SHARKFEST '14

WIRESHARK DEVELOPER AND USER CONFERENCE

JUNE 16-20 2014 · DOMINICAN UNIVERSITY

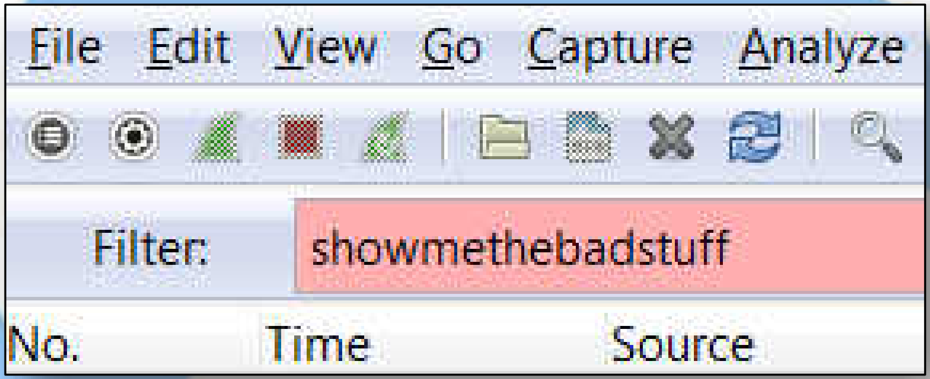
A-2: Defending the Network

Jasper Bongertz, Christian Landström

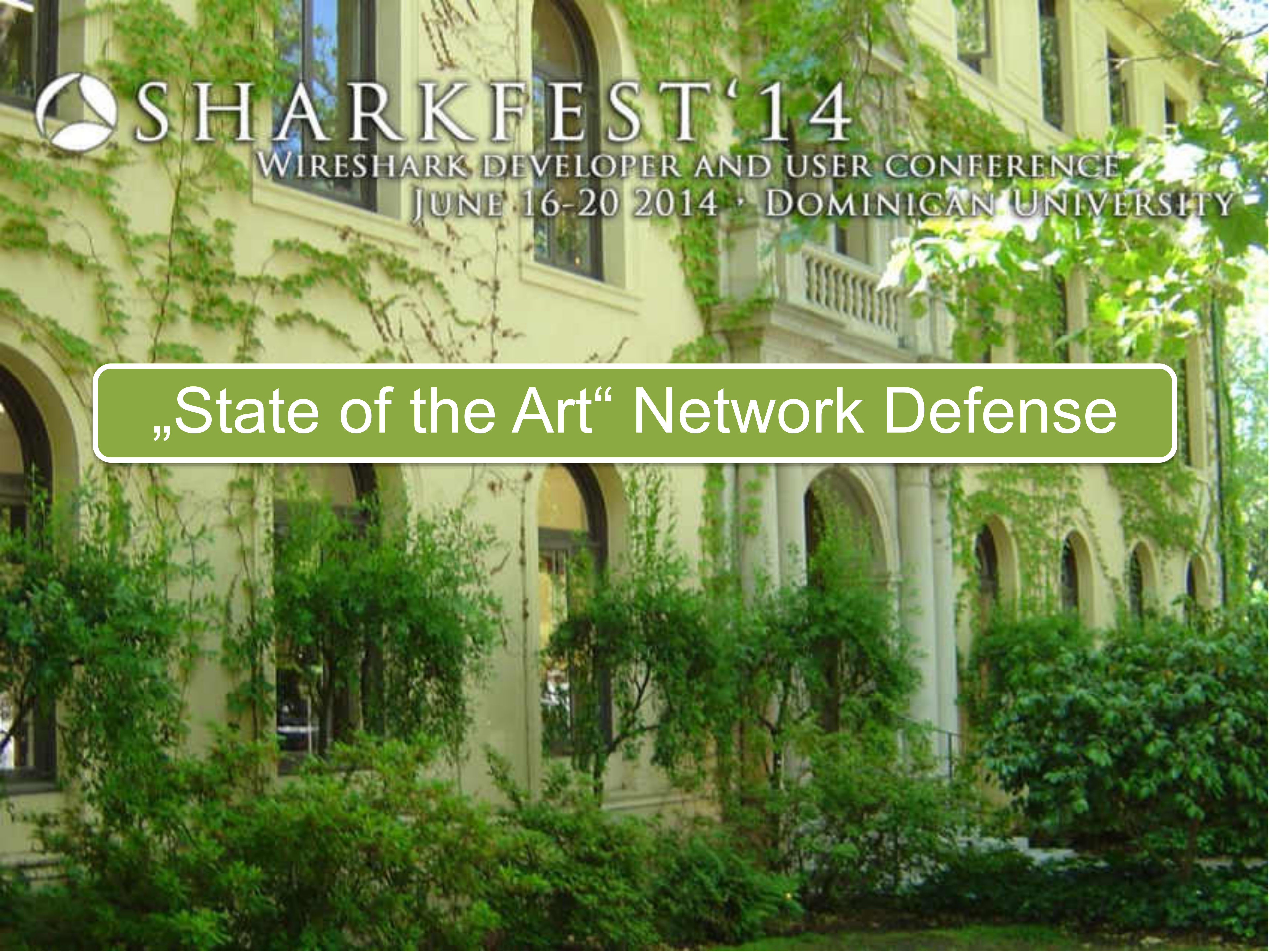
Senior Consultants, Airbus Defence and Space

