



VIRCOM

TRUST YOUR EMAIL. TODAY. FOREVER

Pump and Dump

Same Spam - New Tricks

A Vircom Whitepaper

**Vircom Inc.
460, Ste.-Catherine W.
Suite 600
Montreal, Quebec
Canada
(514) 845-1666**

Table of Contents

• Preface	3
• Introduction	4
• Pump and Dump Overview	5
• Text Messages	6-7
• Press Traps	8
• Image Spam	9-10
• Image and Text Spam	11-12
• Pump and Dump Illustrated	13-15
• Summary	16
• About Vircom	17

Preface

As part of our mission to improve and help fully legitimize email communications and in an effort to educate the public on the complexities of Internet scams, spam messages and frauds, Vircom presents its continuing series of studies explaining the methods and tricks that spammer's use. Based on actual spam messages, this study demonstrates how spammers use a variety of different techniques to create and deliver spam messages in an attempt to elude spam-filters.

Contributing Experts

The following Vircom contributors are quoted throughout this document, imparting extensive industry knowledge, messaging security expertise and important advice to readers.



Sylvain Durocher - Founder and Chief Executive Officer

A technology-savvy entrepreneur, Sylvain Durocher founded Vircom in 1994 to meet the needs of the Bulletin Board Service (BBS) operators wanting to become players in the then-emerging Internet Service Provider (ISP) industry. Sylvain has lead the development of three generations of industry-acclaimed product lines that centered more and more on email assurance, which includes products for BBS, VOP (Vircom Online Platform) and now the Modus™ series for both ISPs and companies.



Marc Chouinard – SpamBuster Team Leader

As head of the SpamBuster Team, Marc oversees Vircom's Internet spam monitoring efforts. Constantly developing pre-emptive tools that analyze spam patterns instead of just instances, Marc ensures that the technology driving Vircom's Sequential Content Analyzer™ engine remains ahead of the latest spam tactics.

Methodology

Vircom’s SpamBuster Team monitors thousands of emails per day. The spam messages used in this study were chosen based on the frequency of occurrence as well as their type. Vircom uses a system of honey pots to create and monitor spam activities throughout the world.

Introduction

Since the advent of electronic mail, unscrupulous persons have used it for personal gains by sending spam. Whether it is to hawk pills, sell porn or to scam people out of their life’s savings, spammers will try anything.

The goal of any spammers is simple – **to make money**. In order to do so, they need to create a message that will entice the recipient to respond quickly and without thinking. They need to send out millions of these messages, and they need to elude the spam-filters set up to protect the recipients’ mailbox from these types of messages.

So how does a spammer do that?

How is a spammer able to elude a spam-filter?

Why are certain types of spam messages still effective after all of these years?

This study examines some of the latest tricks that spammers use in order to elude spam-filters. We examine one of the most common types of spam message occurring today “The Pump and Dump Scheme” and look at how this spam message has evolved, and the tricks that spammers use to stay one step ahead of the spam filter.

“Pump and Dump”

Overview:

“Pump and dump” schemes are also known as “hype and dump manipulation” and “ground floor opportunities;” they involve the touting of a company’s stock through false and often times misleading statements to the marketplace. After pumping the stocks’ value, spammers and scammers make huge profits by selling their shares into the market at inflated prices.

Over the Internet, it is very common to see posted messages that urge readers to buy a stock quickly or to sell it before the price goes down. Often the message will claim to have unique “insider” information about an impending development or the use of an “infallible” combination of economic and stock market data to pick the stocks.

The perpetrators of this type of scam may be company insiders or paid promoters who stand to gain huge profits by selling their shares after the stock price is “pumped” up by the buying frenzy they create. Most of the time though, they are scammers who are not associated at all with the company being pumped and dumped and pick it based upon nothing more than the low value of the stock. In fact most stocks involved in a pump and dump scheme trade initially for less than \$1.00 per share.

Once these fraudsters “dump” their shares and stop hyping the stock, the price will typically fall, and investors will lose all or part of their money. The company being “pumped” may have had nothing at all to do with the scam, but they face the wrath of the investors who were ripped off, as well as the economic community as a whole.



