# Deceptive Hacking:

*How misdirection can be used to steal information without being detected*

Bruce Barnett

<deception@grymoire.com>

## Contents

# Introduction

Let's say that a hacker desires to extract large amounts of intellectual property from a network. However, steganography and covert channels would take too long. Instead, the hacker desires to obtain the information as quickly as possible, without alerting the victims that the information was obtained.

This paper describes a technique to do this, by using the skills employed by professional magicians and applying these techniques to hacking.

Magicians have been deceiving people for hundreds[1] [2], or perhaps thousands[3] of years. Hackers have, perhaps unknowingly, have applied the basic principles of deception. This paper will show how the techniques of Magic and Hacking are similar. The basic arsenal of psychological techniques used by magicians will be explained. Parallels in hacking will be given.

In addition, these techniques can be combined to make hacking more deceptive. To demonstrate the application of this, A scenario will be explains where techniques of misdirection are used to succeed in extracting information without being detected.

Several papers have been published on perception[4], social engineering (scamming)[5], and how it can fool people. This paper goes further than that, by explains deception that can fool incident response and forensics teams.

# Similarities between Magicians and Hackers

There are interesting parallels between the best hackers, and the best magicians. Magicians have an economy based on ethical guidelines, and secrecy.  Creating new and practical techniques is valuable as it can be used to boost direct income (bookings) and

[1] Heironymous Bosch's painting, the Conjuror, dates from the 16th Century. http://en.wikipedia.org/wiki/The_Conjurer_%28painting%29

[2] In 1584, Reginald Scot published *The Discoverie of Witchcraft*. The book is often deemed the first English textbook about conjuring, as it explains how trickery can be done to explain the feats of "witches".

[3] WikiProject Timeline of Magic, http://en.wikipedia.org/wiki/Timeline_of_magic

[4] Stephen L. Macknik, Mac King, James Randi, Apollo Robbins, Teller, John Thompson & Susana Martinez-Conde, "Attention and awareness in stage magic: turning tricks into research"; Nature Reviews Neuroscience 9, 871-879 (November 2008)

[5] Stajano, Frank; Wilson, Paul; "Understanding scam victims: seven principles for systems security". Technical Report Number 754, University of Cambridge. http:// *www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf*

indirect income (marketing the information to others). Some magicians keep their best and most valuable material private. When secret techniques begin to become more public, magicians will often sell their better material to a select group of professionals. The older the material, and the more common, the less it is worth, and the more there are who use it.

The same is true for hackers. If you have unique skills, and can hack into sites using your private collection of zero-days, you have a higher status in the eyes of your peers. A top-notch exploit, that works 100% of the time, is worth more, perhaps up to $50,000. [6]

The more a secret is exposed, the less valuable it becomes. Companies like TippingPoint, and Google[7] are providing financial incentives to hackers. And once a secret is exposed, and becomes public knowledge, (available to script kiddies), the value for these secrets is much less. Magic secrets, like zero days, are priced according to their secrecy and value. The more exposed something is, the less valuable a secret becomes.

Also, the more secrets a magician knows, the more elite a magician is considered. Prestige is given to magicians who can fool other magicians, and to hackers who can penetrate systems others cannot. This is all based on secret knowledge.

There are more similarities, such as a preference for dressing in black. However, that's not the primary purpose of this paper.

## The Magician's Arsenal

Magicians have long used a specialized vocabulary to describe the workings of illusions. I should at first explain some of these terms, and describe the equivalent hacking term.

First I will define some physical devices, which magicians call their "props.[8]"

### *Physical techniques or Props*

Magicians used physical devices, or props for many reasons. Many items are ordinary, and therefore don't require special mention. However, some are not ordinary.

"Malware Attribution: Tracking Cyber Spies and Digital Criminals" BlackHat Briefings, 2010, Greg Hogland [6]

[7] Google offered an additional $20K for Pwn2Own, http://solvater.com/2011/02/google-offering-20000-chrome-sandbox-exploit-pwn2own-2011/

[8] Borrowing the term from Theater and Stage. The person responsible for all of the objects used on stage is the Prop Master. Prop is short for Properties.

The equivalent to a hacker is a program or machine. Most items in a personal every day experience are exactly what they appear to be, Some are not.

### The Gaff

A “**Gaff**” is a device that has a normal function and a secret function. It is either a normal item secretly modified, or else it is built to have a secret function.

For instance, if I were to take a pencil and glue a small magnet to it, it is now “gaffed.”

