DarkNOC

Dashboard for Honeypot Management

Bertrand Sobesto(1), Michel Cukier(1), Matti Hiltunen(2), David Kormann(2), Gregory Vesonder(2), Robin Berthier(3)

(1) University of Maryland, (2) AT&T Labs-Research, (3) UIUC.

Outline

- Honeypots overview
- DarkNOC
- Case study

Do you really want to manage your own honeypots? Join us instead.

Honeypots

- Highly monitored systems meant to attract attackers and analyze their behavior.
- Traffic observed on the honeypot network is considered malicious

- Different characteristics
  - Scale (local vs. distributed)
    - E.g., Leurre.com, Internet Motion Sensor, SGNET
  - Purpose (research vs. production)
  - Level of interaction (high vs. low)
    - Real OS + apps vs. emulated (e.g., Nepenthes, Dionaea, Honeyd)

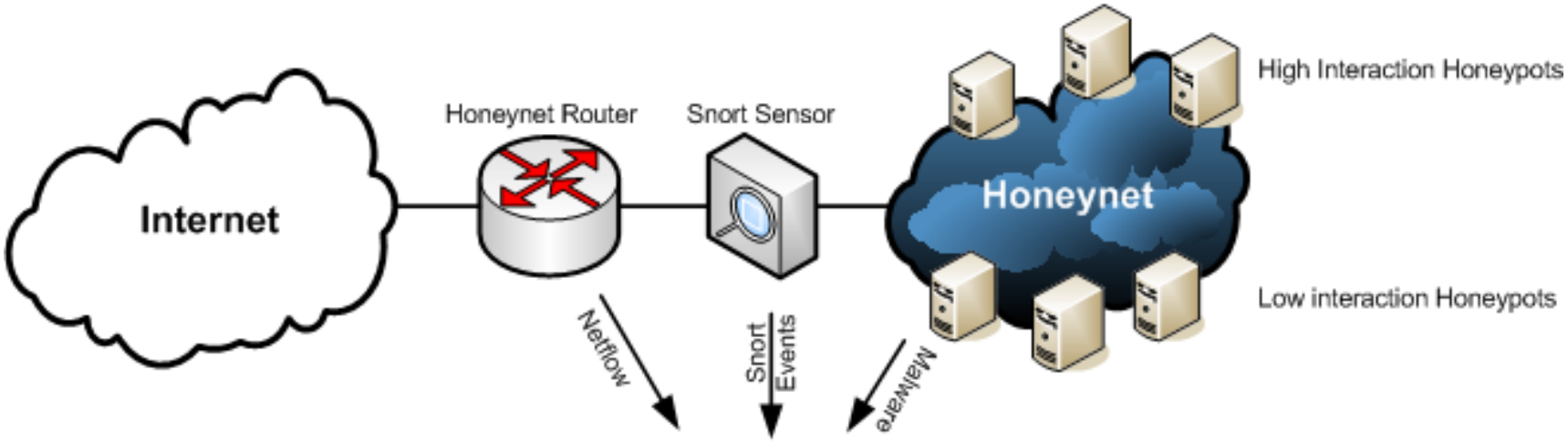
The Problems

- Distributed Honeypots can generate large volume of data
- Running high interaction Honeypots is risky as they can get compromised
- Network infrastructure can suffer from attackers' actions and needs to be monitored

DarkNOC

- DarkNOC (Darknet Network Operation Center) is a management and monitoring tool for complex honeynets
  - Support different types of honeypots (low and high interaction)
  - Support different data collection devices
  - Support both research and production
- Currently used to manage a honeypot network consisting of several subnets with hundreds of IP addresses.

System Architecture



DarkNOC's Web page

```
--------------- Analysis Report ---------------
Flow Time Window: 2011/06/06.06:00:00-2011/06/06.18:00:01
Number of hosts detected: 3
To access the online version of the report:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?report=263

xxx.xxx.xxx.xxx (X.umd.edu)
 - Number of flows: 1
 - Number of packets: 1
 - Number of bytes: 51
To visualize the flows:
   https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1124

yyy.yyy.yyy.yyy (Y.umd.edu)
 - Number of flows: 10
 - Number of packets: 10
 - Number of bytes: 1915
To visualize the flows:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1125

zzz.zzz.zzz.zzz (Z.umd.edu)
 - Number of flows: 10
 - Number of packets: 10
 - Number of bytes: 1915
To visualize the flows:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1126
```

DarkNOC's alert mail

Data sources

Netflow

```
Date flow start      Duration     Port  SrcIP:Port -> DstIP:Port           Packets Bytes Flows
2010-02-09 06:43:... 4294966.937  TCP   218.8.251.187:20347 -> x.x.x.x:80     2     94  1
2010-02-09 06:43:... 4294966.977  TCP   218.8.251.187:20347 -> x.x.x.x:80     2     94       1
```

