

Haxdoor

Anatomy of an ID Theft Attack Using Malware

12 December 2006

Summary

AusCERT assesses that ID theft trojan malware poses a high threat to users of e-government and e-commerce services.¹ To illustrate the rapidly developing nature of this threat, this paper describes the features and impact of a series of ID theft trojan attacks that were directed against Australian Internet users between March and August 2006.

The attacks described in this paper are assessed to be typical of online ID theft attacks using malware that are commonly directed at Australian Internet users. The attacks use variants of the Haxdoor trojan, which is the main piece of malware responsible for the theft of identity related information. These attacks are typical in their ability to compromise thousands of computers, capture sensitive information from the thousands of users of these computers, disable and bypass the computers' security and remain hidden on the compromised computers.

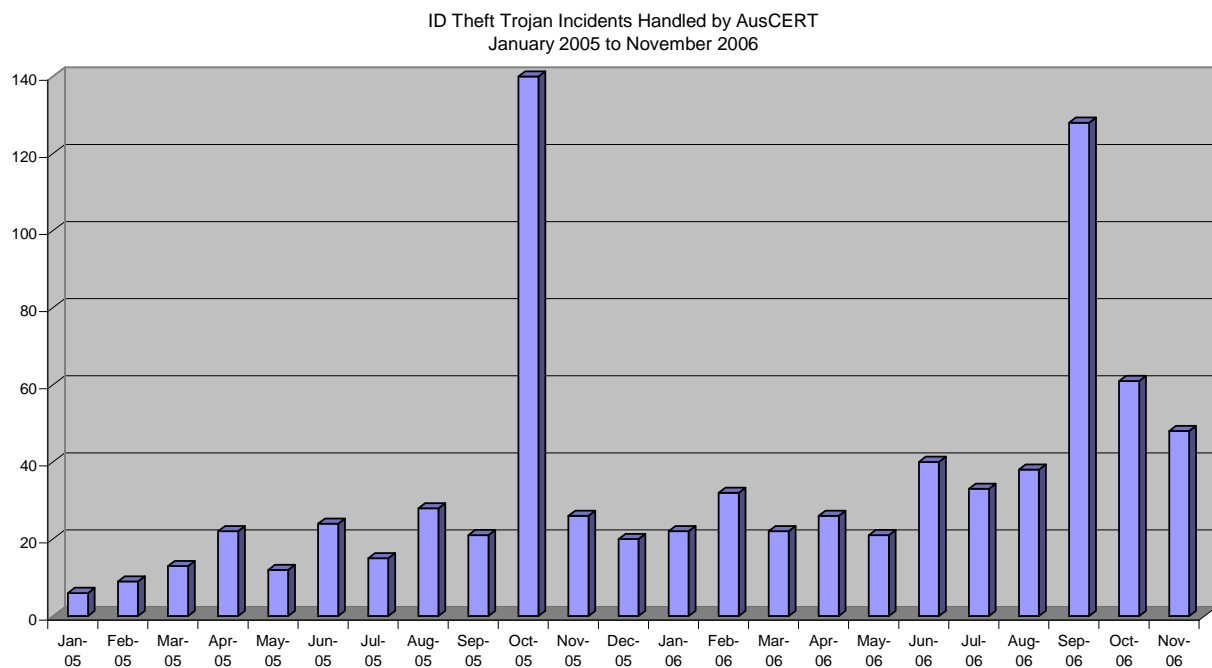
The attacks described in this paper all used a common logging site and therefore, are assessed to have been conducted by a single attacker or group of attackers. While

¹ For further information, please refer to previous assessments on this topic available from www.auscert.org.au, including:

- AusCERT (2005), Managing Risk Associated with Online ID Theft for Government and Providers of e-Government Services
- AusCERT (2005), Trends and Developments in Online ID Theft – Update No. 2
- AusCERT (2004), Trends and Developments in Online ID Theft, No. 1
- AusCERT, Australian High Tech Crime Centre, AFP, NSW Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police, 2006 Australian Computer Crime and Security Survey, page 24 - 28

AusCERT frequently sees evidence that attacks are related to other attacks,² it is unusual for attackers to log multiple attacks to a single site, especially over an extended period of time.

Please note that the attacks described in this paper do not represent the total number of ID theft trojan attacks directed at Australian Internet users during this period. Rather they are illustrative of what one group of attackers has achieved within a five month period. The graph below shows the volume of ID theft trojan incidents currently targeting or otherwise affecting Australian Internet users.



Each incident in the graph represents a single unique URL or domain name that is hosted by one or more hosts in a distributed approach to stealing sensitive information and access credentials from computers. The number of distributed IPs associated in a single attack is variable but can range from one to around 100. This does not depict the number of computer infections associated with each attack of which there are generally many hundreds or thousands.

² For example, the use of common domain name servers, domain name registrars, ISPs, file and domain structure formats, choice of attack tools, etc. across multiple attacks over time are indicative that such attacks are likely to have been conducted by the same group of attackers, for all or parts of the attack.

Lifeisfine case study

Introduction

Lifeisfine.org is the domain registered by an attacker or attackers which was used to log captured data from users' computers infected with a number of Haxdoor trojan variants.

AusCERT became aware of the logging site and received log data from 15 June 2006. The logs showed a series of attacks had occurred since 1 March 2006. For the purposes of this case study the method used to conduct one of the attacks and its impact will be examined along with the broader impact of the series of attacks orchestrated by this single attacker or group of attackers.

The typical approach to conducting an online ID theft attack using malware involves a number of components. The case study described in this paper is typical of many attacks observed by AusCERT, except that it is unusual to reuse a logging site for multiple attacks. Typically, each separate attack will have its own logging site or email address.

Timeline for attacks

Information analysed from the captured log files³ shows compromised data was captured from 1 March 2006 until 9 August 2006, when the lifeisfine.org domain was disabled and removed from control of the attacker. Therefore, the attacks described in this case study occurred during this period, or shortly before the date of the first captured log information on 1 March 2006.

Attack vectors

The attack vector is the method an attacker uses to initiate the attack. Spam email is typically used as the attack vector, as it was in this case. However, it is known that the attacker also embedded links to malicious sites in forum posts. This is an approach that is not commonly used.

AusCERT became aware of the existence of the www.lifeisfine.org logging site after AusCERT began receiving spam email on 15 June 2006 with the hook:⁴

Subject: National Bank goes bankrupt?!

People starting panic withdrawals, some of the accounts were reported closed due to technical reasons, many ATMs are not operating. Does it seem that one of the Australia's greatest goes bankrupt?

³ The log file is the repository of the data captured from the thousands of computers infected with the Haxdoor trojan.

