Fachhochschule Luzern HSLU

Studiengang Digital Ideation, Bachelor
3. Semester

# Image Poisoning

Nam Pham, Valentin Berger, Simon Hischier

January 10, 2018

# Inhalt

# 1 Abstract

Als Pedro versucht mittels der Google Bildersuche Bilder für einen Motor seines Miniatur Hubschrauber zu finden, findet er schnell viele Resultate. Naiv wie er ist, klickt er auf das erste unscheinbare Bild und wird sofort auf eine eigenartige Webseite geleitet. Diese blinkt und schreit herum dass das Antivirus Programm Viren gefunden hat und ein Update nun benötigt wird. Natürlich ist alles nur gestellt. Diese Art des Scams nennt sich Image Poisoning. Diese Arbeit gibt einen technischen Einblick in die Methodik des Image Poisoning. Es wird erklärt weshalb die Motivation für einen solchen Angriff existiert. Auch befasst sich diese Arbeit mit dem Schutz der Benutzer vor solchen Angriffen. Sowohl aus Sicht des Benutzers sowie aus Sicht der Webseitenbetreiber.

# 2 Begriffserklärung

## 2.1 Image Poisoning

Wenn ein User eine Google Image Suche startet, tauchen zu regulären Suchresultaten zusätzlich die Bilder eines Angreifers auf. Sobald der Benutzer auf das Bild des Angreifers klickt, beginnt sogleich der Angriff. Bei der Google Suche werden standardmäßig gecachte Bilder angezeigt. In der Vorschau wird ein Iframe geöffnet, welches die Bilder direkt vom Server des Anbieters lädt. Diese Iframe Anfrage wird auf dem Server erkannt und falls die Anfrage durch die Bildvorschau auf Google ausgelöst wird, wird zusätzlich noch ein Javascript mitgeschickt. Dieses Javascript ändert daraufhin die URL der Google Suche auf eine Virus-Website.[8]

## 2.2 Cloaking

Unter Cloaking ("to cloak" z.D. "verhüllen") versteht man eine Technik um eine Suchmaschine zu täuschen. Die Idee von Cloaking ist, dass dem Bot einer Suchmaschine etwas Anderes gezeigt wird als einem menschlichen Benutzer. Konkret werden Bots üblicherweise über den User-Agent oder über eine festgelegte IP-Range gefiltert. Diese Technik wird oft zur Verbreitung von Malware genutzt. Eine verhüllte Webseite zeigt Inhalte zu einem aktuellen Thema und positioniert sich so in den oberen Rängen der Google Suche. Klickt ein Benutzer auf den Link erhält er statt des erwarteten Inhaltes eine von Malware verseuchte Webseite des Angreifers.[6]

