J Comput Virol (2010) 6:143–159
DOI 10.1007/s11416-008-0093-1

EICAR 2008 EXTENDED VERSION

Small treatise about e-manipulation for honest people

Frédéric Raynal · François Gaspard

Received: 20 January 2008 / Revised: 18 June 2008 / Accepted: 27 June 2008 / Published online: 17 July 2008

Abstract Information warfare is nowadays a well-known concept. However, articles are mainly split into two categories. The first one deals with how information must be managed in a system (e.g. a company or a state), in order to achieve information dominance, that is providing more and better information than the others so that they have to follow what is produced. The second one is more on how information can be used as a weapon. Dominance is one goal, but not the only one: deception, intoxication or misinformation are others. In this article, we chose the second approach. The goal when using information as a weapon is to influence a target so that it does what the attacker wants, or to cause effects. We chose also to focus on a specific battlefield: Internet. One particularly important aspect of the Internet is that it is both a container and contents. For instance, web sites are providing articles, but they are also some servers, referenced by search engines. As such, we combined this duality to increase the effects of the operations given as example. We illustrate the operation through examples, where both information is created, but also its container is improved. We show how Search Engine Optimization can be used for information warfare. Combining oriented action techniques and information based techniques make each of them much more efficient. This article shows how information warfare can be conducted on Internet. The goal is to illustrate how very few people can organize an information based attack, targeting either a company or a state for instance.

F. Raynal (✉)
Sogeti/ESEC, MISC, Paris, France
e-mail: fred@security-labs.org; fred@miscmag.com

F. Gaspard (✉)
New Zealand Telecom International, Wellington, New Zealand
e-mail: fg@tnzi.com; kad@miscmag.com;
polo@polo-chez-les-kiwis.com

1 Introduction

This article shows how attacks based on information can be conducted on Internet. We will also illustrate how these attacks can be enforced using computer based attacks (hacking). The goal is to illustrate how very few people can organize an information based attack, targeting either a company or a state for instance. As an illustration, we will target a consulting and IT services company.

Nowadays, everyone can become a cyberwarrior due to two main factors:

- Democratization of warfare weapons: it is really easy and cheap to create electronic weapons to attack a target, whereas it is really expensive to prevent or repair the damages.
- No entry fees: there is no more need to agree with leaderships of others to act, conducting its own operations is enough.

Such actions can be seen similar to that of multi-agent system in Artificial Intelligence. Each agent is not necessarily aware of the actions of the other ones, and may only have a partial view of its world, but the actions altogether show coherency. In an offensive tactic, it can be viewed as small actions (may be not even offensive) but when they are considered together, they intend to disrupt the whole system.

We choose in our example a distributed approach, combining attacks on different layers (e.g. organisation or corporate image) rather than a centralized attack. In a certain way, we also take some inspiration from the long tail of attackers [5]. This concept deals with the economical model of sales on Internet. It states that it is better not to focus on the top five products, but on all the others. For instance, a usual booksellers has limited room to store the books. Thus, it focuses on the best sellers. Conversely, an Internet bookseller does

not need to store books. This explains why such booksellers make more money with other books than best sellers.

This model is found in real life for modern terrorists, such as those working in Iraq. The purpose is to attract and gather them around the same objective (free Iraq from Americans), but each terrorist cell can act as it wants with no central control. On Internet, it is not that difficult to find people sharing the same hobbies, that being either Star Trek or killing infidels.

We could think to apply this in two ways. First, when the target is very well known it is very convenient to federate all opponents however, this is not always possible. For instance, if the target is a not clearly identified (e.g. not a company) but a sectoral activity like petrol, health care, bank, and so on. Instead of targeting the leader, we could focus on all its competitors, and try to 'aggregate' them in a joined operation (what they may not be aware of). However, this works fine on Internet because the long tail is infinite, which is not true in reality.

In the first section, we introduce the main ideas of the proposed strategy. As it rests mainly on communication on Internet, we explain what is Search Engine Optimization in the second section. Finally, we give details on our example targeting a real (but anonymized) IT consulting company. This operation is built with legal/white means. However, we will also show how illegal/black technical operations could increase efficiency.

2 Principles of information based attacks

Our goal is really simple here: destruction. Rather than focusing on a single weakness and trying to exploit it, we will use several small ones. The strategy can be compared to the one used by pyromaniacs: rather than igniting a forest at a single point, he will do it at several, so that it fully burns. This is the principle proposed by the long tail, that is combining several second order weaknesses.

Once information on the target has been collected, three additional steps are required (see Fig. 1):

1. Populating the attackers, that is recruiting people who will act according to the expected goal (sometimes without even being aware of this goal).
2. Preparing the battlefield: that is the choice of weapons, where and how they will be configured.
3. Exporting the battle: in most cases, an information based attack needs to be public, thus this step intends to make the battle known to the right people (e.g. when targeting a bank, the proper stocks market, or public opinion to target child work).

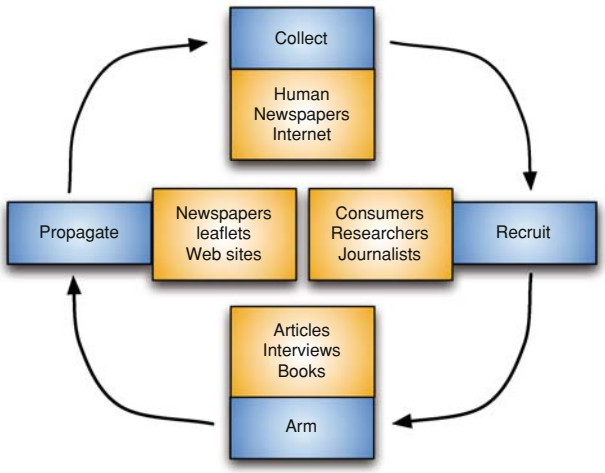


Fig. 1 Cycle of information based attacks

As stated in the introduction, this is what modern terrorists do: several cells with no connection lead an operation without considering what the others do. The damaged parts may appear insignificant, but when everything is put together, it disrupts the political power (mainly because the government seems unable to ensure its duty, e.g. providing electricity or water). Furthermore, any kind of attacker with the same destructive objective can use the same tactic, mainly because it has two strong advantages:

- The real attacker stays hidden, he will just provide information to the ones doing the real attack.
- The attack is not expensive and can be performed by everybody with time and brain power.

Conversely, the difficulty for the attacker will be to keep the control of the actions as the recruited groups may go to unexpected behaviors. This should be anticipated by the attacker who usually does not care anymore of what happens once he has reached his goals.

2.1 Collecting information on the Internet

A first way to find information is to use clever requests in search engines, like:

- Finding passwords
  - `inurl:passwd.txt` (1st result in google.com: `WebAdmin:aeYYajmW204V6`)
- Owned websites
  - `intitle:"hacked by"`: imaginative pictures…
  - `intitle:tt2.swi`: compromised websites installing a java trojan

– Entertainment
  - `intitle:"Live View/-AXIS"|inurl:view/view.shtml`: some surveillance cams
  - `site:free.fr intitle:"index of" mp3`: p2p outdated.

But conversely to what people usually believes, search engines such as Google, MSN or Yahoo only see 10% of the web. For instance, they do not dig into social networks websites (e.g. linkedin, orkut, twitter, facebook, …).

This simply learns us that we need to use the proper tool, depending on the kind of information we are looking for. For instance, when one is trying to find information about contracts with the US government, the website of the Federal Funding Accountability and Transparence (FFATA).

As a matter of fact, everybody is aware that the perimeter of a network has become from known to blurred. In the same time, the perimeter of information is out of control.

A more complete article [6] details what can be done, depending on what is searched.

2.2 Populating the attackers

The first step to conduct such an action is to recruit attackers. This can be achieved in two ways:

1. Infiltrate areas where they are already, that is to join already existing groups (e.g. consumers association).
2. Make them comet to us, e.g. creating your own contesting.