The equivalent hacker technique is to create something, like a web site, or a program, that has a hidden function. Any program with a hidden back door is gaffed. Typically this is done with using special words or commands, URL’s that response to special keywords, keystroke combinations, hidden mouse clicks, etc. When spamers direct users to web sites for pharmaceuticals, the URL of the default page may seem completely innocent, to convince the hosting services that the site is legitimate.   Some systems have been hacked so when special keystroke combinations, like the Sticky Keys sequence, are pressed, a special dialog box opens, allowing special priviledges.

Web sites with malware installed are gaffed. Any program with a back door is gaffed.

### The Fake

A “**Fake**[9]” is a device that appears to be one object, but in reality is another object. If I were to take a metal tube and paint it to look like a pencil, it would be a fake, and not a gaff.

In hacking terms, a Trojan horse is a fake.  A web site that appears to be another site (Man-in-The-Middle) is a fake. Social engineering and spam disguised as legitimate mail encourages people to visit a phishing site, which are usually a fake verision of the legitimate site.

### The Gimmick

A “**Gimmick**” is a secret device that provides a useful but unseen function. Gimmicks are not normally seen.  Rootkits are gimmicks. Any hidden file, or file disguised as something else, is a gimmick.

## *Human Accessories*

Magicians also use humans to create deception.

[9] Some older magic books use the term “feke.”

## Stooge

The stooge is a secret accomplice, a confederate, a shill, or in hacking terms, an inside threat, depending on how much trust you give them, and how well you know the stooge. A shill is someone unknown to the victim. At the other end of the trust spectrum is the Insider Threat. Usually the more trusted the Stooge is, the more effective is the illusion. In some cases, pretending to be the enemy of the illusionist can be very effective[10]. This “Enemy of my Enemy” ploy is a very effect way to gain the trust of someone, and the more one “hates” a hacker, the more trust they can get from someone else who “hates” a hacker or hacker group.

## Unwitting Accomplice

Magicians can use people as stooges, without their knowledge. They help the hacking without realizing this. They may lie to them, or tell them something, so they help the magician unknowingly. Sometimes magicians call this person an unwitting stooge or accomplice

Social Engineering creates unwitting accomplice. Books like Mitnick’s[11] and Hagnagy[12] cover this in detail.

### The Patsy, or Fall Guy

The Patsy, or Fall Guy, is someone who people assume is responsible, or who takes the blame.

## *Psychological techniques*

There are other techniques of magicians, which might be considered psychology rather than physical.

## Appearance of normalcy

The most important psychology to a magician is the appearance of normalcy - that everything is as it appears to be, despite any secret preparation or modification.

Harlan Tarbell emphasizes “Naturalness in Performing.”[13] Dai Vernon, also known as the “Professor,” stressed that lack of naturalness as one of the reason magicians fail to deceive.

[10] Tarbell, Harlan, “Tarbell Course in Magic, Volume 2”, page 35. Louis Tannen, Publisher. Also described in Nelms, Henning, :Magic and Showmanship,”1969, Dover Publishing. Page 3 tells the story, told of Frederich Tilden performing *The Charlatan.*

[11] “The Art of Deception: Controlling the Human Element of Security” Mitnick, K. and Simon, L.

[12] “Social Engineering: The Art of Human Hacking” Hagnagy, C and Wilson, P.

[13] Tarbell, Harlan, Tarbell Course in Magic, Louis Tannen Publisher, 1944, Volume 1, Chapter 2, Page49

A perfect illusion would be perfectly natural and logical. However, no illusion is perfect. Therefore magicians have to use other techniques to hide the flaws in an illusion.

Anything strange or unusual increases suspicion, and provides a clue to how an illusion works. They may not immediately understand the exact technique, but they often could figure out when it happened, and by understanding the result, they can often retrospectively comprehend the secret workings of a magic effect.

In hacking terms, the perfect hack is one that is completely undetected, even when examines in detail by a forensics team.

## Misdirection

Misdirection is the focusing of attention away from something. Some consider it to be merely the focusing of eyes away from something that can be seen. But this is just one example of attention. Focusing the thought process away from the true techniques used to create an illusion is just as important. Some of the techniques below can be used to misdirect. However, misdirection deserves its own section, and will be discussed later.

## The Sleight

A "**Sleight**" is a secret action or move.  Anything that appears to be one action, but has a secret action, is a sleight. A perfect sleight is completely undetectable.[14]

The hacker equivalent is the exploit, such as a buffer overflow. It seems to be a normal library call, but the secret action is to launch a new program. Any file that appears to be another file type is a sleight. A simple example is a program called picture.jpg.exe. A Windows machine will often hide the extension, so the executable appears to be a picture. Obviously, some sleights are more detectable than others.

