RSACONFERENCE2010

SECURITY DECODED

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

Agenda

Stem the tide…

Analysis overview

Tools & Demos

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?

Stem the tide…

- 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

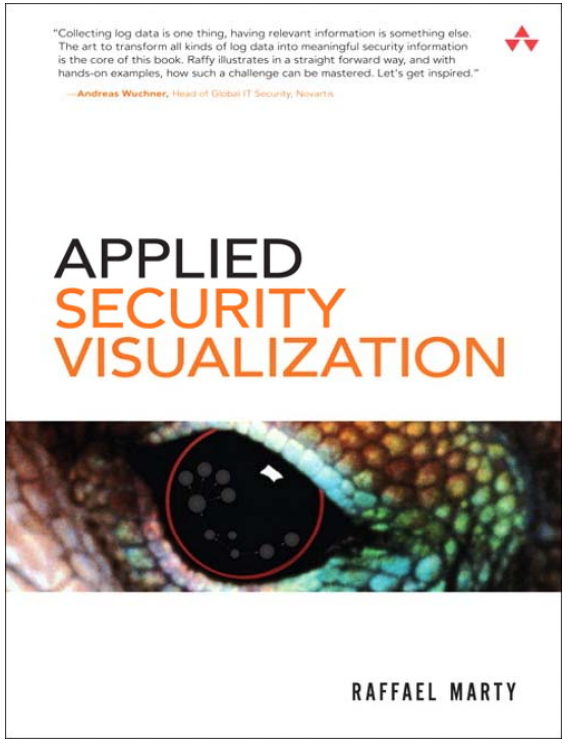
Analysis overview

Analysis overview

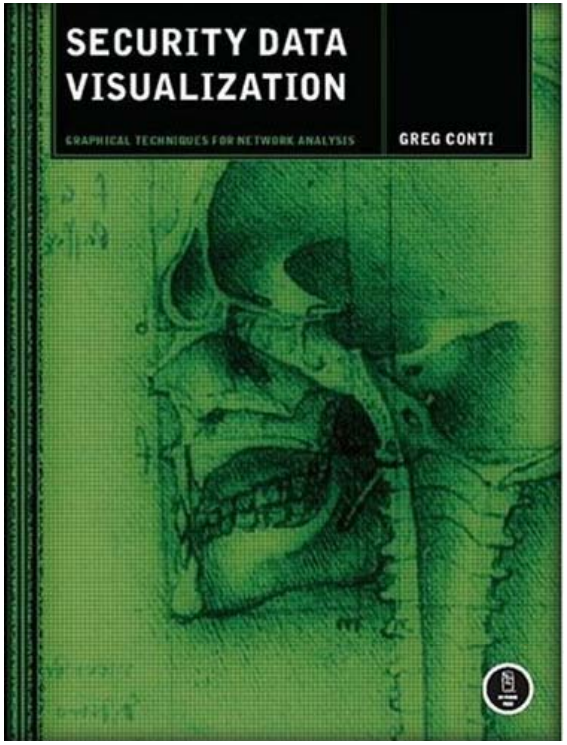
- Captures and real time monitoring are great, but if you manage large networks you need help
- Snort analysis of static PCAPs has always been useful, but visualization can enhance greatly
- We'll look at a set of PCAPs, how they look to Snort versus how they look to visualization tools

Recommened books

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



- **Greg Conti**
  - *Security Data Visualization: Graphical Techniques for Network Analysis*



