A Prolexic White Paper by PLXsert

DDoS Attacks Against Global Markets

www.prolexic.com

PROLEXIC
Now part of Akamai

Table of Contents

Overview 3

What is market manipulation? 3

Identified campaigns against financial institutions 3

Specific DDoS attacks and market movements (by date) 5

- Country of Estonia 5
- Global media and entertainment company 6
- Hong Kong Stock Exchange News 6
- Online finance and trading platform 7
- US securities and commodities exchanges 7
- US securities and commodities exchange 8
- Two US securities and commodities exchanges 9
- Large national oil and natural gas company 11
- US securities and commodities exchange and American financial firms 12
- Bitcoin exchange 13

Evolving DDoS threatscape and DDoS tools 14

- Underground markets and service elasticity 15
- Popular DDoS tools for market manipulation 16
  - Itsoknoproblembro, BroDoS and #OpAbabil PHP scripts 16
  - Distributed Reflection Denial of Service (DrDoS) attacks 17

Types of malicious actors and their motives 18

- Hacktivists 18
- Organized crime 18

Analysis of malicious actor groups 19

- L0ngWave99 19
- Cutting Sword of Justice 20
- Al-Qassam Cyber Fighters (QCF) 21
- What's next? 24

Conclusion 25

About Prolexic Security Engineering & Response Team (PLXsert) 26

Overview

Distributed denial of service (DDoS) attacks can degrade an organization's online presence and restrict the availability of its services. Hacktivists, extortionists and blackmailers frequently use DDoS attacks. In recent DDoS attack campaigns, a rising number of attacks have targeted the financial industry. As a result, financial institutions are anxious, and governments are considering the national security implications associated with digital assaults against the critical economic infrastructure provided by financial firms, including trading platforms.

In this white paper, PLXsert addresses the use of DDoS attacks as a mechanism for damaging the financial industry and interfering with financial markets. In some of the attacks explored here, malicious actors may have sought to influence individual stock values and commodity markets. The paper demonstrates a widespread pattern of denial of service attacks, describes specific DDoS attack campaigns, and identifies the effects on valuations and financial exchanges when possible. In addition, we highlight the DDoS attack tools used by the malicious actors and discuss the underground ecosystem that supports them.

What is market manipulation?

Market manipulation is a deliberate and malicious interference with market values in order to create an artificial price for a tradable security. DDoS attacks can be used to attempt to deliberately reduce the availability of products and services from a targeted company – or even an entire financial exchange platform. Many financial companies, including trading organizations, deliver a significant amount of their client services via their websites or via web applications. As a result, even though a victim enterprise might not suffer any inventory or physical loss as a result of DDoS attacks, the negative consequences associated with site availability and investor confidence may be substantial.

The public image of a financial service firm is intricately associated with its cyber presence, and DDoS attacks and other cyber-attack vectors can modify the online presence of the victim, which can create artificial, false or misleading appearances – a hallmark of market manipulation – as can rumors generated about an organization via online sites, such as Twitter. Overall, PLXsert found a causal relationship between cyber-attacks and a change in the valuation of a company in a given market.

Identified campaigns against financial institutions

Significant denial of service attack campaigns require vast resources, a large number of attackers, and substantial coordination and collaboration. Since 2011, and growing in 2012 and 2013, DDoS attack campaigns have become a significant threat to financial firms.

To understand DDoS attacks, it is important to learn about the groups behind the attacks. Two groups were responsible for the two most significant attack campaigns against financial markets in 2012 and 2013. The Operation Digital Tornado campaign was organized by a group called L0ngWave99. The Operation Ababil campaign was organized by al-Qassam Cyber Fighters (QCF). Although the two groups appear to have distinct identities, there is also a record of them having shared the same attack tools.

Operation Digital Tornado ran for three months from February to April 2012. In this campaign, L0ngwave99 claimed responsibility for attacking multiple US securities and commodity exchanges. The group posted alleged proof of its success on its website.[1]

[1] http://longwave99.wordpress.com/

L0ngwave99 claims to be motivated by political ideals, including support for the Occupy Wall Street movement. The group's website contains rhetoric against financial institutions and harsh criticism of the policies of the United States government and international financial institutions.

Operation Ababil and the *itsoknoproblembro* campaign ran from January 2012 through August 2013. Although official announcements[2] and claimed attributions began appearing on Pastebin only as early as September 2012, PLXsert researchers have identified through Open Source Intelligence (OSINT) that the DDoS attack campaign had been ongoing since at least January 2012. Details of *itsoknoproblembro* are described in a **DDoS threat advisory** from PLXsert.

L0ngWave99, QCF and other malicious actor groups were responsible for several DDoS attack incidents that affected stock and currency valuations or interfered with trading, including those shown below.

Date	Target	Alleged perpetrators
April 27, 2007	Government and finance sites in Estonia	pro-Russian groups
April 2, 2011	A global media and entertainment company	Lulzsec
August 12-13, 2011	HKSC, the Chinese stock exchange	Local attackers
January 5, 2012	Online finance and trading platform	Unattributed
January 12, 2012	Start of operation Ababil targeting American financial firms	Qassam Cyber Fighters
February 14, 2012	US securities and commodities exchange	L0ngWave99
February 14, 2012	US securities and commodities exchange	L0ngWave99
February 14, 2012	eSignal, an electronic trading platform	L0ngWave99
February 14, 2012	US securities and commodities exchange	L0ngWave99
February 14, 2012	US securities and commodities exchange	L0ngWave99
April 26, 2012	US securities and commodities exchange	L0ngWave99
August 15-25, 2012	A large national oil and natural gas company	Cutting Sword of Justice
September 18, 2012	US securities and commodities exchange	Qassam Cyber Fighters
March-April 2013	A bitcoin exchange platform	Unknown
2013	American financial institutions targeted by Operation Ababil	Qassam Cyber Fighters

Figure 1: Several DDoS campaigns have affected stock and currency valuations or interfered with trading

[2] http://pastebin.com/u/QassamCyberFighters

Specific DDoS attacks and market movements (by date)

PLXSert has identified several campaigns that were orchestrated with the intention of manipulating financial markets, either by changing prices or interfering with trading. Some of these campaigns were directed at minor exchanges, some sought to influence a specific valuation, and others targeted specific countries.

Each attack or ongoing campaign is described in some detail below and includes the timeframe of the attack, the name of the campaign, the malicious actors involved, the industry vertical, types of attacks if known, the perpetrators announcement of the attack or other public announcements by the victims or the media, and, most importantly, the market implications of the attack.

Country of Estonia

Date: April 27, 2007

Campaign name: Unknown

Malicious actor: The Russian Federation or individuals sympathetic to Russia

Industry vertical: Widespread DDoS attacks against the Estonian parliament, banks, ministries, newspapers and broadcasters

Types of attacks: Attacks ranged from individuals using ping floods to the rental of expensive botnets for spam distribution, including a spam attack targeting prominent news portals and the defacement of the Estonian Reform Party website.

Attack announcement: No formal announcement was made by the perpetrators, but statements were made by Estonian officials, and some pro-Russian groups claimed attribution.[3,4]

Market implications: This DDoS campaign was the first time that a botnet threatened the security of an entire nation.[5] Ninety-five percent of Estonia’s banking operations were carried out electronically.[6] The largest bank in Estonia was shut down by an attack for more than an hour with losses of at least US$1 million.[7] All major commercial banks, telecommunications companies, media outlets and domain name system (DNS) servers — the phone books of the Internet — were affected.

[3] http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/
[4] http://www.reuters.com/article/2009/03/12/us-russia-estonia-cyberspace-idUSTRE52B4D820090312?feedType=RSS&feedName=internetNews
[5] http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all
[6] http://www.businessweek.com/stories/2007-12-17/estonia-cyber-superpowerbusinessweek-business-news-stock-market-and-financial-advice
[7] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=2

Global media and entertainment company

Date: April 2, 2011

Campaign Name: [redacted]

Malicious actor: Anonymous

Industry vertical: Gaming and entertainment

Types of attacks: The multi-vector attack included three components: a DDoS campaign that took down online services and forced the company to seek DDoS mitigation services, disclosure of sensitive and private information and exposure of the company's infrastructure vulnerabilities, and a media response that amplified the perception of the disruption of company services.

Attack announcement: Anonymous warned the company it was targeted.[8] Later Anonymous took credit for a drop in the target's stock price: "We're already causing [redacted] stock to drop!!!"[9]

Market implications: The data breach caused the market value of the target's shares to drop six percent.[10] The target's online store and network suffered significant outages. The target's main website was also subject to site failure.[11]

Mizuho Investors Securities analyst Nobuo Kurahashi was reported to have estimated that the target could be on the hook for US$1.25 billion in lost business and said, "It could take months for the security woes to settle, and how this may affect consumer confidence in [redacted]'s online services in the long run is harder to assess."

Hong Kong Stock Exchange News

Date: August 12-13, 2011

Campaign name: None found

Malicious actor: Local

Industry vertical: Distribution of financial news and stock exchange

Types of attacks: The malicious traffic originated from personal computers based outside Hong Kong.[12]

Attack announcement: None found

Market implications: The attacks caused the exchange to suspend trading in the shares of seven companies and the exchange operator itself. The seven companies, which were due to make announcements and could not publish them on the news site, included China Power International, the airline Cathay Pacific, and HSBC, described as "the most liquid stock in Hong Kong." Crashing the news site caused the companies to find alternate means of disclosing their information.[13]

[8] http://anonnews.org/?p=press&a=item&i=787

[9] http://bit.ly/1dYI41A

[10] http://bit.ly/1aOZqIG

[11] http://bit.ly/1asVym9

[12] http://www.livehacking.com/2011/08/12/two-days-of-ddos-attacks-affect-hong-kong-stock-exchange-news-web-site/

[13] http://www.ft.com/intl/cms/s/0/f448a9b6-c33a-11e0-9109-00144feabdc0.html#axzz2kSbxNfZ2

Online finance and trading platform

Date: January 12, 2012

Campaign Name: None found

Malicious actor: None identified

Industry vertical: Stock exchanges and trading platforms

Types of attacks: Not available

Attack announcement: No formal announcement or attribution. The company acknowledged the attack.[14]

Market implications: The attack occurred during a less-busy period of trade at the end of the year, and the market was already closed at times during the attack, making it difficult to gauge the full effect. The trading platform experienced an extensive outage from Christmas Day to New Year's. Access was unavailable from some countries for nearly two weeks, preventing customers from trading and accessing information required for the completion of tax returns.[15]

US securities and commodities exchanges

Date: February 12, 2012

Campaign name: Operation Digital Tornado

Malicious actor: L0ngwave99

Industry vertical: Stock exchanges and trading platforms

Types of attacks: Not available

Attack announcement: The cyber group announced its success, including alleged digital proof of the downing of the financial exchange sites.