## The Feint

The "**Feint**" is defined[15] as "a false show, a pretense, an imitation, a simulation. It's a movement that creates a false impression. For instance, one can "feign" to pick up an object and place it in the other hand, and in reality the object never moves. Ideally, there should be no difference between a feint and the real action.

[14] There is a legendary move called the Fizbin Drop, which is supposedly the Perfect Sleight. I personally have never seen it performed properly, and think it is just a myth or a joke.   See Electronic Grymoire #423, et al. Also see http://www.dennymagicsite.com/fizbin/index.html .

[15] Brown, E. "The Feints and Temps of Harry Riser", Kaufman and Greenberg, 1996. This term was first introduced by Jean-Paul Robert-Houdin,

In hacking, one example is purposely looking like the computer is busy, when nothing is happening. A more extreme example of a feint is to attack a machine for the purposes of misdirection, or to hide the true intention of an attacker. A brute force dictionary attack can be launched against a compromised server, creating the illusion that the attacker does not have access to the server.

It could also be used to hide another function. For instance, a hacker can use a brute force attack to covertly send information using steganography, covert channels, etc.

## The Bluff

A "**Bluff**" is speaking or acting falsely. One definition is "An attempt to deceive someone into believing that one can or will do something." This is like a feint, but with extreme attitude. In other words, attention is drawn to the action. It is usually verbal or written. Magicians often do effects, called "sucker tricks", that seems to have an obvious method. The magician will "bluff" the audience by acting as if one method is being used, and encourage the audience to believe they guessed the "real method." The magician pretends to not understand this. At the end, it is revealed that the obvious method is 100% wrong, with a surprise ending. That is, the effect was accomplished by another method.

Some hackers have taunted their victims. Hackers often bluff when bragging about their adventures to other hackers. It is also used to Bluffing is the primary deception tool for social engineers and poker players. A honeypot is a defensive bluff, as it pretends to be what it is not.

## The Subtlety

"**Subtlety**" – While this term is widely used, several "moves" have been labeled as a subtlety, instead of a sleight[16]. To be precise, a subtlety is a move that performs no secret action, as the action is in plain sight. However, it creates a false impression. A subtlety is often illogical when considered closely. However, it escapes detection when seen casually. An example of a subtlety would be a magician placing an object in one pocket, and removing the "same" (not really) object from another pocket, to perform a switch, e.g. a real pencil for a fake pencil.

Hacking examples include steganography and other covert channels of information, such as exchanging information based on timing, or error responses.

[16] Example, The Olram Subtlety, and the Ramsey Subtlety.

## Temps

**"Temps"** – The term is based on the French term a temps originated by Robert-Houdin.[17] It means an act or movement designed to divert the attention of the spectator. The more common term is misdirection.

However, the implication is that timing is critical for misdirection. Time as a factor by itself can be used, sometimes called Time Misdirection.  Some magicians will prepare a year ahead of time, hoping the spectator forgets details. An example in the hacking work is to do port scans over long periods of time, say weeks or months. Misdirection occurs solely because of the extended use of time.

[17] Robert-Houdin, J.P. "The Secrets of Conjuring and Magic"

## *Advanced Principles in Illusion*

As others have reported, people focus on things that interest them. Well known demonstrations include Daniel J. Simmons "Gorilla on the Basketball Court" video.[18]

People also ignore things that seem common, as demonstrated by Richard Wiseman with his "Amazing color changing card trick[19]," where four other color changes occur undetected.

These and many more principles can be used to improve misdirection and deception. I've already mentioned the importance of normalcy, which I call Vernon's **Principle of Naturalness.**

There are several corollaries to this principle.

**Corollary #1 – Minimize the unnatural**. The closer a substitution or action is to the actual object or motion, the more likely it will appear to be natural and therefore innocent.

Magicians spend most of their time perfecting their illusions to make them seem as natural as possible. They practice with video cameras, and mirrors, to see how it looks to the viewer. They strive to eliminate everything unnatural. They test the illusions with friends before attempting the illusion for real. Weeks or months of practice are typical. Spending mere minutes to perfect something is just amateurish.

Unnatural email is one of the biggest reasons phishing attempts fail. We laugh at spam with grammatical errors, because it looks so unnatural. The unnatural is suspicious.

And the more the unnatural is hidden, or minimized, the better.

Consider the task in making an exploit useful. First of all, it has to be successful. Causing the system to crash would hardly be deceptive. In actually increases suspicion. But let's say the exploit works 100% of the time. However, it creates two log entries classified as errors or alarms. If you can reduce the number of alarms to one, that's better. If you can eliminate any alarm, that's better still.

