

Indian Honeynet Project

NepenthesFE

Front-end to the Nepenthes Honeypot

Harsh R. Patel

7/21/2010



**NETWORK
INTELLIGENCE**
An ISO 27001 Company

Based on our previous project, the need for an analysis toolkit for Nepenthes was found which could automate some part of the static malware analysis of the malware captured using low interaction honeypot “Nepenthes”. This document is our review of the NepenthesFE tool, which we have upgraded as part of our study into Nepenthes and Visualization of Honeypot data.

Document details

Document Version Control

Document Details	
Document ID	NII/IHP/0710
Document Version	1.4
Prepared By	Harsh R Patel
Reviewed By	Wasim Halani
Approved By	K K Mookhey
Effective date	26-7-2010

Document Submission details

Date	26-07-2010
Classification	Public
Document Type	Report (Upgrade details)
Submitted to	Indian HoneyNet Project

Document Distribution List

Name	Organization	Purpose
Harsh R Patel	NII Consulting	Document Preparation
Wasim Halani	NII Consulting	Document Review
K K Mookhey	NII Consulting	Document Approval
	Indian HoneyNet project	Document Appraisal and Acceptance

NII Consulting 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
E – Mail	wasim.halani@niiconsulting.com

NepenthesFE v 0.4

Table of Contents

1 Introduction.....	4
2 Setup	4
3 About NepenthesFE.....	5
3.1 Features.....	5
3.2 Modules.....	5
3.3 Bugs Fixes.....	7
4 Screenshots of NepenthesFE.....	8
5 Future Work.....	18

1 Introduction

Continuing our research into honeypots (http://www.honeynet.org.in/reports/KK_Project1.pdf), we found a wonderful open source tool called **NepenthesFE**, which provides a front-end visualization to the data captured by the honeypot. The architecture of NepenthesFE allowed us to add new modules and visualization mechanisms of captured malware.

2 Setup

Initially we started out making our own analysis tool but after some research we found out various tools for analysis like:

- Surfids
- NepenthesFE

After evaluating both the options we found out that NepenthesFE satisfied our requirements of simplicity and scalability. Our setup was built using a single laptop on which we installed the Nepenthes honeypot and also configured NepenthesFE to listen on the loopback interface - using IPtables, MySQL and Apache.

3 About NepenthesFE

NepenthesFE is a front end module for Nepenthes honeypot originally developed by Emre Bastuz (info@emre.de). It helps in cataloging the malware collected using Nepenthes using **http-submit** module of Nepenthes. It receives the data from the Nepenthes and stores the information about the attack on to the MySQL database. It is customizable and hence modules and features can be added on to it. The basic structure of NepenthesFE is simple hence it is can be scaled over various types of implementation ranging from single honeypot to a honeynet.

Details of Features and modules of NepenthesFE (includes upgraded versions)

3.1 Features

The Features of NepenthesFE are:

- Features
V0.3
 - Fetch data from Nepenthes using HTTP-SUBMIT and store the details in the database.
 - Perform analysis based on modules and store the details.
 - Provide the UI for the collected information.
 - Give Statistical reports using RRD to generated statistics based on the attack vectors.
- V0.4
 - Afterglow
It's a set of scripts meant to generate dynamic graphs on to out of CSV file. This feature has been used in to the NepenthesFE module to generate graphs of IP targeting and ASN. The Tool uses data in CSV format to generate the graphs.
 - Google Maps
The Google maps API has been added using GeoIP data stored in the database and provides details of the attack based on sensor.

3.2 Modules

The modules of NepenthesFE are:

- V0.3
 - **ASN**
This module uses the DNS based autonomous system lookup service of the Team Cymru Project (<http://www.cymru.com/>). If an attack is reported by Nepenthes, this module will look up the ASN of the attacker IP and add this data to the database. The

