PRO CYBERSECUR

IN THIS EMAIL→ Commentary & Analysis More from Dow Jones Editor's News Picks

HIGHLIGHTS

Commentary & Analysis

Stronger Authentication Techniques Can Help Firms Avoid Credential-Stuffing Attacks

By Jeff Stone

Hackers are taking advantage of the laziness and poor memories of many internet users, betting that a user name and password someone uses at one site will work on another.

In a hacking technique known as credential stuffing, cybercriminals plug lists of stolen user names and passwords into automated tools, and then use those tools to try to sign on to sites where users might have set up the same credentials. Attackers on average take over 0.1% to 2% of the accounts they seek with this method, which costs the banking and retail industries millions of dollars per day, according to Shuman Ghosemajumder, chief technology officer at cybersecurity vendor Shape Security.

Banks, retailers and other companies now are introducing different forms of authentication, in part because more than 2.3 billion credentials were leaked in reported data breaches in 2017 and 3.3 billion in 2016, according to research from Shape Security. The high number of leaked user names and passwords gives cybercriminals a valuable starting point for infiltrating user accounts, and it's clear hackers have sought to profit from internet users commonly reusing names and passwords, said Mr. Ghosemajumder.

Businesses can fight back by encouraging customers and employees to use more secure forms of identity management, such as multi-factor authentication and password managers, he said.

Banks and retailers, which have been most affected by credential stuffing, recently have invested in continuous authentication security methods, he said. The continuous authentication concept involves analyzing ways in which customers interact with an app or website and validating their identity during their session rather than just once at sign-on. An app or website might ask a user to enter a code sent to their phone, or pick up a phone call, to validate a user mid-session.

Continuous authentication is not the only method of avoiding such attacks. Companies also have begun to tweak their software by adding code that alerts the corporate security team whenever a failed login attempt occurs. A large organization might experience 10,000 failed logins on a normal day but will realize it is under a credential-stuffing attack if 100,000 user names and passwords are denied, said Matt Konda, chief executive of the consulting firm Jemurai LLC and a director at the Open Web Application Security Project, a nonprofit.

Two-factor authentication also can guard against these attacks, Mr. Konda said. Upon entering their credentials, users who have enabled two-factor authentication typically receive a text message with a unique passcode that provides access to their account.

Some firms are reluctant to force people to use this method, however, because it makes the log-in process longer, Mr. Ghosemajumder said. A bank might get around that by letting customers conduct some common tasks under a traditional sign-on process of name and password, and requiring another layer of authentication for more sensitive activities, such as transferring money, said Mr. Ghosemajumder.

More than 90% of the login traffic to online retailers and 58% to consumer banking sites in 2017 was attempted credential-stuffing attacks, according to Shape Security. The activity cost retailers an average of more than $18 million per day and consumer banks nearly $50 million per day, the company said.

Another way corporate cybersecurity executives can guard against the ploy is to check incoming customer user names and passwords against databases of credentials that are known to have been compromised, such as the Have I Been Pwned tool, said Mr. Konda at Jemurai.

Companies using that technique check users' credentials either upon registration or every time they log in, he said. He recently helped one client under a credential-stuffing attack and observed cybercriminals using accounts compromised in a breach of Yahoo Inc. data.

"We could literally see that the login attempts were coming in the order of the list of Yahoo accounts that were involved in the breach," he said.

The client notified the individual whose accounts were affected and helped them change their passwords, he said.

Write to Jeff Stone at jeff.stone@wsj.com.

More From Dow Jones

Equifax Ordered by Eight States to Beef Up Cybersecurity

By Lalita Clozel

Equifax will have 90 days to strengthen its information-security defenses. TAMI CHAPPELL/REUTERS

WASHINGTON—Equifax Inc. must improve how it manages cybersecurity risk, regulators from eight states said Wednesday, responding to a 2017 data breach that exposed the personal data of nearly 148 mil lion consumers.