Or course, completely natural actions are best. Using valid authentication credentials, such as reusable passwords, is normal, and therefore is less suspicious than an exploit. Besides using authorized

[18] http://viscog.beckman.illinois.edu/flashmovie/15.php, http://www.theinvisiblegorilla.com/

[19] http://richardwiseman.wordpress.com/ and http://www.youtube.com/watch?v=voAntzB7EwE

credentials, credentials can be borrowed, such as the Pass-the-hash attack. Subtleties are better that sleights, if that is all that is needed.

Therefore when hacking, attacks should mimic natural activities as much as possible to escape detection.

Corollary #2 –Hide the unnatural.

If the unnatural action cannot be eliminated, then hide it. Create conditions that make the unnatural action hard to see. Mike Murray realized the letters “cl” look like a “d”, and used the domain “orade.com” to impersonate the “oracle.com” domain.[20] He can therefore make a site that looks 99.99% like the actual site, except for a very small difference.

Since magicians can usually control the performance, they can set up the illusion so the unnatural isn’t noticed. For example, the audience might not be allowed to be behind the magician.

For hacking, if most of the security alerts are logged in one file, modifying the attack so the event is logged in another, rarely examined file, or less information is captured, is an improvement in deception.

Payloads can be crafted so they seem more normal. Some exploits repeat the same character to create padding. This might create a log entry, and the padding may show up in the logfile. Patterns like “AAAAAAAAAAAAAAAAAAAAAAAAA” attract the eye. Changing the padding so it looks like a typical log entry makes the exploit harder to spot. One can modify Metasploit scripts, and other frameworks, to mimic natural patterns. For example, an exploit in a HTTP header overflow[21] can be triggered when a number of headers are exceeded. A typical exploit would repeat a single header 31 times, while a more natural approach would use headers similar to normal use. Shellcode payloads can even be described in English,[22] to escape detection.

**Corollary #3 –.Justify the unnatural**. If a magician can’t eliminate or hide anything unnatural, they find a way to justify it. Magicians can create situations that provide a reason for something odd.

[20] Pauldotcom.com podcast episode 232, with Mike Murray and Mike Murr http://www.pauldotcom.com/wiki/index.php/Episode232

[21] http://dev.metasploit.com/redmine/projects/framework/repository/entry/modules/exploits/windows/http/icecast_header.rb

[22] J. Mason, A. Small, F. Monrose, G. MacManus, “English Shellcode”, http://www.cs.jhu.edu/~sam/ccs243-mason.pdf

Social engineers often use this principle. They create a situation can "justifies" some unusual event, such as posing as a colleague from another company who is trying to help a friend who is visiting.

Corollary #4 –Make the unnatural natural.

Repetition and false alarms reduce the unnaturalness of an attack. If some other event can cause the unnatural to happen, then increase the probability that this event can happen.

Suppose you can make a failed exploit create the same log entry as a successful exploit. If you then make that failed exploit part of a script kiddie package, the target may see lots of these entries, and "know" that these are harmless, even when the real exploit left evidence.

**Corollary #5 – Control the perception of the unnatural.** If all else fails, then the magician can create events that prevent the audience from seeing the unnatural. This is where misdirection is used.

Of course one can use the "Look over there!" type of misdirection. But there are many other ways to do the same thing, which will be covered next.

## Advanced Misdirection Techniques

As a perfect illusion isn't always possible, other techniques, especially misdirection, can be used. There are different types of misdirection.

**Direct Misdirection**. This occurs when a performer tells the audience to look somewhere because something is about to happen. In other words, if the magician tells the audience to look at something, they usually do. This can be blatantly obvious (e.g. "Watch my hands!") or subtle. If someone suspects misdirection, or bored by the topic of the misdirection, etc. they may ignore the attempt to control their attention.

Hackers who like to taunt their victim can use Directed Misdirection, if it makes sense to the victim. Hackers can send an email or instant message saying "Have you checked if your server is still up? LOL" And of course the victim will then focus their attention on this. Some hackers have combined this with a fake (like a modified remote login program), and trick their victim into executing a Trojan horse, often combined with a Bluff as in this example.

**Event–based Misdirection** occurs when an event occurs that is unexpected. The reaction to an unusual event is attention, and immediate. To be successful the event has to be something that is of interest to the person being deceived, so if the event is interesting, the victim finds it hard to ignore.

Magicians have several ways to do this. One well-known technique is to have an attractive assistant in a low-cut dress bend over showing cleavage. Asking a spectator a loaded question can also be used. Sometimes eyes alone can accomplish the desired action.[23]

This distraction can be tailored to the individual, or type of individual[24]. The topic of the misdirection may be financial, sexual, physical, emotional, etc.

