June 9, 2016

CYBERSECURITY

US-CERT Warns of Old SAP Software Vulnerability

The U.S. Department of Homeland Security Computer Emergency Readiness Team (US-CERT) recently issued an alert to the public about a vulnerability in old software developed by SAP SE that cyber-attackers are using to infiltrate companies' systems.

According to the alert, "SAP systems running outdated or misconfigured software are exposed to increased risks of malicious attacks." The vulnerability affects Java platforms of SAP. SAP has stated that the vulnerable component, Invoker Servlet, was disabled in 2010, and updated releases of the software do not contain the vulnerability. Although SAP issued a security advisory about the vulnerability (#1445998) in 2010, a recent report by a security firm indicated that it had discovered evidence that the old vulnerability has been used recently by cyber-attackers in attempts to gain access to systems in approximately three dozen companies in all industries.

If successful in its use of the vulnerability, the cyber-attacker is able to execute arbitrary operating systems commands and create SAP administration users using a Web browser without the need to use a valid SAP user ID and password. This in effect allows the attackers to gain free access to the system by creating their own user ID and password. According to the alert, "Exploitation of the Invoker Servlet vulnerability gives unauthenticated remote attackers full access to affected SAP platforms, providing complete control of the business information and processes on these systems, as well as potential access to other systems."

The bottom line is that, when software companies, such as SAP, provide patches for security vulnerabilities, it is important to follow the instructions of the company and run the security configurations and recommendations to protect the system from the known vulnerability.

Heed US-CERT's warning and check with your IT folks now to confirm that the SAP patch has been implemented.

— Linn Foster Freedman

State-Sponsored Attacks Increasing and Targeting Industrial Facilities

A representative of Honeywell Process Solutions (Honeywell), which provides cybersecurity services for over 400 industrial sites worldwide, recently commented publicly that Honeywell is seeing an increase in

nation-state and state-sponsored attackers focusing on the industrial sector, which includes oil refineries, nuclear power plants, chemical and power plants, natural gas processors, and mining and water treatment facilities.

The hackers are targeting the industrial facilities in an attempt to remotely control the site and gain access to the data. Honeywell has seen attacks in two-thirds of the 30 industrial sectors that it monitors. According to Honeywell, "We've seen that there's definitely increasing exposure to what we call high-capability threat actors…Nation-state and sponsored attackers are definitely out there, and they're definitely focusing on these industries."

— Linn Foster Freedman

FBI Report: Ransomware and Phishing Scams Increasing

We can't go a week without commenting on how rampant ransomware is in the industry. The FBI recently released a report confirming how devastating ransomware has become for U.S. businesses.

According to the report, ransomware infections caused more than $1.6 million in losses in 2015. The FBI Internet Crime Complaint Center IC3 received 2,453 complaints of ransomware in 2015. In total, IC3 received 288,012 complaints from individuals and companies, with a reported total loss from hackings of $1.07 billion. Yes, that is with a "b." Ransomware alone resulted in adjusted losses of $1,620,814.

These figures represent only losses that are reported to the FBI, so these figures do not reflect the total picture, as many companies continue to keep such information private and not notify law enforcement when they become a victim of an intrusion. Other sources estimate that losses associated with ransomware is closer to $24 million.

Whatever the true number, ransomware is not going away, and as long as companies continue to pay the cybercriminals to get their data back, the problem will continue. The FBI does not recommend payment to the criminals. Having a robust backup system and testing it is an important part of the strategy to be prepared for a ransomware attack.

Of course, the number one cause of data loss, according to the FBI report, continues to be social engineering and email compromises. The reported losses associated with business email compromises in 2015 was $246,226,016.

More recently, PhishMe has stated that, as of the end of March, 2016, 93 percent of all phishing emails contained encryption ransomware. This figure is up from 56 percent in December 2015. Even more surprising is that, according to PhishMe, the number of phishing emails in the first quarter of 2016 exceeded 6.3 million, which represents a 789 percent increase over the last quarter in 2015.