Topics

- “State-of-the-Art” Defense Infrastructure
  - What it does, what it doesn‘t
- A look at malicious traffic
  - Now you see it, now you don‘t
- Strategies for network defense
- Demos, of course
- How Wireshark ***can*** help



Filter: showmethebadstuff



SHARKFEST'14

WIRESHARK DEVELOPER AND USER CONFERENCE

JUNE 16-20 2014 · DOMINICAN UNIVERSITY

„State of the Art“ Network Defense

„State-of-the-Art“ Network Defense

Defaults:

- Proxy servers with authentication
- Logging, Monitoring, (SIEM)

Layers of Defense:

- Firewalls / WAFs
- Intrusion Detection / Intrusion Prevention
  - NIDS/NIPS
- Malware Sensors / Sandboxing

Proxy with Authentication

- Useful only for access/activity logging
  - Problem: users share/abuse coworker credentials
- Proxies do not prevent malicious outgoing traffic
  - Stealing proxy credentials is trivial if a malware is already running on a users PC
  - … or you simply wait for the user to surf his favorites…

Logging and Monitoring

- Logs are often ineffective
  - not enabled
  - overwritten too soon
  - Nobody knows where they are ?!
- Can grow to huge amounts of data
- Local logs can be deleted by attackers

Firewalls & WAFs

- Firewalls allow access to certain service ports, e.g. web servers
  - Problem: does not know what bad requests look like
  - **W**eb **A**pplication **F**irewalls can help in some cases
- Outgoing connections are not always blocked
- Outdated rules stay in the table
- ANY-to-ANY rules
  - Not as rare as you think (or would like to believe)
- Undocumented internet outbreaks (DSL, 3G/LTE)

