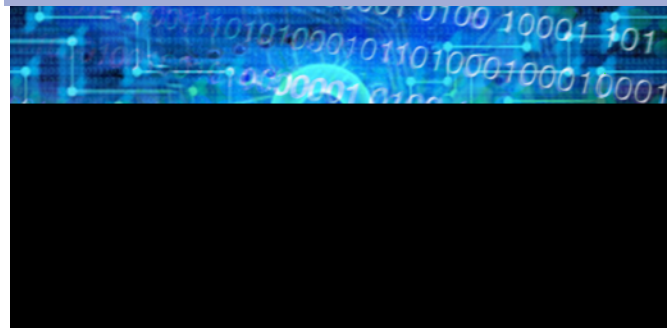
SRI International



Malware Analytics at SRI

Phillip Porras

Computer Science Laboratory, SRI International

Date: Sprint 2012

2011 Great Antimalware Papers in Academia

http://mtc.sri.com/2011BestPapers.html

Tracking Internet Fraudsters

Click Trajectories: End-to-End Analysis of the Spam Value Chain
Levchenko et al., IEEE Security Symposium 2011
Summary: **Perhaps the most comprehensive analysis of the underground spam economy to date. Strong Evidence that SPAM advertisers are bottlenecked at a handful of banks**

Understanding Fraudulent Activities in Online Ad Exchanges
Brett Stone-Gross, Ryan Stevens, Richard Kemmerer, Christopher Kruegel, Giovanni Vigna, Apostolis Zarras, ACM/SIGCOMM Internet Measurement Conference 2011
Summary: **First analysis of fraud in ad exchanges driven by botnets with data from inside an ad network, how botnets are used to perpetrate ad-fraud, and how they make money.**

Measuring Pay-per-Install: The Commoditization of Malware Distribution
Juan Caballero, Chris Grier, Christian Kreibich, Vern Paxson, Usenix Security 2011
Summary**: Another great measurement study of underground malware economy. Best paper award at Usenix Security! PPI is all about the economy that drives criminals to infect victim machines, and how they convert those installs into cash. 12 of the top 20 malware installs employ PPI.**

2011 Great Antimalware Papers in Academia

http://mtc.sri.com/2011BestPapers.html

DNS Abuse Monitoring

Monitoring the Initial DNS Behavior of Malicious Domains, Shuang Hao, Nick Feamster, Ramakant Pandrangi ACM/SIGCOMM Internet Measurement Conference 2011
Summary: **Interesting measurement paper with some important insights for rapid classification of malicious domains. 55% of of malware campaigns use domains registered w/ in 24hrs of campaign + plus key ASs where JIT malware domains are born.**

Detecting Malware Domains at the Upper DNS Hierararchy, Manos Antonakakis, Roberto Perdisci, Wenke Lee, Nikolaos Vasiloglou II, David Dagon
Usenix Security 2011
Summary**: Another malware DNS detection system, but from a unique global vantage point. How to detect malware DNS activity by monitoring upper-level DNS query patterns (Kopis).**

BOTNET DETECTION SYSTEMS

BOTMAGNIFIER: **Locating Spambots on the Internet**, Gianluca Stringhini, Thorsten Holz, Brett Stone-Gross, Christopher Kruegelx, and Giovanni Vigna
Summary**: One of the few botnet detection systems published this year, the other significant one being JACKSTRAW. Using maillogs to detect hosts w/ spam behavioral patterns what match known spammers.**

2011 Great Antimalware Papers in Academia

MALWARE ANALYSIS SYSTEMS

BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis, Jiyong Jang, David Brumley and Shobha Venkataraman, ACM CCS 2011

Summary**: A new approach to the malware classification problem with impressive scalability and performance.**

The Power of Procrastination: Detection and Mitigation of Execution-Stalling Malicious Code, Clemens Kolbitsch, Engin Kirda, Christopher Kruegel, ACM CCS 2011

Summary**: An important step in improving the state of dynamic analysis.**

Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection, Brendan Dolan-Gavitt, Tim Leek, Michael Zhivich, Jonathon Giffin, and Wenke Lee, IEEE Security Symposium 2011

