

# Indian HoneyNet Project

## HONEYPOT & MALWARE ANALYSIS

**Sponsored By**



**N I I**  
**Consulting**  
An ISO 27001 Company

## DOCUMENT DETAILS

### DOCUMENT VERSION CONTROL

<b>DOCUMENT TITLE</b>	Honeypot & Malware Analysis Report
<b>DOCUMENT ID</b>	NII/IHP/report/001
<b>DOCUMENT VERSION</b>	Version 1.0
<b>PREPARED BY</b>	Wasim Halani
<b>REVIEWED BY</b>	K. K. Mookhey
<b>EFFECTIVE DATE</b>	Jul. 23, 09

### DOCUMENT SUBMISSION DETAILS

<b>DATE</b>	23 JULY 2009
<b>CLASSIFICATION</b>	Highly Confidential
<b>DOCUMENT TYPE</b>	Report
<b>SUBMITTED TO</b>	India HoneyNet Project
<b>DESIGNATION</b>	
<b>ADDRESS</b>	
<b>CONTACT NUMBER</b>	
<b>E-MAIL</b>	

### DOCUMENT CHANGE CONTROL

Issue Date	Version	Description	Requested BY	Changed By	Approved By

### DOCUMENT DISTRIBUTION LIST

Sl. No	Name	Organization	Purpose
01.	Wasim Halani	NII Consulting	Document Preparation
02.	K. K. Mookhey	NII Consulting	Document Review
03.		India HoneyNet Project	Document Appraisal and Acceptance

## NOTICE

This document contains information which is the intellectual property of Network Intelligence (India) Pvt. Ltd. (also called NII Consulting). This document is received in confidence and its contents cannot be disclosed or copied without the prior written consent of NII Consulting.

Nothing in this document constitutes a guaranty, warranty, or license, expressed or implied. NII Consulting disclaims all liability for all such guaranties, warranties, and licenses, including but not limited to: Fitness for a particular purpose; merchantability; non infringement of intellectual property or other rights of any third party or of NII Consulting; indemnity; and all others. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of NII Consulting.

NII Consulting retains the right to make changes to this document at any time without notice. NII Consulting makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

### Copyright

Copyright. Network Intelligence (India) Pvt. Ltd. All rights reserved.

### Trademarks

Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

## NII CONTACT DETAILS

Name	Wasim Halani
Title	Security Analyst
Company	Network Intelligence (India) Pvt. Ltd.
Address	204-Ecospace, Mogra Village, Off Old Nagardas Road, Andheri(E), Mumbai-400069
Tel. No	+91 22 28392628
Mobile No	+91 9819643034
E – Mail	<a href="mailto:wasim.halani@niiconsulting.com">wasim.halani@niiconsulting.com</a>

## Contents

1	INTRODUCTION .....	5
2	SETUP .....	5
3	PRECAUTION .....	5
4	INSTALLATION .....	5
5	CONFIGURATION.....	5
6	STARTING NEPENTHES .....	6
7	THE ANALYSIS.....	6
8	CONCLUSION.....	9
9	REFERENCE.....	9

## 1 INTRODUCTION

Based on the ongoing research, we obtained quite a few malware samples from the wild web using a malware-capturing Honeypot called “**Nepenthes**”. Of these, an executable file named ‘**msnnger.exe**’ was selected for further analysis.

## 2 SETUP

We initially, started the project looking for software-based honeypots. The applications could be categorized into Windows and Linux applications. Also, based on their interaction with the malware/attacker, they can be classified further into Low-interaction and High-interaction.

Since, this was our first step into malware research, we decided to go one step at a time. Hence, it was decided that we opt for a Low-interaction software based Honeypot. We kept our options open as far as the OS was concerned.

A few applications that we found were:

- Honeyd
- WinHoneyd
- Honeybot
- Multipot
- **Nepenthes**
- Honeywall

We selected the ‘Nepenthes’ application as it acted as Honeypot and also provided a Malware-collection and Analysis feature.

## 3 PRECAUTION

To prevent infection of systems (worst-case scenario) on our network we decided to use a Datacard to provide ‘direct’ internet connectivity. The Linux system was setup as a Virtual Machine.

## 4 INSTALLATION

Our Honeypot was built using a virtual Ubuntu system with 256 MB of RAM. We download the Nepenthes application from the Ubuntu repository itself using the command

```
# sudo apt-get install nepenthes
```

## 5 CONFIGURATION

To utilize the optional analysis feature, we need to modify the ‘conf’ file in Nepenthes as mentioned below.

We edit the file /etc/nepenthes.conf. Uncomment the following lines.

```
“submitfile.so”,      “submit-file.conf”  
“submitnorman.so”,   “submit-norman.conf”  
“logdownload.so”,    “log-download.conf”
```

Also change the replace\_local\_ip to **0**

Corresponding changes need to be made in submit-norman.conf file. The submit-file.conf is used to store the path where the malware binaries will be stored. In the submit-norman.conf file, we need to uncomment the email and URL links. Enter a valid email address, where the analysis results should be mailed.

