April 7, 2016

CYBERSECURITY

Chinese National Hacker Pleads Guilty to Sending Military Data to China

The FBI and DOJ continue their effort to bring cyber hackers to justice.

Last week, Chinese national Su Bin pled guilty to stealing data related to Boeing's C-17 military cargo plane and trying to steal information related to U.S. F-22 and F-35 fighter jets. Bin was indicted, along with other co-conspirators, in August 2014 by a California federal grand jury of stealing computer data of The Boeing Co. and other U.S. military contractors from 2006 to 2014 and attempting to send the data to China.

Su will be sentenced on July 13, 2016. Although he faces up to five years in prison and a $250,000 or twice the gross gain or loss from the scheme, the gain is that China's military planes have an uncanny resemblance to U.S. planes. How does one value a gain or loss?

— Linn Foster Freedman

FBI Cyber's Most Wanted: Spotlight on Firas Dardar and Ahmed Agha

New additions to the FBI Cyber's Most Wanted List show that "the line between ordinary criminal hackers and potential national security threats is increasingly blurry," according to Assistant Attorney General for National Security John Carlin. The FBI is offering a $100,000 award for information leading to the arrest of two Syrian nationals suspected of committing dozens of cyber-attacks, including extortion, against U.S. government agencies and private companies.

Firas Dardar and Ahmad Agha are suspected of being members of an entity called the Syrian Electronic Army (SEA), which the FBI alleges to be a group of hackers working in support of the Syrian Regime. The indictments against the alleged co-conspirators were under seal until late March 2016. The FBI added both to the Cyber's Most Wanted list as soon as the indictments were made public.

Charges include conspiracy to gain unauthorized access to and to damage computers, convey false information regarding a terrorist attack, cause mutiny of U.S. Military members, commit identity theft, access device fraud, commit money laundering, commit wire fraud, violate Syrian sanctions regulations, and receive the proceeds of extortion.

Dardar is alleged to have worked with Agha to target computer systems at the Executive Office of the

President, although those attempts failed. They were successful in hacking into a media outlet's Twitter account, tweeting that a bomb explosion at the White House had injured the President. They also used a third party vendor to commandeer a U.S. Marines recruiting website, posting a message to U.S. Marines to "refuse [their] orders." Dardar and another co-conspirator are also alleged to have hacked into private computers and threatened damage to the computers, deletion of data, or sale of stolen data if the victims did not make payments into Syrian accounts.

— Nuala E. Droney

ENFORCEMENT + LITIGATION

21st Century Oncology Faces Second Class Action Suit for Data Breach of 2.2 Million Records

We previously reported that 21st Century Oncology (21st Century) experienced a data breach of up to 2.2 million patient records that compromised the names, Social Security numbers, and health and diagnostic information. It began notifying patients on March 4 and delayed notification at the request of law enforcement. 21st Century was sued days later by patients stating that it violated the Florida Deceptive and Unfair Trade Practices Act and the Fair Credit Reporting Act.

On March 30, 21st Century was hit with a second proposed class action suit alleging that it failed to properly secure the patient records and failed to notify the patients in a timely manner, despite specifically being asked not to by law enforcement. Further, the suit alleges unjust enrichment, claiming that a portion of the amounts paid by patients should have been used for data security.

The plaintiffs complain that 21st Century notified the SEC and investors but thereafter waited a week to notify patients. The named plaintiff alleges that his information was used to try to open several credit card accounts.

Interestingly, the Federal Trade Commission issued a blog alert on April 4, 2016, about the breach and providing consumers with information about what they can do if they get a notification letter from 21st Century.

— Linn Foster Freedman

FTC, ONC, OCR and FDA Release Online Tool for Mobile Health App Developers

While attending the International Association of Privacy Professionals' annual global event and listening to Chairwoman Edith Ramirez discuss the Federal Trade Commission's (FTC) concerns about consumer privacy, the FTC, the Office of National Coordinator for Health Information Technology (ONC), the Office for Civil Rights (OCR), and the Food and Drug Administration (FDA) announced that they had combined efforts and created a web-based tool for mobile health app developers to use in determining which federal laws and regulations might apply to their app.