The first situation, when recruiting on Internet, we will need anonymizing techniques (e.g. tor, proxies but also using open WiFi access points, like those provided by McDonald fast foods for instance). However, other kinds of contesting groups are available, like customers associations, NGO, and so on. However, such groups require a physical interaction, which will then need more people and time. Anyway, this is still an interesting source of information if needed.

In order to attract and organize the opponents, several techniques are available (and can be combined of course):

– Create a honeypot web site: it is a reliable source of information for a long period of time, based on truth, impartiality and legitimacy to deal with the given topic. Once the public refers regularly to this site, the content evolve slowly toward opposition or rumor (e.g. blogs and rss feeds are really nice for that).
– create a site to bring together the opposition to the target, to its products, to its ethic, to its behaviors, and so on.
– Rest on the will of some NGOs to fight your target, for instance by providing piece of information they will be able to use (e.g. reports written by experts or intelligence gathered by putting pieces together).

No matter what solution is used: as soon as the battlefield is Internet, we will need to get the best audience, or at least one which is higher than the target. This is why Search Engine Optimization (see Sect. 3) will be so useful to give audience to our sites.

Another way to promote them is very simple: mails. Blind mailing (spam) is often put into trash directly. However, a targeted mail sending can be easily performed. First, one need to collect addresses from the target. That is easily done using Search Engines (once again). For instance, a query like `site:target.com intext:mailto` or `site:target.com intext:@target.com` may give many results. Also, looking for addresses in newsgroups is usually profitable. Once this collection is done, we just have to write a specific mail promoting cleverly our sites. It must not look like spam, so we can fake the headers, e.g. it seems to come from Human Resources working on a poll to improve working conditions. Mail aliases, like `*@target.com` or `department@target.com` could also be tested if the server is badly configured. However this may overload the mail server, and then be spotted.

A quite famous example was organised against Danone: some employees were really unease to be fired whereas the company was making amazing profits. They created a website (see Fig. 2) to organize the contesting. Since Danone was included in the name of the website, the company decided to assign them to court, but lost. Instead of shuting down the website, it gives it an increased audience.

2.3 The battlefield

For this article, we chose to focus on a small part of the battlefield, that is Internet. However, when dealing with information based operations, one must not forget:

– Consequences of our actions can be far from Internet (e.g. prosecutions).
– It is usually much more efficient to combine several battlefields (e.g. distributing leaflets at the entry of a sensitive location).

Moreover, it is very important to keep in mind that our targets are human beings, much more than computer systems or networks. These are just means to reach our objectives. Thus, we need to consider these different targets, whether they are intermediate or final. In order to help to distinguish what can be done, we rest on three kind of truth (Fig. 3):

– Subjective truth (ST): what is understood, interpreted.
– Objective truth (OT): what is perceived, or does not need to be known neither interpreted to be true.

Fig. 2 Opposition website: employees versus employers

– Informational truth (IT): what is told, repeated, . . . and thus believed to be true.

Usually, perception is modeled based on a subject using captors to perceive an object. The very same model can be applied on Internet: a human is looking for information (usually based on a Search Engine), and then visits the top sites corresponding to his query. Based on perception model, the human is the subject, the top sites are the objects and the Search Engines are the captors.

Let us consider some usual influence operations related to information, and see how they adapt to our battlefield:

– Intoxication: attempt to misguide the interpretations, the reasoning of the target, that is its analysis capacities.
  Ex.: spreading a wrong information, 'false/false' strategy (Tell the truth but in a way the target will believe it is false).
– Deception: can be either based on hiding (camouflage, blinding, …) or simulation (create, lure, invent).
  Ex.: WW2, when a false military base was created in order to abuse the German on the d-day location.
– Misinformation: based on alteration, removal, addition and so on of information.
  Ex.: "Clearstream" in France, where an alias name for Nicolas Sarkozy was added to some listings about off-shore accounts, or more seriously, the supposed lethal benzene in the bottles of Perrier.

Whatever the nature of the attack, the goal is always to trick the human brain in order to influence it, to bring it to take an action (or not to, which is the same). The target may or may not be aware of that, it is not important. The main difference between these three kinds of attacks is *according to the authors* the targets, and thus the means used to reach them. We consider intoxication targets the reasoning, deception the perception and misinformation the environment. Once the target is chosen, then the attacker knows what tools will be useful.

Once again, remember that information based attacks are not the only ones. For instance, prosecuting because of a supposed violation of a patent require from the defense (target) to provide elements that either he is owning the patent (and is legitimate to use it) or that he does not rely on it. In both cases, the target bring to light some of the solutions he is using (which can be a very valuable information for a competitor).

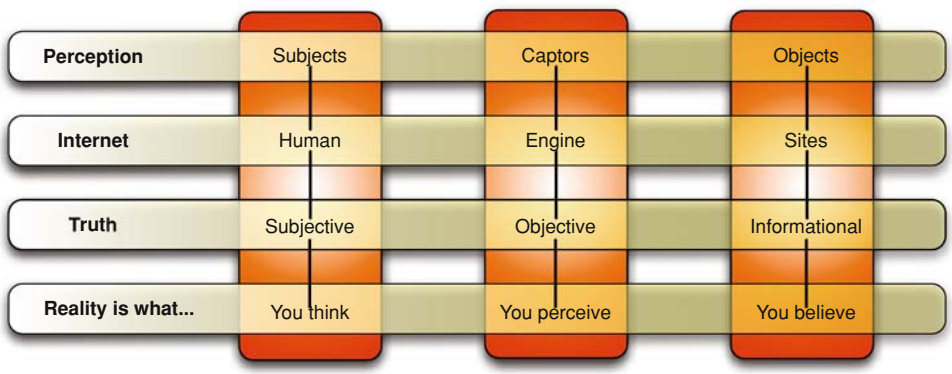


Fig. 3 Different meaning of truth

But let us come back to Internet and the human being behind the screen. How these three attacks can adapt on Internet:

- Intoxication: imagine a website controlled by an attacker which published articles. Once it is well established and regarded as a reference, it slightly changes the orientation of the new articles in order to influence the usual readers. Technically, it is easy to know if the target is reading it by looking at the server logs and all the information spread by the browsers.
- Deception will target the search engines as they are our looking glass on Internet, but these glasses can be tricked to warp the results.
- Misinformation is something known for years on Internet. Think about hoaxes, rumors spreading from a forum to another one, then by mail, and so on.

Note something specific to this Internet environment: Search Engines can be at the same time captors but also part of the environment. As such, they can be targeted using both deception but also misinformation. This can be achieved by changing the normal behavior of the Search Engine. For instance, a few years ago, it was possible to steal the page rank of sites mainly by putting an appropriate redirection from a fake site to the original one: Search Engines also have bugs …

This is the longest part of the attack since it requires to prepare many material: articles, reports, web sites and so on, but most of it before the attack really starts. This can (or even must) be started at the same time as recruiting attackers when possible. Furthermore, this is the step of the operation where we will need most of the gathered information, whether this is to feed the attackers, or to spot the right targets. Also, do not forget that the recruited attackers also have their useful information, if not their own weapons, and they should be included in the attacker's strategy as most as possible.

2.4 Exporting the battle

In the two previous steps, we have populated the attackers and prepared information which will be used for the attack. That is time now to perform the attack. However, information based attacks can be strengthen using a good technical knowledge of how Internet works.

Once the tactic has been decided, the goal is usually to take the battle to the public. In fact, most information based attacks rely on public opinion in order for the attacker to succeed. The information we have previously built will follow two directions:

1. Increase the doubts on the target in people's mind.
2. Increase the bad conscience of the target.

It is then time to use all the information we have built and provided to all the attackers so that the public learns about our target.

This will be achieved by promoting our own contesting but also by decreasing the echo made to the answers of the target. Our goal is to emphasize our information and make the target's answers almost unintelligible. Hence, during our preparation, we must also focus on some technical weaknesses, which have to be spotted before starting the operation.

Quoting Google:

> Q: What can I do if I am afraid my competitor is harming my ranking in Google?
> A: There is almost nothing a competitor can do to harm your ranking or have your site removed from our index.