Intrusion Detection/Prevention

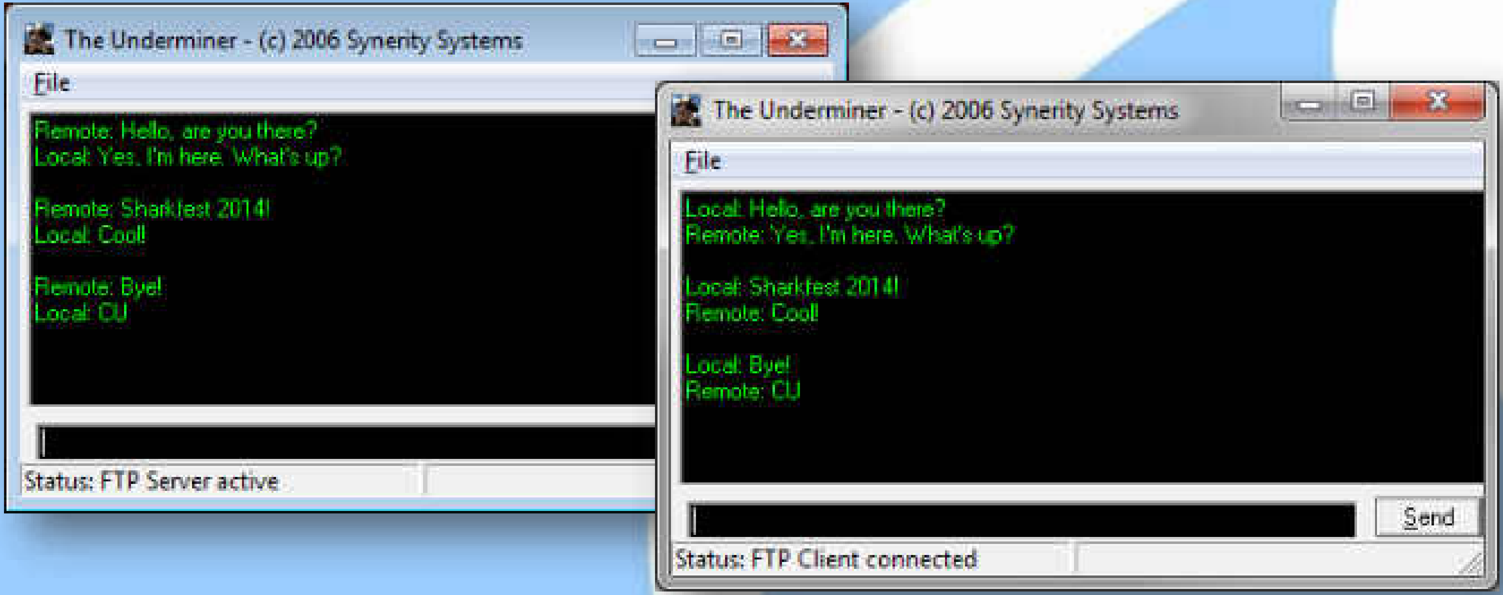
- Intrusion Detection has several problems
  - Does not **P**revent malicious traffic it **D**etects
  - Signatures are often very unspecific, because nobody cares about false positives
- Intrusion Prevention has a different problem
  - Signatures must be precise to prevent false positives
- Both have a common problem
  - IPS are usually very easy to detect
  - IDS and IPS are easy to evade for dedicated attackers

Malware Sensors / Sandboxing

- Devices that run suspicious files in sandboxed environments
  - Record behavior and score it
  - Need significant amounts of CPU/Memory resources to do the job
  - Scaling is a problem
- Not that hard to evade, either
  - Detect virtual environments
  - Wait longer than 5-15 minutes before doing bad stuff

Demo 1 – „Hidden“ Communication

- Nothing fancy, but might simply be overlooked



The Underminer - (c) 2006 Synerity Systems

Remote: Hello, are you there?
Local: Yes, I'm here. What's up?

Remote: Sharkfest 2014!
Local: Cool!

Remote: Bye!
Local: CU

Status: FTP Server active

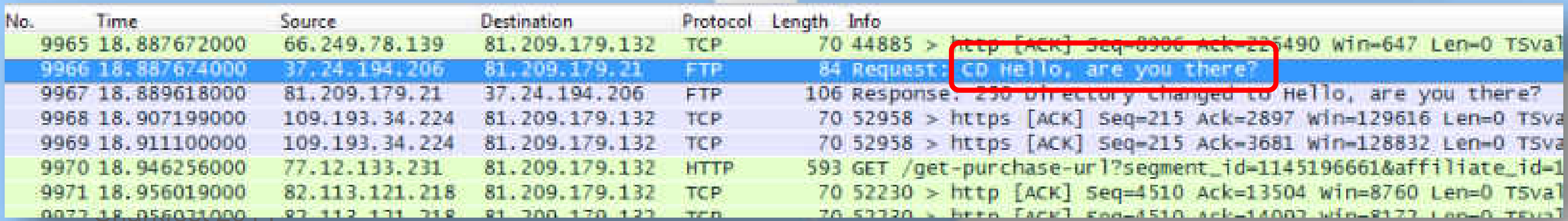
The Underminer - (c) 2006 Synerity Systems

Local: Hello, are you there?
Remote: Yes, I'm here. What's up?

