Cybercrime & The Dark Web: 3 Steps to Stay Vigilant

cyber security risk management

Summary: Dark web sites are only accessed with encrypted software to allow stolen financial information to be sold to cyberthieves anonymously. It is a lucrative operation as these illegal sites have been known to make over $1B. Three ways to help stem the tide of stolen financial data are using Open Source Intelligence tools to search the dark web, keeping updated on new threats, and working with law enforcement.

According to Cybersecurity Ventures, the cost due to global cybercrime is expected to reach $10.5T annually by 2025, growing 15% YoY. That is a staggering number. To help mitigate increasing security risks and data loss, community financial institutions (CFIs) must consider not only how they are being breached, but where stolen information could be funneled.

With the increase in “everything online” this past year, including shopping and banking, it is hardly surprising that organized cybercriminal syndicates and nation-states are scaling up both the pervasiveness and the professionalism of their tricks, including selling their information on the dark web.

After infiltrating bank systems and taking valuable financial and personal information, cybercriminals increasingly sell that information on the dark web. Dark web sites can only be accessed using encrypted software so that users can be anonymous, which is the reason cyberthieves like using them. These sites deal in the sale and trade of illegal wares alongside stolen information, such as bank account numbers, credit and debit card numbers, and sensitive personal data. The stolen data is then used to make fraudulent purchases or establish fake accounts.

Lucrative cybercrime operations. It is difficult to estimate how many of these dark web, illegal forums are currently in operation, given that many are run by shrewd cybercrime syndicates that are experienced at covering their tracks. However, experts estimate that there are hundreds of sites worldwide that specifically deal in financial or card information. Further, while nefarious operations like Silk Road have been shuttered by authorities rather quickly, many of the more successful dark web sites have been operating for years. (Case in point: Though it recently shuttered operations, Russian dark web forum, Joker’s Stash, had been active since 2014 and raking in more than $1B in revenue.)

Mainly stolen US credit and debit cards. Much of this ill-gotten revenue is from stolen credit and debit cards. These underground sites were estimated to be selling more than 23MM stolen credit and debit card numbers in early 2019, which was before the online surge last year during the pandemic. Not only that, but a disproportionate amount of those legitimate account numbers come from US bank customers — almost two-thirds of them.

While it may be difficult for CFIs to keep up with all of this, being informed and proactive plays an important part in helping to stem the tide of stolen financial data. In that vein, we give you three ways to do this.

1. Make sure that your **IT team uses Open Source Intelligence tools** (OSINT) to help them conduct automated dark web searches. By using automated tools that can alert them to potentially stolen data from your institution or your customers, IT security can efficiently uncover problems and take immediate action.
2. **Keep abreast of any new threats from** the FBI website as well as local law enforcement. This allows you to patch any potential cyber vulnerabilities or boost certain security measures before anything happens. These threats should also be communicated with executives, staff, and customers to make sure they are educated on the latest dangers.
3. **Coordinate with law enforcement,** if you uncover cybertheft so that they can take the appropriate measures on their end. They have technical teams specialized in this type of crime and can shut operations down.

The dark web is like a black hole for thievery. So, it is important to stay actively focused on cybercriminals and their tricks to mitigate the cyber risks and keep your data safe. As always, keep communicating with your employees and customers also. This way, you can remain a vigilant front against the nefarious activities of the dark web.

LOOKING TO GROW YOUR LOAN PORTFOLIO?

Financial institutions are looking for ways to boost their loan portfolio. Depending on your portfolio concentration, you may need C&I loans or choose a hedging solution to satisfy the long-term, fixed-rate needs of your customers. Check out our Lending Services to find the right solution for your institution.

ECONOMY & RATES

Rates As Of: 05/10/2021 10:59AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.02	0.01	-0.07
6M	0.04	0.01	-0.05
1Y	0.05	0.00	-0.06
2Y	0.16	-0.01	0.03
5Y	0.79	-0.06	0.43
10Y	1.62	-0.02	0.69
30Y	2.32	0.02	0.68
FF Market		**FF Disc**	**IORB**
0.06		0.25	0.10
SOFR		**Prime**	**OBFR**
0.01		3.25	0.05