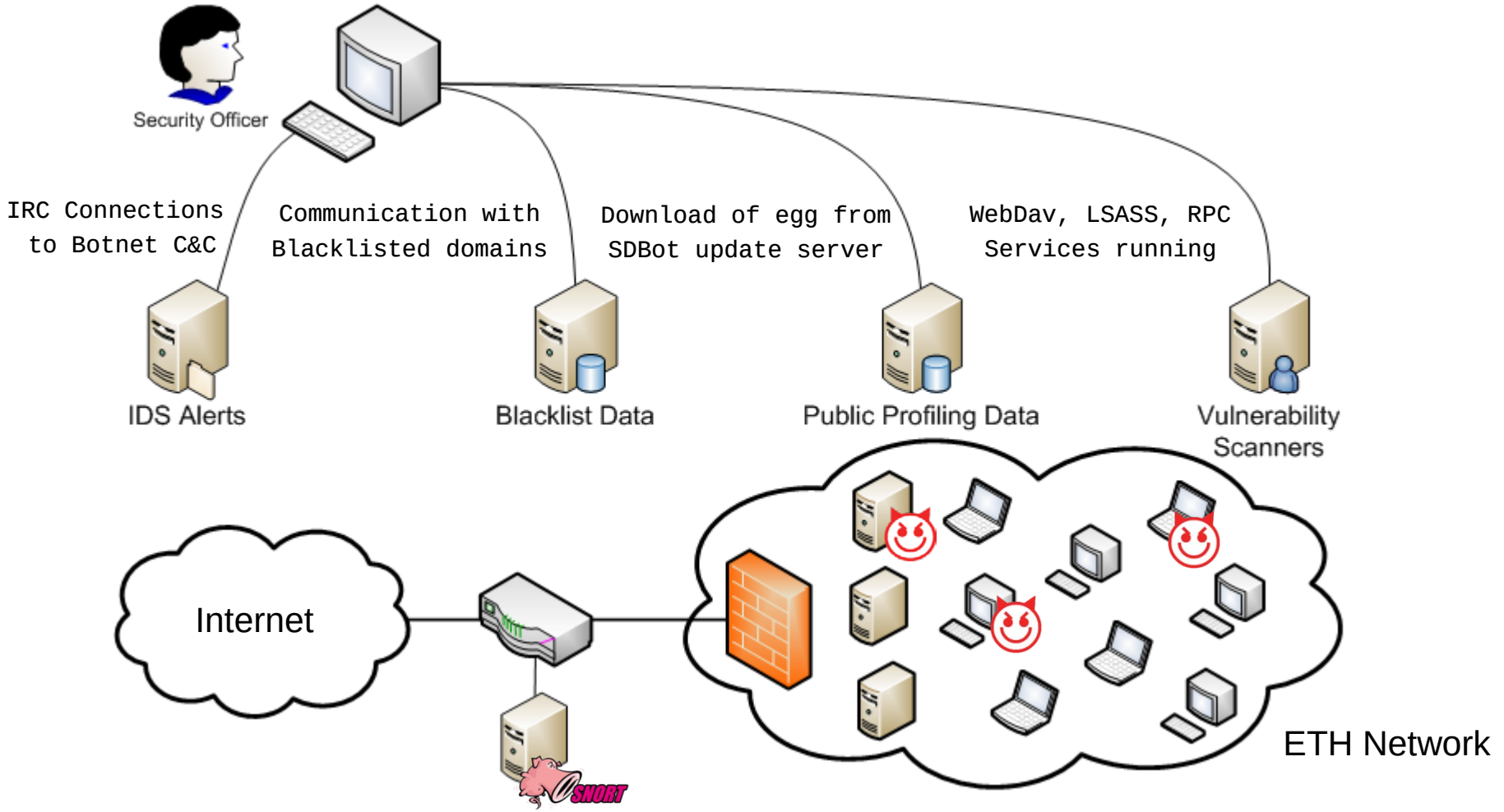
ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Shedding Light on Log Correlation in Network Forensics Analysis

DIMVA
27/07/2012

Elias Raftopoulos
Matthias Egli
Dr. Xenofontas Dimitropoulos

The Battlefield



Motivation

- Modern malware exhibit complex behaviors that cannot be easily detected using a single sensor

> Multi-vantage point monitoring is critical

- Security sensors provide an overwhelming amount of data that need to be analyzed and prioritized

> Cross-correlation of heterogeneous security data is required

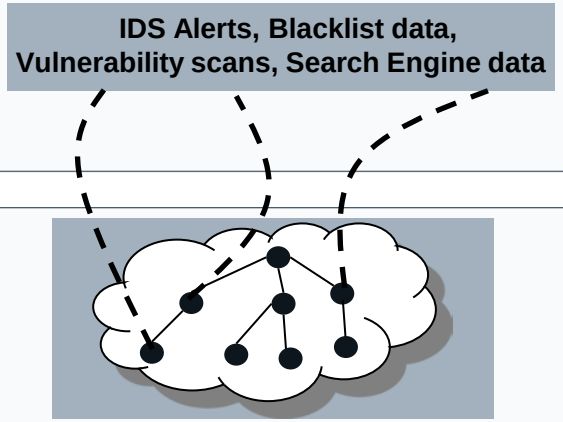
- Combining diverse security sources to validate a suspected infection is both demanding and extremely time-consuming