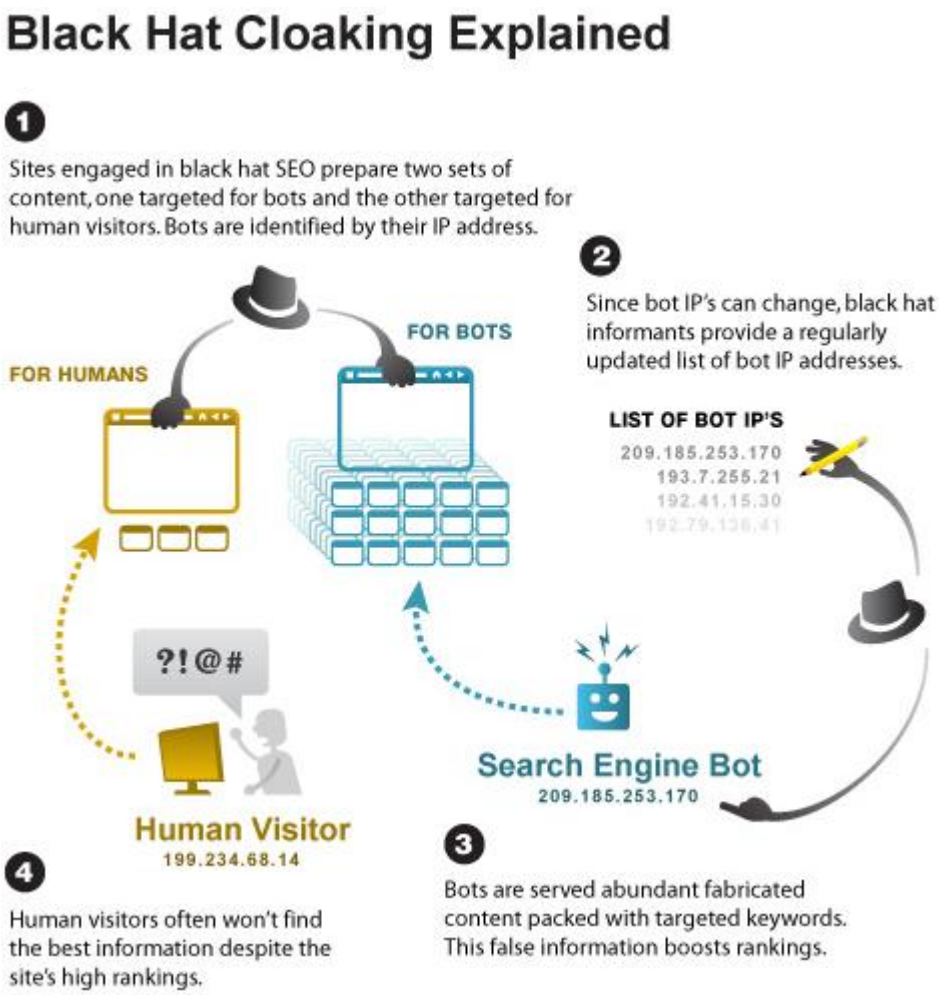


Figure 1: Cloaking visualisiert. Source: https://goo.gl/BRtnSr

# 3 Funktionsweise

## 3.1 Vorbereitung des Angriffs

Der Angreifer besitzt eine Webseite, auf der er die Viren verbreitet. Bei bekannten Image Poisoning Attacken, wird das Aussehen der Webseite so angepasst, dass diese das Aussehen eines Windows Vista Explorer Fenster annimmt. Um genauer zu sein eines Windows Vista Explorer Fensters da Image Poisoning seinen Hype um die Jahren 2011 und 2012 hatten.[3] Dabei wird sowohl das Aussehen imitiert sowie aber auch mittels geschickten Animationen das Fehlver-

halten des Explorer Fenster. Dies soll dazu führen dass der Besucher das Gefühl hat sich nun im System zu befinden und nicht auf der Webseite. Der Fensterinhalt beinhaltet meistens die Laufwerke welche mit "C:" und "D:" beschriftet sind. Die Animation imitiert das Aussehen eines Virenscans auf dem Laufwerk C: und nach vollenden der Animation wird eine Windows Vista Warnfenster eingeblendet und animiert. Das Warnfenster zeigt ein Virenscan Resultat und fordert den Benutzer auf, die Viren zu entfernen. Beim akzeptieren wird eine Datei heruntergeladen und es wird ein Virus ausgeführt. Die Browserinterne zurück-Funktion wird mit einer Meldung überschrieben. Diese warnt den Benutzer vor dem verlassen des Scans und ob dieser wirklich abgebrochen werden soll.