We would not be so sure of that …Here are a few (nasty but not illegal) ideas of what can be done:

- Create duplicate content for the target website, and then denounce it to the main search engines: they will remove all duplicated content as they consider it as illegal.
- Using so common cross site scripting, redirect some pages of the target's site to on-line casino or porn sites.
- Create link farms for the target as they are prohibited by search engines, target's pages will be under-ranked in response pages.

Whereas the previous section dealt with creating appropriate information in order to attack, we combine it here with technical attacks in order to increase the efficiency of the operation.

During this period, many black operations can be conducted to increase the efficiency of the attack. For instance, there is a really easy way to forbid the target to answer through Internet: do a denial of service on its network. He could then answer on its web site, but nobody will be able to reach it. If the target's network has previously been compromised (either through a remote weakness in it, through a physical access to it, or help of an insider), everything can be done: slightly change the answer given to the attack, put illegal contents on a server and denounce them to the officials, organize information leaking, and so on.

However, these illegal actions are not a necessity for the attack to succeed. They may facilitate it, but the risk is also much higher. As always in strategy, this is a bet and the stakes are to compare with the gains and loss.

So, what if you can increase the perception of all our vectors and in the same time, decrease the perception of the target's answers? This is where Search Engine Optimization comes into play.

3 Introduction to search engine optimization

Search Engine Optimization (SEO) is a technique well-known from the web sites developers. The aim is usually to not only create a web site, but also make it the most visible. This is where SEO techniques come into play. The purpose is to get the best rank in the answers provided by a Search Engine, so that the site is the first returned in the pages when a user queries for specific keywords.

Definition 1 (Search engine optimization, SEO [1])
SEO is the process of improving the volume and quality of traffic to a web site from search engines via "natural" ("organic" or "algorithmic") search results for targeted keywords.

Most of the people do not look at the answers which are not in the first Search Engine Response Pages (SERP[1]). Most do not even click bellow the third answer, and since a site gets higher in the pages when it has visibility.

Understanding the value of being well ranked, some people and companies have developed techniques to increase the ranking.

Definition 2 (Web spam)
The practice of manipulating web pages in order to cause search engines to rank some web pages higher than they would without any manipulation.

What is the link with IBA? Users trust search engines as a means of finding information. Thus we will exploit this misplaced trust. As they usually do not look past the first ten results returned by the SE, we will also exploit this laziness.

SEO is commonly separated in two categories:

- White hat SEO: a site conforms to the search engines' guidelines and involves no deception.
- Black hat SEO: attempts to improve rankings in ways that are disapproved of by the search engines, or involve deception.

We will start by showing some common techniques in order to be well referenced. Then, we will discuss about some darker ways. Then, we will provide examples of black hat SEO (two examples and the analysis of weird site selling certified viagra). Last, we will go into *aggressive SEO* where the goal is to decrease page rank of a target.

3.1 White hat SEO

Here are a few things to keep in mind when designing a web site:

- Keywords: need to be really creative, to avoid generic keywords (those used by everybody else), poison keywords (e.g. viagra or casino), but think also to use misspelled keywords.
- Good architecture: the way incoming pages and outgoing links are spread in the web site is really important in the way the page rank is computed. Thus, pages must not be organised randomly but structured in order to maximize the flow of the page rank.
- Update the content regularly: the most a site changes, the most robots used by Search Engines will come to update.
- Provide innovative content.

We will stop here. SEO is a very wide topic and outside the scope of this article. Just keep in mind how webmasters use SEO to be well ranked in SERP. It is not always easy to follow all good SEO tricks and even if you follow them it could take months to have a website well ranked. Moreover guidelines are not written as a series of rules

A good strategy is based on long term and does not make any use of deception:

- Create content for users, not for search engines.
- Make that content easily accessible to the spiders.

In this way, the content indexed by SE is the same as the one seen by users

However, as being well ranked is also interesting in order to make money, people have started to use tricks not approved by SE: that is black hat SEO.

3.2 Black hat SEO

Let us start be summarizing a very brief example [4]: on-line pharmacy. All these companies prefer not to use spam directly, mainly because of anti-spam laws in US and Europe. Then, they create an affiliate program. The affiliates cause a regular income, and increasing sales. But another interesting advantage for these companies is the limited liability: affiliates are used as escape goats.

Business model of the affiliate is based on spam: the more they sell, the more they are paid. When looking at the affiliation program, one can notice that none of them forbids the use of spam:

- No terms of agreement at the sign-up page.
- Some companies operate in jurisdiction where spam is not illegal (ex. Seychelles).
- Spam is "restricted" to email spam.
- And so on.

Thus, when looking for viagra on the most common SE (Google.com, Yahoo.com and Live.com), results are

[1] SERPs are pages returned by Search Engines as the answer to the query.

Table 1 Search results and spam links for some common keywords related to on-line pharmacy

Keywords	Google	Yahoo	Live	Spam links
Buy viagra online	11,200,000	44,600,000	57,400,000	G: 4/10 Y: 6/10 L: 10/10
Cheap viagra	12,100,100	36,700,000	53,100,000	G: 7/10 Y: 7/10 L: 9/10
Buy cialis online	7,810,000	33,400,000	25,000,000	G: 8/10 Y: 9/10 L: 10/10
Buy phentermine online	4,340,000	27,000,000	52,600,000	G: 8/10 Y: 8/10 L: 10/10

amazing: spam is everywhere as it can be seen in Table 1 (source [4]).

Black hat SEO is generally defined as the use of techniques that Search Engines do not like in order to be well ranked in SERPs. Content indexed by SE is often different from the one seen by users.

It is important to notice that most techniques are nasty, but not illegal. However, the increase of the money is changing the rules. Nowadays, black hat SEO is also combined with *hacking*: exploiting flaw on web sites to be better ranked (see example in Sect. 3.3.3). This is not a new area, but it seems relatively neglected by the computer security industry.

The two main reasons of using black hat SEO are to increase the visibility of a website, but also to take advantages of PPC systems (Pay Per Click). As PPC is out of scope of this article we will not go further, let us focus ourselves on black hat SEO base tricks.

Before focusing on some advanced techniques, we briefly introduced some black hat SEO techniques:

- Content spam: altering the view of a SE over a page
  - Invisible text, keyword stuffing, doorway page, scraper sites,…
- Link spam: take advantage of link-based ranking algorithms
  - Link farms, hidden links, sybil attacks, spam blogs, page hijacking, …
- World-writable spam: add links to sites editable by users
  - Blog entries, forums, wikis, referrer spamming, …

Since it is not the purpose of this article to detail every such technique, we prefer to dig in a few of them in order to show how large the topic is. This kind of SEO is much more efficient when the user have developer skills, either in web language, signal processing or hacking.

3.3 Advanced examples of black hat SEO

3.3.1 Cloaking

Cloaking is probably the most well known technique (but not the most widely used). The goal is to modify the content of a web page depending on visitor parameters. The idea is to be well ranked on some keywords but when a user arrives on the web page it will display totally different information. In our case (information based attacks), we can use this trick to reference a page with legitimate information on our target but when a user arrives on the web page he will see a lot of contrasting information (for example information about financial fraud, connexion with occult networks).

There are different kinds of cloaking. They all have the same goal but do not work differently. Further more, some become too easily detectable by Search Engine (obviously SE try to detect Cloaking).

User-Agent cloaking

The oldest and simple cloaking is User-Agent cloaking. When an HTTP request is made, one of the most interesting field is User-Agent. For a web crawler ,and especially for Google, this field is set to something similar to Google Bot. It is easy to know if a HTTP request comes from a web crawler and not from a user. The following PHP script will redirect Google crawler to a specific web page:

```
$flag=strpos($_SERVER["HTTP_USER_AGENT"],"Googlebot");
if ($flag) {
 include("googlebot-special.html");
} else {
 // afficher page normale
}
```

(a) BMW for the spiders

(b) BMW for the humans

Fig. 4 Different view of `bmw.de` depending on who is looking

This technique is not very difficult to use, however it is almost unusable. Indeed, it is very easy to fake the value of the User-Agent field. A web crawler could come one day with a specific User-Agent and another day with another one. Our PHP script would become unusable as it will not be able to detect the web crawler anymore. We also have to keep in mind that when a Search Engine detects that you have cheated (with cloaking or others), it is most likely that you will be banned, and this is the last thing that we want!