> Automation of the correlation and decision making process is imperative

Our Work

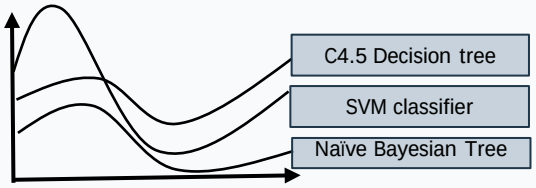
Systematically monitor the security assessment process of 200 live infections

Evaluate the complementary utility of four different security sources in performing a diagnosis

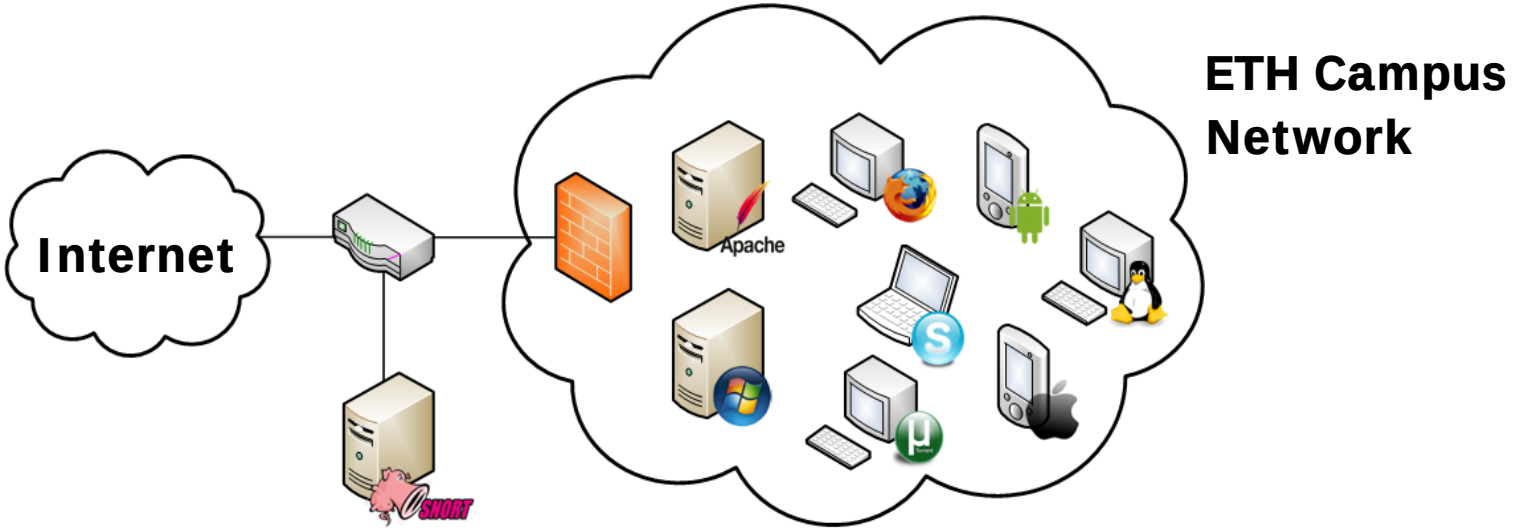


Build a decision support tool that captures the cognitive process followed for infection validation

Compare the effectiveness of different classifiers in performing automated diagnosis



Data Collection and Feature Extraction - IDS Data



- Configured Snort to use both VRT and ET rulesets (~38K signatures)
- Manually re-classified signatures to 3 classes
  - Attacks , Compromised hosts (security relevant) ✔
  - Policy violations (not related to security incidents) ✘

Data Collection and Feature Extraction - IDS Data

- For each internal investigated host extract features from raw IDS data
  - Example : Torpig infected host

