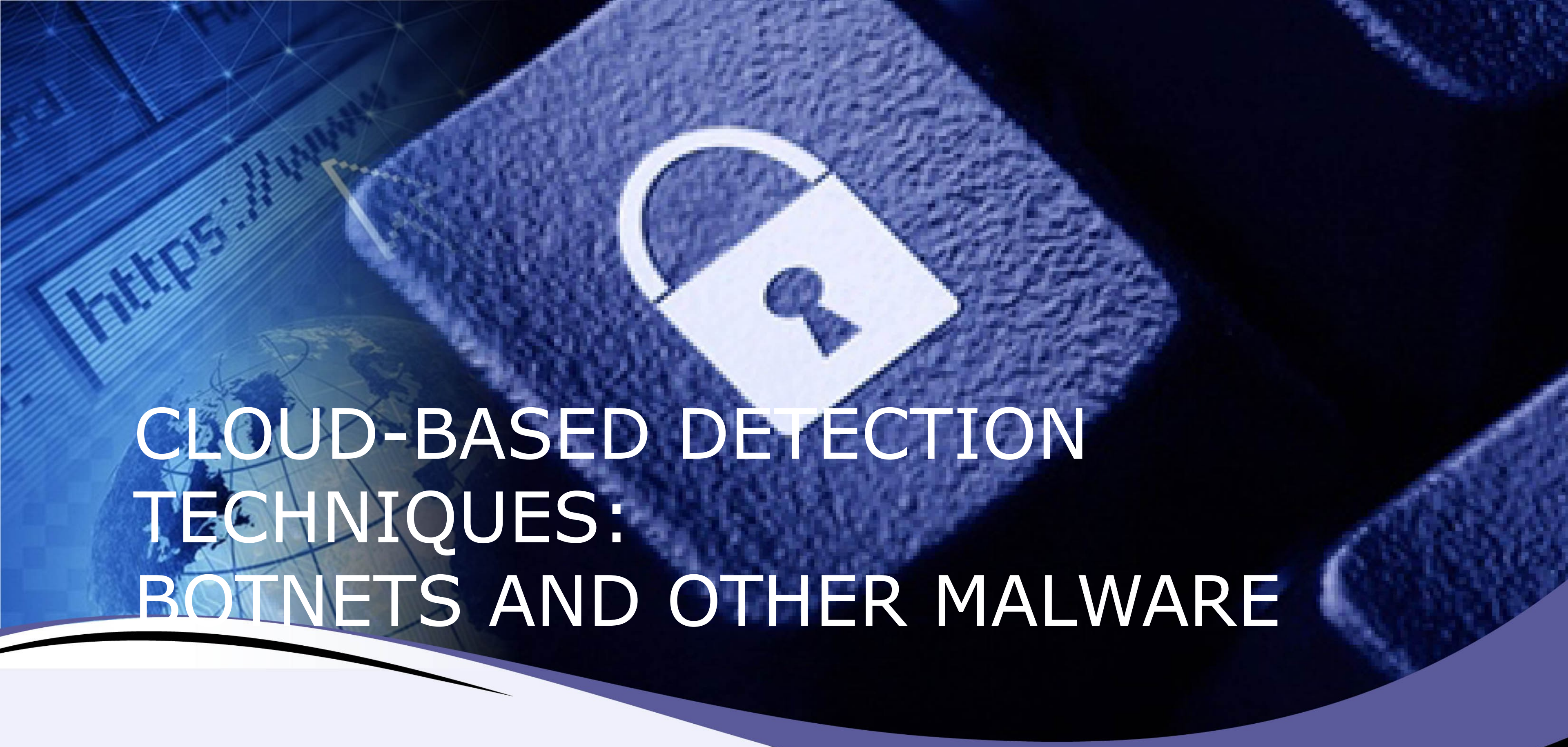


CLOUD-BASED DETECTION TECHNIQUES: BOTNETS AND OTHER MALWARE

Mark Graham
Anglia Ruskin University

OWASP
The Open Web Application Security Project

INTRODUCTION

Mark Graham

Ph.D. Candidate at Anglia Ruskin University

"Behaviour of Botnets and Other Malware in Virtual Environments"