Market implications: On its website, the group boasted of its attacks of six "fundamental economic websites" of the U.S. and offered a link purporting to offer evidence of its success.

[14] http://bit.ly/1dYpnK6
[15] http://bit.ly/1aP4gFR

US securities and commodities exchange

Date: February 14, 2012

Campaign Name: Operation Digital Tornado

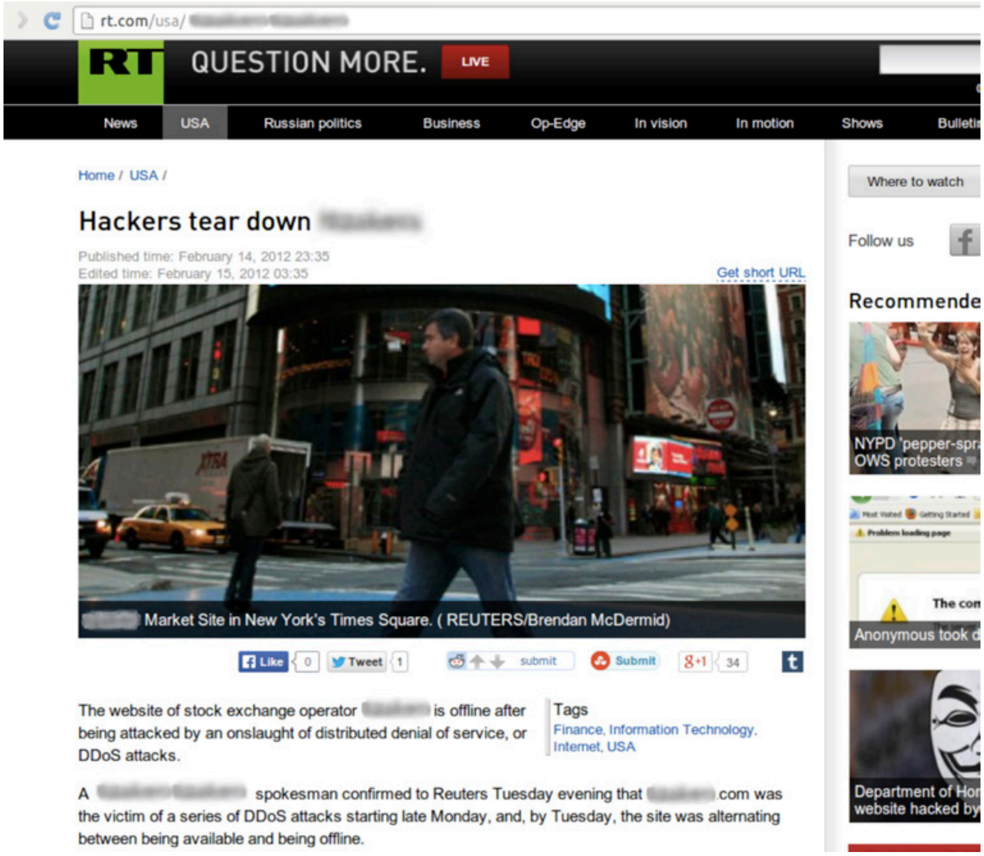
Malicious actor: L0ngwave99

Industry vertical: Stock exchanges and trading platforms

Types of attacks: Not available

Attack announcement: L0ngwave99 posted a visual report as proof of attacking the target on its website.[16]

Market implications: Although the site was disrupted intermittently over a 24-hour period, affecting the target's corporate site and its main portal for trader communications, other customers continued to access portions of the target's other websites.[17] Although customers were unable intermittently to use some of the exchanges' websites, there was no indication that trading systems were affected.[18]



Home / USA /

Hackers tear down [redacted]

Published time: February 14, 2012 23:35
Edited time: February 15, 2012 03:35

Get short URL

[redacted] Market Site in New York's Times Square. (REUTERS/Brendan McDermid)

The website of stock exchange operator [redacted] is offline after being attacked by an onslaught of distributed denial of service, or DDoS attacks.

Tags
Finance, Information Technology, Internet, USA

A [redacted] spokesman confirmed to Reuters Tuesday evening that [redacted].com was the victim of a series of DDoS attacks starting late Monday, and, by Tuesday, the site was alternating between being available and being offline.

Figure 2: Media announces the target's downtime

[16] http://bit.ly/1cZCQwK
[17] http://on.wsj.com/1jEZssh
[18] http://ubm.io/1jEZxfn

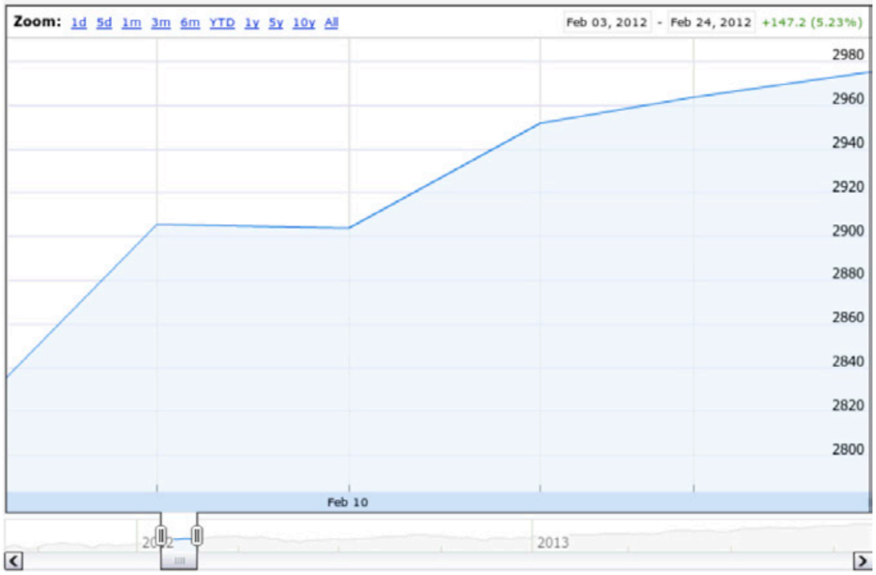


Figure 3: There was no indication that trading was affected

US securities and commodities exchanges

Date: April 26, 2012

Campaign name: Operation Digital Tornado

Malicious actor: L0ngwave99

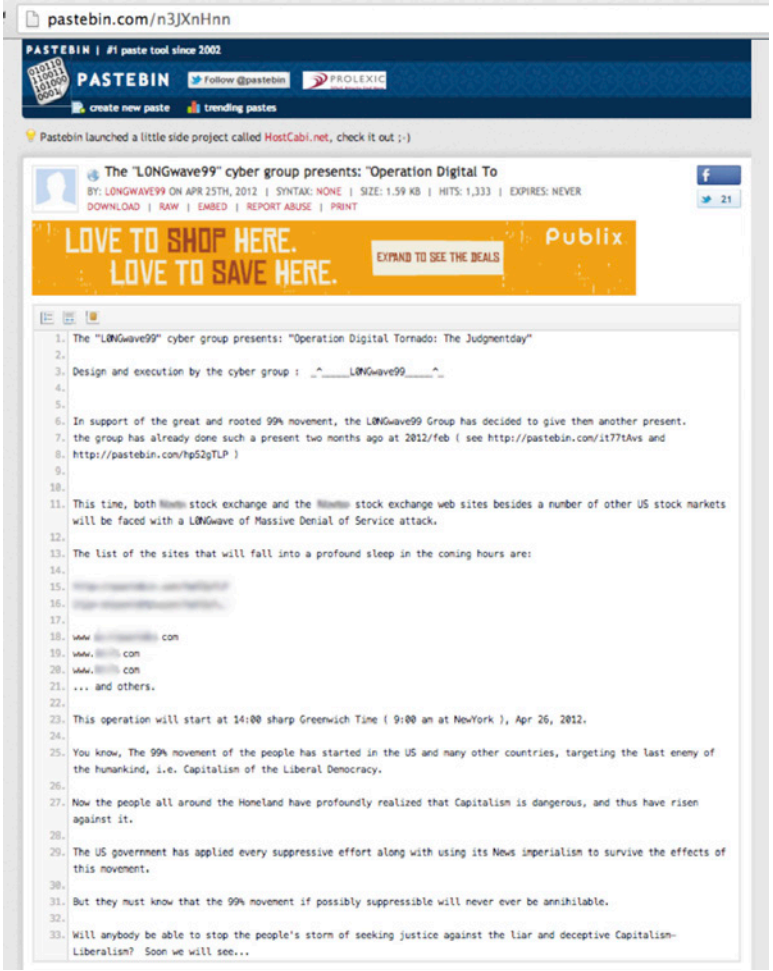
Industry vertical: Stock exchanges and trading platforms

Types of attacks: Not available

Attack announcement: The group announced its planned attack in a Pastebin post.[19] L0ngwave99 posted a visual report to provide alleged proof of its role in the attack against the targets.[20]

Market implications: There were no observed effects.[21]

[19] http://pastebin.com/n3JXnHnn
[20] http://bit.ly/1aP34lO
[21] http://fxn.ws/KOmot0



