Revealing the Dark Web: How to Leverage Technologies to Alert and Block Dark Web Access

Veriato

www.veriato.com

The Threat of the Dark Web

The Dark Web represents the seediest place possible on the Internet today – the modern-day "black market" where the exchange of ideas, illegal goods and services, and any evil most of us haven't considered takes place. It also contains the 99% of the Internet inaccessible to search engines. While it's possible that some visitors are simply curious, the majority of this underworld community are up to some degree of no good.

With few exceptions, there is no reason for an employee from your organization to be visiting – let alone utilizing – the Dark Web. So, the combination of the two should raise a red flag for anyone concerned about organizational security.

In this paper, we'll provide an overview of what is the Dark Web, discuss why employee use of the Dark Web can mean trouble, and how to utilize current security technologies to detect and block the use of the Dark Web.

Dark Web 101

We all tend to think about the Internet as the sites you interact with every day made up of countless servers throughout the world hosting applications, portals, and data. But the web is actually divided conceptually into three parts.

There's More to the Web Than you Think

The web you're on every day – the one that includes search engines and their website listings – is considered the Surface Web. This is the web every one of us can see, search through, and access. The next layer of the web is called the Deep Web – think of this as the sites and systems that are accessible to the Internet but aren't on any search engine. For example, if an organization has an application exposed to the Internet by IP address only for use by another organization, that application is on the Deep Web. The last – and most criminal – part is the Dark Web. This is where the world's most immoral, evil, and sinister content and purveyors reside. It's relatively hidden from the world and does take a bit more work to reach than just "making a wrong turn" down a dark alley.

Getting on the Dark Web

Access to the Dark Web requires a special browser, called a TOR (The Onion Router) browser. Essentially a modified Firefox browser available for Windows, Mac, and Android, the TOR browser provides secure communications with a private set of systems using a .onion domain. These sites are only accessible from a TOR browser, with no registration within traditional DNS. There have been browser extensions in previous years that turn a standard browser into a TOR browser, but the predominant method is to use a standard TOR browser. Because anonymity is imperative when visiting the Dark Web, many users augment obscuring any remnants of identifiable details about them by first using a VPN, although it's not required.

Is it Illegal to Get on the Dark Web?

The simple answer is No. BUT... unfortunately, it's not that simple. In the United States, in a landmark Supreme Court ruling, the FBI was allowed to search and seize any computer around the world, found to be using privacy tools like VPN or Tor. Now, that doesn't mean if you use either of these tools that you're in for a visit from men wearing sunglasses in dark-colored SUVs. But, it does mean that, if you're suspected of doing something illegal, they aren't going to need to ask for your permissions to hack your machine.

Since we're not lawyers, please seek your own legal counsel before deciding to access the Dark Web.

What's on the Dark Web?

This is the place on the web where anything and everything illegal lives. Commodities such as counterfeit money, drugs, and weapons are readily available. Services like hacking for hire are a commonplace. And if you're new to the Dark Web, there are even wiki sites to help educate you on finding your way around. In general, think of anything illegal someone could want to purchase or learn about, and the Dark Web is where you'll find it. From an IT perspective, cybercrime-as-a-service is alive and well on the Dark Web. Malware, credentials, confidential data, email lists, and services ranging from custom hacking, to malware creation, to laundering funds. It's the place one would turn to if they wanted to obtain an illegal product or service.

Employees and the Dark Web

So, does the Dark Web pose a risk to your organization?

In essence, the Dark Web becomes a medium by which employees-turned-insiders now have easier direct access to bad guys. Think of a scenario where a disgruntled employee decides they want to make money off the company by selling its customer list, corporate secrets, or intellectual property. But, how many of us know someone off the top of our head who would buy such information (or know where to find someone like this)? The Dark Web is literally the place for criminal minds to communicate and transact with one another.

There are a number of ways employees can leverage the Dark Web for malicious purposes:

- **Solicitation** – Finding "job post" listings on forum sites is not uncommon. Cybercriminals silo their activity to the parts of an attack they know well, leaving additional tasks to another member of the team. Employees that can play an inside role – and be monetized for their efforts – is already a reality on the Dark Web.
- **Data** – You can buy just about anything on the Dark Web. And that includes data. Employees with access to data need to do little more than offer it up and see if there are any takers.
- **Credentials** – These are the key to lateral movement in attacks, used in 60% of all attacks[1] . With credentials representing 59% of all data sold on the Dark Web[2] , the sale of access to your organization is a very real potential threat.
- **Exfiltration** – The Dark Web can also be used as a conduit to exfiltrate data. Sites within the Dark Web can be the destination, as well as the Dark Web can merely be used as a conduit to pass data to another point on the Internet, anonymizing the path taken, making it tougher for an employee to be identified.

Beyond the risk of employees-turned-insiders, there is always the risk the employee is exposing one of your endpoints to malware, remote access trojans, etc. The folks on the Dark Web aren't there to be friends; they're there to make money.

So, what can you do to detect employee interaction with the Dark Web?

