The 'pubstro' phenomenon: Robin Hoods of the Internet

Richard Braithwaite

School of Information Systems
Deakin University
Burwood, Victoria
e-mail: richardb@deakin.edu.au

Abstract

This paper presents a case study of a compromised Web server that was being used to distribute illegal 'warez'. The mechanism by which the server was compromised is discussed as is the way in which it was found. The hacker organisations that engage in these activities are viewed as a Virtual Community and their rules and code of ethics investigated.

Keywords

Web servers, hacking, pubstro, warez, security, computer forensics, ethics, virtual communities.

INTRODUCTION

While there is disagreement on the actual definition a 'hacker' (Rogers 2000), the term 'hacking' is considered to equate to the act of gaining unauthorised access to a computer system (Jordan & Taylor 1998, Rogers 2000). Van Beveren (2001) reported that hacking generally involves causing havoc once unauthorised access has been gained, however, this paper reports on a case of hacking in which the hackers have at no stage attempted to cause deliberate havoc. On the contrary, they have deliberately avoided any activity that would raise awareness of their activities in order to avoid detection for as long as possible.

DISCOVERY OF A PUBSTRO

During November 2002, maintenance was being performed on a Windows NT computer that was used to run Microsoft Internet Information Server (IIS) in order to host a small client-oriented Web site. In accordance with the organisation's policy on machines that require a fixed IP address, the server in question was located outside the corporate firewall. It was also physically located in a locked machine room which meant that administration tasks were normally performed using VNC and, as it had been performing without any noticeable problems in its exclusive role as a Web server, maintenance was irregular and infrequent. During maintenance it was noticed that there was very little available space on the D: drive on which the Web server root was located. A search to reveal why this should be found 15 Gigabytes of foreign language video files in the Recycle Bin. These files were immediately deleted and the server scanned for viruses and trojans after updating the data file for scanning software to the latest version. The virus scan identified the following infections:

- Exploit-IIS.Crack.
- Backdoor-JY.
- RootCMD.

Exploit-IIS.Crack is a trojan DLL which gives a guest account full administrator access to the system and enables a person at a remote site to spawn commands via the Windows NT command interpreter and thus perform a variety of actions such as installing, configuring and running new software (McAfee Security – AVERT: Exploit-IIS.Crack 2002). Backdoor-JY is also a trojan designed to facilitate remote access and control (McAfee Security – AVERT:Backdoor-JY 2002) . RootCMD is not actually a virus or trojan but is in fact evidence of a previous security compromise, typically but not exclusively as a consequence of a CodeRed infection (McAfee Security – AVERT: RootCMD 2001). One aspect of a CodeRed infection is that it leaves a copy of the standard Windows NT command interpreter in non-standard locations under the name `root.exe`. This can then be used in combination with a Web server exploit such as a buffer overflow in order to use a Web browser to remotely run commands on the server (McAfee Security – AVERT: W32/CodeRed.c.worm 2003).

Evidence of a Long Term History

After virus scanning and deleting the offending files, the server was presumed to be clean, however, a more thorough search of the hard disk and Web server log files was performed one week later. This revealed more details of the mechanism by which the server had been compromised as well as evidence to suggest how the compromise was used to establish a 'pubstro' (a hacker underground term for a compromised Windows NT server that is running an illicit FTP server) in order to distribute 'warez' (pirated copies of software, music or videos). It also revealed a history of prior use as a pubstro that extended back to just over one year before discovery.

The evidence of both current and prior involvement as a pubstro included the presence of a number of odd and unusual files including:

- Various versions of the Serv-U FTP daemon. These were in some cases renamed in order to make them appear as system files (eg. rundll.exe or ntask.exe) and thus avoid detection. Serv-U is a commercial FTP server product which has been adopted and modified by the hacker community as the server of choice for establishing pubstros. The presence of these files was most easily recognized by a visual scan for the standard Serv-U icon, a green letter "U".
- INI (Windows application initialisation) files for strange applications. These were mostly configuration files for the various versions of the Serv-U daemon that had been found.
- Copies of cmd.exe (the Windows NT command interpreter) in unexpected locations. As stated previously, this is often due to prior CodeRed infection, however, the relocating and renaming CMD.EXE is common in order to customize the system to facilitate easy access at a later date. Names used for relocated versions include cmd2, superlol, setup and root.
- Odd directory names. Pubstros are usually installed in directory locations that either mask their presence (such as in the Recycle Bin) or make it unlikely that they will be found by being buried very deeply under existing directory structures. However, while the directories may be difficult to find, the names that are used are typically blatantly unusual (eg. -- == [200k] == -- , stro and yehaw) and may indicate either the hackers on-line 'handle' as a tag to indicate ownership or the purpose.
- Tags. These are text files containing a hacker's handle, an on-line identity that is used to maintain offline anonymity (Jordan & Taylor 1998). Tags are placed as a message to other would be hackers that the system in question is currently 'owned' in order to avoid conflict. Tags may be just simple text or possibly contain elaborate ASCII art work, perhaps suggesting a strong on-line identity or ego. A simple tag is shown in Figure 1.

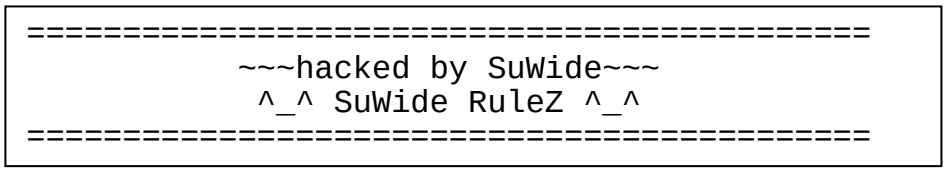

Figure 1: An example of a simple tag left behind on a pubstro.

Another potential symptom of a pubstro compromise is empty or corrupt Web server log files in which the corruption is in the form of blank lines or sections overwritten by spaces. This is the result of hackers vetting log files in order to remove evidence of how the server was compromised. It is not, however, a good indicator of pubstro compromise as such corruption can also happen as a result of power failure or improper server shutdown. Also, analysis of the log files in this specific case showed that not all hackers took the trouble of sanitizing Web server log files in order to cover their trails.

Based on the file time and date stamps of the artifacts of previous pubstro compromises it became evident that a pubstro is a transient phenomenon with a typical life span in the order of two to three weeks followed by a fallow period of another two to three weeks. Thus pubstros were typically established every four to six weeks. Once a pubtsro reached the end of its term, most of the directory structure and associated files (with the possible exception of the evidence mentioned above) were deleted. In the case in question, examination of the system revealed not only evidence of past pubstro usage dating back to October 2001 but also a pubstro in the process of being established, a happy coincidence that shed extra light on the processes of establishing and operating a pubstro. No warez had as yet been uploaded but the directory structure was in place and the Serv-U FTP daemon was installed, configured and ready to use. At this stage in the investigation the latest Microsoft security patches were applied and the server was monitored daily for changed files and any evidence of further pubstro activity.

MECHANISMS FOR COMPROMISE AND CONTROL

Identification of a vulnerable server is based on sending HTTP requests to test for various known weaknesses and exploits. The most common techniques identified in the Web server log files were variations of the directory traversal/Unicode exploits. The directory traversal exploit, also known as the "Dot Dot attack" (Miller 2001), is based on passing in a URL argument that causes the Web server to move up to the root directory, down into the system directory and then run the command interpreter to perform, for example, a directory of the C: drive. If this is successful then other commands can be passed to the command interpreter in the same way to gain entry to the system. The URL argument for a directory traversal exploit is typically in the form of:

```
/scripts/../../winnt/system32/cmd.exe?/c+dir+c:\
```

A patch for the directory traversal exploit was released by Microsoft in August 2000 (Shields 2001) hence many systems are now no longer vulnerable to this exploit. However, a variation called the Unicode exploit emerged. By using Unicode representations of the '/' character this exploit achieves the same effect as directory traversal even on servers that have been updated with patches for the earlier directory traversal exploit. The URL argument for the Unicode exploit is typically in the form of:

```
/scripts/..%c1%c1../winnt/system32/cmd.exe?/c+dir+c:\
```

Another exploit evident in the log files was the buffer overflow approach. This technique is based on the fact that most systems allow for a fixed buffer space for command arguments, and that if a command is issued that exceeds the allocated buffer space then it will overwrite operational code (Nelissen 2002). In the case of IIS Web servers, this technique is most often associated with the various versions of the CodeRed worm. Other observed probes for exploits included searches for sample applications that are typically installed by default and backdoors left behind by CodeRed and Nimda infections.