The "L0NGwave99" cyber group presents: "Operation Digital To

BY: L0NGWAVE99 ON APR 25TH, 2012 | SYNTAX: NONE | SIZE: 1.59 KB | HITS: 1,333 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

```
The "L0NGwave99" cyber group presents: "Operation Digital Tornado: The Judgmentday"

Design and execution by the cyber group :  _^_____L0NGwave99_____^_


In support of the great and rooted 99% movement, the L0NGwave99 Group has decided to give them another present.
the group has already done such a present two months ago at 2012/feb ( see http://pastebin.com/it77tAvs and
http://pastebin.com/hp52gTLP )


This time, both [redacted] stock exchange and the [redacted] stock exchange web sites besides a number of other US stock markets
will be faced with a L0NGwave of Massive Denial of Service attack.

The list of the sites that will fall into a profound sleep in the coming hours are:

[redacted]
[redacted]

www [redacted] com
www.[redacted] com
www.[redacted] com
... and others.

This operation will start at 14:00 sharp Greenwich Time ( 9:00 am at NewYork ), Apr 26, 2012.

You know, The 99% movement of the people has started in the US and many other countries, targeting the last enemy of
the humankind, i.e. Capitalism of the Liberal Democracy.

Now the people all around the Homeland have profoundly realized that Capitalism is dangerous, and thus have risen
against it.

The US government has applied every suppressive effort along with using its News imperialism to survive the effects of
this movement.

But they must know that the 99% movement if possibly suppressible will never ever be annihilable.

Will anybody be able to stop the people's storm of seeking justice against the liar and deceptive Capitalism-
Liberalism?  Soon we will see...
```

Figure 4: Pastebin announcement of the planned attack[22]

[22] http://pastebin.com/n3JXnHnn

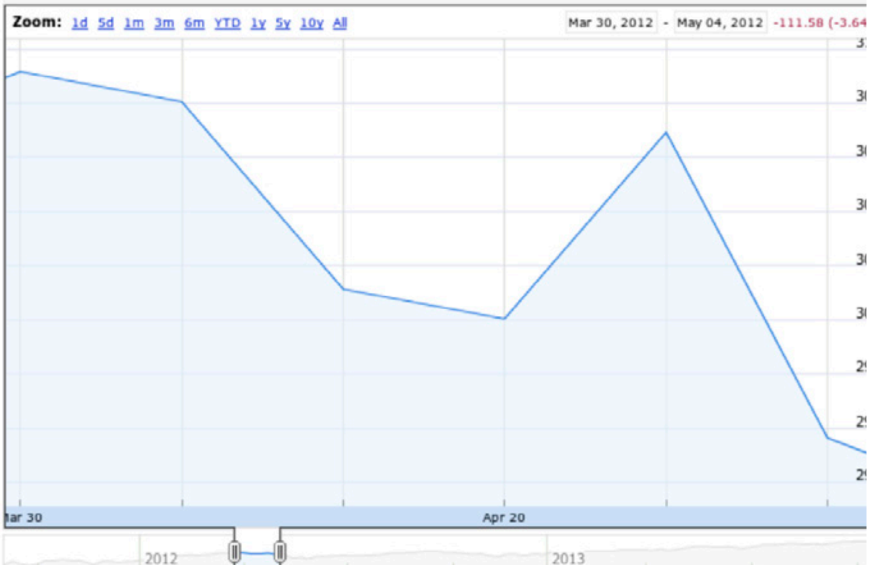


Figure 5: There were no observed effects to the exchange's index during the month of April 2012

Large national oil and natural gas company

Date: August 15-25, 2012

Campaign name: [redacted]Hacked

Malicious actor: Cutting Sword of Justice. With several vectors of attacks, alleged inside cooperation, and collusion of groups and tools attributed to highly sophisticated campaigns, there is the suggestion of participation of state actors as well, possibly related to oil export market gains and geopolitical rivalry in the Middle East.

Industry vertical: Energy

Types of attacks: This multi-pronged campaign had a high-level of sophistication. A malware component allegedly wiped out over 30,000 computers, and a data leak suggested proof of network footprinting and infiltration.[23] It was estimated that it took the target about a week to restore all the computer systems. The campaign had also a very large DDoS component.

Attack announcement: The Cutting Sword of Justice announced that the target was hacked and went down, claiming the data and operating systems of tens of thousands of computer clients and servers were destroyed.[24]

Market implications: The target is state-owned, not publicly traded and not bound by rules of full disclosure. One of the largest petroleum companies in the world, the target has an estimated value of more than US$7 trillion dollars, accounting for 55 percent of GDP. In addition, a post stated there were fuel shortages and closure of gas stations in the company's country as result of this attack.[25]

[23] http://pastebin.com/tztnRLQG
[24] http://pastebin.com/p5C4mCCD
[25] http://hilf-ol-fozoul.blogspot.com/2012/09/blog-post_2.html

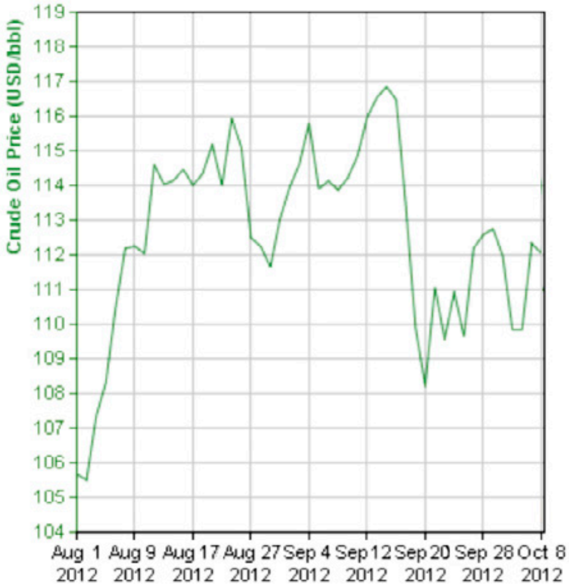


Figure 6: Crude oil price during the week of the attack on the national oil and gas company

US securities and commodities exchange and American financial firms

Date: September 18, 2012

Campaign names: #OpAbabil, *itsoknoproblembro* and BroDoS

Malicious actor: Qassam Cyber Fighters (QCF)

Industry vertical: Stock exchange and financial firms

Types of attacks: Not available

Attack announcement: All pro-Palestine groups active in cyberspace were invited to attack American and Zionist web sites.[26] The group claimed that the website of a major American financial institution went down. Mainstream media announced the attack on the US commodity and security exchange.[27]

Market implications: The campaign extended well into 2013. During February, March and April of 2013, American banks were estimated to be offline for a period of 249 hours.[28] One bank's stock was reported down 1.8 percent on September 18, 2012[29], but overall the effect was negligible on the firm's market value.

There were no reports of outages or any other significant effect on the exchange's online operations and market functions. The campaign did not succeed in altering the market as a whole, and there is no proof of the altering of stock values for any of the targeted institutions.

The attacks kept the financial industry on high alert for many months. The psychological and economic effects on the financial industry were widespread, however, with many of the companies' IT security teams investing extensive time and resources to fend off the attacks.

[26] http://pastebin.com/mCHia4W5
[27] http://fxn.ws/LM1OJZ
[28] http://bit.ly/LM0FSH
[29] http://on.mktw.net/KzojBD

Bitcoin exchange

Date: March-April 2013

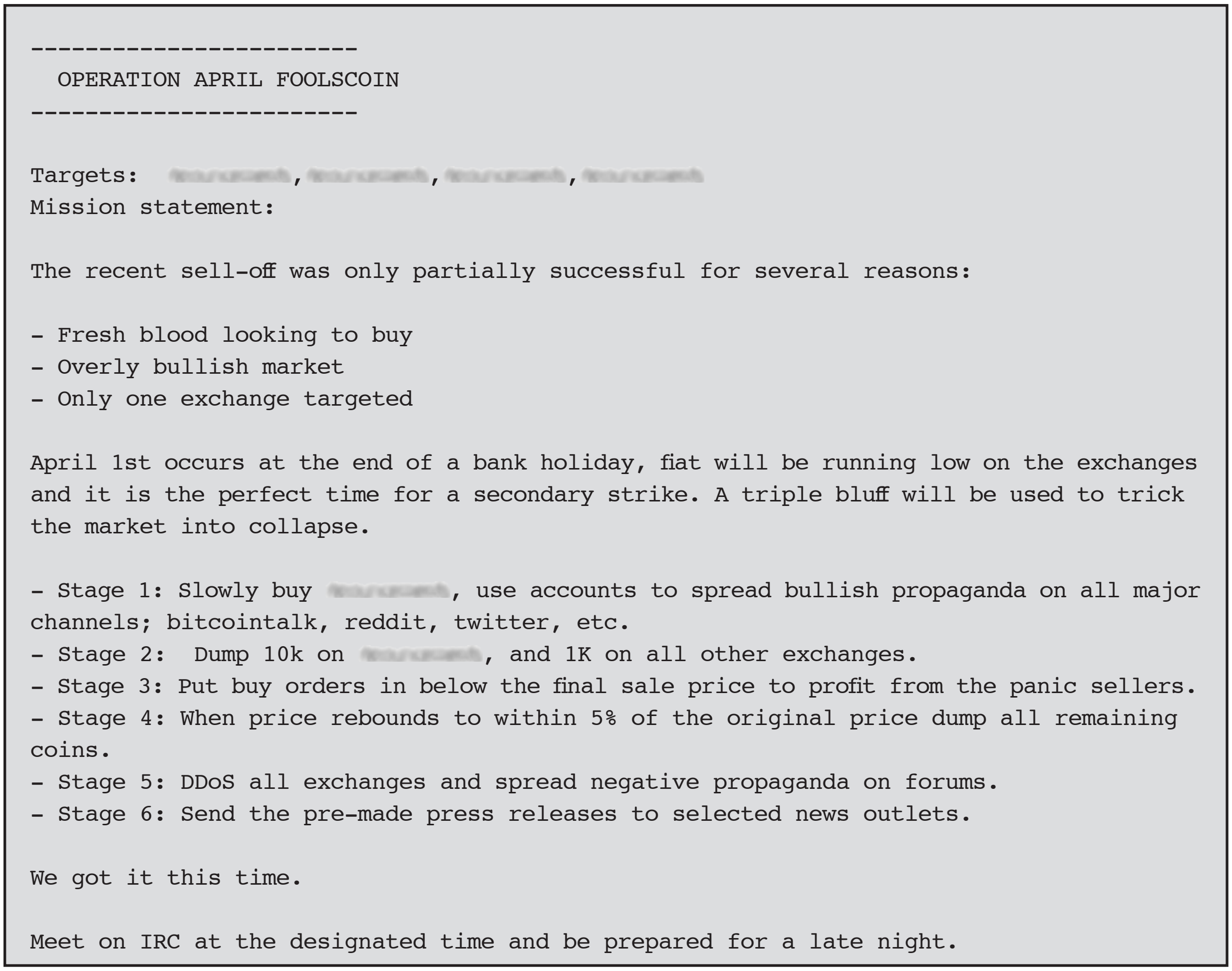
Campaign name: Operation April Foolscoin

