Yui Kee Computing Ltd.

Newsletter

August 2011

Contents

Trading at Hong Kong Stock Exchange Suspended after Cyber-Attack

<web-link for this article>

The Hong Kong Stock Exchange (HKEx) adopted a half-day (one trading session) suspension policy for issuers that announced price-sensitive information during the lunch hour on 10th August. The decision was made because the Hong Kong Stock Exchange's regulatory disclosure website, HKExnews became unavailable, thus creating a situation where some investors might be unaware of information that others knew.

HKExnews began to have problems about midday and was mostly inaccessible for the rest of the day, thus triggering the suspension of trading as part of a contingency plan. Announcements were made through an alternate website, bulletinboard.hk. The HKEx said that the failure was due to malicious outside attacks, but the source of the attacks and motive behind them were unknown. The trading systems were not affected. The Police and the Securities and Futures Commission have been contacted about the incident.

Seven stocks were affected by the suspension, HSBC, HKEx (the stock exchange itself), Cathay Pacific Airways, China Power International, China Resources Enterprise, Dah Sing Financial and Dah Sing Bank. The first three account for 18% of the Hang Seng Index.

Some investors and brokers criticised the decision because it prevented them profit-taking after Tuesday's 5.66% fall and Wednesday's 2.34% rebound in the HSI.

No information has been released about the mode of the attack, though a Distributed Denial of Service attack seems likely.

Updated: 12th August 2011

Attackers continued disruption attempts on the HKEx disclosure website on 12th August, but trading continued as the attempts failed and other methods for disseminating statutory information were in place. Details of the attacks are still sketchy, but Bill Chow Tang-bill, chief technology officer of HKEx, described a Distributed Denial of Service (DDoS) attach in a press briefing, "The malicious traffic originated from a network of hundreds of personal

computers, most of which were based outside Hong Kong". He also said that a mixture of techniques were used.

The Police say that they suspect overseas attackers are responsible and they will, if necessary, get outside assistance in their investigation. The motive for the attack is unclear, there has been no blackmail attempt and no trading information or money was lost. If the intent was to use the disruption of results announcements to make favourable trades with ignorant investors, then the suspension effectively countered the risk.

The exchange plans to prevent a recurrence by introducing more diverse channels for information dissemination. The backup website, bulletinboard.hk, was already available, but it is now much more widely known. Starting on the 12th August, the exchange will use newspaper advertisements to publicise in advance when companies will have result announcements. Thirdly, the exchange will use email to alert brokers and the press when companies have published financial information on their own websites. These multiple channels will make a future DDoS attack more complex and less likely to succeed.

More Information

Hack on Hong Kong Stock Exchange disrupts trading
Harry's view in the South China Morning Post
Hong Kong exchange trading disrupted as hackers target website
Anger as blue chips suspended
Fears over online-only platform realized
Hong Kong bourse hit by 'malicious hacking'
HKExnews
Bulletin Board for Listed Company Information

Will Mining Bots Kill Bitcoin?

<web-link for this article>

Bitcoin is an open-source, peer-to-peer digital cash system that uses cryptographic proof-of-work problems to validate transactions. A recent trojan, called Trojan.Badminer, installs a Bitcoin client on the victim's computer, uses it to validate transactions, and sends block reward bitcoins generated to a predetermined location. The bitcoins can be converted to traditional currency at various trading websites. Essentially, the attacker is using the victim's computer to generate money.

Previously in June, a different trojan, Infostealer.Coinbit simply stole bitcoins from the digital wallet on Bitcoin users' computers. Another incident, around 21 June 2011, saw the bitcoin exchange rate drop to almost zero as bitcoins stolen by password guessing were dumped on one of the major bitcoin-to-traditional currency gateways.

The latest attack goes beyond the earlier robberies because stealing computing power to generate bitcoins undermines the economic model of the currency. The Bitcoin model rewards people for dedicating their computing power to the difficult cryptographic task of securing transactions on the Bitcoin network (Bitcoin mining). If criminals steal computing power to generate bitcoins, then the system becomes a way to reward criminals. At the time of writing the US$ / bitcoin (BTC) exchange rate is 10.98999, and some back-of-the-envelope calculations reveal that the cost of electricity to generate a bitcoin is US$17.84 (assuming a fast, efficient GPU, and Uzbekistan's electricity tarrif). Any sane, honest bitcoin miner should turn off their mining rig at those prices.

The situation is not quite as clear as that, bitcoins are generated at a limited rate and the economics of the limited supply is expected to increase the value of existing bitcoins in the future, assuming that usage of bitcoins continues to grow. Therefore, an honest bitcoin miner might decide to continue mining in the face of uneconomic electricity prices, in the expectation

they could hoard the bitcoins until the value rose. Conversely, the perception that all bitcoin miners must be crooks could reduce confidence in the currency, making it worthless.

