

## **SIG^2 G-TEC Labs Honeynet Project (Singapore) Bi-Yearly Honeynet Alliance Report**

Written in May 2007 by - Cecil Su (Director, SIG^2 G-TEC Labs) - Vijay Vikram (Deputy Director, SIG^2 G-TEC Labs)
---

### **1.0 Deployments**

#### *1.1 Current technologies deployed*

In addition to the operational honeynets deployed (ref: April 2006 bi-annual report), the current hardware capacity of 5 server blades and 2 x switches, we have another 4 test servers and an image server setup in our test lab dedicated for the purpose of testing and a future GDH node.

- 1) Image server (where images are backed up to or restored from)
- 2) Honeywall/Sebek test server
- 3) Honeypots (virtual PC-based)
- 4) Nepenthes
- 5) Honeyd

The switches connects up the ImageNET and TestNET.

#### Data Control and Capture

The last version of the publicly-available Honeywall cdrom (roo hw1.0-189) is installed on the operational. Sebek is installed to enhance the monitoring of hacker activities beyond captured honeynet traffic at the honeywall.

#### Data Analysis

In the production zone, all intrusion attempts are parsed through a script and then sent back to another server which performs the automated incident reporting.

Walleye and CLI commands is used extensively to analyze data.

#### *1.2 Activity timeline*

The current interest of the group is to have a GDH node up and running in the second quarter of 2007. A site has been identified at the National University of Singapore and we are now in discussions with another tertiary institution to try and obtain another second GDH node.