Referer cloaking

A technique similar to the previous is to use the referer field which is used to know where a user comes from (in other words if he has arrived on our website by clicking a link from another website, if he has performed a Google request, etc.). It is then possible to filter on keywords used by users:

```
if (isset($_SERVER["HTTP_REFERER"])) {
  $referant = strtolower($_SERVER["HTTP_REFERER"]);
if ((strpos($referant, "http://www.google.")!==false)
  && (strpos($referant, "q=israel")!==false)) {
  header("Location: http://www.pro-hezbollah.com");
  exit();
}
}
```

IP cloaking

The last way in which we will see how to perform cloaking is based upon IP address. One more time, this address will be retrieved from the HTTP header (`REMOTE_ADDR`).

```
$ip = strval($_SERVER["REMOTE_ADDR"])
```

This method is the most efficient as it is more difficult to fake an IP address. However, it is the most difficult one to implement, as we need to maintain a IP address list of all web crawlers.

An (in)famous example: BMW.de

In January 2006, the site `bmw.de` was removed from the index of Google because it does not follow the guidelines. When a search engine came to the site, it could see Fig. 4a: the content has been optimized to be well ranked. However, a human visiting the same page was redirected to Fig. 4b. The example of cloaking discovered by Google make a lot of noise (moreover, at the same time, Ricoh also in Germany was removed from the index). This looks like a big and noisy warning to all european companies.

3.3.2 Solving captcha

An important point with black hat SEO is that it is based on quantity rather than quality. Farm links are a common example of that: privilege is given to create lots of links to the site one wants to be highly ranked.

In order to have many links, a common trick is to inject them in *open sites*, which are sites allowing everybody to post. Usual examples are now forums, blogs or even wiki. However, posting a message on such site is more and more protected by a question a human is supposed to be the only one to answer. This is to avoid automatic answering and web spamming. If this worked for a time, this time has gone now.

Most of the time, the question is an image containing letters and numbers ab user needs to validate before being authorized to post. Such a picture is called a *captcha*. Unfortunately, most of them have been broken. *Broken* here means an algorithm is able to solve them with a good success rate.[2]

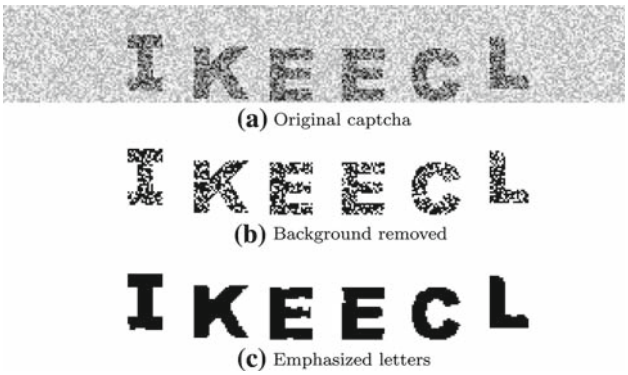
There are several ways to solve these captchas:

- By hiring students, or people with low incomes, and pay them a few an hour (see Fig. 5).
- By using a man in the middle attack: a fake program/message is given to a user proposing some services (e.g. access to porn videos), but this user needs to solve a captcha. However, this captcha has been taken from another

[2] Success rate is both not time consuming and good results.

Fig. 5 Job offering to solve captchas

Status:	Closed
Budget:	$30-100
Created:	08/30/2006 at 13:34 EDT
Bidding Ends:	10/02/2006 at 13:34 EDT
Project Creator:	afmatt View PM Post PM Buyer Rating: ********** (25 reviews)
Description:	I will provide a piece of software that will display CAPTCHA's - you will provide the service of solving them for one 50 hour week. Post your price and internet connection type. Report Violation
Job Type:	• Data Entry • Data Processing
Database:	(None)
Operating system:	(None)
Bid count:	58
Average bid:	$ 57



(a) Original captcha

(b) Background removed

(c) Emphasized letters

Fig. 6 Three signal processing steps in order to solve a phpbb2 captcha

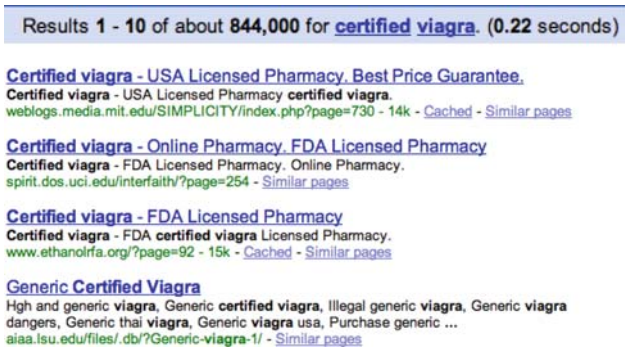


Fig. 7 Looking for certified viagra

site (e.g. gmail, yahoo, …). When the human answers, he is also answering to the other website.
– By using programs able to solve this question, which are usually based on optical character recognition (OCR).[3]

A generic algorithm has been proposed [2] and validated against phpbb2. The same kind of algorithm is also working for many other captchas :

– Remove the background: denoising
– Join points in the letters: filtering
– Derotate the letters: geometric transformation
– Read the letters: pattern recognition

The algorithms used here are not for that simple (e.g. signal processing and neural networks), and hard to calibrate. However, the author of [2] has got some really interesting results (see Fig. 6).

Other articles are also available on the Internet in order to solve many other kinds of captchas, including Google's or Yahoo's. An extension for firefox (captcha killer [7]) has also been developed: when a captcha comes in a page, the user send it to a server which solves it based on an OCR algorithms

Hence, web spamming is not that difficult for someone who wants to had many links to a target site.

3.3.3 Case-study: certified viagra

Here is an example mixing both black hat SEO and hacking. Obvisouly, cross site scripting can be interesting to lead people to a wrong site. But affiliates do even worst by exploiting flaws in software in order to get more traffic to their web site.

We will analyse here an example based on someone wanting to buy *certified viagra*. First, he goes to Google, and enter these two words as a query. As seen on Fig. 7, there are 844,000 answers. But when one looks at the four first answers, what a surprise: three universities (.edu) and an organisation (`.org`) are selling viagra!

We will now focus on the university of California Irvine (second answer, `uci.edu`). Assume the user trust the `.edu` (without questioning why a `.edu` would sell viagra). A quick analysis of the target site tells us its page rank is 6/10 (quite good), and it has 3,420 backlinks.[4]

[3] We are dealing here with optical captchas but audio ones are starting to appear.

[4] A backlink is a link pointing to the target site. They can be obtained with the keyword `link:` in Google.

