;login:

THE USENIX MAGAZINE

December 2003 • volume 28 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow

inside:

USENIX

The Advanced Computing Systems Association

coordinated incident response procedures

by Dario Forte

Dario Forte, after working for the Italian government for 15 years, is now security advisor for the European Electronic Crime Task Force (EECTF), a nongovernmental group dedicated to incident response. He is also the founder of Incident Response Italy, developed at the University of Milan, where he teaches incident response management.

dario.forte@acm.org

A Case History

Background

In mid-2002, two groups of malicious hackers were identified by the Italian Financial Police as being responsible for a series of attacks on over a thousand targets throughout the world. The backtracing procedure was seriously complicated by the fact that the groups used numerous stepping-stones and camouflage techniques, such as IPv6 tunneling. In this article we take a general look at the attack methods and illustrate the techniques and steps used to backtrace them. For reasons of privacy we will not name the targets but will use letters instead:

A – The German target used as an initial stepping-stone to attack the American governmental sites indicated below

B – The main American governmental target attacked by the group

C – Another American governmental target attacked by the group, which served as the starting point for the investigation

SS1 – A university machine used as a repository to hide rootkits and other tools used in the post-intrusion phase

A Coordinated Attack

In September 2001, the owner of C realized that one of his machines (an IRIX) had been attacked. The exploit had been launched from a German machine, which had previously been compromised by an exploit from its resident Web server. The system administrators for C later reported that commands had been sent from the German machine to download certain post-intrusion tools (including rootkits) from a third machine, SS1, located at an American university. Here is the general scheme.

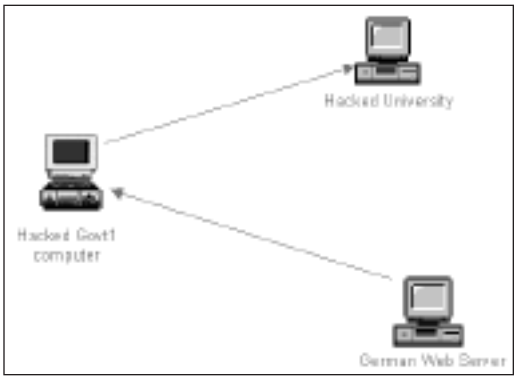

Figure 1

Reconstructing what happened to C was possible thanks to the presence of an IDS that monitored the target. While this did not permit a response in realtime, it did make it possible to recover a series of logs that illustrated what had happened. The logs were usable because they were not on the attacked machine. In the meantime a post-mortem exam was carried out on the German machine, A, that had been used as a stepping-stone. The method used to compromise the German machine was generally conventional, but had a number of personalized touches added by the attackers.

Requirement No. 1: Reconstruct the Events

One of the first steps in this sort of investigation is to check how much time passed between the last update of the machine and the attack. This may help identify the exploit that was used to achieve the intrusion. In this case it was a Linux machine that was not running the latest release. At the time of the intrusion, the bug exploited to compromise the box was the then-known wu-ftpd site command exploit.

An attacker who penetrates a machine installs a rootkit in order to keep the machine compromised. One of the attack group's characteristics was the use of completely self-made rootkits along with materials known to the security community. The choice depended on the type of target (in the case we are examining, there were nearly a thousand boxes compromised worldwide).

The t0rn rootkit was chosen for the German machine and installed in /usr/info/.t0rn. Evidently, the reasoning used in this case was, given that the system was generally poorly administered, it was not worthwhile to keep it compromised with something exotic, since it was unlikely that the administrator would realize what was going on anyway. In any case, it may be helpful to consult /usr/src/ to try to determine what is going on. In the specific case, a lot of information was found in /usr/src/.r00t.

t0rn rootkit, like most tools of its ilk, is configured to hide certain network connections. This is the usual syntax found during a post-mortem (the IP addresses are fictitious):

```
65.93.*.*
195.242.20.*
```

where * is used to hide all the addresses of the block. The first instance usually occurs to hide classes of dynamic IPs that the attacker has access to (e.g., ADSL and dialup based on DHCP). In the second instance, an entire class is indicated, including one or more machines compromised for the long term by the attacker.

Once the groundwork is laid, the hacking tools are installed. The choice of tools is completely up to the attacker. In our case, the hacktools installed were:

`7350wu`	exploit to hack into the wu-ftpd (used on this system, too)
`massroot`	exploit for a bug in the telnetd of IRIX systems
`statdx`	exploit for the rpc.statd of RedHat
`mirkforce`	attack tool to disrupt IRC communication
`papasmurf`	smurf attack tool, a denial-of-service tool
`seclpd`	exploit for lpd in RedHat 7.1

Please note that we are talking about an attack that occurred in 2001. Interestingly, several text files made clear that A was the machine used to attack the governmental sites. The attacked networks, in fact, were in the 136.*.*.* and 137.*.*.* nets. It might be useful to seek subdivisions by operating system in these files. In this case FreeBSD, IRIX, Linux, and SunOS were found, along with a ".txt" file which contained progress info of the scanning.

