The CINBAD Project Update
From statistical analysis to traffic signatures

Milosz Marian Hulboj - CERN/Procurve

Ryszard Erazm Jurga - CERN/Procurve

9th December 2008

Outline

- Statistical anomaly detection
- Transition to snort
  - Snort setup
- Findings
- Plans

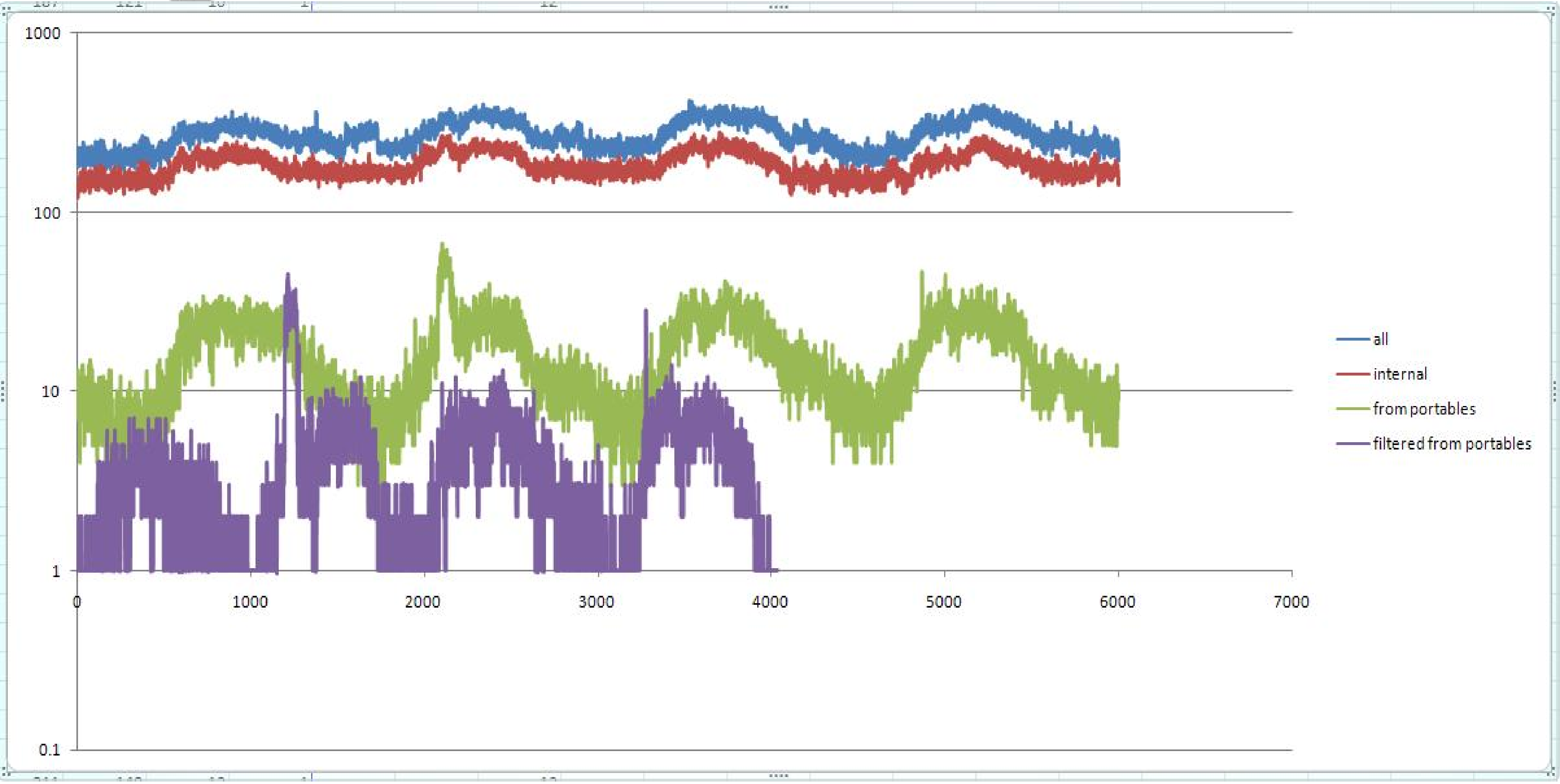
Flow Analysis

- Top-down approach
  - start with all possible flows
  - divide flow into categories, e.g.
    - external/internal/network domain/network device
    - udp/tcp/icmp/others
    - static/dynamic addresses
- Analysis is challenging
  - very noisy traffic
    - many different protocols, applications
  - isolating anomalous traffic is difficult and might require payload inspection