Snort IDS events

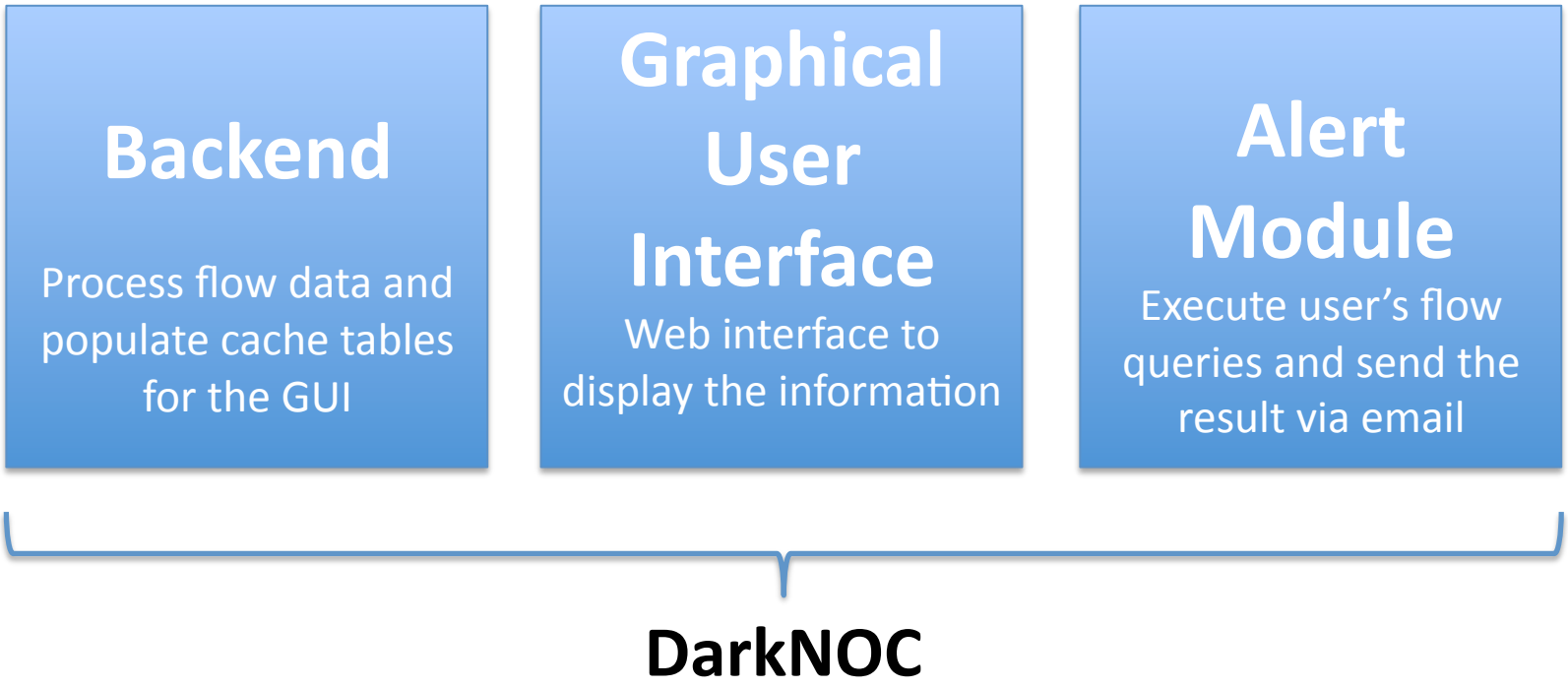
```
04/15-06:49:15.474819 [**] [1:12799:3] SHELLCODE base64 x86 NOOP [**]
   [Classification: Executable Code was Detected]... {TCP} a.b.c.d:15017 -> W.X.Y.Z.:80
04/15-06:49:15.474819 [**] [1:12802:3] SHELLCODE base64 x86 NOOP [**]
   [Classification: Executable Code was Detected]... {TCP} a.b.c.d:15017 -> W.X.Y.Z.:80
04/15-06:49:15.619028 [**] [1:12800:3] SHELLCODE base64 x86 NOOP [**]
   [Classification: Executable Code was Detected]... {TCP} a.b.c.d:15017 -> W.X.Y.Z.:80
```