Local: Sharkfest 2014!
Remote: Cool!

Local: Bye!
Remote: CU

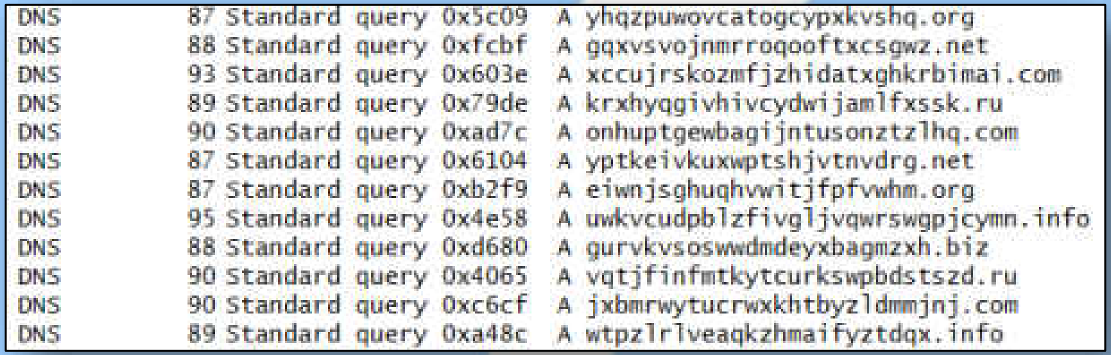
Status: FTP Client connected



No.	Time	Source	Destination	Protocol	Length	Info
9965	18.887672000	66.249.78.139	81.209.179.132	TCP	70	44885 > http [ACK] Seq=8906 Ack=225490 Win=647 Len=0 TSval
9966	18.887674000	37.24.194.206	81.209.179.21	FTP	84	Request: CD Hello, are you there?
9967	18.889618000	81.209.179.21	37.24.194.206	FTP	106	Response: 250 Directory changed to Hello, are you there?
9968	18.907199000	109.193.34.224	81.209.179.132	TCP	70	52958 > https [ACK] Seq=215 Ack=2897 Win=129616 Len=0 TSva
9969	18.911100000	109.193.34.224	81.209.179.132	TCP	70	52958 > https [ACK] Seq=215 Ack=3681 Win=128832 Len=0 TSva
9970	18.946256000	77.12.133.231	81.209.179.132	HTTP	593	GET /get-purchase-url?segment_id=114519666l&affiliate_id=1
9971	18.956019000	82.113.121.218	81.209.179.132	TCP	70	52230 > http [ACK] Seq=4510 Ack=13504 Win=8760 Len=0 TSval
9972	18.956031000	82.113.121.218	81.209.179.132	TCP	70	52230 > http [ACK] Seq=4510 Ack=14002 Win=8172 Len=0 TSval

Demo 2 - Outbreak

- Common malware communicating on the network
  - If it phones home, it WILL be somewhere
  - Start with the obvious, go for DNS and TCP SYN‘s first

