Practical Applications of AI in Cybersecurity — Threat Detection, Prevention, Containment and Response

Rik Turner

Principal Analyst, Infrastructure Solutions

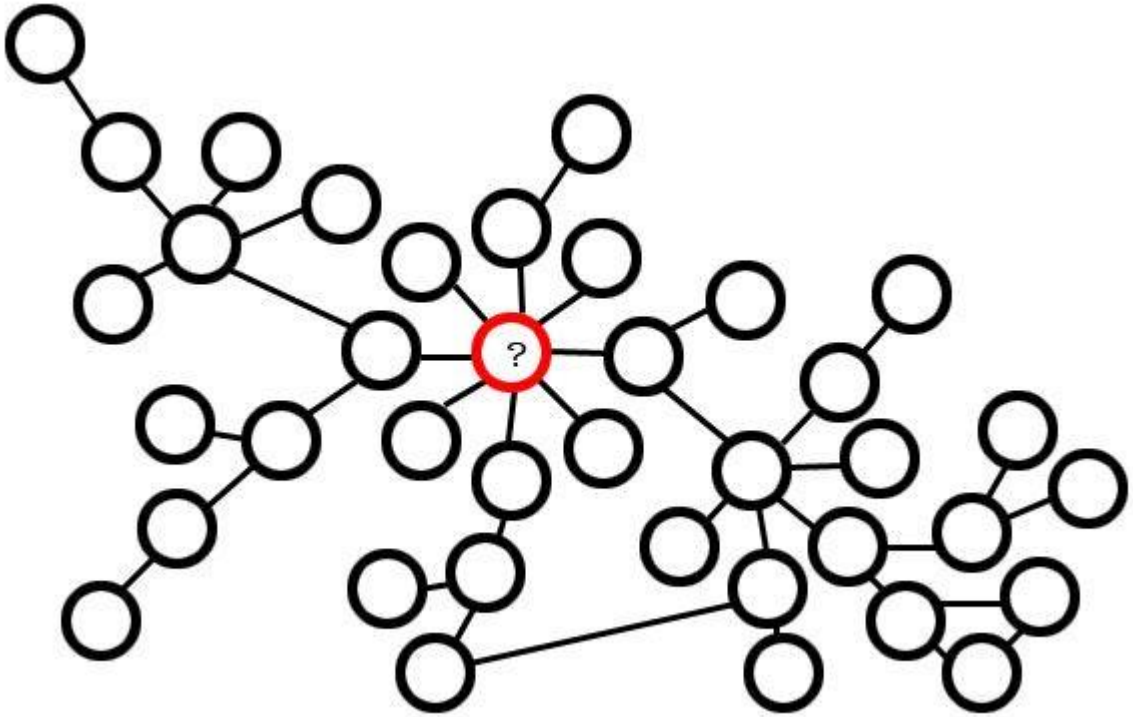
Ovum

rik.turner@ovum.com

What's going on in Cybersecurity?

