CPNI
Centre for the Protection of National Infrastructure

SPEAR PHISHING

UNDERSTANDING THE THREAT

SEPTEMBER 2013

Due to an organisation's reliance on email and internet connectivity, there is no guaranteed way to stop a determined intruder from accessing a business network. Reliance on email and the internet brings vulnerabilities which must be recognised and addressed appropriately. The IT security community has assessed that Spear Phishing is a remarkably effective cyber-attack technique and its use to gain access to business systems is unlikely to decline in the near future.

This paper describes how Spear Phishing attacks work, the likelihood of being targeted and the steps an organisation can take to manage the business risks.

Key points

- Spear Phishing is a targeted form of email deception.
- Most targeted attacks against an organisation begin with a Spear Phishing email.
- Spear Phishing has a high success rate and its use as a means of attack looks set to continue.
- Successful attacks can result in exploitation or compromise of individual devices and organisational networks. This can have significant implications for an organisation.
- The risk from Spear Phishing can be reduced through good educational awareness and effective technical controls.

Introduction

Phishing is a form of email deception used by a range of adversaries in an attempt to obtain sensitive information or cause disruption to an organisation's business operations. Spear Phishing is a more targeted version of phishing where an adversary conducts online reconnaissance against an individual or organisation in order to construct an email which appears to be of significant interest to those targeted. The email is designed to persuade the target individual to open a file attachment or click on a website link. In doing so, malicious software (or malware) is executed, designed to exploit and compromise the individual's IT device.

Spear Phishing email attacks are persistent and often have a high success rate as they are able to bypass traditional security defences and exploit vulnerable software.

Reconnaissance

An adversary will use information sources (free and subscription-based) to build background knowledge of a target individual or organisation. This information found online is called Open Source Intelligence (OSINT) and the process of collecting it is known as Reconnaissance. Organisations share information across the internet via their public website or social media sites. This information may be published by themselves or by their business partners. An adversary will aim to acquire as much information about a target as possible, as the more information they have available, the greater the chance the Spear Phishing email will be seen as a legitimate communication.

Research conducted as part of CPNI OSINT studies included investigation into online information relating to a number of participating companies. This highlighted the information an adversary would look to obtain when conducting a Spear Phishing attack; this information includes staff contact details, organisation charts, job descriptions and technical information such as IP addresses, project names and software versions in use within an organisation.

To construct a successful Spear Phishing attack, an adversary requires a target email address. Using search engines, an adversary will look for online profiles which contain contact details of a target individual. If an email address is not within the contact information, an adversary may attempt to guess the address, by trying a common format such as firstname.surname@companyx.com. Adversaries will often send Spear Phishing emails to a range of plausible email addresses to determine a valid address. CPNI has published guidance, entitled *Online Reconnaissance – How your internet profile can be used against you* which describes this scenario in further detail.[1]

[1] See CPNI guidance on Online Reconnaissance www.cpni.gov.uk/advice/cyber/online-reconnaissance

Construction and delivery of Spear Phishing emails

After conducting online reconnaissance an adversary now has enough information to create a Spear Phishing email. The email will include all information discovered through the reconnaissance phase and contain an attachment or website link which is of interest to the target. The adversary will then attempt to alter the email to make it appear as if the message was sent from a trusted contact of the target individual. An email which appears to be from a trusted contact increases the likelihood of a successful compromise.

Attachments contained within Spear Phishing emails will appear as a common file type such as .rtf or .pdf. The name will be of interest to the target, e.g.' pay award.PDF' When the attachment is opened embedded malicious software is executed designed to compromise the target's IT device.

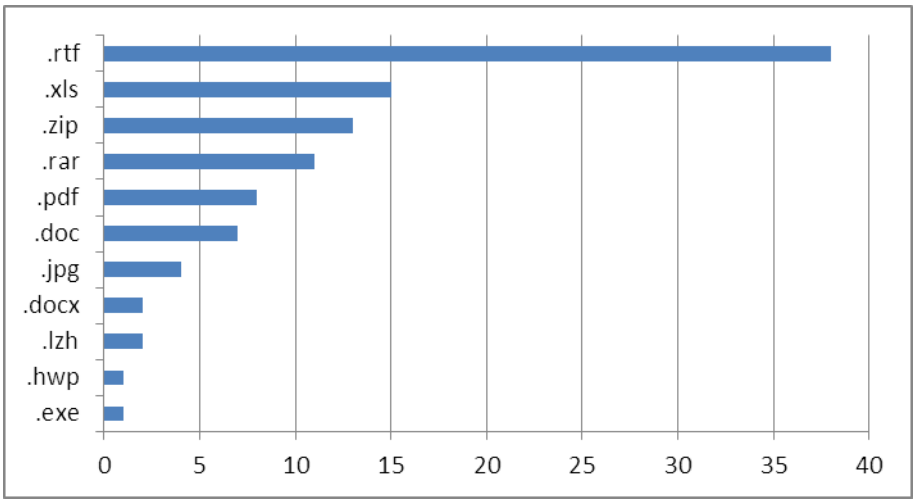

Figure 1 - Top spear-phishing email attachment file types (Trend Micro 2012)