- ASN module gives the direct links to Robtex and phish tank. *Visualization modules have been added.*
- **GeoIP**
This module uses the GeoIP service to determine the geographical location of an attacker by looking up the attacker's IP address in the GeoIP database.
 - **BitDefender**
This module uses the BitDefender AV scanner to locally scan the binary. If the binary is considered malicious, the result will be saved in the database.
 - **File**
This module executes the UNIX command "file" to determine the type of the caught binary.
 - **Objdump**
This module executes the UNIX command "objdump" to retrieve information specific to an executable
 - **Strings**
This module executes the UNIX command "strings" to extract the ASCII characters from the binary.
 - **UPX**
This module executes the UNIX command "upx" to determine if the binary has been packed with UPX
 - **VirusTotal**
This module sends the binary to "scan@virustotal.com" for further analysis. The NepenthesFE cron job checks a configured POP3 account for the analysis result from VirusTotal and saves it in the database.
 - V 0.4
 - **VirusTotal**
The module of VirusTotal has been reconfigured such that it provides dual methods to fetch information regarding a binary either using mail or via automated script from VirusTotal.
 - **Packer**
This module executes a script and gives the details of the packer used to pack the malware.
 - **PE Info**
This module executes a script and gives the PE Structure of the malware.
 - **Section**
This module executes a script and gives the Section and Entropy information of the PE based malware.
 - **ASN**
The ASN module has been upgraded by adding Visualization module using AfterGlow. The Links of Robtex and PhishTank have been added.

3.3 Bugs Fixes

The following bugs were fixed:

- Add user Variable.
- Add sensor Variable.
- Authentication of Cron.php

4 Screenshots of NepenthesFE

Main Page (list instances)


The screenshot shows the main page of the NepenthesFE web interface. At the top left is a logo of a Nepenthes (pitcher plant). At the top right are navigation links: Malware, Stats, Users, Reports, Geocode, Maps, Logout. Below the navigation is a table listing instances. The table has columns for Hash, Source IP, Target IP, Date, Country, and City. There are 8 rows of data, all showing source and target IPs from 115.240.163.X and dates from 2010-07-01. The country for all entries is India, and the city is Mumbai. Each row has a small 'x' icon in the rightmost column.

Hash	Source IP	Target IP	Date	Country	City
dc26cc0ff704bc0c839d8bc975597551	115.240.163.X	115.240.163.X	2010-07-01 12:31:39	India	Mumbai
4c9b9c89c491c9d9c9d1d9c491b9c49	115.240.163.X	115.240.163.X	2010-07-01 12:31:31	India	Mumbai
3b7d93b476Xcellfcb7cb737X1bb4db	115.240.163.X	115.240.163.X	2010-07-01 12:30:11	India	Mumbai
64571e507e4e40f93c6e10647f1e06	115.240.163.X	115.240.163.X	2010-07-01 12:27:20	India	Mumbai
64771e507e4e40f93c6e10647f1e06	115.240.163.X	115.240.163.X	2010-07-01 12:24:26	India	Mumbai
1c453be3c35c75d7ccca6e0b78e03ce	115.240.163.X	115.240.163.X	2010-07-01 12:19:35	India	Mumbai
fef04c51b13543b1db852936c6406aa0	115.240.163.X	115.240.163.X	2010-07-01 12:17:49	India	Mumbai
6c2e71c88c128df1401bac26154c148	115.240.163.X	115.240.163.X	2010-07-01 12:14:20	India	Mumbai
f1ba7117dbd421c949ba0b8e8e1194	115.240.163.X	115.240.163.X	2010-07-01 12:13:52	India	Mumbai

The Users Page

Username	Last Login  	Comment
admin	2010-07-08 12:30:45	Default Admin User
root	2010-06-11 12:03:05	sub Admin User

The Sensors Page

Name	Username	IP Address	Last Submission  	Comment
local_sys	root	127.0.0.X	2010-07-08 12:50:02	root

The Google maps visualization



The instance details

Details obtained from Nepenthes

Hash MD5	dc26cccff704bc0e8396bb0979557551	URL	http://hikmccnbnukaic.com/Kc/
Date of occurrence	2010-07-01 12:31:39	Sensor	Local Sys
E-Mail	abc@abc.com	Target IP Address	115.240.163.X
Source IP Address	115.240.163.X	Filename	v.exe
Trigger	generic url decoder.X		
Filetype	PE32 executable for MS Windows (GUI) Intel 80386 32-bit		
Hash SHA512	e9eud77afdc006c5046De16De6ad0f170dL0888L006954e9Cb22a070c0e94b547c4f4d2a8c02c6c		

