An introduction to the parasite economy

(Research in Progress Short Paper / Student Paper)

Stefan Görling
The Royal Institute of Technology (KTH), Sweden

About the author

Stefan Görling is a graduate student at the department of Industrial Management at the Royal Institute of Technology in Stockholm, Sweden. He is a part of the Pink Machine research group which focus on wide variety of aspects of technology and economy that are routinely ignored by the research community out of fear of not seeming "serious" enough, and that at the same time form an intimate part of both everyday life and the post-industrial production of value. His research interests presently include the economy behind the less popular artefacts of the Internet, adware, spyware, spam and computer viruses.

Mailing Address: INDEK, KTH, 100 44 Stockholm, SWEDEN; Phone +46-70-815 38 26; Fax: +46-8-790 76 17; E-mail: stefan@gorling.se; Home page: http://www.parasite-economy.com

Descriptors
Spyware, adware, malware, spam, computer viruses, worms, immoral business-models, navigators, affiliate programs, social engineering.

Reference to, or **Citation** of this paper should be made as follows:
Görling, S. (2004). An Introduction to the Parasite Economy. In U.E. Gattiker (Ed.), EICAR 2004 Conference CD-rom: Best Paper Proceedings (ISBN: 87-987271-6-8) 13 pages. Copenhagen: EICAR e.V.

An introduction to the parasite economy

Abstract

This paper gives an introduction to a number of immoral business-models that have been established as a part of the Internet-economy. It discusses how breaking into computers has become a viable business model for corporations and how the Internet-underground is challenging our view of what a company is. The paper tries to group a number of similar business models such as spyware, adware, viruses, spam etc. under a common term, parasites, and discuss how they are a part of viable business-models rather than merely an annoyance to the computer users.

Introduction

There is an old saying that the porn industry is the leader of technical development in the Internet era, pushing the limits with high demands on availability, security and payment options. Whether this is true or simply a myth that has become famous as an amusing sales pitch is unclear.

However, when Oracle Corporation recently called for attention by releasing their new product under the theme: "Enter the Grid!", the saying just might have become true.

Grid technology is a group name for various methods to connect a large number of small computers into a larger network, using standard computers working together, delivering more performance than the largest supercomputers in the world. Mostly in the same way as our common power-grids are (supposed to be) working, connecting a number of small power-sources on a network serving all users, instead of having each user dependent on a single power-source, which were the case in the era of the wind-mills.

"We are at the beginning of a revolution, a whole new way to look upon computing in terms of performance and cost", their CEO told us. And suddenly, I realize that the myth might be true. Grid technology is the answer. Finally, all the crackers and creators of trojans, viruses and spyware have a decent use for all the computing power they have obtained by breaking in to ordinary home PCs.

Earlier attempts to sell distributed computing resources have failed, not only because there was no usable standard on how to do it, but it also raised the question on how much a cpu-cycle was worth and how to reimburse the large number of users who contributed. Current applications such as SETI and the Google toolbar cancer project live on as they are non-profit, for the better of humanity. However, if you start to earn money on selling other peoples resources, they want their share of it.

Enter the viruses.

There are a number of parasites (viruses/worms/trojans/etc) that break in into your computer and take control of it. Earlier viruses focused on spreading rapidly, to be efficient in the means of getting a large number of machines infected, but without doing any useful with the resources as they control them. We are now seeing viruses that actually do something, viruses with a purpose.

One famous example was W32.SOBIG.F. During a few days in the beginning of September 2003 newspapers reported rapidly on its progress. First it spread like no other virus earlier had done. Once it was spread, it was supposed to report to base and await further instructions. The virus contained 20 encrypted web-addresses where it could retrieve the instructions on certain dates. Virtually all computer-crime fighting agencies in the world worked to break the code and they disabled the 20 computers before they were able to do any harm. The computers were ordinary home computers with broadband connections that had been kidnapped by the virus creator at some earlier occasion.

We don’t know what the real intent of this virus was, but it revealed the fact that viruses are a powerful tool, which could not only be utilized by teenagers bored with school but by professionals such as terrorist organizations to create powerful threats.