While the pubstro phenomenon was definitely occurring throughout late 2001 and 2002, there is very little mention of it in the literature. This is quite possibly because in many cases, attacks have gone undetected altogether or have been misdiagnosed as Nimda as one common means of initial compromise was the Unicode/Directory Traversal bug of IIS (Jelver 2002). Jelver commented on two types of probes for server vulnerabilities; single probes, which he described as being generated by the sfind.exe scanner, and two line probes. Jelver also commented on the increase in probing from January 2002 onwards and noted that early probes were from dial up lines whereas later probes were coming directly from other compromised Web servers hosting remotely controlled scanners.

Evidence from Web Server Log Files

The Web server log files of the affected server were scrutinised manually for significant patterns of activity and also statistically analysed for frequency of specific request types, most of which result in "404 File not found" errors. This analysis showed firstly that, contrary to Jelver's experience, probing started as far back as May 2001. Probing also increased rapidly in the month following the CodeRed infection of August 2001 before tapering off again. In keeping with Jelver's observations, probing did increase steadily from January 2002 onwards. Another difference from Jelver's observations is that the complexity of probes also increased significantly over this time. Up until October 2002, most probes were from one to five lines in length and looked for the most common variations of the Unicode exploit. From October onwards the complexity increased exponentially such that by January 2003, some probes consisted of up to as many as 1732 individual requests, each testing for a different potential exploit which, in one case, took over 69 minutes to perform.

The trend of increasing frequency and depth of probing continued after discovery and elimination of the pubstro in November 2002, up until March 2003, at which point it dropped to insignificant levels. During January 2003, there were 12,375 failed requests recorded in the log file, the vast majority of which were the result of failed probes. The increase in frequency and complexity of probe after discovery may be a global trend but may also possibly have been a consequence of the hackers trying to regain control of the lost pubstro. The sudden end to activity in March 2003 is believed (but as yet unproven) to be due to communication throughout the hacker community that the domain in question is being watched and hence it is no longer scanned.

Anatomy of a Pubstro

Analysis of the Web server logs and pubstro artifacts found on the exploited server enabled the modus operandi to be reconstructed. The broad steps in establishing a pubstro are as follows:

- Probe for unpatched exploits. Probing can be performed using one of the many readily available and purpose built scanners such as Grim's Ping, sfind, FxScanner or pubview.

- Copy cmd.exe to a new name and location. This step is not essential but appears to be done for reasons of either simplifying the path for subsequent commands or to leave a backdoor for subsequent access.
- Create a directory structure in an obscure location.
- Start either an FTP or TFTP client via the command interpreter and use it to upload files from a remote server. The files to be uploaded would typically include the Serv-U daemon and its initialisation files but may also include one or more trojans and scanners to facilitate the process of scanning for other vulnerable servers.

The Serv-U daemon is typically configured to be password protected and to operate at a non-standard port to avoid detection. Once configured it is controlled remotely in order to perform FXP transfers (File eXchange Protocol) from other pubstros to populate the site with warez. FXP is a protocol designed for server to server transfer, a process which eliminates the need to first download from one server to a local system and then upload again to a second server. Server to server transfers take advantage of the high bandwidth connections available between servers thus the connection speed of the client is irrelevant (Crocker 2000). The use of FXP for such purposes is not new. Crocker (2000) reported on open anonymous FTP servers being used to distribute warez as far back as 1993. Such anonymous FTP servers are known as 'pubs' in the hacker scene and FXP is frequently used to transfer files between pubs.

PUBSTRO ORGANISATION – A VIRTUAL COMMUNITY OF HACKERS

A search on Google (performed in March 2003) for Web sites that mention pubstros returned 179 hits. The same search on Yahoo returned 186 hits and Lycos returned 254 hits. Of these hits, many were in languages other than English (typically German and French) and most of those that were in English were effectively entrance portals to FXP boards; communities of users engaged in hacking and using pubstros amongst other related activities. FXP boards are Web-based bulletin boards in which members share information about pubstros and warez. Because of their nature they tend to be closed to the general public. Password access is granted only to members who agree to abide by the rules and contribute to the operation of the board. Such sites sometimes openly publish rules of membership and, in some cases, tutorials on how to scan for vulnerable servers and establish a pubstro once a vulnerable server has been located (Warez Guide – FXP Boards; Another Scanning & Pubbing Guide). The documented techniques very closely matched the observed modus operandi discussed previously.

