Q&A: FBI agent fights cyberattacks on corporate America

September 27 2013, by Andrew Tangel

Corporate America has increasingly found itself under siege by hackers backed by organized criminals and foreign governments alike.

A group called the Syrian Electronic Army claimed responsibility for knocking the New York Times' website offline for nearly two days. And in recent months, major U.S. banks have withstood a barrage of "distributed denial of service," or DDOS, attacks aimed at crippling their websites or worse.

The high-profile computerized assaults in the past year have highlighted the digital age's vulnerabilities, coming in an era when a message sent via a hacked Twitter account can roil the stock market and a runaway trading program can nearly kill a Wall Street firm.

On the front lines of this battle is Austin Berglas, assistant special agent in charge of the FBI's cyber branch in New York. Agents under his command handle major cyber cases and support other computer-intensive FBI investigations.

Cyberattacks have grown so exponentially, Berglas says, that there are basically two types of firms these days: "Those companies that have been hacked, and those that are going to be hacked again."

The Los Angeles Times recently sat down with Berglas. Questions and answers were edited for length and clarity.

QUESTION: What's the one emerging cyber threat on your radar that is the most alarming? What keeps you up?

ANSWER: Destructive capabilities of certain nation-states.

Q: How have you seen that evolve or intensify in the last year?

A: We see them scanning, looking for vulnerabilities. And then we see certain nation-states DDOS-ing, looking to create that annoyance and push the red line, to see how far the United States government will go before we strike back or what can be done politically. But knowing that these nation-states have the capability to do destructive activity is the most concerning out there. Whether they've done it or not is irrelevant to me.

Q: Given the growth of cyberattacks and crimes hitting major U.S. banks and Wall Street firms, how worried should average Americans be about the safety of their savings and investment accounts?

A: As long as these major financial institutions are making customers whole - so that if someone gets their bank account compromised, and the company is accepting losses and making them whole - that would comfort me as a consumer. ... But that's not to say that, down the line, maybe banks are going to determine that if it's the end-user's responsibility - i.e., they click on some sort of malware or fall victim to a phishing scheme - then maybe they're going to hold that individual responsible.

Our message always boils down to everybody protecting themselves while on the Internet. ... The No. 1 vector of attack for these bad guys is social engineering - the spear phish, the phishing emails (aimed at stealing user names, passwords and credit card information). ... It's the path of least resistance.

Q: To what extent have attacks on financial institutions grown over the last year?

A: An attack on a major company on Wall Street - a trading company or one of these major financial firms - to take one of them down and to disrupt the country's economy is basically a terrorist attack. It's increasing ... with certain nation-states that there are tensions with. Cyber is a way that you can push those red lines and test everybody's buttons without physically having somebody here on the ground to blow that building up.

Q: How close have hackers come to breaking into the core trading platforms of Wall Street exchanges and brokerages?

A: Cannot even touch that one.

Q: The FBI recently took part in a major Wall Street trade group's cyberattack war game called Quantum Dawn 2. How did the exercise go and what did the FBI learn?

A: I was not personally there; I sent a couple of my supervisors down. But what Quantum Dawn 2 showed was the importance of that joint private-sector/law enforcement relationship in all phases of cybersecurity, not only (during) actual incidents ... where of course we're going to be talking constantly, but leading up to it.

Q: Starting late last year, we've heard a lot about distributed denial of service attacks on major U.S. banks, but what can you tell us about actual break-ins to bank systems and thefts of funds? How often are external hackers able to break in and steal money?

A: Not able to talk about the recent (DDOS attacks). ... But historically, yes. We've had lots of instances where DDOS attacks were used to

penetrate banking systems by shutting down the online banking platforms and then doing injections into the network and gaining access while that DDOS was (underway).

Q: Are U.S. companies fighting back - or trying to - against cyberattacks now? If so, how, and what's the FBI's advice to companies looking to take matters into their own hands?

A: We call it "hack back." ... "Hack back" is illegal, and if companies are found to take matters into their own hands, there is a large possibility they will be criminally prosecuted by the Department of Justice.

Say if some financial company is being DDOS-ed so much and they know the (IP addresses) that it's coming from, and they decide to do something to take out the infrastructure that's doing it, they don't know what that infrastructure is. It could be legitimate infrastructure that's being used for nefarious purposes (unbeknownst) to the person that owns the infrastructure.

If it's in the United States, and that company hacks back and tries to blow up the box that's attacking them, what are they blowing up? Are they blowing up some other company's infrastructure? ... Or, worse, it could be the box is international and ... you're probably violating international law as well. So now you've got a whole host of problems. I've been asked this by a couple of companies recently, and the answer is backed by the Department of Justice, especially (federal prosecutors) here in the Southern District (of New York), that they are poised to prosecute.

Q: How many major U.S. companies still aren't taking cyber threats seriously? Have you seen any glaring lapses in cybersecurity?

A: No, I think it's pretty well-known out there. There really aren't too

many companies we've dealt with in the past year that have been blind to this. Do we have recommendations for how they can do things better? Yes. But no, there haven't been any instances where someone is just totally disregarding the threat. I don't think they would exist anymore, really.