Ms. Ramirez explained that the number of mobile apps being developed is staggering, and often the app developers don't know which regulatory scheme is applicable to the product. She stressed how important it is that app developers build privacy and security into the app from the start and that the FTC, along with the other agencies, wanted to provide a tool to assist developers to understand the regulatory rubric that might be applicable.

The tool asks app developers a series of questions, including the following:

- Do you create, receive, maintain, or transmit identifiable health information?
- Are you a health care provider or health plan? Do consumers need a prescription to access your app?
- Are you developing this app on behalf of a HIPAA-covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?
- Is your app intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease?
- Does your app pose "minimal risk" to a user?
- Is your app a "mobile medical app?"
- Are you a nonprofit organization?
- Are you developing this app as or on behalf of a HIPAA-covered entity (such as a hospital, doctor's office, health insurer, or health plan's wellness program)?
- Do you offer health records directly to consumers (or do you interact with or offer services to someone who does)?

Each question has a drop-down explanation after the user chooses "yes" or "no," and the tool also offers a glossary and short explanations to the Health Insurance Portability and Accountability Act (HIPAA), the Federal Food, Drug & Cosmetic Act (FD&C Act), the Federal Trade Commission Act (FTC Act) and the FTC's Health Breach Notification Rule. The website also provides a link to tips on how to protect and secure consumer data.

The FTC released simultaneously "Mobile Health App Developers: FTC Best Practices," which provides guidance for app developers "to help you build privacy and security into your app." The points made in the guidance are the following:

- Minimize data.
- Limit access and permissions.
- Keep authentication in mind.
- Consider the mobile ecosystem.
- Implement security by design.
- Don't reinvent the wheel.
- Innovate how you communicate with users.
- Don't forget about other applicable laws.

The regulatory scheme for app developers is often unclear and any guidance from regulators is a valuable read.

— Linn Foster Freedman + Kathryn M. Rattigan

DATA BREACH

Hacker Steals Norfolk Admirals Customer Data

A Norfolk Admirals fan notified the Admirals last week that his information was posted online. Another customer found out that her information was posted online from the service Have I been Pwned? Her son's name and address were included because she had signed him up for the Admirals Kids Club several years ago.

According to the Admirals, a hacker posted several thousand Admirals customers' names, addresses,

email accounts, and credit cards used (but not the credit card numbers) to purchase items through the Admirals website. Although the original number of customers affected was 4,476, the Admirals claim that after de-duplicating and eliminating spam email addresses, the actual number of customers affected is 250.

The alleged hacker said in an interview on Twitter that he had emailed warnings to the Admirals about inadequate security and that his emails were ignored. He also claimed that he had the team's Twitter password but had not tried to get into the account.

— Linn Foster Freedman

Trump Hotels Investigating Second Credit Card Breach

KrebsOnSecurity has reported that sources from the banking industry have advised of a pattern of fraud on credit cards used at Trump Hotel Collection (Trump) properties. Trump has confirmed that it is investigating the matter. If confirmed, this would be the second breach of its credit card systems in the past year.

Trump notified card holders in October 2015 that its payment systems had been compromised by malware [view related posts here and here].

— Linn Foster Freedman

Tidewater Community College Hit with Phishing Scam Exposing Data of 3,193 Employees

Tidewater Community College (Tidewater) has announced that the personal information, including names and Social Security numbers of 3,193 current and former faculty and staff members, was compromised in a phishing scheme, and the information has been used to file fraudulent tax returns.

The hacker impersonated a Tidewater employee and asked another Tidewater employee to send 2015 W-2 data of employees. The duped employee did so, exposing the names, Social Security numbers, and wage information of 3,193 employees.

According to Tidewater, over 100 of their employees have been unable to file tax returns, as a return has already been filed by fraudsters. When Tidewater found out about the high number of employees suffering from tax refund fraud, it detected the exposure. Tidewater is offering its current and former employees credit monitoring and is training employees on cybersecurity.