The consent order, issued by regulators in Texas, California, New York and five other states, is the first major regulatory punishment for Equifax, which agreed to the order but neither admitted nor denied wrongdoing.

“The breach never should have happened,” Jan Owen, the commissioner of the California Department of Business Oversight, said in a statement. “This order will help ensure it doesn’t happen again.”

Under the terms of the order, the credit-reporting firm will have 90 days to strengthen its information-security defenses, including in vendor-risk management, patches and disaster response.

Equifax will have a month to create an annual internal audit program monitored by members of its board, and the company will have to issue reports to the regulators by July 31, detailing the steps it has taken to respond to the breach.

The hack, which exposed consumers’ personal information such as names, addresses and Social Security numbers, hasn’t resulted in a major fine or regulatory action from policy makers in Washington.

But it has prompted probes by the Federal Bureau of Investigation as well as the Federal Trade Commission. A banking deregulatory bill signed by President Donald Trump last month will force credit-reporting firms to offer free credit freezes to consumers, allowing them to prevent potential hackers from gaining access to their information.

Equifax said measures to improve its cybersecurity policies were already under way.

"A good number of the action items agreed to in the consent order have been completed," an Equifax representative said. "In fact, the findings, with a very few exceptions, are not new findings and are already part of our remediation plans."

Write to *Lalita Clozel at lalita.clozel.@wsj.com*

Quantum Computing Will Reshape Digital Battlefield, Says Former NSA Director Hayden

By Jennifer Strong

Former NSA Chief Michael Hayden, pictured here speaking in Washington in April, said it's unclear whether quantum computing will favor offensive or defensive cyber operations. TOM WILLIAMS/ZUMA PRESS

When retired Air Force General Michael Hayden took the helm of the National Security Agency in 1999 he found intelligence gathering, namely electronic espionage, to be in the midst of a sea change. Rather than “waiting for someone to send a message,” he says, “we could penetrate an adversary's information system and extract information, whether or not they ever intended to transmit it.” A former director of the NSA and CIA, Mr. Hayden calls the years that followed the “golden age of electronic surveillance” -- when foreign intelligence was widely available because “the human species was putting so much of its information” into poorly protected digital systems.

Fast forward to the current emphasis on data security and end-to-end-encryption, and another massive change for intelligence gathering, albeit one long anticipated. We’ve moved out of what he calls “a period that was a bit of an anomaly” to one where it’s harder to retrieve the contents of intercepted communications. “You adjust,” he says.

In the ongoing battle between law enforcement and Apple Inc. over whether the company should assist the government in cracking into iPhones, Mr. Hayden says it "surprised a lot of folks that people like me generally side with Apple” and its CEO Tim Cook. He says his position in support of Apple and the case for keeping encryption keys out of the hands of law enforcement, has nothing to do with privacy or business concerns but the integrity of security systems. “On security grounds, I'm not so sure we should make Mr. Cook punch a hole inside the security of his operating system,” he says,

because “we've all put really valuable things in this digital space and the government is going to have to depend on the private sector to help us defend it.” He continues, “we ought to think twice, maybe three times, before we make the private sector do something that will make it harder for them to do what probably only they can.”

We spoke to Mr. Hayden for an episode of WSJ’s The Future of Everything podcast. Edited excerpts are below.

Do you believe there’s a deterrence failure when it comes to cyber threats?

Yes, and it's been really interesting watching this debate take shape. I'm hearing folks who think we should be more aggressive using our offensive cyber power for defensive purposes. Now that's not been national policy. We have not tried to dissuade other countries from attacking us digitally by attacking them digitally.

During the nuclear period we thought of deterrence in two ways. We had counterforce strikes, which means we're going to go hit your weapons so your weapons can't hurt us. We also had something called countervalue strikes, which means we're going to go hurt something that can't hurt us, but you think very dear. That's a debate going on now.