Malicious actor: Unknown

Industry vertical: Currency exchange

Attack Announcement: The April 1 attack was announced as a follow-on campaign to promote a sell-off with the strike to target a bank holiday when digital currency would be running low on the exchanges. The stated aim was to trick the market into collapse.[30]

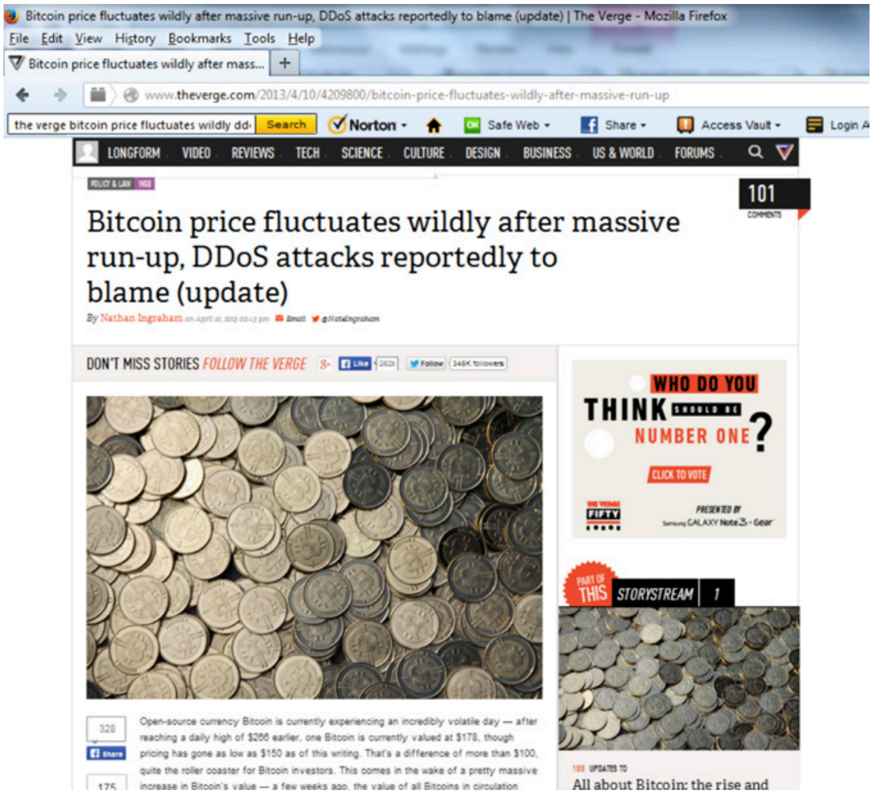
Market implications: At times, users were unable to log into their accounts. After a 12-hour halt in trading, the exchange resumed trading. However, it was struck again, causing trading to stop once more.[31] Panic selling occurred as did abuse of the system for profit.[32] Bitcoin values fluctuated wildly with the price of one bitcoin swinging from US$266 to US$105.[33]



```
------------------------
  OPERATION APRIL FOOLSCOIN
------------------------

Targets:  [redacted], [redacted], [redacted], [redacted]
Mission statement:

The recent sell-off was only partially successful for several reasons:

- Fresh blood looking to buy
- Overly bullish market
- Only one exchange targeted

April 1st occurs at the end of a bank holiday, fiat will be running low on the exchanges
and it is the perfect time for a secondary strike. A triple bluff will be used to trick
the market into collapse.

- Stage 1: Slowly buy [redacted], use accounts to spread bullish propaganda on all major
channels; bitcointalk, reddit, twitter, etc.
- Stage 2:  Dump 10k on [redacted], and 1K on all other exchanges.
- Stage 3: Put buy orders in below the final sale price to profit from the panic sellers.
- Stage 4: When price rebounds to within 5% of the original price dump all remaining
coins.
- Stage 5: DDoS all exchanges and spread negative propaganda on forums.
- Stage 6: Send the pre-made press releases to selected news outlets.

We got it this time.

Meet on IRC at the designated time and be prepared for a late night.
```

Figure 7: The announcement of Operation Foolscoin was a deliberate attempt to swing the bitcoin currency market

[30] http://pastebin.com/h7iGK49T
[31] http://bit.ly/1i4UswB
[32] http://bit.ly/1jC5hch
[33] http://www.theverge.com/2013/4/10/4209800/bitcoin-price-fluctuates-wildly-after-massive-run-up



Bitcoin price fluctuates wildly after massive run-up, DDoS attacks reportedly to blame (update) | The Verge - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bitcoin price fluctuates wildly after mass...
www.theverge.com/2013/4/10/4209800/bitcoin-price-fluctuates-wildly-after-massive-run-up
the verge bitcoin price fluctuates wildly dd
Search
Norton
Safe Web
Share
Access Vault
Login
LONGFORM
VIDEO
REVIEWS
TECH
SCIENCE
CULTURE
DESIGN
BUSINESS
US & WORLD
FORUMS
POLICY & LAW
WEB
101
COMMENTS
DON'T MISS STORIES FOLLOW THE VERGE
Like
Follow
345K followers
WHO DO YOU THINK SHOULD BE NUMBER ONE?
CLICK TO VOTE
THE VERGE FIFTY
PRESENTED BY
PART OF THIS STORYSTREAM
328
Share
175
100 UPDATES TO

Bitcoin price fluctuates wildly after massive run-up, DDoS attacks reportedly to blame (update)

By Nathan Ingraham

Open-source currency Bitcoin is currently experiencing an incredibly volatile day — after reaching a daily high of $266 earlier, one Bitcoin is currently valued at $178, though pricing has gone as low as $150 as of this writing. That's a difference of more than $100, quite the roller coaster for Bitcoin investors. This comes in the wake of a pretty massive increase in Bitcoin's value — a few weeks ago, the value of all Bitcoins in circulation

All about Bitcoin: the rise and

Figure 8: An online publication reports wild swings in bitcoin prices

Evolving DDoS threatscape and DDoS tools

Just as DDoS attackers have evolved new attack types and new tools to perform campaigns, profit models for DDoS attacks against financial firms have also evolved. Underground markets spring up as needed to meet the demand for DDoS botnets and attack tools.

Dow falls 143 points on Twitter hack

Of course, not all cyber-attacks are DDoS attacks. Even a technically weak attack may garner media coverage that can rock financial markets. Once an attack hits the media, especially online media, the targeted organization may have to surmount extensive scrutiny and produce proof that their services are reliable and will remain so. A prime example of the effect of online media in markets by a cyber-attack was a Twitter hack of the Associated Press account that falsely reported explosions at the White House and that Barak Obama was injured. The false tweet caused panic on Wall Street, sending the Dow Jones Industrial Average plunging on April 23, 2013.[34]

[34] http://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall

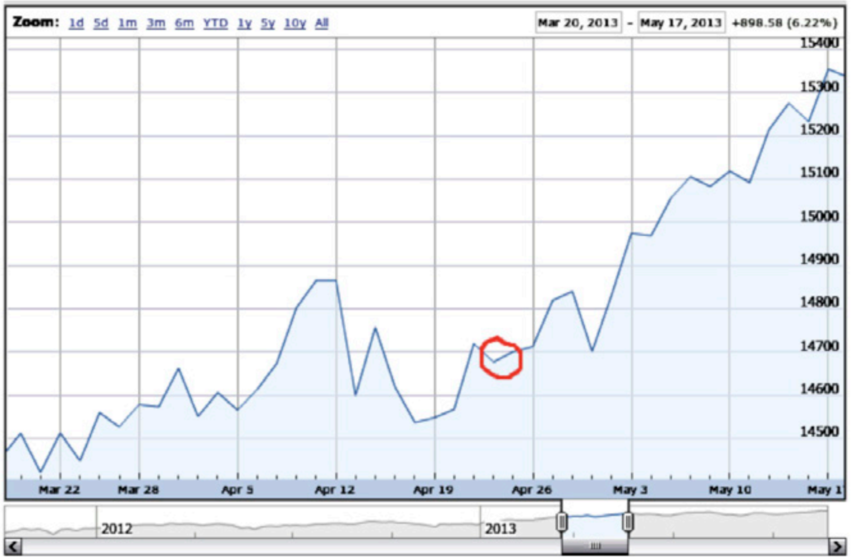


Figure 9: The market value drop during the AP Twitter hack event is shown in red

Underground markets and service elasticity

A vibrant and burgeoning DDoS-as-a-Service market is now available where anybody with sufficient financial resources, regardless of technical acumen, can rent a large botnet to perform a DDoS attack. Bigger botnets with greater bandwidth translate to more lucrative botnet rental profits.

Furthermore, these services now offer an elastic capability to ramp up or ramp down legions of botnets, adding a new dimension to the attack strategy of malicious actors. The elasticity of these botnets comes from the customization of service offerings where malicious actors charge by the number of servers and zombies available to their clients. This pay-per-use flexibility allows attack size to vary depending on the purchasing power of each client. Such *a la carte* services let customers purchase DDoS services customized to their needs.

