Signature report

1. "ICMP PING" (icmp), Count: 1627, Unique sources: 592, Sid: 384

* This is a signature for every ICMP ping request.

2. "PSAD-CUSTOM Nachi worm reconnaisannce" (icmp), Count: 1575, Unique sources: 587, Sid: 100209

* The Nachi worm attacks windows 2000 and windows xp that don’t have the MS03-026 vulnerability patch. It creates an initial ICMP packet that is 92 bytes, which makes them easy to detect with the criteria of ip\_len = 92.

3. "PSAD-CUSTOM Slammer communication attempt" (udp), Count: 244, Unique sources: 159, Sid: 100208

* This is the Sapphire worm. It can be easily identified with 2 factors, UDP port 1434 and IP len of 404.

4. "MISC Windows popup spam attempt" (udp), Count: 241, Unique sources: 19, Sid: 100196

- A scam popup saying that the computer is infected with a virus and usually makes the user call a phone number to remove the “virus” and get scammed out of money. It is typically found utilizing UDP port 1026.

5. "PSAD-CUSTOM Kuang2 virus communication attempt" (tcp), Count: 142, Unique sources: 2, Sid: 100206

- This is a very serious virus. Kuang2 the Virus is a program that infects all the executables on the system, as well as set up a server that allows the remote control of the computer. The client program allows files to be browsed, uploaded, downloaded, hidden, etc on the infected machine. The client program can also execute programs on the remote machine. It also has plugins that can be used that allows the client to do things to the remote machine, such as hide the icons and start menu, invert the desktop, pop up message windows, etc. It generally uses TCP port 25.

6. "MISC Microsoft SQL Server communication attempt" (tcp), Count: 52, Unique sources: 2, Sid: 100205

- This is generally a sign of SQL injection attack. It has SYN flags and will be on Destination port 1433.

7. "BACKDOOR typot trojan traffic" (tcp), Count: 15, Unique sources: 2, Sid: 2182

* This is Trojan.Linux.Typot is a trojan horse that affects Linux systems. It generates TCP packets with a window size of 55,808. There are 4 functions of this. Every second, Trojan.Linux.Typot sends a spoofed TCP packet on the network. The source and destination IP addresses of the packet are randomly picked. The packet has some fixed characteristics, including the TCP window size, which is set to 55,808.. Trojan.Linux.Typot attempts to browse network traffic, watching for packets that have a TCP window size of 55,808. When such a packet is detected, Trojan.Linux.Typot creates a filename, "r," in the current directory. Every 24 hours, Trojan.Linux.Typot checks whether the "r" file has been created. If this is the case, the Trojan attempts to connect to a fixed IP address (probably a machine that the author of the Trojan controls) on port 22/tcp (the SSH port). If the connection succeeds, Trojan.Linux.Typot deletes the file, "/tmp/.../a," and exits. The deleted file may be the Trojan executable itself.

It is statically linked against the libnet and libpcap libraries, which it uses to forge and capture network traffic. The Trojan is also encrypted with the cryptelf utility.