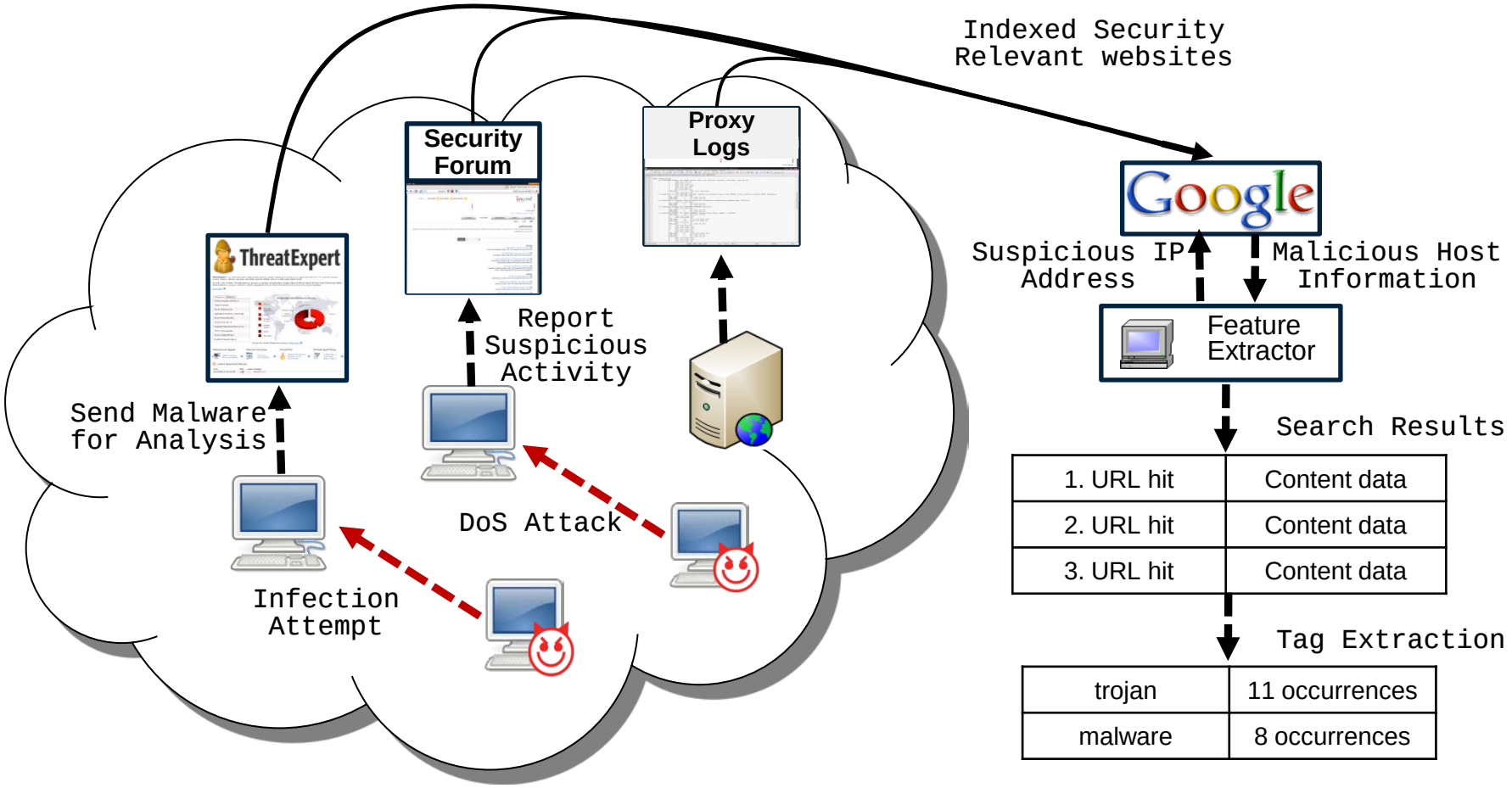
Feature	Value
Frequent remote hosts	{91.20.214.127,194.146.207.220}
Frequent remote services	{80}
Frequent local services	{80,135,443}
Count of severe alerts	271
Infection duration (hours)	23
Common severe alerts (IDs)	{2801953,2012642,2912939}

Data Collection and Feature Extraction - Blacklists

- Leverage 5 public providers which provide partly labeled blacklists
- Build a different feature for each available label
- Count the total number of hits for each label across all providers

	ads	attack	bot	chat	drugs	generic	malware	porn	rbn	religion	spam
Apews											√
Dshield		√				√					
Emerging Threats		√	√			√			√		
Shadowserver			√								
URL Blacklist	√			√	√		√	√		√	

Data Collection and Feature Extraction - Query Search Engine (Googling)