Malware Collection

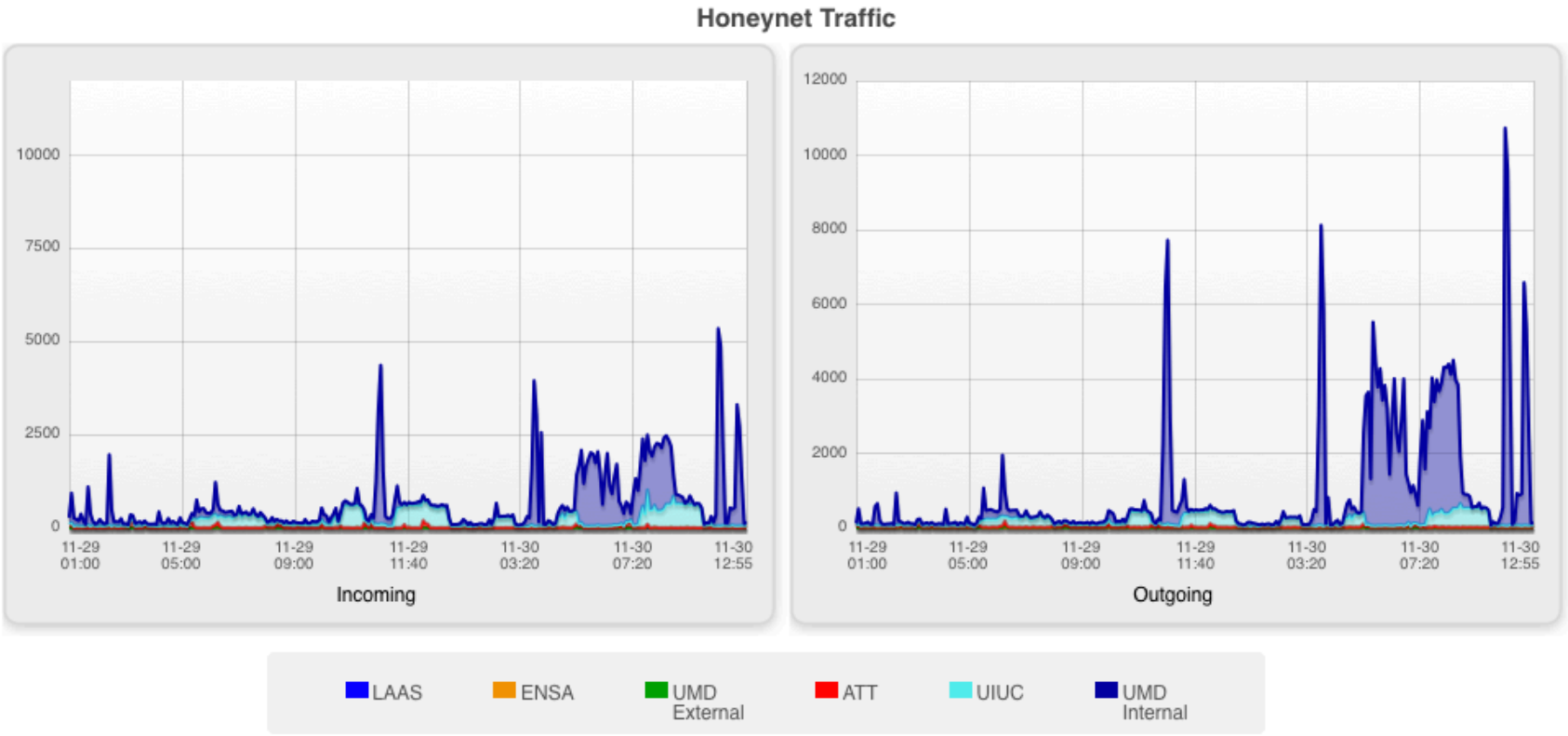
[2011-04-15T06:49:19] a.b.c.d-> W.X.Y.Z. ftp://1:1@a.b.c.d:21/Rewetsr.exe c511c4f9bdd3bb892e582fbc9a00da9c

Software Architecture

- Constraints
  - Easy to use (any web browser), intuitive.
  - Speed: User interface fast despite the volume of data
  - Data validity: Data displayed up to date even under high data volume.