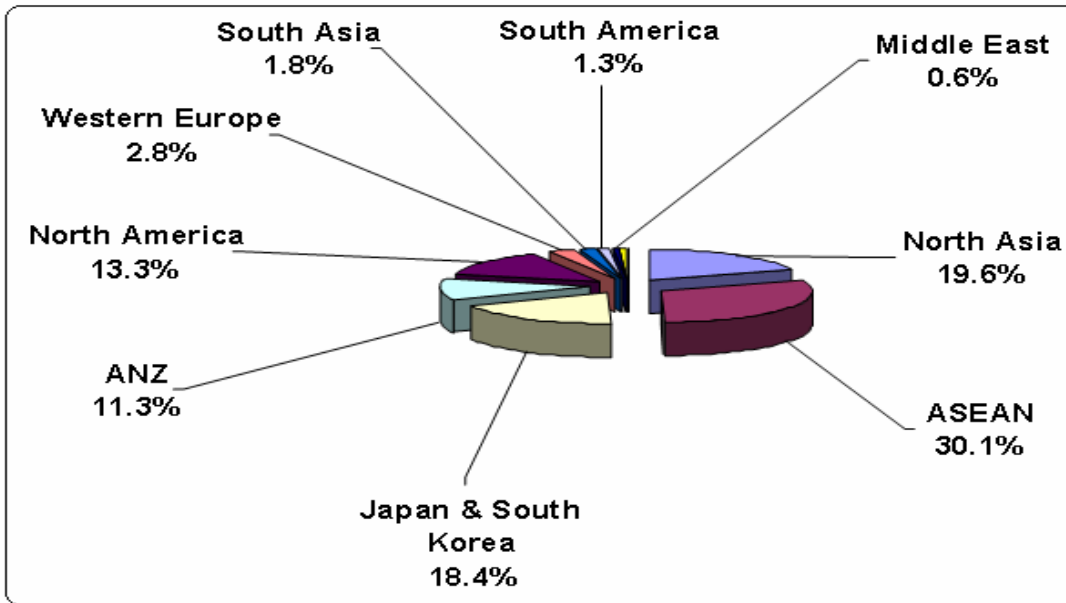
### **2.0 Findings**

#### *2.1 Highlight any unique findings, attacks, tools, or methods*

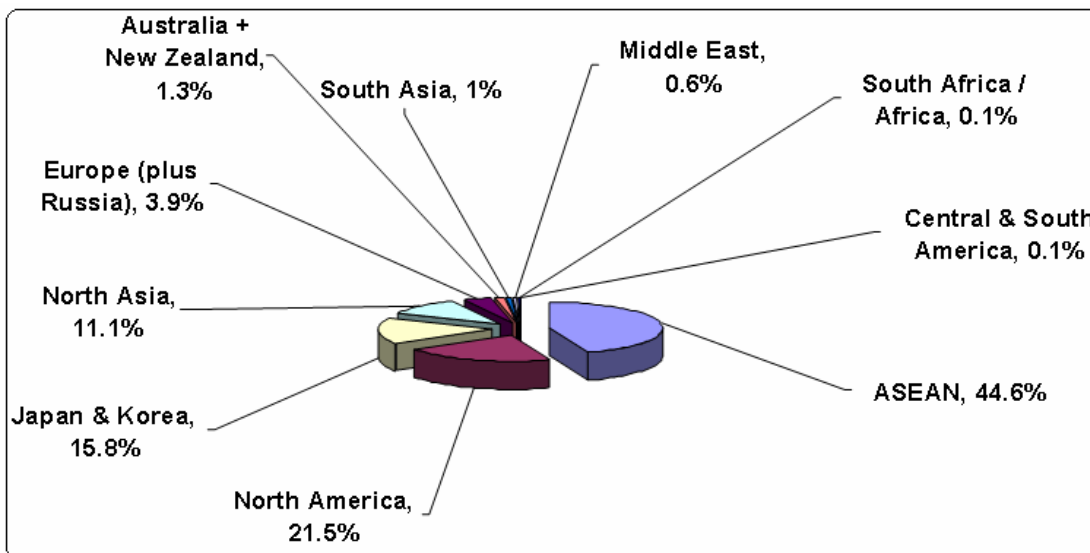
Looking at the top 5 TCP attacks, the top intrusions are HTTPS attacks, RPC (port 111) enumeration, a large number of scans on port 8080, malformed HTTP requests, Win32 TCP print service DoS attempts, and WebDAV search accesses.

Concerning the top 5 UDP attacks, most of them are basically spoofed IP addresses performing Windows messaging service spams which mostly comprise of illicit scams. The highest numbers of ports targeted at this range are 53, 138, 1434, 38293, and 32769.

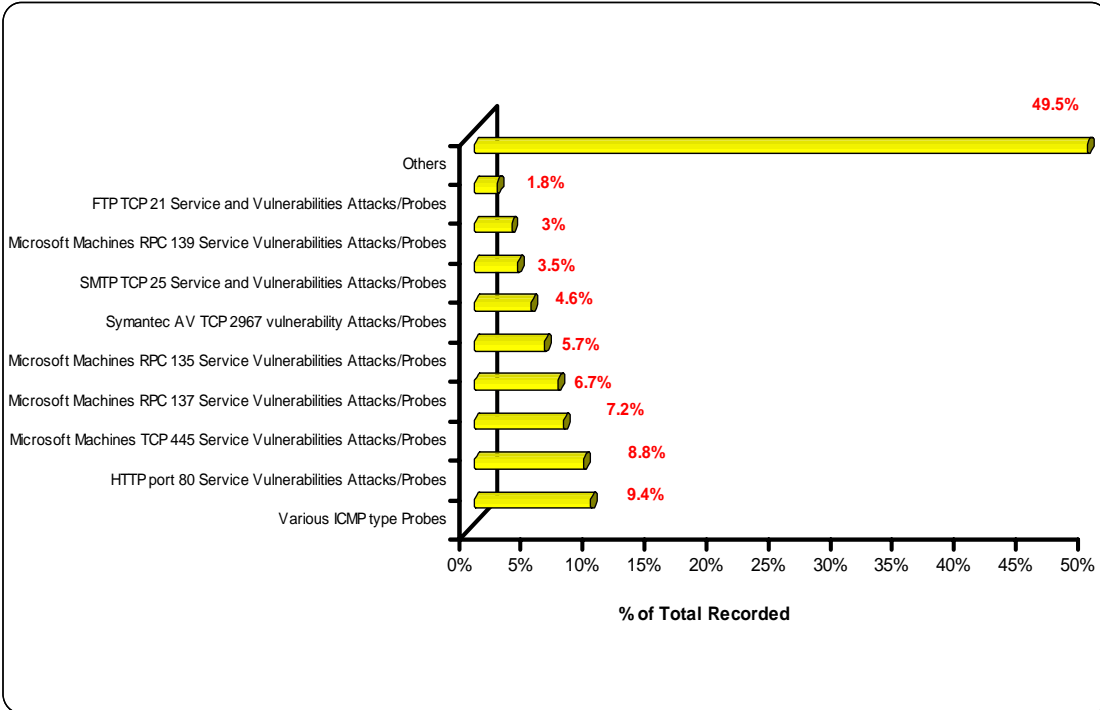
Most of the ICMP traffic we get are ICMP Destination Unreachable Communication prohibits with varying request sizes which are characteristic of the type of tool used to generate the ICMP traffic.