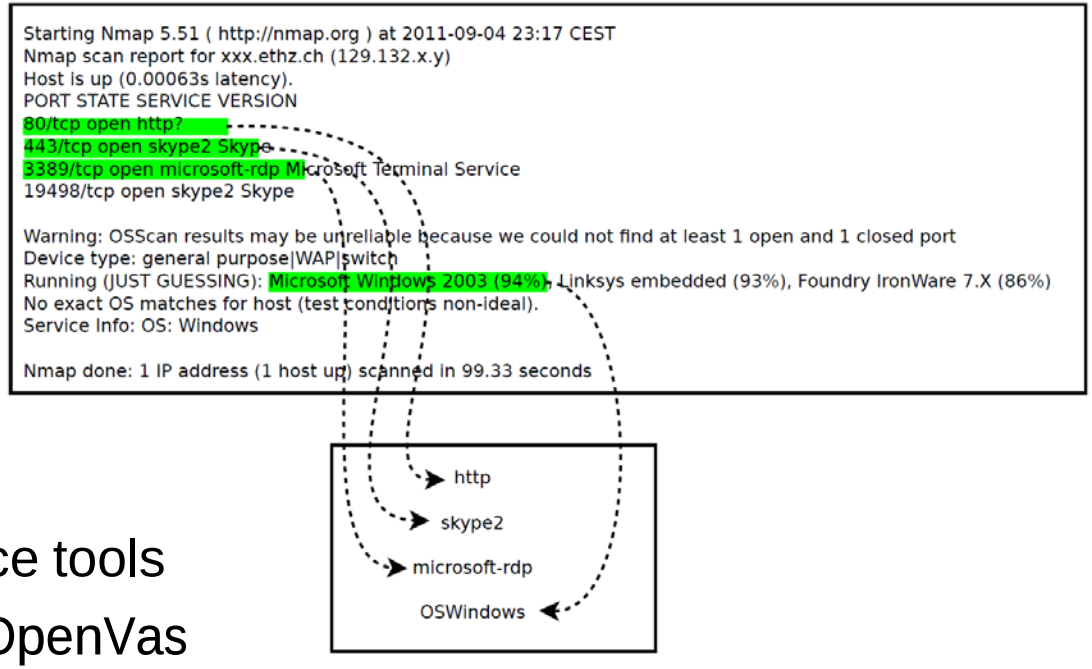
Data Collection and Feature extraction - Search Engine Data

- Google profiling tags and extracted features

Tags	Feature
ftp, webmail, email, mysql, pop3, mms, netbios	Benign Host
dhcp, proxy	Benign Server
malware, spybot, spam, bot, trojan, worm	Malicious host
blacklist, banlist, blocklist, ban	Blacklisted hosts
adaware	Adaware
irc, undernet, innernet	IRC Servers
torrent, emule, kazaa,edonkey, announce, tracker	
xunlei, limewire, bitcomet, uusee, qqlive, pplive	P2P clients

Data Collection and Feature Extraction - Reconnaissance and Vulnerability Scans

- Actively probe suspicious local hosts to collect more information about
  - running services
  - patching level of critical components
  - existence vulnerabilities



- Use different reconnaissance tools
  - *whois*, Nmap, Nessus, OpenVas

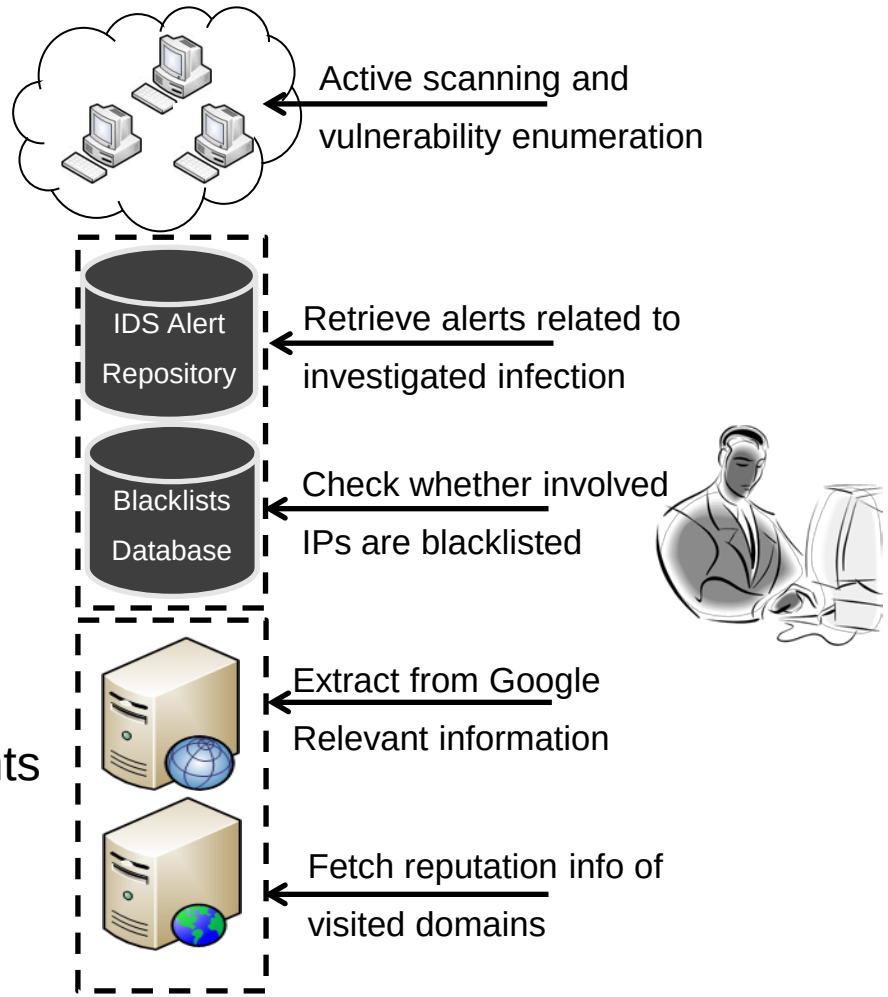
Methodology

Goal

- Build a **set of validated** infections

Process

- Extract information from the available security sources
- Correlate collected evidence vs expected malware behavior (1)
- Manually analyze 200 consecutive incidents reported by our heuristic in 1 month



