CPNI
Centre for the Protection of National Infrastructure

# ONLINE RECONNAISSANCE

## HOW YOUR INTERNET PROFILE CAN BE USED AGAINST YOU

**May 2013**

Most people and organisations put information about themselves on the web. Companies advertise their work and achievements and people use social media, blogs and forums to share personal and professional information, such as projects they work on and contact details. Sensitive information about us can also be put on the internet by other people and organisations without our knowing. Online information can easily be used by rival companies, malicious individuals and even Foreign Intelligence Services (FIS) to learn about their targets. Online information that can be used this way is called Open Source Intelligence (OSINT) and the process of collecting it is called **reconnaissance**.

CPNI has recently conducted several studies to collect information on a number of organisations, with the aim of developing a better understanding of methods used for online reconnaissance. These have highlighted many avenues that could be exploited by an adversary. This short viewpoint document draws on these findings to raise awareness of the risks from online reconnaissance and of the safeguards they can take to mitigate against them.

## Using reconnaissance to target an organisation

Our focus here is to describe how online reconnaissance can elicit information that can be used to carry out cyber compromises, but online information can also be used to plan physical attacks against installations and personal approaches to staff.

To conduct a successful cyber compromise, an adversary needs to gain access to the victim's network. This is made much easier if they have certain details about the network and its users. Many of these details may be found by gathering OSINT on the target.

CPNI's OSINT case studies found that many details were available online such as employee contact details and job descriptions, company projects and commercial ventures, the company's IP addresses and software versions used on its networks. There were also many examples of third party suppliers posting sensitive details about their customers online. Once adversaries know the software versions that a company uses, they can find or develop malware (software designed to do

something malicious) that exploits particular vulnerabilities in unpatched versions, simply by searching online. Up-to-date patching is a key mitigation for this scenario.

Malware is usually introduced to a victim system when a user inadvertently opens an email with the malware embedded in an attachment. These emails are known as **spear-phishing** and the adversary needs to know victims' email addresses to carry them out. Adversaries may find these email addresses online, or may even be able to guess them, if company email addresses have a standard form[1].

## Spear-phishing

Cyber-attacks are usually initiated by a spear-phishing campaign, which involves fooling the victim into opening an email and clicking on an attachment or link that runs malware on the system. These days, people are less likely to open random obvious mass-mailing messages and so attacks are becoming more targeted and informed. Adversaries conduct reconnaissance to find background information and carefully craft email messages which look interesting enough to entice recipients into opening attachments or links.

Once on the system, the malware will 'beacon' or signal to IP addresses owned by the adversary, who may then task the malware to transmit sensitive information from the network, across the internet. Enticing or duping the user into opening the attachment or link is the key stage in a successful compromise.

## Using OSINT for spear-phishing

Lockheed Martin[2] recently developed the 'kill-chain' representation for the steps involved in an effective cyber-attack (see Figure 1). OSINT collection forms a key part of what they refer to as the RECONNAISSANCE phase.

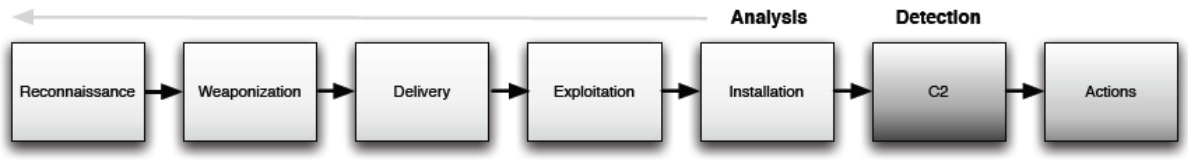


*Figure 1: Lockheed Martin's Cyber Attack Kill Chain*

[1] Such as firstname.surname@company.co.uk.
[2] www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Some OSINT sources that are useful for spear-phishing are directly visible, other sources are more hidden. We will distinguish between two types of information as:

- **Visible information**

This is information that is useful to an adversary and can be found in a number of easily accessible places on the internet.

Company websites often show employee names, job titles, e-mail addresses and even phone numbers. They can also show organisation structure, details of events, or projects and partner organisations. Employees also use social networking sites[3] to share personal details, discuss work matters or even post gossip or derogatory information about their employers. Adversaries may find career details by searching on an employee name in a database like LinkedIn and may even identify whole project teams by searching on keywords in for a like Facebook or LinkedIn. People who put details of their employment, interests, expertise or affiliations on such databases or websites should bear in mind that anyone can contact them and that simply following a link in an email sent to them could be enough to lead to a cyber-compromise. It is not just the CEO of an organisation who is of interest in this respect; any staff member can open a compromising link, so could be targeted in this way.

Web forums are popular for exchanging solutions to technical and IT problems and technical staff who use them might provide a great deal of detail or even copy and paste command lines and other configuration files onto them to help their discussions. This can provide an adversary with the information they need to focus an attack against a company's systems. There have even been cases where employees have shared corporate account and password details on text-sharing forums. If adversaries find interesting postings, they can search on the user's ID or email address to find postings by them on other forums.