To build armies of botnets, attackers recruit a large number of hosts across the Internet. These hosts range from compromised home computers with DSL, fiber or cable bandwidth to large server farms. The mission of these DDoS-as-a-Service entrepreneurs is to compromise and control as many hosts as possible, turn these hosts into controllable zombies, and unite these zombies to perform coordinated attacks.

Every new zombie strengthens the overall power and reach of a botnet. In fact, the more geographically distributed the compromised hosts are, the better the result, because scattered hosts make it more difficult for cyber-attack mitigators to pinpoint the perpetrators and to identify the best countermeasures to use against an attack.

Indirect impacts on financial markets

Besides the financial upsides of botnet attacks, more and more DDoS attackers are aiming their botnets at news, government and military entities. The ability for attackers to play havoc on the services supplied by these institutions has resulted in an indirect impact on currency and financial markets in the United States and other countries.

Popular DDoS tools for market manipulation

The tools that malicious actors develop and use to affect financial markets vary in complexity from simple Open System Interconnection (OSI) network layer 3 attacks (e.g., SYN, UDP and TCP floods) to more complex application layer 7 attacks (e.g., GET and POST floods). Regardless of the layer of the OSI model attackers use as a vector, DDoS tools permit the orchestration and management of large numbers of zombie bots.

Some of the most prominent DDoS attacking tools used to interfere with the financial industry include *itsoknoproblembro*, which was originally known as BroDoS, and distributed reflection denial of service attacks, also known as DrDoS attacks.

***Itsoknoproblembro*, BroDoS and #OpAbabil PHP scripts**

The *itsoknoproblembro*/BroDoS botnet has been identified in multiple campaigns against financial firms, corporations and countries, and it represents one of the most powerful and sophisticated botnets ever used for denial of service attacks. The level of effort, coordination and sophistication of the tools and attacks suggest that the actors behind it are at a level of sophistication of a state-sponsored organization or military.

Throughout the fall of 2012, a very public DDoS campaign emerged that targeted multiple critical infrastructure sectors with unprecedented levels of malicious traffic. These attacks, called Operation Ababil by Qassam Cyber Fighters (QCF), made use of thousands of compromised web servers while utilizing a multi-tiered attack and control topology.

Unlike traditional botnets that relied on infected workstations, the BroDoS toolkit utilizes an advanced booter script suite that makes use of hacked web servers. The use of hacked web servers allows attackers to harness much larger amounts of bandwidth with fewer infections.

The web servers were compromised through the exploitation of publicly known web application vulnerabilities in multiple applications. Analysts discovered instances of this toolkit on compromised web applications such as Joomla, WordPress, AWStats, Plesk, cPanel, phpMyFAQ and numerous other applications.

Attackers made use of vulnerabilities within outdated versions of the applications or exploited public vulnerabilities within third-party plugins or themes. Some of the common vectors were the Joomla Bluestork theme vulnerability and the WordPress TimThumb vulnerability. Attackers would make use of SQL injection (SQLi) vulnerabilities, Remote File Inclusion (RFI) vulnerabilities and Remote Code Execution (RCE) vulnerabilities in order to drop PHP shells and file uploaders onto the web servers. Later, this feature matured into a specific file that allows for execution of dynamic code on a compromised server.

Oftentimes, servers that contained the *itsoknoproblembro* toolkit showed evidence of multiple points of compromise and were being used for multiple malicious purposes such as spam and phishing. This capability indicates that the malicious actors who were behind the attacks were either making use of previously compromised web servers that they were able to identify and control, or they coordinated with other groups to pool together a large amount of hacked servers in which to push out the *itsoknoproblembro* toolkit. Whichever the scenario, the result was a large number of zombie web servers that were able to generate more than 70 Gbps of malicious traffic at its peak.

In July 2013, PLXsert confirmed the addition of new files and instructions to sampled zombies that were part of the BroDoS botnet. The toolkit had undergone several evolutions throughout the yearlong campaign. At first, the attack instructions were hard-coded into the PHP shell directly. As time went on, attackers switched to the use of base64-encoded eval() statements to execute attack scripts. This prevented identification of attack signatures through toolkit analysis.

Various logging mechanisms exist to obtain attack codes as they are being executed in memory. These attack codes are often shared among the intelligence community. It appears that attackers continue to follow the practice of modifying file names in an attempt to evade existing tracking mechanisms.

File content indicates that the actors behind the campaign were making use of an MJDU-style of attack. The attack utilizes message digest algorithm 5 (MD5) authentication for infected hosts and uses *eval(base64_decode())* functions to receive attack instructions. The use of the MJDU eval() scripts were found in the same hosts identified to have the *itsoknoproblembro* scripts. *Itsoknoproblembro* earned its name from the status message displayed when the parameter "action=status" is received by an infected server, displaying the text: `itsoknoproblembro`. The MJDU scripts do not identify themselves in this manner, and the use of the hard coded *itsoknoproblembro* attack scripts has been significantly reduced and replaced with MJDU attack scripts in the hosts analyzed by PLXsert.

The network of compromised hosts maintains a multi-tiered framework, using callbacks to register into a command and control (C2).

For more information about itsoknoproblembro, download the ***itsoknoproblembro* DDoS threat advisory from PLXsert**.

Distributed Reflection Denial of Service (DrDoS) attacks

Throughout 2012, there was a significant increase in the use of a specific DDoS methodology known as Distributed Reflection Denial of Service attacks (DrDoS). These attacks have been a persistent and effective method of attack for more than 10 years. The technique is showing no signs of obsolescence as it continues to grow in effectiveness and remains a popular attack style of numerous malicious actors.

DrDoS techniques rely on the ability to receive a reply from an Internet host or server using a spoofed request. These techniques usually involve multiple victims and one primary target. When the requests are the same size as the response, there is not much to gain other than anonymity. However, when a request yields a response that is larger than the initial spoofed request, the attacker gains the benefit of greater attack bandwidth without expending additional resources.

The Domain Name System (DNS) reflection attack vector, a type of DrDoS attack, has been identified as one of the principal attack vectors used during the attacks on the financial industry. This DDoS technique relies on the exploitation of the DNS protocol. Malicious actors will spoof the IP address of their primary target and then send requests to a list of victim DNS servers. When the DNS servers receive the forged requests, the servers are tricked into responding to the spoofed target IP address. Victim DNS servers will do exactly as they are instructed, resulting in a flood of unwanted responses sent to the attacker's primary target.

The scale of the attack is dependent on the quantity of victim DNS servers for which the attacker knows the IP addresses. These IP addresses can often be found by scanning IP ranges looking for port 53. Furthermore, since the nature of this type of attack is one that utilizes spoofed IP requests to a legitimate DNS server, attribution to the original malicious actor becomes a difficult task.

Types of malicious actors and their motives

When assessing the actors behind market manipulation campaigns, it is necessary to analyze their motives and skills. PLXSert uses the following classification system:

- **Script kiddies** - Low technical barrier to entry, may engage in denial of service attacks for fun, fame or profit

- **Hacktivists** - These groups are motivated by political and philosophical ideals. They have performed attacks on corporations, governments and financial institutions. These groups do not seek financial benefits. They seek political and public opinion effects.

- **Criminal enterprise** - DDoS-as-a-Business. Engages in criminal activity for profit. This group is not loyal to an ideology and usually has no motive other than profit.

- **Veteran criminals** - Creators and executors of sophisticated and mature DDoS attack techniques. Veteran criminal groups are able to create large botnets quickly and to generate very large amounts of damaging traffic. This classification includes digital mercenaries for hire and state-sponsored actors. This classification includes groups that may follow particular ideologies or have ulterior motives.

In order to understand the full impact of market manipulation campaigns, it is necessary to look at the malicious actors and their motives. It seems clear that the attackers in these financial services attacks wanted to affect target market value by effectively disrupting or denying the availability of services.

Hacktivists

A good example of hacktivist attacks are the attacks against payment processing and online auction sites on July 27, 2011. Hacktivists groups targeted the corporations in retaliation for stopping the processing of funds for WikiLeaks.

It is evident that hacktivists believe in the potential of DDoS attacks to deliver a political message and to affect the market value of targeted organizations, even though the hacktivists' goal is political change.

The mainstream media attention gathered by hacktivist attacks has created the perception in the Internet underground that there are big benefits to harvesting and fostering the creation of large botnets that can be used for DDoS attacks for political, financial and even military purposes. Such perception appears accurate based on the current expanding DDoS-as-a-service market. Furthermore, these attacks can deliver an effective political message to the institutions or organizations subject to these types of attacks.

Organized crime

This segment of actors is composed of individuals who run their DDoS services (DDoS-as-a-Service) and offer attack tools and resources to paying customers. With enough financial resources, anybody can rent as much firepower as they like in the DDoS-as-a-Service market, a dynamic market that constantly adapts the latest attack vectors to the newest technology. It is this segment of malicious actors that keeps the DDoS threatscape alive by expanding the base of their botnets and creating and adapting the latest malware to work with DDoS attack vectors.

This ecosystem is composed of several layers of operators, financers and researchers who find, probe, test and develop DDoS tools and harvest as many zombies as possible. This ecosystem provides an availability of resources and services that caters to demanding customers who include criminal organizations, low-level criminals, script kiddies, and circumstance-driven customers. This segment of actors is also always facing threats to its resources by competing criminal organizations, security corporations and law enforcement.