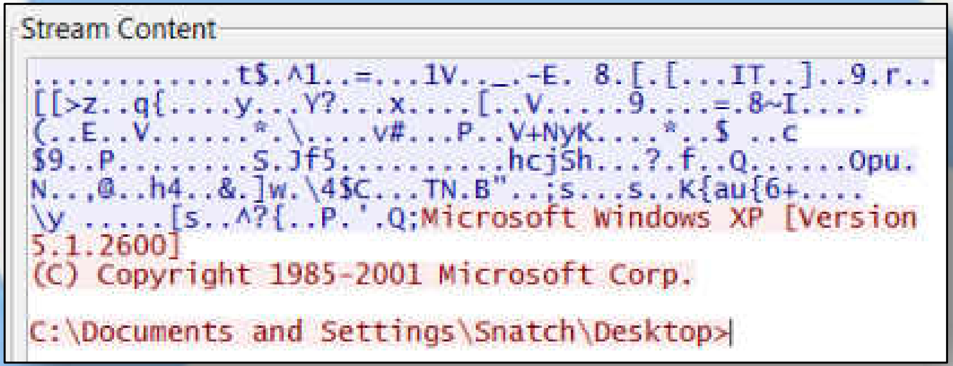


```
DNS          87 Standard query 0x5c09  A yhqzpuwovcatogcypxkvshq.org
DNS          88 Standard query 0xfcbf  A gqxvsvojnmrroqooftxcsgwz.net
DNS          93 Standard query 0x603e  A xccujrskozmfjzhidatxghkrbimai.com
DNS          89 Standard query 0x79de  A krxhyqgivhivcydwijamlfxssk.ru
DNS          90 Standard query 0xad7c  A onhuptgewbagijntusonztzlhq.com
DNS          87 Standard query 0x6104  A yptkeivkuxwptshjvtnvdrg.net
DNS          87 Standard query 0xb2f9  A eiwnjsghuqhvwitjfpfvwhm.org
DNS          95 Standard query 0x4e58  A uwkvcudpblzfivgljvqwrswgpjcymn.info
DNS          88 Standard query 0xd680  A gurvkvsoswwdmdeyxbagmzxh.biz
DNS          90 Standard query 0x4065  A vqtjfinfmtkytcurkswpbdstszd.ru
DNS          90 Standard query 0xc6cf  A jxbmrwytucrwxkhtbyzldmmjnj.com
DNS          89 Standard query 0xa48c  A wtpzlrlveaqkzhmaifyztdqx.info
```

  - Some are quite an eyecatcher, others are not…

Demo 3 – Browser Attack

- Regular Drive-By-Attack like 1000s per day happen
- Identifying different types of command and control traffic is challenging:
  - Regular clear-text protocols inside the „shells“
  - Encoded/Crypted custom CnC protocols

