YOUR BUSINESS DATA MAY BE OUT THERE AND YOU DON'T EVEN KNOW IT:

A SIMPLE GUIDE TO THE DARK WEB

Why the continued rise of the dark web is a threat to corporate data and why businesses need to take action.

The dark web is a nefarious place, where criminals lurk and communicate, buy, sell, plot and plunder. The clue, of course, is in the name. Speaking to NBC[1] in July 2018, FBI Supervisory Special Agent Mark Knoll referred to it as "like your new drug dealer on the corner in the virtual world". The UK Home Secretary Amber Rudd[2] went further, saying it's a place where "anonymity emboldens people to break the law in the most horrifying of ways with platforms that enable dangerous crimes and appalling abuse".

Highlighting the broader impact of the dark web is important because much of the publicity surrounding it in recent years has been related to drug trafficking. The Silk Road marketplace was perhaps one of the best known sites for this, at least until it was closed down in 2013, after the capture[3] and imprisonment of its founder Ross Ulbricht.

Its relevance to fuelling other crimes cannot be understated, but it is perhaps in cybercrime where the dark web truly thrives. As a recent CNBC article suggested,[4] the building blocks for ID theft are on the dark web. Selling personal information to fraudsters is, anecdotally at least, booming, which is not surprising given the cybercrime statistics. ▶

What is the dark web?

The dark web is an encrypted part of the internet that uses non-standard communication protocols and ports to help hide digital identities. It features forums and marketplaces (often referred to as darknets), where products and services are bought and sold. Individuals can enlist the services of a "hacker for hire", buy the leaked contents of the latest data breach, purchase credit cards from any country, drugs, weapons, counterfeit goods and so on. Anyone can visit these pages via technologies like TOR (The Onion Router) and i2p (Invisible Internet Project). Information, products or services can be requested and paid for in Bitcoin or other digital currencies.

DATA THEFT:

How does the dark web heighten the situation?

Corporate data breaches are becoming a regular occurrence. Facebook, TicketFly and Cathay Pacific Airlines were just some of the many organizations that suffered data breaches during 2018 and this comes at a cost.

A 2018 study by the Ponemon Institute – the 13th Annual Cost of Data Breach study[5] – found that the global average cost of a data breach is up 6.4 percent over the previous year to $3.86 million. The average cost for each lost or stolen record containing sensitive and confidential information also increased by 4.8 percent year over year to $148. Given that the majority of breaches tend to run into the millions of records, it's easy to see how costs can dramatically escalate.

While the financial cost to businesses is clear, there are other costs to consider such as reputational damage, customer confidence and staff morale. The effects of a breach can impact across an entire operation and for publicly listed businesses, this can also mean taking a hit on the share price.

Clearly this is a growing problem but it is also worrying that it is not isolated to static networks. A 2017 study by IntSights[6] [PDF] found a 30-fold increase in mobile dark web activity since 2016, with the likes of Discord, Telegram, and WhatsApp being used to "trade stolen credit cards, account credentials, malware, drugs and to share hacking methods and ideas". ▶

$3.86 MN

global average cost of a data breach[5]

$148

average cost for each lost or stolen record containing sensitive information[5]

"It's not an understatement to suggest dark clouds are looming over businesses. Information is the new currency, and as long as the trading of personal information on the dark web remains relatively painless for criminals, we should expect to see increased attacks, and the resulting theft of corporate data. Sadly, it's supply and demand."

Vali Ali *HP Fellow and Chief Technologist of Security and Privacy for Business*

This can make gleaning information from the dark web especially difficult and it's only going to get harder. In 2018, the increasingly popular Tor browser tightened its privacy by hiding the .onion address that identifies dark websites and generating cryptographic keys instead. In essence, it will be almost impossible to stumble across or guess a specific darknet site address and even more difficult to determine the actual owner of that site.

For law enforcement this represents an on-going challenge. Although we occasionally hear of success stories – US agents arrested[7] 35 dark web weapons and drugs dealers in June this year – the goal posts are constantly shifting. For businesses it is a constant headache. Keeping up with the pace of change and identifying often stealthy breaches is a problem. According to FireEye[8] the average time to discover a breach in systems is now 57.5 days, but as soon as criminals have exfiltrated data they are likely to attempt to sell it online.

Typically, hackers will look to package personal data. They will search the stolen data files for authentication material – names, addresses, phone numbers and even credit card details – and offer them up for sale in bulk to scammers and other hackers. It's all done very quickly, which means from a criminal's point of view; the data is sold before the company even knows it is missing. ▶

57.5 days
the average time to discover a breach in systems[8]

MITIGATING RISK:

What can companies do about the problem?

Understanding what needs to be protected is a crucial first step. Only then can organizations put in place effective security tools and policies. All organizations should build a threat model and keep that model up to date, as assets and threats change.