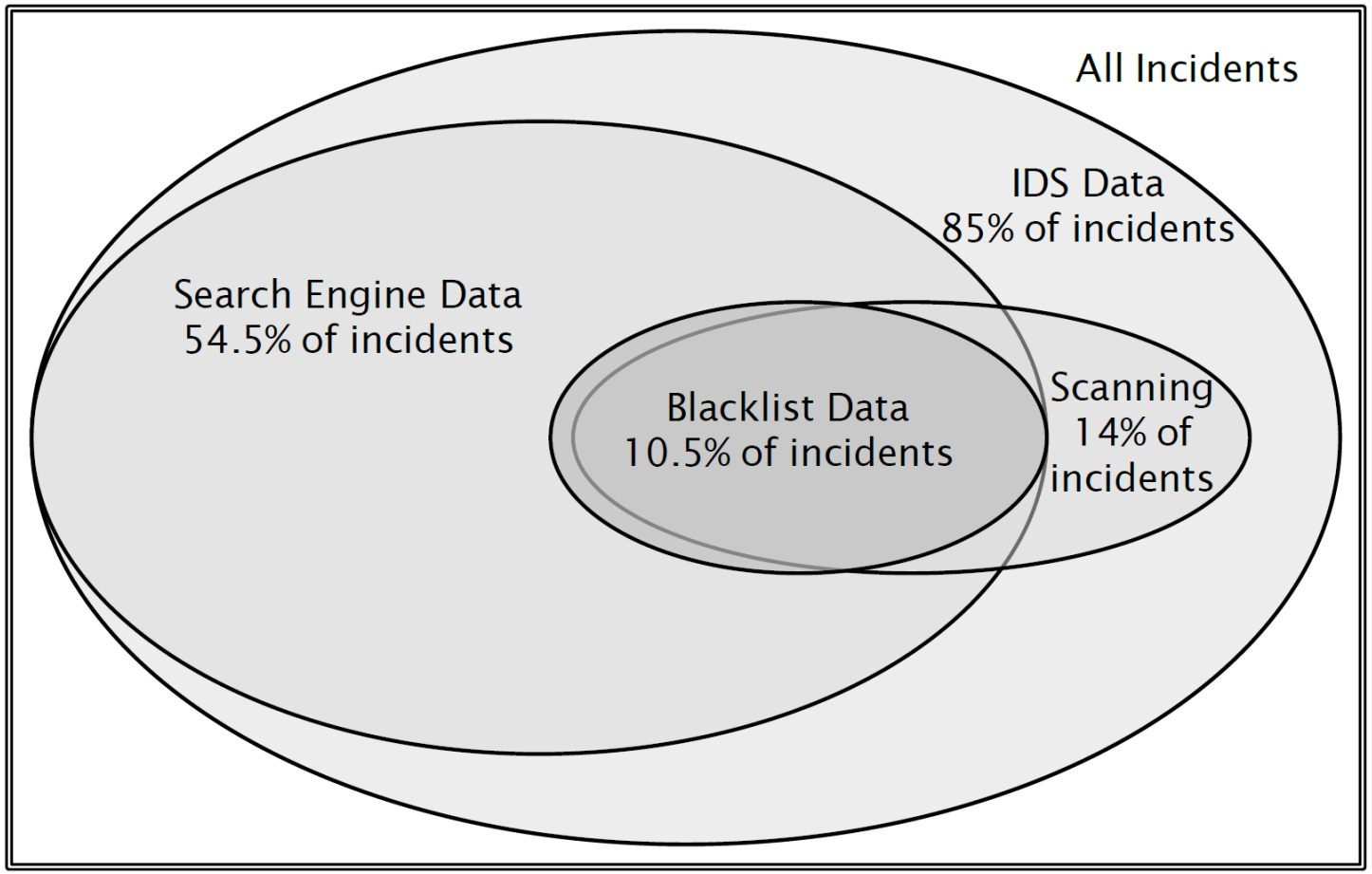
(1) Detecting, Validating and Characterizing Computer Infections in the Wild

Elias Raftopoulos, Xenofontas Dimitropoulos, ACM SIGCOMM IMC 2011

Complementary Utility of Security Sources

Malware Type (#incidents)	Malware Family (#incidents)	Security Data Sources			
		IDS	Blacklist	Googling	Scanning
Trojans (85)	FakeAV (27)	√		√	
	Simbar (26)	√		√	
	Monkif (18)	√		√	
	Torpig (10)	√	√	√	√
	Nervos (4)	√		√	
Spyware (59)	AskSearch (50)	√			
	MySearch (9)	√			
Backdoors (18)	SdBot (5)	√	√	√	√
	ZBot (5)	√		√	√
	Blackenergy (4)	√	√	√	√
	Parabola (2)	√	√	√	
	Ramsky (2)	√			√
Worms (8)	Koobface (6)	√		√	
	Conficker (2)	√		√	√