MC ” *One aspect that is nearly always forgotten when we speak of a pump and dump scam is the devastating effects that this type of scam can have on the company that is being pumped. A legitimate company that falls victim to a pump and dump scheme may face all sorts of legal and disciplinary charges including lawsuits and possible de-listing from stock markets.”*

How Spammers Elude the Spam Filter

Most pump and dump schemes are created by a spammer in one of three specific methods, which is dependant upon the techniques and sophistication of the spammer and the ways they have to distribute the message.

Method 1: - Text Messages

Text messages although the simplest to create are probably the most difficult types of message for the spammer to deliver effectively. The simple fact that most spam-filters can easily be trained to identify specific key words, sentences or message structures, makes the job of the spammer a lot more challenging when they create a spam message using text only. However, depending upon the type of spam-filter the text message method can be quite effective.

Trading A|ert Starting Friday!

We pick our companies based on there growth potential.

IF you are Receiving this email, you are among the first public investors to know about E G L Y !!! A \$1,000 do||ar investment could yield a \$2,000 do||ar profit in just ONE trade if you trade out at the top. We have come across what we feel is one of those rear deals that the public has not heard about yet. We believe that E_G_L_Y is a perfect addition to any traders portfolio

Typical Pump and Dump Spam Message

The idea although simple in nature lacked a number of important aspects to make it truly effective:

1) Spam-filters – Most spam-filters are very effective at detecting and eliminating this type of spam message. In fact, over 98% of these types of messages are caught in a spam-filter. Because of this, the spammer was forced to try to disguise the message. As illustrated, the spammer attempted to disguise the message by misspelling certain words like **do||ar** and **A|ert**.

2) Credibility - Receiving a vague email with purposely misspelled words does not entice most recipients to give it a second glance. In fact, the majority of the messages that would bypass a spam-filter would be simply deleted by the recipient and never opened.

**T
e
x
t

M
e
s
s
a
g
e
s**

MC "A low quality spam-filter relying upon key words exclusively as its main method to detect spam can be tricked easily by a spam message that focuses upon financial information rather than typical spam words like "Viagra" or "Cialis".



SD "In an attempt to trick certain spam-filters a spammer when creating a text-based pump and dump message will make the message long containing a great number of words. One of the basic functionalities of any spam-filter is to measure the "spamminess" of a message. So for example, if the message is short and has a high percentage of key words in it that the filter classifies as spam, then the message will most likely will be blocked. However, if you are to take the same message and simply increase the length of the message but have the same number of words that would be considered spam, then the overall percentage of "spaminess" of the message would be lower, and thus the spam may be able to bypass certain spam-filters".

phlebolith

Coiled tubing units are so compact and have such great potential, the Mars Drilling Project is evaluating a coiled tubing unit to drill for water on Mars. blade

aghost

SPRING, TX--(MARKET WIRE)-- Coil Tubing Technology, Inc. (CTBG) announces the delivery of the first group of 8 Rotating Tools to oil and gas well service companies operating in Mexico and Oklahoma. Designed for use in "fishing" applications utilizing 2" coiled tubing strings, these tools were delivered and "in the field" the week of May 1, 2006 testamentum

regrator

In addition, CTBG has received orders for ten more of these 2 7/8" Rotating Tool units, plus five 2 1/8" Rotating Tools, all of which are scheduled for delivery to customers before the end of the month of May... embark

obdurately

... There is less visual impact as the units are small with no large derrick tower. arenicolous

atheromata

All of this means that coiled tubing units are more cost effective, energy efficient, have a much smaller environmental footprint, and create less waste. In certain drilling operations, coiled tubing units cost approximately half of what a conventional drill rig would cost. multiplier

feedstuffs

In fact, coiled tubing units are so compact and have such great potential, the Mars Drilling Project is evaluating modifying, miniaturizing and fully automating a coiled tubing unit to drill for water on Mars. Realistically, it will be years before the unit is developed and sent to by rocket to Mars, but it would be an important first step before Mars could be colonized. And coiled tubing technology will be be greatly improved by the research.

laughter

basketwork

[For more information on CTBG, please visit Yahoo Finance - CTBG](#) rhone

took

The BottomLine Report is not liable for any decisions by its readers or subscribers. The information contained herein has been provided as an information service only. The BottomLine Report purchased 270,000 shares at 0.15. We may close our positions at any time. forensicality

ascospore

**P
r
e
s
s

T
r
a
p**

MC "The above is a very poor example of a text-based pump and dump spam message. The spammer copied a press release word-for-word and placed it into the spam message. The spammer neglected to add the call to action until the very last sentence of this message, which is a mistake given that the odds are very slight that anyone would read this message in its entirety."