— Linn Foster Freedman

Panama Law Firm Mossack Fonseca Faces Leak of 11 Million Documents Exposing Thousands of Clients

In late 2014, an anonymous source secretly leaked to a German newspaper reporter nearly four decades of confidential and proprietary data about shell companies registered by the multinational Panamian-based law firm Mossack Fonseca.

The German newspaper contacted the International Consortium of Investigative Journalists (ICIJ), who

assembled more than 100 other international news outlets, including the U.S.-based McClatchy newspapers, to secretly review and investigate the massive amount of leaked data. Last Sunday, journalists in these news outlets began publishing stories on the so-called Panama Papers. While offshore shell companies have legitimate business purposes, these journalists reported that many of the 214,000 companies were formed to mask the true owners, citizens from more than 200 countries and territories worldwide.

Mossack Fonseca's co-founder confirmed the leaked data was authentic and alleges the firm's records were externally hacked. The firm has already notified its clients and law enforcement of the unauthorized access to confidential and proprietary documents and information, which includes corporate and financial records, email addresses, and passports.

No one, including Mossack Fonseca and its partners, has been directly accused of breaking any laws. However, just being linked to these offshore companies has already had some dramatic repercussions. Iceland's prime minister and the head of global corruption watchdog Transparency International's Chile branch have resigned. Several other politicians, professional soccer officials, celebrities, and professional athletes and their families are under scrutiny. United States and European law enforcement officials announced investigations into the leaked data to determine whether tax or other laws in their countries were broken.

According to the McClatchy newspapers, the only U.S. newspaper involve in ICIJ's efforts, thus far about 200 scanned U.S. passports, 3,100 companies were tied to people in the U.S., and about 3,500 shareholders of offshore companies with U.S. addresses listed have been found in the leaked data. However, as yet, very few U.S. residents have been publicly identified.

Encryption and anonymity technology played a significant role in keeping the Panama Papers project secret for more than a year. Encrypted channels were used by the original whistleblower to originally contact the German reporter. During the challenging process of transferring, indexing, and analyzing the data, ICIJ journalists working on the project created a secure database to enable them to access the data and communicated with each other about their findings. In fact, ICIJ and the news outlets have no current plans to release the 2.6 terabytes of leaked data, comprising 11.5 million documents, as much of the data is sensitive and relates to private individuals. To date, the group's reporting has focused on public figures linked by the data to offshore companies.

— Kathleen M. Porter

DRONES

Get Your Student Pilot Certificate and Commercial Drone Operator Certificate Sooner Rather than Later

As of April 1 individuals seeking their student pilot certificate must wait until the Transportation Security Administration (TSA) background checks are completed before receiving the certification, whereas prior to the beginning of this month, you could go to a local aviation medical examiner and pick up a student pilot certificate that same day. The Federal Aviation Administration (FAA) estimates that the turnaround time for this certificate from the TSA will only be three weeks. However, in the FAA's proposed commercial drone operator regulations from last year, the FAA stated that it "could take about 6 to 8 weeks after receipt of an application for the FAA to issue an applicant an unmanned aircraft operator certificate with a small UAS rating." Most likely, the FAA's original estimate will be closer to the real wait time.

Additionally, after the 6 to 8 weeks have passed, and you have obtained your student pilot certificate, you will still need to take the Part 107 exam for an actual drone operator certificate. The good news is that the individual's TSA background check can be used for the drone operator certificate and speed that process

along, getting the drones in the sky a bit faster than before, when individual's needed the background check conducted after taking the Part 107 exam. So if you or your company is considering drone use, start this process sooner rather than later.

— Kathryn M. Rattigan

DATA PRIVACY

Sensor System Technology to Track a Driver's Every Move

A new, proprietary sensor system technology has arrived on the market that can track drivers using cameras and sensors, including whether the driver is speeding or turning without signaling, or even data such as the driver's heart rate and blood pressure. It could even gather data about the passengers in the vehicle. The auto insurance industry hopes to use this type of technology to allow insureds the opportunity to decrease (or maybe, unfortunately, increase) their auto insurance premiums based on their driving habits. Insured could choose to opt-in to this surveillance system for this benefit.