Complementary Utility of Security Sources

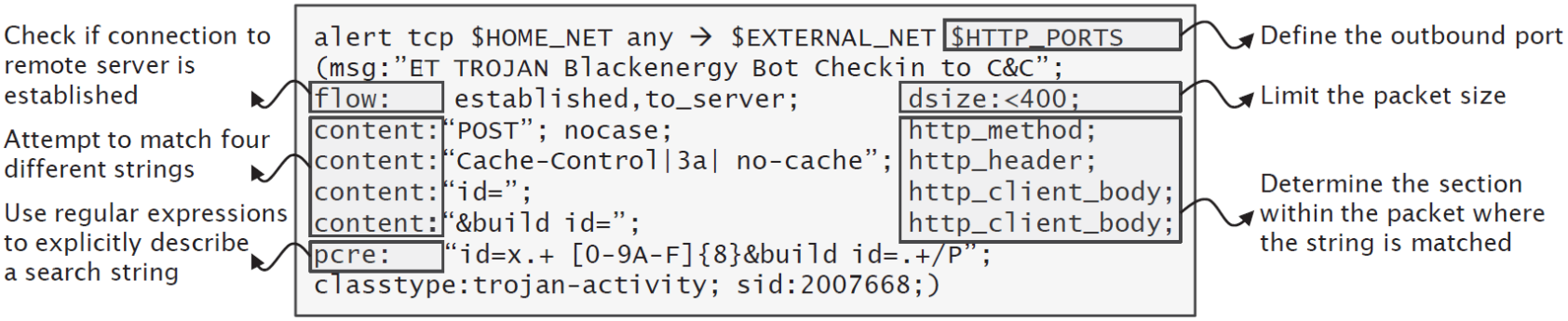


‘Good’ Snort Signatures

- For each validated incident extract IDS signatures relevant to infections
  - 138 signatures in total
- Classify signatures based on exhibited malicious activity

[C&C Communication] Update malicious binary instruction set
2007668 ET TROJAN Blackenergy Bot Checkin to C&C 2010861 ET TROJAN Zeus Bot Request to CnC 16693 SPYWARE-PUT Torpig bot sinkhole server DNS lookup attempt 2802912 ETPRO TROJAN Backdoor.Nervos.A Checkin to Server
[Reporting] Share stolen user confidential data with controller
2008660 ET TROJAN Torpig Infection Reporting 2011827 ET TROJAN Xilcter/Zeus related malware dropper reporting in 2009024 ET TROJAN Downadup/Conficker A or B Worm reporting 2010150 ET TROJAN Koobface HTTP Request
[Egg download] Update malicious binary
2010886 ET TROJAN BlackEnergy v2.x Plugin Download Request 2802975 ETPRO TROJAN Linezing.com Checkin 2010071 ET TROJAN Hiloti/Mufanom Downloader Checkin
[Redirection] Redirect user to malicious domain
2011912 ET CURRENT EVENTS Possible Fake AV Checkin 2003494:2003496 ET USER AGENTS AskSearch Toolbar Spyware 2009005 ET MALWARE Simbar Spyware User-Agent Detected
[Propagation] Detect and infect vulnerable hosts
2008802 ET TROJAN Possible Downadup/Conficker-A Worm Activity 2003068 ET SCAN Potential SSH Scan OUTBOUND 2000347 ET ATTACK RESPONSE IRC - Private message on non-std port

Best Practices for Writing 'Good' Snort Signatures



	Bytes Checked	Fields Checked	Byte Offset is Set	RE is set	Destination Port is Set	Packet size is Set
Regular Sigs	11	1.2	8%	15%	17%	7%
Good Sigs	23.5	2.8	28%	50%	22%	15%
Increase	2.14 x	2.3 x	3.5 x	3.3 x	1.29 x	2.14 x