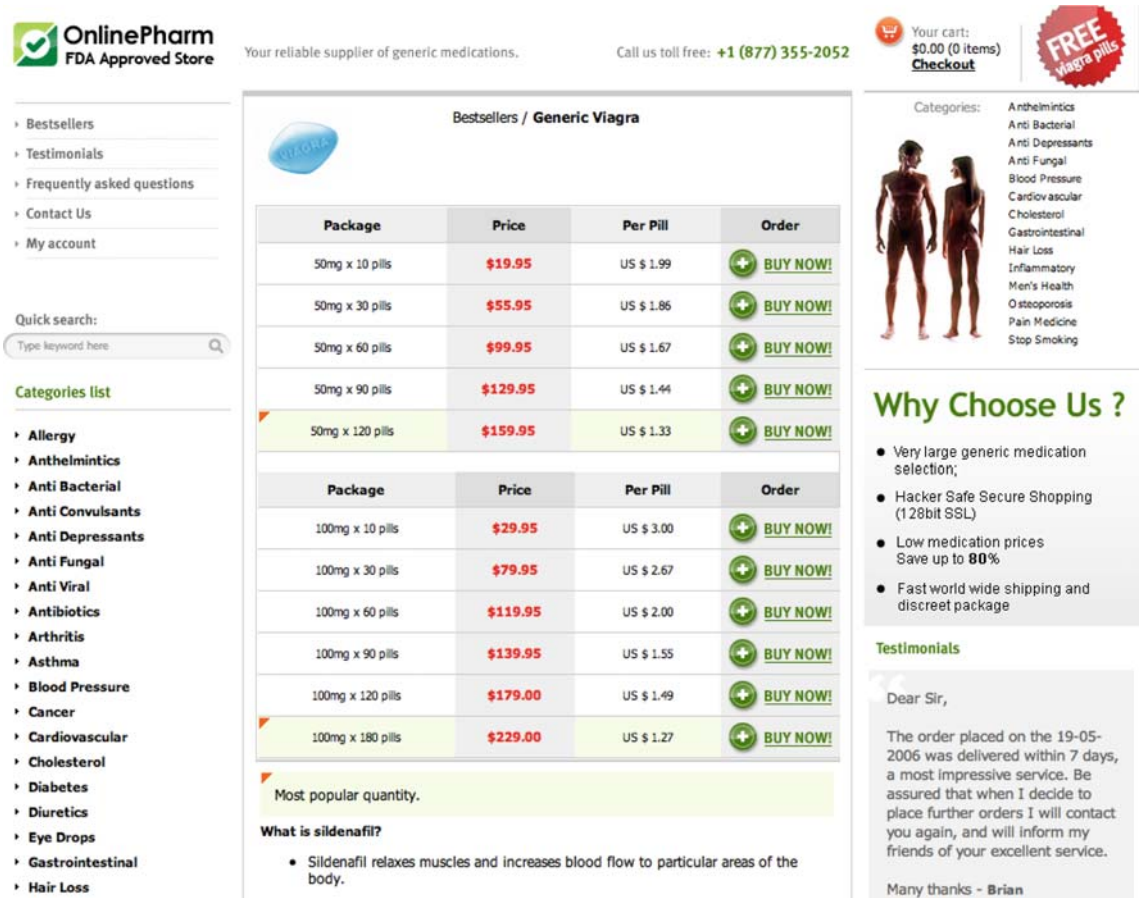


Fig. 8 Target site for the redirection

The target url is weird: http://www.spirit.dos.uci.edu/interfaith/?page=254. It looks like a page on a forum or a blog. As a matter of fact, when we look at the main page, we see the site is running Nucleus CMS v3.23 (current version at time of writing is 3.32). We find some security advisories about this software. One of them explains there is a flaw in default skin which allows to inject code in generated pages. And that is exactly what is happening:

```
<script src="http://focusa.net/gcoxiio.js"></script>
```

We download the script `gcoxiio.js` which is really simple: depending on the referrer, the user is redirected to various places. Here, we click on a link given by Google, so our referrer is:

```
www.google.fr/search?q=certified+viagra&ie=utf-8
```

The script `gcoxiio.js` will extract the keywords *certified viagra* and dynamically create a redirection:

```
if (document.referrer.toLowerCase().indexOf('viagra')!=-1)
  location.href='http://pillsonline.biz/viagra.htm';
```

Thus, we are in the end redirected to http://www.pillsonline.biz to buy viagra (see Fig. 8).

3.4 {Aggressivelnegative} SEO

Techniques we have seen intend to increase the visibility of a web site on the Internet. However, a tricky operator can chose to use them in order to decrease it: that is aggressive or negative SEO.

3.4.1 Always improve your own pagerank …

Another efficient trick to increase the number of backlinks is adding interesting comments on guest-book, blogs or forums. The comment will contain a link to our website. If the content does not make sense, the probability that the web administrator will delete our comment is high. Therefore, it is probably not the best idea to have a system that automatically posts comments.

3.4.2 …Or decrease competitors' one

In the category 'I want to annoy my competitor' one trick is to use keyword poisoning. The idea is to inject poisonous keyword on your competitor website. Search Engines supposedly do not like these words, and penalize websites that use

them. Of course, the competitor website has to allow posting from an external user: forum, blog, guest book or other.

Another technique is Google Bowling. This technique, which is one of the most widely known, is to create the largest amount of bad links to your target. All sexual websites, on-line games, racism website, etc. are good candidates. The more bad backlinks your target will have, the lower ranked it will be become.

Even better, we can use Google Washing. Here we do not talk about links, but rather duplicating the whole website of our target. Only the domain name will be (slightly) different. Search engines do not like duplicate contents and will tend to ban a web site. If Search Engines can ban your competitor website and not ours, we will be winner. Indeed, generally only one website is banned and often it is the newest one, therefore a good idea is to buy a very old domain and use it as Google Washing.

For patient people, it is possible to create a website totally legitimate, with quality content on a specific topic. Once the website is well ranked (and first in SERP) and has credibility, we change the content this is known as Google Insulation.

Spamouflage (Spam + camouflage) is again another trick to inflict damage to a target website. The idea is to post a message on a blog or others and include a lot of bad links (to sexual websites, on-line games, etc.). In this list, right in the middle, we include the website of our target. It is not obvious how search engines will react to this trick, but it happened they banned the whole list. It is worth the try.

Lets again mention other techniques like Black Hole SEO, 302 Page Hijack, Blogger Bowling, Black hat Blog and Ping. For curious readers, two websites are a must read to be kept up to date with latest black hat SEO tricks: bluehat SEO (http://www.bluehatseo.com) and seoblackhat (http://www.seoblackhat.com). Note for the last one, that the forum is not free but the blog is.

3.5 To go further...

Something really important to remember when playing with aggressive SEO, is that you can take as many risk as you like. As long as you keep your main and legitimate website separate, there are no rules. The more noise you can make the more your target will be disrupted.

Everything here is short term. You want to make the more damage to your target without affecting your main website. This is where Google Bowling, Google washing and other techniques can be used. Stay the more invisible you can. All these actions should not be seen coming from your side. Also, do not forget that generally you have a big advantage over big companies: you are a small entity. You can act and move quickly. For example, in a big company, they often need a lot of time and procedures in order to change a simple thing on their web page (Request For Change for system in production, etc.). You should exploit this weakness.

3.6 In real life

It is difficult to know where all these techniques are used and not a lot of examples are available. This it perfectly normal in a sense that no one claims he does Negative SEO! However, we have seen some companies caught for Google Bowling.

A final word about negative SEO. If it is true that it is already used between companies (economic warfare is everywhere), there is another area where it can be used. Remember the war between Israel and Lebanon two years ago. This war did not only happen on the classic battlefield ground (with air/sea/land attacks) but also on the Internet. In this case, the goal was to modify the perception of the media about the conflict. For example, the Hezbollah (Lebanese side) set up an amazing web galaxy of websites pro-Hezbollah. They installed websites all around the world (Syria, Iran, Lebanon, Kuwait, Qatar, Malaysia, Tanzania…), with different domain names, very well chosen and in different languages. All websites were also accessible from several host names. For example http://www.moqawama.org, which was the main Hezbollah website, was also accessible at http://www.hizbollah.org, http://www.nashrollah.org, http://www.hizbollah.tv, http://www.moqawama.info, http://www.ghaliboun.net, http://www.moqawama.net, etc., where "Al Moqawama" means "The resistance", Al Ghaliboun means "The winners" and so on.

The people behind this strategy perfectly knew how the web works. if only has one goal: influence the perception of the media. The more visiblity they can get the more the impact there is. Now think on how they can even do more damage. All they need is more visiblity. That is where combining what the Hezbollah did with negative SEO like Google Washing, Google Bowling, 302 redirect [3], etc., can be very efficient. They can easily target different entities: allies, enemies or neutral people. And at the end, the disinformation risk becomes much more difficult to control for all parties.

4 Case-study: attacking a consulting and IT services company

Briefly, the idea of information war is to produce information to influence the target by combining actions on different battlefields: human, technical, information, etc.

Now that we have established the foundation of our scheme, it is not time to act. It is obvious that everything showed in this article is totally fictitious, and none of the following situations are based on reality.