Microsoft Global Foundation Services

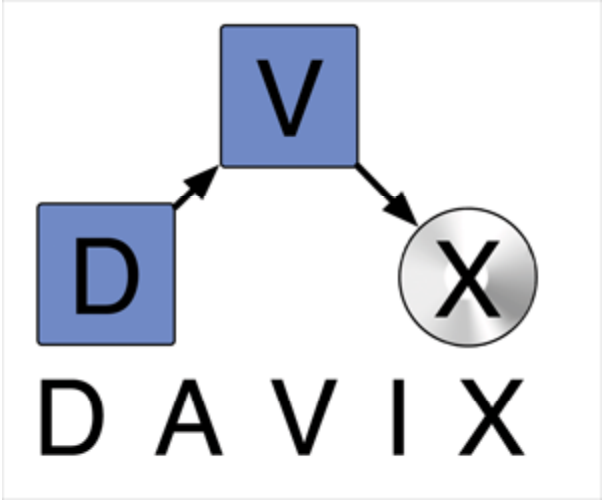
ONLINE SECURITY

RSA CONFERENCE 2010

Tools & Demos

Tools - DAVIX

- 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



Tools – Snort & Emerging Threats

- 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

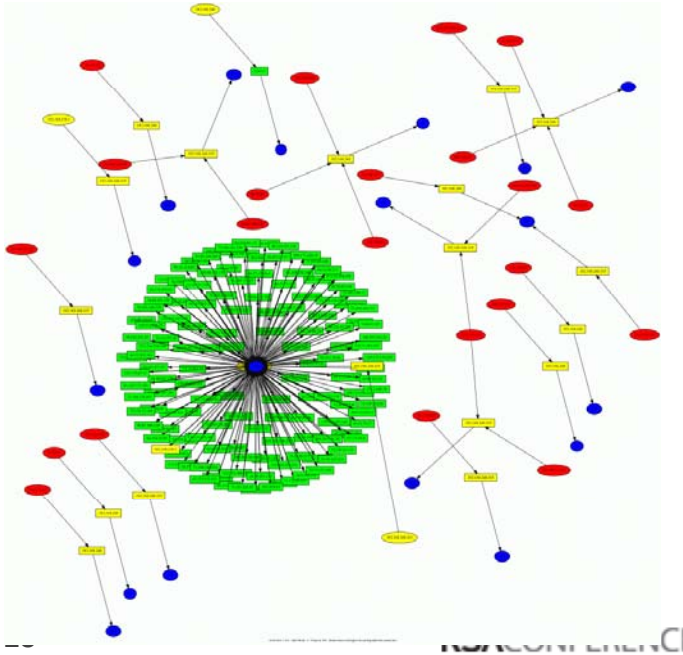
Tools

- 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

AfterGlow

"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



Demo: AfterGlow & IRC.Flood

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 05/03-14:52:09.693897 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: 0xA4EB6BC  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]
```

Outbound (egress)

Demo: AfterGlow & IRC.Flood

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
```

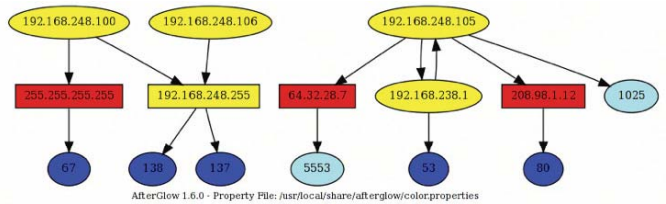
Snort

```
01 [**] [1:2000347:7] ET ATTACK RESPONSE IRC - Private message on non-std port [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
03 05/03-14:52:09.693897 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: 0xA4EB6BC  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]
```

```
tcpdump ➘
-vttttnnelr camda.pcap | ➘
/usr/local/bin/tcpdump2csv.pl ➘
"sip dip dport" > camda.csv
```