Supervisor: Adrian Winckles

M.Sc. Network Security at Anglia Ruskin University

15 Years in the IT Industry

OWASP
The Open Web Application Security Project

AGENDA

Malware attack vectors are evolving

Botnets

Weaknesses of traditional Anti-Virus software

Signature-less detection methods

ADVANCED MALWARE

Malware propagation methods are changing

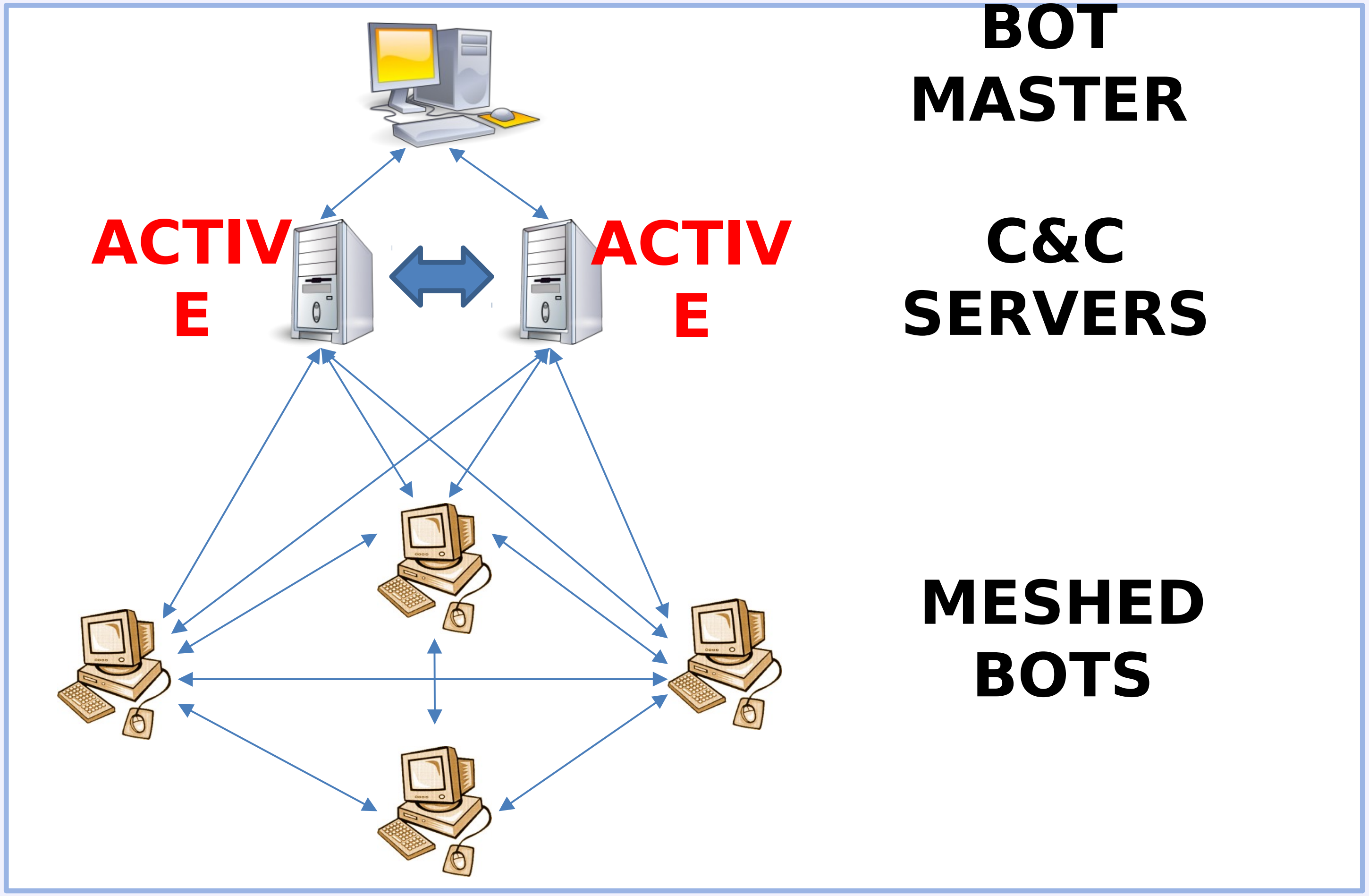
1st Generation Malware - Virus

2nd Generation Malware - Worms/Trojans

3rd Generation Malware - Botnets

OWASP
The Open Web Application Security Project

BOTNETS



BOT
MASTER

C&C
SERVERS

MESHED
BOTS

TRADITIONAL ANTI-VIRUS SOFTWARE IS "DEAD" [1]