Examination of the FXP boards (Rulez; Board Rules; Project Generation X - Rulez), which by their closed and private nature was limited to the publicly available information that they provided, suggested that there was a high degree of commonality between them. All encouraged the use of IRC for communication between members, most likely to help maintain privacy and anonymity, and all promulgated a similar strict set of rules governing membership and acceptable behaviour. The "FlexFXP" board welcome message includes the following:

> "You are committed to work for the board, that means that you have to do "something" to remain member and not only leech!! This "something" can be fillen (sic) pubs or making scans. These activities are also allowed as a team. The point is that you have to work to keep your account here! If you don't you're not welcome here. Your status is evaluated by the admins/mods." (Board Rules)

All of the FXP boards require both prospective members and continuing members to earn membership rights by scanning for servers, creating pubs or pubstros. For example, the rules for "Project Generation X" stipulate that:

- Prospective members must establish a pub or pubstro of at least 1.5 Gigabytes in order to be granted membership.
- Current members must post a pub or pubstro of at least 2.5 Gigabytes per month to maintain membership.
- Postings are checked and validated by board administrators. Failure to comply with monthly targets and deadlines (with a margin of only 36 hours) results in loss of access rights to the FXP board.
- Once lost, access rights will only be granted again after posting a pubstro of at least 3 Gigabytes.
- Subsequent failure to meet deadlines results in permanent expulsion.

Acceptable behaviour, which effectively includes a code of ethics, is also defined. The following quote (copied verbatim) draws an analogy between the behaviour of FXP board members and library patrons:

> "Pubs are like Books in a Library….. you go searching for a Book…… you find the book…… you Tag it on ur Library card and you walk off with it….. 3 weeks later you've finished with book and you bring it back…..If you keep that book more than 4 weeks… you deserve a FINE! Never take credit

for another Authors Book Renew your book as many times as you like Never and I mean Never! Pull out the Pages of a Book, this will only cause Grief!" (Another Scanning & Pubbing Guide)

Other examples of ethical and acceptable behaviour within the FXP boards' rules include:

- Ownership and rights of the owner: Never spread a pub or pubstro to another FXP board or Warez group/channel on IRC without permission of the builder.
- Punishment for non-conformance: Never post a pub or pubstro that you didn't build. Stealing won't be tolerated!
- Punishment for damage to another's property: Never delete, rename or lock anything that you didn't build! Other FXP boards will be told of your actions.
- Citizenship and reciprocal rights between groups: Your nickname or groupname should be included in your tag.
- Working for the good of the community: Never complain about speed or quality of a pub or pubstro! Try to make a better one instead.
- Optimal use of resources for common good: To prevent mass leeching and slow speed for everyone try to keep your pub's and pubstro's size in good relation to the FTP speed.
- Equity: Never post a pub or pubstro that isn't ratio free! Warez should be free for everyone.
- Authority: If you have a problem with another member then let the administrator or any responsible moderator know! Do not start personal wars!
- Courtesy: Thank the people who created the pubstro when you download.

Despite the fact that what they are doing is labelled as hacking and no doubt illegal, FXP boards and their members have evolved into virtual communities. According to Rheingold, virtual communities "are social aggregations that emerge from the Net when enough people carry on those public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace" (Rheingold 1993, p. 5). Jordan and Taylor reported that "there are no formal ceremonies to pass or ruling bodies to satisfy to become a hacker" (Jordan and Taylor 1998, p. 766), yet both creating and using pubstros are restricted activities that are very much governed by the rules of the virtual community.

Why do it?

Rogers (1999) commented on how hackers often see themselves as modern-day "Robin Hoods", stealing from the rich (in this case, producers of software, music and films) and giving to the poor (working members of their society). While to the world in general their behaviour appears unethical in that it contravenes laws governing such things as theft and copyright, they do have their own code of ethics which in their minds provides a justification for their actions.

