Back to life, Back to correlation

A realistic approach to botnet detection across your IS

Vasileios Friligkos
Security Analyst at CERT-INTRINSEC

Botnets - Heterogeneity

- Architecture
  - Central mode
  - Distributed mode
- Communication
  - IRC
  - HTTP
  - P2P
  - TOR
- Infection – Propagation
  - Phishing
  - Software vulnerabilities
- Motives
  - Hacktivism
  - Fraud
  - Espionage
- Malicious actions
  - DDoS
  - Web Inject
  - Spamming

Botnets – Common behavioral characteristics

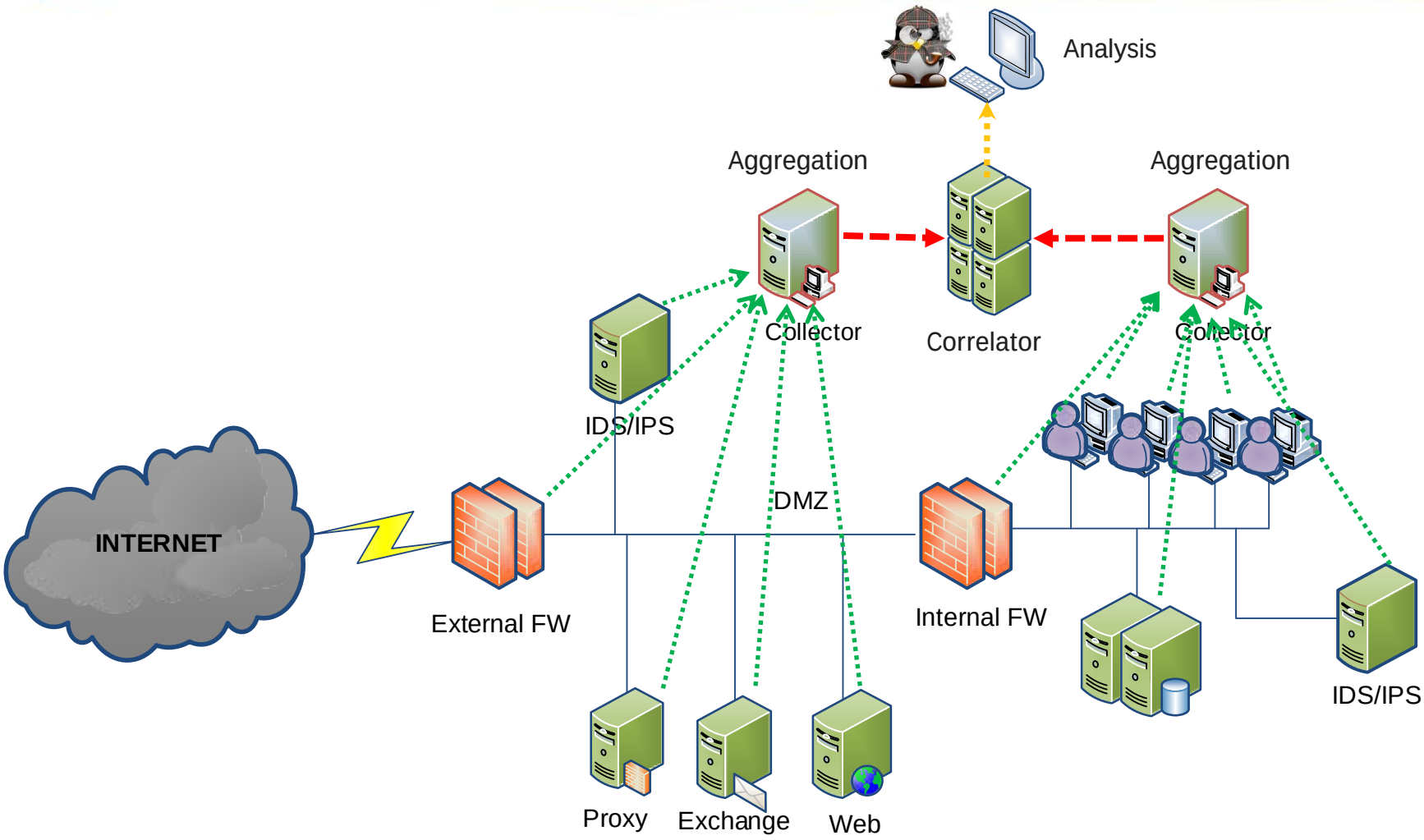
- Infection
- Propagation
- Receive commands – Be coordinated
- Perform malicious actions

