Cyber Security Hack: How to Trade Facebook's Wake Up Call

Facebook dropped another bombshell in September 2018.

It revealed an unknown hacker breached the site, compromising the accounts of 50 million users. While the company found and fixed bugs used in the attack, the damage has again been done. Trust has again been put in jeopardy.

Worse, not only did the hackers obtain the ability to access the Facebook accounts, they could access other services you use with your Facebook account registration.

The latest hack is another major misstep for Facebook, which has been trying to win back consumer trust after several recent debacles. Besides the Cambridge Analytics issue, Congress has strongly criticized the company for failing to prevent the spread propaganda.

What Happened this Time?

Attackers were able to trick Facebook into issuing them "access tokens," or digital keys that allow them to access accounts as if the attackers were the users.

The access keys allowed the attackers to even access any other services that someone used Facebook's login service to log in to, whether that's dating app Tinder, or a niche smart phone game, and gain access to highly personal information.

Unfortunately, it's not clear who carried out the attack.

They may never know. What we do know is that the company patched the problem. And, while Facebook doesn't believe this attack will hurt its business, we're not so sure. If users can't trust their data to Facebook, they'll delete their accounts and go elsewhere, or just stop using Facebook altogether.

It Highlights the Need for Cyber Security

A few keystrokes are all it takes. All of a sudden, your most private information is in the hands of criminals. Your most personal information, banking details, social security numbers, your children's information... all at risk.

Our digital over-dependence means that our risk is greater than ever before with new attacks surfacing all the time. The latest one attacks your cell phone to mine crypto currencies.

And, just in case you think hackers can't get to you behind your locked, alarmed doors, they're already inside your home computer.

If you think it can't happen to you…

You've already been hit, as you just learned the hard way from Facebook.

It has cost U.S. businesses billions of dollars. Consumers are having their most private data exposed for the world to see. Credit cards, social security numbers, bank account information, even your child's information in the hands of strangers.

Arguably, the threat is very real and expensive to fight.

Damages related to cyber crimes are expected to hit $6 trillion a year by 2021.

Unfortunately, despite the scale and potential harm of such attacks, many companies and government agencies still are not prepared. Up to 75% of all U.S. companies are not prepared. Up to 65% haven't devoted the time or resources to prepare.

Making that worse, Microsoft predicts that by 2020 data volumes online will be 50 times greater than what they are today with 111 billion lines of new software code produced each year, including billions of potential vulnerabilities that can be exploited.

For investors, this is another opportunity to look at cyber security stocks, like FireEye (FEYE).

FireEye (FEYE)

FireEye offers network security, malware analysis, endpoint security, e-mail security and file content security. After being ignored for quite some time, FEYE has become an industry high-flier to own long-term.

Not only is it one of the hottest "go to" stocks of the sector again, but underlying fundamentals look polished, too. For the third quarter of 2018, FireEye expects revenue of $206 million to $210 million, billings of $210 million to $220 million, and adjusted net income per share of $0.01 to $0.03. Better yet, it just reiterated its guidance for full-year 2018 revenue of $820 million to $830 million, but also boosted its outlook for billings of $825 million to $845 million (up $10 million from both ends of its previous ranges). FireEye also continues to expect 2018 adjusted net income per share of between $0.00 and $0.04.

According to FireEye CEO Kevin Mandia:

"Sales growth in the second quarter was broad based across all geographies and product families, and

demand for our differentiated security products and services is increasing as we enter the second half of 2018. New logo customers added in the quarter increased year-over-year and sequentially for the first time since early 2016, and we added more than 75 new Helix customers in the second quarter. We continue to leverage our unique innovation cycle to quickly adapt our products with knowledge gained on the front lines of combating cyber attacks."

Pure Funds Security ETF (HACK)

We can also look at the Pure Funds Security ETF (HACK), which jumped from a 2016 low of $19 to nearly $38 this year. It's sure to draw more interest especially as threats worsen. The ETF has holdings in Fortinet Inc., Check Point Software, CyberArk Software, Imperva Inc. FireEye, Proofpoint and dozens more.

The beauty of holding an ETF is the diversification and cheaper cost.

If we were to buy shares of each stock this ETF holds, it wouldn't cost us thousands of dollars. But at just $38 a share, you have exposure to most of the heavyweights.

HACK holds 47 stocks and its top 10 holdings combine for about 45% of its weight. HACK is a global ETF with exposure to seven countries, but U.S. stocks account for more than 76% of the fund's weight.

Rapid7 Inc. (RPD)

Rapid7 Inc. (RPD) provides security data and analytics solutions that enable organizations to implement an analytics-driven approach to cyber security and IT operations. It offers threat exposure management solutions, including Nexpose, which enables customers to assess and remediate their exposure to cyber risk; Metasploit, a penetration testing software solution; and AppSpider, an application security testing

solution.

The company also provides incident detection and response solutions, such as InsightIDR, a cloud-based offering for incident detection and response; Managed Detection and Response, a managed service, which provides customers with attacker behavior analytics, machine learning algorithms, and threat intelligence to hunt attackers; and incident response services that provide customers with access to security experts and experience.