Flow Description

- Example of known flows:
  - network services like dhcp, dns, ldap, kerberos, …
  - applications like mail servers, antivirus, afs, …
  - OS characteristic traffic like netbios, P&P, …
- Example of the flow description:
  - <source address; dst address; protocol; src port, dst port>:
    - <dns server;*;UDP; 53; *>
    - <*, dns server; UDP; *; 53>
    - <*;*;UDP;1900;1900>
    - BUT works only with the services using standard protocols and ports

UDP flows

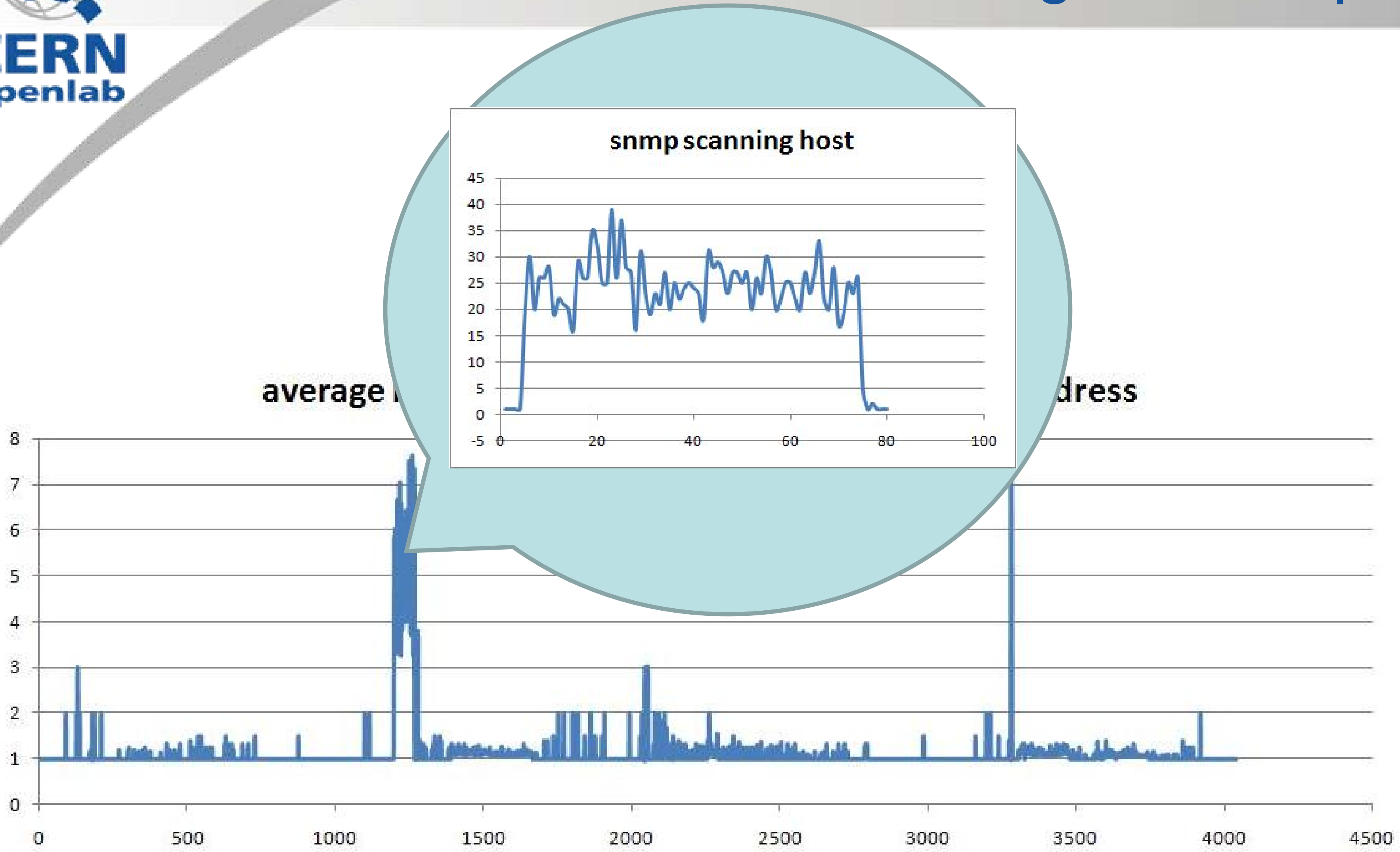

1000
