Safeguard your business against Dark Web scams during the Pandemic

Bad Actors and Hackers are taking advantage of turbulent times, creating pressure on IT organizations to step out of their comfort zone and budgets, to review their security posture, and apply multiple layers of cyber protection to their business. These Hackers live on the Dark Web, praying on vulnerabilities and creating mayhem for businesses that can potentially cause catastrophic outcomes. With attacks on the rise, the number of Bad Actors on the Dark Web has increased, this shift has pushed Bitcoin prices to rise, and companies to fear more about how to respond to an attack.

What is the Dark Web and why can it be dangerous to organizations?

The Dark Web is a hidden layer of the internet that is not accessible to search engines, and that requires specific software for access. The Dark Web is where stolen information, such as bank account numbers and SSNs, are sold. Through the Dark Web, private computer networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location.

Accessing the Dark Web requires using Tor, (The Onion Browser) an anonymous browser. Unlike other web browsers, like Chrome or Firefox, which take the most direct route from your computer to the web, the Tor browser makes use of a random path of encrypted servers to connect to the web without the risk of being tracked.

PreciseSecuirty research has determined over **30% of North Americans use The Dark Web regularly.** More than 2 million people use the Tor network each day to anonymously make connections online. Surprisingly, over 98% of Tor traffic is directed towards public websites, rather than hidden sites that can only be reached by the Tor network. Since Tor can mask a user's real identity online, including their location, they are often used for malicious actions online.

Bitcoin Dark Web Activity Increasing

Bitcoin is basically a computer file which is stored in a 'digital wallet' app on a smartphone or computer. People can send Bitcoins (or part of one) to your digital wallet, and you can send Bitcoins to other people. Every single transaction is recorded in a public list called the blockchain. A study from Crystal Blockchain Analytics on May 19, shows **that the total USD value of Bitcoins transferred on the dark web rose by 65% in Q1 2020, during the same period in 2019.**

A recent report published by a bitcoin tech company, Bitfury has revealed the startling volume of trade now taking place on the dark web. The report found that the **total value of bitcoin transacted increased by 65 per cent over the course of the last year,** and by a staggering 340 per cent since 2017.

Scams on the Rise During Pandemic

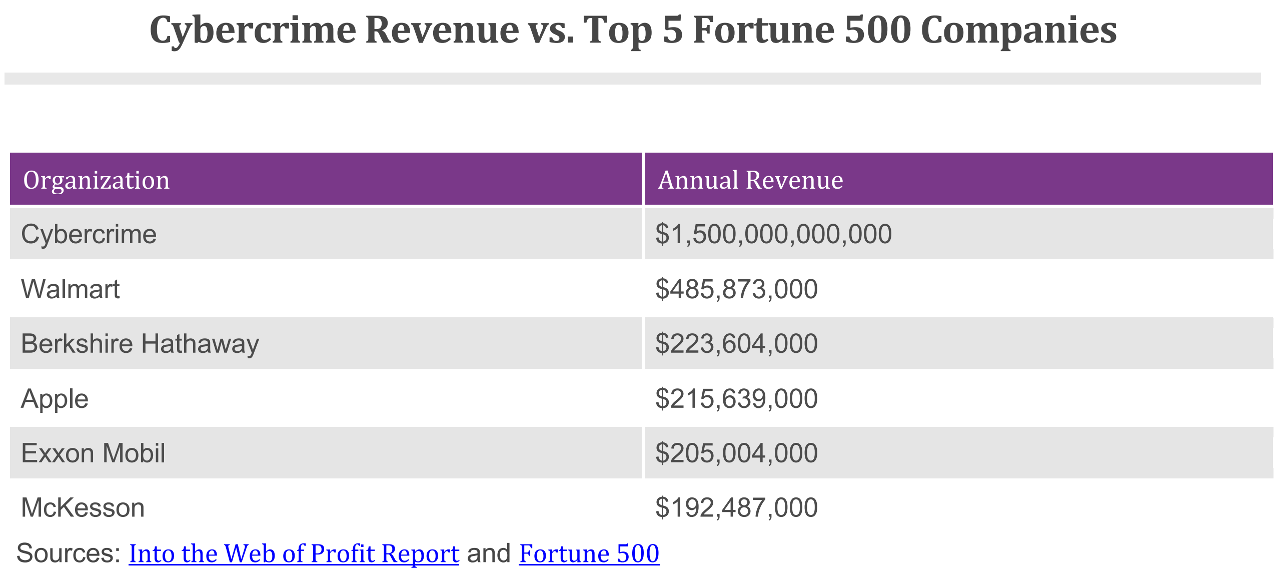
Now, instead of just preying on virus-related fears, cybercriminals are targeting stimulus payouts. A total of 4,305 domains related to new stimulus or relief packages have been registered since January, Check Point Researcher's report. This includes 2,081 new domains registered in March; of these, 38 were malicious and 583 were suspicious. **In the first week of April, 473 new domains were registered; of these, 18 were malicious and 73 were suspicious.** Researchers saw a big spike in registrations starting March 16, when the government proposed the stimulus package.

Additionally, recent security surveys suggest most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. Let's look at some of the most interesting findings:

1. 95% of cybersecurity breaches are caused by human error. (Cybint)
2. 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
3. On average, only 5% of companies' folders are properly protected. (Varonis)
4. Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
5. 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)

To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention and security best practices a part of their culture.

If cybercrime is a business, then this business is AMAZING! Ransomware attacks, data breaches, theft of intellectual property, sales of counterfeit goods and other illicit activities are generating at least $1.5 trillion in annual revenue, according to a new academic study, Into The Web of Profit.



Cybercrime Revenue vs. Top 5 Fortune 500 Companies

Organization	Annual Revenue
Cybercrime	$1,500,000,000,000
Walmart	$485,873,000
Berkshire Hathaway	$223,604,000
Apple	$215,639,000
Exxon Mobil	$205,004,000
McKesson	$192,487,000

Sources: Into the Web of Profit Report and Fortune 500

How can you safeguard your business against Cyber attacks? Here are nine tips:

1. NEVER pay the ransom: These people are criminals and typically won't unencrypt the data.
2. Implement a good cloud backup solution: Restoring data from your last clean backup, could be the fastest and cheapest way to get your data back.
3. Do NOT provide personal information in an email, unknown call, text, etc.
4. Provide your employees with Security Awareness training programs to educate them on what a phishing email look and feel like.
5. Use a reputable antivirus and firewall solution.
6. Be sure to use content scanning and filtering on your mail server.
7. Make sure patching is up to date on all systems and software.
8. Use a secure tunnel (VPN), if you will be on a public Internet.
9. Employ a Managed Service Provider to manage your IT infrastructure.

Not sure if your company is protected from these increasing threats? TechWerxe can help you evaluate your cybersecurity protocols. Email Jodi Madsen at jmadsen@techwerxe.com or call 973-577-4556.