Summary**: Introspection has featured prominently in many recent security solutions, such as virtual machine-based intrusion detection, forensic memory analysis, and low-artifact malware analysis. This system shows lots of promise and will hopefully inspire a new suite of introspection systems.**

A Study of Android Application Security, William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri, Usenix Security 2011

Summary**: An interesting tool that would likely be useful for next-generation Android malware analysis systems.**

MALGRAM

Malware Binary Reverse Engineering
malgram.mtc.sri.com

Automated Malware Reverse Engineering

- Binary Structural Analysis
- Dynamic Analyses
  - API Hooking
  - Peer App Kernel Probing
  - VM Introspection

- Static Program Analysis
  - Unpacking
  - Code Deobfuscation
  - Decompilation
  - Program Analysis
  - Program Rewriting

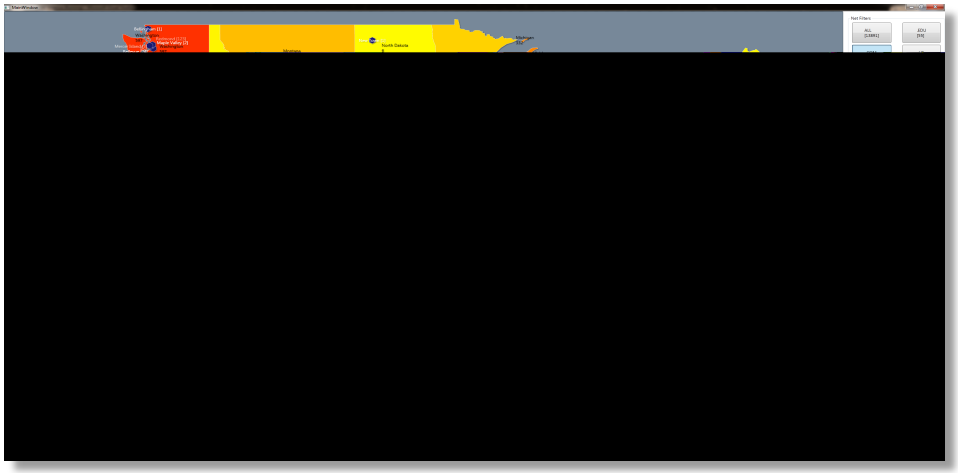
BotHunter
www.bothunter.net

What's Novel Here ➔ BotHunter

- Flip the IDS Paradigm - INFECTION DIAGNOSIS not INBOUND EXPLOIT ALARMS
- Network Dialog Correlation (patent pending)
- Analyze **two-way communication** flows between internal assets and the Internet
- Analyze all *dialog exchanges* against defined ***malware infection lifecycle model***

Next Steps: Integrating Infection Diagnosis with Binary object interception |= Infection Validation

SRI



Malware Threat Tracking
http://tinyurl/InfectedUSA

SRI does multiple forms of malware Threat Intel Tracking

- Honeynets
- ReflectorNets
- IP Reputation Service
- CALO – Web Tracking and Interpretation
- Free Sensors

SRI Threat Reputation Service:
http://kb.bothunter.net/ipInfo/IPRep.php?IP=%s&FORMAT=csv
- the FORMAT arg can be CSV, TEXT, TAB, XML

OpenFlow

Security Through
Software Defined Networking

www.openflowsec.org

Fresco / FortNOX

Publications

Current Video Demos
- Automated Malware Quarantine
- Reflector Nets
- Stopping Illegal VTunnels

http://www.bothunter.net

www.wired.com/gadgetlab/2011/12/sri-threat-detection/

Wired Magazine

12/30/2012

First Siri, Now Threat Detection: Inside SRI's Amazing R&D

By Christina Bonnington | December 30, 2011 | 6:30 am | Categories: Miscellaneous, R&D and Inventions

Follow @redgirlsays 3,655 followers

Pat Lincoln, director of SRI's Computer Science Laboratory, stands next to a huge display running BotHunter, SRI's botnet detection software. *Photo: Jon Snyder/Wired*

SRI International