A related principle, known to scam artists, is **Know Your Mark**.  If you understand the victim's interests and motivations, you can control what they look at and how they react.

**Misdirection by Uniqueness** is a variation that occurs when an object has such unusual qualities; attention is immediately drawn to it. A magician may bring out some device that looks unlike anything else. A server behaving in a strange fashion (such as randomly making noises) will draw attention. In this case the event is interesting because it is abnormal.

In system penetrations fire alarms have been used to distract the victims and hide the hacker's activities. Other attacks may be based on social engineering, attacking the power and air conditioning[25], or a denial of service against another server[26]. Having the anti-virus system attack the operating system is another technique[27]

**Discovered Misdirection** occurs when there is something that will cause the victim to focus their attention when it is discovered. However, attention is not drawn to it beforehand. It sits there waiting.

[23] Magicians Harlan Tarbell and John Ramsey made famous comments about the importance of eyes in misdirection.

[24] ZigJoelFilm made a concentration test for men only. http://www.gjk2.com/test/test.swf

[25] Suggested by Larry Pesce in Episode 197 of Pauldotcom Security Weekly.

[26] Sony's PSN network suffered two attacked. One article reported  "Hirai went on to claim that the [second] breach occurred at the same time as the DoS attack, which was not immediately detected because of its 'sheer sophistication' and because a 'system software vulnerability' was exploited." http://www.scmagazineuk.com/sony-blames-anonymous-for-playstation-hack-but-confirms-it-has-not-identified-those-responsible/article/202140/

[27] http://abcnews.go.com/Technology/wireStory?id=10437730 "McAfee Anti-virus goes Beserk, Freezes PCs". ABC news, April 21, 2010

Magicians sometimes use these after an effect to confuse the spectator[28] after an effect.

One disadvantage on of this is that the timing is not always controlled. That is, the person may look at the wrong place at the wrong time.

I will describe a hacking equivalent later.

**Constrained Misdirection** occurs when a person is placed in a situation where they have limited perception, and this is used to prevent them from seeing a secret action. Spectators are brought up on stage, and it can be amusing when that spectator is fooled, yet everyone else sees how the trick is accomplished. Classic examples in magic includes *A Comedy Handkerchief Vanish*[29], Slydini's *Flight of the Paper Balls*[30], and Corinda's *Power of Darkness,* which is the inspiration for a routine with a large metal ring used by Penn and Teller. The hacking equivalent would be a "client" who complains about a problem that is only seen from their desktop. If the help-desk person remotely accesses that desktop, so they can verify what the "victim" sees, they are constrained to see when the client sees. The help desk person may be given access to a controlled environment, or through a different VPN tunnel. One can control experiences of the investigator, and hide other activities during this action. This is an application of the **Control the perception of the Unnatural** corollary**.**

**Misdirection by Time Delay.** Magicians often introduce delays between two events to make them seem unrelated. If two events are necessary to accomplish something, and if these two events occur days apart, and from two different IP addresses, the difficulty in correlating these events is harder. This is the **Hide the Unnatural** corollary, and a variant of the **Temps** concept.

**Misdirection by Differences in Scale** – Magician Tony Slydini taught his students that large motions hide small motions. The hacking analogy is a large obvious hack will hide a small hack, if performed simultaneously. Exploiting one server while another is being DDoSed is an example. This is a way to accomplish **Hide the Unnatural** corollary**.**

**Misdirection by Repetition** – This applies to the 4th Corollary **Make the unnatural natural.** Magicians will often repeat actions. Repetition causes relaxation, because the mind will filter out repetitious and

[28] Lee Earle, is his book "Making Manifestations", called them "Mind Bombs."

[29] H. Tarbell, "Repeat Handkerchief Vanish", Tarbell Course in Magic, Volume 1., 1941

[30] http://www.youtube.com/watch?v=FW6oQZc_c80

unimportant actions. This may be done because the unusual action can hide a secret sleight. By making the unusual action more "normal," the sleight is less detectable. A hacker can use this by making an exploit very similar to an unusual, yet harmless action, and repeat the unusual action until it becomes more "natural" by repetition. A variation with an exploit may not be as easily detected.

The investigator may examine the first few occurrences, and when it is determined that the actions are harmless, and there are large number of them, the investigator may not notice the single anomaly.