Neben der Webseite muss der Angreifer eine Webseite die in der Bildersuche hoch angezeigt wird kompromittieren. Der Angreifer muss in der Lage sein, auf der Webseite die normalen Benutzern von den Google Crawler zu unterscheiden (Javascript, PHP, etc.). Auch gehören zu den verschiedenen Anfragen unterschiedliche Versionen dazu. Alternativ kann der Angreifer eine Fake Webseite aufsetzen und diese so manipulieren, damit dieser in den Suchresultaten höher angezeigt wird. Dazu werden die Google trending Wörter erfragt und Webseiten mit diesen Wörter gefüllt. Diese Webseite müssen bei einer Google Suchanfrage noch zusätzlich ein Javascript mitliefern, welches dann die Url des Hauptfensters verändern kann. Ein Javascript Code Beispiel sieht wie folgt aus:

```
<script>
var url = "http://REMOVED/in.cgi?2&seoref="
        +encodeURIComponent(document.referrer)
        +"&parameter=$keyword&se=$se&ur=1&HTTP_REFERER="
        +encodeURIComponent(document.URL)
        +"&default_keyword=default";
if (window!=top)
{
   top.location.href = url;
}
else
{
   document.location= url;
}
</script>
```

[9]

## 3.2 Durchführung des Angriffs

Der Angriff erfolgt ohne weitere Interaktionen des Angreifers. Als Beispiel sucht ein Benutzer nach Katzen und wird in der Google Suche fündig. Bei Google werden die ersten Bilder der Suche gecached und auf den Google Servern abgelegt. Beim anklicken der Bilder öffnet sich dann eine Vorschau indem die Bilder größer angezeigt wird (immer noch in der Google Suche). Diese Vorschau fragt auf dem

Server nach dem gewünschten Bild (in diesem Fall vom kompromittierten Server des Webhosters). Die Anzeige wird per Iframe eingeblendet und nicht über einen Google Server weitergeleitet. Sobald das Iframe den Server abfragt, erhält er von dem Server eine Antwort mit dem zusätzlichen Script. Der Webbrowser des Suchenden führt das Script sofort aus und leitet somit die Webansicht des Suchers direkt auf die Webseite des Angreifers mit der Antivirus-Meldung. Von dort aus wird der Virus verteilt.

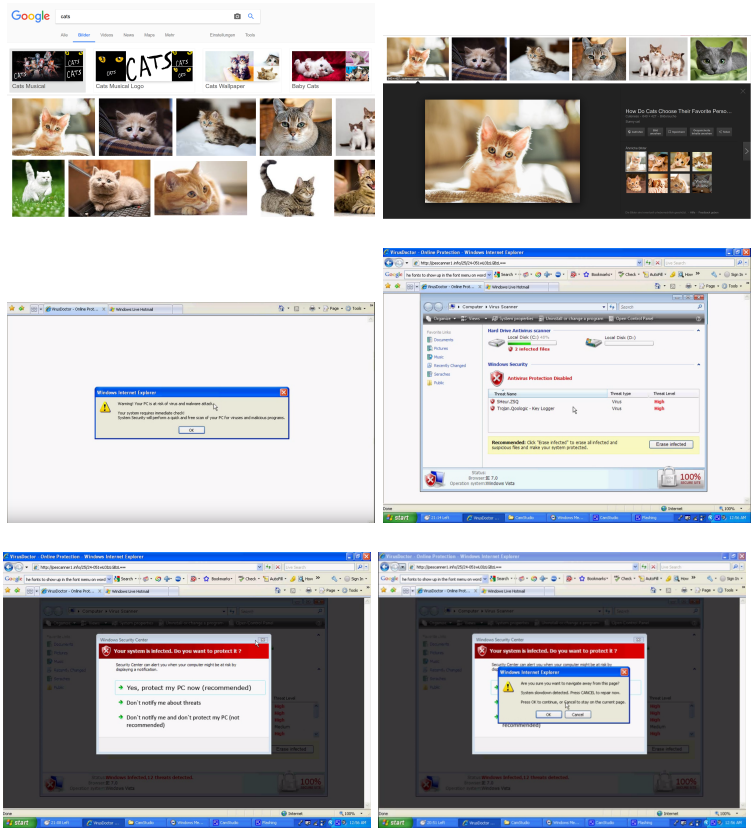


Figure 2: Verlauf Image Poisoning

[5]

# 4 Verbreitung

Image Poisoning war vor allem in den Jahren 2011 und 2012 mit mehreren tausend infizierten domains weit verbreitet.[4]