⁴ The 'hook' refers to the message in the spam email or forum post which is used to entice a user to click on the URL to the malicious site.

The full story could be found here: <http://www.compromised-domainA.com/news.php>⁵

Well, hope that isn't true... Anyway You'd rather check your balance...

The spam emails used URL links to entice users to visit the malicious web sites necessary to compromise users' computers. The emails included one of the following links:

Spammed web link	Date sent
http://www.compromised-domainB.net/news.php	14 June 2006
http://www.compromised-domainA.com/news.php (as shown above)	15 June 2006

On 15 June 2006, AusCERT received a report that the same message was posted to at least 41 different forums in Australia; 38 of which were forums within the .au country code domain between 11 and 12 June 2006. The forum posts included the following link:

Spammed web link	Date sent
http://www.compromised-domainC.com.au/national.php	12 June 2006

The forum posts used the identical message content, but used a different compromised domain name (and URL) link and were sent a few days prior to the spam email. When a user connected to this link, they were redirected to another site:

<http://www.compromised-domainD.net/demo.php>

which in turn was redirected to :

www.compromised-domainE.com/cgi-bin/rleadadmin.cgi

This is the same domain used in the aforementioned spam email attack (see page 7). Therefore, the attackers have used multiple attack vectors which ultimately were directed to a single domain which served the Haxdoor trojan and logged captured user information.

Attack process

Depending on which infection vector a user responded to, the infection process would vary.⁶ In the case of the spam sample shown below, the infection process occurred as

⁵ Where legitimate domains have been used by compromising the web sites for those domains, AusCERT has obfuscated the domain name. However, the top level domain name (TLD) and country code TLD (ccTLD), if present, and URL directory extension remain unchanged.

shown in the diagram (page 7). However, a user may have become infected by clicking on a URL web link in one of the 41 known forum posts that were also used as the initial attack vector.

1. **Distribution:** spam email with URL link sent to user
2. **User hooked:** user clicks on the web link: www.compromised-domainA.com/news.php (attacker domain 1, URL 1)
 - attacker domain 1 contains obfuscated JavaScript to hide the functionality of the site to casual observers.
3. **Victim profiling:** the user's machine connects to the URL link (attacker domain 1, URL 1). This URL contains a commercial malware kit known as WebAttacker,⁷ which profiles the operating system, service pack and web browser of a visitor to determine which exploit may be most effective at delivering malware.
 - Presumably, if a non vulnerable operating system and browser is detected, no further action occurs and the connection ends.
 - If a vulnerable operating system (in this case Microsoft Windows) and browser is detected then the user's computer is immediately redirected to another page (attacker domain 1, URL 2) within the same domain (www.compromised-domainA.com/cgi-bin/ie0606.cgi?homepage)
4. **Redirection:** the user's machine connects to the new URL link (attacker domain 1, URL 2)
 - With knowledge of the user's software, the redirection URL incorporates a parameter which links to an exploit suited to compromising that particular type of browser and Microsoft operating system version. In this case, the malicious site delivered exploits for Microsoft (MS03-11, MS06-014, MS06-006) and Mozilla vulnerabilities (MFSA2005-50). The purpose of this step is to compromise and gain control over the user machine so that further malware necessary for the attack may be installed.
5. **Second redirection:** The compromised user computer is then redirected to another page (attacker domain 1, URL 3) within the same domain (www.compromised-domainA.com/demo.php). This page contains a version of the WebAttacker. From this page, a trojan dropper⁸ is downloaded onto the user's machine.
6. **Dropper installation:** Once installed the trojan dropper is programmed to connect to another URL (www.compromised-domainE.com/cgi-bin/rleadadmin.cgi) (attacker domain 2)

⁶ There was one of at least three different URL links embedded in the spam email and forum posts and each link involved a different set of domains and compromised hosts. However, all were ultimately directed to www.compromised-domainE.com/cgi-bin/rleadadmin.cgi and logged back to lifeisfine.org.

⁷ For further information on WebAttacker, see page 10.

⁸ A dropper is a piece of malware that facilitates the subsequent, generally more harmful, installation of malware on a compromised computer.

7. **Payload installation:** The connection occurs and then the main trojan, Haxdoor, is downloaded and installed on the user's machine.
8. **Payload anti-security measures:** The trojan disables various security counter-measures and when the user visits particular web sites, including those using SSL⁹ connections, it commences capturing passwords and web form data.¹⁰
9. **Data captured:** The capture data is sent to lifeisfine.org (attacker domain 3) where the attacker harvests the data on a periodic basis.

Compromised domains versus fraudulent domains

In the 'national bank bankrupt' hook example, the attacker used five compromised legitimate domains to host and/or redirect parts of the attack and one specially registered fraudulent domain, lifeisfine.org.

⁹ Secure Socket Layer web based sessions are those which are identified by the use of the https protocol within the browser address bar and the presence of a digital certificate which provides some level of assurance of the identity of the remote host to which the client computer is connected.

¹⁰ Web form data is the type of data that can be inserted into web forms and submitted or accessed via the web. Web forms are designed to collect or provide access to user-specific information over the web. Generally they contain user input mechanisms such as drop down boxes, radio buttons, text boxes, etc which require users to input username and password, or names and addresses; or other user-specific information. Web forms are also used to display user specific information in a structured manner after user authentication is complete. For example, web forms are often used to display summary transaction information, invoices for e-commerce transactions, etc.

