Detecting Malware through Dialog Correlation in Software Defined Networking

Bushra A. Alahmadi and Ivan Martinovic
Bushra.Alahmadi@cs.ox.ac.uk, Ivan.Martinovic@cs.ox.ac.uk

Overview:

Threat Model: Malware, botnets, Advanced Persistent Threats (APT).

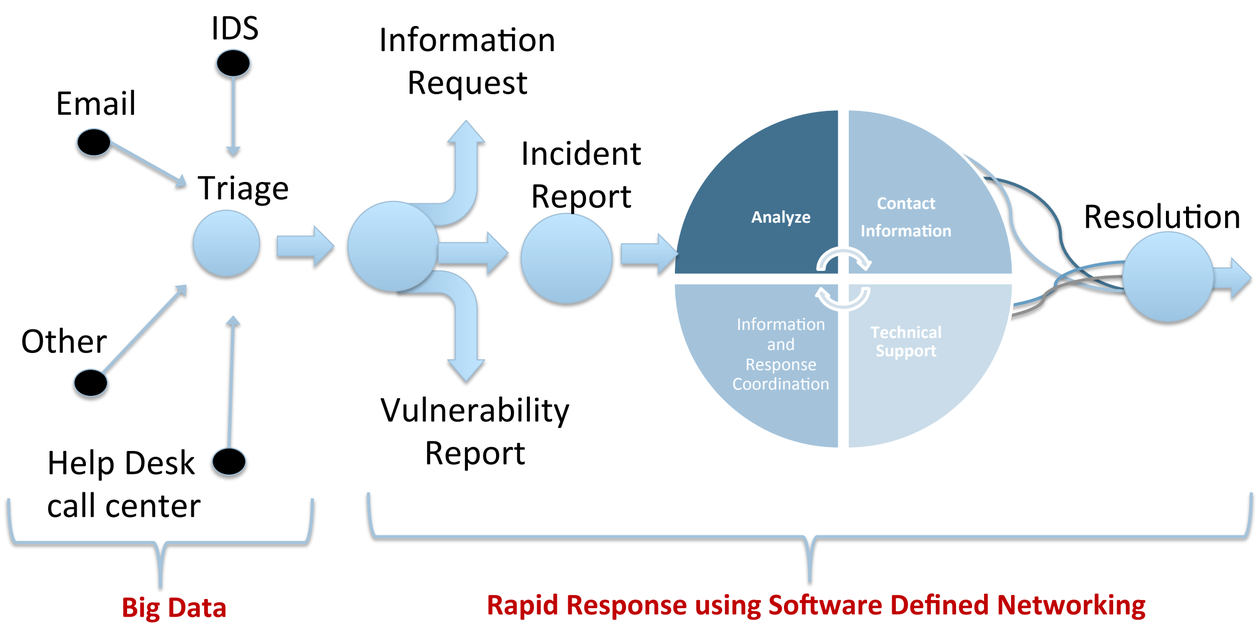
Big Data: On its path of destruction, malware produce a series of events **E** that are recorded in logs. There is a need to provide a system capable of correlating these events to provide analysts with more visibility, when multiple security devices trigger an alert in response to an action, then it's likely that that action is malicious.

Software Defined Networking (SDN): allow greater control over network entities by decoupling the control plane and the forwarding plane enabling the network control to become directly programmable.

Objective: Rapid malware detection and response by leveraging SDN Capabilities.