Eine Studie im Jahr 2012 ergab, dass 65% aller mit Image Poisoning oder cloaking in Verbindung stehende redirects die Suchmaschine Bing, 30% Google

und 5% andere Suchmaschinen betrafen.[2]

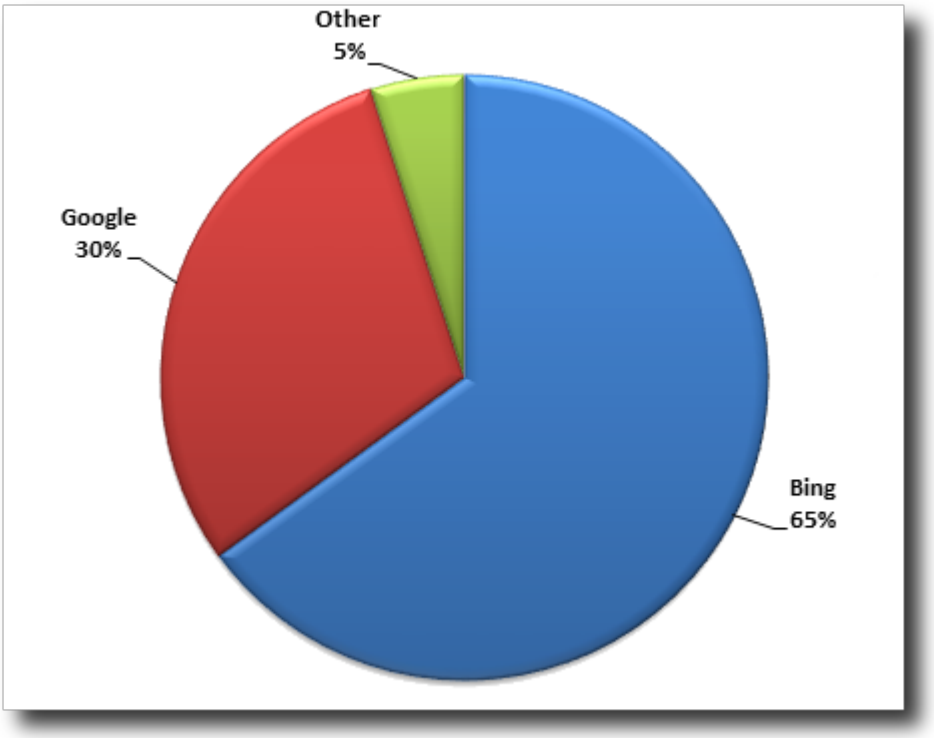


Figure 3: Redirects pro Suchmaschine

Die Studie zeigt dass Angreifer über die Bildersuche um ein vielfaches erfolgreicher sind als über die Textbasierte Suche. Von allen Erfolgreiche redirects stammen 92% aus der Bildersuche.[2] Daraus lässt sich schließen, dass es für Provider der Suchmaschinen einfacher ist, "infizierte" Resultate aus einer regulären Textsuche zu filtern als bei einer Bildersuche.

