TSX CYBR

MONTHLY COMMENTARY

Evolve Cyber Security Index Fund

CYBR invests primarily in equity securities of companies located domestically or internationally that are involved in the cyber security industry through hardware and software development.

As at November 29, 2019

ETF TICKER: CYBR (Hedged); CYBR.B (Unhedged); CYBR.U (USD)
MUTUAL FUND FUNDSERV CODE: EVF150 (Class F); EVF151 (Class A)

MACROECONOMIC HIGHLIGHTS:

The growing prevalence of cybercrime is leading companies and organizations to take greater measures to prevent its spread.

Europe has announced new fraud-prevention rules for online shopping which are set to re-write the playbook on e-commerce security. The rules aim to prevent fraud in the fastest growing segment of the consumer market, which has grown in sync with sales. As a result, the checkout process in Europe would require an additional layer of authentication for between 30-50% of e-commerce transactions, which will require two-factor authentication. This could rely on a password or PIN, possessing a card or phone, or a biometric, like a fingerprint. Although full mandatory implementation was set to begin in September 2019, the complexity of adoption has forced EU nations to push the date to the end of 2020.[i]

Major phone companies are also offering huge rewards to anyone who can hack their phones. Google announced that it will match Apple in how much it will pay for discovering a hack that allows for remote control of its smartphones.

Google will pay $1 million to anyone who can show off a unique attack on its Pixel 3 and 4 phones, as long as they allow for persistent access to the device. Anyone hoping to receive the reward will have to break Google's Titan M "secure element." Similar to Apple's iPhone Secure Element, Titan M is a security chip that acts as a kind of guardian for device data. Google is also offering up to $1.5 million for exploits found on developer preview versions of Android. Rewards for successful hacks of those versions will be given a 50% bonus, similar to Apple's offer. Rewards of up to $500,000 are also being offered for specific attacks that result in data theft and lock screen bypass.

In addition, Huawei also has a bounty of $220,000 for a remote control hack of its Android devices. Until recently, Google had offered a top reward of $200,000, which was lower than Huawei's.[ii]

More than a year after the company restricted API access, Facebook announced that it has discovered new data leaks. During the month it said that roughly 100 developers may have improperly accessed user data, which includes the names and profile pictures of individuals in certain Facebook Groups.

Evolve ETFs
Brookfield Place, 161 Bay Street, Suite 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com

The company explained in a blog post that developers primarily of social media management and video-streaming apps retained the ability to access Facebook Group member information longer than the company intended. The company did not detail the type of data that was improperly accessed beyond names and photos, and it did not disclose the number of users affected by the leak.[iii]

Researchers from the University of Electro-Communications in Tokyo and the University of Michigan, funded by the Pentagon's research arm, the Defense Advanced Research Projects Agency, were able to demonstrate that Amazon Alexa, Google Voice and Apple Siri can all be hacked by a laser from up to 110 meters away. As long as there aren't any objects blocking the laser, the attacks can work from long distances, from one building to another, for instance, with windows not making a difference. The researchers also tested successful attacks on Facebook Portal Mini, Amazon's Fire Cube TV, Samsung Galaxy S9 and Google Pixel 2.[iv]

In Canada, the Ontario Provincial Police (OPP) reported that Canadians have lost $43 million to cybercrime so far this year, with the number of crimes rising each year. Phishing, service and romance scams were identified as main ways fraudsters were extorting money from their victims. Romance scams were the most underreported, and accounted for more than half of all the money lost in cybercrimes. Police also estimated that the actual number of romance crime victims is much higher, with probably 95 per cent of these crimes going unreported.[v]

PERFORMANCE ATTRIBUTION:

The top performing holdings in the Fund for the month were Sailpoint Technologies Holdings, followed by Fortinet Inc. The largest holding by weight in the portfolio was Fortinet Inc., which was also the biggest contributor to the Fund's performance for the month.

SOURCES:

[i] https://www.morganstanley.com/ideas/europe-online-shopping-security-rules
[ii] https://www.forbes.com/sites/thomasbrewster/2019/11/21/google-bug-bounty-hits-1-million-if-you-can-hack-its-phones/
[iii] https://www.forbes.com/sites/mnunez/2019/11/05/facebook-is-still-leaking-data-more-than-one-year-after-cambridge-analytica/
[iv] https://www.forbes.com/sites/thomasbrewster/2019/11/05/amazon-alexa-google-home-hacked-with-a-laser/
[v] https://globalnews.ca/news/6077016/canadians-lost-43-million-cybercrime-2019/

DISCLAIMER:

Evolve ETFs
Brookfield Place, 161 Bay Street, Suite 2700, Toronto ON M5J 2S1
416.214.4884 | 1.844.370.4884 | www.evolveetfs.com