Detecting Employee Dark Web Activity

The good news is there are some telltale signs when employees interact with the Dark Web. It should be mentioned, to truly be effective, nearly all of the following detection methods below involve having some kind of Employee Monitoring Software solution in place analyzing user, application, and OS actions on the endpoint.

Some of the clear indicators of employees on the Dark Web include:

- **Use of the TOR browser** – Remember, this is basically an instance of Firefox, so if the organization hasn't standardized on that browser, spotting its use should be relatively easy. Monitoring solutions that can watch for the Firefox process or capture application window titles are perfect to help identify when a user is launching the TOR browser.

- **Site names** – Because Firefox has legitimate purpose within an organization, focusing on the browser may not be useful. All Dark Web sites use a .onion top-level domain. Monitoring solutions that can capture URLs or window titles can be used to identify when Dark Web sites are being visited.

- **Network Traffic** – Traffic between the endpoint and the Dark Web site is encrypted, so you'll need an SSL proxy in place to see any of this traffic. For those organizations without an SSL proxy, abnormal IP addresses is about the extent of your ability to spot Dark Web activity.

- **Presence of VPN** – While not required to access the Dark Web, to add a layer of anonymity, many Dark Web users leverage a VPN prior to accessing. Detection by using either the presence of the VPN application process or by using the contents of the VPN application's title window, you can at least detect that a user – that shouldn't normally be using a VPN to for their job – is utilizing one.

Beyond Dark Web Activity: Using Leading Threat Indicators

If an employee has decided to exchange their loyalty to the organization for malicious activity that benefits them personally, there are additional leading indicators you can use. With a User Behavior Analytics solution in place, shifts in behavior and communications can be used to proactively identify that an employee is no longer happy, is potentially seeking a new job, or simply has strong negative sentiment towards the organization – all leading indicators of a potential threat.

---

[1] *Carbon Black, Global Threat Report (2019)*

[2] *Positive Technologies, Criminal Cyberservices Report (2018)*

Blocking the Dark Web

Rather than detecting, many organizations would choose to block dark web access entirely. While not a perfect science, there are ways you can achieve some success in keeping employees off the Dark Web.

- **Block use of the TOR browser** – As previously mentioned, if Firefox isn't a standard browser, this is easy to define. The challenge lies in whether you have an enforceable means of application white/black listing. Group policy has some basic functionality for Windows (but is easily thwarted by renaming executables). To truly block this, you'll need some kind of endpoint security in place.

- **Block Network Traffic to .onion sites** – The Tor network is designed for anonymity, so getting a list of IP addresses is difficult to impossible. And most traffic runs over an SSL connection (as with normal web traffic) making it even more difficult. The only reasonable way is using deep packet inspection (DPI) to look for unusual SSL certificates.

- **Presence of VPN** – The only means to stop the use of a VPN is to block it from ever running. That means, like the blocking of the TOR browser, creating a white/blacklist of applications that exclude VPN applications – as well as limiting user's ability to install software such as a VPN.

Do keep in mind that even if all of these blocking measures were in place and effective in keeping employees from accessing the Dark Web while at work, there's nothing stopping your employee from visiting the Dark Web at home from their personal computer. This brings organizations back to the need for UBA as part of their security strategy to identify leading indicators of a potential threatening employee – one where the use of the Dark Web is just one more indicator, rather than the final threat activity.

Addressing the Threat of Employees and the Dark Web

The Dark Web elevates employees-turned-insiders into a potentially legitimate threat. Employees wishing to turn company access or data into money suddenly have a marketplace in which to do so both profitably and anonymously. Simply put, the Dark Web enables threatening behavior by giving it a means to benefit the employee.

Employees (other than perhaps security staff who are threat hunting, doing diligence, or are looking for breached data) have zero business visiting the Dark Web. So, the very act of attempting to (or succeeding in obtaining) access to the Dark Web should raise suspicion and be considered at very least a leading indicator of insider threat.

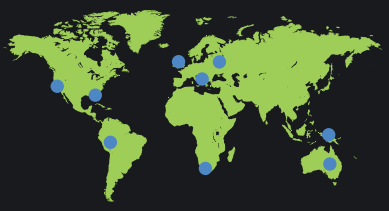
Depending on your security strategy, you can either choose to detect actions that indicate Dark Web intent or activity, or to block and disable a user's ability to access and leverage the Dark Web. Both detection and blocking require focusing on some very specific applications, actions, and activity, and require the use of third-party solutions.

But remember, employees don't need their work computer to access the Dark Web; they only need to access that which they will monetize – credentials, endpoint access, and data. Those do require the use of a work computer, giving you the ability to monitor for changes in employee sentiment and activity using UBA and UAM solutions.

The Dark Web isn't a place for employees. By combining your security efforts around watching for both specific Dark Web activity and leading indicators, organizations can more accurately and proactively identify potential threats before the actual threatening action – such as the exfiltration of sensitive data – takes place.

To learn more about how Veriato can help you, contact our product specialists today.
1-888-598-2788

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions



Our solutions are deployed in **110+ countries**

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom

https://plus.google.com/+Spectorsoft
https://www.linkedin.com/company/veriato
https://twitter.com/veriato
https://www.youtube.com/SpectorSoft
https://www.facebook.com/VeriatoInc/