Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

July 14, 2016

CYBERSECURITY

Hackers Using Cyber Weapons to Attack IT Systems

A depressing new report by security firm LightCyber opines that hackers are using cyber weapons to evade detection when deploying attacks to IT systems rather than malware. In fact, the report says that cybercriminals are using sophisticated tools and cyber weapons to compromise networks and exfiltrate data once they use malware to access the system.

Although malware is used to intrude into the system, it is not used in the active phase of an attack. Once hackers use malware to intrude into the system, they are then using other tools to gain control of the compromised system to expand their access throughout the system to take over more machines and access data of the victim company.

According to the report, 99 percent of "internal network reconnaissance and lateral movement" once the hackers gain access into the system originates from the use of legitimate applications, such as scanner and riskware to access data and move throughout the system. This is how the hackers are able to have undetected access in a system for months, or even years. It also enables the attackers to have access to the system even *after* the malware is removed from the system. Sigh.

Even more depressing is the conclusion of LightCyber that the hackers are exploiting Chrome, Internet Explorer, and Firefox for command and control activity once they are successful in using malware to get into the system. Another disappointing conclusion of the report states that malware detection tools are "almost entirely fruitless" once access is successful.

So now what? According to the report, the final conclusion is this: "[T]o thwart attacks, organizations need to effectively monitor the entire 'attack kill chain.' By implementing defense-in-depth based on detecting anomalous attack behavior as well as enforcing perimeter and endpoint prevention, organizations can stop the attacker at any stage of an attack and make sure that if one safeguard fails, another one can prevent a costly breach." Bottom line? It is important to implement tools to detect malware and other tools that are enabling hackers access into, and movement throughout, an IT system.

— Linn Foster Freedman

ENFORCEMENT + LITIGATION

Federal Government and Their Contractors Immune from TCPA Restrictions

On July 5, the Federal Communications Commission (FCC) released an opinion stating that robocalls made by the federal government (or its contractors) are exempt from the Telephone Consumer Protection Act (TCPA). Because the federal government does not meet the definition of "person" under the TCPA, the federal government and its contractors who are complying with the government's instructions do not need to worry about TCPA restrictions. "Person" includes individuals, partnerships, associations, joint-stock companies, trusts, and corporations—no mention of the federal government.

Specifically, the FCC said, “Our clarification comports with congressional intent and advances the public interest. As noted, there is no evidence in the text or legislative history of the TCPA that Congress intended to restrict federal government communications, and we agree with members of Congress that the goal of the TCPA has never been to impede communications from the federal government, especially those that gather data for important government research.” This decision stemmed from the U.S. Supreme Court’s decision in *Campbell-Ewald Co. v. Gomez*, where the court held that the United States and its agencies are exempt from the TCPA’s prohibitions.

In its opinion, the FCC specifically noted that this ruling does not make robocalls made by state or local governments (or their agents) exempt from TCPA requirements nor robocalls made for political campaigning. However, the FCC did carve out an exception for tele-town halls when used by federal legislators or their agents, research survey calls made by the federal government, or calls provided by the National Employment Network Association.

— Kathryn M. Rattigan

DATA BREACH

Omni Hotels Latest Hotel Chain Hit with Malware

Omni Hotels notified guests on Friday, July 8, 2016, that its point of sale systems were compromised with malware from December 23, 2015 through June 15, 2016.

The compromise affected approximately 50,000 guests who used their credit and debit cards at 49 of its 60 locations. The information included names, credit and debit card numbers, expiration dates, and security codes.

Omni has warned its customers to watch their bank statements carefully. It is offering one year of free identity theft and repair services to affected guests.

— Linn Foster Freedman

Wendy’s Reports over 1,000 Restaurants Affected by Breach Announced Earlier This Year

In May of this year, Wendy’s reported “fewer than 300” locations had been hacked by malicious malware that targeted customer credit card information. Last week, Wendy’s released a list of 1,025 restaurant locations that were affected by the data breach.

The breach originated from a compromised unnamed third-party “service provider.” The attackers were able to use the service provider’s credentials to access and install malware into the credit card systems of the restaurant, also known as the point-of-sale systems. As a result, the attackers had access to customer credit card information, including names, credit card numbers, expiration dates, and security

codes.

The investigation is still ongoing and it is possible other restaurant locations may have been hacked. The "service provider" is still unnamed, and it is unclear if other businesses are at risk.

Wendy's is offering fraud counseling and identity restoration services for customers who used a credit card during the time of the breach at one of the listed restaurant locations. The full list of restaurant locations affected by this breach can be accessed here.

— Kathryn M. Rattigan and summer associate Leonel Gonzalez

DATA PRIVACY

EU-US Privacy Shield for Transatlantic Data Transfers Finalized

This article co-authored with guest blogger Peter Wainman, a partner with Mills & Reeve LLP

Transfers of personal data from most European countries to the U.S. have been exposed to legal attack since October 2015, when privacy campaigner Max Schrems successfully sued the Irish authorities over data transfers made by Facebook Ireland. The main objection with the Safe Harbor was that transferring EU citizens' data to the U.S. subjected the data to the U.S. government's bulk surveillance.