→ Elements to identify botnet activity

Procedure

- Centralization – Formalization
  - Common description protocol
  - Log enrichment with metadata
- Data Aggregation
  - Minimize data volume
  - Keep all necessary information
- Correlation
  - Temporal: ordered sequence of events
  - Spatial: events across multiple sources
  - Rule-based: based on detection signatures
  - Statistical: based on learned baseline and deviations

Procedure


Analysis
Aggregation
Aggregation
Collector
Correlator
Collector
IDS/IPS
INTERNET
DMZ
External FW
Internal FW
IDS/IPS
Proxy
Exchange
Web

Malware – Scenario

- New malware variant
  - No antivirus detection
  - No network activity signature-detection – IDS/IPS
- No blacklisted target IP or Domain Name
  - Unknown C&C servers
  - P2P architecture
- Malware already established inside the network

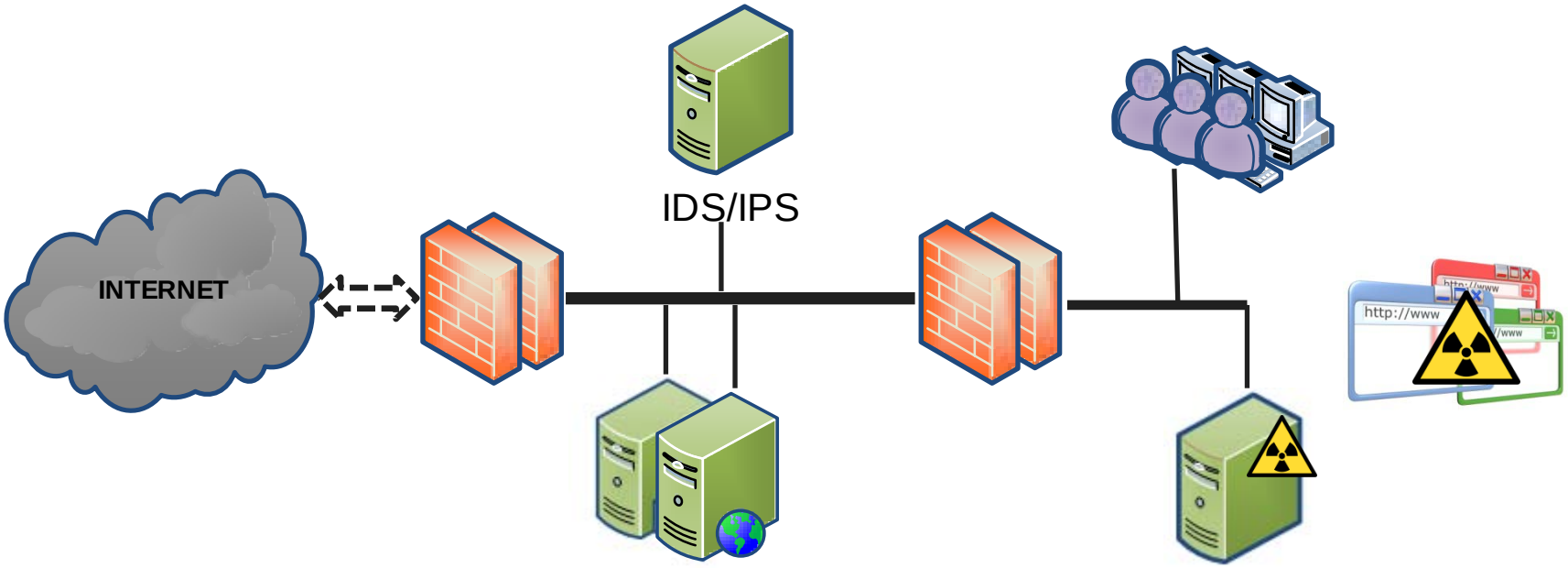
So, no “conventional” means of detection