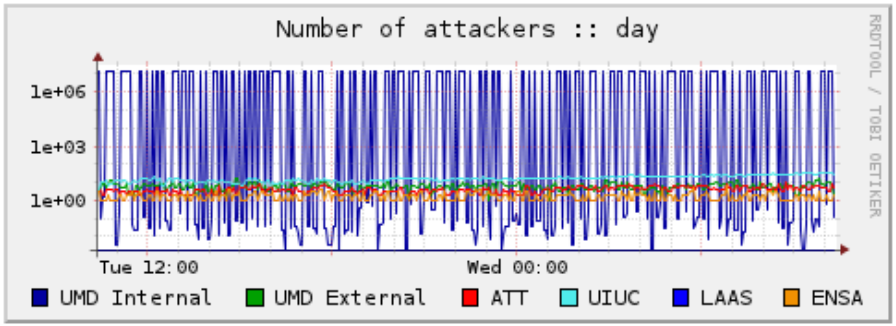


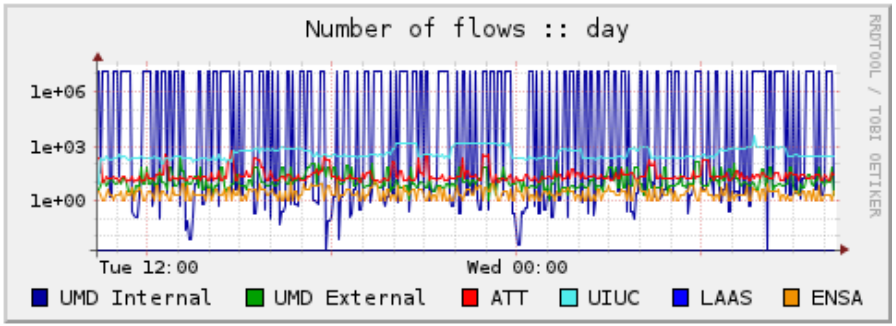
Graphical User Interface
Flows / subnet

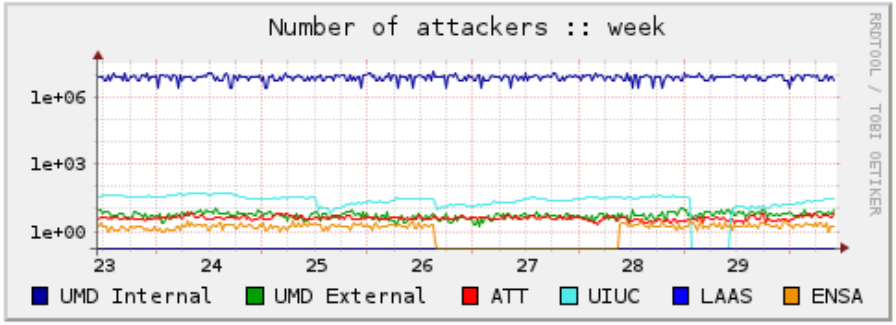


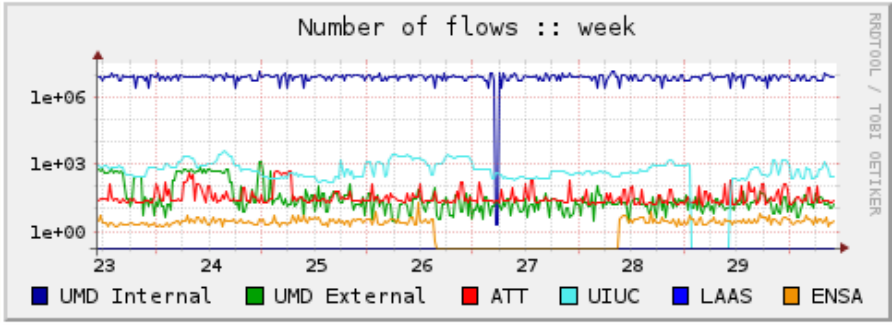
GUI: NetFlow Data

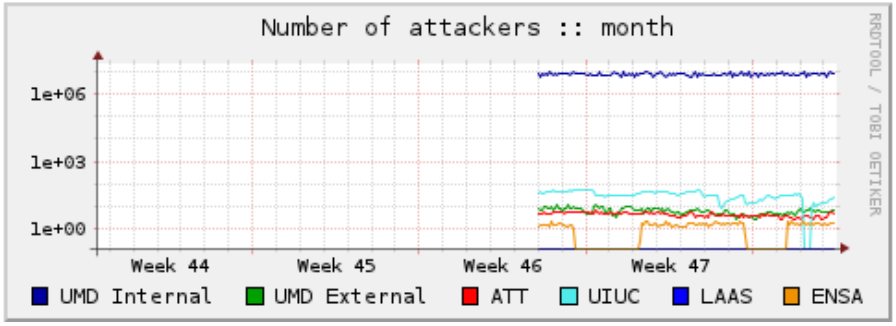
- RRD Graphs
  - Number of attackers
    - Number of unique external source IP addresses
  - Number of flows
  - Different scales: Day, week and month
  - Updated every 5 minutes by the backend program

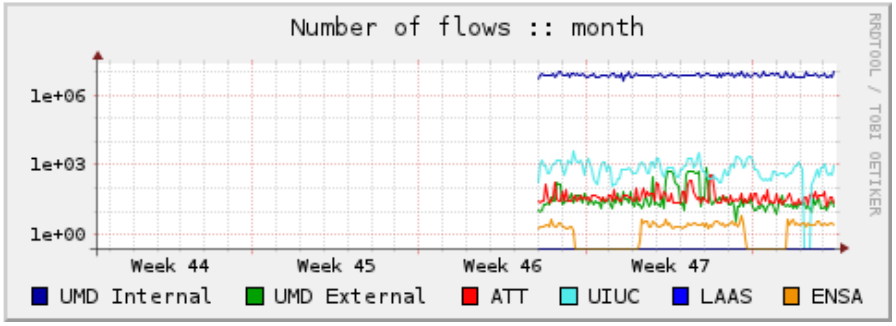

Number of attackers :: day
1e+06
1e+03
1e+00
Tue 12:00
Wed 00:00
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER


Number of flows :: day
1e+06
1e+03
1e+00
Tue 12:00
Wed 00:00
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER


Number of attackers :: week
1e+06
1e+03
1e+00
23
24
25
26
27
28
29
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER


Number of flows :: week
1e+06
1e+03
1e+00
23
24
25
26
27
28
29
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER

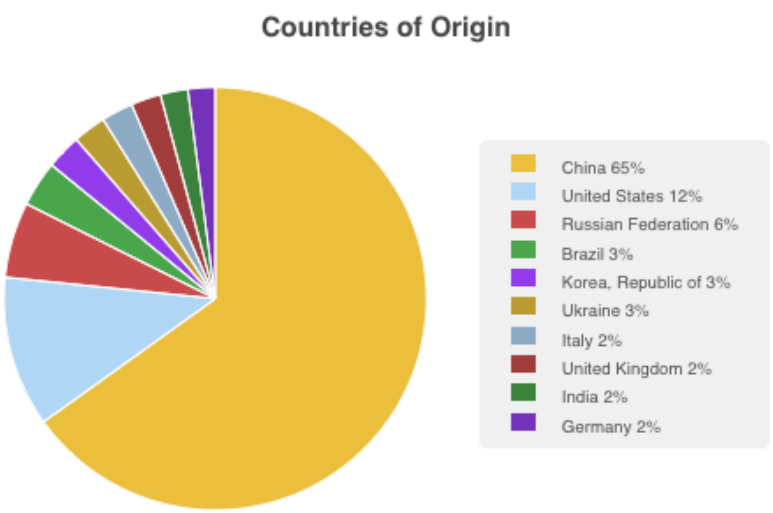

Number of attackers :: month
1e+06
1e+03
1e+00
Week 44
Week 45
Week 46
Week 47
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER


Number of flows :: month
1e+06
1e+03
1e+00
Week 44
Week 45
Week 46
Week 47
UMD Internal
UMD External
ATT
UIUC
LAAS
ENSA
RRDTOOL / TOBI OETIKER

GUI: More on NetFlow Data

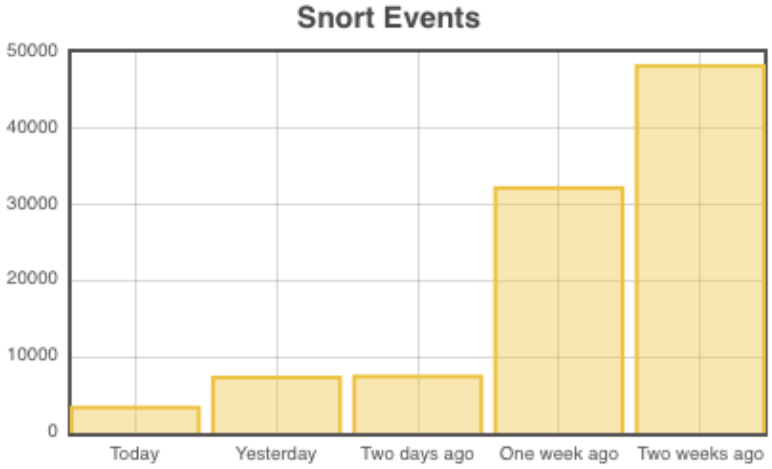
- Top and bottom targeted ports
- Top attackers, top targets
- Top origin countries

Top 10 Ports (last 24 hours)		Bottom 10 Ports (last 24 hours)		
Port Number		Protocol	Number	%
9999		TCP	3754849	0.21
6884		TCP	220386	0.01
1433		TCP	116115	0.01
22		TCP	27392	0
80		TCP	13718	0
6889		UDP	13541	0
8		ICMP	10105	0
8080		TCP	9445	0
8909		TCP	7919	0
9415		TCP	6008	0



GUI: Snort Events

- Number of Snort events
- Last 50 snort events (source and destination IPs hidden here).