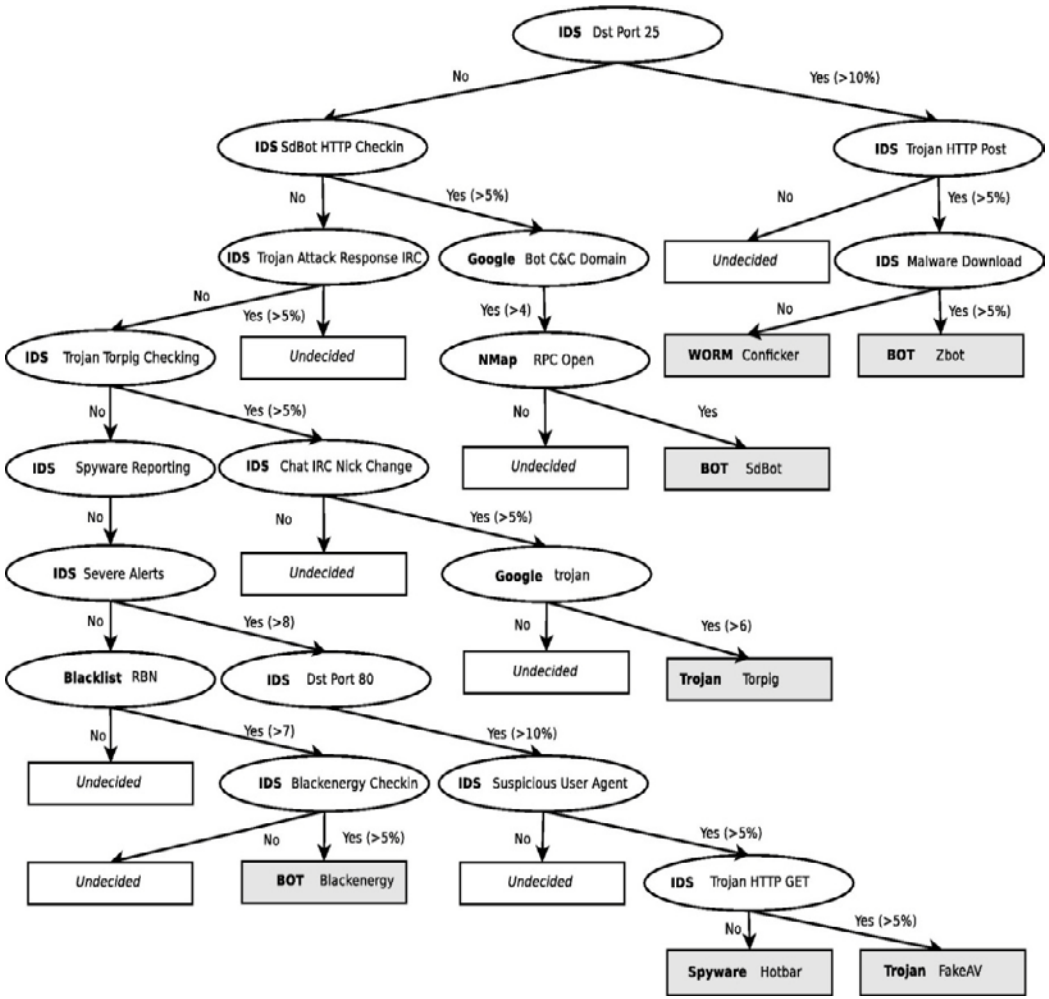
Good signatures are significantly complex

Decision Support Tool

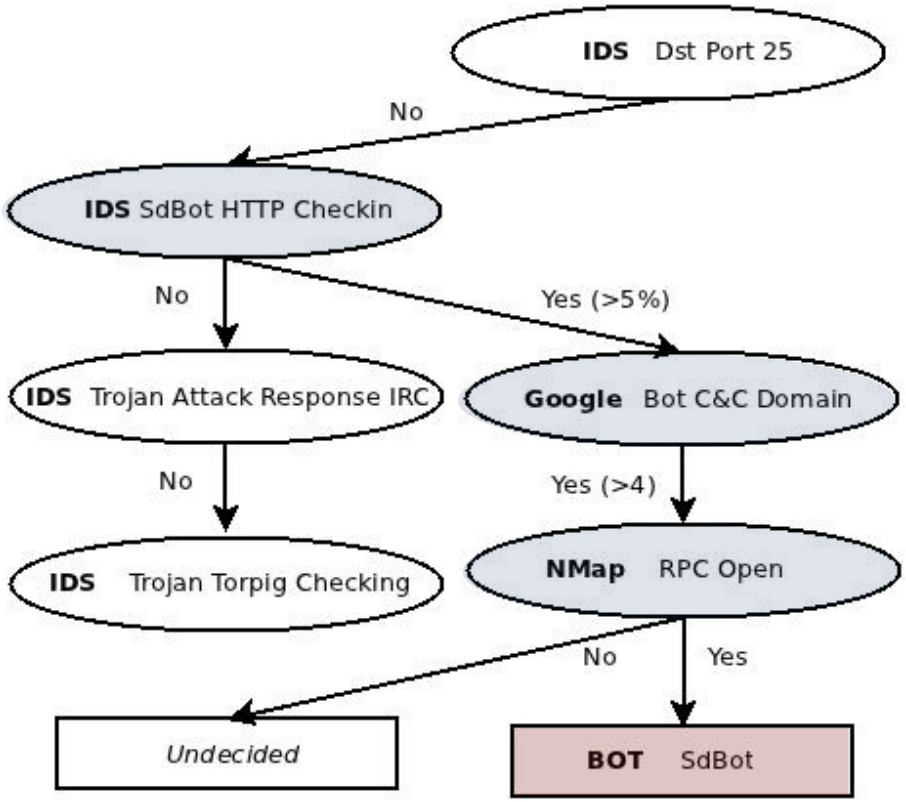
- C4.5 decision tree induction
- → Computationally Efficient
- → Publicly available
- → Interpretable Results