## 6 STARTING NEPENTHES

Once the configuration has been setup, we simply restart the nepenthes service

```
# /etc/inint.d/nepenthes restart
```

Nepenthes opens up several ports on the system, where it waits for a malware to come knocking.

To collect a larger sample, we left the honeypot system working over a few days, while monitoring the malwares being captured frequently. Nepenthes automatically sends the malware binaries for analysis to the configured URLs. The analysis reports are mailed to us a few days later, depending on the resources available at the server.

An interesting malware binary we captured was the ‘msnnger.exe’.

## 7 THE ANALYSIS

This binary size was **419 KB**. On VirusTotal 34 out of 40 antivirus programs detected it as a malware, mostly as a **SdBot** or **RBot** (<http://www.virustotal.com/analysis/8e27047decb22e9017b94331ec3a5d0b>)

The malware was found to be packed using the **Themida** packer. Themida is a commercial packer, apparently popular in China, which supports many advanced features such as anti-debugging and virtual machine detection. Newer versions claim to support anti-dumping as well to prevent another program from dumping the unpacked executable from memory while the program is running.  
( <http://isc.sans.org/diary.html?storyid=1871> )

This prevented us from actually running the malware to analyze it’s working. But the Nepenthes analysis report was available to us from which we present some interesting results.

A brief summary of the malware’s activities on a Windows system is shown below:

Open File: C:\WINDOWS\system32\KERNEL32.dll (OPEN\_EXISTING)

Open File: C:\WINDOWS\system32\USER32.dll (OPEN\_EXISTING)

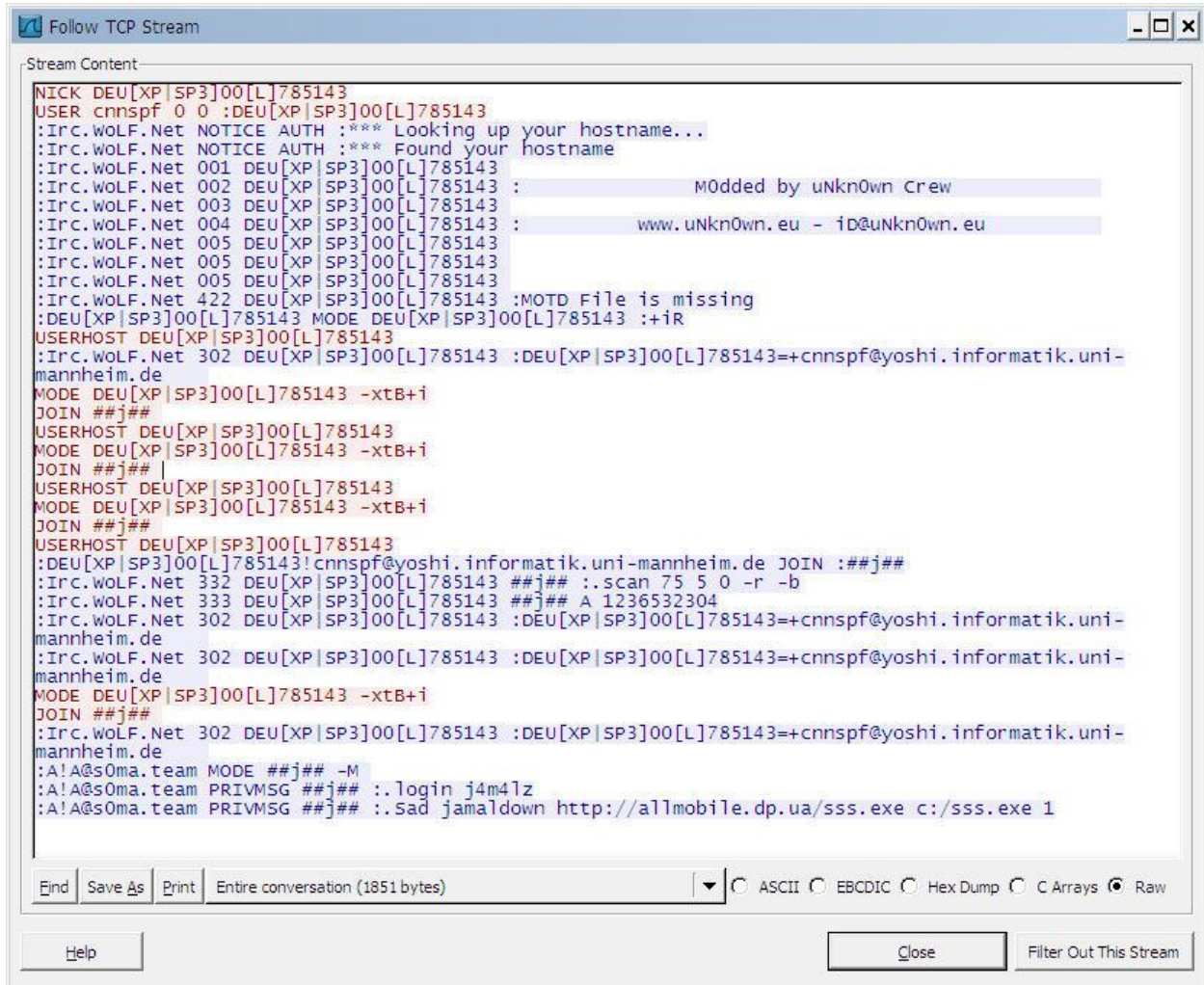
Open File: C:\WINDOWS\system32\ADVAPI32.dll (OPEN\_EXISTING)