GeoIP Details

Country	 India
City	Mumbai

Autonomous System Details

Autonomous System Number	217303
Network	115.240.123.0/17
IP Registry	apnic
Map of ASN	Link
Links to Robtex	ROBTEX LINKS
Links to Phish Tank	Phish Tank Links

Detail Sample and Modules

Details obtained from Nepenthes

Hash MD5	43b6bb86e341ad62fdf8c004206e8c36
Hash SHA512	63776c1a030576b8dedc755c515ce148152e8586bdeda1215edad2118702114c1ac07ded2a7439ca5214451d920c3a838fa8c
Last Seen	2010-07-01 12:31:43
Hitcount	1

Statistics 

Details from VirusTotal 

Results from :- 'strings' 

Results from :- 'upx' 

Results from :- 'objdump' 

Results from :- 'file' 

Results from :- 'peinfo' 

Results from :- 'section' 

Results from :- 'packerid' 

The detail module PEINFO

```

Results from :-'peinfo'

[['Microsoft Visual Basic v5.0'], ['Microsoft Visual Basic v5.0/v6.0']]
  DOS_HEADER

[IMAGE_DOS_HEADER]
e_magic:          0x5A4D
e_cblp:           0x90
e_cp:             0x3
e_crlc:           0x0
e_cpshdr:         0x4
e_minalloc:       0x0
e_maxalloc:       0xFFFF
e_ss:             0x0
e_sp:            0xB8
e_name:           0x0
e_ip:             0x0
e_cs:             0x0
e_itaric:         0x40
c_ovno:           0x0
e_res:            0x0
e_oemid:          0x0
e_naminfo:        0x0
e_res2:           0x0
e_lfanew:         0xB8

-----NT_HEADERS-----

[IMAGE_NT_HEADERS]
Signature:        0x4550

-----FILE_HEADER-----

[IMAGE_FILE_HEADER]
Machine:          0x14C
NumberOfSections: 0x3
TimeDateStamp:    0x4C22:BEE [Wed Jun 23 16:53:02 2010 UTC]
PointerToSymbolTable: 0x0
NumberOfSymbols:  0x0
SizeOfOptionalHeader: 0xE0
Characteristics:  0x10F
Flags: IMAGE_FILE_LOCAL_SYMS_STRIPPED, IMAGE_FILE_32BIT_MACHINE, IMAGE_FILE_EXEC

-----OPTIONAL_HEADER-----

[IMAGE_OPTIONAL_HEADER]
Magic:            0x103
MajorLinkerVersion: 0x6
MinorLinkerVersion: 0x0
SizeOfCode:       0x17100
SizeOfInitializedData: 0x3000
SizeOfUninitializedData: 0x0
AddressOfEntryPoint: 0x1FCC
BaseOfCode:        0x1000
baseOfData:        0x1800
ImageBase:         0x4000C0
SectionAlignment: 0x1000
FileAlignment:     0x1000
MajorOperatingSystemVersion: 0x4
MinorOperatingSystemVersion: 0x0
MajorImageVersion: 0x1

```

The Detail Sample Section, Entropy and packer information

Details obtained from Npenthesis

Hash MD5 43b6c088e341ad021c18c0J42Ute8C3b
Hash SHA512 63776c1a030576b8dedc755c515ee148152e8586bdada1215dad2118702114c1ac07ded2a7439ca5214451d920c3a938fa8:
Last Seen 2010-07-01 12:31:43
Hitcount 1

Statistics

Details from VirusTotal

Results from :- 'strings'

Results from :- 'upx'

Results from :- 'objdump'

Results from :- 'file'

Results from :- 'peinfo'

