Visualizing IDS Output: Tools and Methodology

Russ McRee
Microsoft Corporation

Session ID: NMS-402
Session Classification: Advanced
Bio

• Team Leader for Microsoft Online Services Security Incident Management

• Holisticinfosec.org – all files discussed today will be available here

• Toolsmith, other publications
  – ISSA Journal
Stem the tide
Stem the tide...

- Parsing logs, oh joy!
- Buy SEM, SIEM…money grows on trees right?
- How do you watch your network?
  - Coming or going?
  - If one assumes compromise by default, which matters more…ingress or egress?
We can’t even begin to pay attention to noise bouncing off the front door.

What matters is what’s leaving your network bound for the Axis of Evil.

Whitelist anyone?

– What should be leaving versus what is leaving your network?
– What if you had a baseline of expected norms from your network, and everything else was considered suspicious?

Visualizing egress traffic helps optimize baselines & conduct thorough investigations.
Captures and real time monitoring are great, but if you manage large networks you need help.

Snort analysis of static PCAPs has always been useful, but visualization can enhance greatly.

We’ll look at a set of PCAPs, how they look to Snort versus how they look to visualization tools.
Recommened books

- **Raffael Marty**
  - *Applied Security Visualization*

- **Greg Conti**
  - *Security Data Visualization: Graphical Techniques for Network Analysis*
• **Data Analysis & Visualization Linux (DAVIX)**
  
  – The DAVIX Live CD: for data analysis & visualization providing free tools for data processing and visualization
  
  – Slackware-based distribution that includes:
    
    • well known SecViz tools
    • a comprehensive manual
    • extensive bookmark collection for online resources on visualization tools, libraries and applications
Everyone knows what Snort is, right?
Matt Jonkman’s project drives open source, community driven rules for use with Snort
Very bleeding edge
Funding by Army Research Office & National Science Foundation to continue project & research
Detect new threats in your environment and write new rules for public release to the community
Rulesets are updated as new information surfaces (many times daily), update at least 2x a week
• **AfterGlow**
  – collection of scripts which facilitate the process of generating graphs

• **Rumint**
  – network and security visualization tool that can load pcap datasets and capture live traffic, including VCR/PVR interface

• **NetGrok**
  – visualizes in real-time via group-based graph layout & treemap. Read PCAPs & captures from live interface

• **Maltego**
  – intelligence & forensics app with data mining and intelligence gathering capabilities. Identifies relationships.
Demos
“I am often faced with the problem of looking at a complex dataset and understanding the relationships of various. Instead of reading through the file, line by line, I like to look at graphs that visualize the data. One powerful type of graphs useful to visualize relationships among entities, are so-called **linked graphs** or network graphs.” – Raffael Marty
IRC.Flood – classic IRC bot, noisy and obvious, a Trojan that connects to tcp 5553

01 [**] [1:2000347:7] ET ATTACK RESPONSE IRC - Private message on non-std port [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
03 05/03-14:52:09.693987 192.168.248.105:1156 -> 64.32.28.7:5553
04 TCP TTL:128 TOS:0x0 ID:24739 IpLen:20 DgmLen:122 DF
05 ***AP*** Seq: 0xDE571EA6 Ack: 0x4EB6EC Win: 0xFD92 TcpLen: 20
06 [Xref -> http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/ATTACK_RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC]
07 [Xref => http://doc.emergingthreats.net/bin/view/Main/2000347]
LIVE DEMO (AfterGlow)
Demo Summary: AfterGlow & IRC.Flood

- Source file: camda.pcap

```
sudo snort -c /etc/snort/snort.conf -r camda.pcap -l output/camda
```

**Snort**

```
01 [**] [1:2000347:7] ET ATTACK RESPONSE IRC - Private message on non-std port [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
03 05/03-14:52:09.695897 192.168.248.105:1158 --> 64.32.28.7:5553
04 TCP TTL:128 TOS:0x0 ID:24739 Tlplen:20 DgmLen:122 DF
05 ***AP*** Seq: 0XDES71EA6 ACK: 0XA4EB6EC Win: 0XFD97 TcLLen: 20
06 [Xref => http://www.emergingthreats.net/cgi-bin/cvsvweb.cgi/sigs/ATTACK_ RESPONSE/ATTACK_RESPONSE_Non-Standard_IRC]
07 [Xref => http://doc.emergingthreats.net/bin/view/Main/2000347]
```