- Perform training using the 200 validated incidents

- Pruning and over-fitting fine-tuning using sub-tree raising
  - Stratified ten-fold cross-correlation

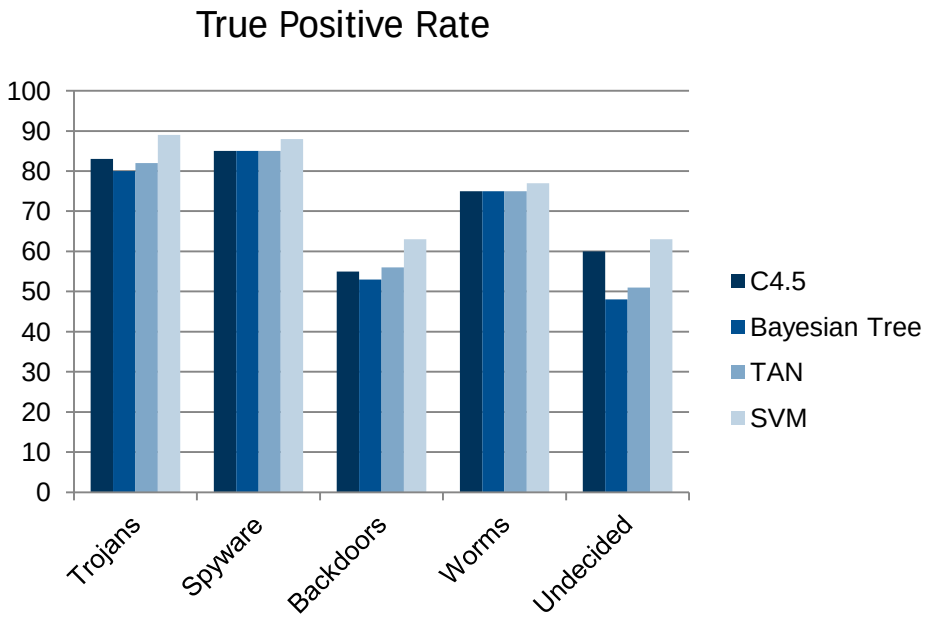


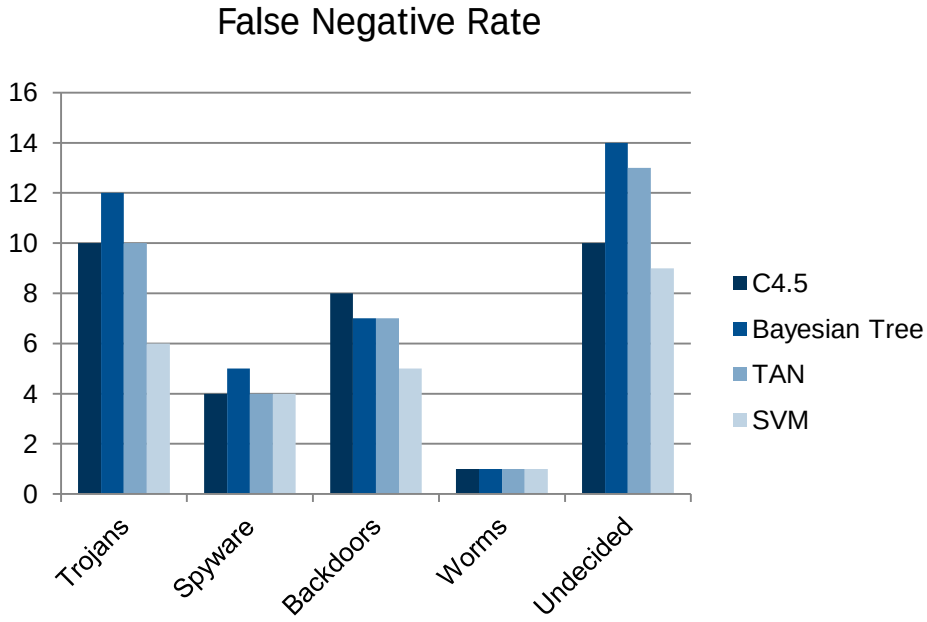
Decision Support Tool
Example Infections : SDBot



- Frequent communication with C&C using known rendezvous addresses
  → "ET WORM SDBot HTTP Checkin"
- Contacted domains are typically tagged by Google as malicious
  - Extracted tags for contacted domains "bot", "innernet", "backdoor", "IRC"
- Periodically attempt to propagate using MS network shares
  - RPC service (135) is open

Automated Diagnosis





- C4.5 decision trees
  - perform accurate diagnosis in 72% of the cases
  - exhibit comparable performance with SVM classifier
  - retain high interpretability

Conclusions

- Search engine provided useful evidence for diagnosing many more incidents than more traditional security
- Decisions made by a security specialist in assessing real-life infections can be accurately modeled using a decision tree
- C4.5 decision trees exhibit similar performance in automated diagnosis with more sophisticated classifiers without sacrificing interpretability
- Make available and analyze a list of good Snort signatures
  - highlight a number of differences between good and regular signatures