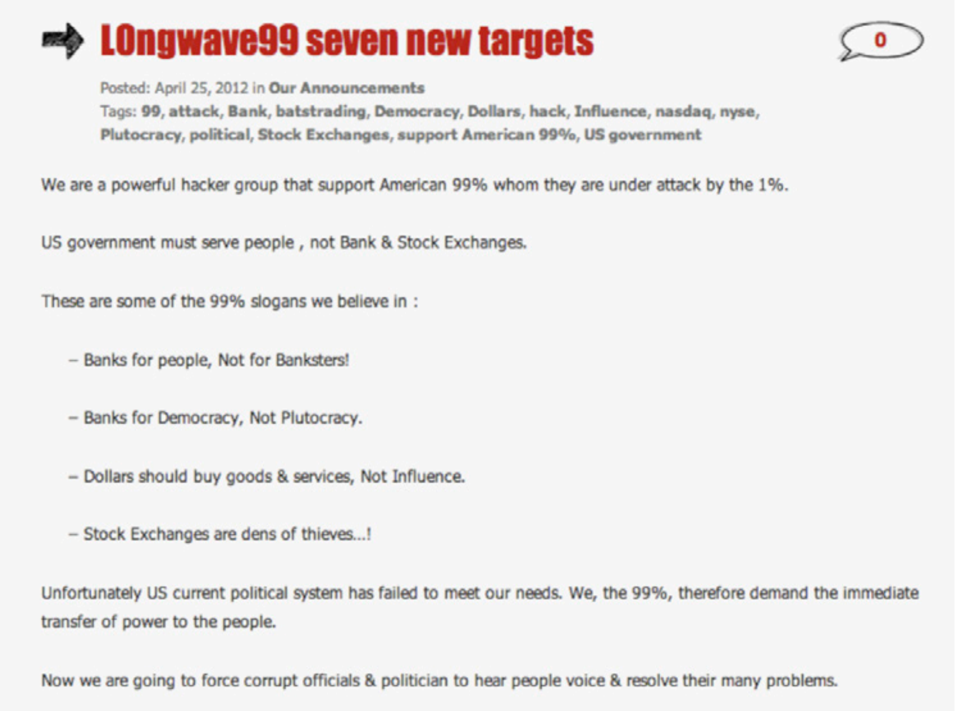
Analysis of malicious actor groups

As discussed in the first section, a few specific groups appear to be responsible for the majority of attacks against American corporations and financial exchanges in an effort to damage market values and trading platforms. They include L0ngWave99, Cutting Sword of Justice and al-Qassam Cyber Fighters (QCF).

L0ngWave99

L0ngWave99 appeared and disappeared from the world stage. The group presented its members as supporters of the Occupy Wall Street movement and claims to have orchestrated campaigns against seven stock exchanges.

The group's success in these campaigns is questionable, but its communications signal an intention and the perception that the operation of trading platforms and leading businesses can be damaged by DDoS attacks. The brief appearance and subsequent disappearance of L0ngWave99, and the tools used during its campaigns, raises the question of whether L0ngWave99 is only a hacktivist group or has an ulterior motive.



L0ngwave99 seven new targets

0

Posted: April 25, 2012 in **Our Announcements**
Tags: **99, attack, Bank, batstrading, Democracy, Dollars, hack, Influence, nasdaq, nyse, Plutocracy, political, Stock Exchanges, support American 99%, US government**

We are a powerful hacker group that support American 99% whom they are under attack by the 1%.

US government must serve people , not Bank & Stock Exchanges.

These are some of the 99% slogans we believe in :

– Banks for people, Not for Banksters!

– Banks for Democracy, Not Plutocracy.

– Dollars should buy goods & services, Not Influence.

– Stock Exchanges are dens of thieves...!

Unfortunately US current political system has failed to meet our needs. We, the 99%, therefore demand the immediate transfer of power to the people.

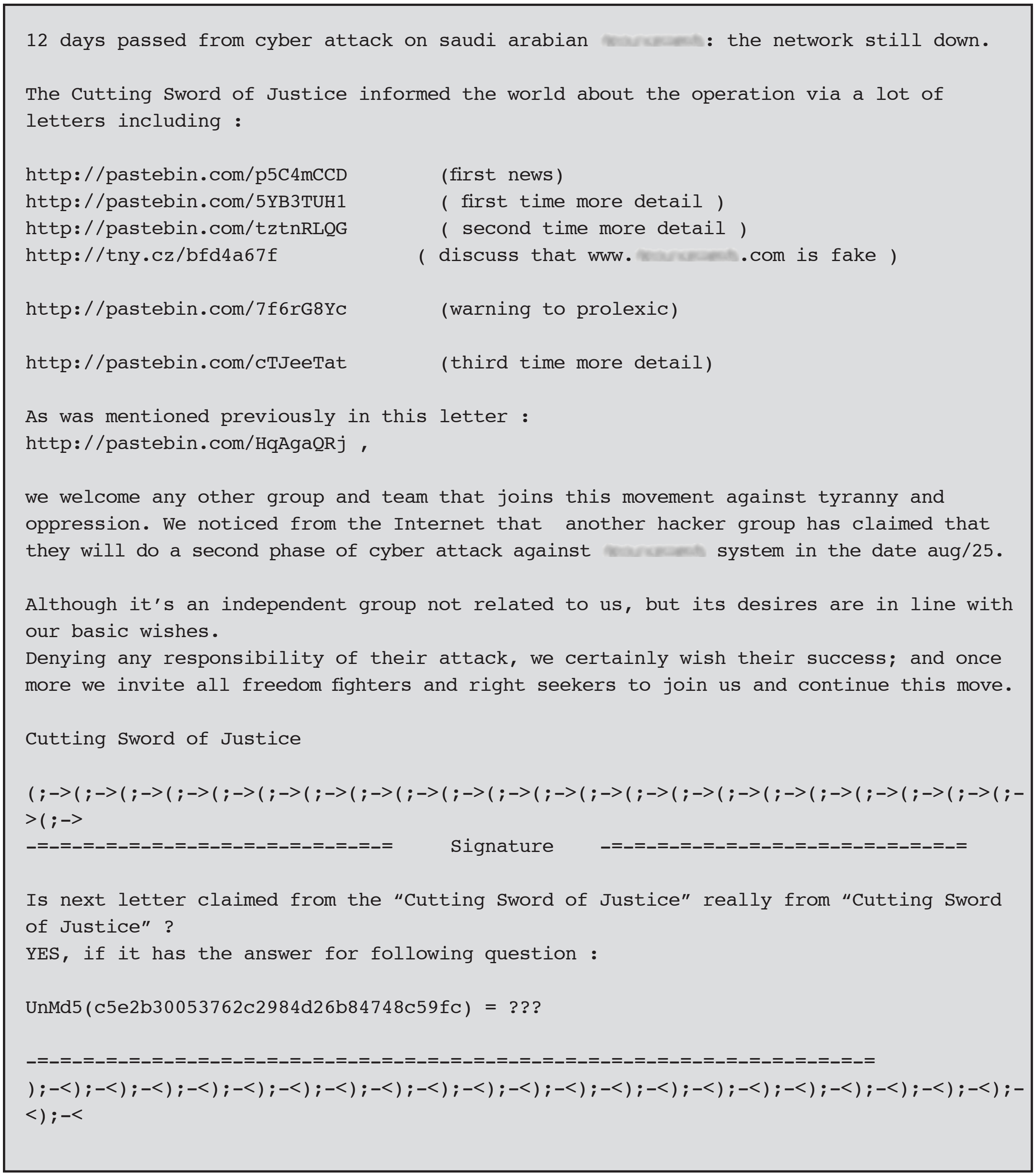
Now we are going to force corrupt officials & politician to hear people voice & resolve their many problems.

Figure 10: An announcement by L0ngWave99 on its website showed support for the goals of the Occupy movement[35]

[35] http://l0ngwave99.wordpress.com/category/our-announcements/

Cutting Sword of Justice

Cutting Sword of Justice pledges its support of the Middle Eastern fight against oppressive governments, specifically the government of Saudi Arabia. In the second week of August 2012, the group started posting Pastebin announcements in which it claimed responsibility for the DDoS and malware attacks on a Saudi Arabian oil company.



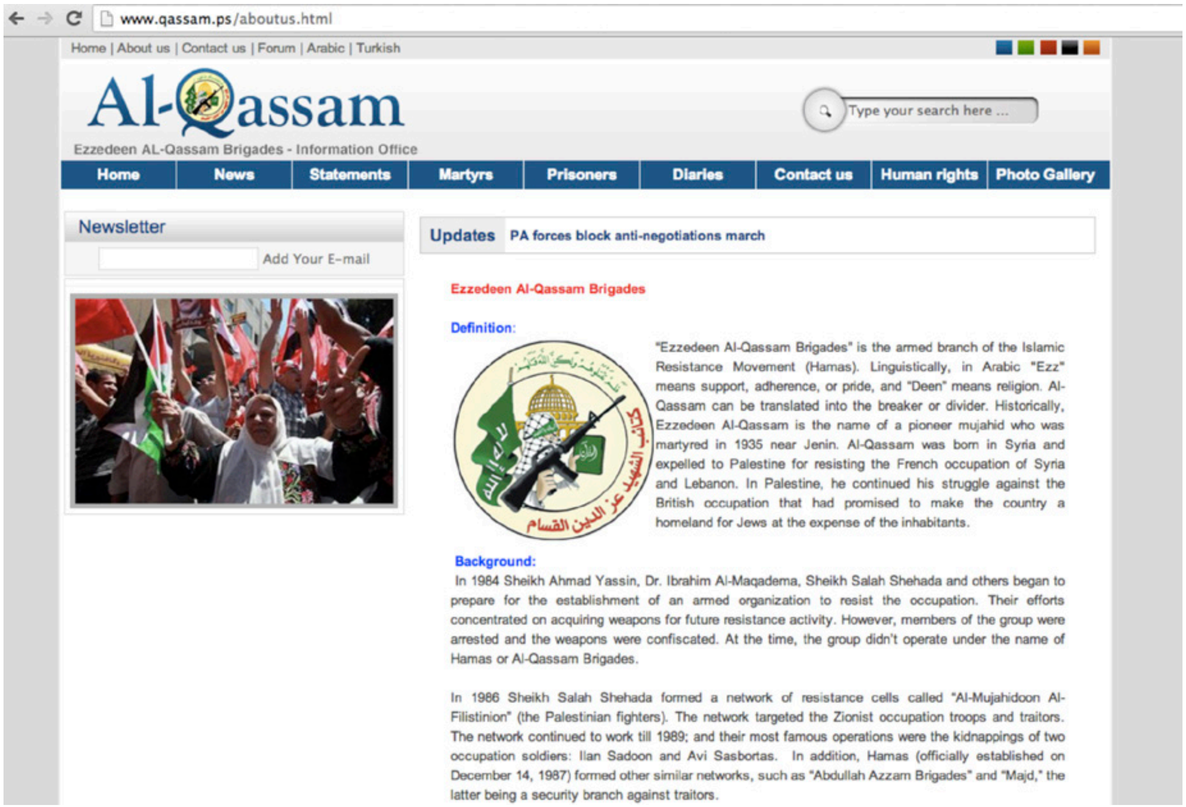
```
12 days passed from cyber attack on saudi arabian [redacted]: the network still down.

The Cutting Sword of Justice informed the world about the operation via a lot of
letters including :

http://pastebin.com/p5C4mCCD        (first news)
http://pastebin.com/5YB3TUH1        ( first time more detail )
http://pastebin.com/tztnRLQG        ( second time more detail )
http://tny.cz/bfd4a67f            ( discuss that www.[redacted].com is fake )

http://pastebin.com/7f6rG8Yc        (warning to prolexic)

http://pastebin.com/cTJeeTat        (third time more detail)

As was mentioned previously in this letter :
http://pastebin.com/HqAgaQRj ,

we welcome any other group and team that joins this movement against tyranny and
oppression. We noticed from the Internet that  another hacker group has claimed that
they will do a second phase of cyber attack against [redacted] system in the date aug/25.

Although it's an independent group not related to us, but its desires are in line with
our basic wishes.
Denying any responsibility of their attack, we certainly wish their success; and once
more we invite all freedom fighters and right seekers to join us and continue this move.

Cutting Sword of Justice

(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;->(;-
>(;->
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=     Signature    -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

Is next letter claimed from the “Cutting Sword of Justice” really from “Cutting Sword
of Justice” ?
YES, if it has the answer for following question :

UnMd5(c5e2b30053762c2984d26b84748c59fc) = ???

-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-<);-
<);-<
```