**AfterGlow**

```
cat camda.csv | afterglow.pl -c
/usr/local/share/afterglow/color.properties -v | dot -Tgif -o camda.gif
```

```
tcpdump
-vvttttunnel camda.pcap |
/usr/local/bin/tcpdump2csv.pl
"sip dip dport" > camda.csv
```
“I caution you not to fall into the trap of just creating pictures. Instead, seek to address problems only where it makes sense.” - Greg Conti
Korgo (aka Padobot) is a network worm written by the Russian Hangup Team virus group. It spreads using a vulnerability in Windows LSASS.

02 [Classification: A Network Trojan was detected] [Priority: 1]
04 TCP TTL:128 TOS:0x0 ID:49609 IpLen:20 DgmLen:1500 DF
05 ***A**** Seq: 0xDEBC709A Ack: 0xB8E50743 Win: 0xFDEF TcpLen: 20
06 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIrus/WORM_konco]
Summary: Korgo & Rumint

- **Source file:** korgo.pcap

**Snort**

```
sudo snort -c /etc/snort/snort.conf -r korgo.pcap -l output/korgo
```

**Rumint**

```
01 [**] 1:2001337:7 HT WOBK Orgo.P offering executable [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
04 TCP TTL:128 TOS:0x0 ID:48689 IpLen:20 DmLen:1500 DF
05 ***A*** Seq: 0XBD7970A Ack: 0XBD79743 Win: 0XFO38F Tcpl: 80
06 [Xref -> http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WOBK_ORG0]
```
“A picture is worth a thousand words. An interface is worth a thousand pictures.” - Ben Shneiderman

“Leonardo Da Vinci combined art and science and aesthetics and engineering, that kind of unity is needed once again.” - Ben Shneiderman
Demo: Kraken & NetGrok

Kraken – big 2008 botnet, also known as Bobax or Hacktool. Targeted Fortune 500, evades AV

Outbound (egress)
LIVE DEMO (NetGrok)
Demo Summary: Kraken & NetGrok

- **Source file:** kraken.pcap

**Snort**

```
sudo snort -c /etc/snort/snort.conf -r kraken.pcap -l output/kraken
```

**NetGrok**

```
17 [**] [1:2008110:2] ET TROJAN Possible Bobax/Kraken/Odorcor TCP 847 CnC Channel Outbound [**]
18 [Classification: A Network Trojan was detected] [Priority: 1]
19 02/22-04:20:53.810640 192.168.3.5:1054 - 60.20.87.159:947
20 TCP TTL:128 TOS:0x0 ID:458 IpLen:20 DmLen:40 DF
21 ***A**** Seq: 0x1D1E7D Ack: CxC0815DCD Win: Cx470 TcpLen: 20
22 [Xref => http://www.ccmerringthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_Bobax]
23 [Xref => http://doc.ccmerringthreats.net/bin/view/Main/OdeRoar]
```
“Maltego can be used for the information gathering phase of all security related work aiding you in your thinking process by visually demonstrating interconnected links between searched items with more powerful search, giving you smarter results and access to "hidden" information” - Paterva
Zeus Trojan (the original APT): malware that organized criminals use to steal information from countless businesses and government organizations...use the stolen credentials to siphon victim organization’s bank accounts, funnel the money through accomplices, who then wire the cash overseas to Ukraine and other Eastern European nations.
LIVE DEMO (Maltego)
Demo Summary: Zeus & Maltego

- **Source file:** zeus.pcap

### Snort

```
sudo snort -c /etc/snort/snort.conf -r zeus.pcap -l output/zeus2020
```

### Maltego

1) `getSourceClients` from `zeus.csv` via local Phrase transform
2) `getDestinationClients` from all IP addresses acquired from first step

```
tcpdump -vvvtttnelr zeus.pcap | /usr/local/bin/tcpdump2csv.pl "sip dip dport" > zeus.csv
```
In closing

- Jump in. Play with these tools and others not discussed.
- DAVIX is a great way to get started without having to build a dedicated system.
- Read the books!
- I’ll share all my PCAPs, transforms, and visualizations with anyone who would like them.
- russ@holisticinfosec.org