Links within Spear Phishing emails will direct a target individual to a website which, when accessed, will execute malicious software. A common method for an adversary to disguise a compromised website is to compress the address, so it is displayed in a shortened format such as http://tinyurl.com/companyx. Websites which are compromised appear authentic by having the same design and structure as legitimate websites. It is possible that a legitimate website could also be compromised further increasing the chance of a successful attack.

When malicious software is successfully accessed via an attachment or website link, it will seek to exploit vulnerabilities in a target operating system or web browser. Figure 2 describes the stages in a Spear Phishing attack and how the adversary will look to exploit an organisation's network.

Stages involved in a Spear Phishing attack

CPNI uses the Cyber Kill chain developed by Lockheed Martin[2] as a representation of the stages involved in an effective cyber-attack. For a Spear Phishing attack to be successful, the following stages are present:

- **Reconnaissance:** In the reconnaissance phase an adversary browses websites, downloads PDFs, and learns about the internal structure of a target organisation.

- **Weaponization:** In this phase the adversary places malicious code into a delivery vehicle such as an attachment or website.

- **Delivery:** The delivery phase involves the transfer of malicious content to the target in some form. In the case of Spear Phishing this is via email.

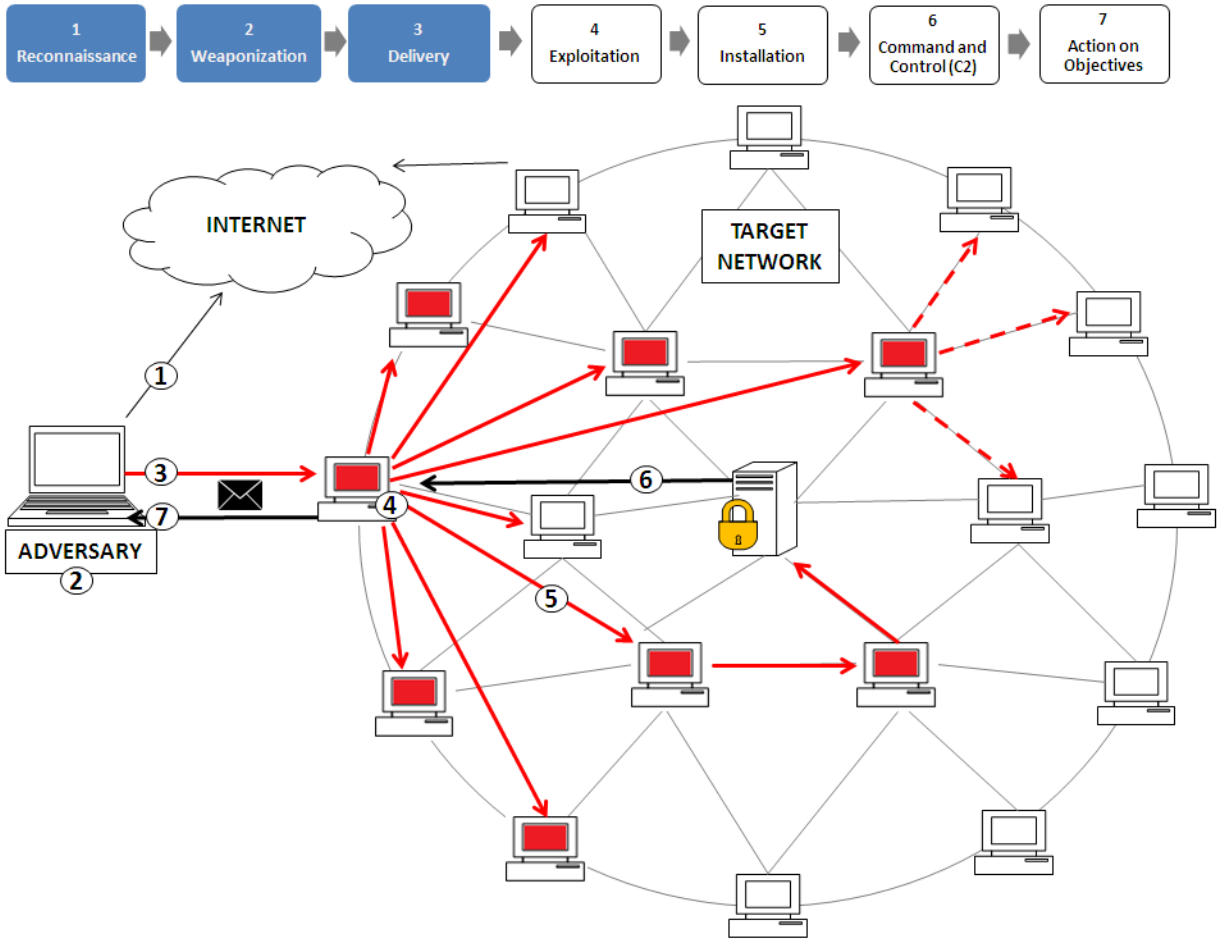

Figure 2 - Spear Phishing stages

[2] www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Business impact

Successful Spear Phishing attacks can have significant implications for organisations. The more serious implications of becoming the target of a cyber-attack are listed below:

Theft of sensitive information: An adversary may steal commercially useful information such as trade secrets, merger and acquisition plans, engineering designs, software codes or details of research programmes. This could result in the loss of competitive advantage and have significant financial consequences.

Sabotage: Once on a network, an adversary may seek to delete or alter data with the aim of disrupting business operations. Depending on the access level gained, they could make changes to company data, log files, configuration settings, and user passwords or alter code for applications running on the network.

Secondary use of compromised machines: An adversary can use a compromised machine to conduct attacks against other individuals or networks. This may involve sending Spear Phishing emails to contacts from a compromised user account. This can cause reputational damage to the initial victim organisation, as its customers and suppliers will initially attribute these communications to the sending organisation.

Incident response and recovery costs: Investigating and recovering from a compromise can be expensive and time-consuming. The cost will depend on how long the network has been compromised and the steps needed to prevent the risk of an adversary simply being able to re-establish a presence on the network.

How to defend against Spear Phishing attacks

In order to successfully reduce the risks posed by Spear Phishing attacks, organisations should seek to achieve a good balance of educational awareness and effective technical controls. CPNI endorses the Critical Security Controls[3] as an effective way to protect against Spear Phishing and other cyber-attacks. This section presents the most relevant Critical Security Controls for defending against Spear Phishing -

