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
„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
  • Web Application Firewalls 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• Outdated rules stay in the table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 prevent malicious traffic it detects
  • 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
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

<table>
<thead>
<tr>
<th>DNS</th>
<th>87 Standard query 0x5c09</th>
<th>A yhqzpwovcatogcypxkvshq.org</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>88 Standard query 0xfc8f</td>
<td>A gqxsvojmrqlootxcsqzw.net</td>
</tr>
<tr>
<td>DNS</td>
<td>93 Standard query 0x603e</td>
<td>A xccujrskozmfjzhdatgxhkrbimai.com</td>
</tr>
<tr>
<td>DNS</td>
<td>89 Standard query 0x79de</td>
<td>A krshyqsigihcydwiianflxsk.ru</td>
</tr>
<tr>
<td>DNS</td>
<td>90 Standard query 0xad7c</td>
<td>A onhuptgewbagijntsonztzlhq.com</td>
</tr>
<tr>
<td>DNS</td>
<td>87 Standard query 0x6104</td>
<td>A yptkeikuxwptshjvtnvdrd.net</td>
</tr>
<tr>
<td>DNS</td>
<td>87 Standard query 0xb2f9</td>
<td>A eiwnjsghuqhyvitjfpwvhm.org</td>
</tr>
<tr>
<td>DNS</td>
<td>95 Standard query 0x4e58</td>
<td>A ukvcccdbzflfivgljvqygrwpgjcmyn.info</td>
</tr>
<tr>
<td>DNS</td>
<td>88 Standard query 0x680</td>
<td>A gurvkyoswmdexybagmzkh.biz</td>
</tr>
<tr>
<td>DNS</td>
<td>90 Standard query 0x4065</td>
<td>A wgtjfinfntkytcurswpbdstsdz.ru</td>
</tr>
<tr>
<td>DNS</td>
<td>90 Standard query 0xc6cf</td>
<td>A jxbrmwytcxrvxkhtbyzldmmjn.j.com</td>
</tr>
<tr>
<td>DNS</td>
<td>89 Standard query 0x48c</td>
<td>A wtpzr1lveaqkzhmaifyztdgx.info</td>
</tr>
</tbody>
</table>

• 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
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“
Demo 5 – Paradise Lost?

• Malware using standard HTTPS connection
  • Cannot tell if it contains malicious 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
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 Indicators of Compromise

Sharkfest 2014
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
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 succeed 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...

That's all Folks!