100
10
1
0.1
0
1000
2000
3000
4000
5000
6000
7000
all
internal
from portables
filtered from portables

Statistical Analysis Methods

- Moving Average approach
  - Monitoring udp connections within CERN from portable hosts
  - Measuring the number of different destination addresses contacted by a give source address
  - Hosts violating a given threshold are being reported

- Top flow analysis
  - Flow table of udp connections to the outside world

Findings - example



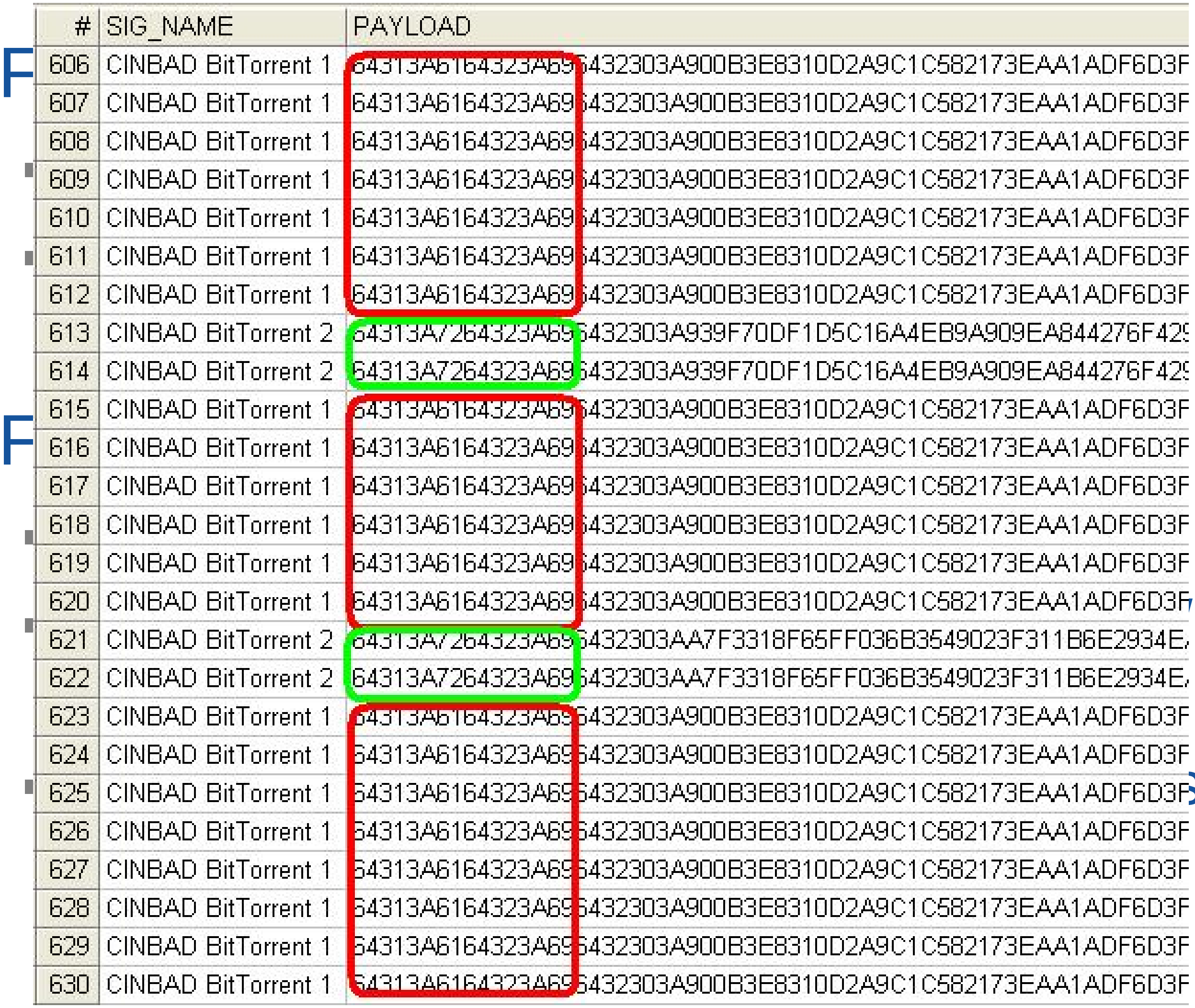
Findings (2)