Firstly, we will introduce the players, the situation and the context. Afterwards, we will give the global view of attacker

strategy. The two last parts will be about white and black operations. As a reminder, these operations have to be performed in parallel with 'on the ground action' in order to consolidate them. In both cases, we will place emphasis on the technical side, which is too often neglected (computes are only a container). However, we will see how the technical side can consolidate actions with the help of SEO.

We will assume the attacker has already done the information gathering step, required for every planed attack, and focus on the tactic and planning of the attack itself.

4.1 The players

Lets start with the players. The operation is initiated by a computer service company from India, which wants to take over a similar company but based in Europe and more precisely in France. Why? Mainly to acquire its address book. We will call this company *Proctor* to make it easier. We will play the game as the Indian company. The final goal of the operation is to take over Proctor to access its network relation.

One more thing before starting: depending on objectives, context, players, etc. the strategy will evolve. If our attacker wants to obtain a know-how, it will have to ensure that the key people in the company remain present. Lets give an example, one way to decrease the value of a company is to recruit its most important employees. For example an engineer who would be the creator of almost all technical developments. Lets says that an investment firm wants to take over a company, having the engineer hired by a competitor or destroying the reputation of this engineer will not help the investment company at all, but instead: it will decrease its investment.

4.2 The strategy

At the beginning of our article we have showed the three steps of our strategy: populating the attackers, preparing the battlefield and exporting the battle. It is really important to understand that all these steps are very closely linked together and a clear separation between them does not always exist. In our case, these steps will be interconnected. Also, do not forget that our battlefield will be only the Internet. However, as said before, it is important that these operations are combined with other action not on the Internet.

The main idea here is to weaken the link between Proctor and its address book, in other words its customers. Nevertheless, we will not directly attack customers but rather, try to overload the commercial division of Proctor.

Our strategy has two effects: firstly Proctor value will decrease and secondly Proctor will consume its energy as they do not want their address book damaged. This is where we want to go: if Proctor consumes its energy to save its address book, it will not spend this energy for something else (to counter the take over for example).

A full picture of the strategy is given in the end in Fig. 9 as there are several layers.

4.2.1 Double jeopardy: suspicion toward the bride

This is the heart of our operation. The Indian company contacts Proctor asking it to collaborate on a different market to that of Proctor. Proctor is an international company but mainly based in France with business in Europe and USA. The first step for the Indian company is to attract Proctor by saying Asia is a highly desirably and financially attractive place for business. As Proctor is not in Asia yet, it has an opportunity not to miss: there is a financial income and a new market to embark upon. However, Proctor is not stupid and knows very well that this kind of deal could lead to adverse outcomes. For compensation, the Indian company requires a similar arrangement: collaborate on European markets.

At this stage, everything looks wonderful for Proctor. The attacker will reveal its hidden agenda only after a time that will be too late for Proctor to recover.

What are the advantages for the attacker? Firstly, the attacker can study Proctor from an inside perspective, thus, being able to identify key people and processes in the company. Furthermore, by attracting Proctor to the Indian market, it will consume its resources (commercial and juridic mainly). For example, during the negotiation there is great probability that Proctor will use its own lawyer, but also an external council. Always asking for minor changes during negotiation does take time.

Once the collaboration is legally sealed, Proctor has to work on the first big contract with the Indian company (and vice-versa). In order to initiate the new collaboration, the Indian company has to propose a first real contract between themselves. Once this first contract is complete, the Indian company can then move onto a contract that is only good in appearance. Again, the main idea is to consume Proctor's energy and resources, but with minimum profit (Proctor is mainly interested by accessing Indian market). These contracts could ideally include long and endless legal negotiation. Do not forget that all these contracts must be highly consuming to ensure a lot of Proctor's employees be involved.

4.2.2 Focus: drug the salesmen or deception for the groom

At the same time, we will target salesmen. Briefly, a salesman owns an address book, makes phone calls and tries to get appointments. When he can get an appointment, he negotiates with his customer to get information that could help him to anticipate future needs. He also has a system that knows when invitations to tender are coming out.

With Proctor, it is exactly like this except that salesmen are junior: pressure is high and they are not very aware of invitations to tender. Also, one more thing that we know about

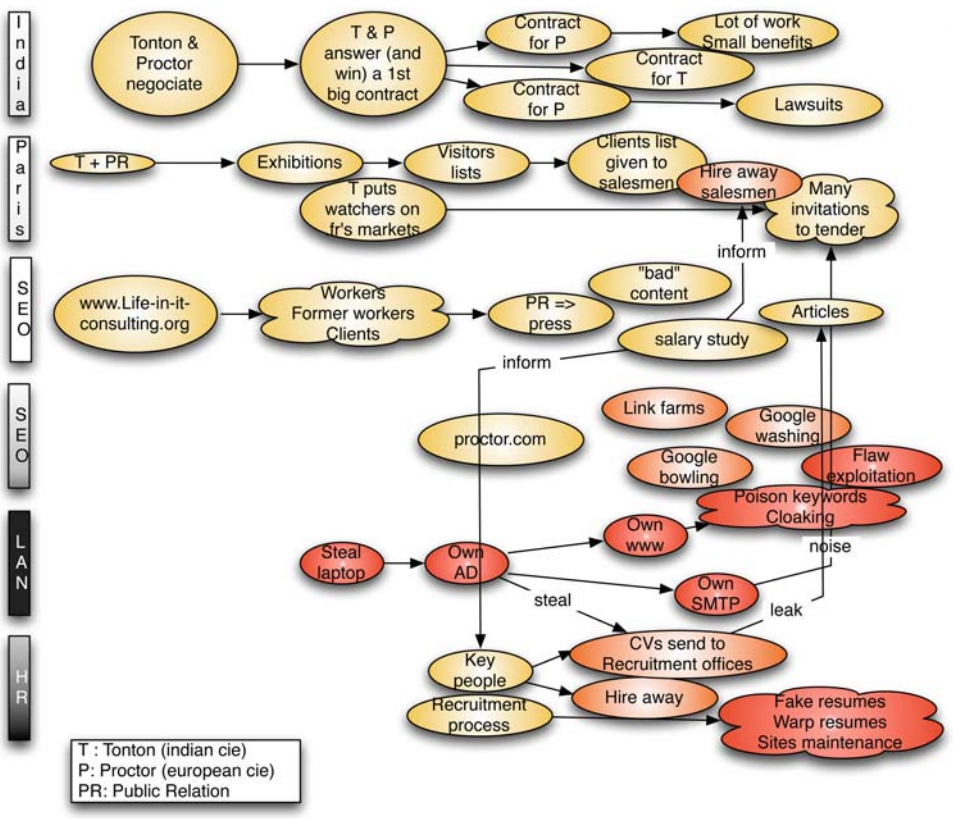


Fig. 9 Complete strategy

Proctor is that divisions are very isolated and do not share information between them.

What is our tactic? Make salesmen happy!! For this, very easy, we just need to provide them what they need:

- a contact list: the goal is to get a contact list and give it to salesman except that this list is not directly exploitable. In order to get this list we can use a public relation council. This council will be selected with significant care, as we require one that participates in commercial shows. As a matter of fact it has a visitor list (exactly what we need). Note that if the Indian company goes to this kind of commercial show, it can get this list itself and will also gain visibility.
  Now we have to give this list to salesmen. A possibility is simply to give this list to Proctor and say that it is high profile customers. Another idea is to target some salesmen and organize meetings. At these meetings, they are only allowed to bring USB key but not laptop. Then they have to plug this key on a laptop where, by *accident*, a file named customer.xls is present.
- Invitation to tender: as salesmen are under high pressure and lack experience they are not always aware of all invitations to tender. So we will do the job for them: we will identify the invitations to tender. When we find some, we transmit them to salesmen: a simple e-mail from Mr. Durant, who belongs to the purchasing service of the respective company, is enough. Also, as Mr. Durant wants Proctor to answer to this invitation of tender, he will transmit it to several Proctor employees.
- Last but not least is to propose more money to salesmen. We can use a recruitment company which will try to hire key salesmen with big salary, bonus, etc. The idea is to have several interviews. Of course the goal is not to hire these employees, but rather to make them confused about their current jobs and the possibility to get more money elsewhere.