1990s | 2000s | 2010s

The Signatures-based Paradigm



Find Patient Zero…

The Signatures-based Paradigm

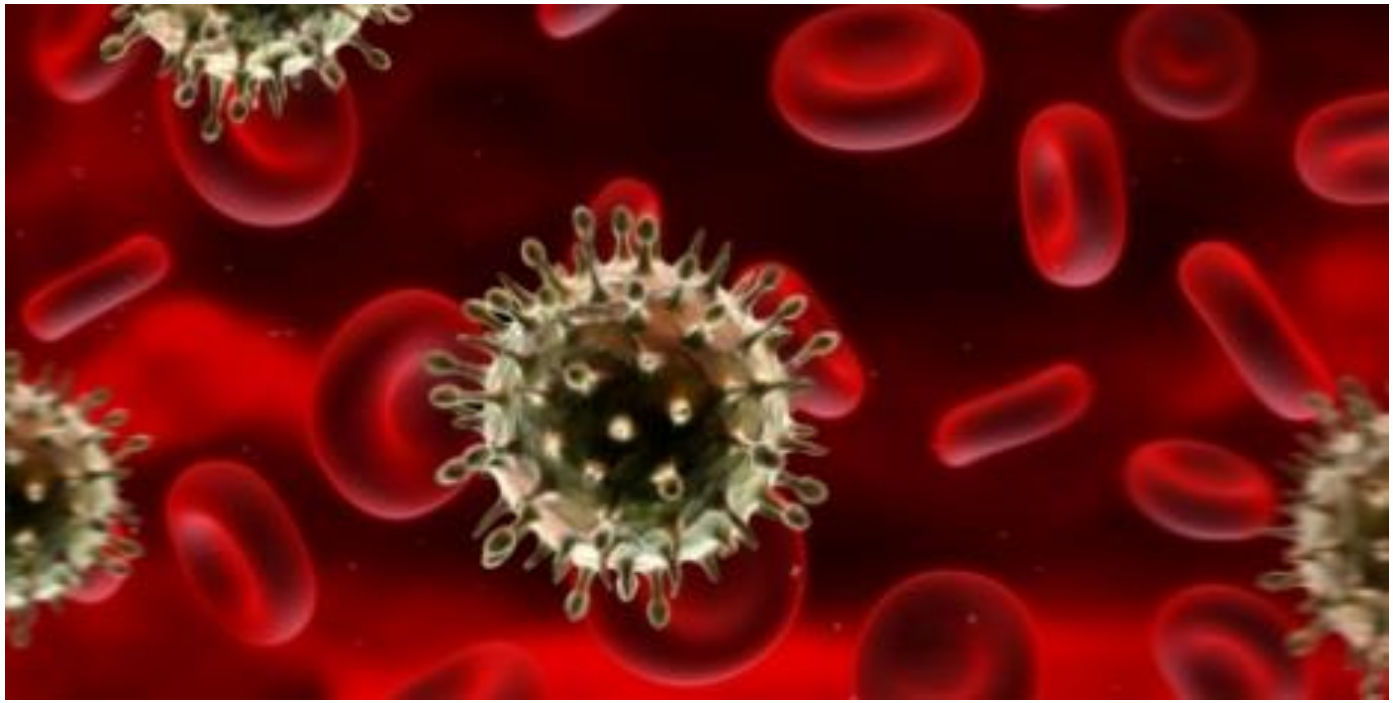
Create an antidote (i.e. a signature)…

The Signatures-based Paradigm

…and disseminate to immunise all other machines

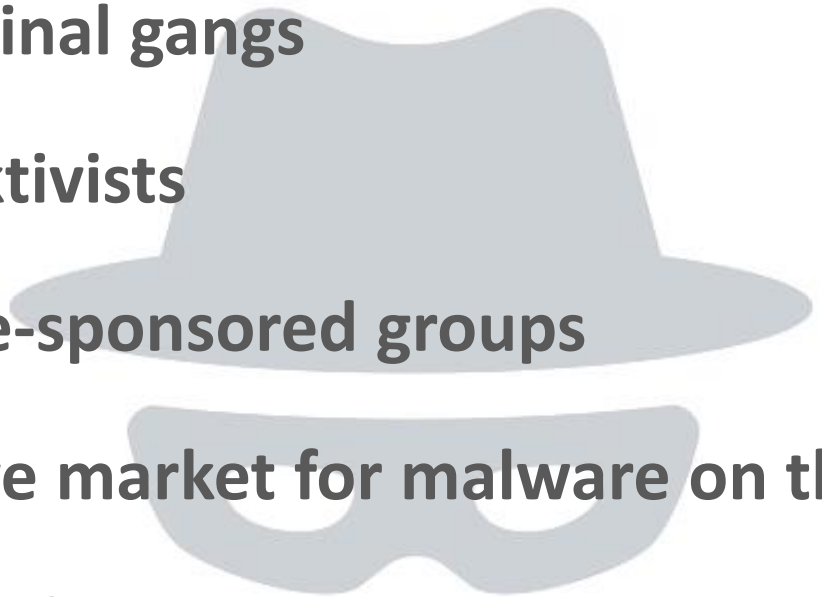
But now…

Anti-virus signatures catch no more than 30%-40% of malwares



Why?

- **Many more malware actors:**
  - **Criminal gangs**
  - **Hacktivists**
  - **State-sponsored groups**
- **An active market for malware on the Dark Web**
- **The Cloud**