Membership of FXP boards, pubstro groups and similar groups is now very risky from a legal point of view. Operation Buccaneer is an ongoing international copyright piracy investigation. As part of a coordinated international effort, the U.S. Customs Service and the Department of Justice executed or arranged for more than 65 searches across the U.S. and five other countries in December 2001. As a result of the Operation Buccaneer investigation, 16 defendants have been convicted in the U.S. of felony criminal copyright offences as of October 2002, and 13 defendants have been sentenced to federal prison terms of up to 46 months (Operation Buccaneer).

With the obvious threat of legal action if caught, the obvious question is why do they it? Jordan and Taylor (1998) recognised five motivations for engaging in hacking:

- Addiction to computers
- Curiosity
- The thrill of illicit on-line activity
- The ability to gain power over other people's or organisation's computer systems
- Peer recognition from other hackers or group members

Any one of these may be sufficient motivation for joining an FXP board, however, the strong sense of community and belonging to an FXP board may well help satisfy needs for individuals who do not relate well in the physical world.

STOPPING THE PUBSTRO/WAREZ MOVEMENT

Stopping the proliferation of pubstros and similar means of disseminating warez is likely to be difficult for a number of reasons. Firstly, new exploits are always being found. When exploits are found and publicised, the information becomes available to hackers as well as security aware system administrators. The uptake of information about new security exploits is likely to be quicker amongst hackers than system administrators because, unfortunately, not all Web servers are maintained by security aware administrators. Many of the probes identified in the log files were traced back to other compromised Web servers which were used to stage attacks on other systems. This is the case because using an exploited Web server to host the scanning software gives the hackers a layer of anonymity. Of the exploited servers being used to scan, some were still functioning as normal Web servers hosting sites for colleges, small businesses and government departments. Others were functioning as servers but only hosting default pages which suggests that a significant number of Windows NT and Windows 200 installations have Web servers running as system processes without the operators being aware. Such systems are fertile ground for pubstros as they are unlikely to be detected over the lifetime of the system. The sheer number of exploited servers evidenced in the log files also suggests that there is in general a lack of awareness of Web related security issues. Indeed, the need for operating system patches appears to be either widely ignored or ineffective in its dissemination to administrators.

Prevention by attempting to find and identify hackers is fraught with difficulty. Typically, backtracking to the IP address of probe inevitably points to another exploited server. Even if the log files on these servers were checked in order to go back one more step, it is unlikely that the individuals could be traced as contact with the Web servers is most likely through either an anonymising proxy or via a temporary ISP account. Gollman (1999) provided a definition of computer security that covers three aspects:

- Confidentiality: prevention of unauthorised disclosure of information
- Integrity: prevention of unauthorised modification of information
- Availability: prevention of unauthorised withholding of information or resources

Assuming a pubstro is managed properly by its 'owners' in order to avoid detection it does not conflict with any of these aspects therefore it is not adequately covered by such a definition of computer security. As opposed to the general concept of hackers as mischief makers who cause havoc through data destruction and denial of service, pubstro operators do no such damage. They are a form of cyber parasite that goes to great lengths to avoid detection or damage to the host. Nonetheless, crimes are still being committed. Obviously, copyright violation is the predominant crime, however, while no system damage is done, significant amounts of bandwidth are likely to be consumed as part of both FXP transfers and FTP downloads. For example, a 3 Gigabyte pubstro that is transferred in by FXP, downloaded by 100 people over a two week period and then transferred out again by FXP would amount to theft of over 300 Gigabytes of bandwidth, and at the same time may well cause load problems on the affected server and its associated network.

Many of the legal issues are unclear. Because computer crimes associated with pubstros are very likely to occur across international boundaries, the question arises as to which jurisdiction would be responsible for investigating and prosecuting, assuming someone could be caught. Another potentially grey area would be determining liability for copyright violations found on a server that was unknowingly hosting a pubstro. Would the organisation hosting the Web server be in anyway liable for the copyright violation, perhaps because of poor and ineffective maintenance and security practices? If so, could perhaps Microsoft then also be held accountable for contributing to the problem by releasing a product that is used to facilitate the dissemination of copyright violations?

