



**NISCC Briefing 08/2005
Issued 16 June 2005**

Targeted Trojan Email Attacks

Reference to any specific commercial product, process, or service by trade name, trademark manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this notice shall not be used for advertising or product endorsement purposes.

NISCC shall accept no responsibility for any errors or omissions contained within this briefing notice. In particular, they shall not be liable for any loss or damage whatsoever, arising from or in connection with the usage of information contained within this notice.

**National Infrastructure
Security Co-ordination Centre**
PO Box 832
London, SW1P 1BG

Tel: 0870 487 0748
Fax: 0870 487 0749
Email: enquiries@nisc.gov.uk
Web: www.nisc.gov.uk

Key Points

- **A series of trojanised email attacks are targeting UK Government and companies.**
- **The attackers' aim appears to be covert gathering and transmitting of commercially or economically valuable information.**
- **Trojans are delivered either in email attachments or through links to a website.**
- **The emails employ social engineering, including use of a spoofed sender address and information relevant to the recipient's job or interests to entice them into opening the documents.**
- **Once installed on a user machine, trojans may be used to obtain passwords, scan networks, exfiltrate information and launch further attacks.**
- **Anti-virus software and firewalls do not give complete protection. Trojans can communicate with the attackers using common ports (e.g HTTP, DNS, SSL) and can be modified to avoid anti-virus detection.**
- **This document provides detection and protective advice. There is no complete mitigation for computers connected to the Internet.**

Introduction

1. Parts of the UK's Critical National Infrastructure (CNI)¹ are being targeted by an ongoing series of email-borne electronic attacks. While the majority of the observed attacks have been against central Government, other UK organisations, companies and individuals are also at risk. This briefing seeks to raise awareness of these attacks and provide protective advice.

Attack Description

2. These electronic attacks have been underway for a significant period of time with a recent increase in sophistication. They use unsolicited emails containing either a trojanised² attachment or a link to a website that hosts a trojanised file. When opened, the file installs a trojan onto the user's machine.

3. Unlike "phishing" attacks and email worms, the attackers are specifically targeting governmental and commercial organisations. Although they use similar methods, the attacks are distinct from incidents of industrial espionage recently reported in the press.

4. Accurate attribution for the originators of the attacks is extremely difficult, but IP addresses used for sending emails and controlling trojans, along with email header information, are often linked to the Far-East.

5. Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal. The attacks normally focus on individuals who have jobs working with commercially or economically sensitive data.

6. The emails use social engineering to appear credible, with subject lines often referring to news articles that would be of interest to the recipient. In fact they are 'spoofed', making them appear to originate from trusted contacts, news agencies or Government departments. The attackers make use of distribution lists to target large numbers of recipients with similar interests.

7. Once a trojanised attachment is opened, the remote attacker may use it as a launchpad to gain full control of the user's machine. A compromise poses a threat to the confidentiality, integrity and availability of data stored on the computer and its associated networks. It could also be used to launch attacks against other networks.

8. Files used by the attackers are often publicly available on the Web or have been sent to distribution lists. The attackers are able to receive, trojanise and resend a document within 120 minutes of its release, indicating a high level of sophistication.

¹ The UK's vital computer networks.

² A Trojan Horse ('trojan') is an attack method in which malicious or harmful code is contained inside apparently harmless files.

9. The trojanised files can be common types such as databases, documents, executables (.exe) and help files (.chm) and are often compressed (.zip or .rar). The files exploit known software vulnerabilities to install a trojan on the user's computer.

10. A number of open source³ and bespoke trojans, altered to avoid anti-virus detection, have been used. The wide variety and constant evolution of the trojans used appears to be an attacker strategy to identify the conditions needed to successfully penetrate a network.

11. Once installed, trojans run in the background and can be used to perform functions including:

- collection of usernames and passwords for email accounts;
- collection of system information and scanning of drives;
- uploading of documents and data to a remote computer;
- downloading of further programs (e.g. more sophisticated trojans); and
- relaying of further attacks against other computers and networks.