There are other factors affecting mining bots. One is the opportunity cost of using a botnet for bitcoin mining rather than other, proven illicit enterprises, such as DDoS attacks or spam distribution. Another might be the potential for other criminals to target mining bots, attempting to steal their bitcoins.

What of law enforcement? One possibility might be to examine a victim's computer to identify the account it generated bitcoins for, and then trace the transaction record stored in the Bitcoin blocks to identify the first transaction for those coins. The difficulty of doing this, and successfully linking it to a real person, seems extreme and, as the loss to the victim would be a few cents of electricity per day, not worthwhile. The indirect cost of loss of confidence in and collapse of a novel form of currency may be irrelevant to Police investigators used to dealing with traditional currency.

More Information

Malware mints virtual currency using victim's GPU
Trojan.Badminer
Password cracking, mining, and GPUs
New malware ferrets out and steals Bitcoins
Bitcoin Botnet Mining
bitcoinX charts
Bitcoin Miner
Mining hardware comparison
Mining rig
Mt. Gox
Bitcoin
Pooled mining
What is BitCoin and What is BitCoin Mining?
How to Get Rich on Bitcoin, By a System Administrator Who's Secretly Growing Them On His School's Computers
Blocks
Bitcoin Mining Calculator
Electricity pricing
Bitcoin currency collapse - where next for digital cash?
Bitcoin Miner

New Attack Weakens AES

<web-link for this article>

Researchers Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger have presented a paper that allows attackers to recover AES keys up to five times faster than previously thought possible.

Cryptographer Nate Lawson praised the work, saying, "This research is groundbreaking because it is the first method of breaking single-key AES that is (slightly) faster than brute force". In cryptographer's terminology, any method of finding the key faster than trying every possibility in turn ("brute-force analysis") is called a breaking the algorithm, though this does not necessarily mean that the algorithm is unsafe to use. In this case, AES will still be safe to use for many years because the technique, known as biclique cryptanalysis, is not practicable.

Cryptographers, no doubt, will continue to work on improved techniques, as celebrity-cryptographer Bruce Schneier reports the NSA saying, "Attacks always get better; they never get worse."

More Information

Biclique Cryptanalysis of the Full AES
AES crypto broken by 'groundbreaking' attack
define "Broken"
New Attack on AES

Businessman Arrested for Stock Exchange Attack

<web-link for this article>

A 29-year old businessman has been arrested in Hong Kong in connection with the attacks on the Hong Kong Stock Exchange news site earlier in the month. Computers, mobile devices and storage were seized from his Yuen Long home and the IT company he owns in Kwun Tong.

Referred to as a computer expert, Police said they tracked him down from records on the stock exchange computers after the first attacks. He was arrested for the offence of access to computers with dishonest or criminal intent, but the Police are still investigating the motive and the possibility of accomplices. Police statements on 12th August indicated that they suspected overseas attackers were responsible.

It is usually difficult to determine the origin of DDoS attacks, unless the Command and Control computers can be examined.

More Information

Police arrest man suspected related to HKExnews hacking
Police seize tools believed used to attack HKEx (HKG:0388) website
Trading at Hong Kong Stock Exchange Suspended after Cyber-Attack

Video of Chinese Cyber-attack Software Leaked

<web-link for this article>

A documentary on the Chinese Government's military and agriculture channel, CCTV 7 broadcast on 17th July 2011, and available online until 23rd August, appeared to show a cyber-attack tool in use. The original footage has now been replaced with other computer stock footage.

The imagery was used as background to a discussion about the potential and risks of cyber-warfare, and it seems likely that the editor did not understand the significance of those shots. The clip shows the selection of an attack destination, with the list including Falun Gong and Falun Dafa sites, but the selected destination is 138.26.72.17, an address that is allocated to the University of Alabama in Birmingham, USA, but not currently in use. The attack is not confirmed, but, instead, cancelled.

The Epoch Times, a USA-based newspaper founded in 1999 by Falun Gong supporters has a still image of the attack destination selection on their website and the F-Secure website has a 15 second clip of the aborted attack from the 22 minute program.

The fact that the PLA, and other leading militaries, have cyber-attack tools is no surprise, given previous discussions of cyber-warfare, but evidence that they have tools configured to attack the websites of civilian organisations must be an embarrassment to the Chinese Government.

More Information

Image of Cyber-Attack Target Selection
[军事科技] 网络风暴来了 (20110716) CCTV 7 Documentary
Chinese Military Academics Compare Cyber War to Nuclear War
Chinese Government Launching Online Attacks

[Chinese PLA video shows cyber-attack software]

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/