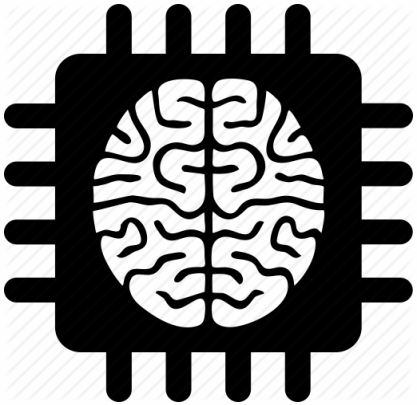
So now… NEW DETECTION TECHNOLOGIES

Sandboxing

UEBA

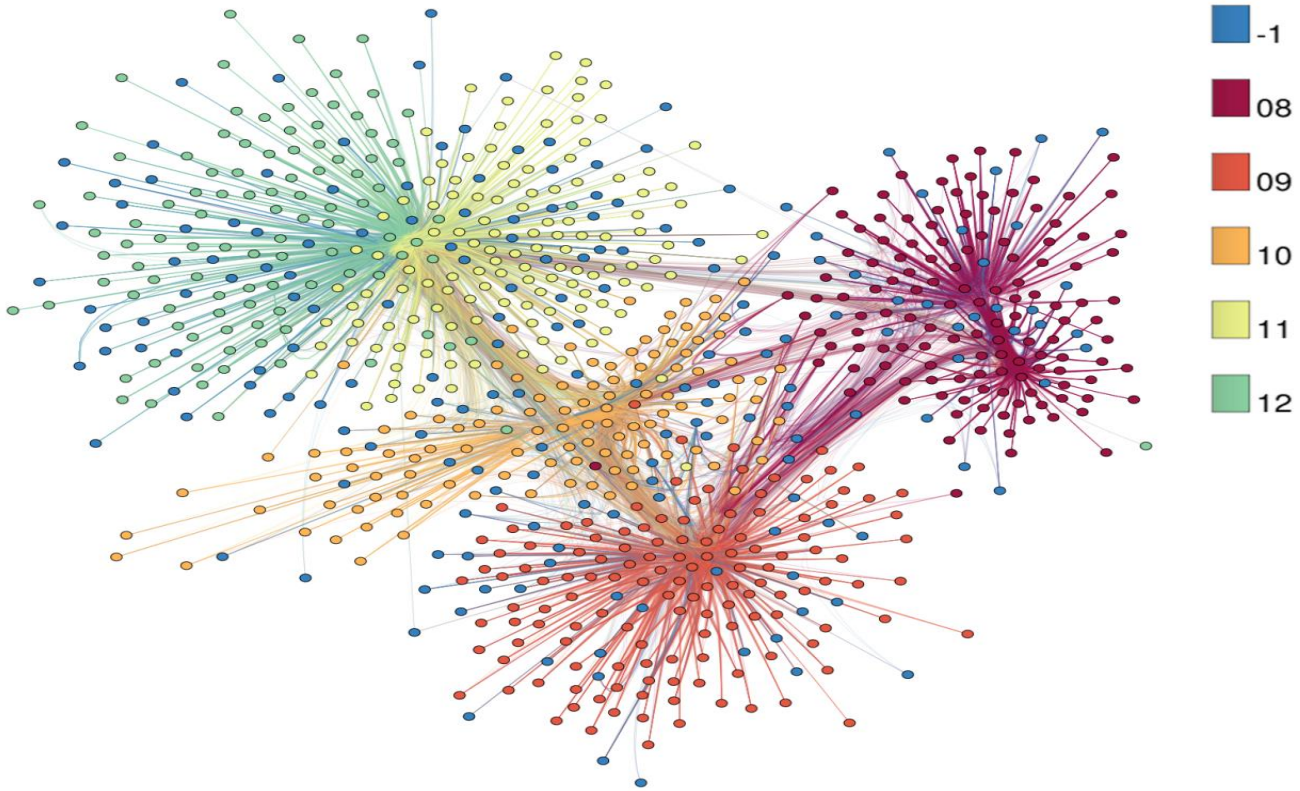
EDR

AI / Machine Learning



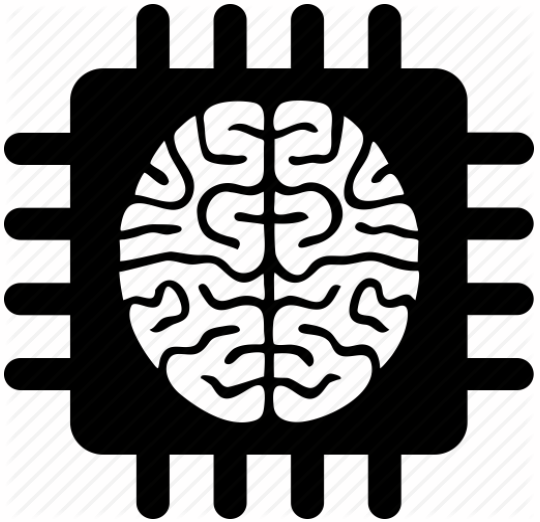
NEW DETECTION TECHNOLOGIES (cont'd)…

Threat Intelligence



Tasks for AI/Machine Learning in Cybersecurity

1. Model “Normal” to Alert on “Abnormal”
2. Filter out the noise in Threat Intel
3. Find hidden trends



Copyright notice and disclaimer