SD "The spammer also used a technique called hashing (highlighted in grey) not in an attempt to trick the spam-filter, but as a method to format the email with new paragraphs. This lack of coding skills on the spammer's part actually made it a very simple spam message for us to catch."

Hashing involves trying to disguise text by creating words or a legitimate message in a font color that is the same or very similar to the background color (for example, white on white or black on black). The results of this would be that the recipient would not be able to read the words or legitimate text but only see the displayed text. Most spam-filters can easily detect and eliminate spam messages that incorporate this technique.



MC "What was needed by the spammer was a way in which to add some credibility to the message, as well as to make it appear official. The answer came in a new trick in the spammer's arsenal, the "Press Trap."

Spammers Get Smarter with 'Press Trap' Con

By 2004, spammers started using a con called a "press trap" to add credibility to a pump and dump message. To do this, the spammer might take a newly published press release from the particular company, and add it to the spam message that they have created. The release is usually no more than a few days old and the spammer will then target the pump for several days before the dump occurs.

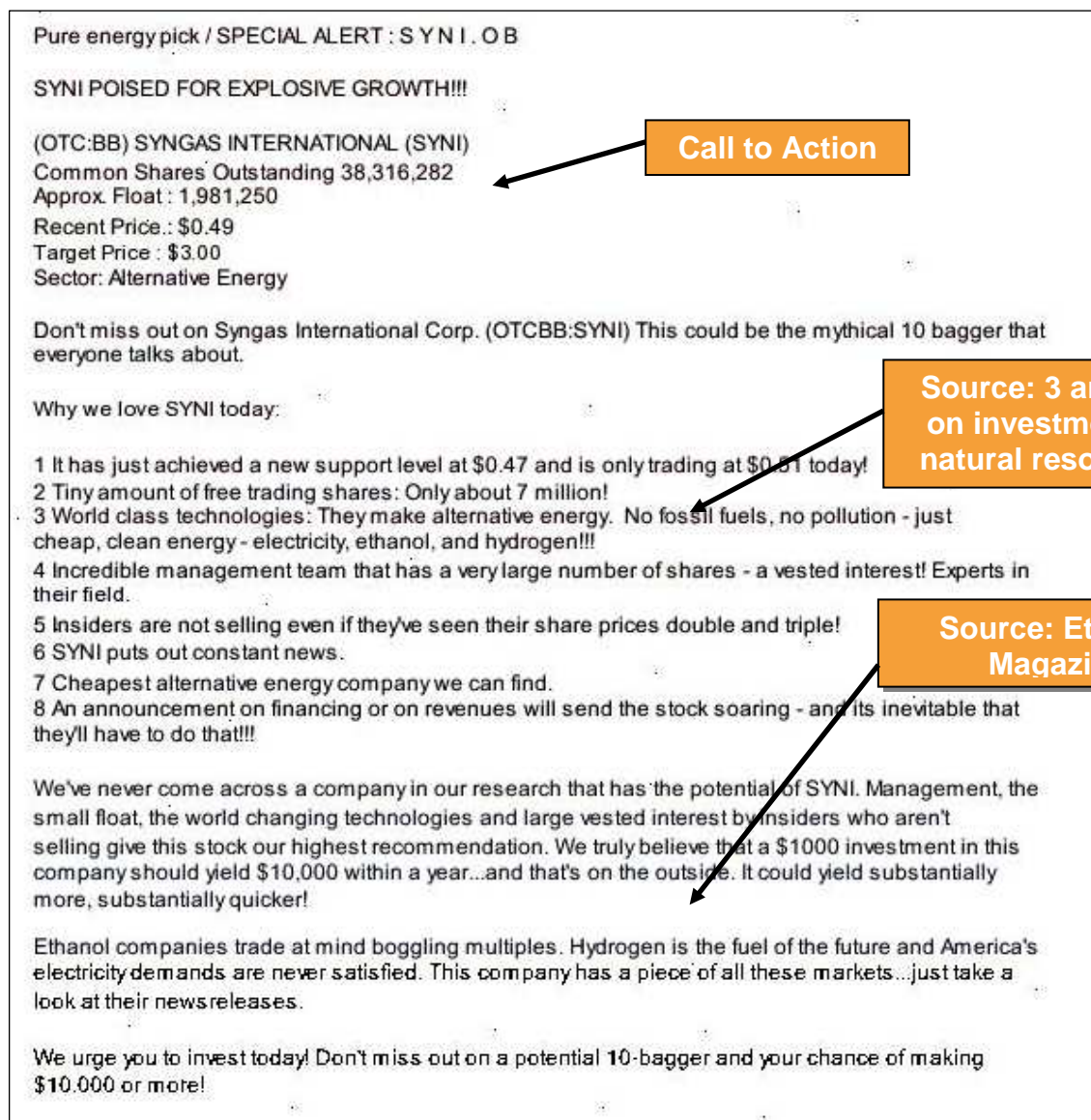


SD "Timing is critical in any pump and dump scheme when using a press trap. Spammers we have spoken with have all told us that in order to have an effective spam campaign, it must be able to bypass a spam-filter. If the message is successful and can bypass the filter, then it can usually be distributed for a three to five-day period before a fix can be put into place by the company that develops the spam-filter. Additionally for a pump and dump scheme to be effective, the spammer must make the recipient react quickly and without thinking, therefore sending the blast within the three to five-day timeframe will create the right sense of urgency to be potentially quite effective."

Method 2 – Image spam

Today spammers must incorporate new techniques in order to bypass a spam-filter. Since any key word can be eliminated by a spam-filter, it is imperative that the spammer disguise or camouflage the word so that the recipient can read it easily, while at the same time making it impossible for the spam-filter to recognize.