This proves how important it is to correlate what is found on one machine with what is found on the one that appears to be directly connected to it. The correlation, especially if done on more than two machines, can map out the events with a certain margin of certainty and point back to a single source.

Another item usually installed is psyBNC IRC Bounce BOT. In this case it was used as a deflector to participate in IRC communication without revealing the hacker's IP number, thus avoiding DoS attacks on the hacker's machine. Usually the attacker installs BOT with the his IRC nick, which, in many cases, turns out to be very important for final backtracing.

The following presents the main steps taken by the attacker after the intrusion:

1 System is penetrated through an exploit.
2 A rootkit is installed.
3 nc-ftpd is installed.
4 A port scanner is installed.
5 A sniffer is installed.
6 A psyBNC BOT is compiled and installed.
7 A rootkit is fine-tuned.
8 A file with IP numbers is created.
9 The "real use activity" starts.

The compilation of the items downloaded by the third machine (SS1 in this case) is generally carried out either on the attacker's machine or directly on the compromised machine. Both choices have their pros and cons. For example, compiling on the attacker's machine might speed things up but risks instability due to potential differences in platforms. On the other hand, one cannot be sure that there is a compiler on the compromised machine, even though it is quite probable for relatively simple cases.

Further Correlations

In the case in question, there was another positive factor for the investigation: cross-checking of the SS1 machine. When a machine is used as a repository for tools that will be downloaded onto target machines, it may happen, with a bit of luck, that additional cross-references can be found to correlate all the necessary information. Given that most such "containers" are located on university networks, we find ourselves confronted with the following situation:

- University officials provide system logs and an image of the compromised computer.
- The compromising of the US university machine is linked to the compromised third-party computer.
- The university computer is used as a "toolbox." All links between the .edu computer and the real target require a physical-level search that, very often, reveals a dialup connection.
- A proper HD analysis can uncover the intruder's rootkit.

This check, in the specific case, allowed the real departure-point ISP of one of the attackers to be backtraced. The same control also provided several important correlations regarding attacks on B, from which important sensitive files were stolen. Figure 2 diagrams the basic correlation.

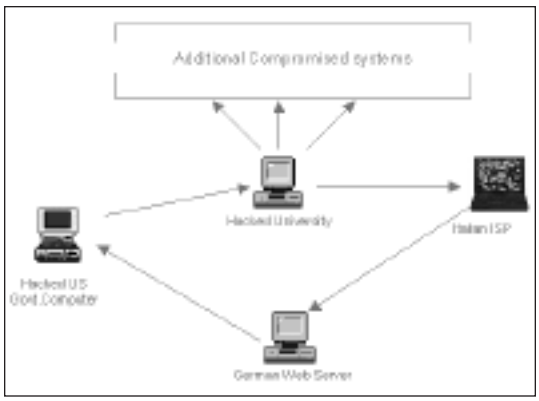

Figure 2

Conclusion

Another successful aspect of the investigation was that all the investigators spoke the same technical language. Terminology, log type, image format, tools, and PGP keys were agreed on before beginning the investigation, proving the fundamental importance of setting things up well before getting started.

We have only touched the tip of the iceberg in this article and discussed only those parts of the investigation not protected by nondisclosure restrictions. The investigation was anything but simple. The operation, known as "Rootkit," took more than one year and involved five European and American investigative agencies (military and civilian). Fourteen people were charged, including four minors. Most of them worked as security consultants or managers in large multinational companies. More than 40 computers and almost one terabyte of data were seized, along with thousands of CD-

ROMs and DVDs. Many credit card files were recovered. If it had not been for the close international collaboration, it might not have been possible to track down the perpetrators of over 1000 worldwide attacks, who were so active and so skillful as to be able to write their own rootkits and log wipers, used on the most "important" machines, and so crafty as to use IPv6 tunneling. Unfortunately (or fortunately), it's a small world: Some of the people charged as a result of this investigation had also punched holes in a Mexican honeynet, going so far as to get into the Honeynet Project's famous "scan of the month."

Acknowledgments

I would like to thank Eddie Autelli, Dave House, Alvin Allen, Kevin Manson, Troy Bettencourt, and Chris Fischer, all members of EECTF, for all the incredible support I have received over our years of working together.