There are now a rapidly growing number of viruses with an outspoken intent to do something more than to spread. Taken a sample day, October 1st introduced three new viruses of which two intended to be able to redirect the infected computers to certain home-pages when the user surfed. One of the viruses changed the home page and bookmarks to an Asian home page (Symantec 2003-10-01). The other one took control over the name-server resolve so that they could direct to different homepages on the fly, perhaps in accordance to the wishes of the highest bidder.

A possible next generation might soon be here, considering the current trends in distributed computing as well as virus creation. A “company” might spread the next generation of viruses. It could take control over your computer and install a Grid computing toolkit and then check back to its master, a server on an oil-rig on international water where the "company" is located. Customers requiring vast amounts of computing resources could hire the "company" as a sub-contractor to perform certain calculations with "their" computing resources. Even if the company are unable to obtain serious companies as customers there are a vast amount of less "moral" organizations in need for more computing resources.

After all, code-breaking is one of the classical uses for distributed computing and terrorist organizations are only one popular example of well-financed organizations in need of code-breaking capacity.

The parasite economy

The purpose of this rather long introduction was not only to frighten you what your computer could be used for. It was also supposed to illustrate how parasites work and what they could be used for.

We will now move on to a more formal discussion on what the parasite economy is and what kinds of parasites there are. My research on the parasite economy is an ongoing project and this paper will discuss some of properties of this economy that I have discovered so far.

Using lack of moral to gain competitive advantage

As the competition increases in a market, finding new relative advantages towards your competitors is being increasingly difficult. The closer your market comes to become a "perfect" market; your margins are steadily decreasing. In a perfect market, the margins are near zero. If anyone could produce a product at a lower cost, they would do it in order to take your profit. So the competitors are chasing each other, in an every increasing pace.

"So they increase the pace. But, no matter how fast they run they never move from the spot. Because, no matter how fast they run they always have to run twice as fast to get anywhere" (Gustafsson, 2001, p. 10, my translation)

Gustafsson argues that companies in a market economy are continuously trying to find ways to run faster, but since everyone is doing it you have to run only to keep your position on the market.

As discussed by among others Philip Kotler et al. (1996), the key to surviving in a certain market is to gain some kind of competitive advantage. You have to do something better than the others. Most agree that the tougher your competition is, the better your competitors are, the harder it is for you to gain a significant competitive advantage. At some point people get tired of running.

Even though the competition in a market initially seems to be tough, there is an old and proven way to gain this advantage. Gaining competitive advantage within the rules of your legal entity might be hard. But if everyone is obeying to the rules, you would get a significant advantage if you were not bound to them yourself. If you were not to obey environment laws, production-costs would be lower. If you stole your products, your marginal production cost most certainly would go down.

The parasite economy is built by companies who have noticed this and made it the core of their business.

The Internet-era is interesting in many ways. One of them is its reach beyond the legislation of local countries. This makes Cyberspace an environment where local laws and moral standards can be avoided easily. There are attempts to legislate Cyberspace but as long as there exist no common legislation covering all countries, as well as oil-rigs on international water, there are ways to circumvent local legislation.

The Internet-economy is steadily gaining momentum. As companies are able to make business entirely on-line, we have to change our view on what a company is. If you operate your business from an oil-rig on international water, there exist few reasons why you should register your corporation in any local country, putting yourself at risk of paying taxes and respecting local laws.

Even though they might not be registered corporations in the legal sense (Some of them are. Gator and KaZaa are two examples of large companies in this industry who are formal corporations.) We must still refer to them as companies in the economical sense. They are conducting business in the same way as every ordinary corporation, except that they don't have to oblige to the legal and moral laws of a certain society.

I consider the established companies acting in the parasite economy even more interesting as they are hybrids. They are ignoring the legal and moral laws of our societies when operating on the Internet, but they operate as legal, registered corporations with share-holders, CEOs and employees in the real world. As their business is based on the Internet, they are not considered immoral business, they are Internet-business.

