Global Information Assurance Certification Paper

Investigating One Incidence of Anomalous Network Traffic
Stan Sander
May 3, 2003
Version 1.2d

Introduction

I'm sure that like most people who take the SANS Security Essentials course, I was having a little difficulty deciding exactly what to research. I selected what I thought would be a good topic and began my research. I had about a page of hand written notes, when 'it' happened. 'It' was anomalous traffic leaving my network. This paper is an effort to describe just how I was able to detect this traffic and an account of how I reacted to the situation once it was discovered.

The Detection

In order to adequately describe how I detected the strange behavior on my network, I think it necessary to give you a bit of background information. First, would be what I call a common sense approach to handling potential security incidents. My interpretation of this principle has evolved into a portion of my own personal security policy, which is isolate, investigate and verify, gather and preserve evidence, eradicate the problem, and recover from the incident. There is a lot more to a good policy, and the discussion of that topic is beyond the scope of this document and has been covered thoroughly in other places.[1] The main point I want to raise in mentioning this is no matter what circumstances you are in, you should have a plan (i.e. Policy) in place before you experience an incident and realize you need it.

Second, is a general overview of the network I am discussing. I have set up a small network in my home, consisting of four PC's. One each for my two step-sons, running Windows 98 SE, my Linux machine which acts as a server as well as my desktop, and another machine running Solaris 8 x86 that is utilized as a router with firewall and NAT software. We do not have any high speed connection options available in our area yet, so we connect via a 56k modem. The Solaris machine brings up the internet connection on demand and tears it down after a specified time of inactivity.

As part of my defense strategy, I run intrusion detection software both inside my firewall and on the modem interface outside the firewall. I selected snort, www.snort.org, for this purpose. One of the known weak links in the network is the two boys do not run current anti-virus software on their machines by their own choice. The morning of May 17, 2001 during a normal daily review of the logs, I detected something that obviously did not belong. The modem had established a connection at 1:58 PM the previous day, May 16. This meant that one of the machines on the network was sending traffic outbound. The problem with this instance was no one was home at that time. The modem connection was torn down as expected earlier that day after the time-out period for no activity. Further checking of other logs indicated that one of the PC's had initiated a SYN scan of port 1214 across at least 11 hosts in a span of 34 seconds. I checked that machine and verified that there were no processes running that could be expected to generate that kind of traffic legitimately. At that point, I disconnected the network cable leading to that machine at the hub. I felt I had enough evidence to be suspicious, and there was no indication of current

suspicious activity where leaving it connected would have been beneficial for investigating the incident, which is true in most cases. I would investigate and find out more details later when I had time. In the meantime, if this did turn out to be malicious, it was now isolated and couldn't spread through the network.

The Investigation

At first, my investigation was not too aggressive or intense. Since I knew that current anti-virus software was not in place, I was expecting to discover that some well-known virus or trojan had infected the machine. I went to Symantec's virus encyclopedia[2] and did a search for port 1214, and was not successful at identifying what this could be. I knew that many viruses are written using Microsoft's Visual Basic Scripting language, so I searched the system for files with a .vbs extension, which is typical for those types of files. I did find one file with that extension that interestingly enough was modified about 10 minutes after the scan.

I did a check to see exactly who the machine had scanned. I discovered it included:

- 3 universities in the US
- 1 university in the Netherlands
- 1 university in Sweden
- 1 cable modem in the US
- 1 university in Canada
- 1 university in Great Britain
- 1 ISP in Great Britain
- 1 university in Germany

The total number of packets sent out was only 33 across all 11 sites. Not a massive scan by any means, but enough to raise a flag for my small network.

I explained to my step-son what I suspected had happened to his machine, and that it was isolated and would remain so until the hard disk was formatted and the operating system re-installed or a definitive determination was made about what had happened and that any malicious components were unquestionably removed. I questioned him about having installed new software recently or if he knew why his machine would be trying to connect to other machines on it's own in the middle of the day. He denied having installed any new programs in the days immediately preceding the incident. At the time I am writing this paragraph neither he or I have an answer to why the machine scanned port 1214. Nevertheless, the machine will not get reconnected to the network unless I can prove that there was and is no malicious activity.

The next step I performed in trying to identify why this happened was to check for open ports that could be an indication of a back door program. I failed to find any. Since he was not anxious to have the issue resolved as I expected he would be and I was busy trying to work on my GSEC research paper, I let the issue sit on the back burner for a while, but kept my "radar" on for potential explanations.

