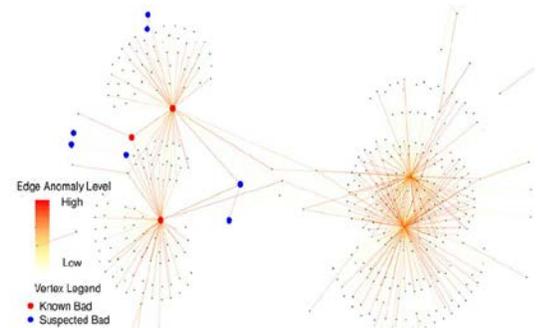


LANS TECHNOLOGY & INTELLECTUAL PROPERTY SUMMARY

See attached technology summaries and technical papers for more information

PathScan targets the traversal behavior of hackers inside a computer network by building behavioral models to reflect normal activity, followed by passively monitoring network traffic and comparing it with the behavioral models. LANS’s three step approach includes:

- building statistical models to characterize the network traffic between each pair of communicating computers;
- breaking the network into millions of small paths; and
- passively monitoring each path and testing whether the data observed is likely to be normal according to the models built in Step 1 or, alternatively, the data appears to be caused by a hacker moving along this path.



With a single commodity Symmetric Multi-Processing (SMP) machine, we are able to rapidly analyze LANL’s 20,000 node unclassified network, examining the network in near real-time. This process requires network connectivity information in the form of DNS or NetFlow data. The output is a ranked list of the most anomalous hosts along with a heat map, as depicted in Figure 1 above.

PathScan Intellectual Property

Patent Applications:

- S-129,387 entitled “Path Scanning for Detection of Anomalous Subgraphs and Use of DNS Requests and Host Agents for Anomaly/Change Detection and Network Situational Awareness,” Patent Cooperation Treaty Application No. PCT/US13/31402 filed March 14, 2013, priority date March 22, 2012.
- S-133,020 entitled “Non-harmful Insertion of Data Mimicking Computer Network Attacks”, U.S. Patent Application No. 13/826,736 filed March 14, 2013, priority date March 22, 2012.
- S-133,032 entitled “New Edges for Anomaly Detection in Computer Networks”, U.S. Patent Application No. 13/826,995 filed March 14, 2013, priority date March 22, 2012.
- S-133,046 entitled “Anomaly Detection to Identify Coordinated Group Attacks in Computer Networks”, Patent Cooperation Treaty Application No. PCT/US13/31463 filed March 14, 2013, priority date March 22, 2012. *(co-owned)*

Copyrights:

- International Copyright on all PathScan software

CodeVision is a malware analysis framework and repository that provides a unified interface for collecting, storing and analyzing malicious executable code using a variety of commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) backends in parallel. The system employs commercial and custom signatures, static and dynamic analysis, and advanced machine-learning techniques to identify malicious code.

CodeVision Intellectual Property

Patent Applications:

- S-129,177 entitled Integrating Multiple Data Sources for Malware Classification, U.S. Patent Application No. 13/909,985 filed June 4, 2013, priority date June 5, 2012. *(co-owned)*

Copyrights:

- International Copyright on all CodeVision software