This is what I refer to as I talk about immoral business-models and the parasite economy. Companies (registered or not) who earn profit from conducting business on the Internet, using methods that would be considered illegal or at least heavily immoral if they were carried out in our local community.

Popular examples of today are spam, viruses, adware and spyware, as described above, and as they will be discussed further in this text.

The open society

I argue that the primary reason why parasites can live on is our move towards an open society. Connecting every computer to the Internet is a vision that is well underway. Every kind of fraud is evidence on how an open society is build. Credit-card transactions are not secure; it is easy to steal money in our society, which has described by, among others, Abagnale (2002). The open society is possible only as long as few use the openness to their advantage. As long as the number of actual exploits of the system is low, we are keeping the system, even though the number of potential exploits is almost infinite. The same theory applies to the Internet. An open system of computers, as every system that involves a large number of people, is full of flaws and possible exploits. As long as there are few who take advantage of this fact, the openness will be preserved. The immoral business-models are based upon the assumption that there exist an easy exploitable system, and that by exploiting the system you gain competitive advantage.

Trust

Another prerequisite for the parasite economy is the issue of trust. Most of the time when you surf the web, read e-mail or download files you are perfectly safe. We have a general pragmatism when it comes to the Internet. People click around on the web feeling safe, everyone who have asked a computer professional about whether to click on a certain box or not have most likely been given the advice to simply click on it, as most buttons are to be clicked

Gustafsson writes on trust (2003):

"Views and beliefs are held until they are challenged and it is by no means guaranteed that they ever will be challenged. This also applies to trust. Trust is the view the trustor holds of the trustee. That view holds and is in fact strengthened by every day it goes unchallenged. It is also strengthened by each challenge it overcomes."

When it comes to computers, most of us are pragmatic. We are used to being safe and therefore we have a general trust when it comes to installing software or selecting options in dialogue boxes. If a box pops-up and asks you to click OK, you do it. Further we are used to computers malfunctioning. If we are affected by a parasite, which makes the computer goes slow or in other ways causes problems. We often accept it as a normal computer problem, thinking that perhaps it will disappear if we reboot the machine.

Trust is the key to all forms of social-engineering, of which parasite infection is a type. Social-engineering is a group name for a number of methods to break into systems by relying on its prime weakness: the user. One example is when you phone a user claiming to be a system operator and asks for their password (Mitnick 2003).

Identified types of parasites

I use the term parasite to describe a small piece of software that infects your computer and performs various tasks without your knowledge. The parasite could be installed through a worm, through a spam-message, a web-site or it could be bundled with a piece of software which you choose to install. I refer to the person or business entity that is responsible for the creation and distribution of the parasite as its master.

I have divided the parasites that I have found into two different categories depending on that type of control it strives after. There is control over the computer and control over the user.

Control over the computer means that the parasite now is in total charge of your computer. Without your knowledge it may use your computer to perform various tasks, send spam, distribute viruses, run an ftp-server for child pornography or anything else the master of
the parasite wishes. In the best-case scenario, the user will not notice it. After the infection, the parasite has no need for the user.

Control of the user means that you have control over everything the user does, you snoop on the web-addresses one uses, logs the keystrokes and get to know your behavioural patterns. This information can thereafter be used to change your behaviour. Your favourite home-page could be redirected to the highest bidder; targeted ads could be popped when you visit a certain homepage. The parasite is not only dependent on the computer as a host environment; it needs a user to fulfil its destiny.

Computer controlling parasites

A home computer is a resource which is seldom utilized to its full capacity. Most of the time a user performs simple tasks such as browsing the net, reading e-mails or writing documents, most of the cpu-cycles are wasted. There are masters who believe that they can use your computer in a much more efficient way.

- *Spam Relays*, parasites which enable the host to act as a relay for spam
- *Reverse proxying*, parasites that configure the host as a proxy, providing anonymized homepages.