Deviations from normal behavior

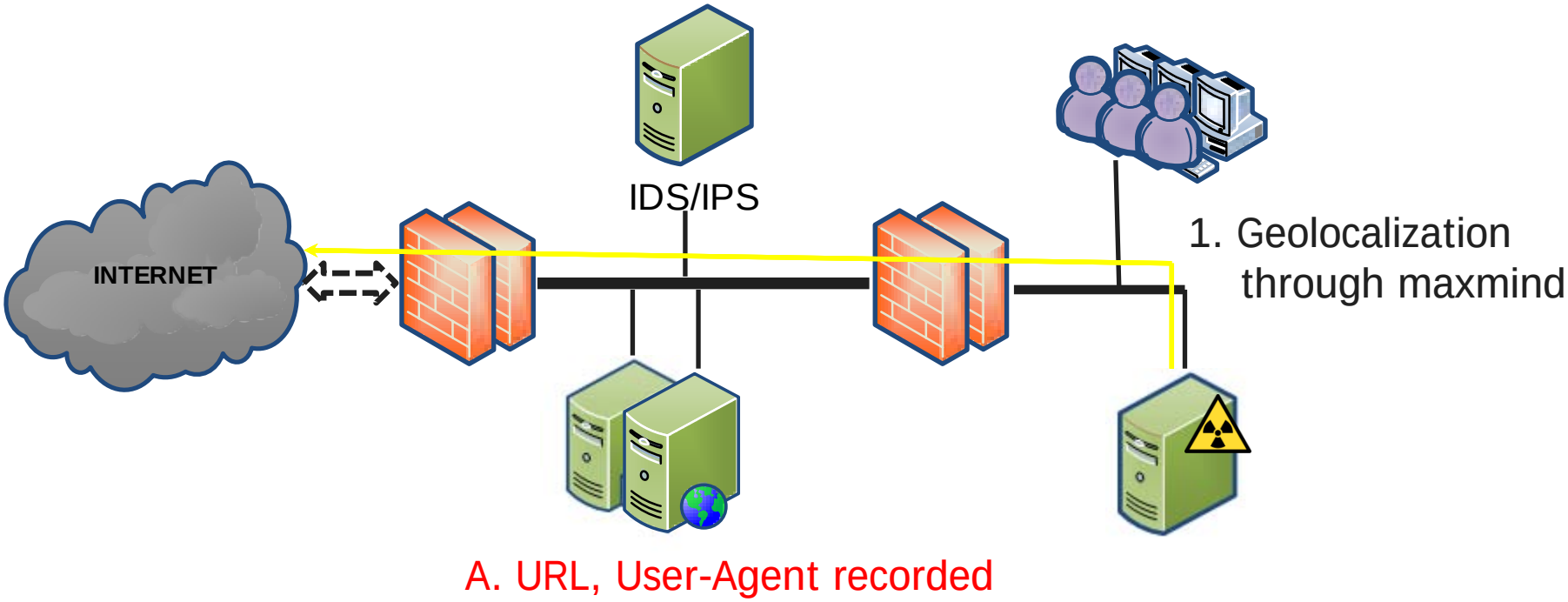
Ex.

- Unusual traffic – Ports, volume, destination addresses
- Unusual resources overload
- Outgoing replay of same incoming behavior