With a threat model in place, the best way to really mitigate against the threat of the dark web is to understand and monitor it. Organizations can also try simple tactics such as setting up fake accounts within legitimate datasets. These can act as a decoy and help organizations find breached material.

There is a new wave of companies – like Webhose, RepKnight, Terbium labs, Massive, Recorded Future, Sixgill, Hold Security, and AlienVault – which are trying to make the dark web as easily searchable as the normal internet. This should enable organizations to at least try and monitor breach activity.

Organizations such as the FBI also release regular communications[9] about threats. Understanding active threats and historical patterns can also help businesses determine likely threats to their systems from criminal activity. ▶

How to create a threat model

- **Identify assets** – this includes hardware, business processes, IP, mobile devices, ERP systems, databases and even end of life systems.
- **Create security profiles for each asset, identifying what is actually protecting each asset from cyberattack** – this should enable the organization to identify potential vulnerabilities. This includes looking at layers of security, for endpoints, software and then networks.
- **Identify the potential threats and prioritize** – where is the threat coming from? Opportunistic hacker, hacktivists, cyber criminal gangs, internal disgruntled employee, internal error, untrained or unauthorised freelance worker, physical loss of devices.
- **Match risks with potential action** – apply appropriate tactics and procedures to each asset based on potential severity.

CLEAR ACTIONS:

What should companies look for on the dark web?

With access to the dark web, it is still not easy to find what you are looking for, as you have to try specific forums to see what is being bought and sold. It's a bit like looking for a stolen radio in a flea market, difficult but not impossible.

It's important to remember this is also a moveable feast of information. Nothing remains static and for this reason alone, countering threats will for the foreseeable future demand an intelligent mix of machine learning analytical technology and human vigilance. This is why cybersecurity skills are in short supply. [10] The demand is such that there are not enough to go around, so businesses need to be clever, to partner with expert groups and ensure suppliers adhere to their own security policies.

Checklist of what companies should look for

- Any data related to their organization or partners and suppliers, such as bank information.
- Internal data such as usernames, emails, company-related documents or personally identifiable information of employees or customers.
- Exploit kits, malware, and other potential threats that aren't specifically targeting your organization but could pose a threat in the future.

The key challenge for organizations is consistency. Criminals only need one opportunity to break through defenses, so ensuring any potential vulnerabilities are shored-up is essential and demands a solid technology solution – coupled with best-in-class business processes – to mitigate risk. The stakes are too high for businesses to bury their heads in the sand. Ongoing alertness is imperative to stop critical business data appearing on the hidden underground forums of the dark web. ■

How DaaS can help

Building security into systems is a must. This means sophisticated technologies that are baked into the very fabric of hardware and applications, to rebuff any potential threats. It also requires ensuring devices are always up to date – which is where a centrally managed Device as a Service (DaaS) model can help.

HP DaaS provides a one-stop solution that combines hardware and lifecycle services to make your company more efficient, improve the employee experience, and free up IT resources. The transformative nature of this service model brings with it increased and centralized security on the latest hardware – in fact the security stack built into HP hardware substantially improves manageability and security.

This means regulations change or threats increase, so devices can be easily switched out to meet requirements. And by helping to manage volatility and fast-changing business needs, HP also enables analytics-based prediction of security and hardware needs.

In this sense, HP DaaS [11] helps to proactively protect businesses from attacks to their data by monitoring every device and how it adheres to security policies, data access, and approved apps. It also allows for analytical perspective on inventory, device location and condition, as well as end-of-life disposal to prevent physical security breaches.

Sources

1. NBC, FBI: Dark web is like a 'drug dealer on the corner in the virtual world, July 2018
2. Gov.UK, Law enforcement crackdown on dark web: Home Secretary speech, April 2018
3. CNN, How FBI caught Ross Ulbricht, alleged creator of criminal marketplace Silk Road, October 2013
4. CNBC, The dark web is a fraudster's bargain-hunting paradise, July 2018
5. IBM Cost of a Data Breach Study, July 2018
6. Intsights, Messaging Applications:The New Dark Web, October 2017
7. Silicon Republic, US agents arrest 35 dark-web drugs and weapons dealers, June 2018
8. Fire Eye, M-Trends 2018, April 2018
9. Public Service Announcement, Booter and stresser services increase the scale and frequency of distributed denial of service attacks, October 17, 2017
10. CSO, Research suggests cybersecurity skills shortage is getting worse, January 2018
11. HP, HP Device as a Service (DaaS), February 2018

HP DaaS plans and/or included components may vary by region or by Authorized HP DaaS Service Partner. Please contact your local HP Representative or Authorized DaaS Partner for specific details in your location. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

4aa7-3694enw, February 2019