Snort Last Events

Date	Event	Source	Destination
2011-11-30 09:36:17	POLICY VNC server response		
2011-11-30 09:29:14	P2P BitTorrent transfer		
2011-11-30 09:29:06	POLICY remote desktop protocol attempted		
2011-11-30 09:26:33	P2P BitTorrent transfer		
2011-11-30 09:26:33	P2P BitTorrent transfer		
2011-11-30 09:26:30	POLICY remote desktop protocol attempted		
2011-11-30 09:26:30	POLICY remote desktop protocol attempted		
2011-11-30 09:24:41	SPECIFIC-THREATS OpenSSH sshd Identical		
2011-11-30 09:24:41	SPECIFIC-THREATS OpenSSH sshd Identical		
2011-11-30 09:21:33	P2P BitTorrent transfer		

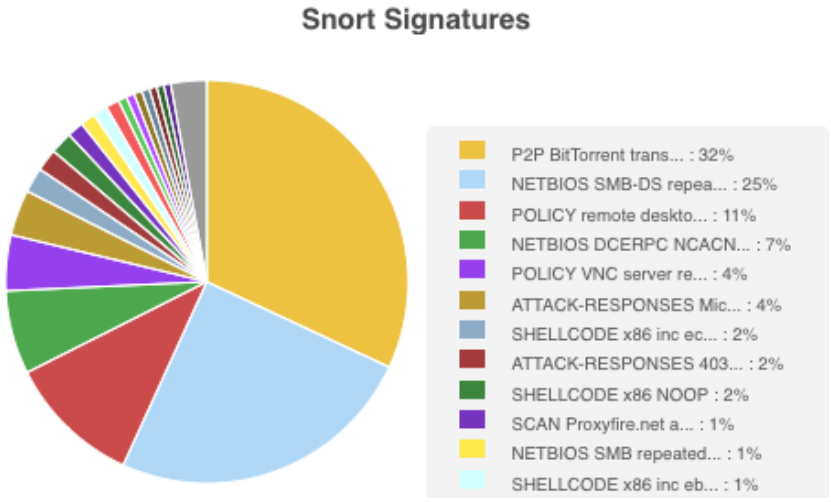
Page 1 of 3 20 View 1 - 20 of 50

GUI: More on Snort events

- Top 10 and bottom 10 snort signatures within the last 24 hours

Top 10 Signatures | Bottom 10 Signatures

Signature	Number	%
P2P BitTorrent transfer	170708	31.96
NETBIOS SMB-DS repeated logon failure	132791	24.86
POLICY remote desktop protocol attempted administrator connection request	57418	10.75
NETBIOS DCERPC NCACN-IP-TCP srvsvc NetrPathCanonicalize overflow attempt	35809	6.7
POLICY VNC server response	23827	4.46
ATTACK-RESPONSES Microsoft cmd.exe banner	19671	3.68
SHELLCODE x86 inc ecx NOOP	10721	2.01
ATTACK-RESPONSES 403 Forbidden	9585	1.79
SHELLCODE x86 NOOP	9489	1.78
SCAN Proxyfire.net anonymous proxy scan	7031	1.32