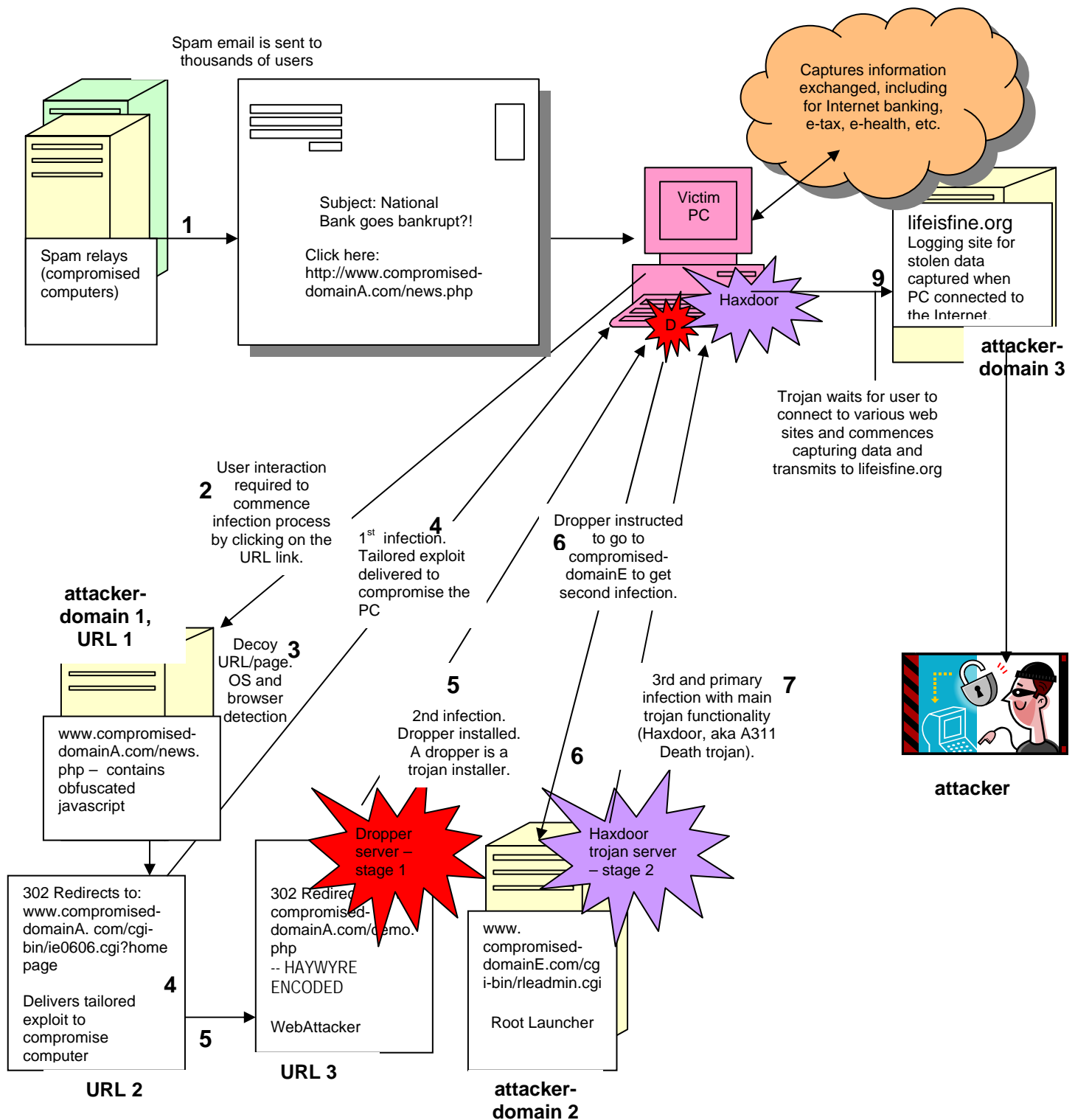


Figure 1. Online ID Theft Attack System

Log analysis

Log format

The following is a typical format of the data fields captured by the trojans on the lifeisfine.org site.

```
[captured form data]
[Web browser title bar]
[Referring URL]
[-- URL --]
[Captured web page or application output]
\0
[unique ID]
[ID:[run ID] IP:[IP address] [Date] [Time]]
```

The unique ID is assessed to uniquely identify each computer compromised by the trojan. The run ID is assessed to refer to the particular variant and associated attack vector used to infect the computer. “Unique ID” and “run ID” are descriptors given by AusCERT. The unique ID is a non-sequential pseudo-random number ranging from 14 – 19 digits in length.

An analysis of the logs during this period showed there were:

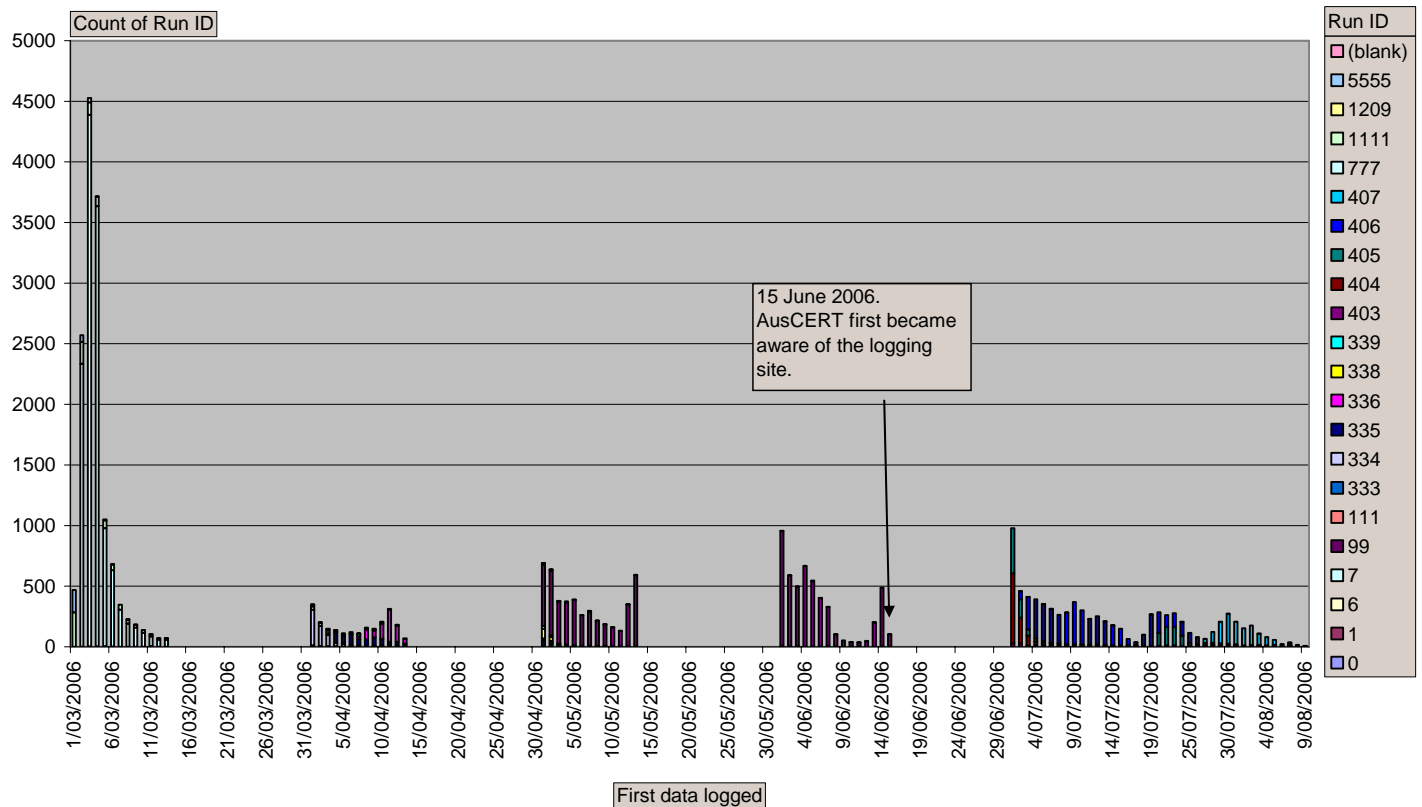
- 34,553 computers infected
- 149 countries with infected computers
- 11,449 infected computers within Australia, with 33% of total infections
- Countries with the highest number of infections overall were:

Australia	11,449	33%
Germany	4,889	14%
United States	3,605	10%
Poland	2,459	7%
New Zealand	1,976	6%
Spain	1,071	3%
Turkey	777	2%
France	749	2%
Brazil	678	2%
United Kingdom	519	2%

Note that by the time AusCERT became aware of the logging site’s existence, the attacker had removed logging files on a periodic basis for parts of March, April, May and June 2006. Therefore, the figures provided here are from a subset (probably just over half) of the logs and do not fully reflect the complete scale or impact of these attacks.

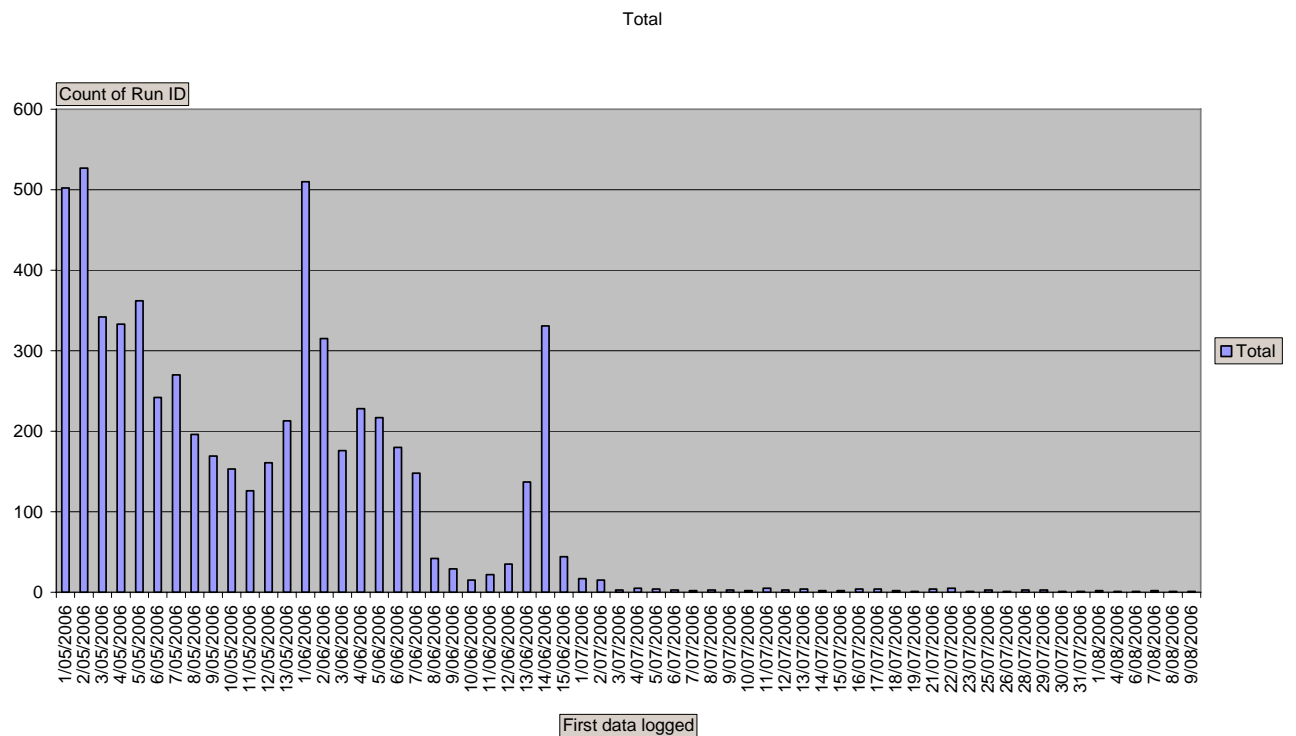
The diagram below shows the gaps in data captured each month. For March from 14 – 31 March 2006, inclusive a period of 18 days no data was present. For April from 14 – 30 April, inclusive a period of 17 days no data was present. For May from 14 – 31 May 2006, inclusive a period of 18 days no data was present. For June from 16 – 30 June

2006, inclusive for a period of 15 days, no data was present. The distinct pattern of gaps indicates the attacker used an automated and/or regular approach to removing captured data from the logging site. AusCERT was able to gain access to all the log data for July and the remainder of August prior to the site being shut down.

