COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 1: Summer 2014

TABLE OF CONTENTS

Click on the below title to jump to page

Don't Fear the Zombie Apocalypse -- the (Relatively) New Texas Anti-Botnet Law

By Reid Wittliff

It has been almost five years since the Texas Legislature enacted an anti-botnet law, Texas Business & Commerce Code § 324.055, to combat botnets on the Internet. But as of the date of this writing, there are no reported Texas cases interpreting the law, and botnets continue to be as big an online scourge as ever.

Just this June, the FBI and DOJ announced the take down of the GameOver Zeus Botnet, a particularly pernicious botnet designed to steal banking credentials from infected computers or install "ransomware" to encrypt users' files until a ransom is paid. *See* FBI News Release, June 2, 2014, http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

The anti-botnet law seeks to combat just this sort of organized army of hijacked computers. The anti-botnet law makes it illegal to:

- make or offer to make another person's computer a "zombie" or part of a botnet
- knowingly create, use or offer to use a botnet or zombie to:
    - send spam
    - send signals to other computers to cause a loss of service (i.e., a denial of service attack)
    - send data from a computer without authorization from the computer's owner
    - forward computer software designed to damage or disrupt another computer or system
    - collect personally identifiable information
    - perform an act for another purpose not authorized by the owner or operator of the computer

Tex. Bus. & Comm. Code § 324.055(b),(c)(1)-(6).

Zombie computers are one focus of the law, and, perhaps unique to Texas, Texas now has a legislatively enacted definition of "zombie." "Zombie" means: a computer that, without the knowledge and consent of the computer's owner or operator, has been compromised to give access or control to a program or person other than the computer's owner or operator. Tex. Bus. & Comm. Code § 324.002(9). The definition adds considerable reach to the law, because

any computer that has been "hacked" such that the hacker has access to the computer is, by definition, a zombie.

In my practice, I frequently receive inquiries and handle matters regarding computer intrusions. A typical matter involves the legality of one spouse secretly installing a commercially available spyware program like SpectorSoft on the other spouse's computer and using it to record emails, web surf sessions etc.

Consider the following scenario -- one spouse (who we'll refer to as the "second spouse") becomes suspicious that the "first spouse" is having an affair. To find evidence of the affair, the second spouse secretly installs SpectorSoft on the first spouse's computer. The second spouse proceeds to use SpectorSoft to collect emails and reports of web usage from the first spouse's computer, usually by causing SpectorSoft to send reports to the second spouse without the first spouse's knowledge.

It seems clear that under the statutory definition of "zombie," the first spouse's computer (infected with SpectorSoft) is a "zombie," because SpectorSoft enables access to the computer by the second spouse without the first spouse's knowledge and consent. A violation of the statute is established when the second spouse uses SpectorSoft on the first spouse's "zombie" computer to send data (emails and web surfing sessions) without the first spouse's knowledge or consent. Tex. Bus. & Comm. Code § 324.055(c)(3). A violation also occurs because the second spouse created a zombie by installing SpectorSoft on the first spouse's computer. Tex. Bus. & Comm. Code § 324.055(b).

But can the first spouse sue the second spouse under the anti-botnet law? Or is the first spouse relegated (as with many other laws targeting malicious online activity) to filing a report with law enforcement or the Attorney General and waiting for these government officials to take action?

The answer is that the first spouse can sue if they can show they incurred a loss or disruption of the conduct of their business. The statute says the following persons have standing to pursue a civil action under the statute:

- persons acting as an Internet Service Provider (broadly defined as a person "providing connectivity to the Internet or another wide area network) whose network is used to commit a violation of the act
- a person who has incurred a loss or disruption of the conduct of the person's business, including both for-profit and not-for-profit activities as a result of a violation of the act

Tex. Bus. & Comm. Code § 324.055(e).

So in my example, if the first spouse could show they incurred a loss or disruption of their business as a result of the second spouse's use of SpectorSoft, they likely could bring a claim under this provision.