Top Originating Attack Sources (aggregated over 12 months) April 2006- April 2007



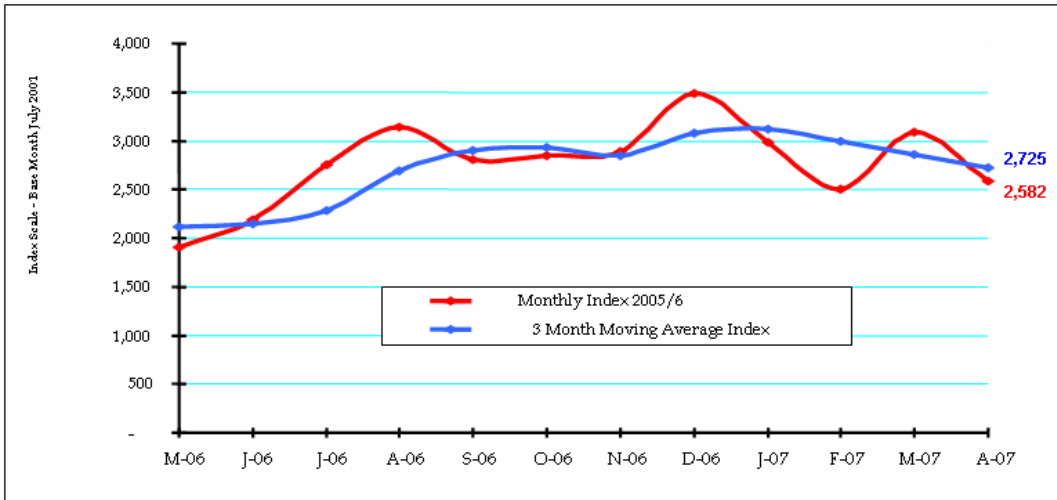
Top Originating Attack Sources (April 2007)



**Top 10 Attack Types (April 2007)**

*2.2 Any trends seen in the past six months*

The number of attacks appear to fluctuate over the last quarter (4 months back). Index is based on April data collected.



12 Month High: 3489 (Dec '06)  
 12 Month Low: 1904 (May '06)

12 Month Median: 2829  
 12 Month Mean: 2765

*2.3 What are you using for data analysis? What is working well, and what is missing, what data analysis functionality would you like to see developed?*

The following tools are used:

- Walleye
- Sbk\_extract
- Tcpdump
- NetDude
- Wireshark
- Chaosreader
- Custom-modified walleye.pl scripts to sanitize traffic
- Custom-created reporting scripts to perform incident reporting of external intrusions

Walleye and tcpdump are great tools. Customized walleye.pl performs analysis really well.

### **3.0 Lessons learnt**

*3.1 What positive things can you share with the community, so they can replicate your success.*

It is imperative for volunteers to be passionate about information security and specifically in this case, honeynet technologies. We try to meet at least once a month to share and gather information. University collaboration is one of the best ways to get good lab resources (e.g. space, utilities, infrastructure etc).