To conclude on this part, the goal here is to overload the commercial division from inside and outside. From inside via a new partnership or outside by offering invitations to tender, which will give the illusion that the commercial division is working fine but in reality it is completely overloaded.

This part of the operation is not about creating information but rather to saturate a division by providing a deluge of information, information that it can not find by itself and even better that it can not process. This needs effective information gathering techniques which is not so easy. In some ways, salesmen are Proctor captors and we make them blind (they could miss traditional invitations to tender by focusing themselves on newer more attractive ones): these methods fall into deception domain.

4.3 Complementary white ops

In this part, we firstly focus on computer attacks. The good thing with computers is their ability to perform as either a container or content. Generally, actions target one of them, however in the following part we will use both.

Do not forget that all actions described below are performed together, in order to increase the success of the operation. Some actions on a battlefield can consolidate actions on another one (cf. actions from the global strategy).

4.3.1 Intoxication via website promoting

How can we reach such a result? Let us start by making a new contesting website which is not trivial but more importantly, will not be immediate.

During the information gathering part, we have collected a lot of information regarding Proctor, but also the whole sector. Instead of making an opposition website against Proctor, we will create a website which will be the reference in the sector by rating each actor. This website will also contain information (articles) about each actor. Luckily, this kind of website does not exist for this sector.

This kind of website exists in the financial world, for example the SRI (Socially Responsible Investing), which takes into consideration different factors, such as: ethical, financial, human, structural …to rate a company. We will use the same process for the Proctor sector. This will allow us to support a company or even better, to disadvantage a company. By this way, our website will appear neutral at the beginning as we quote all actors. During the start up process, we will have to be careful with Proctor and ensure they are not put at a disadvantage (we stay neutral). As said before, this strategy is really good as there is no such website for the whole sector (there are only forums where ex-employees explain their vision about the sector, we could use this information later).

Creating and installing such a website will take time. We have to give exposure to our website, but also make it credible. The more people who will use/read our website, the more it will become credible. We can also use SEO or black hat SEO to give it more exposure. Moreover, we send an email to all employees of this sector alerting them of the new website created (email addresses are easy to find [6]).

To get even more visibility we contact web newspapers like ZDNet or 01. We can send an email to journalists explaining the creation of a new website and after that asking them directly for interviews. This can be done through public relation professionals (they are not necessary aware of what they are doing).

In order to be well ranked on Internet, we have to publish real and useful content. The sector rating will be based upon different factors, but we can focus on a factor which is often neglected: human resource. We can use a forum used by ex-employee to get interesting information. We can find these ex-employee by consulting directories of high schools or look at social networks.

Another idea is to find (un)satisfied customers. Nothing complicated here, we can just consult websites of all the actors in the sector, as they generally proudly display their customers. Unsatisfied customers could be found by looking at archives.org. By comparing two versions of a website we could find customers that are no longer listed on the website.

The first 6 months, we keep as neutral as possible. Our only goal is to attract the largest amount of people on our website and obtain credibility. At the same time, we consult web logs to know where users come from and more interestedly what pages they are interested in.

To increase and obtain credibility of our website we can create a forum or blog. Whatever we chose, we will have to moderate it with great care in order to increase our fairness. For example, we post a message on the forum going against Proctor. Soon after (just the time needed for people to see and read it), the moderator (us) performs two actions:

- We moderate the message by deleting it.
- We post a message explaining that this kind of post is not welcome on the forum.

This will give us two things. Firstly, the calumny is spread. Secondly we have consolidated our fairness and thus the confidence of our website.

After several months, when our website has a good credibility and exposure, it is now time to publish articles against Proctor. However, we will go step by step and articles will not be completely against Proctor at the beginning. We do not even have to focus articles on Proctor at the beginning, we can focus on several companies at the same time.

We now have a great resource to influence our target, a website consulted by a lot of people. Influencing people is first point, but we also have a tool to identify actors which could help us in our action. Indeed, we can now identify people who are hostile to Proctor.

At the end, in conclusion to this part, let us resume our methodology:

- Populating the attackers: we recruit people via our website giving it more exposure, but also giving us information needed to prepare our attack.
- Preparing the battlefield: with the help of SEO, we give more exposure to our website.
- Exporting the battle: after giving the battlefield and information on our website, public relation council and other journalists will move and amplify our message.

Ideally, Proctor should be aware of our website once it is well known on the Internet, in order for Proctor to monitor it, or even better try to counter-attack (via its website or others), which will consume its resources and energy.

4.3.2 Proctor on the web: welcome to emptiness

Contesting site is far from enough. Since we are dealing with Internet, we will stay there and use the search engines. Based on how they work and on some of their flaws, we will use mainly black hat SEO in order to decrease the visibility of Proctor on Internet. Considering the time line of the operation, this has to be done once our contesting site is well established, just before it starts to intoxicate its readers. In that way, visitors wont be able to find Proctor's answers to our critics.

Our goal is mainly to decrease the page rank of the web site of Proctor. This company sells a service, service which is also provided by other companies (foreign or not). When someone will look for the information on this kind of service, Proctor is currently the first answer. There are two ways to change that, and we will use both of them. First, we can use SEO in order to increase competitor's page rank. This will not be described as the techniques used are the same as the ones used for the contesting site. Instead, we will give some examples on the second way: decreasing Proctor's page rank.

- Google Bowling: we want to create many backlinks pointing to Proctor. We automatized the research of forums, blogs, guest books and so on, but those dealing with racism, pornography, on-line casinos, and viagra for instance.
  More efficient, we can create these sites and we include keywords close from the ones Proctor is also using. We also add the same keywords but misspelled. Creating automatically porn content is really easy: very small texts, many pictures which can be found all around the Internet. It is easy to write a small program doing these around one topic.
  Then, we can also use blacklisted sites. Either we create them ourselves and have them blacklisted, or find some (we need to cross-research on several search engines and compare the results).
- Google Washing: we duplicate the web site of Proctor. Prior to that, we need to buy a domain name older than Proctor's, no matter whether it is related to the topic or not. Then we clone the web site and claim for duplicate content. Of course, this can be done several time to decrease Proctor's page rank.
- Create a link farm, with content dealing with Proctor (automatically generated), but what is important is that all pages of the link farm have many links pointing to Proctor.

All the actions bring activity around web site of Proctor, but also take down its corporate image. Since now, earthing we have done was not against the laws since they are withe techniques.

Last word, we are attacking Proctor's corporate image on two bases. Firstly, we increase how our contesting site is seen. Secondly, we decrease Proctor's site audience. Both are due to SEO, used in different ways. All by themselves, these two are not enough. But they come as complementary actions in the main strategy, in order to strengthen it. And damaging its image is a good way to lower the price paid to buy Proctor.

4.4 Complementary black ops

Up to now, we have taken great care about laws. However, what if these operations were combined with computer based attacks? The previous actions target the corporate image, but what will happen once it is combined with some actions supposed to downgrade the way the company works.

4.4.1 Hacking for profit

The take over of the network is really easy, especially form the inside. Here are some examples coming quickly in mind: using a botnet, compromising of the DNS server, changing the configuration of the router (backuping the routers is not that usual), spying on the emails, crashing some sensitive servers (like the domain controller, especially when the backup server itself has *unfortunately* a failure), installing a rogue DHCP server and so on. Many options are open but all require a trustworthy agent to arrange them, agent that our Indian company may not have. Anyway, with the increasing number of mercenaries in IT fields …

Assume now we have such a capable man. He will act in a very covert way. First, he learns as much as he can about Proctor's network. Then, takes the control of it. We will not give details on how he gets an access to the network (e.g. fake recruiting, con trick) since it is really easy with proctor (high turn over, no warden at the entry of the offices). We suppose our pirate can get access to a laptop (stolen, borrowed, given by the company, whatever). Analyzing it gives already two important information:

1. The password of the user the laptop belongs to.
2. The password of the local admin.

The pirate could learn much more by digging into this laptop (passwords used for some websites, VPN authentication, emails, important files and so on). A skilled guy will need something like 2 or 3 days (or even hours!) to learn almost all he needs about the network, from the servers (files, printers, back ups) to the privileged accounts. Most of the time, no exploit will be necessary. Instead, cleverness, imagination

and experience are enough to guess passwords and found badly configured (but critical) servers. Then, it is just a matter of (short) time before the passwords are obtained.