Spammers quickly realized that the easiest way to do this is to create an image with the message in it. Because the text message is now embedded within the image, this technique attempts to trick the spam-filter by eliminating the analysis of text as a method to detect spam.



Pure energy pick / SPECIAL ALERT : S Y N I . O B

SYNI POISED FOR EXPLOSIVE GROWTH!!!

(OTC:BB) SYNGAS INTERNATIONAL (SYNI)
Common Shares Outstanding 38,316,282
Approx. Float : 1,981,250
Recent Price : \$0.49
Target Price : \$3.00
Sector: Alternative Energy

Don't miss out on Syngas International Corp. (OTCBB:SYNI) This could be the mythical 10 bagger that everyone talks about.

Why we love SYNI today:

- 1 It has just achieved a new support level at \$0.47 and is only trading at \$0.51 today!
- 2 Tiny amount of free trading shares: Only about 7 million!
- 3 World class technologies: They make alternative energy. No fossil fuels, no pollution - just cheap, clean energy - electricity, ethanol, and hydrogen!!!
- 4 Incredible management team that has a very large number of shares - a vested interest! Experts in their field.
- 5 Insiders are not selling even if they've seen their share prices double and triple!
- 6 SYNI puts out constant news.
- 7 Cheapest alternative energy company we can find.
- 8 An announcement on financing or on revenues will send the stock soaring - and its inevitable that they'll have to do that!!!

We've never come across a company in our research that has the potential of SYNI. Management, the small float, the world changing technologies and large vested interest by insiders who aren't selling give this stock our highest recommendation. We truly believe that a \$1000 investment in this company should yield \$10,000 within a year...and that's on the outside. It could yield substantially more, substantially quicker!

Ethanol companies trade at mind boggling multiples. Hydrogen is the fuel of the future and America's electricity demands are never satisfied. This company has a piece of all these markets...just take a look at their news releases.

We urge you to invest today! Don't miss out on a potential 10-bagger and your chance of making \$10,000 or more!