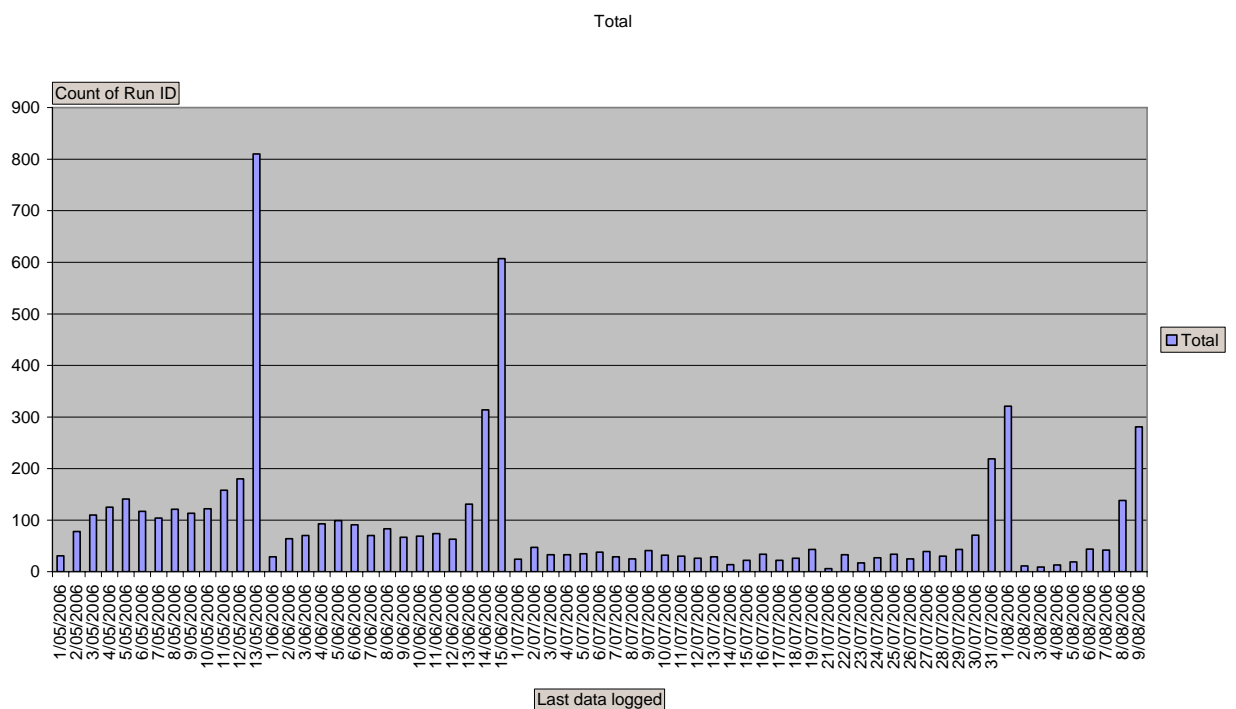


It is assessed that runID 0403, as shown in the graphs below, was the run that was associated with the ‘national bank bankrupt’ hook spam and forum based posts that began circulating on 12 June 2006. However, run 403 first commenced logging from May 2006 so it is assessed these were not the only vectors associated with this particular run.

Run ID 403 Country Australia



Run ID 403 Country Australia



These graphs depict the first and last known infection dates, respectively, for Haxdoor infections on computers located within Australia with runID 403. Without mitigation intervention, most compromised computers are likely to continue to remain

INTERNAL USE ONLY – NOT FOR FURTHER DISTRIBUTION WITHOUT PERMISSION FROM AUSCERT

Enquiries: auscert@auscert.org.au

compromised and be used for criminal purposes beyond 9 August 2006, the last recorded capture date. Only the attacker's ability to log captured sensitive data to lifeisfine.org has ceased with the deactivation of this domain.

Run Sequence and Range

Analysis of the log data shows there were 15 separate runs. The very low infection levels of some of the runs suggest they were test runs, to see if the attack was working.

The table below shows the chronological sequence of the runs; the duration of infections from each run and the countries which had most infections and the number of infections. The sequence of the runs is based on the first known log date of an infected computer from the run, which may coincide with or follow the actual date the run occurred.

The data shows that Australia was frequently targeted and that in many runs, Australia was among the countries with the highest number of compromised computers.

The run ID, like the unique ID, is generated by the Haxdoor trojan. Each run potentially represents a configurable variation of the malware and is probably used by the attacker to distinguish and then compare and contrast different attack vectors, spam distribution lists, content hooks or other features of the attack, which are particular to each run. Such information would enable the attacker to refine subsequent attacks based on an analysis of the effectiveness of particular attack features and techniques used.

RunID	First known start date	Last known end date	Longest duration of infection for a single computer (in days) *	Number of logged infections	Countries with most infections	Percentage of infections in these countries
1111	1 March 2006	9 August 2006	161	1,041	USA Poland	51% 5%
5555	1 March 2006	9 August 2006	161	318	USA Poland Canada	49% 16% 7%
777	2 March 2006	9 August 2006	159	13,214	Poland United States Turkey	18% 14% 6%
6	3 March 2006	13 April 2006	38	5	Cyprus Ukraine	83% 17%
7	3 March 2006	5 March 2006	< 1	2	Ukraine	100%
1	11 March 2006	11 March 2006	< 1	4	Ukraine	100%
334	1 April 2006	31 July 2006	130	684	Australia Brazil USA UK	50% 14% 12% 3%
333	1 April 2006	31 July 2006	129	28	Spain USA	36% 32%

RunID	First known start date	Last known end date	Longest duration of infection for a single computer (in days) *	Number of logged infections	Countries with most infections	Percentage of infections in these countries
1209	1 April 2006	6 April 2006	5	1	Argentina	100%
0	2 April 2006	31 July 2006	127	4	Australia	75%
					Italy	25%
335	3 April 2006	31 July 2006	127	695	Australia	50%
					USA	14%
					Brazil	11%
					UK	2%
336	7 April 2006	31 July 2006	123	781	Australia	96%
111	7 April 2006	8 April 2006	< 1	2	Ukraine	100%
338	12 April 2006	9 August 2006	100	146	Australia	60%
					UK	30%
					USA	7%
403	1 May 2006	9 August 2006	100	9,449	Australia	65%
					Germany	24%
					USA	8%
339	1 May 2006	7 August 2006	97	50	Australia	98%
					NZ	2%
99	7 June 2006	7 June 2006	< 1	1	Ukraine	100%
404	1 July 2006	9 August 2006	39	1,074	Australia	66%
					Germany	31%
405	1 July 2006	9 August 2006	39	1,289	Germany	66%
					Australia	30%
406	2 July 2006	9 August 2006	37	4,469	Australia	48%
					NZ	32%
					Germany	14%
407	27 July 2006	9 August 2006	12	1,293	NZ	33%
					Australia	27%
					Spain	26%
					Germany	12%

* Please note that infection period may have been longer than this. This is the confirmed longest infection period for one of the compromised computers based on captured log data from that computer.

Compromised user profile

With over 34,000 computers infected between 1 March and 9 August 2006, the attackers can potentially harvest information about at least the same number of users and potentially many more since many of the computers will be used by more than one individual.

Appendix A provides two examples of the type of personal information that can be gleaned from just two compromised computer in Australia. The impact of each computer compromise will vary depending on the nature of the web sites visited by the users of the computer, the volume and type of transactions conducted and the number of passwords stored within each computer or provided over the Internet. In both cases, personal information from more than one person was stolen.

Attack tools and malware functionality

As is typical of this type of attack, the attacker used a suite of malware attack tools. The main malware components were:

- WebAttacker
- Root Launcher
- Haxdoor, also known as the A311 Death trojan

All three malware components are available on a commercial basis from Russian language web sites. WebAttacker and RootLauncher are available from inet-lux.com and Haxdoor (sold as A311 Death) is available from corpsespyware.net.

WebAttacker

The compromised-domainA.com site hosted a version of WebAttacker (version ie0606) in this attack.

The WebAttacker is an attack tool, which contains exploit code (malware) designed to detect, then exploit, specific software vulnerabilities in the computers which connect to the web page where WebAttacker is hosted. This tool has frequently been used in attacks of this kind since c. 2005. Given its commercial availability, its use is not necessarily restricted to any group or individual. The attacker requires no knowledge of coding to deploy the tool.