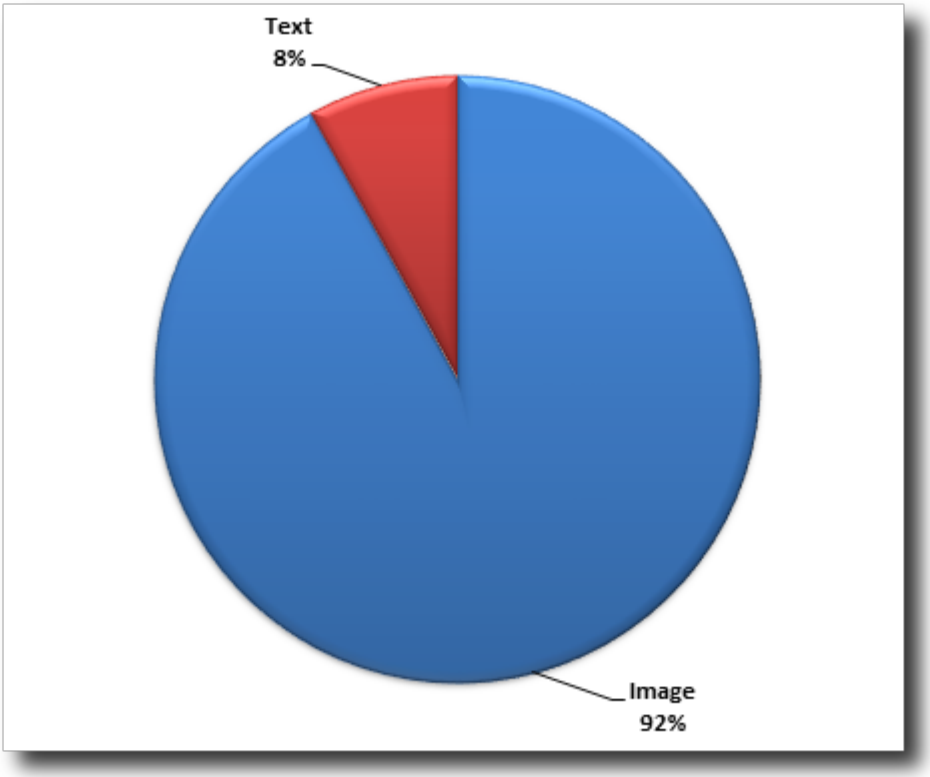


Figure 4: Art des Angriffs

[2]

Es ist davon auszugehen, dass das Ausmaß von Image Poisoning in der Zwischenzeit stark abgenommen hat.[2] Jedoch ist es nicht auszuschließen, dass Image Poisoning nach wie vor praktiziert wird. Deshalb lohnt es sich dennoch beim Suchen im Web vorsichtig zu sein.

# 5 Gefahren / Ziele der Angreifer

Kriminelle versuchen mitunter, an sensible Informationen wie Bankdaten oder Passwörter zu kommen oder die Kontrolle über einen oder mehrere Rechner zu erlangen. Dabei wird eine Webseite mit einem guten Ranking gehackt oder die eigene Webseite Search Engine Optimization optimiert (siehe cloaking). Bei Malvertising wird eine Werbeagentur oder ein ganzes Netzwerk infiltriert. Dabei werden herkömmlichen Werbebannern, Programme oder Flash-Applikationen mit Skripten verteilt und gestartet.

Klickt ein Nutzer auf eine solche Werbung oder lädt eine Website mit einer schädlichen Werbung, kann ein Download, ein Programm oder ein Skript aktiviert werden. Sobald dies geschehen ist, hat der Nutzer kaum noch Möglichkeiten angemessen auf einen solchen Angriff zu reagieren. Die Schadsoftware lässt sich schon durch einen Klick auf den Banner aktivieren.

Die Folgen können beispielsweise folgende sein:

- eine Offenlegung von privaten Informationen
- eine Weiterleitung zu nicht vertrauenswürdigem Inhalt
- der Systemabsturz
- der Verlust der Admin-Rechte eines Computers
- Installation eines Virus

Dies kann wiederum finanziellen Schaden nach sich ziehen oder weitere unangenehme Konsequenzen haben.[8]

# 6 Rechtslage

Wie oben bereits erwähnt, gibt es zwei verschiedene Arten von Image Poisoning. Bei der ersten werden fremde Webseiten mit hohem Ranking gehackt um eigene Inhalte zu verbreiten und bei der zweiten werden Inhalte über Search Engine Optimization mittels falschen Schlagworten verbreitet.