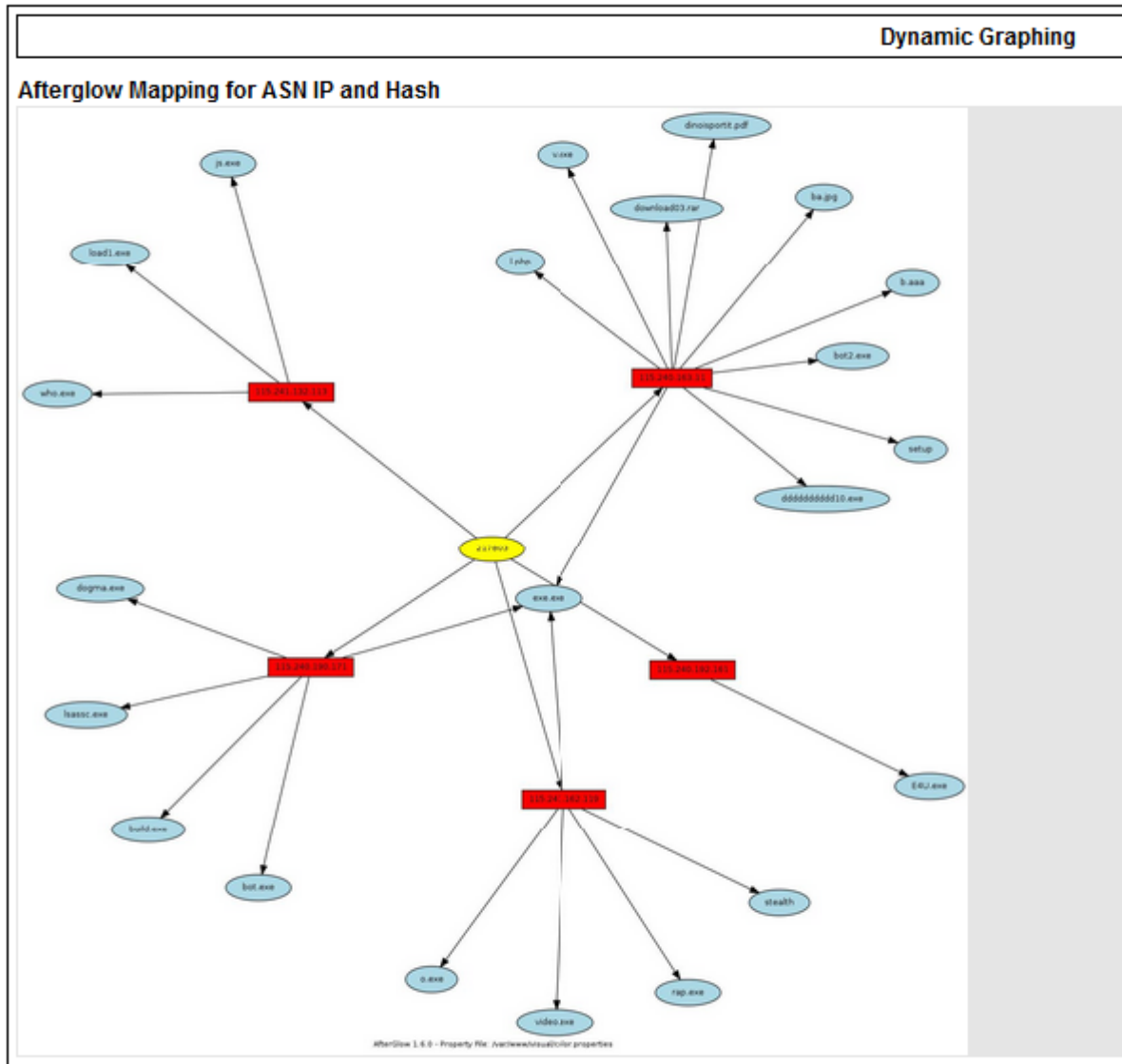
Results from :- 'section'

```
['Microsoft Visual Basic v5.0/v6.0']
-----
                        Section Information
-----
Section Name      Entropy
.txt&#0;4#0;6#0;      5.67836706919
.d&#0;4#0;6#0;      0.0
.rsrc&#0;4#0;6#0;    1.91633542382
```

Results from :- 'packerid'

```
['Microsoft Visual Basic v5.0/v6.0']
```

The afterglow based dynamic mapping based on ASN number



5 Future Work

Following is the list of work that can be done:

1. Integration of other nepenthes sensors.
2. Adding a malware Hash Search feature.
3. Visualizing structure of each malware.
4. Traceroute module can be added.

Emre Bastuz (info@emre.de) has graciously offered Network Intelligence to take over the project. We are glad to announce that henceforth we will be hosting the project on our website at <http://www.niiconsulting.com/nepenthesfe/> and any upgrades to the project will be added on our site. As this will remain an open-source project, we call forward volunteers to contribute new modules, bugs-fixes etc. to us at nepenthesfe@niiconsulting.com