Call to Action (points to "SYNI POISED FOR EXPLOSIVE GROWTH!!!")

Source: 3 articles on investment in natural resources (points to "World class technologies: They make alternative energy...")

Source: Ethanol Magazine (points to "Ethanol companies trade at mind boggling multiples...")

**I
m
a
g
e

S
p
a
m**

"This is a typical pump and dump image-based spam message. The spammer who created this message though was quite original in that they used a variety of different press trap techniques, cutting and pasting several different press clippings to create the message. The top section is the call to action created by the spammer. The middle section was taken from several articles on investment in natural resources, while the lower section of the message was taken from an article in Ethanol Magazine. Usually a spammer will simply create the call to action and add the pumped company's press release as the press trap."



"This particular company has been the victim of numerous pump and dump schemes. Over the last six months. On average we have received two distinct spam campaigns per month, with a minimum of three email blasts per campaign. This particular campaign took place over a three-day period where four email blasts in total were sent."

**I
m
a
g
e
&
T
e
x
t
s
p
a
m**

Method 3: - Image and Text Messages

Incorporating a combination of images and text within a spam message is the latest tool in a spammer’s arsenal. By disguising key words or phrases within an image and by adding text that is not considered spam such as a press release, or text from magazines and books, a spammer can trick all but the most sophisticated spam-filter.

Hot Pick For the week of July 17th
Our last weeks picked gained over 600 %
Get PSUD First Thing Monday, This Is Going To Explode!

PETROSUN DRILLING (PSUD)
Current Price: 1.35
Est 5 day 2.86

Image →

Current News:

PetroSun Announces Formation of Algae BioFuels
 Thursday June 22, 1:00 pm ET
 Subsidiary to Develop Algae-Based Biodiesel
 Alternative Energy Resource to Supplement Petroleum-Based Fuels

Press Trap →

PHOENIX--(BUSINESS WIRE)--June 22, 2006--PetroSun Drilling Inc. (Pink Sheets: PSUD - News), an emerging provider of oilfield services to major and independent producers of oil and natural gas, announced today that the company has formed Algae BioFuels Inc. as a wholly owned subsidiary. Algae BioFuels will be engaged in the research and development of algae cultivation as an energy source in the production of biodiesel, an economically feasible and eco-friendly alternative to petroleum-based transportation fuels. The R&D and production facilities for Algae BioFuels will be based in Arizona and Australia.

"PetroSun's formation of Algae BioFuels is a forward-looking strategy," said L. Rayfield Wright, president of PetroSun. "The opportunity to produce a renewable energy product that will assist in providing a healthier planet for future generations cannot be ignored."

Biofuel is any fuel that is derived from biomass -- which contains recently living organisms or their metabolic byproducts. Biofuel is a renewable energy source, unlike other natural resources such as petroleum, coal and nuclear fuels. Agricultural products specifically grown for use as biofuels include corn and soybeans.

Extensive research is currently being conducted to determine the utilization of microalgae as an energy source, with applications being developed for biodiesel, ethanol, methanol, methane and even hydrogen. Independent studies have demonstrated that algae is capable of producing 30 times more oil per acre than the current crops now utilized for the production of biofuels. Algae biofuel contains no sulfur, is non-toxic and highly biodegradable.

The Office of Fuels Development, a division of the Department of Energy, funded a program from 1978 through 1996 under the National Renewable Energy Laboratory known as the "Aquatic Species Program." The focus of this program was to investigate high-oil algae that could be grown specifically for the purpose of wide-scale biodiesel production. Some species of algae are ideally suited to biodiesel production due to their high oil content, in excess of 50%, and extremely rapid growth rates.

One of the biggest advantages of biodiesel, compared to many other alternative transportation fuels, is that it can be used in existing diesel engines, which relieves automotive manufacturers of having to make costly engine modifications. Biodiesel can also be mixed, at any ratio, with conventional petroleum diesel. As a result, the alternative fuel can be used in the current distribution infrastructure, replacing petroleum diesel either wholly, or as a diesel fuel blend with minimal integration costs.