Signature-based detection requires a sample of malware

- No Zero-Day protection
- Cannot cope with malware variants
- False positives
- Post-infection protection

[1] Brian Dye, Senior VP for Information Security, Symantec. May 2014

BOT EVOLUTION

Centralised

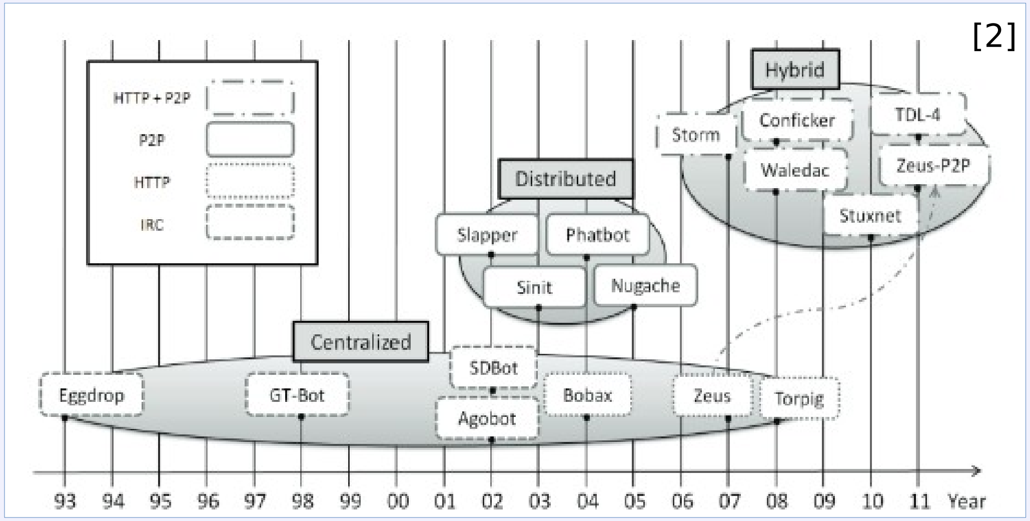
- IRC (Agobot)
- HTTP (Zeus)

De-centralised

- WASTE(PhatBot)
- Overnet (Storm)

Hybrid

- (Zeus/SpyEye)


[2]

[2] Rodriguez-Gomez R., Macia-Fernandez G., Garcia-Teodoro P., 2013. Survey and Taxonomy of Botnet Research through Life-Cycle

SIGNATURE-LESS DETECTION

We can detect Botnets because:

Bots must talk to their C&C server

Bots use the Internet

Bots typically use HTTP

DNS EVASION TECHNIQUES

Fluxing

- IP Fluxing
- Domain Fluxing
- Domain Generation Algorithm (DGA)

FLOW

A uni-directional stream of packets that pass through a network element and share a common[3] set of attributes

NetFlow was developed by Cisco System in 1996

IPFIX (NetFlow v9) – defined in RFC 7011 - 7016

When used to identify agents producing additional load on the network, NetFlow is effective in identifying unusual programs such a[4]s botnets

[3] Drago, I., Barbosa R., Sadre, R., Pras A. and Schonwalder J., 2011. Report of the Second Workshop on the Usage of NetFlow/IPFIX

[4] Amini, P., Azmi, R., Araghizadeh, M., 2014. Botnet Detection using NetFlow and Clustering