Beide Formen sind rechtlich gesehen problematisch. In der Schweiz ist das hacken einer fremden Webseite illegal und steht unter Strafe.[7] Die zweite Art des Image Poisoning beziehungsweise das Verbreiten von Inhalten unter falschen Schlagwörtern verstößt gegen die Google Quality Guidelines. Dies gilt auch für das ausfiltern des Google Bots um dem Bot etwas anderes zu liefern als einem menschlichen User.[1]

# 7 Motivation

Ziel des Angreifers ist es grundsätzlich, den Benutzer auf eine vom Angreifer kontrollierte Webseite zu locken. Von da an will sich der Angreifer selbst bereichern oder dem Opfer Schaden zufügen. Er versucht den Benutzer dazu zu bringen z.B. seine Kreditkartendaten oder andere persönliche Daten preiszugeben.

# 8 Malvertising

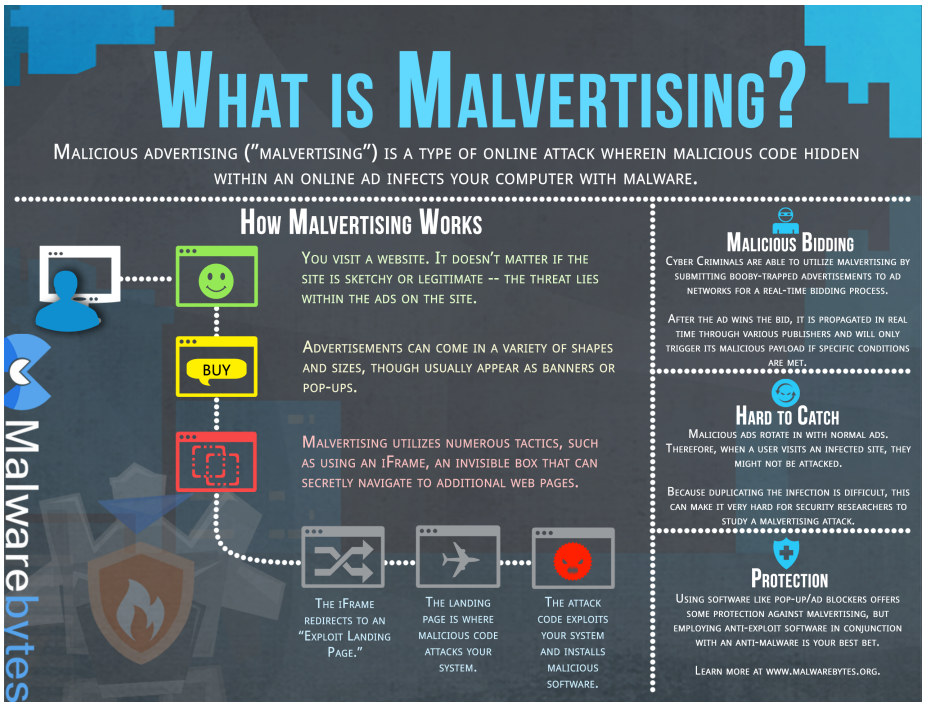


Figure 5: Malvertising Flussdiagram Source: https://goo.gl/NY2HDU

Malvertising ist ein Kofferwort aus Malware (schädliche Software) und Advertising (Online Werbung).[8] Hierbei wird nicht eine Website Angegriffen bzw. doppelt verwendet sondern ein Netzwerk mit Virenbehafteter Werbung gefüttert. Da die Werbenetzwerke auf vielen Seiten eingebunden sind, erhält man eine grosse Verbreitung. Die User werden dann auf vertrauenswürdigen Webseiten mit Viren angegriffen.

# 9 Schutz vor Image Poisoning / Malvertising

## 9.1 Benutzer

Mit Browser Plugins wie NoScript und AdBlock lassen sich die Angriffsmethoden Image Poisoning und Malvertising verhindern. Bei NoScript werden nur noch Javascripts von vorher als vertrauenswürdig markierten Webseiten ausgeführt. Adblock schützt vor Malvertising indem das ganze Werbe-Iframe garnicht erst geladen wird.

## 9.2 Webseiten

Um sich vor Image Poisoning als Webseitenbetreiber zu schützen, muss die Seite vor Hackern geschützt werden. Die Webseite muss dabei einen Hacker daran hindern, die Seite zu editieren (FTP, SQL Injection).