AfterGlow

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



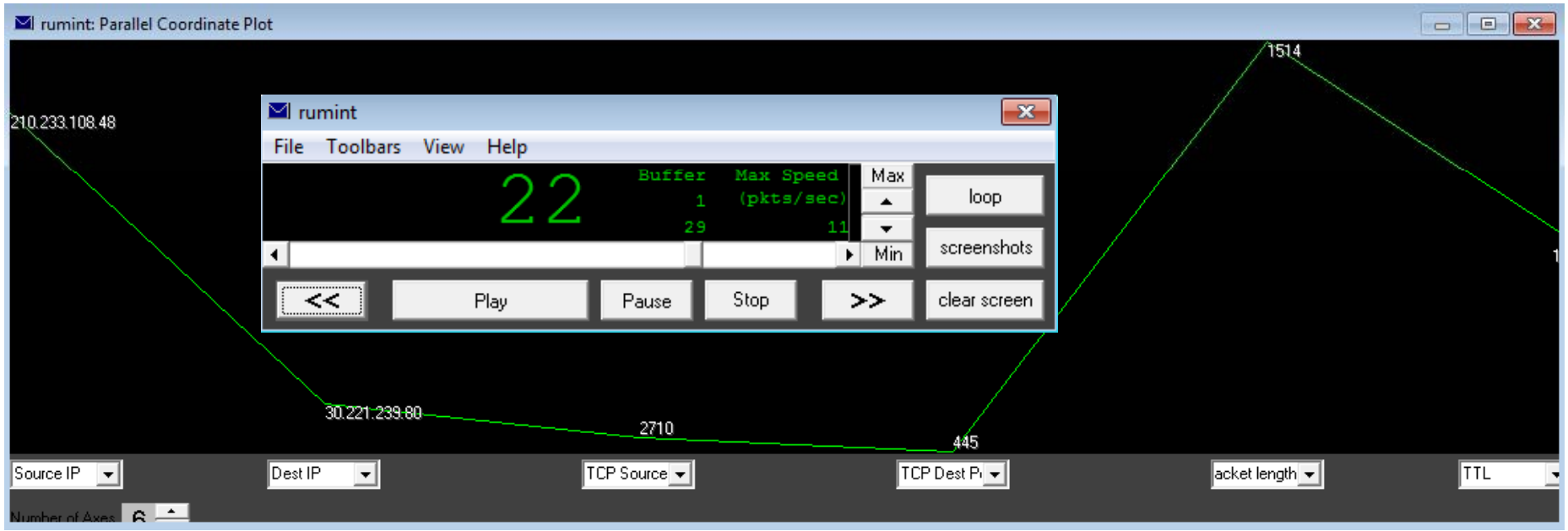
Microsoft Global Foundation Services

ONLINE SECURITY

RSA CONFERENCE 2010

Rumint

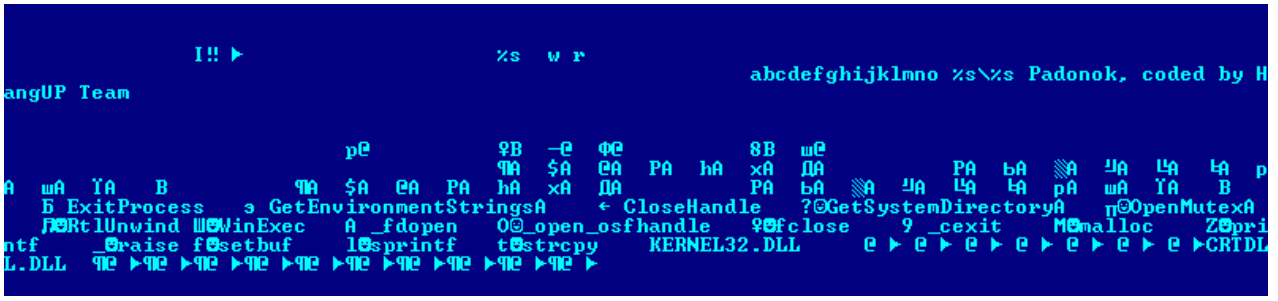
"I caution you not to fall into the trap of just creating pictures. Instead, seek to address problems only where it makes sense." - Greg Conti



Korgo & Rumint

Korgo (aka Padobot) is a network worm written by the Russian Hangup Team virus group. It spreads using a vulnerability in Windows LSASS

```
01 [**] [1:2001337:7] ET WORM Korgo.P offering executable [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
03 06/27-19:47:17.324095 210.233.108.48:2710 -> 30.221.239.80:445
04 TCP TTL:128 TOS:0x0 ID:49809 IpLen:20 DgmLen:1500 DF
05 ***A**** Seq: 0xDBBC709A  Ack: 0xB6E50743  Win: 0xFDBF  TcpLen: 20
06 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_
   KORGO]
07 [Xref => http://doc.emergingthreats.net/2001337][Xref => http://www.f-secure.
   com/v-descs/korgo_p.shtml]
```