"Loss," however, is not defined. It is not clear if the legislature meant to limit "loss" to only a direct economic loss or whether a less direct loss, like expenses incurred to hire a computer forensic expert, or an even more intangible loss, such as a loss of privacy, would qualify as a "loss" under the statute. Hopefully, issues like these will begin to work their way into reported decisions as more claims are filed under the anti-botnet law.

And more claims should be pursued, as the law's allowance of generous statutory damages creates strong incentives to assert anti-botnet law claims. The law provides that violators can be forced to pay **statutory damages of $100,000.00 for each zombie** used to commit a violation and further that these damages can be **trebled** if a court finds violations have occurred with such frequency as to constitute a pattern or practice. Tex. Bus. & Comm. Code § 324.055(f)-(g). In addition, a prevailing plaintiff can obtain attorneys' fees and costs.

The meaning of this part of the law is clear: every additional zombie involved adds the potential of an additional $100,000 in statutory damages. In other words, if you are plaintiff's counsel in an anti-botnet case, you *want a zombie apocalypse*, because if thousands of hijacked, zombie computers are involved, the potential statutory damages are stratospheric!

This statutory damages provision might significantly impact even garden-variety computer intrusion cases. This is because it may be possible to recover a sizable statutory damages award, even when actual damages are minimal or hard to prove.

Actual damages are often minimal or hard to prove in a typical computer intrusion case. Take for example the spying spouse scenario -- the second spouse has egregiously violated the privacy rights of the first spouse, but may not have caused the first spouse any economic harm. Hence, any claim for actual damages may not merit litigation. But if the first spouse can recover $100,000.00 in statutory damages plus fees and expenses, litigation might be financially justified.

Whether such statutory damages are available in these types of cases will likely turn on courts' interpretation of "loss" as used in the statute. Of course, the best way to get judges to decide what "loss" means is to squarely present the issue to them in cases brought under the anti-

botnet statute. For that, we need more anti-botnet law cases. And you know what that means . . . more zombies. Don't fear the zombie apocalypse!

About the Author

Reid Wittliff is a technology lawyer with a deep understanding of the fast-developing law governing online activity, privacy and data security. He has represented both fortune 100 companies and small start-ups in technology and intellectual property disputes. He also frequently negotiates and drafts software licenses and other technology contracts. He is a certified mediator. Reid's prior experience includes serving as the founding Division Chief of the Texas Attorney General Office's Computer Crime Division and as a federal prosecutor responsible for leading computer crime investigations and prosecutions in the Dallas, Texas area. In 2008, Reid founded R3 Digital Forensics, LLC as an independent company to provide digital forensics and e-Discovery services to clients throughout the nation.

Dealing with Digital Detractors – A New Ethics Trap for Divorce Lawyers?

By John Browning

Ah, the good old days – when dealing with an irate client meant fielding a few angry phone calls or responding to a curt letter informing you that your services were no longer needed. You moved on, presumably the client moved on and that was usually the end of it. But in today's digital age where everyone is just keys away from airing their grievances with the world, comments posted to lawyer ratings sites like AVVO.com or even consumer complaint sites like Yelp! or RipoffReport.com can live online forever and pop up in response to internet searches of your name. As with any criticism, there's a right way and a wrong way to respond – and the wrong way can land you in front of the disciplinary board.

Chicago employment attorney Betty Tsamis learned this lesson the hard way in January 2014, when she received a reprimand from the Illinois Attorney Registration and Disciplinary Commission for revealing client confidential information in a public forum. Tsamis had represented former American Airlines flight attendant Richard Rinehart during late 2012 and early 2013 in an unsuccessful quest for unemployment benefits (Rinehart had been terminated for allegedly assaulting a fellow flight attendant during a flight). After firing Tsamis, Rinehart posted a review of the lawyer on the attorney review site Avvo.com. In the post, Rinehart expressed his dissatisfaction bluntly, claiming that Tsamis "only wants your money," that her assurances of being on a client's side "is a huge lie," and that she took his money despite