Once he gets the control on the domain controller, he can reach every single machine on the domain. First, he will look at the mail server. As the Indian company wants to know what is happening internally, this is a critical point. Every email by itself is interesting. But analysing who talks to who also reveals important people (that is the ones with influence, with the real powers), others we could recruit as insiders. Based on the mail server, many annoying actions are possible, like:

- The pirate can then arrange a fake information leak. Once he has spotted an important employee (e.g. he is the best engineer, or has clear sight of what is happening), the intruder can impersonate the guy on his computer and send away some sensitive information (e.g. confidential documents of a client, internal notes, and so on) so that it is noticed, especially from outside the company.
- The pirate can manage the mail system, and thus he can cancel or delay the sending and receiving of emails. As he can not read every mail, a random action can enough (and most of the time, they are the most difficult to notice). Since email communication works now in a deteriorated way, such are communication with both external and internal people.

Controlling such a server is really interesting for our attacker, even if this is usually not regarded as the master piece of the information system. Nevertheless, the attackers need to be very cautious with the information obtained in this way, since it is usually information they are not supposed to have.

Some other system are also interesting, like the DNS server or the proxy cache. We can analyze what sites are frequently used by the employees, which can help a lot when doing profiling. Moreover, we could also use that to randomly redirect some visit to our contesting web site.

Lastly, since we own the network, we will help Proctor with SEO. During the discovering of the network, we have found that Proctor hosts its own web site. Thus, we connect to this server and install some cloaking program. Depending on the origin of a query, different pages will be displayed. Using the appropriate module (LKM, backdoor, …), either on the DNS or web server, we can redirect the traffic wherever we want. For instance, we could keep the real web site for internal queries but a fake one for external ones. This can be quickly detected as many employees are working outside the company itself. However, since we control who can be redirected, we can select our targets cleverly. For instance, if some visitors come from a recruitment web site where Proctor puts some announce, we can display a poor web site with fake information, in order to discourage people to come and work at Proctor.

Of course, since search engines do not like cloaking, we denounce Proctor and provide a proof so that the cloaking we installed is detected. Then, Proctor's page rank will decrease very quickly.

This is much more simple than it may look. A simple kernel module (abusing skbuff under Linux, or at the NDIS level for Windows) leads the attackers where they want. A few hundreds of C is enough to reach this. Strangely, providing alternative web pages is probably much more difficult as it needs to be done cleverly.

4.4.2 Focus on the attack of human resources: when the human is the weak link

Consulting and IT services companies are not well-known for their *human* aspect. Even if their website promotes the way the handle the human resources. Conversely, when one looks for less corporate information, sites like munci.org or forums hardware. fr are very talkative about life inside the company. Most of the time, it is very different of the official presentation.

All these companies are very alike, and recruiting people works in an industrial way to compensate a high turn-over. When a company claims it will hire 4,000 people whereas the whole company has 15,000 workers (without buying another company), one can wonder what are the expectations of people leaving the company. Thus, we will target this critical process, playing on the two part of the recruitment process: making hiring harder, and encourage the resignations.

We start with hiring important workers (e.g. salesmen, engineers) noticed during the information gathering step. We can provide them opportunities they are not looking for, for instance by feeding them with job offers for a similar job, but much more paid. However, this is not enough: even if they see those offers, they may not dare to answer: we will have them contacted then. Since we have full control of the network, we can find in the Human Resource department the resume of all the employees. Unfortunately, it will leak, for instance to another alike company, a recruitment agency, or even on Internet. Such a leak is a double advantage for us. First, it increase the suspicion about how Proctor is managed from the inside. Second, if some employees leave, it means the price to buy the company will decrease.

Secondly, we corrupt the hiring process. Most of the people in charge of that process are young and they seek always on the same websites (e.g. monster). Let us do several tricks. It is easy with the help of the DNS server to redirect from time to time the request to another computer, one we control. It then displays `Server is down, sorry for the inconvenience. We are working hard to repair it.` Still to keep the recruiters occupied, we create fake profiles, so that they hunt ghosts. This can be done easily with the help of the script and the use of some

keywords we know recruiters will look for. More difficult, since we control the network, we can look for the resumes gathered by the recruiters (and nicely stored on a shared repository) and slightly change what looks like a phone number or an email address. More ghosts to hunt.

Additionally, we can also use some piece of information found during the information gathering step. For instance, we have discovered that one of the executive director has just put his resume on many social network and seems to be looking for a new position: that is not very motivating for the people working with him. Of course, as the to managers has also imposed a co-executive director to this one, in charge of half of his missions, he is not very happy and feel like he will be soon pushed away. This insecurity feeling can be shared with the others employees since it deserves our goals.

Furthermore, Human Resources have an Intranet which is reachable through Internet since many employees work far from the company. A poll has been submitted to the workers. It reveals that a majority of people consider themselves badly paid. This is the main charge again Proctor, so let us increase this feeling too. We dug up some information and found an article in a famous and well-considered newspaper *Le Figaro Economie* giving the average wages for the same kind of company, and the repartition between fixed part and variable part. Proctor is badly ranked for both of these factors. A similar document can also be found in a well-known agency in charge of the employments of engineers. We can now use our contesting website to share these pieces of information with the Proctor's employees. We create a document explaining what is the strategy about salaries at Proctor, and publish it on the website. First, it will not encourage people to come working at Proctor. Second, those already working there may want to work somewhere else.

Last words about these black operations. They are a matter of imagination, but also of technical skills. Many actions are possible, but they are greatly risky for the attacker. Most of the time, they are particularly interesting in order to get some information or to disrupt the system from the inside. However, it is very important not to be identified, and thus well concealed otherwise, the answer will be stronger.

5 Conclusion

Attacks based on information are happening every day, at different scales. We showed how they could use Internet (which is far from being the only vector) using it both as a container and the content. The advantage of Internet comes from the speed at which information propagates, and its durability, (it is almost impossible to erase an information from Internet). Furthermore, we have explain how some SEO techniques can also improve our effects. Combining both the content (use of information) and technical issues of the container (e.g. SEO, hacking) is much more efficient than each of these domains alone.

In the example we chose, most assumptions come from a real but anonymzed case studies. It shows how such operations can be complex as each element interacts with others. The difficulty is to evaluate the impact of an element on the others, so that they increase the effects, rather than canceling them.

Attacks based on information rest on information, whether it needs to be created, modified, hidden or revealed, whether it is true or false. Of course, the piece of information itself is very important. Nevertheless, the way it reaches its target also influences the target. Both the medium and the appearance have an essential role to play in the operation. This is what we emphasized through the use of SEO for instance.

Proctor is supposedly too busy to run its own business to detect what is happening until it is too late. A consulting and IT services company is like an empty shell (in the way it does not have its own products, its own specific knowledge). Thus, attacking based only on information is not easy. That is why we chose to target some internal mechanics, vital for it to work properly: trades, corporate image, human resources. With enough sand in it, Proctor will surely become an Indian company.

References

1. Search engine optimization. http://www.en.wikipedia.org/wiki/Search_engine_optimization
2. Captcha Breaking W/ PHPBB2 Example. http://www.bluehatseo.com/user-contributed-captcha-breaking-w-phpbb2-example/
3. Page Hijack: The 302 Exploit, Redirects and Google. http://www.clsc.net/research/google-302-page-hijack.htm
4. Liverani, R.S.: Web Spam Techniques. http://www.malerisch.net/docs/web_spam_techniques/web_spam_techniques.html
5. Anderson, C.: The Long Tail. October (2004). http://www.wired.com/wired/archive/12.10/tail.html
6. Raynal, F., Gaspard, F.: L'information, nouveau nerfs de la guerre. MISC 34. September (2007)
7. CAPTCHA Killer—Automated CAPTCHA Bypass. http://www.captchakiller.com/