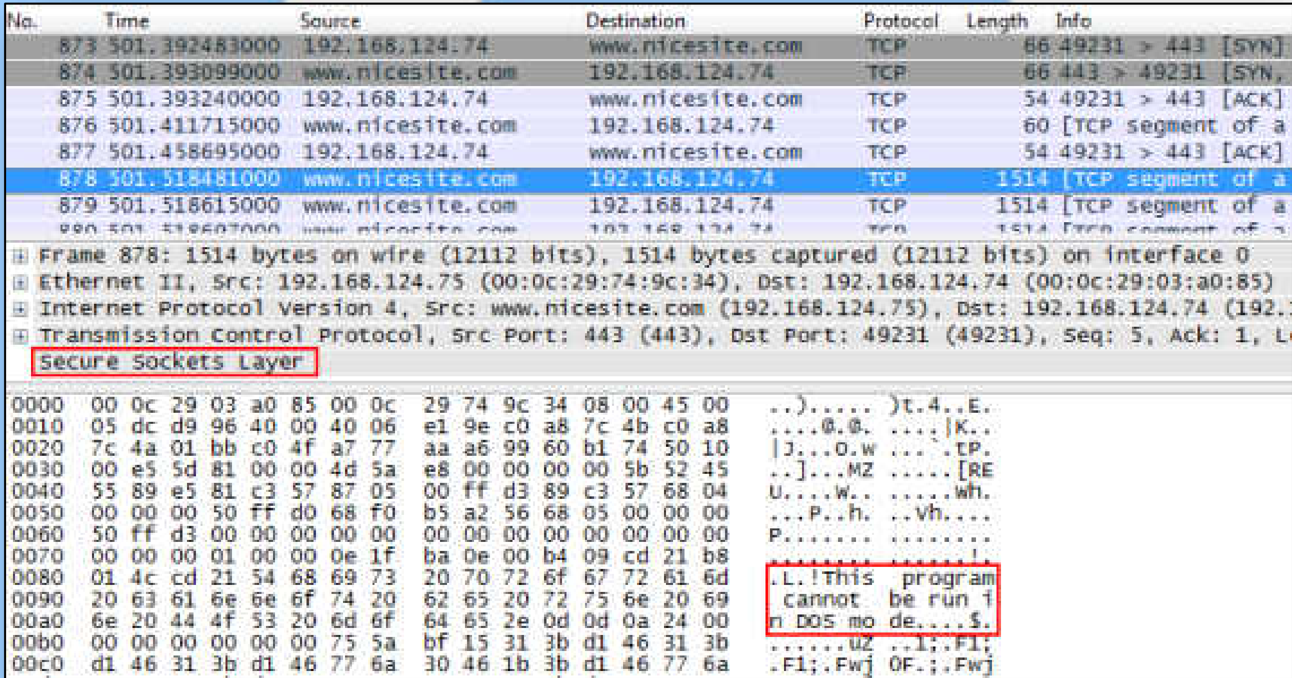


```
.............t$.^1..=...1V.._.-E. 8.[.[...IT..]..9.r..
[[>z..q{....y...Y?...x....[..V.....9....=.8~I....
(..E..V......*.\.....v#...P..V+NyK....*..$ ..c
$9..P........S.Jf5..........hcjSh...?.f..Q......Opu.
N..,@..h4..&.]w.\4$C...TN.B"..;s...s..K{au{6+....
\y .....[s..^?{..P.'.Q;Microsoft Windows XP [Version
5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Snatch\Desktop>
```

Demo 4 – Standard Protocols

- Malware „using“ HTTP, HTTPS, SSL
  - Watch for indications of invalid HTTP(s) or SSL inside the stream
  - Don‘t rely on the dissector stating „Secure Sockets Layer“



```
No.     Time              Source             Destination        Protocol  Length  Info
    873 501.392483000  192.168.124.74     www.nicesite.com     TCP          66 49231 > 443 [SYN]
    874 501.393099000  www.nicesite.com   192.168.124.74       TCP          66 443 > 49231 [SYN,
    875 501.393240000  192.168.124.74     www.nicesite.com     TCP          54 49231 > 443 [ACK]
    876 501.411715000  www.nicesite.com   192.168.124.74       TCP          60 [TCP segment of a
    877 501.458695000  192.168.124.74     www.nicesite.com     TCP          54 49231 > 443 [ACK]
    878 501.518481000  www.nicesite.com   192.168.124.74       TCP        1514 [TCP segment of a
    879 501.518615000  www.nicesite.com   192.168.124.74       TCP        1514 [TCP segment of a
    880 501.518607000  www.nicesite.com   192.168.124.74       TCP        1514 [TCP segment of a
⊞ Frame 878: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: 192.168.124.75 (00:0c:29:74:9c:34), Dst: 192.168.124.74 (00:0c:29:03:a0:85)
⊞ Internet Protocol Version 4, Src: www.nicesite.com (192.168.124.75), Dst: 192.168.124.74 (192.1
⊞ Transmission Control Protocol, Src Port: 443 (443), Dst Port: 49231 (49231), Seq: 5, Ack: 1, Le
  Secure Sockets Layer

0000  00 0c 29 03 a0 85 00 0c  29 74 9c 34 08 00 45 00   ..)..... )t.4..E.
0010  05 dc d9 96 40 00 40 06  e1 9e c0 a8 7c 4b c0 a8   ....@.@. ....|K..
0020  7c 4a 01 bb c0 4f a7 77  aa a6 99 60 b1 74 50 10   |J...O.w ...`.tP.
0030  00 e5 5d 81 00 00 4d 5a  e8 00 00 00 00 5b 52 45   ..]...MZ .....[RE
0040  55 89 e5 81 c3 57 87 05  00 ff d3 89 c3 57 68 04   U....W.. .....Wh.
0050  00 00 00 50 ff d0 68 f0  b5 a2 56 68 05 00 00 00   ...P..h. ..Vh....
0060  50 ff d3 00 00 00 00 00  00 00 00 00 00 00 00 00   P....... ........
0070  00 00 00 01 00 00 0e 1f  ba 0e 00 b4 09 cd 21 b8   ........ ......!.
0080  01 4c cd 21 54 68 69 73  20 70 72 6f 67 72 61 6d   .L.!This  program
0090  20 63 61 6e 6e 6f 74 20  62 65 20 72 75 6e 20 69    cannot  be run i
00a0  6e 20 44 4f 53 20 6d 6f  64 65 2e 0d 0d 0a 24 00   n DOS mo de....$.
00b0  00 00 00 00 00 00 75 5a  bf 15 31 3b d1 46 31 3b   ......uZ ..1;.F1;
00c0  d1 46 31 3b d1 46 77 6a  30 46 1b 3b d1 46 77 6a   .F1;.Fwj 0F.;.Fwj
```

