The global capital markets are highly vulnerable to cyber attack…and Greece could be the warm-up

Posted on **September 9, 2015** by **Bil** — **No Comments ↓**

By: John Edge

Because my roles have always involved new technologies applied to existing markets, I've been trained to think about technology related governance and risk; now as I look to a future of affordable mass compute power and artificial intelligence driven threats, I can't help but think of where the weak points may be. And my hunch leads me to places where both manpower and system power may be depleted. And there's an obvious one right now. The Greek capital markets. My gut tells me that Greece could be the warm up for an attack on the system integrity of capital markets.

I know that this is an odd statement to make, given that capital markets do not have systemic risk weak points and are designed to be resilient to cyber attacks – theoretically invulnerable to all comers. But, instinctively, we all know that this cannot be the whole story – that risk cannot be entirely eliminated and that where there is human life, things can go wrong. So, the question is – how bad could it get?

The truth is: bad, very bad. In theory, global collapse of hitherto unseen proportions.

Automation of the capital markets infrastructure started in the 80's, as technology evolved. Both performance and price created the opportunity to splice automated functions into what were once manual processes. This concept of splicing is essential to understanding where we are today, in that we did not design for an end goal, we designed for what worked in the here and now.

As such capital markets grew organically from a technology point of view, with layer after layer of systems being built, duplication and overlap were created, whereby systems ran out of capability and were patched back together or replaced, often partially,

Throughout the 90's and early 2000's the rate of adoption of technology accelerated, driven by the relentless hustle to hit quarterly targets. Machines were built to trade millions of times a second, competition for trading flow at the exchange level was opened up, so exchanges were driven to advance their technology to stay competitive, which meant more machines were built. The cycle has continued at this pace and now extend to retail and commercial banking, with digital demand from customers driving the transformation of these markets.

Then we introduced cloud computing, which offered the opportunity to increase performance and scalability whilst reducing cost. So markets took a complex organic system and started to distribute it, across internal and external data centers plus service providers. Vendor technologies exploded in popularity; the age of ‘FinTech’ was born, bringing substantial advantages to market participants. Marvelous progress indeed.

However, much as it’s a downer – sometimes the ‘bear view’ needs to be considered. What does the bear view show us?

Starting with the basic truth that old code often has holes in it and modernizing code is essential to system health. Ah ha – you say – simple. Just modernise the code, and everything will be fine. But here’s the rub: Modernising code costs money. Which eats into quarterly returns, making it somewhat unattractive to those who make the decisions. “Heigh-ho,” they may say. “Let’s just hope the thing doesn’t break down on my watch.”

The next layer up is the compilation of the systems and the architectures in place; were they designed for entities with malicious intent? Entities armed with, thanks to a Mr. Moore and his law, low cost massive computer power? The answer is, of course not. Some of the newer types of cyber attack couldn’t have been conceived of when these systems were build. That’s criminal ingenuity for you.

So, with aging code bases and system architectures not designed to resist the kind of power modern cyber threats at large have, we at least have well trained teams operating in a coordinated fashion globally to manage this fragile ecosystem. Oh wait, nope… we don’t have that either.

For a “mini” taste of how things can go wrong, there’s the bankruptcy of Knight Capital, caused by a rogue algorithm, a human ‘non malicious’ error that went undetected, which turned the largest trader in US equities into rubble in a little under a week. Then there were the SIP issues with NASDAQ that shut off that market, and all other markets, for a large part of a trading day. Most recently we have seen glitches with NYSE.

All three of these crises, which were nothing on what could happen on a global scale, were created by human error and are in practice being addressed through Reg SCI. These incidents are indicative of what occurs when critical systems fail in capital markets. The elephant in the room is the possibility of a malicious attack. Because that’s going to be worse than anything human error could cause.

Let’s, for a moment, create a nightmare scenario. How could that come about and what would be the effect?

Imagine a powerful group looking to insider trade, which is trading with non-public information. This group decides to create the non-public information by shutting down a stock exchange for two days. The night before the attack the group buys options contracts that will pay off, if the market moves down. When they shut down the market for two days, panic ensues and the market “sells off”.

Of some comfort is that the fictional baddies might be deterred by the fact that if the plan could go horribly wrong for them – the futures position may go against the intent and lose the monies deposited as margin.

Currently, all businesses in Greece are suffering a high amount of disruption. What we know is that often it is human error that causes problems, rushed code releases and poor processes creating production issues. The duress being suffered by business operators in countries such as Greece could increase the likelihood of human error.

But on top of this, opportunistic criminals could use these markets as a training ground – a ‘cyber attack gym’. The functional layout of capital markets is roughly the same everywhere, although the volumes change significantly between countries. Could the current Greek crisis present an opportunity for practices attacks, and would the operators, in the current state of chaos, even know this was occurring?

There are global automated market places that have not trained enough people to operate information security defenses. Systems have been developed to aid humans in the management of security perimeters, however standards and processes have not yet been developed for many smaller market places.

On top of these challenges there is the issue of system re-engineering, the moving from the organic spaghetti infrastructure to an infrastructure designed for today’s environment. Which all comes down to budget.

Chewing the fat with my friend and colleague Alexei Miller, a managing director at global technology consulting firm, DataArt, he pointed out that chaos always begets criminal creativity and that Greece was that chaos. Cheaters, he said, will look for ways to circumvent capital controls. He noted that if the Greek situation were happening in certain other countries (and he didn’t say which) and Europe was sending massive checks to keep them afloat, the biggest question would be how much of it would be stolen.

It is true that technology fosters spending accountability. But when it is left to tick along, in the way the global capital markets technology often is in many places and organisations, it can be a force for evil.

Sleep tight. Don't have nightmares, now

John Edge is an innovator and social entrepreneur in the digital economy, with a recognized expertise in financial technology and a track record of creating breakthrough business models by harnessing network capital to identify patterns created by market needs, inefficiencies and new technologies. With the mission to create value for individuals, corporates, investors and society. He is an advisor to global technology consulting firm, DataArt. (234)

Original article — http://digitalforensicsmagazine.com/blogs/?p=771