CORRELATION

Vertical Correlation

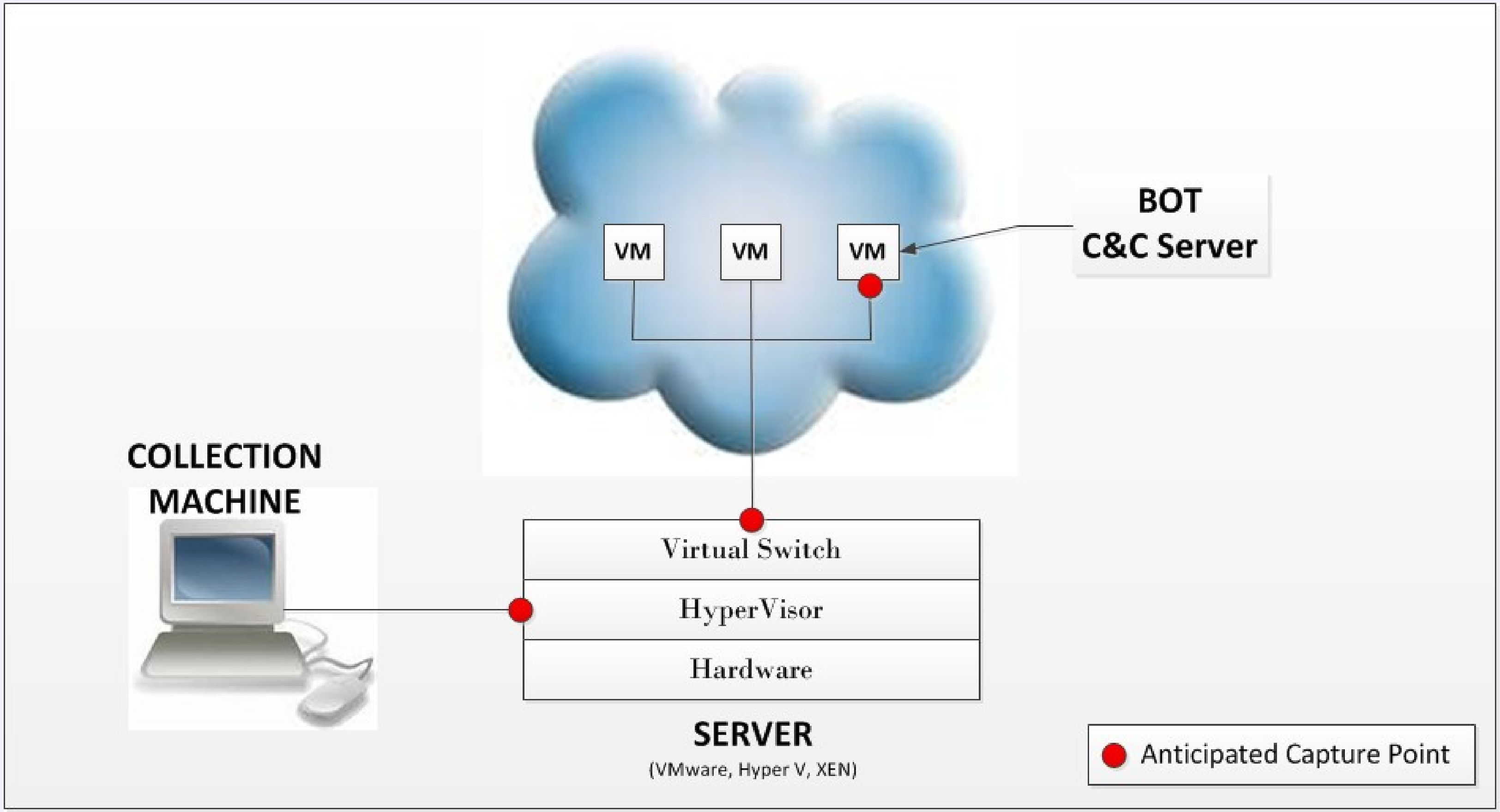
Detection of individual bots by correlating bot related [5] activities (outbound scans, C&C domain visits, and bots downloaded)

Horizontal Correlation

Detection of botnets by correlating network events to identify two or more hosts involved in similar, [6] malicious communications

[5] Bilge L., Balzarroit D., Robertson W., Kirda E. and Kruegle C., 2012. Disclosure: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow

DETECTION TECHNIQUES IN VIRTUAL



SUMMARY

Signature-based Anti-Virus

- Struggles with variants
- Struggles with Zero Day malware
- Post-infection forensic techniques

Signature-less cloud-based detection

- DNS, Flow
- Correlation, Clustering
- C&C takedown, rather than endpoint disinfection

THANK YOU

MARK GRAHAM

mark.graham@anglia.ac.uk