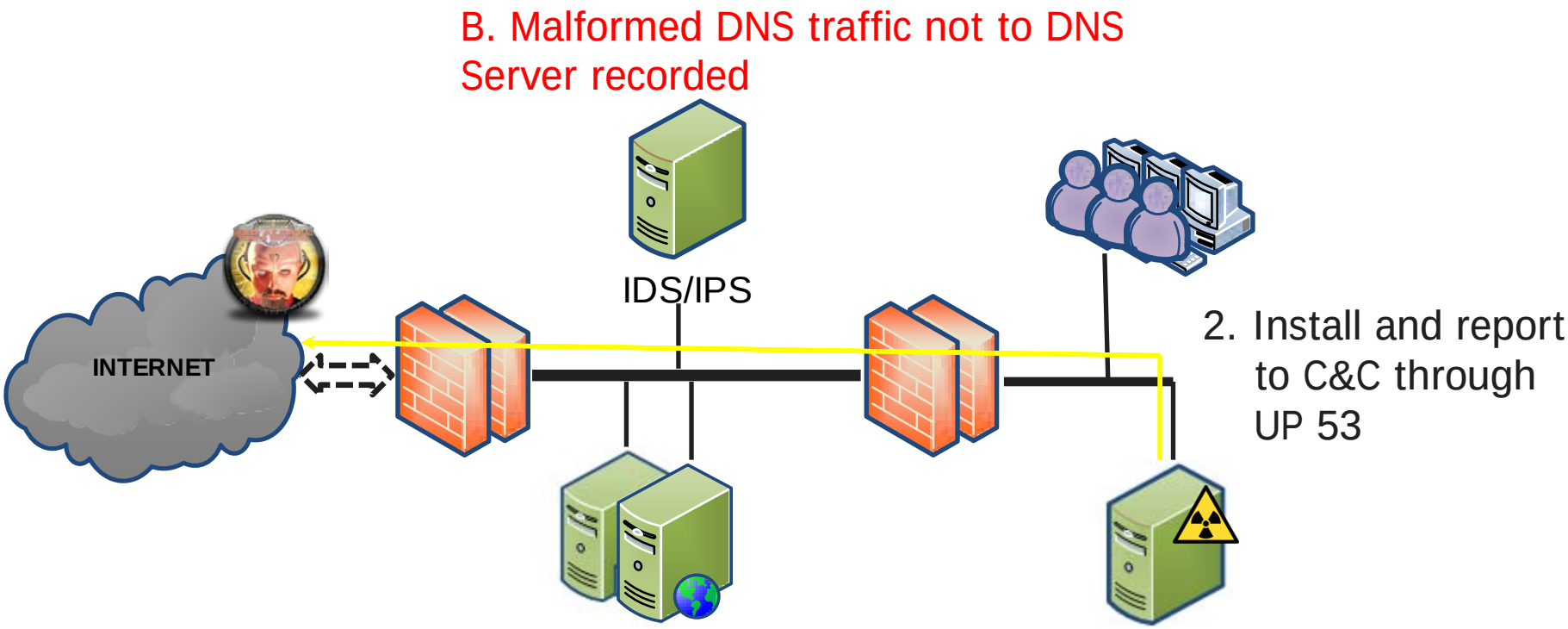
ZeroAccess



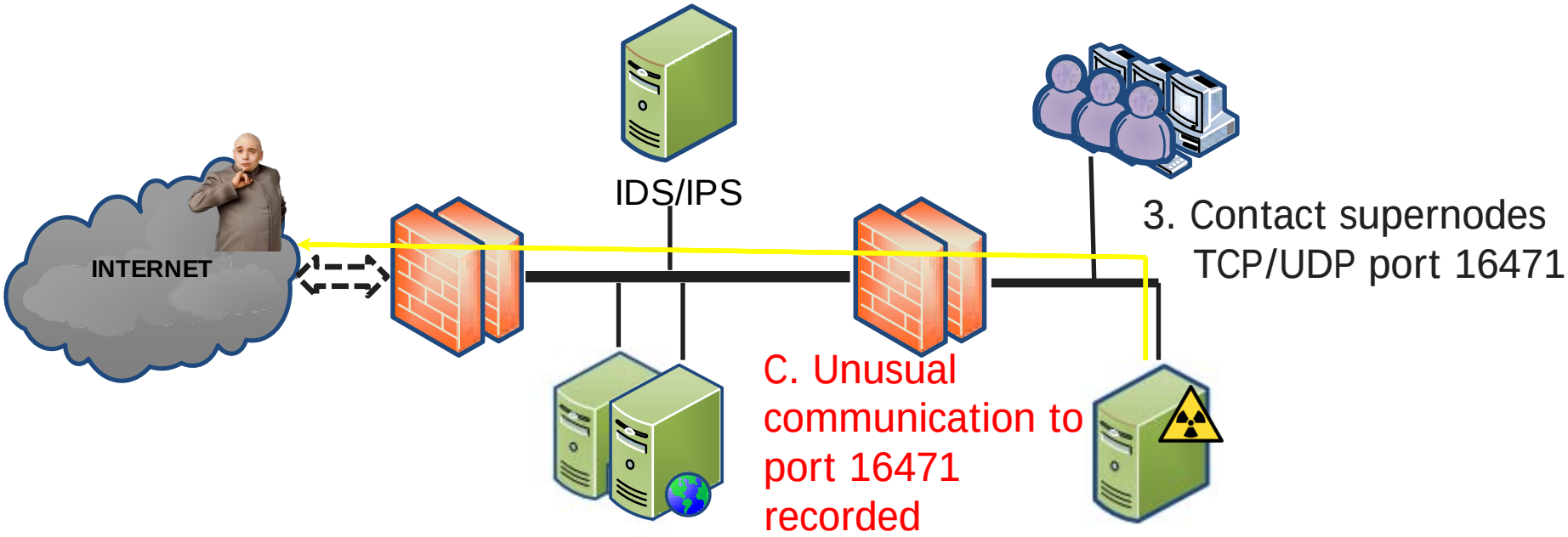
ZeroAccess


IDS/IPS
INTERNET
1. Geolocalization
through maxmind
A. URL, User-Agent recorded

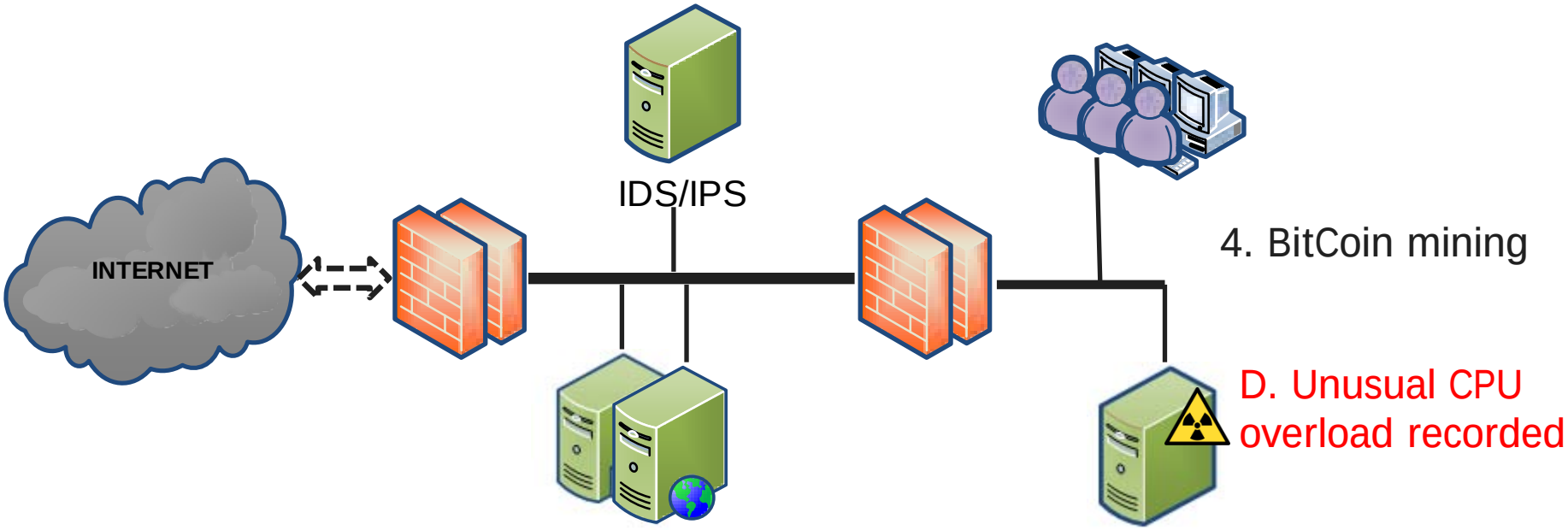
ZeroAccess


B. Malformed DNS traffic not to DNS Server recorded
IDS/IPS
INTERNET
2. Install and report to C&C through UP 53

ZeroAccess


IDS/IPS
INTERNET
3. Contact supernodes
TCP/UDP port 16471
C. Unusual
communication to
port 16471
recorded

ZeroAccess


IDS/IPS
INTERNET
4. BitCoin mining
D. Unusual CPU overload recorded

ZeroAccess

Correlation

1. Malformed DNS traffic not to DN Server
2. Unusual communication to port 16471 over a long period
3. Unusual CPU overload over long period

→ Incident: Potential Infection – Unusual Behavior

Malware – Indicators of Compromise

- Further enhance detection across your IT system
  - Detection and Investigation of malware
  - Artifacts and Behavior associated to the threat
  - Construction of Indicator of Compromise
  - Investigation using IoC

ZeroAccess

Indicators of Compromise

1. 53/UDP traffic not to designated DNS
   AND
   8-9 bytes set to our country code (XORed)

2. User-Agent = User-Agent of ZeroAccess

....

Conclusion

Automated Correlation across the IT infrastructure allows to:

- Obtain situational awareness
- Decrease false positives
- Increase detection rates

However, it cannot replace human intervention

→ Still, it can provide all necessary threat intelligence

Thank you for your attention

Questions?