the Availability Digest

www.availabilitydigest.com

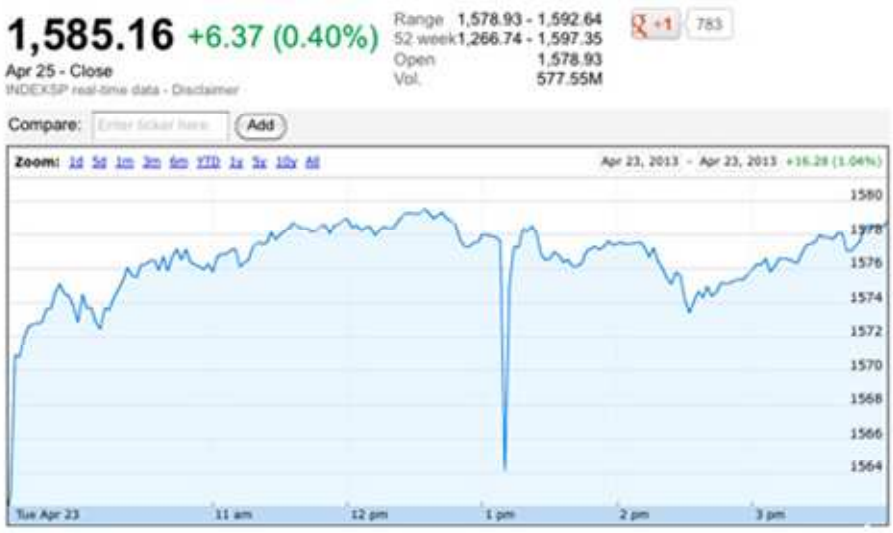
Hacked AP Tweet Crashes Markets

May 2013

On Tuesday, April 23, 2013, an Associated Press (AP) tweet reported that President Obama had been injured in an explosion at the White House. It sent the U.S. financial markets into an instant tailspin. Fortunately, the tweet was false. The AP Twitter account had been hacked. However, what does this mean for "flash crashes" in the future when unverified and perhaps malicious information is disseminated via social media?

The False Tweet

A little after 1 PM EST on April 23rd, the AP twitter feed @AP reported "Breaking: Two Explosions in the White House and Barak Obama is injured." The stock markets reacted instantly. Between 1:08 and 1:10 PM, the Dow Jones Average dropped 143 points. The S&P lost 1%. Almost $2 billion in the market value of securities evaporated.



Google Finance

Within minutes, AP issued a retraction via another Twitter account saying "The @AP Twitter account has been suspended after it was hacked. The tweet about an attack on the White House was false." The AP also used its Web site and blogs to inform its followers about the hacking. However, the tweet had already been seen by many of AP's two-million followers. Almost 1,500 followers re-tweeted the tweet.

Following AP's retraction, the markets recovered in minutes. During the peak of the crises, though, trades were delayed up to four minutes by the heavy trading volume. This was perhaps fortunate, since many of

the panic orders that were placed as a result of the false tweet were never executed. The drop in the market could have been much worse.

It was not only the equities markets that suffered. All of the U.S. financial markets fell, including bond markets and commodity markets.

An organization calling itself the Syrian Electronic Army, a supporter of Syrian President Bashar al-Assad, claimed responsibility for the hacked tweet. The FBI and securities regulators such as the Commodities Futures Trading Commission (CFTC) are investigating, along with AP and Twitter.

People or Computers?

How could major markets react so swiftly to such bad news? Were thousands of traders hovering over their trading terminals watching news reports and ready to hit the sell key?

Not likely. The AP launched an instant investigation and noted that only computers could react this quickly. High-speed trading has become the norm in the markets. Powerful computers located next to the exchanges to minimize network latency place thousands of orders each second, most of which are not executed, in an attempt to gauge the market and make rapid trades worth pennies. In 2012, 50% of all trades were executed via high-frequency trading.

These computers use highly sophisticated algorithms to maximize trading profits. Some of these algorithms follow news stories and other social media such as Twitter looking for buzzwords. They react instantly to good or bad news. In this case, they reacted with great alarm to some serious bad news. They then reacted with supreme optimism when the good news about the hack came out.

How Did @AP Get Hacked?