The WebAttacker Control Panel (WACP) is a password protected graphical user interface (GUI) through which the attacker can view statistics on the number of computers that have made connections to the site and have become infected using the WebAttacker tool. It records in a table format the following information:

- Operating system type and version of computer which made connection to the WebAttacker URL/page
- Browser type and version
- Name of the vulnerability detected and exploited on the computer
- Number and percentage of infections arising from each vulnerability and associated exploit

This version of the WebAttacker (version ie0606) detected and exploited the following operating system and application vulnerabilities, including in the browsers, Internet Explorer and Firefox:

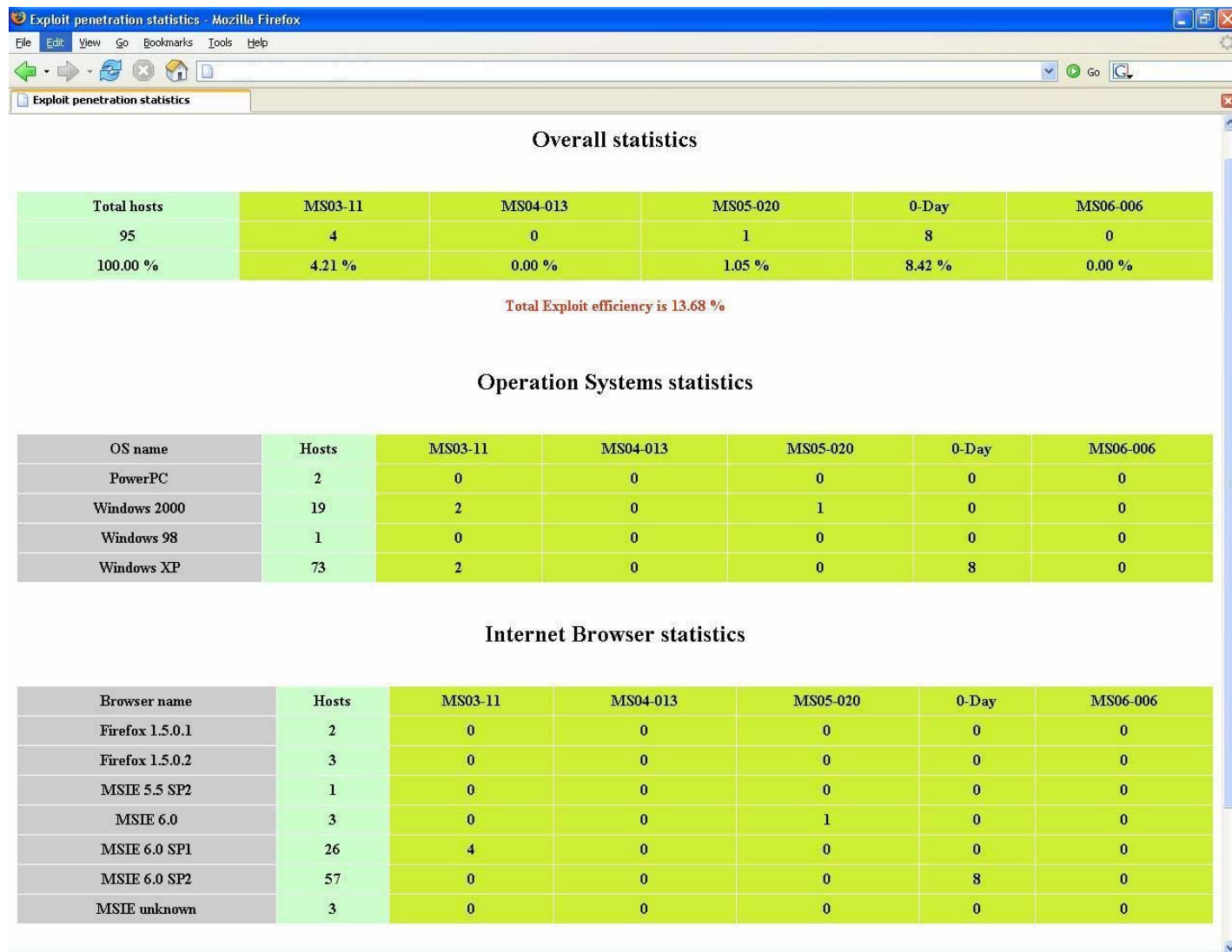
- MS03-011¹¹
- Mozilla Firefox Security Advisory (FMSA) 2005-050¹²
- MS06-006¹³
- MS06-014¹⁴

¹¹ <http://www.microsoft.com/technet/security/bulletin/MS03-011.msp>

¹² <http://www.mozilla.org/security/announce/2005/mfsa2005-50.html>

¹³ <http://www.microsoft.com/technet/security/bulletin/MS06-006.msp>

The following screen shot shows some of the statistics that can be generated by the WACP. The output is not related to the attacks identified in this case study. Also it depicts the use of a previous version (ie0604) of WebAttacker.



The version ie0604¹⁵ used a combination of old and new exploits compared to ie0606:

- MS03-011
- MS04-013
- MS05-020
- 0-day (MS06-013)
- MS06-006

¹⁴ <http://www.microsoft.com/technet/security/Bulletin/MS06-014.msp>

¹⁵ AusCERT has noted variations within specific versions. For example another attack that used the WACP version ie0604 used seven exploits, compared to only five in the example above.

Note the use of an unspecified 0-day exploit, which in this case was the 'CreateTextRange' vulnerability, subsequently patched by Microsoft in update MS06-013.¹⁶

Though not evident from the screenshot above, it is also possible to configure the WebAttacker to conduct a geographical look up of the connected computer's IP address to identify and record its location by country. This feature is particularly useful for subsequent sale of captured data or extraction of funds from financial institutions and for subsequent more focused targeting of users and their computers.

Root Launcher

The compromised-domainE.com site hosted a version of Root Launcher in this attack. In this attack, "Root Launcher" was used to install the main trojan binary, Haxdoor. Root Launcher is designed to download a malicious payload, in this case, Haxdoor, to computers which supply a specified 'user agent'.¹⁷ This is assessed to be an anti-analysis technique designed to hinder access to the trojan payload to only legitimately compromised computers as identified by specific user agents. Security professionals seeking to access and analyse the trojan may attempt to do so with non-vulnerable computers which will produce a different user agent string.

Haxdoor

The Haxdoor trojan is also known as the A311 Death trojan which was developed by 'corpse', a Russian programmer, who sells two versions for \$US250 and \$US450 respectively for others to deploy.