Figure 11: Pastebin announcements from Cutting Sword of Justice[36]

[36] http://pastebin.com/k2HFJ2LY

Al-Qassam Cyber Fighters (QCF)

Al-Qassam Cyber Fighters, known as QCF, is a group thought to be an extension of the al-Qassam brigades of Hamas. This group is believed to be located in the Middle East, and its website at http://hilf-ol-fozoul.blogspot.com/ promotes pro-Palestine and anti-Western rhetoric. The group claims responsibility for Operation Ababil, a series of DDoS attacks against American financial institutions in 2012 and 2013. The group has a considerable voice in the mainstream media and computer underground.


www.qassam.ps/aboutus.html
Home | About us | Contact us | Forum | Arabic | Turkish
Al-Qassam
Ezzedeen AL-Qassam Brigades - Information Office
Type your search here ...
Home
News
Statements
Martyrs
Prisoners
Diaries
Contact us
Human rights
Photo Gallery
Newsletter
Add Your E-mail
Updates
PA forces block anti-negotiations march

Ezzedeen Al-Qassam Brigades

Definition:

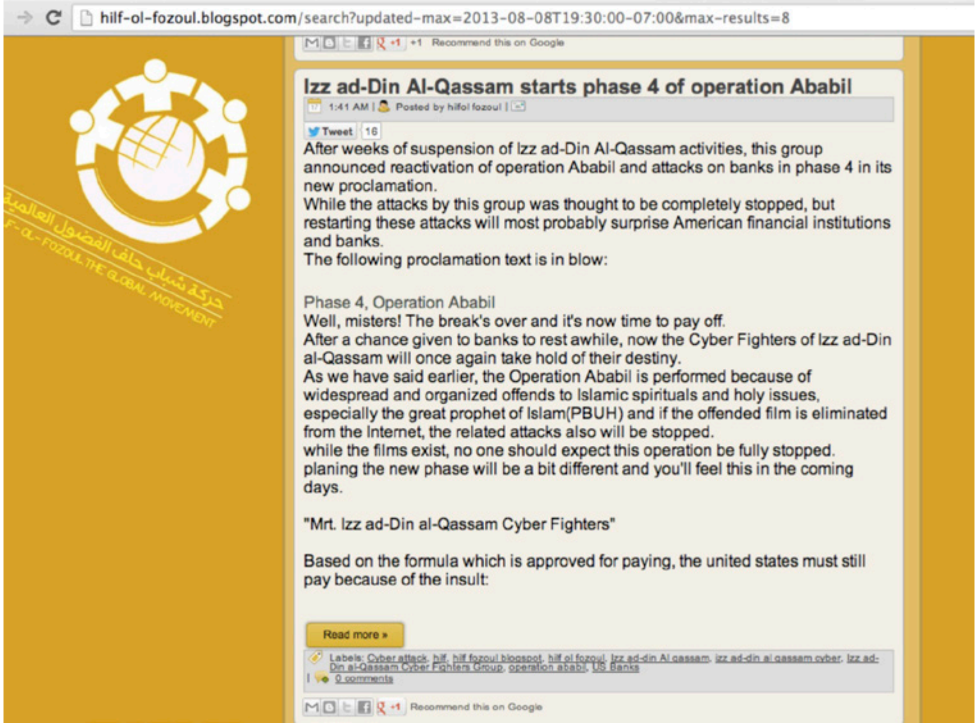
"Ezzedeen Al-Qassam Brigades" is the armed branch of the Islamic Resistance Movement (Hamas). Linguistically, in Arabic "Ezz" means support, adherence, or pride, and "Deen" means religion. Al-Qassam can be translated into the breaker or divider. Historically, Ezzedeen Al-Qassam is the name of a pioneer mujahid who was martyred in 1935 near Jenin. Al-Qassam was born in Syria and expelled to Palestine for resisting the French occupation of Syria and Lebanon. In Palestine, he continued his struggle against the British occupation that had promised to make the country a homeland for Jews at the expense of the inhabitants.

Background:

In 1984 Sheikh Ahmad Yassin, Dr. Ibrahim Al-Maqadema, Sheikh Salah Shehada and others began to prepare for the establishment of an armed organization to resist the occupation. Their efforts concentrated on acquiring weapons for future resistance activity. However, members of the group were arrested and the weapons were confiscated. At the time, the group didn't operate under the name of Hamas or Al-Qassam Brigades.

In 1986 Sheikh Salah Shehada formed a network of resistance cells called "Al-Mujahidoon Al-Filistinion" (the Palestinian fighters). The network targeted the Zionist occupation troops and traitors. The network continued to work till 1989; and their most famous operations were the kidnappings of two occupation soldiers: Ilan Sadoon and Avi Sasbortas. In addition, Hamas (officially established on December 14, 1987) formed other similar networks, such as "Abdullah Azzam Brigades" and "Majd," the latter being a security branch against traitors.

Figure 12: Al-Qassam website



hilf-ol-fozoul.blogspot.com/search?updated-max=2013-08-08T19:30:00-07:00&max-results=8

Izz ad-Din Al-Qassam starts phase 4 of operation Ababil

1:41 AM | Posted by hilfol fozoul |

After weeks of suspension of Izz ad-Din Al-Qassam activities, this group announced reactivation of operation Ababil and attacks on banks in phase 4 in its new proclamation.
While the attacks by this group was thought to be completely stopped, but restarting these attacks will most probably surprise American financial institutions and banks.
The following proclamation text is in blow:

Phase 4, Operation Ababil
Well, misters! The break's over and it's now time to pay off.
After a chance given to banks to rest awhile, now the Cyber Fighters of Izz ad-Din al-Qassam will once again take hold of their destiny.
As we have said earlier, the Operation Ababil is performed because of widespread and organized offends to Islamic spirituals and holy issues, especially the great prophet of Islam(PBUH) and if the offended film is eliminated from the Internet, the related attacks also will be stopped.
while the films exist, no one should expect this operation be fully stopped.
planing the new phase will be a bit different and you'll feel this in the coming days.

"Mrt. Izz ad-Din al-Qassam Cyber Fighters"

Based on the formula which is approved for paying, the united states must still pay because of the insult:

Labels: Cyber attack, hilf, hilf fozoul blogspot, hilf ol fozoul, Izz ad-din Al qassam, izz ad-din al qassam cyber, Izz ad-Din al-Qassam Cyber Fighters Group, operation ababil, US Banks
| 0 comments

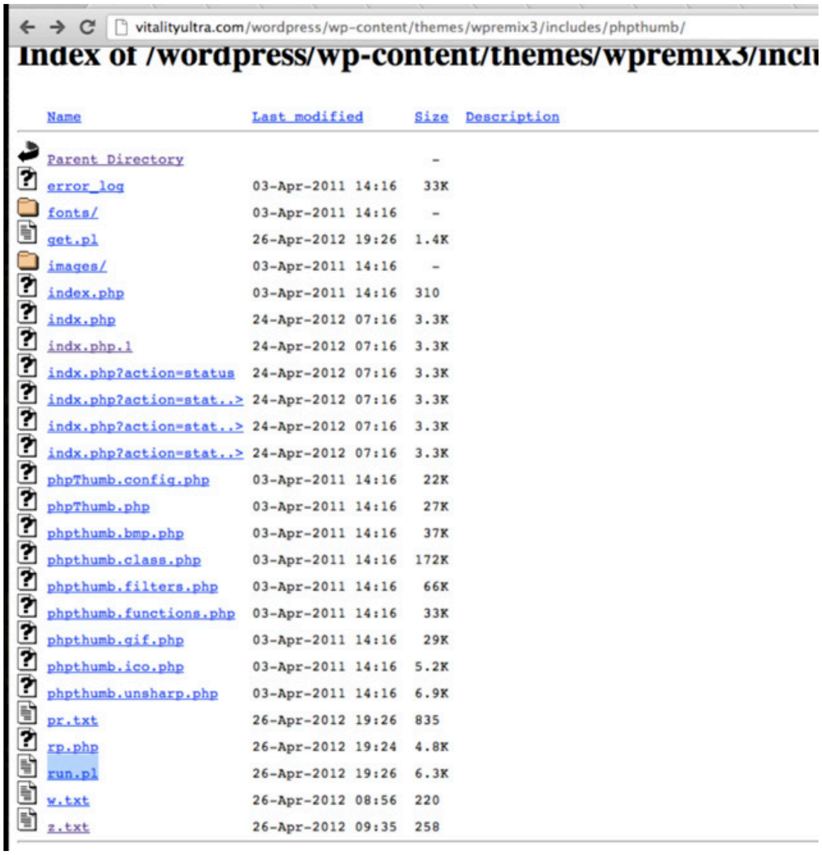
Figure 13: Hilf Ol Fozul website announcement of Operation Ababil phase 4

The group’s supposed motive was the insult to Islam by the publication of a video in YouTube[37], but its real motives seem to be to advance of the cause of free Palestine and to fight against oppressive governments in the Middle East and Western ideals.[38]

QCF claims to have created the tools used during Operation Ababil, which was initially called *itsoknoproblembro* and then evolved into variants, yet L0ngwave99 used the same tools in the same the campaigns and both groups claimed responsibility for the same dates.