Further research presents significant challenges. The chain of deception used to maintain anonymity means that it is practically impossible to clearly identify an individual involved in establishing or using a pubstro. The rules for joining an FXP board are such that one must engage in illegal activity in order to be eligible. Even the use of a honeypot, a server designed to attract and trap potential hackers, is questionable as the process of observing ongoing pubstro operation via a honeypot would also imply that the controllers of the honeypot were knowingly allowing illegal activities to take place.

CONCLUSION

Pubstros are an example of essentially non-destructive hacker activity that involves breaking into susceptible Web servers using techniques such as the directory traversal and Unicode exploits and then establishing covert FTP servers to distribute copied software and media files. Damage and mischief is avoided at all costs so as to avoid detection, thus pubstros operate as a parasite within a host environment. Pubstros are established and maintained by members of FXP boards which are effectively virtual communities of hackers that operate with their own strict rules and code of ethics. While their activities involve illegal actions, FXP board members

justify their actions by interpreting them within their own code of ethics and thus see themselves as Robin Hoods.

REFERENCES

Another Scanning & Pubbing Guide (n.d) URL http://66.128.99.149/ubb/tuts/anotherguide.htm, Accessed March 7 2003

Board Rules (n.d.) URL http://www.flexfxp.com/rules.html, Accessed February 18 2003

Crocker, S. (2000) FTP and the Warez Scene(SANS Info Sec Reading Room) URL http://www.sans.org/rr/toppapers/warez.php, Accessed January 24, 2003

Gollman, D. (1999) Computer Security. Wiley, New York.

Jelver, P. (2002) Pubstro-hacking - systematic establishment of Warez servers on Windows Internet servers URL http://www.esec.dk/pubstro.pdf, Accessed January 24, 2003

Jordan, T. and Taylor, P. (1998) A Sociology of Hackers, The Sociological Review Vol. 46, No. 4, 757-780.

McAfee Security – AVERT: Backdoor-JY (2002). URL http://vil.nai.com/vil/content/v_99355.htm, Accessed May 30, 2003

McAfee Security – AVERT: W32/CodeRed.c.worm (2003). URL http://vil.nai.com/vil/content/v_99177.htm, Accessed June 2, 2003

McAfee Security – AVERT: Exploit-IIS.Crack (2002). URL http://vil.nai.com/vil/content/v_99505.htm, Accessed May 30, 2003

McAfee Security – AVERT: RootCMD (2001). URL http://vil.nai.com/vil/content/v_99254.htm, Accessed May 30, 2003

Miller, N. (2001), Microsoft IIS Unicode Exploit (Lucent Technologies White Paper). URL http://www.lucent.com/livelink/0900940380004b2d_White_paper.pdf Accessed June 3 2003

Nelissen, J. (2002) Buffer Overflows for Dummies (SANS Info Sec Reading Room) URL http://www.sans.org/rr/threats/dummies.php, Accessed January 24, 2003

Operation Buccaneer (n.d.) URL http://www.cybercrime.gov/ob/OBMain.htm, Accessed June 3 2003

Project Generation X - Rulez (n.d.) URL http://www.project-generation-x.org/rulez/rulezeng.htm, Accessed February 18 2003

Rheingold, H. (1993) The Virtual Community: Homesteading on the Electronic Frontier. Addison-Wesley Publishing, Reading MA.

Rogers, M. (1999) Modern-day Robin Hood or Moral Disengagement: Understanding the Justification for Criminal Computer Activity URL http://www.mts.net/~mkr/moral.doc, Accessed June 2, 2003

Rogers, M. (2000) A New Hacker Taxonomy "Revised Version" URL http://www.mts.net/~mkr/hacker.doc, Accessed June 2, 2003

Rulez (n.d.) URL http://heimwaren.net/allg/rulez.php, Accessed February 18 2003

Shields, S. (2001) Web Server Folder Traversal Vulnerability (SANS Info Sec Reading Room) URL http://www.sans.org/rr/threats/traversal.php, Accessed January 24, 2003

Van Beveren, J. (2001) A Conceptual Model of Hacker Development and Motivations Journal of E-Business Vol.1, No. 2.

Warez Guide – FXP Boards (n.d) URL http://core-knowledge.tripod.com/wg_fxpboards.htm, Accessed December 6 2002

COPYRIGHT