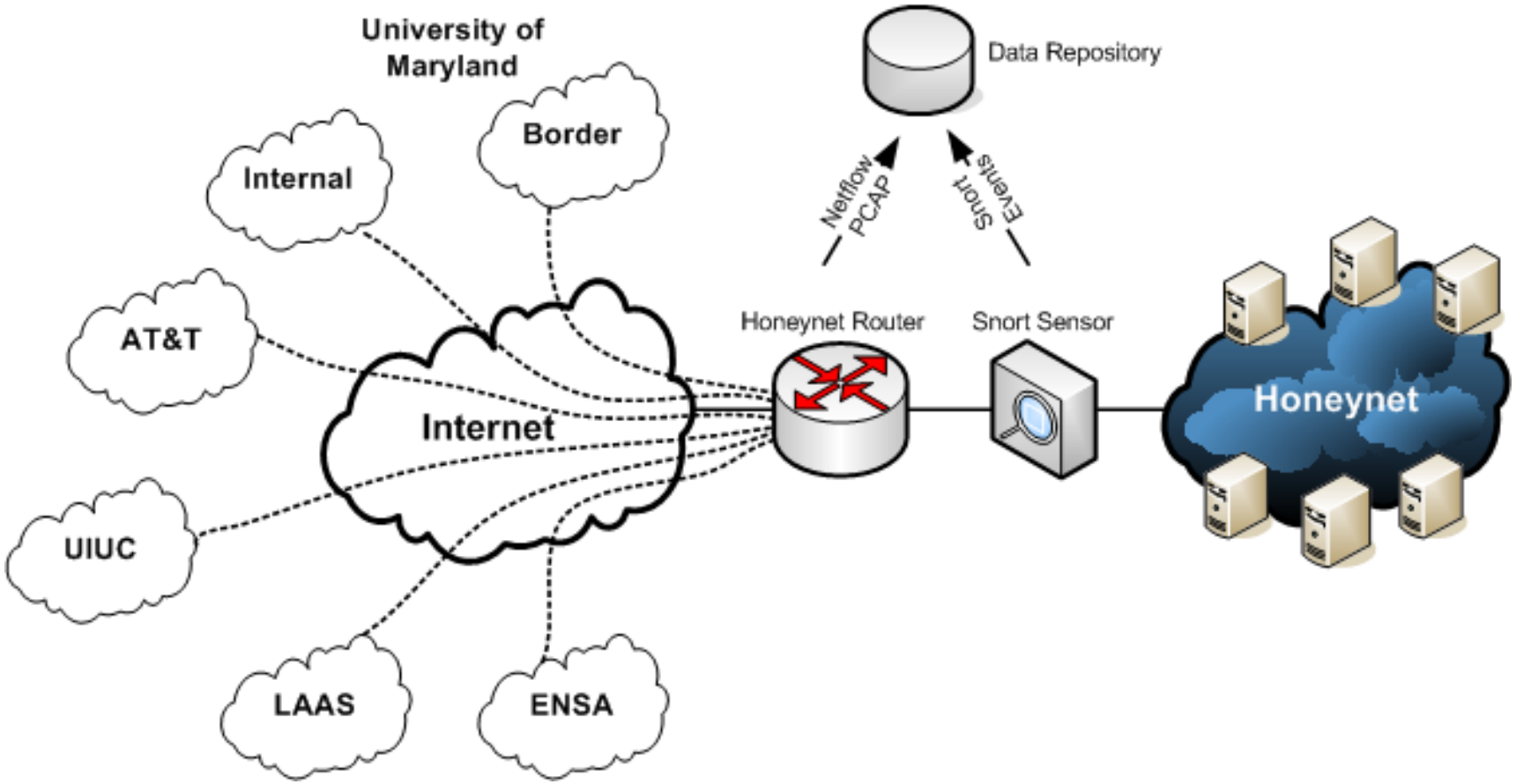
Case study: UMD Honeynet

- An infrastructure to support honeypot-based experiments
  - Provide data collection infrastructure (Flow, Snort and PCAP)
  - Controlled environment

- Currently about 2,000 IP addresses from 5 different institutions:
  - University of Maryland
  - AT&T
  - University of Illinois at Urbana-Champaign
  - “Laboratoire d’Analyse et d’Architecture des Systèmes” (LAAS) in Toulouse, France
  - “Ecole Nationale des Sciences Appliquées” in Marrakech

- The UMD Honeynet is hosted at the University of Maryland, traffic from other institutions is forwarded through a secured tunnel (Honeymole).

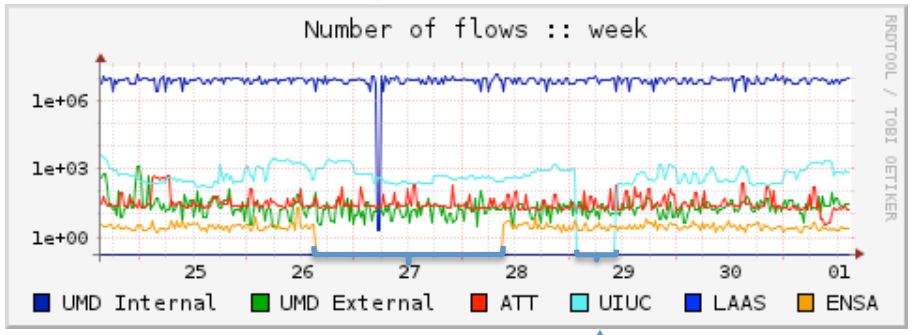
UMD Honeynet Architecture



Case Study: Honeynet management

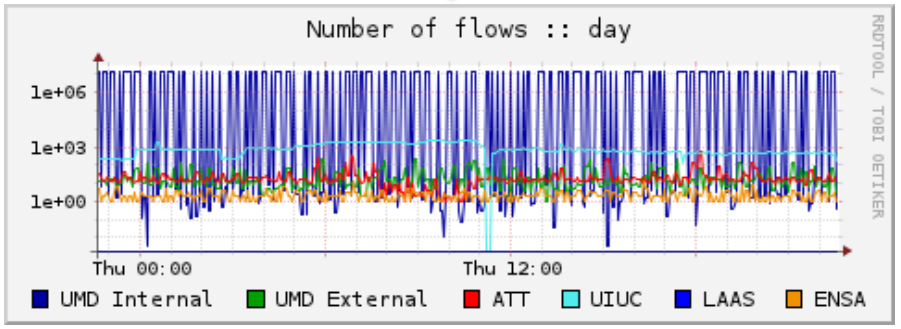
- Monitoring of the core components of the architecture (tunnels, honeypots)
- Identification of data collection failures
- Identification of network failures

UMD Internet network is not tunneled
Network issue?



Tunnel issues

Significant variations in the number of flows for the UMD Internal subnet
Network issue?