- *Distributed calculations*, parasites that use the host to perform various calculations, such as code breaking.
- *Arbitrary control*, parasites that provide a general back-door so that the master can execute arbitrary code.
- *Denial of service*, parasites targeted to disable a certain host or web server by creating great load

User controlling parasites

The other type of parasites is directly aimed at controlling the behaviour of the user. The parasite is dependent on a user to be able to fulfil its purpose.

- *Explorer Toolbar*, parasites that installs a third-party toolbar with features to "help" you visit the right pages, such as buttons and/or search-boxes.
- *Homepage & Bookmarks*, parasites that change your default homepage and add bookmarks.
- *Spyware*, parasites that send back privacy information to a central server.
- *Adware*, parasites that trigger ad-displays when you enter specific urls.
- *DNS takeover*, parasites that take control over the Domain Name Resolution, intercepting and redirecting traffic in various ways.
- *Dialers*, parasites that make your modem dial a 900-number.

Business models in the parasite economy

Given an only a brief description of the parasites themselves, there might be a need for an overview on how they could be used for a company in a business model. We have established that there are parasites, and that they are annoying for the users, but where is the money?

Some of the types of parasites described previously maps rather simple to a certain business-model without the need for a further explanation. Companies running dialer-parasites infects computers in order to get money through their 900-numbers, adware shows advertising and receives money from the advertisers, but there are some other, more fuzzy, models.

The business-models have only been briefly described here, we still have little knowledge about how the revenue-models looks, how large this economy really is and what kind of customers there are.

Navigators

All those parasites aiming to control the users, showing ads and directing them to various home-pages could be described as Navigators. The term was initially coined in the book "Blown to Bits" (Evans & Wurster, 2000) which explains how Internet is removing the glue that keeps the value-chain together. On the Internet there often are different companies who work with attracting the customer, running the store, delivering the product and processing the payment. Therefore, an actor could easily specialize in directing traffic to various websites and earning money through affiliate programs.

The principle of affiliate programs is simple. You sign up as a traffic attractor, or a navigator, and each time you refer a visitor to their site and they buy a product, you get a kick-back. This is the reason why you can receive spam advertising products and companies with a strict anti-spam policy, the spam is not sent out by the company itself, but by one of their affiliates.

I believe that the role of navigators is important as they provide the means for specialization and anonymization. If spam were to be sent by the actual company selling the advertised product, they would be unable to remain anonymous and would have to handle complaints. The role of navigators as glue in the parasite economy is therefore one of the areas which I am currently studying.

Computer control

Parasites aiming to control your computer can be used for a number of different things. Having full control over a large number of computers all over the Internet enable their master to disable any Internet-service they want. There are companies who claim to have control over 450 000 computers which they sell to the highest bidder (McWilliams, 2003). All computer systems are sensitive for overloading, if you direct such a large number of machines to a web-server, requesting pages at the same time it will be overloaded and unavailable for other users.

The computers could also be used for relaying spam, hosting anonymous websites, breaking codes, searching for extra terrestrial life, or anything else someone is willing to pay for. Selling access to other peoples computers is obviously an interesting business-model.

Theft of privacy data

Tracking web-surfers activity and generating statistics from their patterns is another business-model. You can also extract large amount of useful data from the infected computers. Credit card information and other personal information could easily be used in fraud. Copying Internet banking certificates combined with a DNS-takeover could give the master access to your bank account.

There have been a few examples of targeted attacks against corporations to record confidential corporate data (Borland 2003), but most attacks are still towards broadband connected computers in the home. There are many ways to retrieve privacy data from a computer, sometimes without breaking any law. A usability study has shown that 10 out of 12 KaZaa users were unable to say whether they are sharing any files or not (Good & Krekelberg 2003). Chances are that they have shared their whole hard-drive, complete with on-line banking certificates and confidential work-related reports. The researchers in the KaZaa study tried to search for files like CreditCard.xls and were able to retrieve a large number of private documents.