Demo 5 – Paradise Lost?

- Malware using standard HTTPS connection
  - Cannot tell if it contains malicous communication without decryption
  - Breaking HTTPS encryption for e.g. sandboxing appliances sometimes critical from jurisdictional POV

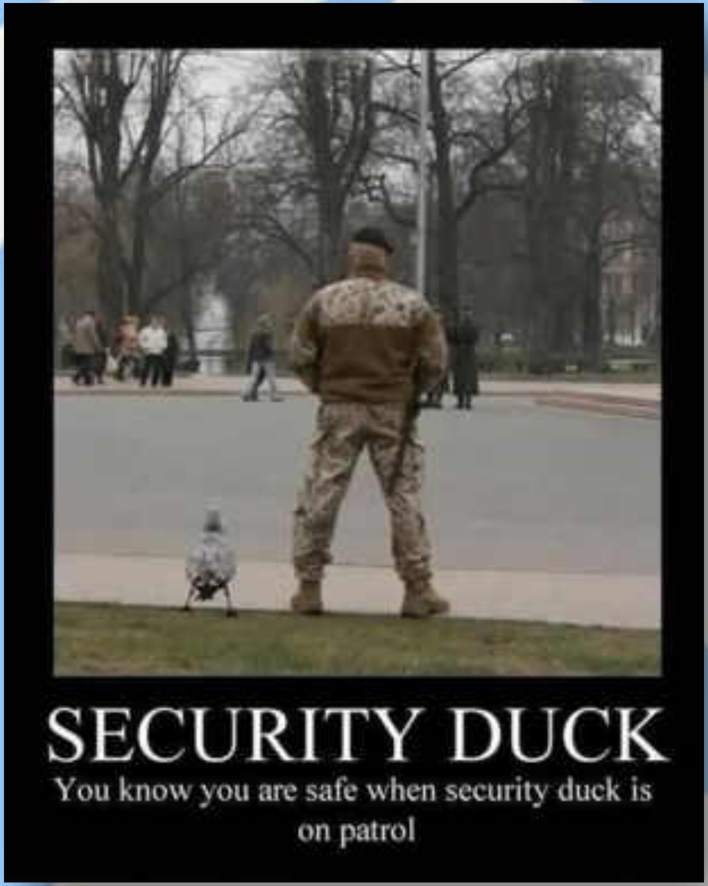
    → private eMail

    → Online Banking
- Welcome to Reputation-based analysis

Defense Strategies

Monitoring Networks - Proactive

- Use NetFlow to monitor meta data
  - Set up alerts for unusual patterns
- Use IDS/IPS with optimized signatures
  - Reduce false positives as much as possible
- Set up Passive DNS / Passive SSL recording servers
  - Helps in tracking down name resolution and certificate history