Case Study: Security tool

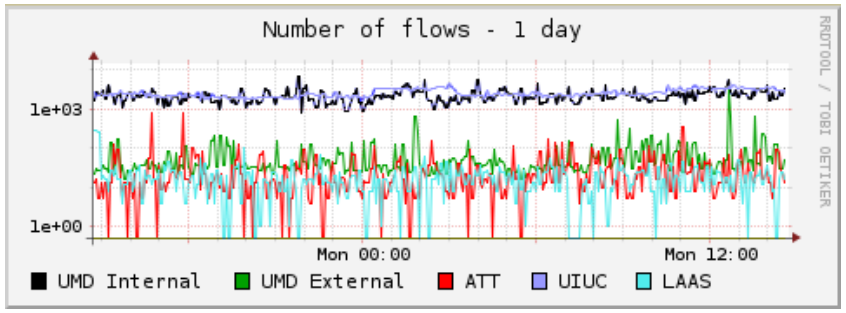
- Alert module
  - Alert on compromised campus hosts targeting the Honeynet
- Attack profiling
  - Origin countries and services targeted most
- Identify misconfigurations
  - Traffic that is not normally allowed

Alert module

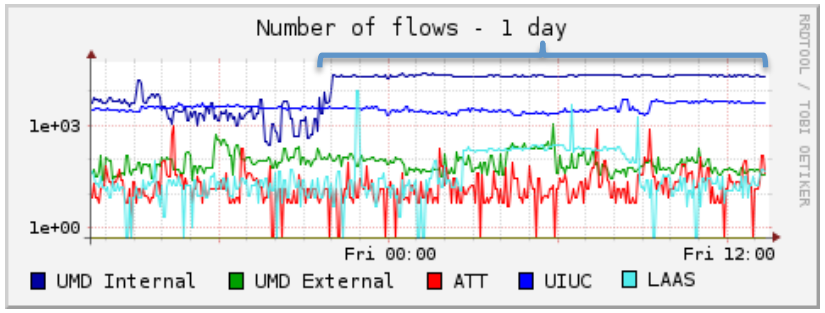
- Report to U. Maryland security folks twice a day:

```
--------------- Analysis Report ---------------
Flow Time Window: 2011/06/06.06:00:00-2011/06/06.18:00:01
Number of hosts detected: 3
To access the online version of the report:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?report=263

xxx.xxx.xxx.xxx (X.umd.edu)
 - Number of flows: 1
 - Number of packets: 1
 - Number of bytes: 51
To visualize the flows:
   https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1124

yyy.yyy.yyy.yyy (Y.umd.edu)
 - Number of flows: 10
 - Number of packets: 10
 - Number of bytes: 1915
To visualize the flows:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1125

zzz.zzz.zzz.zzz (Z.umd.edu)
 - Number of flows: 10
 - Number of packets: 10
 - Number of bytes: 1915
To visualize the flows:
  https://xxx.xxx.xxx.xxx/darknoc/alert_hosts.php?id=1126
```

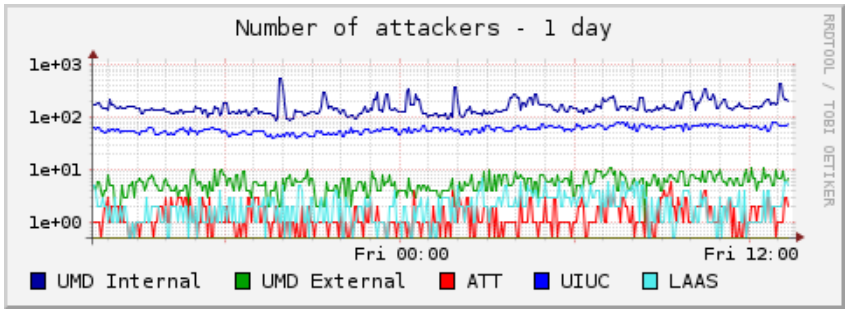
Attack profiling



A typical day of traffic on the honeynet



Significant increase of traffic on the UMD internal subnet



No particular increase of the number of attackers

Top 10 Ports (last 24 hours)		
Port Number	**Number**	**%**
TCP / 22	240597	57.49%
TCP / 27977	20000	4.78%
UDP / 42332	18247	4.36%
TCP / 80	11248	2.69%
TCP / 1433	8464	2.02%
TCP / 443	5552	1.33%
UDP / 19756	5550	1.33%
TCP / 3306	5033	1.2%
TCP / 3389	4513	1.08%
ICMP / 8.0	4286	1.02%

But port TCP/22 moves to the first place in the Top 10 ports…

You can join the adventure!

- Interested joining the UMD Honeynet? All you need is:
  - A Linux machine
    - An “old” box (Honeymole works great on a PII), can even be a VM
    - 2 network interfaces
    - Internet connectivity (Honeymole works with NAT)
  - Unused IP addresses (from 3 to… a lot)
  - We take care of the honeypot deployment at Maryland.
- What you will get:
  - Access to DarkNOC and our data repository (subject to partners’ approval)
  - Possibility to deploy your experiments using IP addresses of other institutions (within reason and subject to other institutions’ approval :-)

The authors would like to thank the Office of Information Technology at the University of Maryland for permitting this work