It is not theoretically impossible that one could base a business solely on searching peer-to-peer networks for shared confidential information and using it to your benefit. For example, downloading the quarterly report for a listed company before it is released. Another way to get hold of confidential data is to buy second-hand hard drives. Companies have repeatedly shown that they are unable to destroy their data in a proper way (Hamilton 2003; Garfinkel & Shelat 2003).

Effects of immoral business models

Even though the parasite economy is an Internet phenomenon, the actions taken in the virtual world of Cyberspace affects the world we are normally studying when discussing economics. The parasite economy affects our society in many ways, but there's only room for a brief discussion here.

The questionable accountability

The existence of these new parasites raises the question how this affects the accountability of the user. There have recently been a few legal cases where people have been freed from various crimes such as intrusion and owning child-pornography, as this could have been the result of a parasite infecting the computer (Cullen 2003). No computer expert could find any evidence of such a parasite existing in those systems, but the possibility was considered reasonable doubt enough. Convicting people for computer related crimes was hard even before the existence of parasites, but at least one could assume that the user could be held accountable for the actions taken with his/her computer. The potential existence of parasites makes the need for evidence even greater.

Who own my computer?

Most of us receive a fair amount of e-mail spam to our mailboxes. If we are active Internet-users we are targets of Spam-Instant Messages (SPIM), if we blog, there will be spam there. If we are using a Windows computer, there might be WinPopup-messages popping up on our screen when we least expecting it.

Somehow, others feel that they are allowed to push messages upon us no matter if we like it or not. In many cases, we might have signed an electronic agreement that allows it, accepting the End User License Agreement (EULA) when installing a certain piece of software. Nobody reads them, everybody agree to them. Our experiences tell us that if we simply click yes, we will get on with our lives. We have always accepted these messages, and agreeing to the terms have always led to the installation of the software, and never given us any problems. Therefore our experience tells us that pressing yes is the right thing to do.

Many companies from which you have purchased software or services from actually feel that they have the right to execute software on your computer. More and more programs tell you that there is an update of the software, and ask you if you want to download the new version, some even do it without asking. As the software filled with those kinds of back-doors becomes more available and acceptable, the back-doors in themselves are becoming more and more legitimate, an accepted business practice.

American Online, the largest ISP in the world, had a number of complaints that pop-up messages were appearing at the screens of the users. This is due to the fact that spammers use a seldom used feature in Windows to send those messages.

There are ways of handling this problem. One is to simply instruct the complaining users on how to disable the service. They used another way, which is much cheaper. They simply ordered their software-clients to execute a remote piece of software as the users logged in to Internet, which disabled the service (Slashdot 2003-10-24). They felt that they had the right to change whatever settings they liked on your computer. What if they feel that they should switch your desktop picture the next time?

The future of moral

How come these kind of immoral business-models are allowed on the Internet? Is there a discrepancy between the norms in Cyberspace and our local norms? Are the rule-based norms of Cyberspace here to stay? Will they spread to the real world? Or is the discrepancy only due to the fact that users are unaware of what is happening?

Even though one might argue that this parasite economy merely is a temporary state in the gold-digger era of the Internet you might suspect that it is a result of the globalization of society in general. Will the lack of morality be an established future key-success factor which is necessary to be competitive? The fact that some of your competitors purchase advertising from services such as Gator at a significantly lower cost than traditional advertising makes moral a competitive disadvantage.

Discussion

The parasite economy is on the rise, the latest quarterly threat report from Symantec (Symantec, 2003-09) shows that threats are increasing both in volume and in complexity. The time between a possible exploit is found in a piece of software and a working worm exploiting it is on the loose is steadily decreasing. The threats is also becoming more and more advanced, worms carries parasites which are able to call back to its master in several different ways to receive new instructions.

The purpose of this paper is to introduce my research on the phenomena of parasites and to give a brief introduction of how they work and how they are used by various entities which could be referred to as companies. The parasite economy is something we are all exposed to. Even though most people have not heard of them, a huge number of computers are infected. Reports stating that 450,000 home-computers are being sold to the highest bidder. Companies stating that they have client software installed on 40 million of computers (Claria Inc. 2004).

