach as well as determining how the data was gained and ensuring that breach is secured against further data beach attempts.

54% of companies have experienced one or more attacks in the last 12 months.*

2. Detecting Physical Threats Against People and Assets

The big draw for criminals to the dark web is that all users need to use an encrypted browser to access the dark web which entirely anonymises their presence. This means, very simply, that criminals can and do talk about their activity, either to brag or as part of their preparations.

Using software like Signal you can constantly monitor the dark web and when a criminal talks about or potentially threatens one of your staff or assets you can know instantly. Whilst they are anonymised and you won't know who is planning something, you will know that there is a very real potential threat that you can now guard against.

3. Predicting Potential Terrorist Actions

In the same vein as detecting potential physical threats against a company online, the dark web is also a place where terrorists go to communicate and organise. By monitoring the dark web then you can pick up on their conversation and use the data gathered to potentially predict and deter terrorist attacks aimed at the company.

*__Source:__ Statista - Dark Web Access

How Does Signal Monitor the Dark Web

During dark web scanning our security software monitors and detects any data that is relevant to the particular search queries that have been set up. This allows you to create a customised highly relevant stream of data and information around key points of interest for your company.

The information can also be run through a sentiment filter to create an even further refined stream of data, we explore this in further detail below.

Data sources include all major dart web forums. We maintain a third party integration with a specialist dark web monitoring team to maintain our access.

Signal provides a single point of access to the hidden internet by gathering data from hundreds of sources. Your team will save time on investigations and remain safe and secure. Signal protects your team by parsing data, removing image content, and showing you only what you've searched for. Comprising about 90% of the internet, deep web content is not discoverable by search engines.

Features of Everbridge Signal

An all-in-one OSINT tool. Monitor the Surface, deep, and dark web and stay one step ahead of potential threats.

- Deep and Dark Web
- Message Boards
- Pro-active Alerting
- Pastebin / Bin Sites
- Emotional Analysis
- Multi-language and Translation
- API Integration Capabilities
- Unlimited Users
- Single Sign-in
- Marketplaces: discussion forums and messaging apps
- Entity Extraction
- Flagging and workflow

Get in contact to book a Live Product Demo or just to learn more

info@everbridgesignal.com