An infected computer is under the control of the attacker and can be directed to carry out any function normally only available to the system owner.

12. Trojans often communicate back to the attackers using standard application ports (for example TCP port 80, used for web traffic) making it very difficult to detect the data they send and receive amongst legitimate network traffic. Firewalls that allow access to these outbound ports will not block such data.

13. NISCC is working with CERTs worldwide to neutralise IP addresses used to send and control trojans used in these attacks.

Detection Advice

14. Detection is an important step in implementing effective protection against the attacks as it allows appropriate and timely responses to incidents. Implementing the following measures will improve detection of the attacks:

- Implement the methods described in the Current Advice document (<http://www.niscc.gov.uk/niscc/docs/currentAdvice.pdf>), particularly from the sections on Detection (paragraph 5) and Protective Monitoring and Intrusion Detection Systems (IDS).
- Investigate anomalous slow-running machines, looking for unknown processes or unexpected Internet connections, as this may be an indication of malicious programs operating in the background. User reports of such behaviour should be encouraged and fully investigated.

³ Including Nethief, MoFei, GWBoy, Grey Pigeon and Magic Link.

- ☑ Examine firewall logs of critical systems for connections to anomalous IP addresses to assist identification of installed malicious programs.
- ☑ Consider traffic analysis to identify compromised computers that are exfiltrating files. Data on the size and times of HTTP transactions or TCP port 80 flows may help detect exfiltration by highlighting connections where the data volume sent is far greater than that received from the remote server or when data is being sent at times outside of normal working hours.
- ☑ Review mail server access logs for evidence of connections from unusual IP addresses if your infrastructure allows email to be accessed from the Internet. The attackers have shown an interest in collecting email usernames and passwords which may be used to access accounts covertly.

Protective Advice

15. While the attacks cannot be entirely prevented on an Internet-connected machine without having a major impact on email and Web browsing, there are measures that can be taken to mitigate the threat. Focus should be placed on securing computers handling sensitive information in areas such as commercial contracts, R&D, IPR, etc. as these are most likely to be targeted.

General

- ☑ Refer to existing NISCC advice available on the Web:

Configuration and Use of Web Browsers (05/03)

<http://www.niscc.gov.uk/niscc/docs/re-20030801-00725.pdf>

Mitigating Risks to Email Based Trojans (UNIRAS 308/04)

<http://www.niscc.gov.uk/niscc/docs/br-20040618-00343.html>

Mitigating the Risk of Malicious Software

<http://www.niscc.gov.uk/niscc/docs/currentAdvice.pdf>

Spam Mitigation Techniques (02/04)

<http://www.niscc.gov.uk/niscc/docs/re-20040227-00102.pdf>

Understanding Firewalls (10/04)

<http://www.niscc.gov.uk/niscc/docs/re-20041221-00963.pdf>

Anti-Virus

- ☑ Update anti-virus definitions to provide a base level of protection against the attacks. As the attackers are constantly evolving new variants this does not provide complete protection.
- ☑ Anti-virus product names for trojans used in, but not unique to, these attacks are listed in the Annex.

Application Software

- ☑ Implement operating system and software updates to patch the vulnerabilities exploited by these trojans. As Microsoft Office vulnerabilities have been particularly exploited, advice contained in all Microsoft security bulletins should be followed. These can be found at:

Microsoft Security Bulletin Search

<http://www.microsoft.com/technet/security/current.aspx>

Email

- ☑ Educate users not to open attachments from any source unless they have been through anti-virus scanning and the email is consistent with previous communications with the sender.
- ☑ Turn off 'Preview Pane' functionality in email clients and set the default options to view opened emails as plain text.
- ☑ Implement spam filtering to guard against infrastructures commonly used by the attackers. Anti-spam measures such as greylisting/blacklisting of dial-ups, open proxies and open relays, in addition to more sophisticated methods (e.g. Bayesian filtering) can be effective protective measures.
- ☑ Consider implementing draft standards such as Bounce Address Tag Verification (BATV) or Signed Envelope Sender (SES) to protect the availability of mail servers against large quantities of bounced emails spoofed to appear from your domain ('backscatter'). Log files should be analysed to determine whether the attackers are spoofing your domain.

