Case Study: "Calling Home?"

The Beginning

On a sunny Tuesday afternoon, at 2:00PM, we received a call from Namal, the System Administrator at a Government Department providing a critical service to citizens. He informed us that the Department was experiencing a network slowdown. According to him, the firewall logs showed blocked connection attempts which were generated by hosts within the Department network pointing towards some specific IP addresses outside the Department network.

Namal had another interesting observation; there had been a recent visit from a security consultant, who had browsed the Internet using the Department network. While Namal was scanning the Firewall logs, he had observed the Security Consultant's machine also trying to connect to the same outside IP range. Basically, the Security Consultant's machine also showed the same behavior as the hosts inside the Department Network.

There was also a Proxy Server present in the network, and all the hosts in the network were had Anti-Virus Software already installed.

Suspicions

Namal was under the impression that the hosts in his network were victims of a Distributed Denial of Service (DDoS) attack, possibly unknowingly being used as *zombies* to attack a single target site. Upon performing a DNS Lookup, he had discovered that the destination IP Addresses were registered in the IP range(s) belonging to one "Akamai Technologies". Namal contacted us to ask for assistance in resolving the issue.

The Investigation begins

We asked Namal to provide us some information about the Security Consultant's notebook and other Hosts on the network. He reverted promptly with the answers to the following questions:

a. What is the Operating System being used?
b. Is there any Anti Virus software running? What is the brand?
c. Is there a Personal Firewall operating in the host?
d. What is the make of the machine(s)?
e. What are the other applications running on the host?
f. Firewall Logs.

We had three major questions to answer. ***What*** was the *cause* of this event? ***How*** was it causing this event? ***Why*** is it causing this event?

Analysis

We set to work analyzing the information provided.

First, we took a look at the Firewall Logs; the source of the suspicion. As the excerpt from the Firewall logs below shows, the Source Port number on the Department Host, 192.168.0.13, was continually incremented in each successive connection attempt. It was also interesting to note, that the connection attempts were retried at specific time intervals during the course of the day.

Date	*Time*	*Protocol*	*Source IP*	*Source Port*	*Destination IP*	*Destination Port*
17-Nov-06	13:12:50	TCP	192.168.0.13	2499	72.246.53.81	80 (HTTP)
17-Nov-06	13:12:49	TCP	192.168.0.13	2498	72.246.53.96	80 (HTTP)
17-Nov-06	13:12:48	TCP	192.168.0.13	2497	72.246.53.91	80 (HTTP)
17-Nov-06	13:12:47	TCP	192.168.0.13	2496	72.246.53.89	80 (HTTP)
17-Nov-06	13:12:46	TCP	192.168.0.13	2495	72.246.53.96	80 (HTTP)
17-Nov-06	13:12:45	TCP	192.168.0.13	2494	72.246.53.89	80 (HTTP)
17-Nov-06	13:12:44	TCP	192.168.0.13	2493	72.246.53.74	80 (HTTP)
17-Nov-06	13:12:44	TCP	192.168.0.13	2492	72.246.53.83	80 (HTTP)
17-Nov-06	13:12:43	TCP	192.168.0.13	2491	72.246.53.73	80 (HTTP)
17-Nov-06	13:12:43	TCP	192.168.0.13	2490	72.246.53.81	80 (HTTP)
17-Nov-06	13:12:42	TCP	192.168.0.13	2489	72.246.53.72	80 (HTTP)
17-Nov-06	13:12:42	TCP	192.168.0.13	2488	72.246.53.80	80 (HTTP)
17-Nov-06	13:12:41	TCP	192.168.0.13	2487	72.246.53.96	80 (HTTP)
17-Nov-06	13:12:40	TCP	192.168.0.13	2486	72.246.53.90	80 (HTTP)
17-Nov-06	13:12:22	TCP	192.168.0.13	2484	72.246.53.83	80 (HTTP)
17-Nov-06	13:12:21	TCP	192.168.0.13	2483	72.246.53.81	80 (HTTP)
17-Nov-06	13:12:20	TCP	192.168.0.13	2482	72.246.53.80	80 (HTTP)
17-Nov-06	13:12:19	TCP	192.168.0.13	2481	72.246.53.74	80 (HTTP)
17-Nov-06	13:12:18	TCP	192.168.0.13	2480	72.246.53.73	80 (HTTP)