*3.2 What mistakes can you share with the community, so they don't make the same mistakes.*

1. Understand and improve data analysis knowledge before deployment
2. Maintaining / tracking all logs and data. Possibly automate the process for later analysis
3. Incident response plan to be worked upon for emergency situations

### **4.0 New tools**

*4.1 What new tools or technology are you working on?*

The SoHo Honeypot project is in the testing stage with nepenthes being added to the OpenWRT firmware. The project was stalled for a while due to time constraints and the fact that OpenWRT which is the base of the project had undergone a major redesign last year. In order to provide low-interactive honeypot capabilities, the team is working on the re-direction of dropped packets but routing, VPN and TTL issues remained to be solved.

*4.2 Would you like to integrate this with any other tools, or you looking for help or collaboration with others in testing or developing the tool?*

Most definitely. We are always open for further collaboration with other Alliance members.

### **5.0 Papers and presentations**

*5.1 Are you working any papers to be published, such as KYE or academic papers?*

None at the moment. We are interested in joint-collaboration papers and/or are planning to come up with a paper this year by the group.

*5.2 Are you looking for any data or people to help with your papers?*

The respective principal investigators will approach the alliance through alliance representatives should help be needed.

*5.3 Where did you publish/present honeypot-related material?*

The NUS Honeynet is part of the SIG<sup>2</sup> G-TEC Labs Honeynet Alliance which is part of Honeynet Project's Research Alliance.

18<sup>th</sup> Annual FIRST Conference Baltimore, Maryland –  
**A Strategy for Inexpensive Automated Containment of Infected or Vulnerable Systems**  
*(presented by Steven Sim)*

Link: <http://www.first.org/resources/papers/conf2006.html>

## **6.0 Organisational**

*6.1 Changes in structure of organization*

There are minimal changes. The SIG<sup>2</sup> Labs Honeynet Project is known as the SIG<sup>2</sup> G-TEC Labs Honeynet Project because the name of G-TEC is better known locally.

Principal Investigators (PIs):

Honeywall: Vijay Vikram  
Sebek: Royston  
Honeypots: Alvin Ho  
Mwcollect: Christopher Lek  
Honeymole: Rick Zhong  
SoHo Honeypot: Michael Boman

*6.2 Your feedback on Alliance activities.*

So far the activities that were conducted within the SIG<sup>2</sup> G-TEC Labs were very much beneficial to the local INFOSEC scene. This is especially so when the local government and organizations are all gearing towards a more information-assured society. The goals and direction of the alliance provide a good baseline and balance towards greater awareness in general and focused research of blackhat activities for defense-in-depth purposes. We are trying to see how we can fit in the new restructuring of the Alliance.

*6.3 Any suggestions for improving the alliance.*

We felt that there should be more collaboration between honeynet alliance within a particular zone or continent and then once that is achieved, a connected "grid" of honeynets to provide an early warning system can be achieved.

## 7.0 Goals

### *7.1 Which of your goals did you meet for the last six months?*

During the analysis of the intrusion attempts and attacks in our honeypots since mid last year, we had realized the importance of vulnerability research. As a result of this, we have been organizing monthly Vulnerability Research workshop sessions in the Singapore Polytechnic.

### *7.2 Which of your goals did you not meet for the last six months?*

We had wanted to be one of the beta-testers for the GDH node but getting consensus and approvals (ie., red tapes) proved to be a real challenge.

### *7.3 Goals for the next six months*

We hope to be running more honeynet-related initiatives in our lab. Besides that we hope to be able to launch one or possibly two GDH nodes in this part of the region.

Besides the above, we would also be aiming more specifically the goals below:-

1. Get more active members in the project
2. Write KYE papers
3. Publishing basic attack statistics in the website
4. To spend value time on Research and development in malware capture and analysis to be integrated with the nepenthes

-END-