What are your current thoughts on quantum encryption or quantum codebreaking?

When machine guns arrived it clearly favored the defense. When tanks arrived? That favored the offense. One of the tragedies of military history is that you've got people making decisions who have not realized that the geometry of the battlefield has changed because of new weapons. And so you have the horrendous casualties in World War I and then you've got the French prepared to fight World War I again and German armor skirts the Maginot Line. Now I don't know whether quantum computing will inherently favor the offense or inherently favor the defense, when it comes to encryption, security, espionage and so on, but I do know it's going to affect something.

What other emerging technologies are you watching?

Henry Kissinger wrote an article about this recently in which he warned against our infatuation with data and artificial intelligence. We can't let data crowd out wisdom. And so when I talk to people in the intelligence community who are going all out for big data and AI and algorithms I say, “you really do need somebody in there somewhere who understands Lebanese history, or the history of Islam.” Put all the silicon you want into this process but remember it's all designed to support the carbon-based machine at the end of the process.

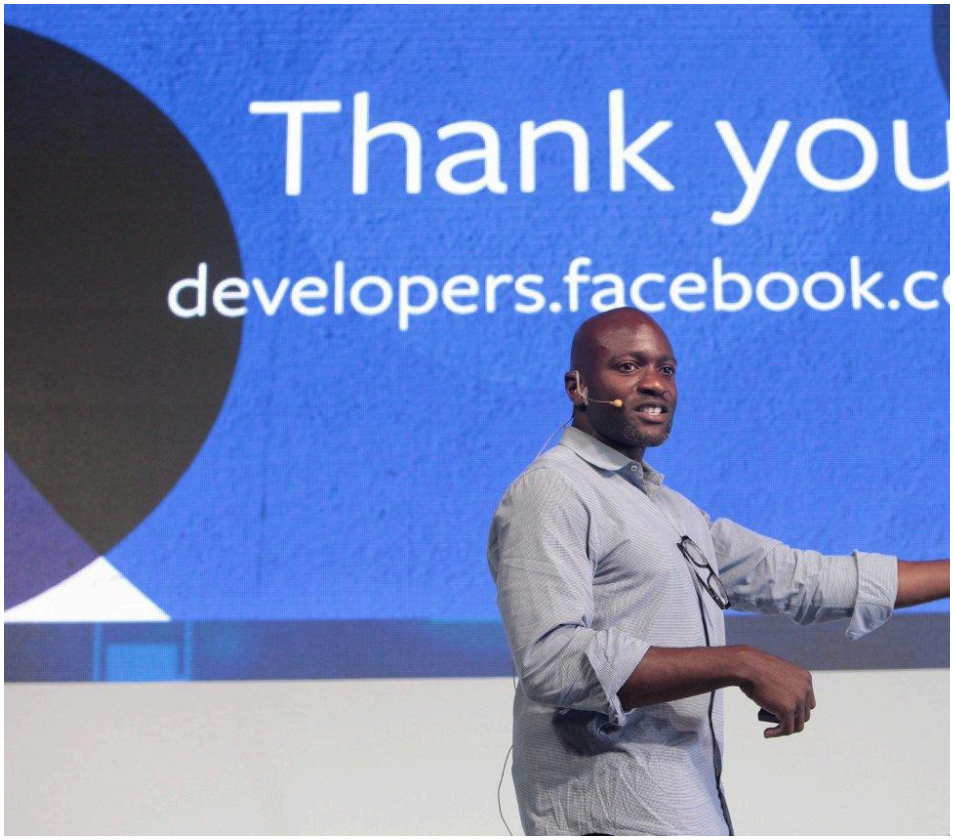
Do you worry about the lower barrier to entry for acquiring these kinds of capabilities and what that could mean?