- F

- F

ports

same



#	SIG_NAME	PAYLOAD
606	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
607	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
608	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
609	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
610	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
611	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
612	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
613	CINBAD BitTorrent 2	64313A7264323A696432303A939F70DF1D5C16A4EB9A909EA844276F42
614	CINBAD BitTorrent 2	64313A7264323A696432303A939F70DF1D5C16A4EB9A909EA844276F42
615	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
616	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
617	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
618	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
619	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
620	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
621	CINBAD BitTorrent 2	64313A7264323A696432303AA7F3318F65FF036B3549023F311B6E2934E
622	CINBAD BitTorrent 2	64313A7264323A696432303AA7F3318F65FF036B3549023F311B6E2934E
623	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
624	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
625	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
626	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
627	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
628	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
629	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F
630	CINBAD BitTorrent 1	64313A6164323A696432303A900B3E8310D2A9C1C582173EAA1ADF6D3F

How to use signatures

- simple_filter
  - CINBAD tool based on libpcap for filtering collected data
  - Signatures can be written as pcap filter strings

- Snort
  - Rule based network traffic monitoring system
  - Rules for detecting numerous anomalies available
  - Does not work with sampled traffic out-of-the box

Snort

- Porting to work with sampled data
  - workaround for truncated payloads
  - snort rules translated into stateless ones (if applicable)
- Oracle backend
- 7000+ rules with daily updates
  - cinbad rules
    - e.g. bittorent, zatto, QQ …
  - http://www.emergingthreats.net
- Internal and External traffic analysis

Snort (2)

- Findings
  - ~45% alerts compared to the snort analysis of full traffic traces on the firewall
    - we expect this ratio to increase when we add more switches
  - internal and external traffic inspected
    - p2p file sharing applications, e.g. Bittorent, Edonkey,…
    - instant messengers, e.g. MSN, ICQ, Yahoo, …
    - p2p streaming video, e.g. Zatto
    - two trojan likely infections
      - Password Stealer
      - Win32/Alureon.gen!J

Trojans

- Password stealer
  - GET /xmfx/help1.rar, /xmfx/help.rar , /fm4/help.exe, /xmfx/mg11.txt, /xmfx/mg12.txt,
  - Identified as:
    - TrojanDropper: Win32/Frethog.k
    - PWS: Frethog.d
    - Trojan.Win32.Vaklik.ccf

- Win32/Alureon.gen!J
  - http connections to default gw with default credentials
    - GET /hpppoe.htm

Bottom-Up approach

- Define the normal behavior for a given network element
- Narrow the analysis domain down only to this given network element
- Report any deviation from the initial behavior description as an anomaly
  - check if this anomaly is not a part of the normal behavior

Bottom-Up approach example

- Connections from/to switch management interfaces
  - In normal conditions there is hardly any traffic on the management interfaces (some monitoring)
  - The traffic should involve only a group of well known hosts
- Snort rule
  - alert tcp !$SW_TALKERS any <> $SW any (msg:"CINBAD undefined TCP connection to/from switches/wireless management interface“; sid:7000012; rev:1;)
- Findings
  - two wireless bridges that might be performing NAT

Plans

- Identify well known services (by protocol type, address, ports, etc) and exclude them from the analysis
- Monitor the behaviour of the known services for changes (bottom-up)
- Feed the anomalous traffic into the signature extraction system