Even though the parasite economy is significant and growing, some people might object to the study of it as a prospering economy. Investigating the business-models behind spam, spyware, adware and computer viruses is often considered a taboo, arguing that it will only create positive attention to an area that should be banned.

To rephrase the words of sociologist Elias Norbert:
If I were free to choose my world, I would probably not have chosen a world where the parasite economy did exist. I would probably have chosen to say: avoid it. Let us all live in peace with each other. But it so happens that, as a scientist, I cannot present the world as I would wish it to be. I am not free to present it otherwise than as I find it.

And I have found that there is such a thing as the parasite economy. I have seen that this is a significant, growing economy that affects us all. And I have set out to increase our knowledge about it.

I see no way to eliminate the parasite economy in any foreseeable future. The computer virus recently celebrated its 20th birthday. The ongoing chase between the virus creators and the hunters is increasing in pace, but the threat is only becoming worse as more people connect themselves to an open network.

Spam is currently fought in much the same way as viruses. Spammers and anti-spammers are chasing each other which create specialists both in detecting spam as well as creating undetectable spam. There is currently no reason why spam won't celebrate its 20th birthday in the future.

Even though there never have been so many efforts on eliminating the parasite economy, it prospers. The reason why I argue that all those efforts will not solve the problem is that the prerequisites introduced above are not technical but social. As long as we want an open society, there will be people exploiting it. As long as we want to be able to send a message to an unknown person, people will exploit it to spam. As long as we want to be able to add software to our computers, people will exploit it. Installing a parasite is a type of social-engineering, and is possible as long as there is trust.

As our odds to eliminate the parasite economy are low, we have to gain a wider understanding on how it works. By studying how they conduct their business, we might learn how to regulate their behaviour so that they have to oblige to law and moral behaviour. We have to focus on understanding the cause, rather than try to block the symptoms.

References

Abagnale, Frank W. (2002), The Art of the Steal: How to Protect Yourself and Your Business from Fraud, America’s #1 Crime, Broadway Books

Borland, John (2003-11-19),'Spyware' steps out of the shadows, Available: http://news.com.com/2100-1032_3-5108965.html

Cullen, Drew (2003-10-17), Teen hacker is not guilty, Available: http://www.theregister.co.uk/content/55/33451.html

Evans, Philip & Wurster, Thomas, (2000). Blown to Bits: How the New Economics of Information Transforms Strategy, Harvard Business School Press

Claria Inc, (2004-01-10), Claria – Advertise - Overview, Available: http://www.claria.com/advertise/

Garfinkel, S. & Shelat, A., (2003), Remembrance of Data Passed: A Study of Disk Sanitization Practices, IEEE Security and Privacy, January/February issue 2003

Gustafsson, Claes (2001), Idiergi - eller funderingar på gränsen till kaos [Idiergy - or thoughts on the border to chaos], The Pink Machine Papers, #2-2/2001, INDEK, Kungliga Tekniska Högskolan, Stockholm

Gustafsson, Magnus (2003), Chasing ghosts, Absolute presuppositions in the discussion on trust, PBI-institute, Åbo

Good, Nathaniel S. & Krekelberg Aaron (2003). Kazaa Usability Study, Available: http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf

Hamilton, Tyler (2003-09-15). 'Error' sends bank files to eBay, Available: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1063577414565&call_pageid=968332188492&col=968793972154

Kotler P., Armstrong G., Saunders J. & Wong V. (1996), Principles of Marketing, Prentice Hall Europe

McWilliams, Brian (2003-10-09). Cloaking Device Made for Spammers, Available: http://www.wired.com/news/business/0,1367,60747,00.html

Mitnick Kevin D. & Simon William L. (2003). The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons Inc

Slashdot (2003-10-24). AOL Hacks Subscribers' Computers, Available: http://slashdot.org/article.pl?sid=03/10/24/1337201

Symantec (2003-09), Symantec Internet Security Threat Report September 2003, Available: http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0

Symantec (2003-10-01), Symantec Security Response, Available: http://securityresponse.symantec.com/