The main functionality of the trojan, which works on Windows operating systems, is to provide remote administration access to the compromised machine, keylogging, web form and password grabbing. The malware is feature rich, consisting of a configuration tool allowing attackers without programming skills to configure custom versions of the trojan with an easy to use interface.

For example, the attacker can specify a runID to be recorded by the trojan; the logging site or an email address to post captured data; specify particular key words to activate both keylogging and form data capture, or other modifications to ensure a high chance the created variant will be undetectable to commonly used AV products. For example, changing the way malware is compressed and packed is often sufficient to alter the file's signature if examined by anti-virus products.

The malware can be controlled from a graphical user interface (GUI), reminiscent of the Sub-Seven trojan,¹⁸ and includes the following functionality, inter alia:^{19 20 21}

¹⁶ <http://www.microsoft.com/technet/security/Bulletin/MS06-013.mspx>

¹⁷ In this context, a user agent usually identifies the type and version of the application used to connect to the remote web site, typically a browser. When a connection is made with a web site, a text string is generally sent to identify the user agent to the server. This forms part of the HTTP request, prefixed with "User-agent:" and typically includes information such as the application name, version, host operating system, and language.

¹⁸ <http://www.f-secure.com/v-descs/subseven.shtml>

¹⁹ <http://www.f-secure.com/v-descs/haxdoor.shtml>, http://www.f-secure.com/v-descs/haxdoor_m.shtml

- Contains a rootkit^{22 23} and therefore is capable of hiding files, registry keys, processes and listening or open TCP ports.
- Dumps passwords from protected storage and logs keystrokes to capture additional passwords which haven't been saved on the infected system. Attackers can capture VPN passwords as well as passwords for any web based login.
- Allows the system to be used as a proxy. Therefore, once an attacker has captured useful personal information from the infected computer, the compromised computer (bot) can then be reused in other attacks for other purposes, eg, to distribute spam, scan for vulnerabilities in other Internet connected PCs, or log on to financial accounts from the same geographical location as the account holder, participate in DDOS attacks, etc.²⁴
- Terminates firewalls and anti-virus processes. The latter is achieved by preventing their ability to do automatic updates.
- Captures data and sends it to a web site or to an email address.
- Provides complete control over the file system to copy, rename, remove or add data or system files, including the ability to upload or download additional files from the Internet with breaks in connection.
- Control various aspects of the compromised machine (CD-ROM, monitor, shutdown/ restart etc).
- View current network connections
- HTML injection. The trojan can be configured to inject HTML code into the browser interface when a user connects to a particular site to enable the attacker to capture additional sensitive data through form data input. The technique means that checking the digital certificate and URL no longer provides assurance that the user has accurately verified the identity and integrity of the remote site as it *appears* to the user. This feature is only available in the newer versions.

Haxdoor was responsible for capturing and posting captured information to lifeisfine.org. An examination of the log files from lifeisfine indicates that multiple trojan variants were likely to have been used and configured by the attacker. It is assessed that multiple variants were released with the same runID, based on the fact that some runs 'peaked' on more than one occasion over several months and that the effective life span of any one variant is generally no greater than 48 hours from the time the variant is discovered, submitted to AV vendors, signatures developed and downloaded to AV products. The effective life span refers to the malware's ability to

²⁰ http://www.symantec.com/security_response/writeup.jsp?docid=2006-061510-5124-99&tabid=2

²¹ <http://www.sophos.com/security/analyses/trojhxdoorhm.html>

²² <http://www.f-secure.com/weblog/archives/archive-022006.html#00000821>

²³ For more information on rootkits, refer to AusCERT's paper, Windows Rootkit Prevention and Detection, <https://www.auscert.org.au/5093>

²⁴ A third version of the A311 Death trojan sells for \$US3,250 and includes DDOS attack functionality.

infect new computers, not its actual life span, ie, how long it can remain active and undetected on a computer that has been compromised by the malware.

Specific targeting of the trojan

The trojan has a very broad targeting range. It includes search strings which target specific organisations and key words can be configured for logging. However, given its form-grabber, password grabber and keylogging functionality, inter alia, there is almost nothing it cannot capture on the host computer, if configured to do so. Given the nature of the files captured in these logs, it appears these versions were configured to capture all web form data for and from login sessions and passwords.

The fact that these variants captured data predominantly from Australian-based Internet users is likely to be a function of the composition of the spam run and forum posts, rather than the configuration of Haxdoor per se.

Detection and Removal by Anti-Virus Products

On 15 June 2006, the main executable (Haxdoor, aka A311 Death) which was being distributed from compromised-domainE.com was tested on 26 different anti-virus products and in four cases detected as trojan malware. In a further three cases it was identified as a suspicious file. Therefore, only seven out of 26 products detected this malware and 73% of the products did not detect it at all.

The trojan disables resident anti-virus software installed; therefore, it is highly unlikely the trojan will be subsequently detected when AV vendors update their signatures. This is due to the ability of the trojan to stop an infected host from updating signatures in the first instance and to the use of rootkit functionality that hides the presence of critical trojan files, preventing detection in the event that the anti-virus software is successfully subsequently updated.

AusCERT, as part of its incident response process, immediately supplied anti-virus vendors with the malware samples on 15 June to enable them to update their signatures.

Removal

Some AV vendors have provided removal instructions and/or removal tools for this trojan;^{25 26} however, due to the presence of the rootkit, AusCERT regards compromises of this nature require the format of the hard drive and subsequent reinstall of the operating system from trusted media (operating system and application software) followed by replacement of data files. In AusCERT's experience, some rootkit removal tools resulted in the crash of the operating system.

²⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2006-061510-5124-99&tabid=2

²⁶ http://www.zdnet.com.au/news/security/soa/Security_firms_develop_anti_rootkit_tools/0,130061744,139267346,00.htm

Attack impact

In analysing the information the Haxdoor trojans logged to lifeisfine.org, Australian Internet users were the primary target of attacks overall with at least 33% of total infections recorded.

It is assessed that the actual scale of the attacks, in terms of the number of compromised computers and captured data was significantly larger (almost double) than is reported here as log files for nearly half the period were missing.

The huge volume of text (over 6 GB) captured by the trojan between March and August 2006 requires the attackers to be highly methodical in isolating the data of potential use to them for further criminal purposes, even if they are only potentially harvesting a portion of the data captured. The attackers in this case require data mining tools/capabilities. There is now a Russian language log parser available for efficiently processing Haxdoor log data. While the verbose and indiscriminate data capture capabilities of this trojan may seem inefficient due to the need to further process and analyse the captured data, it is possible that the attackers have used this approach as a form of broad based intelligence gathering from which the attackers may more effectively stage more focused targeted attacks drawing on intelligence gleaned.