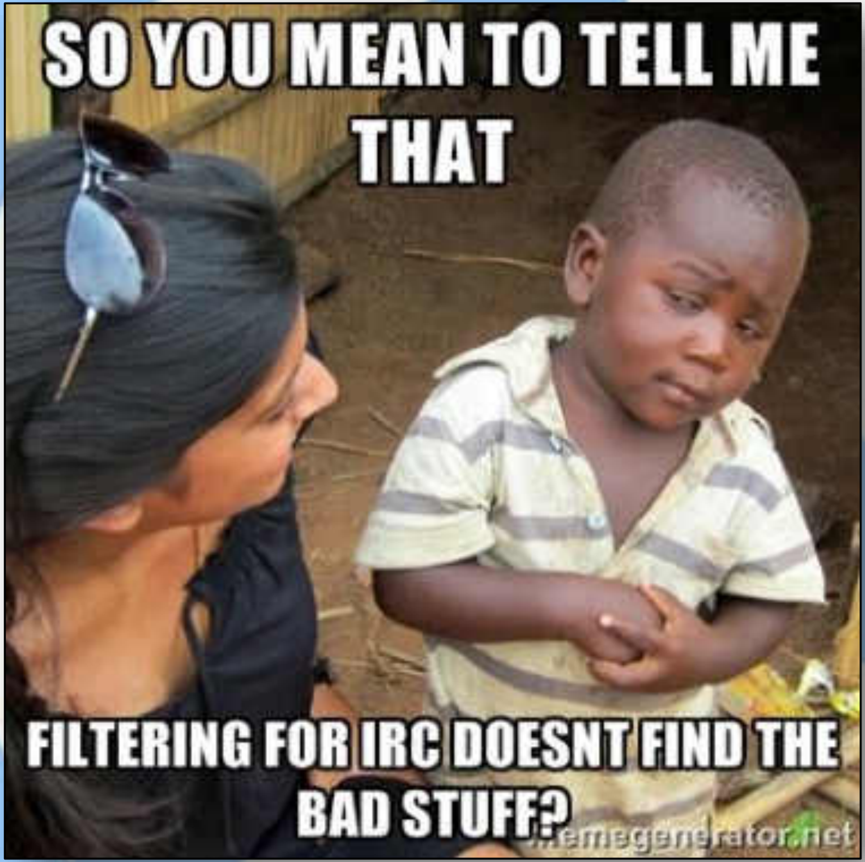


Monitoring Networks - Reactive

- Forensic analysis on full packet captures
  - Has to be recorded before something happened, of course
  - Carefully selected locations, e.g. Internet outbreaks
- Use NetFlow for meta data
  - Long term storage for forensic searches, e.g. „where did the attacker connect to from the infected system?“
- Use IDS/IPS as custom IoC alarm system
  - Write custom IDS rules for known **I**ndicators **o**f **C**ompromise

Detecting malicious traffic

- Forget „silver bullets“ – there is no easy Wireshark filter
- Attackers hide in plain sight
  - DNS, HTTP(S), FTP,...
- Filter out positives
  - E.g. Alexa 1 Million
  - Known update sites: OS, AV, Vendors


SO YOU MEAN TO TELL ME THAT
FILTERING FOR IRC DOESNT FIND THE BAD STUFF?
memegenerator.net

Detecting malicious traffic

- Do a baseline aka “Know your network”
  - Deep Packet inspection
  - Traffic patterns via NetFlow
- If no suspicious activity is found: dive deeper into „good“ traffic
  - Twitter messages
  - Facebook posts
  - Google Docs / Collaboration sites
  - Redirects from TCP:80 to local backdoor

Final Words

- Defending the network is hard work
- Attackers only need to suceed once, defenders would need 100% success
  - Read as: it‘s not „if“ but „when“ an attack will succeed.
  - Expect successful attacks on your network.
- Keep searching
  - It‘s a continuous task
  - Don‘t just wait for some alarm to go off

!! Thank you for your attention !!

Q / A…