Folks—phishing is not going away. Phishing scams are increasingly including ransomware, and paying the ransom will only give the hackers incentive to keep phishing away.

— Linn Foster Freedman

DATA BREACH

EMR Company Settles with FTC for Posting Physician Surveys that Contained Health Information

on Its Website

Cloud-based electronic medical record (EMR) company Practice Fusion has agreed to settle an enforcement action with the FTC that alleges that it misled consumers when it solicited reviews of their doctors. The FTC alleges that Practice Fusion failed to tell consumers that the reviews would be posted on the Internet, "resulting in the public disclosure of patients' sensitive personal and medical information."

According to the FTC, "Practice Fusion's actions led consumers to share incredibly sensitive health information without realizing it would be made public."

The FTC listed three examples of information consumers provided, which shows they thought the information would be shared only with the provider and not with the public. The examples include information relating to dosage of the anti-anxiety medication Xanax, help with a depressed child, and diagnosis of a yeast infection.

The settlement agreement will require Practice Fusion to stop misrepresenting how it will use, maintain, and protect the confidentiality of the information it collects and to obtain consumers' affirmative consent before making the information accessible to the public.

The agreement is open to public comment until July 8, 2016.

— Linn Foster Freedman

Medical Records of NFL Players Taken in Theft of Unencrypted Laptop

A Washington Redskins trainers' unencrypted laptop was located in a backpack that was stolen on April 15. Unfortunately, the laptop contained medical exam results for NFL Combine attendees since 2004, which is estimated to include most current NFL players, as well as Redskin players, which could be accessible by the thief.

The backpack was in the trainer's locked car, but the culprit broke the car window and absconded with the backpack, the laptop, with the medical exam results, as well as some paper records.

The NFL Players Association notified the players of the incident by email and is alleging that the theft is a "violation of NFL and NFLPA rules regarding the storage of personal data." The Players Association is asking the NFL to provide details about its plans to address the incident.

This is another reminder of how vitally important it is for all companies to encrypt laptops and train employees not to download data to a laptop or other portable device and how to protect portable devices from loss or theft. It is a double whammy that paper medical exam results were included, and the security of paper records should not be forgotten.

— Linn Foster Freedman

Chiropractic Clinic Hit with Malware

Complete Chiropractic & Bodywork Therapies, located in Ann Arbor, Michigan, recently notified 4,082 patients that its server, which contained the electronic medical record and billing information of patients, was infected with malware from November 2015 until it was discovered through a server malfunction in

March 2016.

The server contained the names, addresses, birth dates, Social Security numbers, and health information of the patients. The clinic notified its patients and provided them with one year of identity theft protection.

This is another example of the insidiousness of malware infections and how intruders have the ability to enter and stay in a system undetected for months or even years. It shows the importance of a continual analysis of IT systems and vulnerabilities to detect intrusions as quickly as possible to limit the risk of data loss.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

In Landmark Case, Utah Jury Decides in Favor of FTC, Against Companies for Violations of the Telemarketing Sales Rules and Do Not Call Registry Rules

Last week, a Utah federal court jury decided in favor of the Federal Trade Commission's (FTC) claims against Forrest S. Baker and his film firms, Feature Films for Families, Inc., Corporations for Character, L.C., and Family Firms of Utah (collectively "companies"), stating that they engaged in deceptive and unlawful telemarketing campaigns and made illegal calls to consumers in violation of the Telemarketing Sales Rule (TSR). This case was filed back in May 2011 and is now the first-ever jury verdict in a case seeking to enforce the TSR and FTC's Do Not Call (DNC) Registry rules.

Not only did the court and the jury find that the companies' telephone calls qualified as illegal telemarketing calls (as opposed to surveys, fundraising, and informational calls), the jury also found that the companies' used deceptive sales tactics when making many of these calls by promising that "all of the proceeds" from sales of DVDs it was pushing would be used to complete a recommended list of movies for the nonprofit Coalition for Quality Children's Media; instead 93 percent of the sales went directly back to the companies.

