

INFORMATION SECURITY BRIEFING

NOVEMBER 2007

DEFENDING AGAINST ELECTRONIC ATTACKS

CPNI disclaimer

CPNI has taken every care in preparing this protective security advice, which is informed by intelligence on the threat. However, CPNI cannot accept any liability to any person or company for any financial loss or damage arising from the use of this advice or from any failure to give advice.

INTRODUCTION

1. This document is a technical brief designed to help organisations in the UK Critical National Infrastructure, government and wider industry defend themselves against electronic attack.
2. Electronic attack in this context refers to emails with malicious attachments or websites that have been compromised in order to deliver malicious software. The aim of the attacks is the covert theft of documents and other intellectual property from the target organisations.
3. Electronic attacks are directed at a wide range of public and private sector organisations globally, including in the UK.
4. This document covers technical details of attacks and provides mitigation advice.
5. This briefing also provides links to further advice on the CPNI website (www.cpni.gov.uk).

DESCRIPTION OF ATTACKS

6. In general, the types of electronic attacks most often reported to CPNI take two main forms; email borne Trojans and compromised websites. Description of both of these follow below:

Email Borne Trojans

7. A Trojan is defined as a seemingly benign file, but which has hidden within it malicious software (malware) that will compromise the PC of the victim when opened.

8. Trojans are usually delivered to the victim via email. These emails demonstrate a sophisticated level of targeting:

- They appear to be from a legitimate sender (the 'from' field will be spoofed),
- they are of interest to the recipient, and
- the attachment will often be a genuine document of interest to the recipient (often the attachment is a real document that has been stolen from elsewhere).

9. The effort put into the targeting of emails is sometimes let down by poor English in the email body itself. However, in general, the text is short (e.g. 'Please see attached document') and hence the language used is sufficiently convincing.

10. Less commonly, attack emails will contain a hyper link to what appears to be an item of interest to the victim (e.g. a link to a current news story on a website). Clicking on the hyperlink will result in a Trojan being delivered from what is in fact a malicious site.

Web based attacks

11. Web based attacks are not targeted to the same degree as email attacks. This delivery vector involves the compromise of a website in a sector of likely interest to the attackers (e.g. the website of a defence sector company).

12. The website is modified in a way that enables the silent (meaning transparent to the victim) delivery of a Trojan to anyone visiting the website. This is usually achieved by inserting a zero pixel iframe onto a legitimate page of the website.

13. These types of compromise have a number of stages. The iframe itself will call the first stage of the compromise, usually obfuscated javascript. This script will attempt to exploit a vulnerability in the visitor's browser. If the script runs successfully, it will then download and run an executable, with the end result being the compromise of the visitor's PC.

14. The location of each of these stages may vary. The iframe may reference a script that has been placed by an attacker on the compromised website at the same time as the iframe itself. However, sometimes the script will be on an unrelated server that is being used by an attacker to host malware. The same is true of a Trojan.

MITIGATION

15. Trojans are designed to provide an attacker with a way into a network. To be effective, once they are running on the compromised PC they will attempt to connect back to a command and control (C&C) server. This enables an attacker to make contact with compromised PCs even on a network that prohibits inbound connections (as the connection is instigated from inside by the Trojan itself).

16. More sophisticated Trojans are proxy aware. Connections back to C&C servers are usually over http or https, as these are the only connections that most organisations will permit outbound.

17. There are a number of possible ways to disrupt an attacker's activity:

- Prevent the Trojan reaching the user through email and web filtering.
- Change user behaviour to prevent execution of any malware that breaches perimeter security software
- Remove the vulnerability hence rendering the exploit used ineffective
- Prevent the Trojan contacting the C&C server

18. CPNI has the following relevant documentation available online:

- Briefing 08/05: Targeted Trojan Email Attacks
<http://www.cpni.gov.uk/niscc/docs/ttea.pdf>
- Technical Note 08/03: Trojan Horse Programs and Rootkits
<http://www.cpni.gov.uk/niscc/docs/re-20030911-00728.pdf>
- Technical Note 04/2006: Spyware
<http://www.cpni.gov.uk/niscc/docs/re-20060601-00384.pdf>
- Technical Note 01/04: Increased Use of Trojan Horse Programs
<http://www.cpni.gov.uk/niscc/docs/re-20040216-00080.pdf>
- Technical Note 03/04: Guidance on Handling Files with Possible Malicious Content

<http://www.cpni.gov.uk/niscc/docs/re-20040319-00147.pdf>

- Current Advice: Mitigating the risk of Malicious Software (2004)
<http://www.cpni.gov.uk/niscc/docs/currentAdvice.pdf>

19. CPNI strongly recommends a comprehensive patching programme. It is understood that frequent patching across a large organisation, with all the testing that must be carried out, is onerous.

