

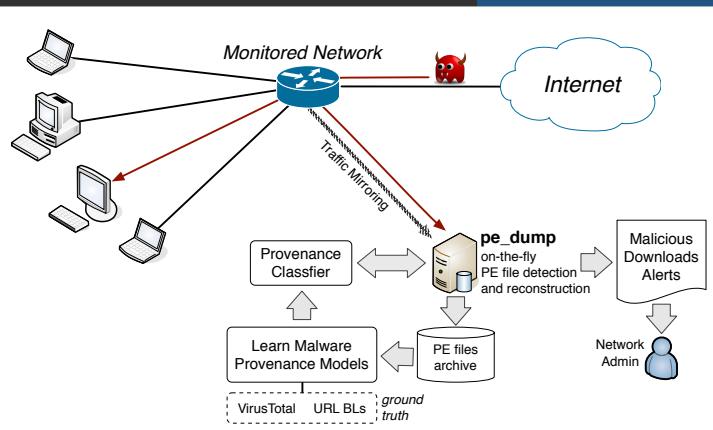
Malware Defense via Download Provenance Classification

Phani Vadrevu, Babak Rahbarinia, Roberto Perdisci, and Kang Li

Goals

- Reconstruct PE files downloaded from live network traffic at high speed
- Identify malware downloads based on provenance information
- Detect zero-day malware samples that are not currently detected by anti-virus tools
- Immediately blacklist malicious domains/URLs and share them with other network defense systems

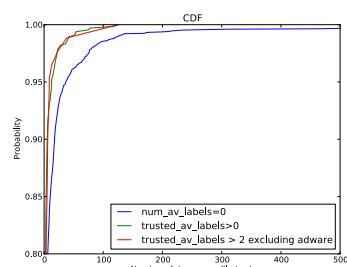
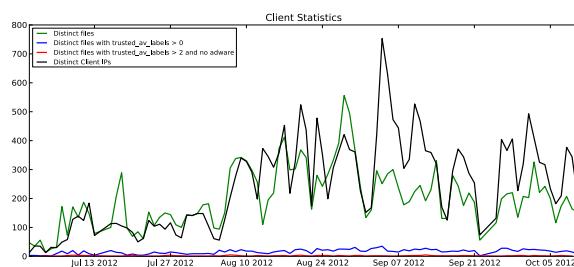
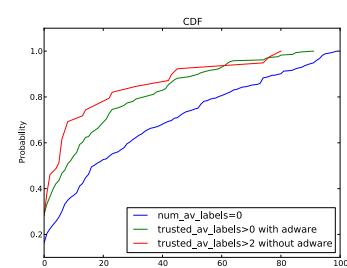
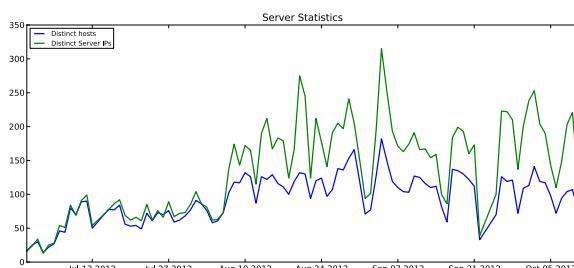
System Overview



Ongoing Work

- Feature Selection
- Verification of samples never submitted to VirusTotal
- Estimate zero-day detection accuracy
- Comparison with domain name blacklists (e.g., SafeBrowsing)
- Correlation with domain name reputation systems

Preliminary Results



timestamp	md5	host	server	avs
2012-10-22 10:52:27	c63c9bc18de063b55f2b21c40f1de45	com.privitize	46.17.101.157	5
2012-10-21 08:09:17	d250c870d2ed4893292391291f4312de	nl.3a4.n70	46.17.53.69	8
2012-10-21 08:13:38	1faad20c3706bb009285aa178918d01f	com.comnames	220.73.162.14	3
2012-10-20 04:55:33	1faad20c3706bb009285aa178918d01f	com.comnames	220.73.162.100	3
2012-10-19 18:03:04	e6bd18e242247e0403fd65984b59f4b	kr.co.tomon.app2	222.231.59.169	3
2012-10-19 18:02:39	8eeea26741377c1c7094a2ddcfdf05e8a	com.goutil	218.146.254.33	3
2012-10-19 18:02:07	809f6bd696b454bda6afe3947fdbe537	net.daum.uf.cffile203	174.35.32.96	5
2012-10-19 12:30:03	daac0870bcfe238aeafb8d1bf43f12de	220.73.162.3	220.73.162.3	3
2012-10-19 12:25:31	cceed9741dd69efcd7a73008365197	com.filenoija.file	218.38.12.97	3
2012-10-19 12:24:51	baf18dbc8add0148f5acab6ab741e53	com.filenoija.file	218.38.12.97	4