Summary: Korgo & Rumint

- **Source file:** korgo.pcap

```
File → Open → korgo.pcap
```

Snort

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

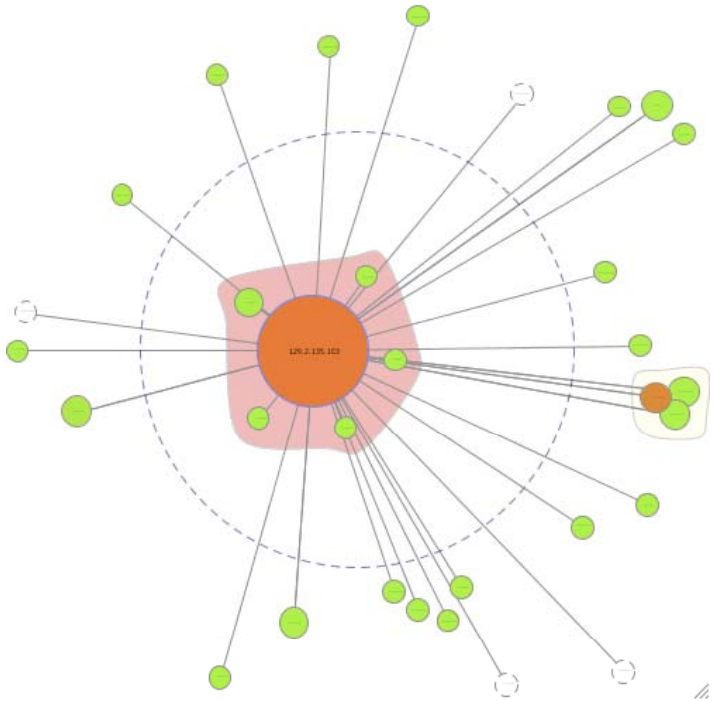
```
01 [**] [1:2001337:7] ET WORM Korgo.P offering executable [**]
02 [Classification: A Network Trojan was detected] [Priority: 1]
03 06/27-19:47:17.324095 210.233.108.48:2710 -> 30.221.239.80:445
04 TCP TTL:128 TOS:0x0 ID:49809 IpLen:20 DgmLen:1500 DF
05 ***A**** Seq: 0xDBBC709A  Ack: 0xB6E50743  Win: 0xFDBF  TcpLen: 20
06 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/WORM_
   KORGO]
07 [Xref => http://doc.emergingthreats.net/2001337][Xref => http://www.f-secure.
   com/v-descs/korgo_p.shtml]
```

Rumint

NetGrok

"A picture is worth a thousand words. An interface is worth a thousand pictures." - Ben Shneiderman

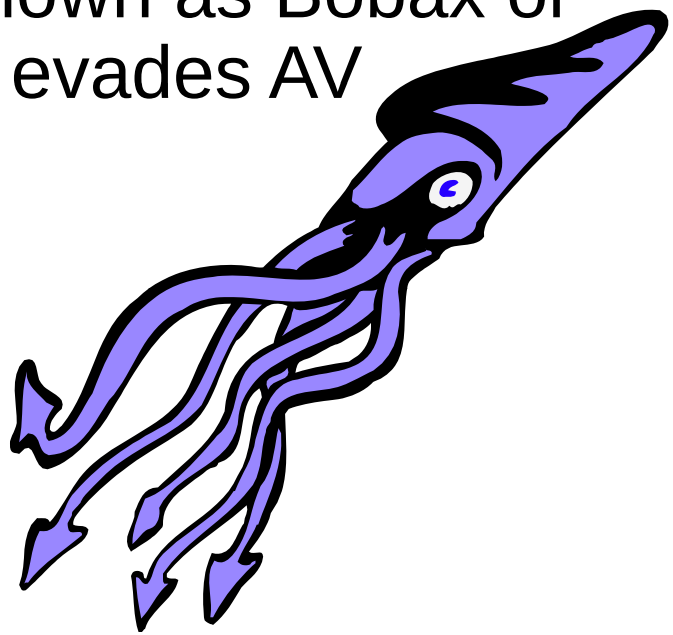
"Leonardo Da Vinci combined art and science and aesthetics and engineering, that kind of unity is needed once again." - Ben Shneiderman