**Misdirection by False Alarms** – A magician may act as if he is performing a sleight, when he is not. The observant spectator may assume a sleight is in progress. For instance, a magician may move an object from one hand to the other, but pretend that the object is still hidden in the first hand (Bluff). Typically the magician will later reveal that the hand really is empty, as a joke. The False Alarm also draws the attention of observant and intelligent spectators, and can be used by anticipating the victim's reaction to suspicious moves. When it is discovered to be a false alarm, the victim often has to refocus their attention, and is more vulnerable to distraction at this time. However, there are times when it is not discovered to be false. This is described next.

There are not many examples of this in the hacking community. An example could be running an exploit against a server when it's already exploited.

**Misdirection by False Conclusion** - Another techniques magicians' use is to create the situation so that the spectator draws a false conclusion on the technique used. The silk to hollow egg[31] is one such effect, as is the "Backstage" illusion where the magician repeats the effect showing how it looks from the back. Of course as soon as the spectator understands how the effect works, the magician throws a spanner in the works, and by using another method the magician can fool the audience a second time.

There are many variations of this effect, even when the spectator knows the technique. Magicians love to duplicate the same effect that use a gimmick, and they either use a different gimmick, or else use sleight of hand to replace the function of the gimmick, for the sole purpose of fooling those who know about the gimmick.

[31] H. Tarbell, "An Eggs-Troidinary Eggs-planation", ibid.

Another technique some magicians use is to purposely create situations that suggest other methods are used. The spectator may think they understand the method, but when they try to re-create the exact conditions, they find out that their method doesn't work.

The False Conclusion was used by the FBI/DarkMarket sting operation.[32] The FBI did not perform any illegal action. However, they were able to create the illusion that they did, and therefore gain the criminal's trust. For example, when the FBI agent purchased some credit card accounts, he reported them to the financial organization, which then shut the accounts down, citing the reason as "fraud." The other criminals, who had a merchant account, saw this status on the number, and assumed the FBI agent did use the cards fraudulently, and was therefore trusted.

A very simple example is to place a string inside malware that suggests the malware came from another source, or by attacking a system from an IP address from a country different from the attacker.

There have been reports of a Shockwave file that has two attachments. The first is the EICAR test virus, and the second is actual malware.[33] This can fool both programs and humans.

This False Conclusion is extremely effective in deceptive attacks, as will be described later.

**Misdirection by Revealing Inferior Method** – Magicians may reveal, expose, or suggest one technique, especially if there is a superior method available. These techniques are also useful in hacking, as you will see later. This is related to the False Conclusion, as it explains how an action could occur, and indirectly makes the victim assume a false conclusion. It also acts as misdirection, because it will encourage the victim to investigate if the inferior method was used. This delays the discovery of the proper solution.

**Misdirection by Multiple Methods** – Another common technique is to have multiple methods to accomplish the same effect, especially if the effect is repeated. Someone familiar with one technique will see that it cannot be used in all cases. They therefore conclude that it was not used in any of the cases.

In hacking, an attacker may have three different ways to get into a system. The victim may find one, and fix this. If the attacker then gets

[32] http://en.wikipedia.org/wiki/DarkMarket
[33] http://isc.sans.edu/diary/Strange+Shockwave+File+with+Surprising+Attachments/10612

access to the system, the victim may conclude that this exploit was not the method used to gain access.

**Misdirection by use of a Switch** – Magicians will also distract the audience by switching a gaffed or fake object for the real object. If the object is examined, and is normal, it could not possibly be used for the illusion. Or so it seems. Malware that deletes itself is an example of a switch.

**Misdirection by use of destruction of evidence**– Magicians will hide the true workings of an illusion by destroying the gaff or fake, or by removing any evidence. However, there should be a logical reason for the destruction, or else this will seem suspicious. In hacking some hackers wipe out the system logs to hide the forensics evidence. If the evidence can be destroyed without being obvious, it is much more deceptive. A system log file that is empty is suspicious. A system log with a few gaps in the record is harder to detect.

Another technique is to use social engineering to obtain evidence, such as creating a forged e-mail detailing how evidence will be gathered. The victim may then give the evidence to the attacker unknowingly, thus “destroying” it.

## A detailed scenario

Now that you understand the basic principles, this paper will create a scenario that combines several techniques in a deceptive manner, as a magician will combine several techniques for a single illusion.

Let’s assume that the attacker wants to extract the contents of a large and valuable database of intellectual property from the XYZ Company. However, there are three problems: a) the theft must be undetected during the theft, as the attempt will be aborted. b) The theft should be undiscovered, as the data becomes more valuable. c) There are time constraints. A slow extraction using steganography would take too long.

Let’s also assume the attacker is inside the network.

Here’s how it can be done.