Moving on, we analyzed the rest of the information:

- ✓ All the machines in the host network were Hewlett-Packard machines running on Windows XP Professional Operating System. The Security consultant's machine was a DELL, and also running on Windows XP Professional.
- ✓ Some Hosts were using Symantec Anti Virus Software, while the consultant was using AVG as the Anti Virus software.
- ✓ All users had enabled the Windows personal firewall except this new person (the security consultant). He was using AVG firewall.
- ✓ Most of the machines had been installed with Microsoft office and Adobe acrobat reader.

- ✓ The Security consultant used Firefox as his web browser. All other users used Internet Explorer.

The DDoS scenario began to seem more and more improbable, and our suspicion was that all the machines had an *agent* installed in them, which was trying to "Call Home" for some reason, and that was the reason why the Connection attempts were being made. Now, we needed to find out *what* was doing this.

The only similarity between all the machines on the network was the Operating System, Microsoft Windows XP Professional. If Microsoft Live Update were the cause, it would have obtained the Proxy settings from Internet Explorer connection settings. Therefore, it would have detected the Proxy server and would not have attempted a direct connection to the Internet, which is what was happening. Unless, Internet Explorer did not have its proxy settings properly set. Namal got back to us with some interesting information, which reinforced the previous point. He had observed that there were requests to the Microsoft site being generated by the Security Consultant's machine in the network. This indicated that his Internet Explorer settings may be in error.

To verify our suspicions, we asked Namal to monitor a personal firewall log to identify which application was launching the connection request. We asked him to run a sniffer concurrently on the same machine. He then sent us the personal firewall log and the sniffer output.

Analysis of the Sniffer output showed there were attempts to send ACK packets to the outside IP Address by the Host machine, which were blocked by the Firewall, which in turn responded by sending a RESET packet back to the Host machine. But, the personal firewall log showed a regular output of ACK packets. The machine was running Symantec Anti Virus software. Live Update of Symantec was trying to connect to the outside IP Address using different ports. Could this really be the cause?

But, the Security Consultant was using AVG.

Namal had a chat with the Security Consultant, and he had said that he is used the internet facility in his hotel room to update his Anti Virus. So, his AVG was also configured to download updates without a proxy.

Wrapping things up

Now, we knew the cause. The ***Live Update*** of the Anti Virus programs trying to connect to the AKAMAI hosting servers to obtain updates. Since it was not aware of the presence of the proxy server, the connection requests were intercepted and blocked by the Firewall, and so appeared on the blocked connections list in the Firewall Log.

Furthermore, our separate investigation of the Outside IP Addresses which connection attempts were being made to, also revealed IP address ranges registered to companies other than AKAMAI Technologies. We found links between AKAMAI and those companies, which were mostly AKAMAI partners, who resell or redistribute AKAMAI services. While this information did not form the backbone of the investigation, it helped to corroborate our "Agent Theory". AKAMAI technologies hosts rich web content, such as images, files, in a geographically distributed server network, which allows web browsers to download those components from the nearest available servers, thereby improving download times. Many popular sites such as Yahoo! and MSNBC also employ AKAMAI servers to host their website's graphic components, files, etc.

Finally, we recommended that Namal change the settings in the Symantec and AVG Live Update programs to use the Proxy Server. The Security Consultant's had configured his Firefox Browser with the proxy settings. But, his Internet Explorer did not have the proxy settings configured. Applications like Microsoft Live Update use the Internet Explorer settings as a default for their own connections, and therefore, missed the Proxy Server. Once the Internet Explorer connection settings were changed to use the Proxy Server, the requests generated to Microsoft by Live Update were also stopped.

Case Closed.