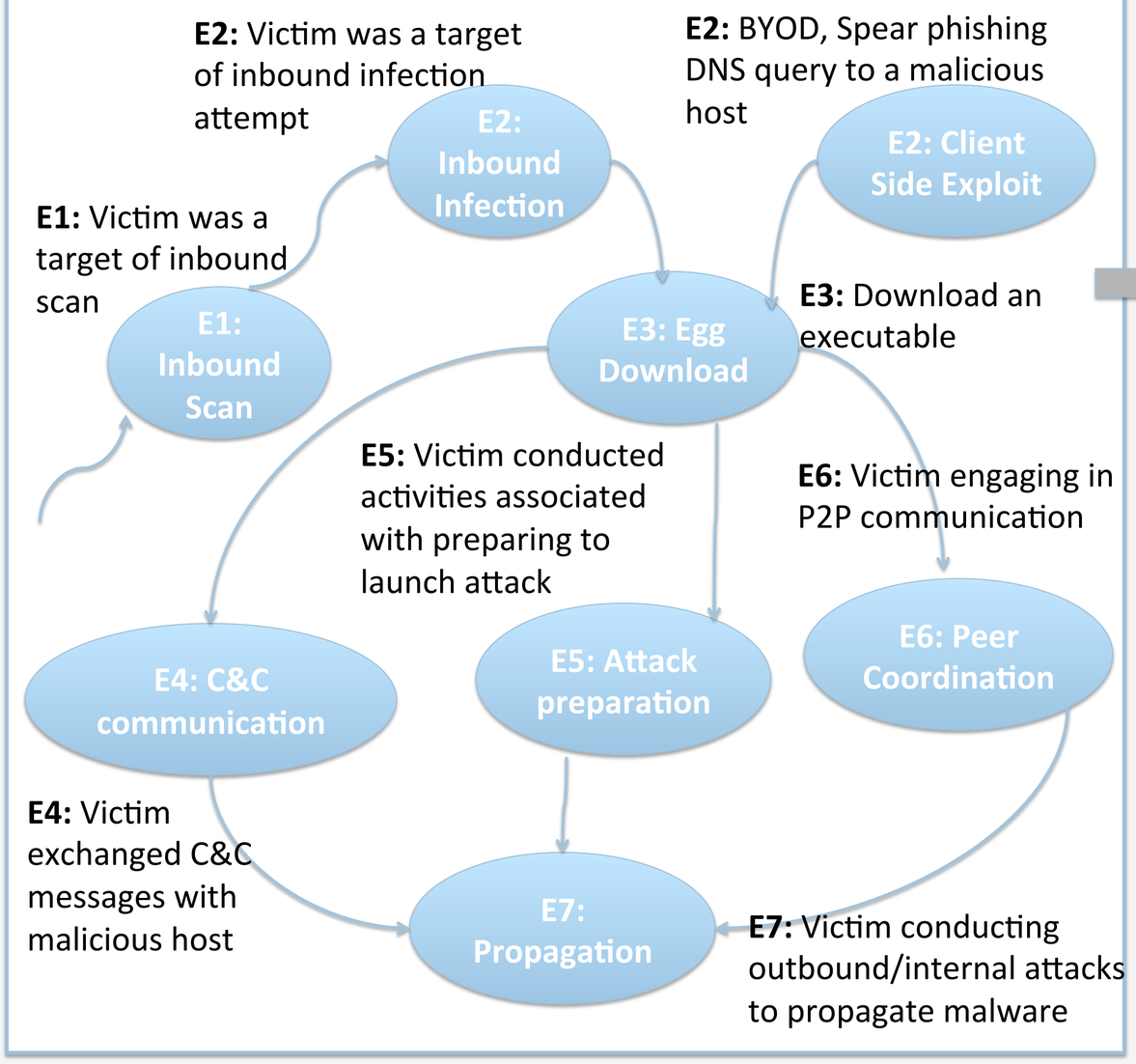
BotHunter: We present a framework inspired from *BotHunter [1]* to track malware communications and develop an evidence trail of message exchanges that match a state-based infection sequence model (*dialog-based correlation [1]*).

Motivation - Security Operations Challenge:

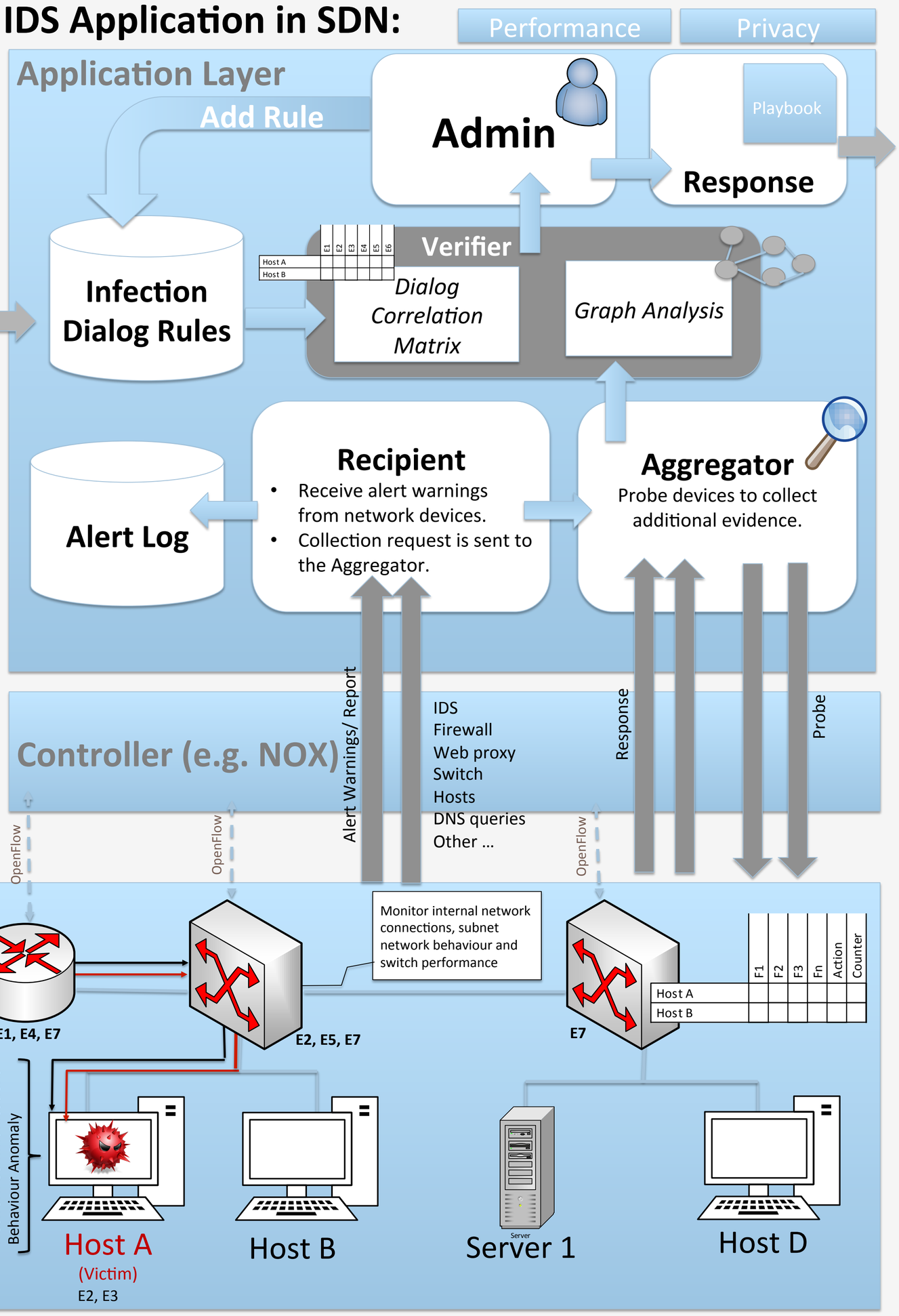


CMU CERT/CC Incident Life Cycle [2]

Infection Dialog Model [1]:



IDS Application in SDN:



References:

1. Gu, G., Porras, P. A., Yegneswaran, V., Fong, M. W., & Lee, W. (2007, August). BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. In *Usenix Security* (Vol. 7, pp. 1-16).
2. West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (CSIRTs)* (No. CMU/SEI-2003-HB-002).
3. Carnegie-mellon univ pittsburgh pa software engineering inst.
4. Gu, G., Perdisci, R., Zhang, J., & Lee, W. (2008, July). BotMiner: Clustering Analysis of Network Traffic for Protocol-and Structure-Independent Botnet Detection. In *USENIX Security Symposium* (Vol. 5, No. 2, pp. 139-154).
5. Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006, October). A multifaceted approach to understanding the botnet phenomenon. In *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement* (pp. 41-52). ACM.
6. Dhawan, M., Poddar, R., Mahajan, K., & Mann, V. (2015). SPHINX: Detecting security attacks in software-defined networks. In *Proceedings of the 2015 Network and Distributed System Security (NDSS) Symposium*.

CENTRE FOR DOCTORAL TRAINING *in* CYBER SECURITY