The attack impact can be assessed from a variety of perspectives:

1. the individuals and/or organisations whose computers were compromised and whose personal or organisation-sensitive information and account credentials were captured.
2. the organisations – from the public and private sector which provide “secure” remote web access to their networks from customers, staff and/or the public.
3. the country – the number of infected computers and the number of users with compromised personal identity information within a country.
4. secondary criminal activities which are now possible from the previous categories within a range of affected countries.

Individual or organisational impact

Individuals, whether they are working from compromised workplace computers, public access computers or their own personal computers, may all have their personal information and personal online activities exposed by trojans of this type. By viewing the captured data for a single computer, it is possible to obtain a whole range of sensitive personal information about them and their work to fraudulently use their identity or, to facilitate further targeted attacks against the individuals, the organisation they work for and the computer itself.

Organisations with e-commerce or e-government presence

It is likely that e-commerce or e-government organisations will have a proportion of their customers and/or clients connecting to their systems from infected computers and, which will result in the compromise of some, or all of the transacted data, including

from SSL protected sessions. Such organisations need to consider the security and privacy implications of this and the extent of their obligations to their customers or clients who are also affected. An example of one such organisation that was affected was the Australian Taxation Office and a small number of taxpayers that used the e-tax service.²⁷

Level of infections within a country

Increasingly citizens use their Internet-connected computers to work, connect to work and access e-commerce and e-government services. Therefore, there are serious implications for any society which substantially depends on secure communications and transactions via the Internet if there is widespread compromise among the computers being used to connect and transact with these systems. This means that the integrity and confidentiality of many of those transactions cannot be assured with any reasonable level of confidence.

While we do not know what proportion of this compromised information will be used by criminal elements involved in such attacks or potentially others who may also have gained access to the log data and who also wish to benefit through illicit means, it is clear that such data would not be collected unless it had an intrinsic value to such criminals. Therefore, it is reasonable to expect that such compromises will be used to facilitate a range of additional crimes in other sectors and arenas – both online and off. Other than through losses due to unauthorised bank account transfers, it is generally extremely difficult to identify examples of secondary flow-on crimes that occur as a result of these widespread and indiscriminate online attacks. However, this does not mean that there are no flow-on crimes of a serious nature occurring on a similarly widespread scale. Unfortunately, the difficulty to demonstrate a secondary impact means there is less incentive to prevent or respond to these attacks, which in turn will ensure that criminals derive maximum benefit from them, and further drive their uptake.

Incident Response

AusCERT's incident response extended from 15 June 2006 until September 2006 and involved many hundreds of person hours during this period. Incident response involved issuing shut down requests for all associated sites and domains in the attacks, including contacting the relevant ISPs, domain name registrars, CERTs and law enforcement agencies. While the malware distribution sites were able to be closed within several days of the attacks, the lifeisfine.org logging site remained available to receive information captured by Haxdoor infected hosts for over five months, despite several occasions when AusCERT notified relevant parties of the need to close the site. One compromised site was owned by a company in Melbourne, Australia, another was a personal site operated by an individual from Queensland, Australia, with the rest of the sites hosted overseas.

²⁷ <http://www.abc.net.au/news/newsitems/200608/s1705312.htm>,
<http://www.abc.net.au/worldtoday/content/2006/s1705047.htm>

The vast majority of AusCERT's incident response time, however, involved processing and parsing the log files into country domains and within the Australian domain space, notifying affected top level domains (TLD) and country code level domains (ccLD) where possible. Where an organisation has a relationship with a set of known customers or citizens (such as a bank or some types of government agencies), those organisations may inform these customers/citizens that their computers are infected and their personal information or passwords have been compromised. In most cases, this is the only way that such individuals will become aware that their computer, or the computer they used to contact that organisation's web site, was infected.

Due to the sheer volume of infections, the unfortunate reality is that the vast majority of owners of infected computers will not be advised or able to detect the infection independently. Anecdotal reporting from these organisations and their customers or clients, indicated that attempts to detect the malware on these infected machines was often unsuccessful, even with solid evidence from recorded data that the computer was infected.

Incident response plays a vital role in mitigating the impact of an ongoing attack by reducing the time that malware host sites can distribute malware and logging sites can capture stolen personal information. The analysis of recovered log files provides further opportunity for mitigating the impact of an ongoing attack by identifying:

- organisations which may have infected computers, and
- organisations whose customers or other users who have infected computers

and therefore identify compromised sensitive information of interest to those organisations and/or users who may then take mitigation action.

Conclusion

The case highlights how criminals are able to use trojan malware to compromise thousands of computers on the Internet primarily for the purpose of identity theft and illicit financial gain, and how many thousands of computers and their users are vulnerable to such attacks. In many cases, these computers will remain compromised and used by attackers for additional cyber crimes, such as identity and financial fraud and denial of service attacks.

It is important to recognise that this is just one of many such attacks that occur on a daily basis and therefore, the number of victims is many-fold larger than has been described here. It is also important to consider the secondary and tertiary impacts of these crimes – how stolen identity information can be used for fraud in a whole range of scenarios within society; including for crimes that affect national security. If the level of compromised computers within any one society continues to worsen, this may substantially erode confidence in the confidentiality and/or integrity of all transactions involving identity documentation more generally, online and off.

Case 1

One compromised computer (ID 480524416528564268) in Australia (run 0335) had data captured from 3 April 2006 to 19 July 2006, which shows the computer was infected for at least 14 weeks and 3 days, possibly longer.

The compromised computer is located within an Australian company in Victoria. Given the nature of the activities, it appears to belong to someone with administrator access to the company's web site. Full personal particulars of the primary user and their personal credit card details were obtained as well as personal information for other company employees who used the same computer.

In addition, information about multiple e-commerce transactions (including Internet banking) were obtained including:

- Purchaser's username
- company's name and address
- purchaser's email address
- purchaser's telephone number
- company account number
- credit card details
- login usernames and passwords

Administrator username and password to company web server and numerous email addresses of subscribers/unsubscribers to company email newsletters were also captured.

Case 2

Another compromised computer [ID 10549222801886065695] in Australia had the following information captured by the trojan from run 0406. It appears to be used by at least four different people and appears to be a home computer. Captured data suggests the computer was infected for at least for 26 days, possibly longer.

Users of this computer had data captured in relation to their use of:

- Australian e-government services, including e-tax services
- Internet banking services, including transaction information and personal information such as full name, occupation, employer, marital status, gender
- Online gambling services including username and password