Security awareness training: An important measure in defending against Spear Phishing attacks is ensuring a high level of security awareness amongst staff. Employees should be educated about the changing nature of Spear Phishing attacks. An adversary will look to exploit an employee's lack of security awareness. There are some questions an employee can ask when receiving an email with a suspicious link or attachment.

- Who is the sender? Can the employee verify it has definitely come from them and is it someone from whom they would expect to receive emails on this subject?
- Is the style of writing consistent with the sender? Does anything appear unusual about the tone, spelling or urgency of the email?
- Is the request out of the ordinary (e.g. to open a file the user wasn't expecting)?
- Have other colleagues received a similar email?

These questions can begin to help employees identify Spear Phishing emails. When training staff, it is important to make them aware of company policies regarding communications and security.

Organisations can look to design their own training package to educate their staff on the threat posed from Spear Phishing using commercially available tools. In the training package, if a user does click on a link or open an attachment in a test email, they will be taken through to a training area that helps them gain a better understanding, making them less susceptible to attacks in the future. A number of anti-phishing tools are also available to alert users to phishing content contained within websites and emails. These tools offer an advanced level of protection above traditional IT security defences.

Boundary defence: Malicious code generated from Phishing emails will exploit systems which can reach across the internet.

To control the flow of traffic through network borders, organisations should use multi-layered boundary defences such as firewalls, proxies, demilitarised (DMZ) perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic to look for any anomalies that may suggest malicious activity.

[3] Critical Security Controls www.cpni.gov.uk/advice/cyber/Critical-controls/

Controlled use of administrative privileges: Organisations should aim to minimise administrative privileges and only use administrative accounts where required. If a privileged user opens a malicious attachment or accesses a website with embedded malicious content, malware will be deployed to their IT system with the adversary assuming administrative privileges. With elevated rights, an adversary can install malware and establish a foothold within the network faster than with standard user access rights.

Continuous vulnerability assessment and remediation: Most Spear Phishing emails aim to exploit known vulnerabilities in software. It is therefore vital to ensure that all systems and software are up to date with the latest patches[4]. Patches should be applied to software that is most likely to be targeted by an adversary. It is important that all types of infrastructure are patched, including laptops, mobile devices, desktops, servers, switches and routers. This way, even if a compromised attachment or link is opened, the malware will not be executed.

For further information on any of the topics discussed in this paper visit www.cpni.gov.uk

[4] A patch is a small piece of software that is used to correct a problem with a software program or an operating system.