Demo: Kraken & NetGrok

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

```
17 [**] [1:2008110:3] ET TROJAN Possible Bobax/Kraken/Oderoor TCP 447 CnC Channel
   Outbound [**]
18 [Classification: A Network Trojan was detected] [Priority: 1]
19 02/22-04:20:53.810649 192.168.2.5:1054 -> 66.29.87.159:447
20 TCP TTL:128 TOS:0x0 ID:459 IpLen:20 DgmLen:40 DF
21 ***A**** Seq: 0x1D12B7D  Ack: 0xC6815DCD  Win: 0x4470  TcpLen: 20
22 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_
   Bobax]
23 [Xref => http://doc.emergingthreats.net/bin/view/Main/OdeRoor]
24
25 [**] [1:2008103:3] ET TROJAN Bobax/Kraken/Oderoor TCP 447 CnC Channel Initial
   Packet Outbound [**]
26 [Classification: A Network Trojan was detected] [Priority: 1]
27 02/22-04:20:54.367395 192.168.2.5:1055 -> 66.29.87.159:447
28 TCP TTL:128 TOS:0x0 ID:475 IpLen:20 DgmLen:64 DF
29 ***AP*** Seq: 0x95E9CBD1  Ack: 0xC63DF5FA  Win: 0x4470  TcpLen: 20
30 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_
   Bobax]
31 [Xref => http://doc.emergingthreats.net/bin/view/Main/OdeRoor]
```



Outbound (egress)

Demo: Kraken & NetGrok

LIVE DEMO (NetGrok)

Demo Summary: Kraken & NetGrok

- **Source file:** kraken.pcap

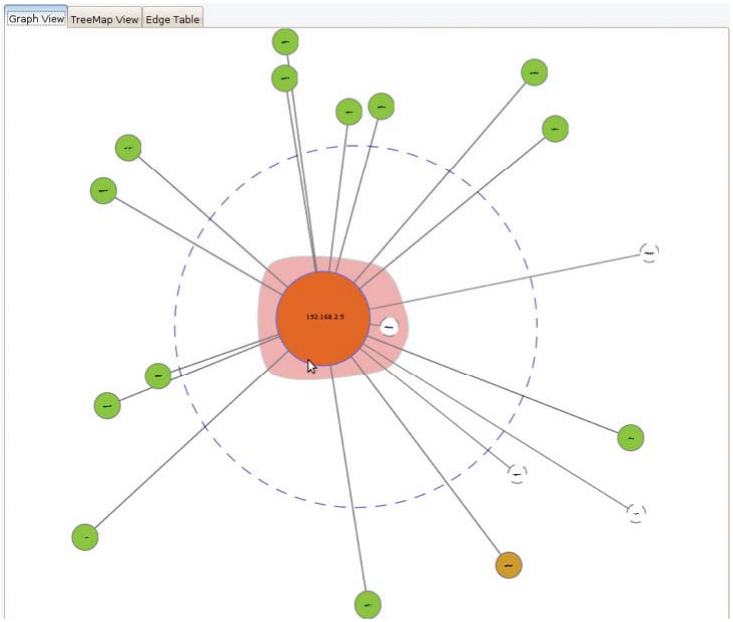
Snort

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

```
17 [**] [1:2008110:3] ET TROJAN Possible Bobax/Kraken/Oderoor TCP 447 CnC Channel
   Outbound [**]
18 [Classification: A Network Trojan was detected] [Priority: 1]
19 02/22-04:20:53.810649 192.168.2.5:1054 -> 66.29.87.159:447
20 TCP TTL:128 TOS:0x0 ID:459 IpLen:20 DgmLen:40 DF
21 ***A**** Seq: 0x1D12B7D  Ack: 0xC6815DCD  Win: 0x4470  TcpLen: 20
22 [Xref => http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_
   Bobax]
23 [Xref => http://doc.emergingthreats.net/bin/view/Main/OdeRoor]
```