### *Mastering the sleights*

Our attacker has several zero-day exploits. Let’s call the least valuable exploit in the attacker’s collection the Fizbin Drop. Like a magician mastering sleights, the exploits are mastered until perfected. This means that they are constructed to appear as normal as possible.

In addition, one of the key attributes, or evidence, of the Fizbin Drop is found in a binary object, inserted into a Microsoft Word document. Let's call this file the Decoy File. It will be used later. It has an exploit, and a payload, which we will discuss later. It's harmless, and used just for deception.

## *Setting up the Props*

The props needed are placed inside the network. Gaffs and gimmicks and fakes are installed, waiting for use. The gimmicks are unseen, the gaffs appear normal, and the fakes are not closely examined. The external web site has been gaffed so that new files can be uploaded onto the server, and then after they are uploaded, they can be made to appear with a simple "sleight."

The audience is scanned, looking for a suitable stooge. Some preparations are done, and the hacker is now ready for the next phase.

## *The Impromptu Stooge*

Someone, whom we will call Unlucky Lucy, is one of the people responsible for the database.  Another system administrator is Ivy. But we'll talk about her later.

Files are placed in Lucy's directory, hidden, but just barely. They can't been seen by a casual observation, but a detailed scan will reveal these files (gimmicks).

Lucy also has a process where she can execute the distributing of certain files to other computers. This process is gaffed, so special files can be placed in the outgoing queue.

Meanwhile, profiles on web forums are created with Lucy's name. Some unusual opinions are posted in these public forums (**Discovered Misdirection**).

Some more work has to be done. The daily backup of the database is typically incremental (only new changes) instead of complete (copying all data). This has to be modified so that larger backups are not considered unusual (**Make the unnatural natural**).

## *Day 1: Enter Stage Left*

Now's the time for the real misdirection to begin. Details of the Fizbin Drop are released on Full Disclosure.[34] Hackers start writing exploits. Anti-Virus companies start developing signatures. It will take a few days before the signatures come out. (**Misdirection by Revealing Inferior Method**).

## *Day 2: Nothing up my sleeve!*

Next, after an appropriate delay, a press release is sent to the media. It announces that due to declining revenue, the XYZ Company will be providing services for the Adult industry. In other words, porn. This happens Late Friday, giving time for the media to contemplate the news. And of course XYZ does not provide a public key that can be used to verify the press release.

And this point, the hacker sends a special command to the gaffed web server, which then modified some pages so some new pages and files are now visible on the XYZ Company's external web site.

And the backups on the database increase in size.

## *Day 3: Presto!*

The CEO is woken by a phone call from someone in a panic, telling him about the faked press release.[35] "Is this real?" they ask. This is obviously a Public Relations nightmare. A team is gathered, and another press release is sent out denying the entire incident.

Meanwhile, those new files on the external web site are discovered. Some anonymous email, some tweets, and some blog posts discuss the interesting news that the web site now offers some adult services, along with some extremely revealing pictures.

## *Day 4: You've been a wonderful audience*

The CEO is again awoken to discover that his web site now has adult pictures, thereby proving the first Press Release was entirely accurate. In addition, another press release comes out announcing the new section on the web site where these services are available. It also provides the public key which can be used to verify the authenticity of the digitally signed press release. This key, by the way, is also found on other external web servers. Perhaps the hacker even gets the new

[34] http://seclists.org/fulldisclosure/

[35] The associated Press was fooled by a faked press release from "GE," in April 2011. http://www.businessinsider.com/ge-press-release-hoax-2011-4

press release on the company's web site where press releases are published.

Bloggers are saying this is a publicity stunt. Other bloggers are spreading rumors that the CEO is a sexual conservative, and that he is in disagreement with the others in the direction of the company. In other words, the second press release is wrong, and the first and third are correct.

The security team has shut down the site with porn, and then does an internal audit, trying to find out how these files appeared on the web site. They noticed several anomalies in the logs, and they appear to have come from someone inside the company. They investigate further.

Meanwhile, another anonymous email comes in, addressed to Innocent Ivy, describing how one of the employees of the company was making comments on a public forum about "nothing wrong with porn" and how it's profitable, and how "expect a big announcement." And the email states that the name associated with the external account is the same as Unlucky Lucy. Ivy reports this. (**Impromtu Stooge**).

Also – using some sleight-of-hand, those Decoy files are replicated throughout the company's network, apparently by way of Unlucky Lucy's account. Some of the files associated with the creation of the malware are also placed in Ivy's account,

The hacker also sends a nasty email to Lucy, apparently from Ivy. Lucy is shocked that Ivy did this. Ivy is of course Innocent of this.