The following screen capture shows a tool verified to be BroDoS and later called *itsoknoproblembro* was used on the same date as the DDoS campaign against a US securities and commodities exchange.

[37] http://hilf-ol-fozoul.blogspot.com/2013/07/izz-ad-din-al-qassam-starts-phase-4-of.html
[38] http://www.qassam.ps/aboutus.html



```
vitalityultra.com/wordpress/wp-content/themes/wpremix3/includes/phpthumb/
Index of /wordpress/wp-content/themes/wpremix3/incl

Name                         Last modified      Size  Description

Parent Directory                                  -
error_log                    03-Apr-2011 14:16   33K
fonts/                       03-Apr-2011 14:16    -
get.pl                       26-Apr-2012 19:26  1.4K
images/                      03-Apr-2011 14:16    -
index.php                    03-Apr-2011 14:16  310
indx.php                     24-Apr-2012 07:16  3.3K
indx.php.1                   24-Apr-2012 07:16  3.3K
indx.php?action=status       24-Apr-2012 07:16  3.3K
indx.php?action=stat..>      24-Apr-2012 07:16  3.3K
indx.php?action=stat..>      24-Apr-2012 07:16  3.3K
indx.php?action=stat..>      24-Apr-2012 07:16  3.3K
phpThumb.config.php          03-Apr-2011 14:16   22K
phpThumb.php                 03-Apr-2011 14:16   27K
phpthumb.bmp.php             03-Apr-2011 14:16   37K
phpthumb.class.php           03-Apr-2011 14:16  172K
phpthumb.filters.php         03-Apr-2011 14:16   66K
phpthumb.functions.php       03-Apr-2011 14:16   33K
phpthumb.gif.php             03-Apr-2011 14:16   29K
phpthumb.ico.php             03-Apr-2011 14:16  5.2K
phpthumb.unsharp.php         03-Apr-2011 14:16  6.9K
pr.txt                       26-Apr-2012 19:26  835
rp.php                       26-Apr-2012 19:24  4.8K
run.pl                       26-Apr-2012 19:26  6.3K
w.txt                        26-Apr-2012 08:56  220
z.txt                        26-Apr-2012 09:35  258
```

Figure 14: Snapshot of a directory of DDoS tools used in attack campaigns

The two specific files that were found in both campaigns and with similar code were *indx.php* and *run.pl*. Indx.php was used to provide status checks on the compromised host/zombie. By browsing to the compromised host plus the path *indx.php?action=status*, the host would print a response status. A couple of different messages were used throughout the campaign but the most prevalent was *itsoknoproblembro*.

QCF has shown a considerable ability to organize, orchestrate and execute DDoS attack campaigns. The complexity of the group's tools also indicates a level of sophistication beyond hacktivists and veteran criminals. In addition, the coordination of the group's posts, announced dates, political motives and constant tool development also speaks of a level of resources that could only be provided by a nation state. QCF has been asked directly about its having a relationship with Iran; the group's responses have been ambiguous.

It is clear that the intention behind its attacks was to inflict as much damage as possible on American financial institutions and their customers. The campaigns created a climate of fear, uncertainty and doubt in the financial industry, with rumors that some financial institutions had decided to go offline completely to avoid exposure to these attacks. The malicious actors also sought to influence the market value of these institutions by creating a climate of doubt regarding the ability of these institutions to continue to do business online.

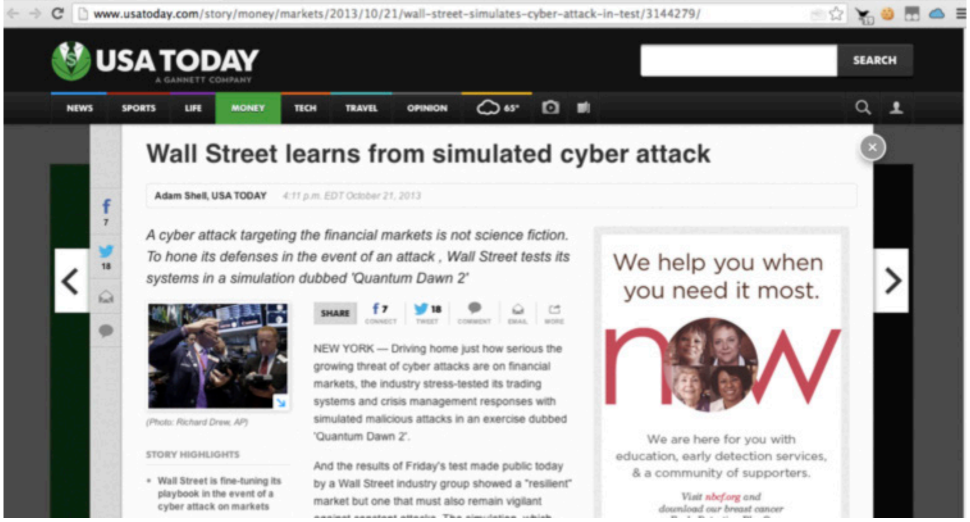
As a result of its perceived success, QCF garnered attention and support from anti-American, anti-Western, pro-Palestinian and, anarchist hacktivist crews, which culminated in #OperationUSA, an unsuccessful campaign that claimed to be a collaboration of hacktivists and anti-Western and state-sponsored actors.

Lately QCF has mostly gone quiet, though the group continues to update its tools and post blogs about anti-Western cyber-attack news relating to Middle Eastern-affiliated groups that share similar goals.

What's next?

Groups like QCF are a sign of the future where insurgency groups migrate their tactics online and adopt hacktivist iconography while targeting American and Western organizations and institutions. PLXSert expects these types of campaigns to migrate to other industry sectors, specifically those perceived to create the most damage to the U.S. if they were to go offline or were unable to operate online.

As a result of these campaigns, American banking and financial institutions are under scrutiny concerning their abilities to withstand these types of attacks. The campaigns have also brought forth a series of initiatives to better prepare the industry for future attacks, as shown in the figure below.



Wall Street learns from simulated cyber attack

Adam Shell, USA TODAY 4:11 p.m. EDT October 21, 2013

A cyber attack targeting the financial markets is not science fiction. To hone its defenses in the event of an attack , Wall Street tests its systems in a simulation dubbed 'Quantum Dawn 2'

(Photo: Richard Drew, AP)

STORY HIGHLIGHTS

- Wall Street is fine-tuning its playbook in the event of a cyber attack on markets

NEW YORK — Driving home just how serious the growing threat of cyber attacks are on financial markets, the industry stress-tested its trading systems and crisis management responses with simulated malicious attacks in an exercise dubbed 'Quantum Dawn 2'.

And the results of Friday's test made public today by a Wall Street industry group showed a "resilient" market but one that must also remain vigilant

Figure 15: A simulated cyber-attack helps financial markets to prepare a better DDoS defense against future attacks

Conclusion

Throughout the history of Internet connectivity, DDoS attacks have proven to be a significant threat to global enterprises and the availability of online resources. This threat continues to the present day.

So far, attacks have not been successful in bringing down an entire major marketplace, such as the two US securities and commodities exchanges, by the sole use of DDoS attacks. This failure might be due to the technological limits of current campaigns. Although there are no indications that a successful attack lies on the horizon without a sizeable increase in attacks and campaigns beyond the scope we have witnessed to date, DDoS attacks keep getting bigger, stronger, longer and more sophisticated, so we cannot rule it out in the future.

With multi-vector attacks within the capabilities of today's malicious actors, it is possible for malicious actors to create conditions that could have negative impacts on markets for specific companies and minor markets, such as:

- A significant DDoS attack campaign that brings denial of service and the disruption of targeted online services
- A number of successful compromises that combine infrastructure vulnerabilities with disclosure of sensitive and confidential information or exfiltration of data that leads to a disruption, pause or suspension of operations
- The effective use of media as a tool to amplify the perceived effect, disruption and damage caused by extended campaigns

The orchestration of multiple factors has been shown to create conditions that can affect public perception (i.e., customers) and the perception of market participants (i.e., investors). Each company targeted by these multi-vector attacks has faced extensive scrutiny and loss of public confidence in its ability to conduct business online successfully.

PLXSert predicts the use of multi-vector campaigns will continue to be employed against not only the financial industry but against other industry verticals. The key factor for malicious actors in their choice of future targets will be their targets' susceptibility to the damage that can be induced by these types of attack campaigns.

About Prolexic Security Engineering & Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through digital forensics and post-attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with customers and the security community. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats.

About Prolexic

Prolexic is the world's largest, most trusted Distributed Denial of Service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission-critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, energy, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Fort Lauderdale, Florida, and has scrubbing centers located in the Americas, Europe and Asia.
To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, follow us on LinkedIn, Facebook, Google+, YouTube, and @Prolexic on Twitter.

PROLEXIC
Now part of Akamai