Malvertising lässt sich als Webseitenbetreiber nicht direkt verhindern. Es muss deshalb besondere Sorgfalt bei der Auswahl der Werbenetze betrieben werden.

## 9.3 Anbieter Bildersuche / Werbung

Als Anbieter der Bildersuche muss beim erstellen von Iframes das Aufrufen von Skripten unterbunden werden. Alternativ lassen sich Bilder auch cachen (was mehr Speicherbedarf verlangt) und so ein erzeugen von Iframes komplett verhindern.

Gegen Malvertising hilft etwa prüfen des Werbeinhalts durch das Werbenetzwerk bevor das Werbenetzwerk den Inhalt ausliefert. Werbenetze müssen zudem den Inhalt auf eigenen Servern hosten, damit die Werbung nicht nachträglich vom Anbieter geändert werden kann.

# 10 Referenzen und Akronyme

## Glossary

**Bot** Roboter 3, 9

**Google Crawler** Beim Google Crawler handelt es sich um einen Programm welches automatisch das World Wide Web durchsucht und Webseiten analysiert. Dieser wird vor allem für das Indexieren von Suchmaschinen (hier Google) verwendet. 5

**Google Quality Guidelines** Die Qualitätsrichtlinien von Google, beschreiben die Handhabung von unerlaubten Verfahren auf Webseiten. Diese können zur Entfernung einer Webseite aus dem Google-Index führen oder einer Beeinträchtigung der Suche für die Webseite. 9

**Iframe** Webseitenelement zum anzeigen einer weiteren Webseite 3, 6

**kompromittierten Server** Als kompromittierter Server bezeichnet man einen Server welcher manipulierte Datensätze aufweist. Der Eigentümer ( der Administrator) hat keine Kontrolle über die korrekte Funktionsweise des Servers oder den Inhalt. 6

**redirects** Der Redirect ist eine Weiterleitung auf eine Webseite, die automatisch erfolgt. Der Internetnutzer ruft eine Seite über eine URL auf, wird jedoch auf eine andere URL weitergeleitet. Dabei kann der Nutzer keinen Einfluss auf die Weiterleitung nehmen. Als Redirect wird eine Weiterleitung auf. 6, 7

**Search Engine Optimization** Die Suchmaschinenoptimierung auch Search Engine Optimization oder SEO genannt, dient der optimierung der Webpräsenz damit dieser bei den Ergebnissen der Suchmaschinen höher angezeigt wird. Die Optimierung beinhaltet sowohl Bilder, Videos sowie die Nachrichtensuche. 8, 9

## References


[1] Google. Google webmaster guidelines, 2017. URL https://support.google.com/webmasters/answer/35769.

[2] Fraser Howard. Searching for images on bing? beware malicious search engine poisoning, 2012. URL https://nakedsecurity.sophos.com/2012/10/05/bing-image-blackhat-seo-poisoning/.

[3] Jan Širmer. Google-images poisoning stats, 2011. URL https://blog.avast.com/2011/05/17/google-images-poisoning-stats/.

[4] Jan Širmer. Google-images poisoning slides, 2016. URL https://goo.gl/G2LdFm.

[5] Pyrodron Productions. Image poisoning angriff, 2009. URL https://www.youtube.com/watch?v=ISO3PSjEQt4.

[6] Dmitry Samosseiko. Google search poisoning – old dogs learn new tricks, 2015. URL https://news.sophos.com/en-us/2015/07/07/google-search-poisoning-old-dogs-learn-new-tricks/.

[7] David Schneeberger. Image poisoning angriff, 2015. URL https://www.lexwiki.ch/hacken/.

[8] Ryte Wiki. Malvertising, 2017. URL https://de.ryte.com/wiki/Malvertising.

[9] Bojan Zdrnja. Searching for images on bing? beware malicious search engine poisoning, 2011. URL https://isc.sans.edu/diary/More+on+Google+image+poisoning/10822.

# List of Figures