Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Locky Ransomware Variant Difficult to Detect

We previously warned readers about the Locky ransomware, which is potent and designed to use phishing emails to lure users to click on links and attachments, including pdfs.

Now, researchers at Cylance have discovered that a new Locky variant, known as Diablo6, is a variant of Locky but much more difficult to detect. According to the researchers, Diablo6 attacks users twice—the first time in the traditional way—through a phishing email that includes a zip file containing ransomware. When it is opened, the file contains a VBS file that attempts to connect to Locky's command and control server for instructions. Then, the VBS script downloads the ransomware. *Read more*

Do You Have "Security Fatigue"?

Every day it seems a new data security breach has occurred or a new "cyber hack" is in the news,—making us run to our phones, computers, bank accounts, you name it, to see if we could be the "one" affected. As a result, more and more online transactions, websites, and financial institutions, for work or personal use, require longer and more complicated login user names and passwords. I can barely remember my name as it is….let alone the now at least 25 unique user names and passwords I have to keep in a notebook. I have security fatigue!

Defined by the National Institute of Standards and Technology (NIST), security fatigue is a weariness or reluctance to deal with computer security, leading to feelings of resignation and loss of control. "These reactions can lead to avoiding decisions, choosing the easiest option among alternatives, making decisions influenced by immediate motivations, behaving impulsively, and failing to follow security rules,"—leading to increased risk, which the hackers are taking full advantage of daily. *Read more*

Data Security Top Concern for Higher Education IT

November 16, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Kathleen M. Porter
Joanne J. Rapuano
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Data Privacy
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Professionals

At its annual conference, EDUCAUSE announced the issue at the top of the 2018 Top 10 IT Issues is data security. This is no surprise. It has been the top concern for the past three years.

The issue, as described by IT professionals, was "developing a risk-based security strategy that keeps pace with security threats and challenges." This is difficult in a higher education setting, as the platform used in higher education is so wide and decentralized. Telling faculty and students they have to take extra measures for data security is challenging in an environment that demands easy access and use of IT assets. *Read more*

DATA PRIVACY

Big Data and Antitrust: Rethinking Competition Law in the Data Economy

As we approach the end of the calendar year, traditionally the busiest time for mergers and acquisitions, it is worth revisiting whether our existing competition law framework can and does properly assess the market power of big data.

This spring, *The Economist* magazine joined the ranks of some antitrust regulators, particularly from the EU, in questioning whether today's measures of anticompetitive behavior, even if the proposed activity would result in higher prices or unfair competition, don't really apply to low cost or free products and services offered by Facebook, Google, and other big data companies. Also, many of the proposed merger transactions among data companies occur under the radar because the selling party's balance sheet or its annual revenue falls below premerger review thresholds. Some acknowledge that other antitrust tests may still be relevant, such as evaluating the vertical foreclosure effects of a potential merger between two companies, one that collects consumer data and the other that sells targeted online advertising. The combination could well result in a powerful market player with the ability to deliver targeted marketing to millions of consumers. *Read more*

DATA BREACH

Data Breach Costs an Average of $3.6 Million

There have been a myriad of research studies attempting to come up with the "cost" of a data breach. The most recent, released by AT&T, estimates it costs organizations $3.6 million to recover from a data breach. The AT&T team surveyed 700 IT professionals in all industry sectors and found the biggest risks to organizations continue to be

malware, viruses and worms, unauthorized access to corporate data, and ransomware.

The AT&T cybersecurity insights report, entitled “Mind the Gap: Cybersecurity’s Big Disconnect,” found that IT professionals face skills gaps in threat prevention, threat detection, and threat analysis. Further, and frankly disappointing, only 61 percent of organizations require security awareness training for all of their employees. We have been urging clients to provide security awareness education to employees, especially in light of the increase of malware and ransomware attacks against companies through phishing campaigns. *Read more*

DRONES

Anti-Drone Technology—a Billion Dollar Business?

While unmanned aerial systems (UAS or drones) are banned from flying over military bases, there isn’t much that the military can legally do to stop a drone intruder. However, if the military was given the authority to stop these intruders, surely the market for anti-drone technology and tools would explode. Market research firm Frost & Sullivan estimates that the anti-drone industry is worth between $500 million and a billion right now—and Frost & Sullivan isn’t the only market researcher with that estimate. Other market research firms project that amount to be $1.5 billion by 2023, based largely on military acquisitions. *Read more*

PRIVACY TIP #114

Your Email May Have Been Hijacked and You Don’t Know It

A new study by Google, the University of California Berkeley, and the International Computer Science Institute has concluded that email users are being threatened by massive credential theft, and phishing schemes are the primary way hackers are stealing credentials.

According to the study, phishing victims are 400 times more likely to have their email accounts hijacked compared to regular Google users. Victims of data breaches are 10 times more likely to have their email addresses hijacked, and keylogger victims are 40 times more likely to become victims of email hijacking.

How the attacker acquires the victim’s credentials is directly linked to whether the email account can be hijacked. Seven percent of those whose information was breached in a third party data breach had their gmail account password exposed, compared to 12 percent of keylogger victims and 25 percent of phishing victims.

What this says to me is that it is very important to change your

password to access your email account any time you are advised that you have been involved in any type of compromise. Even if you don't get notice, change the password on your private email account frequently. Remember to use pass phrases, as they are easier to remember [see blog post about passwords here].