The Needle in the Haystack

Jasper Bongertz
17 June 2015

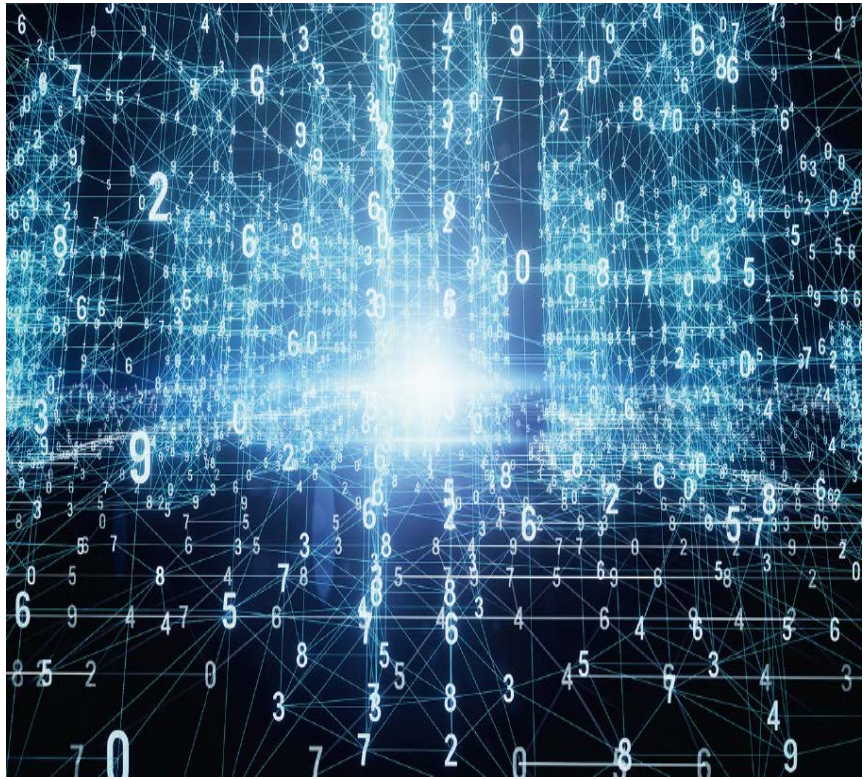
AIRBUS
DEFENCE & SPACE

The Haystack

In an **incident response** situation at least one Indicator of Compromise has been found already

The **haystack** is all of the IT infrastructure that needs to be checked:

- Clients
- Servers
- Network
- ISP uplinks



AIRBUS DEFENCE & SPACE

Looking for the Needle

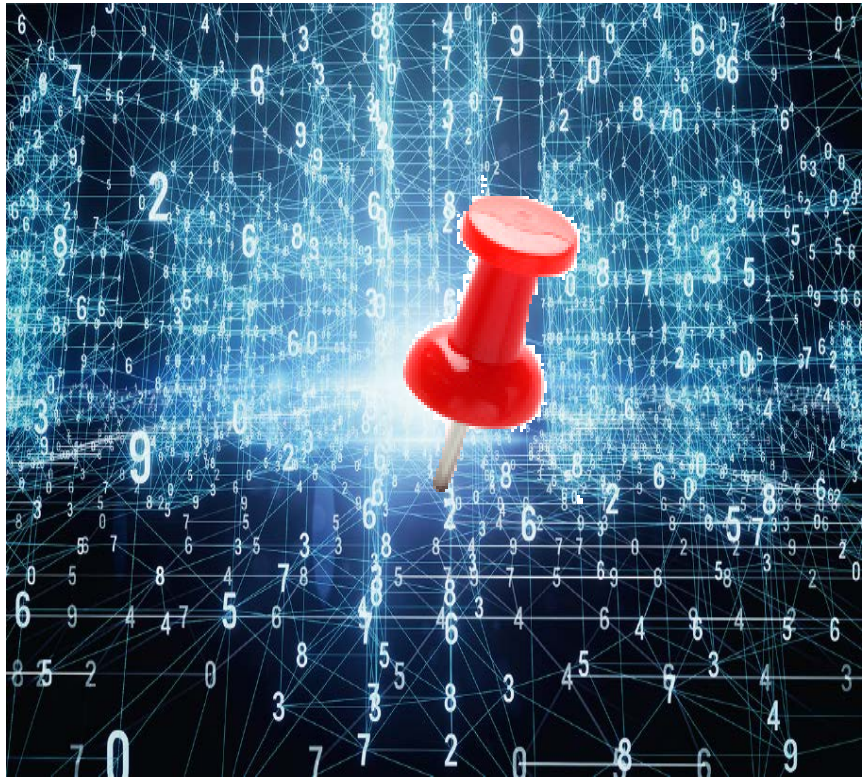
The challenge:

Telling what systems have really been compromised

So how do we usually do that?

Looking at:

- file systems
- log files
- firewall rule tables
- sensor hits (IDS/IPS/NSM/AV/Sandboxes)
- documentation



AIRBUS DEFENCE & SPACE

Looking at the network

Network forensics can be an effective way to spot potential „Needles“

No matter how good **malware hides**, it‘ll use the network sooner or later

- „No place to hide“ if sniffing packets at the right spot

Challenges:

- Sniffing packets at the „right spot“
- Scanning through gazillions of packets, looking for IoCs

AIRBUS DEFENCE & SPACE

Best practices

Looking at Internet uplinks

- Usually there are only a couple of them
- Problem: undocumented/“rogue“ uplinks

Inspecting DNS

- Can be stored a long time, e.g. using PassiveDNS
- Finding CnC patterns:
  - Answers containing Loopback addresses
  - High amount of errors like „no such name“
  - Domain Generation Algorithms
- Still need to sort out false positives

AIRBUS DEFENCE & SPACE

Best practices

Leveraging NetFlow

- Long term storage of metadata of communication flows
- Helps tracking lateral movement of attackers and building timelines
- Can also be used for event correlation

Baselining suspicious systems

- Record everything it does
- Using SPAN ports/TAPs
- Pinpoint assets that require file system forensics

AIRBUS DEFENCE & SPACE

Demo

AIRBUS DEFENCE & SPACE

Thank you!
Questions?