Of course. I mean it's the dark side of the coin. Speed, accessibility, usability, ubiquity -- those things are virtues until you think about them in the hands of someone who wants to do you harm, and then they are tremendous disadvantages. We are going to have to work to keep pace to not be punished by the very attributes we built this thing for in the first place. You've got the lower cost of entry. You've got nation states or sub-state groups or criminal gangs or just simply a, "I'm mad at everybody" group who actually can do things beyond what those groups could have done in the past.

But what are you gonna do -- turn the clock back?

Facebook's Latest Problem: It Can't Track Where Much of the Data Went

By Deepa Seetharaman



Ime Archibong, Facebook's vice president of product partnerships, said most developers have been 'responsive' but noted that the process requires a fair bit of detective work on their end. SáSHENKA GUTIéRREZ/EPA/SHUTTERSTOCK

Facebook Inc.'s internal probe into potential misuse of user data is hitting fundamental roadblocks: The company can't track where much of the data went after it left the platform or figure out where it is now.

Three months after CEO Mark Zuckerberg pledged to investigate all apps that had access to large amounts of Facebook data, the company is still combing its system to locate t he developers behind those products and find out how they used the information between 2007 and 2015, when the company officially cut data access for all apps. Mr. Zuckerberg has said the process will cost millions of dollars.

One problem is that many of the app developers that scooped up unusually large chunks of data are out of business, according to developers and former Facebook employees. In some cases, the company says, developers contacted by Facebook aren't responding to requests for further information.

Facebook is now trying to forensically piece together what happened to large chunks of data, and then determine whether it was used in a way that needs to be disclosed to users and regulators. In cases where the company spots red flags, Facebook said it would dispatch auditors to analyze the servers of those developers and interrogate them about their business practices.

Ime Archibong, Facebook's vice president of product partnerships, said most developers have been "responsive" but noted that the process requires a fair bit of detective work on

their end. “They have to go back and think about how these applications were built back in the day,” Mr. Archibong said.

Facebook said in May it has suspended 200 apps for potentially violating its rules. Mr. Archibong declined to provide a detailed update on the status of the investigation or identify the 200 apps that were suspended thus far.

Facebook’s app investigation is a response to broader criticism over revelations earlier this year that data-analytics firm Cambridge Analytica improperly accessed and retained user data obtained from Aleksandr Kogan, a psychology professor at the University of Cambridge. The data, which was gathered by Mr. Kogan and his associates through a personality-quiz app, was used by the Trump campaign in 2016. Facebook eventually notified around 87 million users that their data may have been improperly shared with Cambridge Analytica, though many questions remain about that incident as well.

Facebook was blocked from accessing Cambridge Analytica servers by the U.K. government and doesn’t yet know what data the now-defunct company may have stored.

The results of Facebook’s internal probe could have far-reaching ramifications as lawmakers world-wide continue to hold hearings and contemplate tougher regulation of social-media platforms like Facebook.

U.S. Sen. John Thune (R., S.D.), the chairman of the Senate Commerce Committee, said at a hearing this month that

Facebook “remains under the microscope” and that lawmakers continue to examine potential measures to protect user privacy.

Some developers say they have little incentive to respond to Facebook’s requests to cooperate with the probe, either because they are out of business, have moved on to other projects or are uneasy about allowing another company to look at their servers and the way their apps are constructed. Such intellectual property is “the lifeblood” of a developer’s business, said Morgan Reed, president of ACT | The App Association, a trade group that represents more than 5,000 app makers and connected-device companies.

In addition, Facebook doesn’t have legal authority to force developers to cooperate.

“They can’t really compel these developers to hand over information,” said Ian Bogost, a professor at Georgia Institute of Technology. “This is not a federal inquiry about a crime or something. It’s a private company. What are the consequences?”

Mr. Bogost is also a game developer, and built a game for the Facebook platform called Cow Clicker. He said Facebook hasn’t contacted him about conducting a full-scale audit of Cow Clicker, which drew about 180,000 users.