That David-and-Goliath litigation saw the end of the "Safe Harbor" decision protecting transatlantic data flows when the European courts declared it invalid. While other legal methods of data transfer are available, the Safe Harbor was widely relied on especially by technology businesses.

A New Privacy Shield

Since then, the EU and U.S. authorities have been working on a replacement—the EU-US "Privacy Shield." After a first attempt was rejected by national and EU regulators, a tightened-up version has now passed the test. The U.S. Department of Commerce has a useful fact sheet and a guide to certification available on its website. Likewise, the European Commission's press release and FAQs document provide a helpful summary.

The revised version of the Privacy Shield consists of: an adequacy decision describing the system of self-certification through which U.S. organizations commit themselves to a set of privacy principles; and a set of seven Annexes dealing with the arrangements that the U.S. authorities will implement to safeguard EU citizens' data.

U.S. companies will be able to self-certify with the U.S. Department of Commerce beginning on August 1. There will be an annual joint review process to check that the system is working.

Certainty offered by agreement of the Privacy Shield has been widely welcomed. The Privacy Shield requires the creation of a new U.S. authority intended to address concerns of EU citizens about U.S. government surveillance. However, this may not be the end of the story. Max Schrems, the activist responsible for the demise of its predecessor, has told journalists that Privacy Shield is full of holes and as such is likely to fail a legal challenge—although he does not want to be the one to bring it.

What Does This Mean for the UK?

The UK privacy regulator, the ICO, has indicated that it will press for UK laws to track those of the EU.

It may be that the UK will adopt most of the changes due to take effect in 2018 under the GDPR but leave out some of the more onerous obligations that could impede the activity of SMEs, for example. If the UK ends up with a relatively distant relationship with the EU compared to an EEA member like Norway, privacy laws could diverge. In that case, the UK will have to demonstrate adequacy of protection for European citizens' privacy, like the US has done, if it is to do business freely across Europe.

— Kathleen M. Porter and Peter Wainman

HEALTH INFORMATION PRIVACY

CMS Allows Qualified Entities to Sell Claims Data

The Centers for Medicare and Medicaid Services (CMS) released a final rule permitting "qualified entities" to sell Medicare claims data to providers and others for use in improving quality of care. The rule expands on CMS's Qualified Entity Program, which permits organizations to apply to become qualified to receive Medicare Parts A, B, and D claims data to evaluate provider and supplier performance and produce public reports regarding such performance. Qualified entities are subject to a number of requirements to participate in the current program, must enter into a data use agreement with CMS, pay a fee for the data, combine the data with non-Medicare claims data, and restrict use to evaluating the performance of providers and suppliers. Under the final rule, qualified entities are permitted to use combined data to perform nonpublic analyses for care delivery and quality improvement functions and to sell or otherwise provide these analyses to "authorized users" such as providers and employers.

The final rule imposes several privacy and security requirements on qualified entities that sell or provide analyses and data to authorized users. For example, qualified entities that are covered entities or business associates under HIPAA will be required to comply with applicable requirements of HIPAA. In addition, qualified entities will be subject to an assessment if patient-identifiable data is improperly disclosed by the entity or an authorized user. According to the CMS press release, the expanded information sharing permitted under the final rule "is part of a broader effort by the Obama Administration to use data to help create a health care system that delivers better care for patients, spends dollars more wisely, and results in healthier people."

The final rule becomes effective on September 6, 2016.

— Pamela Del Negro

DRONES

Drone Mapping the Way of the Future for Insurance Companies

Drone mapping provides insurance companies with an easy, fast, and accurate method of documenting a scene and preserving key details while also letting the process of cleanup and reconstruction to begin as quickly as possible. Recently, Dronotec, a start-up company specializing in drone inspection for insurance companies, conducted a case study to determine just how much money this drone mapping was saving insurance companies. Dronotec's founder, Emilien Rose, worked as a loss assessor in France and Australia for 10 years and conducted assessments of about 8,000 claims. Rose believes that Dronetec and drone mapping can really save time and money for insurers.

For example, recently a fire in France consumed five acres of a vacation destination on the coast. Once the insurance company came in to assess the damages, they realized that the sheer size of the site

posed quite a challenge. Moreover, so much of the property was damaged by the fire, inspectors could not enter the properties or inspect the roofs without the threat of personal injury. A plane attempted to capture photos, but many of the photos were not clear or sharp enough to use. However, the loss adjuster recommend a drone to do the mapping of the scene. In about 10 minutes, the drone collected more than 300 geo-tagged photos flying about 180 feet over the property. The images were uploaded to a drone-mapping program, and three hours later, a 2-D map and 3-D model of the property and the damages were available. The high degree of accuracy of not only the photos but also the mapping improved the likelihood of identifying the cause of the accident exponentially. The insurance company's team members were able to collaborate and review the mapping in one cloud-based space. In this one case, the use of drone mapping saved this French insurance company about €99,985,000 (or about $110,600,000).