Open File: \\.\PIPE\lsarpc (OPEN\_EXISTING)  
Create/Open File: \Device\Tcp (OPEN\_ALWAYS)  
Create/Open File: \Device\Ip (OPEN\_ALWAYS)  
Create/Open File: \Device\Ip (OPEN\_ALWAYS)  
Open File: \\.\Ip (OPEN\_EXISTING)  
Get File Attributes: C:\WINDOWS\system32\msnnger.exe Flags: (SECURITY\_ANONYMOUS)  
**Copy File: c:\nepenthes-5a0ecf35530d52136c7e353ee9ebobf9-msnnger.exe to  
C:\WINDOWS\system32\msnnger.exe**  
Open File: C:\WINDOWS\explorer.exe (OPEN\_EXISTING)  
Open File: C:\WINDOWS\system32\msnnger.exe (OPEN\_EXISTING)  
Set File Time: C:\WINDOWS\system32\msnnger.exe  
Set File Attributes: C:\WINDOWS\system32\msnnger.exe Flags: (FILE\_ATTRIBUTE\_HIDDEN  
FILE\_ATTRIBUTE\_READONLY FILE\_ATTRIBUTE\_SYSTEM SECURITY\_ANONYMOUS)  
Open File: C:\WINDOWS\AppPatch\sysmain.sdb (OPEN\_EXISTING)  
Open File: C:\WINDOWS\AppPatch\sysrest.sdb (OPEN\_EXISTING)  
Open File: \Device\NamedPipe\ShimViewer (OPEN\_EXISTING)  
Open File: C:\WINDOWS\system32\  
Find File: C:\WINDOWS\system32\msnnger.exe

It can be seen from the above listing that the malware copies itself to the 'system32' directory and changes it's attributes to that of a HIDDEN, READ-ONLY & SYSTEM file.

Another very interesting observation made by Nepenthes analysis was that this malware is actually an IRC Bot which tries to connect to the Command & Control center at **j4m4l.kuwaitarmy.net (88.208.209.151)** on port 1231.

Nepenthes also provided us with a PCAP file. Opening the file in Wireshark helped us fill in the gaps for the IRC analysis done by Nepenthes.



**Figure 1 : TCP Stream data of Network Activity of malware**

From the above screenshot we are able to obtain more information about the activities of the binary over the network.

The content in RED is from the victim to the C&C center, whereas the content in BLUE is issued from the C&C to the victim machine (client). An IRC bot is generally controlled remotely by a BOT Master using a IRC channel (they are unmoderated). This channel is the Command and Control center of the BOT master and all BOTs respond to commands sent from the C&C.

**Nickname: DEU[XP|SP3]00[L]785143**

**User: cnnsfp**

**IRC Server: irc.wolf.net**

A command to scan is being issued to the client: **scan 75 5 0 -r -b**

The BOT tries to connect to a domain **yoshi.infomatik.uni-mannheim.de**, which belongs to a University in **Germany** (most probably a PC or user account there has been infected).

The BOT is then directed to connect to a different link <http://allmobile.dp.au/sss.exe> using the username 'j4m4lz'. This binary is stored or most probably executed in **C:\sss.exe**. Interestingly, in the wireshark capture file we see that an initial DNS query has been made for the domain **j4m4l.kuwaitarmy.net** (which returned the IP address as **88.208.209.151**). The domain **kuwaitarmy.net** is hosted on the same IP as the forum of the previous domain **forum.allmobile.dp.ua**, at **82.80.252.205**. The binary sss.exe appears to have been removed.

3	2.124185	10.1.1.2	10.1.1.1	DNS	Standard query A j4m4l.kuwaitarmy.net
4	2.381356	10.1.1.1	10.1.1.2	DNS	Standard query response A 88.208.209.151

Figure 2 : DNS Request - Response Capture

## 8 CONCLUSION

We reached a dead-end after getting to this point as currently we are unable to bypass the virtual machine protection implemented by the packer and secondly, the binary seems to be calling a non-existent file. The article at SANS does mention a few workarounds which we could possibly try, but till then we will keep our honeypot up to capture new malware binaries.

## 9 REFERENCE

Nepenthes - Home

<http://nepenthes.carnivore.it/>

Using Nepenthes to discover Common Malware

<http://www.securityfocus.com/infocus/1880>

Virtual HoneyNet: A Scalable element of your Intrusion Detection/Prevention

[http://articles.techrepublic.com.com/5100-10878\\_11-6076871.html](http://articles.techrepublic.com.com/5100-10878_11-6076871.html)