The testimony also revealed that the companies were responsible for over 117 million violations of the TSR (including 99 million illegal calls to telephone numbers listed on the DNC Registry) and more than 4 million calls where the companies made misleading statements. The jury also found that the companies had 'actual or implied knowledge' of these violations, which will allow the court to assess civil penalties under the FTC Act of up to $16,000 per violation. No civil penalties have been assessed at this point.

— Kathryn M. Rattigan

Credit Card Issuers Cleared to Proceed against Home Depot

Last week, a federal judge in Georgia ruled that the class action filed against Home Depot by credit card companies could proceed. The judge stated that the card issuers' allegations that Home Depot was negligent in its security processes prior to the data breach in 2014 had merit.

The card issuers are requesting reimbursement for the costs associated with reissuing millions of credit and debit cards and reimbursing card holders for fraudulent transactions.

Home Depot has already agreed to settle claims against it for the massive data breach that occurred in

2014, affecting up to 56 million debit and credit card holders for at least $19.5 million, and up to $28 million, including attorneys' fees and costs.

— Linn Foster Freedman

KitNipBox Sues Meowbox for Allegedly Hacking Website and Stealing Trade Secrets

Cat product service provider KitNipBox sued rival Meowbox in federal court in Washington alleging that Meowbox hacked into KitNipBox's website to steal its trade secrets and confidential information and to disrupt its business.

According to the allegations, on March 14, 2016, the chief technology officer of Meowbox, with the support and knowledge of Meowbox's CEO, executed a malicious script on KitNipBox's website, which ran for 40 minutes.

During the run, which included a denial-of-service attack, Meowbox allegedly was able to access and add the email addresses of 8,000 current and former subscribers of KitNipBox to Meowbox's database. The script run also allegedly caused KitNipBox's emails to be placed into its customers' spam folders, which caused KitNipBox damage. The complaint alleges that running the script was a violation of the Electronic Communications Privacy Act, as well as infringement of trade secrets, unfair competition, unjust enrichment, tortious interference, and civil conspiracy.

— Linn Foster Freedman

DRONES

FAA FOIA Request Sheds Light on Fines against Drone Operators across the Country

Last week, the Federal Aviation Administration (FAA) responded to a Freedom of Information Act (FOIA) request, releasing the list of drone pilots (individual and commercial) who have been fined for flying drones recklessly or in restricted airspace (like airports, government buildings, and sports arenas). While this list has only a handful of entries, it can tell us a lot about the current state of drone operation enforcement. The range of fines (and settlements) starts at $400 and reaches the outlier of $1.9 million against Skypan, which we wrote about on our blog back in October. The list also tells us that if you are flying your drone on the East Coast, the FAA's eastern region office seems to be the most active in this area of enforcement so operate your drone properly and safely. Otherwise, there were only a few isolated fines in Texas, Alabama, and Puerto Rico. There have also been fines for not using a drone with "an operable coded radar beacon transponder" and "automatic altitude reporting equipment." However, almost no drones have these capabilities, and the regulations that the FAA is relying on are actually for manned aircrafts.

The list of drone fines is as follows:

- Austin, Texas, August 30, 2014, Shawn Phillip Wyse: $1,100;
- Tuscaloosa, Alabama, November 14, 2015, Gregory Taylor: $1,100;
- Queens, New York, May 25, 2014, Clinton Bascom: $1,100;
- San Juan, Puerto Rico, October 18, 2015, Marcos Plaja-Ferreira and Alberto Haber-Flores: $1,100 each;
- U.S. Coast Guard Housing Complex Rio Bayamon, Puerto Rico, July 5, 2015, Jorge Lubo,

2015: $1,100;