However, the concern arises when the information is used beyond the auto insurance industry. What if the information were sold to third parties like life insurance companies and health insurance companies, potential employers, or credit rating agencies? While many auto insurers have used "telematics" in the past (i.e., technology that transmits data in real time between the car and the company) to collect data on mileage, hours on the road, speed, and brake activation, this new technology seeks to go beyond that.

The Electronic Privacy Information Center's (EPIC) associate director, Khaliah Barnes, said, in response to this new technology, "There is an urgent need to establish meaningful and enforceable privacy and safety protections." But many drivers may not be too concerned about their privacy if they are offered a free gas card for their participation in this sensor system and the potential decrease in their yearly premiums.

— Kathryn M. Rattigan

SOCIAL MEDIA

Google and Oracle Agree Not to Research Potential Jurors' Social Media Accounts

Litigating companies Google and Oracle have mutually agreed, at the strong recommendation of the presiding judge, to refrain from researching the social media accounts of a potential jury pool before and during a high-stakes copyright infringement trial.

Google and Oracle have both agreed not to research the social media accounts of the potential or actual jurors chosen to sit for the trial where up to $8.8 billion in damages is being sought. Further, the companies have agreed to the judge's proposed ban of doing any Internet research on the potential jurors. The judge commented that the jurors' basic right to privacy should be protected.

The judge agreed to give the lawyers an additional 40 minutes to conduct *voir dire* in light of the agreement.

— Linn Foster Freedman

PRIVACY TIP #29

U.S. + Canada Issue Joint Ransomware Special Alert—Read and Follow Recommendations

We have frequently alerted individuals and companies about the increasing risk and success posed by sophisticated phishing schemes.

It has become such a real and grave problem that the U.S. Computer Emergency Readiness Team of the Department of Homeland Security (US-CERT) has teamed up with the Canadian Cyber Incident Response Centre to issue a joint special alert to warn companies of the threat of ransomware and the variants that are being seen by law enforcement.

The Alert (TA16-091A), "Ransomware and Recent Variants," outlines what ransomware is, mentions the specific variants Locky (which has affected the health care industry) and Samas, and seeks "to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware."

The alert states that the rough estimate of how much money malicious actors are making from successful ransomware schemes is $394,400 per month. Because it is so profitable, new ransomware and malware variants have been developed, including Xorist, CryptorBit, CyptoLocker, and now Locky and Samas.

Ransomware can affect home computers and business files and systems. It is applicable to everyone.

Here are the tips that are being offered by US-Cert as preventative measures to guard against a ransomware attack (verbatim):

- Employ a data backup and recovery plan for all critical information. Perform and test regular backups to limit the impact of data or system loss and to expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Use application whitelisting to help prevent malicious software and unapproved programs from running. Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
- Keep your operating system and software up-to-date with the latest patches. Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
- Maintain up-to-date anti-virus software, and scan all software downloaded from the internet prior to executing.
- Restrict users' ability (permissions) to install and run unwanted software applications, and apply the principle of "Least Privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through the network.
- Avoid enabling macros from email attachments. If a user opens the attachment and enables macros, embedded code will execute the malware on the machine. For enterprises or organizations, it may be best to block email messages with attachments from suspicious sources. For information on safely handling email attachments, see Recognizing and Avoiding Email Scams. Follow safe practices when browsing the Web. See Good Security Habits and Safeguarding Your Data for additional details.
- Do not follow unsolicited Web links in emails. Refer to the US-CERT Security Tip on Avoiding Social Engineering and Phishing Attacks for more information.

Individuals or organizations are discouraged from paying the ransom, as this does not guarantee files will be released. Report instances of fraud to the FBI at the Internet Crime Complaint Center.

Privacy Tip this week for individuals and businesses: implement US-CERT's recommendations.

— Linn Foster Freedman

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.