About this same time, I decided it would be beneficial for me to subscribe to the mailing lists offered by incidents.org.[3] I had been following this site for a while and had learned to appreciate the role that it plays and saw the value in the near real-time reporting of activity via the CID

graph.[4] In addition, I was still looking for material to research the original topic I had selected. Then on May 31, a piece of information came in that I couldn't ignore. Someone else posted a report of a scan to port 1214. I immediately responded with a question to see if anyone knew what was generating these scans.[5] The responses to this indicated that it could be KaZaA, a peer to peer file sharing program. Matt Scarborough, offered some traffic analysis and a file to look for for verification whether it was KaZaA or not.[6] I checked the system and found that the KaZaA application was not installed. I also did a more aggressive forensics pass on the machine and discovered that the .pif file for the MS-DOS prompt on the machine had been modified following the scan. I do not know if this is normal for Windows or not, since I'm more familiar with UNIX and Linux. It also occurred to me that I could write my research paper for GSEC on the process of investigating and analyzing this incident.

After receiving the information about KaZaA, I decided to check the logs for the squid proxy I run on the network for the purpose of trying to filter out access to inappropriate web material. I discovered that while the machine was scanning these other hosts it was also talking with musiccity.streamcastnetworks.com. It made another attempt to contact musiccity.com about 45 minutes later, but for some reason this time was unsuccessful. About 30 minutes later, there was some traffic from this machine to msn.com. After approximately another 30 minutes there was more communication to musiccity.streamcastnetworks.com, including this Post to wildtanget.com, a company working to develop multimedia technologies.[7]

> 990049564.625 873 192.168.1.3 TCP_MISS/200 303 POST http://updaterservice.wildtangent.com/appupdate/appcheckin.wss - DIRECT/updaterservice.wildtangent.com text/plain

I contacted Wildtangent, and awaited their response. When I received the response from Wildtangent, they explained that a web driver application that is associated with the ability to view their proprietary file format reports back to them on the sites that make files available in that format, and has an automated bug reporting system that utilizes the same communication channel.[8] The same web page indicates that you can alter the "self-maintaining properties of the web driver" through their Control Panel applet provided. The e-mail I received from Wildtangent also stated that their software will not initiate a connection, but would utilize an existing internet connection.

My next action was to get a system image using tar while his system and my Linux machine were the only ones connected to the network. Given the existence of the W32.Winux virus, this was a calculated risk, but seemed acceptable given the current information available.[9] [10] I then began an extensive search for files that had been modified recently. I started by going back 60 days. My tar file that I generated only contained the Operating System and Program executables. I excluded the entire directory tree that I knew to contain only data and other user specific information. I prepared for a more intensive investigation further by downloading Zone Alarm[11] to install in a Windows 98 SE machine running under vmware. I expect this to give me a more controlled environment for testing software behavior.

I discovered that a program called Morpheus was installed on the system on April 20. This application was downloaded from musiccity.com. In checking into the program, I found that

this was a peer to peer file sharing application that touted it had always open connections to the peer to peer network, was "self-organizing", encrypted, and had embedded Microsoft Media Player functionality.[12] A statement on the same page also stated, "A direct distribution tool that allows content developers unfettered access to consumers and customers." The claims also stated it had automatic CPU and network throttling. I decided I would download my own copy of this program and run it on the virtual machine with Zone Alarm. The downloads page reported the number of downloads to date was over 1.6 million[13], so it has obviously become a popular piece of software. According to the page I downloaded from this application was a preview version first posted on April 12, 2001.

Following the download and install, I compared the file sizes between the two copies of the executables. The newer version was 63K bigger than the original on the system. I executed the install program while running tcpdump in another window. The program generated the following traffic as the install proceeded:

- It initiated connections to web servers at musiccity.streamcastnetworks.com through the proxy, which indicates it must have read some registry settings.
- It initiated connections to the web server at www.musiccity.com through the proxy
- It crafted its own ICMP echo request packets and directed them to 204.152.197.197, which I was unable to resolve through nslookup or whois queries
- After not receiving an echo reply from the above address, it then tried 130.244.215.233, which is in Sweden
- Still not receiving a reply, it tried 202.139.195.203, which is registered to an ISP in Tokyo, Japan
- Still waiting for a reply, it continued down what is apparently a list of IP addresses, the next one being 202.232.17.87, again a site in Japan.
- Without receiving a reply to its echo requests, it then sent SYN packets destined for port 1214 to 206.142.53.27. This address is possibly in the musiccity.com domain, but nslookup returns a Server Failed error when attempting a lookup. According to whois.arin.net this is a cable and wireless provider out of California. The network blocked assigned to this provider includes the addresses used by musiccity.com.
- It then looked for supernodes 1 through 4.streamcastnetworks.com
- It then queried for supernode.kazaa.com
- Next, it continued with 2 more SYN packets directed to 206.142.53.27 port 1214, followed by SYN packets to port 80 at the same IP address
- Since outbound connections are not allowed from this machine to port 80, the program then jumped up to port 8080, and initiated a connection
- It continued to try to reach port 1214 at this address
- While this was going on, I noticed several ICMP type 11/0 packets from
    - 204.152.197.197, the unregistered IP address that had been sent echo request packets
    - 130.244.215.233, the Sweden address
    - 202.139.195.203, the ISP in Tokyo
    - 202.232.17.87, the other Japan address
    - Notice that the internally generated ICMP echo request packets generated an ICMP 11/0 packet in response
    - As I was writing this section, I tried to send echo request packets using the