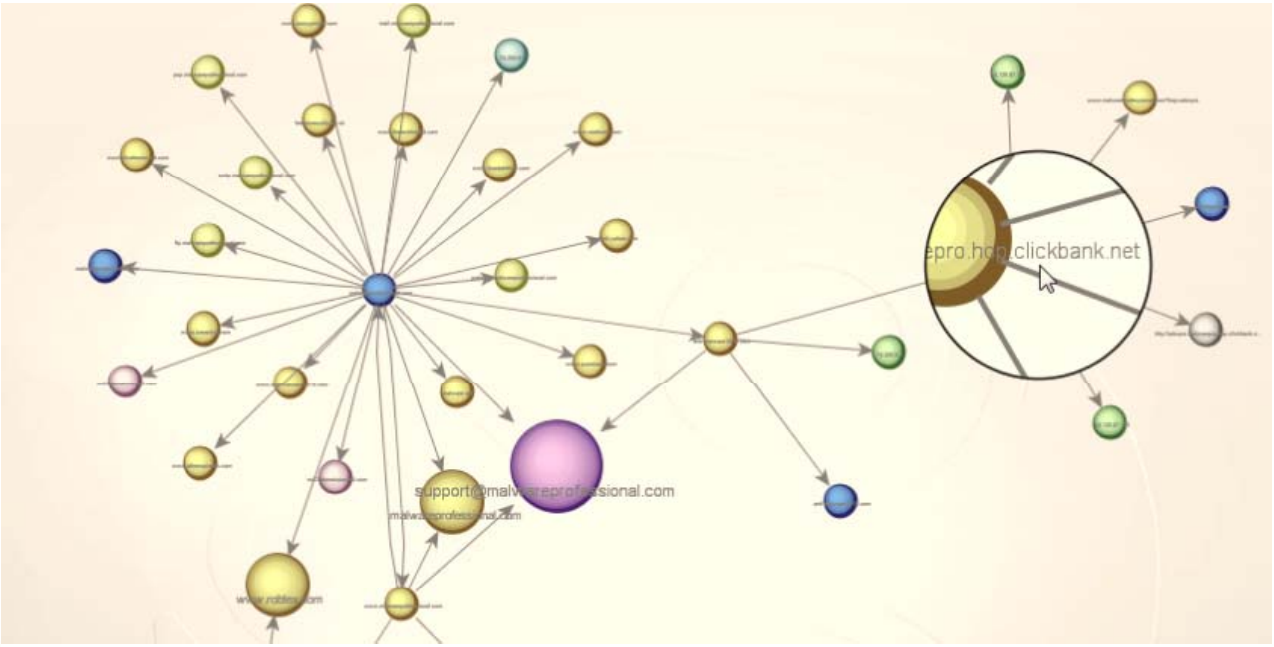
```
File → Open → kraken.pcap
```

NetGrok



Maltego

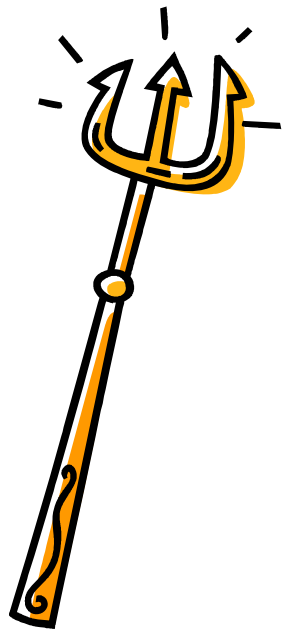
"Maltego can be used for the information gathering phase of all security related work aiding you in your thinking process by visually demonstrating interconnected links between searched items with more powerful search, giving you smarter results and access to "hidden" information" - Paterva