Network Traffic

- Consider implementing IP address whitelisting of outbound Internet connections, denying access except from address ranges relevant to your business activities. Such a “default deny” policy provides some protection against computers in third countries being used by attackers to control trojans.

Web Browsing

- Consider disabling Internet Explorer Browser Helper Objects⁴ (BHOs) as these have been used to install trojans. Microsoft have published instructions on how to disable BHOs at:

<http://support.microsoft.com/default.aspx?id=kb;en-us;Q298931>.

It should be noted, however, that the relevant registry setting could be changed by malicious code prior to installing the BHO.

⁴ A Browser Helper Object, or BHO, is a plug-in program for Microsoft Internet Explorer (IE) which extends its functionality. A BHO may be able to gain full control of the computer it is installed on.

Annex

The following anti-virus product names are associated with trojans used in the attacks since January 2005.

Vendor	Signature Name
Computer Associates	CHM/Fantador.J!Dropper
	W97M/1Table!Exploit!Trojan
	Win32.Multidropper.D
	Win32/Passpro.A!Trojan
F-Prot	W32/Downloader.BSG
	W32/Lecna.A@bd
	W32/Nethiev.M
	W32/Sysgam.A
	W32/Sysgam.B
Kaspersky	Backdoor.Win32.Agent.bx
	Backdoor.Win32.Lecna.c
	Backdoor.Win32.Nethief
	Backdoor.Win32.Nethief.g
	Backdoor.Win32.Nethief.k
	Downloader.Win32.Agent.kz
	Trojan.Win32.Agent.cu
	Trojan.Win32.Pusno.a
	Trojan.Win32.Riler.f
	Trojan.Win32.Riler.j
	Trojan.Win32.Zapchast
	Trojan-Download.Win32.Agent
	Trojan-Dropper.MSWord.1Table.a
	Trojan-Dropper.MSWord.1Table.b
	Trojan-Dropper.MSWord.Lafool.d
	Trojan-Dropper.Win32.MultiJoiner.13.b
	Trojan-Spy.Win32.Agent.m
McAfee	Backdoor-BCB
	Backdoor-BCB
	BackDoor-CPY!chm
	Backdoor-TW
	Downloader-WY
	Downloader-WY
	Exploit-1Table
	JS/BackDoor-CPY
	MultiDropper-MR
	Proxy-Sysgam
	Pusno

Vendor	Signature Name	
	StartPage-DH.dll	
NOD32	W97M.Lafool.D	
	Win32/Agent.CU	
	Win32/Riler.E	
	Win32/TrojanDropper.Mudrop.Q	
Norman	W32/MEWpacked.gen	
	W32/Smalldrp.WN	
Panda	Trj/Multidropper.QM	
Sophos	Troj/Agent-BX	
	Troj/Agent-T	
	Troj/DDrop-A	
	Troj/Dloader-KF	
	Troj/Dloader-KZ	
	Troj/Lecna-C	
	Troj/Nethief-M	
	Troj/Nethief-N	
	Troj/Nethief-O	
	Troj/Netter-A	
	Troj/Riler-E	
	Troj/Riler-F	
	Troj/Riler-J	
	Troj/RPE-A	
	Troj/Sharp-F	
	Troj/VBDrop-A	
	WM97/Loof-D	
	Trojan.Dropper	
	Symantec	Trojan.Mdropper.B
		Trojan.Riler.C
BKDR_NETHIEF.L		
Trend	BKDR_NETHIEF.R	
	BKDR_NETHIEF.S	
	BKDR_TUIMER.A	
	TROJ_AGENT.KZ	
	TROJ_SHARP.C	
	TROJ_WINBLUE.A	
	W2KM_PASSPRO.A	
	W2KM_PASSPRO.C	
	W2KM_PASSPRO.E	
	W2KM_PASSPRO.E	