- Fairfield Avenue and Fort George Hill (Bronx), July 7, 2014, Wilkens Mendoza: $1,100;
- Capitol Building, Albany, New York, September 17, 2015, Adam Rupeka: $1,100;
- Portside Apartments, East Boston, August 30, 2015, Jose Paderes: $1,100;
- Manhattan, New York, July 7, 2014, Remy Castro: $1,600;
- Arlington, Texas, June 8, 2014, Robert Eddelman: $2,200;
- 290 Central Avenue, Brooklyn, September 17, 2014, Isaac Rosa: $2,200;
- 38th Street between 3rd Avenue and Lexington Avenue, Manhattan, September 30, 2013, David Zablidowski: $2,200;
- Citi Field, May 6, 2015, Henry Wolters: $2,200;
- Billie Jean King National Tennis Center, Queens, September 3, 2015, Daniel Verley: $2,200;
- Washington DC, Polo Fields in West Potomac Park, March 25, 2015, Damian Dizard: $3,300;
- West Potomac Park, Washington DC, March 25, 2015, Monica Singleton: $3,300;
- Lafayette Park, Washington DC, May 14, 2015, Ryan MacDonald: $4,400;
- Washington DC, G Street and 10th St NW, January 26 2015, Shawn Usman: $5,500;
- University of Virginia, Charlottesville, April 13, 2012, Raphael Pirker: $10,000;
- 441 East Fordham Road, Bronx NY, May 16, 2015, Xizmo Media Productions: $18,700;
- All over Manhattan, SkyPan: $1.9 Million; and
- Coney Island Boardwalk, July 4, 2015, David Quinones: Surrendered Pilot's license.

Notably, almost all of the FAA's enforcement in this area has been largely created from publicly available information such as YouTube videos, commercial operators' websites, and media and police reports. And since the FAA uses the standard "medium or high actual or potential risk to safety" to determine the fines for improper drone operations, without an exact threshold defined, drone operators must proceed with caution and know where they can and cannot fly around (and above).

— Kathryn M. Rattigan

E-DISCOVERY

The Case for E-Discovery Education in Law School

The lament that law schools do not adequately prepare new lawyers for the actual practice of law is not a new one. The refrain, however, seems more pronounced as the day-to-day practice of law becomes increasingly intertwined with technological concepts that have little place in most law school curricula. This problem is particularly paramount in the field of e-discovery. Although saddled with its own (dubious) moniker, e-discovery is really nothing more than discovery for the modern age. When the world worked through paper, it made sense that discovery involved the exchange of hard copies. Today, in a world governed through bits and bytes, it stands to reason that the information necessary to resolve disputes resides electronically. Indeed, every lawsuit, big or small, is likely to involve electronically stored information (ESI) in one way or another. Whether it is an antitrust matter involving data collections from hundreds of custodians or a divorce matter involving the social media accounts of two individuals, e-discovery has become the rule, not the exception. Despite this, the vast majority of law schools do not teach e-discovery. And those that do tend to offer it as a one-off elective, rather than a component of their civil procedure or evidence courses. E-discovery is here to stay, and new lawyers should be armed with the basic tools to issue spot, lest they run afoul of developing ethics opinions and state rules of professional conduct regarding technological competence.

— Andrea Donovan Napp

PRIVACY TIP #38

Genetic Privacy and the Use of Genomic Information

Genetic information is basically one's DNA sequence, which includes health information and genetic information about the individual and an individual's family. It is at the core of one's individual privacy and provides information on family members. As technology advances, genetic testing is easier and cheaper to obtain, and there are numerous companies in the market that offer quick and cost-effective genetic testing. The ethics of genetic testing is outside the scope of this piece but is interesting in its own right.

Vanderbilt University School of Medicine has announced that it received a four-year, $4 million grant from the National Institutes of Health to establish the Vanderbilt Center for Genetic Privacy and Identity in Community Settings, which will study privacy concerns associated with the use of genomic information.

According to Vanderbilt, the center will "examine the likelihood that lapses in protecting genomic information allow people to be identified, how people perceive such risks, and how effective legal and policy efforts are in reducing them." The center's goal is to develop policy recommendations about this complex area.

