

## Recent attack targets 50 Financial Institutions

Jamie McNeil & Dimitrios Petropoulos  
ENCODE Security Labs  
3, Romanou Melodou Street  
Athens - 15125 - Greece  
[j.mcneil,d.petropoulos}@encode-sec.com](mailto:{j.mcneil,d.petropoulos}@encode-sec.com)

### Background

---



In an attempt to target the clients of financial institutions, unknown attackers have compromised various Microsoft Web servers using a known vulnerability (Microsoft Patch 835732) and added code to the web servers to attack anyone browsing the web server with Internet Explorer. The exploit code uses both a known vulnerability in Internet Explorer (addressed by Microsoft Security Bulletin MS04-013) and, at the time, a previously unpatched vulnerability although Microsoft has now released a patch (KB870669).

### Technical Overview

---

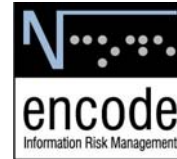
Although the first stage of this attack targets and compromises Microsoft IIS web servers, this attack has actually affected **other secure web servers** (running Apache for example) as these secure servers referenced content (e.g. adverts) from these compromised Microsoft web servers.

The exploit code on the compromised web servers downloads trojan code to the client browsing that website and the trojan is being referred to as Download.Ject, JS.Scob.Trojan, Scob, and JS.Toofeer by the various Anti Virus Vendors. The downloaded trojan is saved on the client in a file named "img1big.gif" which is not a GIF image but, in fact, some code to install a randomly named Windows dynamic library (DLL) into the Windows system directory. This DLL contains a "Browser Helper Object" (BHO) for Internet Explorer.

A BHO is a DLL that allows developers to extend and control the functionality of Internet Explorer. This particular BHO trojan looks for HTTPS connections to various financial institutions and when such a connection is noticed all HTTP GET and POST requests sent by the client are captured by the trojan. Note that the captured requests are obtained before they are sent over SSL so all banking credentials are obtained by the trojan. The trojan then sends the captured details to [www.refestldt.com](http://www.refestldt.com) over an HTTP connection although this server was unavailable as of writing at 10:00 am GMT 1<sup>st</sup> July 2004.

Since this trojan is not installing a simple key logger but is integrating itself into Internet Explorer it is possible for it to obtain access to all banking credentials for a client not just usernames and passwords. For example, in order to authenticate a user many financial institutions require a user to select information from a drop down menu or click on a number pad to enter secret information but even these types of credentials will be obtained by the trojan.





## Mitigation Steps

---

In order to protect against this particular attack:

1. All System Administrators should check that any offsite content that is served through their web server is safe - this includes content served by adverts and partner sites.
2. Microsoft System Administrators should:
  - Ensure web servers are fully patched.
  - Check and, if necessary, remove any infections.See <http://support.microsoft.com/?kbid=871277> for more details.
3. Banking Clients (including home and enterprise users)
  - Ensure Internet Explorer is fully patched including the recent KB870669 patch which is available on Windows Update or at the following URL:  
<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=4d056748-c538-46f6-b7c8-2fbfd0d237e3>
  - Increase Internet Explorer and Email security settings (see <http://www.microsoft.com/security/incident/settings.mspx> for more details)
  - Check, and if necessary, remove any infection. Most Anti-Virus vendors now have signatures for this trojan.

Unfortunately, recently there have been a number of security vulnerabilities in Internet Explorer published on various mailing lists that remain unpatched by Microsoft. In fact, the problem is so serious that the US CERT has taken the unprecedented step of recommending users not use Internet Explorer as their web browser (<http://www.kb.cert.org/vuls/id/713878>).

Useful URLs:

[http://isc.sans.org/presentations/banking\\_malware.pdf](http://isc.sans.org/presentations/banking_malware.pdf)

[http://www.microsoft.com/security/incident/download\\_ject.mspx](http://www.microsoft.com/security/incident/download_ject.mspx)

## Contact Details

---

For any additional information regarding this advisory please contact:

ENCODE Security Labs

Tel. : +30 210 6178410

Email : [d.petropoulos@encode-sec.com](mailto:d.petropoulos@encode-sec.com) or [j.mcneil@encode-sec.com](mailto:j.mcneil@encode-sec.com)

ENCODE is helping companies realise the full potential of the new interconnected economy, by providing services that enable trustworthy e-business. In this new era of technology, the e-business model is creating opportunities for exceptional growth through increased globalisation, reduced cycle time, greater speed to market and enhanced cost-competitiveness. However, the e-business transformation is not free of risk. New technologies are being deployed, business processes are being reengineered and networks are being opened in order for corporate assets to become available to external business parties. Anticipating, understanding and managing the impact and associated risks of e-business are the only means for companies to build competitive advantage and secure their growth.

ENCODE's mission is to assist clients identify relative risk and opportunities, develop a secure environment, from strategy to specialised technology, and sustain the efficiency of this environment.

[www.encode-sec.com](http://www.encode-sec.com)