20. However email and web attacks are often successful using vulnerabilities for which patches have been available for up to a year. Zero day attacks (attack using a previously unknown, and hence un-patched, vulnerability) do occur, however they are infrequent compared to the use of reported and patched vulnerabilities.

21. PC office productivity application files are the most frequently used vehicles for Trojan delivery, and hence security patches for these should be regarded as being of high importance.

USER EDUCATION

22. Given the effort put into making attack emails appear legitimate it is difficult to offer mitigation advice to end users.

23. Broadly CPNI recommend that users:

- Validate emails that contain attachments by contacting the apparent sender
- Look for odd behaviour if opening an email attachment e.g. if opening a Trojanised document file, a word processor application may start, close down and then restart as normal. While being a good indicator of malware, this behaviour does not always occur.

24. Broken or poor English in an email apparently from someone known to the recipient as a fluent English speaker should be regarded as a suspicious indicator.

25. The technique of making email appear legitimate in order to get a user to open the attachment is known as 'Social Engineering'. CPNI has produced mitigation advice on this subject:

- NISCC Briefing 08a/2006 - Social Engineering against Information Systems: What it is and how do you protect yourself against it? (2006)
<http://www.cpni.gov.uk/docs/SocialEngineering08a06.pdf>

26. Web based attacks are more challenging. Offering generic mitigation advice for users against an attack of this nature is not possible, as there is no reason for the ultimate victim of an attack to suspect the sites they are visiting.

27. CPNI strongly advises all companies to monitor their websites for unauthorised modifications. As the end target of attacks is not the website itself, but the visitors, attacks can be stealthy and not obvious in the manner of more traditional website defacement attacks.

28. Regular content checking will find compromises that intrusion detection systems that sit inline may miss.

EMAIL AND WEB FILTERING

29. Blocking email containing Trojan software is clearly effective mitigation against these type of attacks. Content and virus checkers can be effective; however Trojans are often sufficiently different from more mainstream malware as to be unidentifiable by such tools.

30. CPNI strongly recommends blocking any emails that appear to originate internally, but actually originate externally e.g. for the domain example.com, block any emails from person@example.com that come from the internet. Spoofed emails appearing to originate from someone internal can be used to lend legitimacy to the appearance of Trojan emails.

31. Additionally CPNI recommends blocking the download of any executable file types.

BREAKING COMMAND AND CONTROL CHANNELS

32. Trojan C&C domains are often hard coded into the malware itself. Hence to make contact with the C&C server the Trojan running on a compromised PC will need to make a DNS request for the C&C domain (e.g. bad.domain.com).

33. Attackers establish C&C systems by compromising servers on the internet. These are usually servers owned by third parties who are unaware of a compromise and subsequent misuse of their systems.

34. However, when compromises are uncovered the attackers lose access to that particular C&C server. The use of a hard coded domain in the Trojan enables them to re-establish contact with their Trojans by changing the DNS record for the C&C server to point to some newly compromised system on the Internet.

35. In order to be able to move these C&C servers quickly without losing contact with Trojans, the DNS responses to the Trojan requests have a very short time to live. Hence one characteristic of a Trojan compromise of this nature is very frequent DNS requests for a specific domain.

36. Attackers sometimes 'park' C&C domains by setting the DNS record to 127.0.0.1 or 0.0.0.0. This prevents the Trojan attempting any external connection that may be noticed, and enables them to re-establish contact at a later date if so desired. DNS responses of this sort should be regarded as suspicious and evidence of possible compromise.

37. Black Hole DNS can be used to effectively deny the Trojans access to the C&C domains. Black Hole DNS is an implementation of deliberately false DNS responses. By configuring internal DNS servers to be authoritative for the listed bad domains, it is possible to return a junk result (such as 127.0.0.1) thus preventing the Trojan connecting to the real IP address of the C&C server.

38. A guide to implementing Black Hole DNS can be found at:

- <http://doc.bleedingthreats.net/bin/view/Main/BlackHoleDNS/>

39. CPNI recommends Black Holing whole domains rather than just the fully qualified domain name e.g. if the specific C&C domain is given as my.domain.com, the best course of action is to prevent access to the whole of domain.com, unless there is a business reason for not doing so.

40. This technique also can be used to highlight any internal compromise. Have internal DNS servers return the IP address of a dedicated internal server for all malware domain IP address requests. Any subsequent connections to this server from other PCs on the network are likely to be evidence of a compromise.