## *Day 5: How did he do that?*

Well, an internal audit reveals that some of the porn files on the web site are also in Lucy's home directory. That's strong evidence that Lucy was responsible for the web site hack, and hR thanks Ivy for helping identify the culprit. A Google search shows Lucy's apparent interest in porn.

Of course Lucy denies it, but the evidence is strong. Lucy says she did get a strange email from Ivy, threatening her. Perhaps Ivy did it? The HR person obviously thinks Lucy is lying to save her job, and looks at Lucy with pity. This is, or course, **Discovered Misdirection** and **Misdirection by False Conclusion.**[36]

Meanwhile the new anti-virus signatures are installed. Alarms are going off everywhere, indicating massive virus infection. The Decoy file is found on everyone's computer. They also trigger some malware that opens up a connection to an outside web site, and sends large amounts of information. The data is all random, but look like someone trying to export massive amount of intellectual property.. This is a **Bluff**.

And now it is discovered that the porn files are also found in Innocent Ivy's account. And that Ivy dislikes Lucy, according to the eMail. Apparently Innocent Ivy isn't (**Misdirection by False Conclusion).**

## *The Moment of Truth?*

In summary, we have the following events going on.

- The CEO is trying to deal with the aftermath of the fake press release. Many think this is just a publicity stunt, because of the clear evidence that Adult services were available on their external web site. People are still trying to determine which of the press releases are right and which ones were faked.
- Lucy is ejected from the company immediately, at the CEO's insistence. She denies everything, and the best thing she can do is say she thinks Ivy was responsible. But Ivy helped identify Lucy.
- A massive virus is propagating through the network. During the clean-up, they discover that the source code of the virus is found in Ivy's directory. Ivy is dismissed with cause, despite denying everything.

- Of course firing Ivy causes problems because they just fired Lucy because of what Ivy said. But if Ivy is the guilty party, perhaps Lucy is innocent. But she has already been fired. Now they have to worry about wrongful termination lawsuits. More importantly, they begin to distrust their decisions, and perhaps the evidence of the porn and malware infection is flawed. The simple answer is that Ivy and Lucy are responsible. CEO's like simple answers, even if they are contradictory.

- The internal staff is in turmoil. The sudden departure of Lucy and Ivy left the support staff in chaos. They disabled the accounts of

[36] There is a discussion of the trustworthiness of forensic evidence in Bruce Schneier's blog, based on Sergey Bratus's paper "Software on the Witness Stand: What Should it Take for Us to Trust it?" See http://www.schneier.com/blog/archives/2011/04/software_as_evi.html

these sys-admins, and quickly found someone to assume their responsibility.  The database servers Lucy and Ivy were responsible for seem to be operating normally, which is good, because everyone is busy trying to stop the virus while trying to find out what is happening. Friends of Ivy and Lucy don't quite know what to believe, and they think these great co-workers were fired for no reason.  Perhaps they may be terminated next, because no one is telling them what Lucy and Ivy are guilty of. And they are certainly not going to argue with the decision makers, because the decisions are coming from "up high."

- Essentially there are so many crises occurring that small, slightly abnormal events aren't noticed.

## *The Grand Finale*

Meanwhile, the hacker has done two small things. He has poisoned the DNS cache so that the remote backup server now has a new IP address. The second is that the hacker makes sure a full backup of the complete database occurs. This will allow the entire contents of the database to be exported. These are very small changes in the day-to-day operation. Perhaps Lucy and/or Ivy might have detected this. Others might, if they weren't so busy during the chaos.

When this is done, the hacker performs a switch, and the two changes he made to the system vanish, and the system is returned to normal. No trace of the modifications can be found, and the log files show nothing unusual. Examining the log files show nothing outside of the normal actions. If the company does egress detection, the noise generated by the malware hide the activity of the database extraction.

Days later, when the crisis is averted, and the systems patched, no one realizes the theft of information happened.

The hacker still has ways into the system, because he always keeps another Ace up his sleeve.

## Conclusion

This scenario demonstrates that the skills of magicians can be used in a deceptive way to minimize the risk of detection. In addition, it also shows

- Those with administration rights need stronger protection from attacks, and a stronger audit trail. They are valuable assets, and extremely vulnerable.
- Don't have single points of failure in the defensive teams. Use teams, and make sure there are at least two familiar with every active defense response.
- If reacting to active attacks, use focused teams. Don't apply all of your resources, and don't leave other resources undefended.
- Administrators need a more tolerant view if accused of wrong-doing. The people in Human Resources are not qualified to determine guilt or innocence. Make sure they are guilty before disciplinary action.
- Press releases should be digitally signed.

.