Facebook recently sent him an automated message saying he would have to agree to an app-review process by Aug. 1 to retain access to Facebook’s platform and certain slices of user data,

including a user's friend list, a link to their profile, their gender and age range. Mr. Bogost said he would "probably" go through the review process.

It is difficult for Facebook to track down all the user data gobbled up by developers, owing largely to the way the platform was designed, according to developers, former Facebook employees and academics.

Facebook created its developer platform in 2007, giving outsiders the ability to build businesses by leveraging the Facebook data of users and their friends. Facebook tightened access in 2014 and gave pre-existing apps a one-year grace period to comply with the new rules.

Facebook engineers working on the platform didn't always document their changes, according to one former employee. At times, apps would stop working because of some unannounced tweak by a Facebook employee and developers would have to complain to get it fixed, developers said.

Over the years, Facebook at times tried to build systems that would allow the company to track down user info gleaned from the developer platform—but those efforts failed in part for technical reasons, former employees said.

The internal investigation is a sign of what Mr. Archibong, echoing other Facebook executives, described as a massive cultural shift within Facebook to focus more on "enforcement as a key component" of its system. Previously, executives have

said, the emphasis was on growth and connecting more users to one another around the world.

Facebook has said its probe will start with apps that had user bases of around 100,000 people or more, or apps that pulled extensive data about a smaller group of people.

Mr. Archibong said potential examples of wrongdoing would be storing personally identifiable information about users and sharing or selling that information, as the company says Mr. Kogan did. Mr. Kogan said at a Senate hearing this month that he was "very regretful" that people were angry to learn about how their d ata was used but that he didn't do anything different than other developers.

Mr. Archibong said the vast majority—"99.99999999%"— of Facebook developers are good actors and that the firm doesn't want to unnecessarily alienate them. Many of the developers involved in the probe "are going to be the same developers that we're going to be working with five years from now on the newest and latest and greatest stuff and I want them to be excited about our platform," he added.

Facebook said it has "large teams of internal and external experts" working on the investigations. Mr. Archibong said Facebook still expects the investigation to take "months and months" but added that the timing was "somewhat amorphous."

Write to *Deepa Seetharaman at Deepa.Seetharaman@wsj.com*

Editor's News Picks

National security review plans: The Trump administration plans to use a national security review board to examine Chinese acquisitions of U.S. technology manufacturers, Reuters reported Wednesday. The Treasury Department has encouraged lawmakers to grant new powers to the Committee on Foreign Investment, which controls investment deals, Reuters said. The strategy is part

of a larg er effort to encourage the Chinese government to change its trade and technology transfer policies, which U.S. officials have said result in the theft of American intellectual property.

Twitter's security update: Twitter Inc. announced it is tightening security on its social network. Users now can log on to their accounts with a unique USB security key in addition to their password as part of a two-factor authentication process, according to Engadget. The company also said it will fight abuse and automated accounts by requiring new u sers to confirm their account with an email or phone number, Bloomberg reported.

Dark Web sting nabs 35 suspects: A U.S. law enforcement investigation into the Dark Web has resulted in the arrest of 35 people and the seizure of $3.6 billion in cash and gold bars, as well as the seizure of illegal narcotics and bitcoin valued at roughly $20 million, CNET reported Tuesday. Agents posed as money launderers who exchanged U.S. currency for cryptocurrency to uncover the sale of illegal goods on a section of the internet only accessible with anonymity software, according to CNET. The Department of Justice called the investigation "the first nationwide undercover operation targeting dark net vendors."

Hotel booking service breached: Paris-based FastBooking, a provider of hotel reservation software, is alerting partners to a data breach in which information about more than 124,000 customers was stolen, according to SC Magazine. The company said in a statement that a hacker exploited a vulnerability in the company's web application server to install malicious software. Exposed informat ion includes customer names, nationalities, home and email addresses, check-in dates, check-out dates, and hotel names, according to Dark Reading.