**I
m
a
g
e
&
T
e
x
t
S
p
a
m**

“We are coming across this type of pump and dump message more and more lately. The image part of the message contains the words and phrases that a spam-filter could be trained to look for (Hot Pick, current price, This is Going to Explode). The spammer then incorporates a press trap of text incorporating the companies recently announced press release.”



“The spammer also attempted to trick an advanced spam filter by incorporating a number of grammatical errors in the image portion of the message including: Last Weeks Picked Gained, as well as having stock prices without currency signs 1.35 and 2.86.”

Medium strength spam-filters are capable of eliminating image-based spam messages by blocking all incoming messages that contain images or are images. This anti-spam technique will cause high false positive rates as legitimate email correspondence that contain images will also be trapped by the filter.

A superior spam-filter like Vircom’s Modus™ has anti-image spam technology that is capable of analyzing the content of an image and thus eliminating this type of spam with a catch rate in excess of 98% and a false positive rate below 0.1%.

Pump and Dump Example

In order to fully understand the potential hazards of a pump and dump scheme, it is necessary to examine the cycle of this type of message from; how it was created and distributed, through to the end of the pump and dump campaign and its effectiveness.

WHAT A WAY TO START OUT THE WEEK!

Company: ESPION INTERNATIONAL INC(EPLJ)
On: PinkSheets
Symbol: EPLJ.PK
Wednesday Close: 0.23 (up 16%)
Market Cap of: ~\$21 Million

Call to Action

Press Trap

Breaking News Released!
COSTA MESA, CA--(MARKET WIRE)--May 30, 2006 -- The Board of Directors of Espion International, Inc. (Other OTC:EPLJ.PK - News), a publicly traded company with a unique, proprietary, artificial intelligence solution for e-mail security and outbound message compliance, today announced that Stephen C. Dow, 47, was elected CEO effective June 1, 2006. Mr. Dow was the CEO and Founder of Channel Access, LLC until March of 2006 when it was acquired by the Carlo Gavazzi Group of Companies.

Since 1977, Mr. Dow has been a leader in technology sales, marketing, and systems integration. Mr. Dow spent 14 years with Force Computers, Inc. prior to co-founding Channel Access. During his career with Force Computers he progressed through several positions of increasing responsibility in sales and marketing and he ultimately served as COO & General Manager of the America's, where he was responsible for the all operations of an international company which grew from under \$3 million in revenues to over \$150 million in revenues during his tenure. His general management assignments spanned several areas within Force Computer's embedded computer systems business, including the positions of Vice President and General Manager of the America's, Vice President of Operations, Vice President of Sales and Marketing, and Director of Sales. In November of 1996, Mr. Dow led the team that negotiated the sale of Force Computers to Solectron Corporation for \$205 million.
Read more about this breaking news on your favorite financial website.

ADD EPLJ TO YOUR WATCHLIST NOW! WATCH IT TRADE ON MONDAY JUNE 5th!

Disclaimer: www.datezforforall.com and Removal: mail@purgington.com or 702-939-1431

**P
u
m
p
&
D
u
m
p**

The following spam email was received by the Vircom SpamBuster Team on Thursday, June 1, 2006. It was one of ten separate spam blasts that were sent between June 1 and June 3, 2006. The message in each spam blast was the same inviting potential investors to purchase the stock in question on Monday, June 5, 2006. Added to each spam message was a copy of the press release that the company had placed on Market Wire on the 30th of May 2006.



MC *“It is the timing and the fact that the spammers incorporated the company’s press release into the email message that makes this an effective type of spam. The spam message was created and tested, and the first blast was sent within one day of the company’s news release.”*



SD *“Additionally, the spammers pulled the information from a news service like Market Wire. Wire news services are the perfect source to find timely information; they are the source for much of the financial news used by companies like Bloomberg and Forbes. So by using a wire service, it is quite possible for a spammer to create and distribute a spam message before a legitimate news agency publishes it on their site.”*

Effects of this Pump and Dump Scheme:

The best way to see how effective this particular pump and dump scheme was is to look at what exactly took place on and around June 5, 2006.