Demo: Zeus & Maltego

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.

```
1  [**] [1:2007724:7] ET TROJAN Prg Trojan HTTP POST version 2 [**]
2  [Classification: A Network Trojan was detected] [Priority: 1]
3  02/15-21:29:25.299712 192.168.248.114:1137 -> 115.100.250.105:80
4  TCP TTL:128 TOS:0x0 ID:1797 IpLen:20 DgmLen:280 DF
5  ***AP*** Seq: 0x39338191  Ack: 0x9ED49274  Win: 0xFAF0  TcpLen: 20
6  [Xref =>
   http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG][Xref
   => http://doc.emergingthreats.net/2007724][Xref =>
   http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf]
7
8  [**] [1:2003183:5] ET TROJAN Prg Trojan Server Reply [**]
9  [Classification: A Network Trojan was detected] [Priority: 1]
10 02/15-21:29:25.948696 115.100.250.105:80 -> 192.168.248.114:1137
11 TCP TTL:48 TOS:0x8 ID:28210 IpLen:20 DgmLen:247 DF
12 ***AP*** Seq: 0x9ED49274  Ack: 0x39339C7F  Win: 0x4FD8  TcpLen: 20
13 [Xref =>
   http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG][Xref
   => http://doc.emergingthreats.net/2003183][Xref =>
   http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf]
```



Demo: Zeus & Maltego

LIVE DEMO (Maltego)

Demo Summary: Zeus & Maltego

- **Source file:** zeus.pcap

Snort

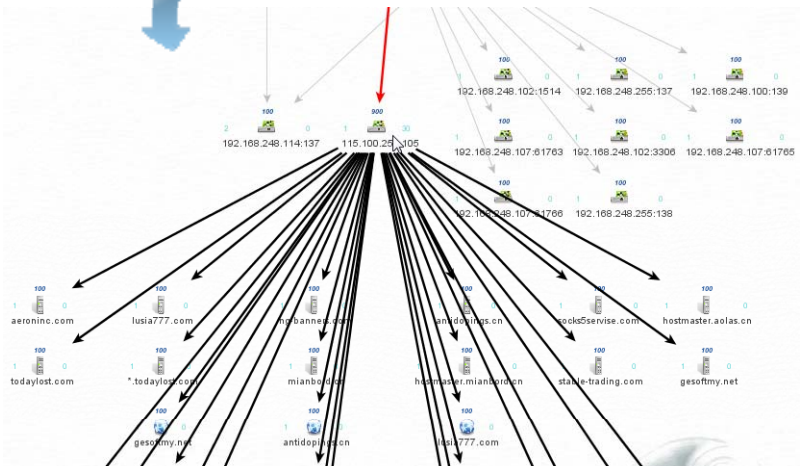
```
sudo snort –c /etc/snort/snort.conf –r
zeus.pcap –l output/zeus2020
```

```
1  [**] [1:2007724:7] ET TROJAN Prg Trojan HTTP POST version 2 [**]
2  [Classification: A Network Trojan was detected] [Priority: 1]
3  02/15-21:29:25.299712 192.168.248.114:1137 -> 115.100.250.105:80
4  TCP TTL:128 TOS:0x0 ID:1797 IpLen:20 DgmLen:280 DF
5  ***AP*** Seq: 0x39338191  Ack: 0x9ED49274  Win: 0xFAF0  TcpLen: 20
6  [Xref =>
   http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG][Xref
   => http://doc.emergingthreats.net/2007724][Xref =>
   http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf]
7
8  [**] [1:2003183:5] ET TROJAN Prg Trojan Server Reply [**]
9  [Classification: A Network Trojan was detected] [Priority: 1]
10 02/15-21:29:25.948696 115.100.250.105:80 -> 192.168.248.114:1137
11 TCP TTL:48 TOS:0x8 ID:28210 IpLen:20 DgmLen:247 DF
12 ***AP*** Seq: 0x9ED49274  Ack: 0x39339C7F  Win: 0x4FD8  TcpLen: 20
13 [Xref =>
   http://www.emergingthreats.net/cgi-bin/cvsweb.cgi/sigs/VIRUS/TROJAN_PRG][Xref
   => http://doc.emergingthreats.net/2003183][Xref =>
   http://www.securescience.net/FILES/securescience/10378/pubMalwareCaseStudy.pdf]
```

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

Maltego

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



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

RSACONFERENCE2010

SECURITY DECODED

Q & A