standard ping command, and received a response of ICMP 3/1. According to RFC 792,[14] both of these responses could be legitimate responses to echo requests. The 11/0 message is time to live exceeded in transit, the 3/1 is host unreachable. It seems interesting that the apparent type of the packet that is returned changes along with the program used to generate the echo request packet.

I interrupted the install at this point as I felt I now had the answer I was searching for. This scan was most likely generated by the Morpheus application from musiccity.com. Below is a copy of the correspondence I sent to musiccity.com.

> Greetings,
>
> I am writing a research paper in pursuit of a GSEC certification from The SANS Institute. During the course of researching my topic, the Morpheus application has become the center of attention.
>
> A brief summary is a machine on my small home network initiated a scan of port 1214 of several hosts on the internet. At the same time, it was in communication with your site. No one was home at the time of this incident. During the course of my investigations I downloaded a copy of Morpheus and began the install process on another machine, while running tcpdump (a network packet sniffer) on my server. There were no other applications running on the machine where Morpheus was being installed. I was hoping that you could provide some insight into the following questions, which come from network packets I observed during the process of installing (partially) this application.
>
> 1. Are there any options that are on by default in Morpheus that would cause it to initiate a scan of port 1214?
>
> 2. Why does the install process send apparent icmp echo request packets to 204.152.197.197, 130.244.215.233, 202.139.195.203, and 202.232.17.87
>
> 3. In the spirit of investigating these incidents, would you be willing to provide a pgp signature file of the unpacked executable as it existed on the download servers on April 20 (the date this app was originally installed on the system in question) and on June 9 (the date I downloaded another copy for my investigative purposes) I did note that the June 9 executable is 63 K larger than the April 20 version.
>
> Thank you for your attention to this matter, and I look forward to hearing from you.
>
> Stan

As of the time I submitted this paper, I have not had any response from musiccity.com.

Conclusion

As explained in the SANS course, you need to be familiar with your network and what is and is not normal traffic for your site. In this case, there are still some questions that are left unanswered. Is Morpheus a trojan or has it been replaced with a trojan? In my opinion, it does exhibit characteristics of a trojan, specifically the echo request packets it crafted, and it is apparently responsible for initiating automated scans to port 1214 at the very least. Both of these actions occurred without the knowledge or intervention of the user. Why does it send apparent echo request packets to an unregistered IP address, one in Sweden and at least 2 in Japan? What about the ttl exceeded packets that came back in response? Was there some embedded payload in these packets, or were they legitimate packets that behaved as expected? The answer to that question lies beyond my scope of resources and expertise, so I will leave it to someone else to answer, or I may acquire the knowledge necessary to find the answer on my own someday. With the popularity of mp3 files and peer to peer network applications, and the reported 1.6 million plus downloads of this program, it seems like a favorable place for the so called "blackhat community" to have a trojan spread and do work of their bidding. As always, user education and the need to be cautious cannot be emphasized enough.

1http://www.sans.org/infosecFAQ/policy/policy_list.htm
2http://www.symantec.com/avcenter/vinfodb.html
3http://www.incidents.org/detect/list_info.php
4http://www.incidents.org
5http://www.incidents.org/archives/intrusions/msg00527.html
6Matt Scarborough, ibid, intrusions archive
7http://wildtangent.com/company/
8http://www.wildtangent.com/candy/privacy.html
9http://www.symantec.com/avcenter/venc/data/w32.peelf.2132.html
10Thomas A. Smit, SANS http://www.sans.org/infosecFAQ/malicious/w2kwinux.htm
11http://www.zonelabs.com
12http://www.musiccity.com/technology_nf.html
13http://download.cnet.com/downloads/0-1896420-108-76172.html?bt.48575.185
14http://www.faqs.org/rfcs/rfc792.html