With an average volume of less than 30,000 shares traded per day, this pump and dump scheme on the surface looks to be quite effective:

Date	Volume (Shares Traded)	Description
May 31	15,170	Day before email blast began
June 1	145,560	3 email blasts sent
June 2	84,370	2 email blasts sent
June 5	484,030	Pump and Dump day
June 6	252,008	Pump and Dump day plus 1

The increases in volumes are quite significant between the days preceding, during and following the pump and dump campaign.

For example, if we were to compare the day preceding the pump and dump campaign (May 31) to the day of the pump and dump (June 5), the results would indicate that more than 39 times the volume of shares were traded on the 5th of June.

**P
u
m
p
&
D
u
m
p**



“In terms of volume, this pump and dump scheme was so successful, that it actually accounted for the highest volume of trade in the history of this stock.”

Profit Effects:

It is difficult to measure the possible profits that the spammers could have made without knowing how many shares they owned to begin with, but it is possible to deduce the following:

The scam was conceptualized between May 30, 2006 (The date the press release was made public) and June 1, 2006 (The date of the first email blast). Reviewing the historical data, it is most likely that the spammers would have purchased their shares at a price of between \$0.16 and \$0.22 per share (The lows and highs for those days).

If the spammers traded their shares on the dump day (June 5), they would have sold it in all likelihood for between \$0.29 and \$0.30 per share (The lows and highs for that day). This would net the spammers between 25% and 45% profit in less than five days.

Price Purchased	Price Sold	Percentage Profit
\$0.16 - \$0.22 The High and Low Market Price for May 30 – Jun 1, 2006	\$0.29 - \$0.30 The High and Low Market Price for Jun 5, 2006	25% - 45%

Company Effects:

The company that was the victim of this pump and dump scheme was forced to release a statement to the media exonerating itself from any knowledge of this particular email campaign:

“I can assure you that no officer, director, or beneficial owner has entertained such an email campaign, nor has hired any email marketing company to send unsolicited emails.” – Espion International

Protecting yourself against Pump and Dump Schemes

Learn to identify its characteristics:

- Calls to action
- Promoting stocks, bonds and shares in publicly traded companies
- Claims of inside information
- Use of free web-mail addresses



SD *"What makes these types of spam messages so difficult for a spam-filter to catch is that by adding a legitimate press or news release to the message, it usually will not contain quotes or words that are typically associated with spam. However, a spam-filter can be trained to recognize and quarantine messages that contain key words or phrases associated with this type of spam. They can also learn to detect patterns and traits in the message that would enable it to eliminate all future spam messages of this type."*

General rules for receiving spam messages

Never respond to any email that looks suspicious or sounds too good to be true. Upon receiving any suspicious email messages, contact your Internet Service Provider via the designated email abuse address (e.g. *abuse@provider.com*). Include the original message and your complaint; the provider should be able to close down the offending account.

Summary

Although we have concentrated on pump and dump schemes, the tricks used by the spammers as outlined in this study can easily be integrated into any type of spam.

As technology advances as long as spammers can make a profit they will continue to create and distribute their messages.

It is the "Same old Spam – New Tricks!"

About Vircom

Montreal-based Vircom is a leading developer of cutting-edge Internet infrastructure and secure messaging solutions for the demanding needs of Internet Service Providers (ISPs) and corporate clients. Vircom's mature Modus™ secure email management technology incorporates over 10 years of industry expertise, making it a powerful driving force in the defence against spam and email-borne fraud.

Labelled the Best Microsoft® Windows®-based Anti-Spam solution by Network Computing Magazine, Modus™ has gained important recognition, among which is a CATAAlliance Innovation & Leadership Award and a record-breaking five-award distinction including "Best Software Product" and "Most Innovative Product" from Windows IT Pro magazine.

Vircom is also the developer of VOP Radius, a full-featured all-in-one RADIUS server that supports the latest RFCs, vendor specific attributes, NAS templates and has a multitude of preconfigured settings.

About the Vircom SpamBuster Team

Vircom's SpamBuster Team is a group of highly trained email professionals who track, adjust and constantly improve the performance of all Modus™ anti-spam solutions to ensure they maintain the highest performance and accuracy levels. The SpamBuster Team is also heavily involved in analyzing spamming trends and ensuring that Modus™ solutions always stay a step ahead of spammers.