OSINT can also be used to plan physical attacks on company sites. Google Earth, Google Street View and Flickr can give information on a company's building layout and physical security measures. Site plans are usually published on Local Authority (LA) websites. LAs are legally bound to make plans available on request, but can provide them in hard copy, rather than via the internet and will do this on request. CPNI recommends that managers of sites whose layouts are sensitive make this request to their LA.

- **Hidden information: meta-data**

Many online documents contain metadata that are potentially useful to adversaries. Document meta-data can provide information about a document's author, its location on the corporate network and the software version used. This information can help adversaries perpetrate cyber-attacks.

[3] E.g. Facebook or MySpace. There are many others. Some are more exclusive to particular sectors, such as academia, finance or law.

Adversaries can also find meta-data by scanning and probing company networks. If a network is connected to the internet, it transmits information like technologies in use and IP address ranges. Knowing the IP addresses allows an adversary to scan a network's ports to see what software versions it uses, whether they are patched and whether they can be exploited by particular malware. This informs the WEAPONISATION phase (see Figure 2) of a spear-phishing campaign. Meta-data like IP addresses can also be extracted from web-pages and company emails.

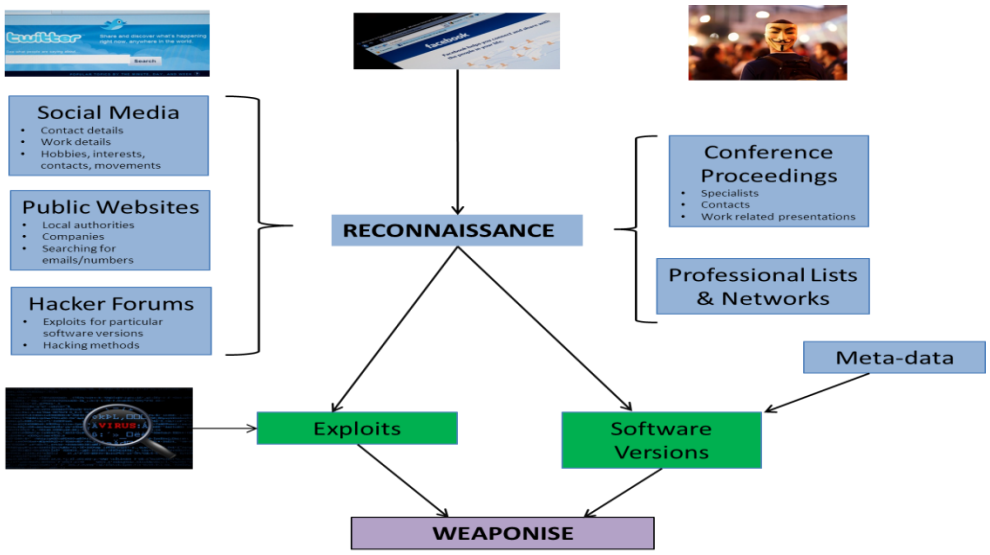


*Figure 2: The range of sources an adversary might use in crafting a spear-fishing attack*.

Adversaries can use a wide range of sources to gather the information they need to develop malware and carry out a cyber-intrusion. Figure 2 shows how some of these sources can be used together.

## How can you mitigate against these risks?

Companies face considerable challenges in minimising their vulnerability, due to the number of information sources in the public domain and the fact that staff online behaviour in a personal capacity is a key risk, which is difficult to address. Companies should develop OSINT strategies to guide what information is published and develop best practice, including guidance on staff personal use of the web. Companies should conduct OSINT reviews to determine how much information about them can be found online. Online information is constantly changing, so these reviews should be conducted at least annually. Many consultancies offer OSINT reviews as a service, combined with comprehensive risk assessments.

As well as conducting regular reviews of their OSINT profile, organisations may consider implementing some of the following measures.

- **Filtering and censoring**: put in place strict channels to screen publication to the web.

- **Removing from internet**: removing content from the internet is difficult and requires co-operation from the owner of the site where the information is stored. Requests can be made to Google to ensure that certain URLs will never appear as Google search results by using the Google URL removal tool. Other search engines offer a similar service, but (assuming their co-operation) this does not guarantee URLs will not appear in searches and does not remove them from the internet itself.

- **Dilution:** where sensitive information is already online and cannot be removed, companies can mitigate its effects by adding more information to distract from the main sensitivities.

- **Supplier contracts:** suppliers and contractors can publish client data in unhelpful ways to advertise collaboration or services they provide (e.g. IT services or software). Companies can safeguard against this by drawing up agreements with suppliers to stipulate what they may or may not publicise online.

- **Technical controls:** Data Loss Prevention (DLP) solutions are available to control data leaving an organisation (e.g. email, portable media or uploading to remote servers), but cannot control external factors. Documents published online should be stripped of meta-data, using meta-data removal tools. Some software (e.g. Microsoft Office 2007) comes with add-ins which do this.

- **Site plans:** companies can request that Local Authorities (LA) do not place site plans or planning requests relating to their sites on LA websites. The LA can retain hard copy only versions of these plans at their offices and can retain logs of requests made to view them.

- **Staff education:** employees are often the weakest link in a security procedure and organisations should promote good security culture and best practice. Employees should be made aware of the threats of spear-phishing and socially engineered attacks. It is also important to educate staff on their personal use of the web so that they are aware of the risk this may present to their organisation and to themselves as employees.