The ability to quickly process claims is very helpful to insurance companies with large scale disasters that have many claims filed related to the same incident.

Rose's study not only supports the effective use of drone mapping but also suggests that maybe insurance companies can start using drones not only for mapping incidents but also to inspect properties and verify risks before issuing insurance. Insurance companies can then work with their prospective customers to mitigate risks and hopefully prevent disasters from even occurring.

Perhaps it is tools like this that have led to the boom of testing and research of drones by insurers in 2015 and this year too. Numerous insurers received Federal Aviation Administration (FAA) drone exemptions in 2015. Exemptions have been granted for activities that include, among others: (1) aerial data collection in support of inspections for insurance underwriting and claims adjusting, and (2) research related to the use of drones for insurance functions including using drone imagery in re-underwriting, catastrophe response, roof inspection, and claims resolutions settings.

The exemption from FAA regulations permits insurers to more efficiently test small drones. Insurers receiving the exemption may fly drones during the day within the line of sight of a trained pilot and air crew, thus avoiding the need to perform test flights at FAA-approved sites. Other insurers received exemptions allowing the insurers to begin operating drones in catastrophic situations. Pending amendments to the current regulations that, if passed, benefit insurers include suspending federal restrictions and requirements that limit the use of drones post-disaster. The passage of this amendment would permit insurers to quickly respond when access to the site of a catastrophe is limited.

And as we previously wrote, the FAA Part 107 final regulations for commercial drones, which will take effect in August, may have a further impact on the insurance industry. However, it is unclear what, if any, impact it will have on the insurance industry other than that drone owners will need to insure that they have proper insurance coverage. At least one insurer has already introduced a policy for drones that covers the pilot, non-pilot "crew," property damage and optional "war, hijacking and terrorism".

Legislative and regulatory activity regarding drones continues to be vigorous at both the federal and state levels.

This post is also being shared on our *Property Insurance Coverage Insights* blog. If you're interested in getting updates on developments affecting insurance coverage, we invite you to subscribe to the blog.

— Kathryn M. Rattigan and Carrie C. Turner

PRIVACY TIP #43

Pokémon Players: Beware

Pokémon GO has been downloaded 7.5 million times in the U.S. alone. It has been reported that it has surpassed Twitter. If you are enjoying the game, you should know how it is collecting and using your information.

How safe is your information? And where is your information (especially your geolocational data) really going? The augmented reality game uses your device's microphone, camera, GPS, and mobile network to pinpoint the location of the player. The game uses the location to display a map of the surrounding area where players can capture Pokémon, collect items, or fight in "gyms." Once the player finds a Pokémon, the game may use the device camera to display the Pokémon in an augmented reality mode.

While the player walks around trying to achieve the dream of becoming a Pokémon master, the game is collecting your data. It knows where you are, can listen to your conversations through the microphone, and is gathering information on the type of device you are using and where you are while you play the game. The data is then collected and stored by Niantic Inc. (Niantic), the developer of Pokémon GO.

According to the privacy policy, the data is used to "improve and personalize" services provided by Niantic. However, the policy also allows Niantic to provide the data to third parties for the purpose of "research and analysis, demographic profiling, and other similar purposes." It is worth noting Google is a major third-party backer of Niantic and Pokémon GO.

Niantic is also allowed to provide information to government or law enforcement officials. The policy states the following:

"We may disclose any information about you (or your authorized child) that is in our possession or control to government or law enforcement officials or private parties as we, in our sole discretion, believe necessary or appropriate to: (a) respond to claims, legal process (including subpoenas); (b) protect our property, rights, and safety and the property, rights, and safety of a third party or the public in general; and (c) identify and stop any activity that we consider illegal, unethical, or legally actionable activity."

The game has even caught the attention of Senator Al Franken, chairman of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law. On July 12, Senator Franken wrote to Niantic CEO John Hanke with concerns on how Niantic plans to use data collected from Pokémon GO players.

Specifically, the senator requested information on what steps Niantic is taking to inform and receive consent from parents about how their child's data is being collected. The letter also inquired into the identity of Niantic's current "third party service providers," which information collected is necessary to improve Niantic's services, and how Niantic is working to fix a mistake that allows the app full access into a user's Google account on IOS.

A PDF of the Senator's letter can be read here.

There is no mention of what Niantic does with data collected from the camera or microphone of the devices. The lesson here is to read the privacy policy for each and every app that you download to your device. The full privacy policy can be accessed here.

— Linn Foster Freedman, Kathryn Rattigan, and summer associate Leonel Gonzalez

---

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:

- August 10 – NSPA Regional Meeting in Washington, D.C. (Linn F. Freedman)
- September 12 - 15 – (ISC)² Security Congress in Orlando, FL (Linn F. Freedman)
- October 11 & 12 – InfoGovCon in Providence, RI (Linn F. Freedman)
- October 24 - 26 – Privacy + Security Forum in Washington, D.C. (Linn F. 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.