AP was already aware that hackers were making repeated attempts to steal passwords of AP journalists.

On the day in question, the hacking was preceded by a “phishing attempt” when journalists received an impressively disguised email encouraging them to divulge their names and passwords. Perhaps at least one journalist succumbed. The Tweet hack came within an hour after the phishing attempt,

Can News Sources Be Trusted?

The media takes great care to be a trusted source of information. Stories are checked and verified before release. Whenever there is a misreporting, the news agency suffers a serious black eye.

The AP is one of the most trusted of news sources. Founded in 1846, the AP is a not-for-profit news organization funded by its newspaper and broadcast members. It has 2,000 journalists worldwide. It is especially sensitive to misinformation since it is a resource for most major newspapers and broadcast networks in the world.

However, the AP is not the only news organization facing this problem. During the previous weekend, CBS’ ’60 Minutes’ and ’48 Hours’ were also hacked. Some of its Twitter accounts were posting malicious links. One hacked tweet from ’60 Minutes’ read, “Terror is striking the #USA and #Obama is Shamelessly in Bed with al-Qaeda.”

NPR said that in the previous week, several of its Twitter accounts were hacked by a group claiming to be the Syrian Electronic Army.

Clearly, in order to remain trusted news sources, these security holes must get plugged.

What Can Be Done to Prevent This?

Twitter has had a history of experience with this sort of problem. In February, it had to reset 250,000 passwords that it feared had been compromised.

Twitter is now working on an optional two-factor authentication procedure. Any time someone who has chosen this option logs onto Twitter via a new device with his user name and password, he must also enter a random security code that is sent to his cell phone in real time. Google and Facebook already offer such an authentication procedure.

Summary

In April, 2013, the SEC began to allow companies to disclose market-sensitive information via Facebook and Twitter so long as their investors have been told in advance where to look. This potentially exposes us to more of the same problem. Imagine a hacked tweet going out about a company's earnings report just before its report is formally presented indicating that it has missed its projections by a wide margin. The company's stock is likely to crash.

Tweets like this could be used by a malicious party to short a stock just before the tweet is released so that the short could be covered at the dip. Alternatively, the malicious party could buy the stock at the dip just before the hacked tweet is exposed.

This was a classic flash crash. If you combine the flood of instant information – often unverified – on social media with automated trading programs that buy and sell based on that information in microseconds, you get the potential for a big mess like the flash crash caused by the @AP tweet. We can expect further such crashes in the future. It's not the fact that social media is subject to hacking. It is that we have high-frequency trading algorithms that react to social media whether it is right or wrong.

In 2010, Congress passed the Dodd-Frank Act, the most comprehensive regulatory reform measures taken since the Great Depression. Nowhere does that act mention high-speed trading or technology. That's how quickly markets are morphing. Now, here we are three years later, woefully unprepared.

Technology moves faster than people

Acknowledgements

The material for this article was taken from the following resources:

AP Twitter Hack Sends Market Spinning, *NY Magazine*; April 23, 2013.
False White House explosion tweet rattles markets, *CNN Money*; April 23, 2013.
AP Twitter hack causes panic on Wall Street and sends Dow plunging, *Guardian*; April 23, 2013.
Market quavers after fake AP tweet says Obama was hurt in White House explosions, *Washington Post*; April 23, 2103.
AP tweet that rattled stock market exposes media vulnerability, *Christian Science Monitor*; April 25, 2013.
False AP Twitter Message Sparks Stock-Market Selloff, *Wall Street Journal*; April 25, 2013.
Associated Press Twitter Account Hacked in Market-Moving Attack, *Bloomberg*; April 25, 2013.
How Computers Temporarily Broke the Stock Market Over A Tweet, *Paste Magazine*; April 29, 2013.
CFTC Holds Twitter #HackCrash Hearing, *Yahoo Finance*; April 29, 2013.
The @AP Twitter account has been suspended after it was hacked. The tweet about an attack on the White House was false, *RT*; April 29, 2013.
CFTC Commissioner on #HackCrash: Beware of a Rise in Twitter Arbitrage, *Yahoo Finance*; April 30, 2013.
Social media and the stock market after that one AP tweet, *Marketplace*; April 30, 2013.