Why should we be concerned about the use of our genomic information? According to the Council for Responsible Genetics (www.councilforresponsiblegenetics.org), one reason why the use of genetic information is important is because of genetic discrimination. It documented over five hundred cases where the use of genetic information was used to deny individuals employment or health or life insurance. The Genetic Information Non-discrimination Act (GINA) was passed in 2008 to provide individuals protection from these types of discriminatory behaviors.

Genomic information is used by law enforcement to investigate crimes, and DNA is now being used to exonerate those who have been wrongfully accused and imprisoned. Often, when one is accused of a crime, s/he is required to submit to a DNA test and has no choice, which was upheld by the U.S. Supreme Court in a 5-4 decision. The FBI's National DNA Index System (NDIS) is a database that is populated with DNA samples of crime scenes, those arrested for crimes, and those convicted of crimes. It holds millions of samples. And it doesn't delete the samples of those arrested but not convicted, or of victims. Privacy advocates contend that the DNA samples can be used for other purposes—there are no rules regarding how a sample can be used by law enforcement once they have it and how a sample collected in a law enforcement setting should have privacy protections over how it is collected, maintained, stored, used, and expunged.

Most concerning are the issues around surreptitious collection of DNA or genomic information. There is no federal law that prohibits surreptitious DNA testing. Some states have enacted legislation prohibiting the use and disclosure of genetic information, but not all. Further, when consumers send off a swab of the inside of their mouth to a private company to perform genetic testing, the company is not prohibited by law from using, selling, or further disclosing the information, as it is not covered by HIPAA and prohibited from doing so like your doctor or hospital is.

In fact, usually the individual has given consent to allow the company to use and disclose the information any way it sees fit somewhere in the fine print.

According to the Presidential Commission for the Study of Bioethical Issues' publication "Privacy and Progress in Whole Genomic Sequencing," one of the greatest concerns of the collection of genomic data is this: "Because whole genome sequence data provide important insights into the medical and related life prospects of individuals as well as their relatives—who most likely did not consent to the sequencing procedure—these privacy concerns extend beyond those of the individual participating in whole genome sequencing...data gathered now may well reveal important information, entirely unanticipated and

unplanned for..."

Another privacy concern listed includes the potential for unauthorized access to and misuse of information. The example given is someone picking up a discarded coffee cup, sending the cup and saliva from the cup to a commercial lab to try to find out the person's predisposition of a neurodegenerative disease, and using it in a custody dispute, or exposing it on social media to embarrass the individual or "adversely affect that individual's chance of finding a spouse, achieving standing in the community, or pursuing a desired career path" or worse, using it as blackmail.

You might not have control over some collection of your DNA, but you do have control of giving your genomic information to commercial entities. Before you do, consider the impact of sharing your DNA with commercial entities and find out what you are consenting to before you send it. Your genomic information includes information about your family members too, so your decision may affect others. Be educated on how your genomic information will be used, sold, or disclosed before you send it off and consent to its unlimited use. It may affect you or your children in the future.

— Linn Foster Freedman

UPCOMING EVENTS

Authors' Events

In addition to their legal practice and involvement with the blog, our Data Privacy + Security Team members regularly serve as presenters at topic-related seminars, and participate on panels that discuss developments in the area. Following, are several upcoming speaking engagements:

- June 15 - New England Fuel Institute's VISIONS Conference (Linn F. Freedman)
- June 21 & 22 – Cloud Financial Services USA Conference in New York City (Richard M. Borden)
- June 22 – National Scholarship Providers Association in Rocky Hill, CT (Linn F. Freedman)
- June 23 – MCLE: Data Security 2.0: The Cloud, Mobile Devices & Encryption Webcast Panel (Kathleen M. Porter)
- July 11 & 12 – Seventeenth Annual Institute on Privacy and Data Security Law (Kathleen M. Porter)

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.