Analyzing and Exploiting Network Behaviors of Malware

Jose Andre Morales Areej Al-Bataineh

Shouhuai Xu Ravi Sandhu

SecureComm

Singapore, 2010

Introduction

- Do malicious and benign processes behave differently from a networking perspective?
- Can we exploit these differences to identify malware, especially zero-day attacks?
- Analyzed 1000 malware samples, with 31 not detected by Virustotal.com 01 April 2010 and 123 benign samples
- Focus on DNS, NetBIOS, TCP, UDP, ICMP

Introduction - 2

- Log file analysis tallied various network event occurrence amounts
- Along with traffic observations we identified behavior occurring mostly in malware
- Defined 7 behaviors dealing with specific observed anomalies in network traffic
- Some behaviors combine network events to form an anomaly
- These behaviors used to differentiate between malicious and benign processes
- Clustering and classification

Contributions

- Identification of network behaviors occurring mostly in malware usable in behavior based malware detection.
- Discovery of novel malicious uses of network services by malware.
- Evaluating the effectiveness of observed network behaviors in identifying malware and benign processes with clustering and classification.

7 Behaviors

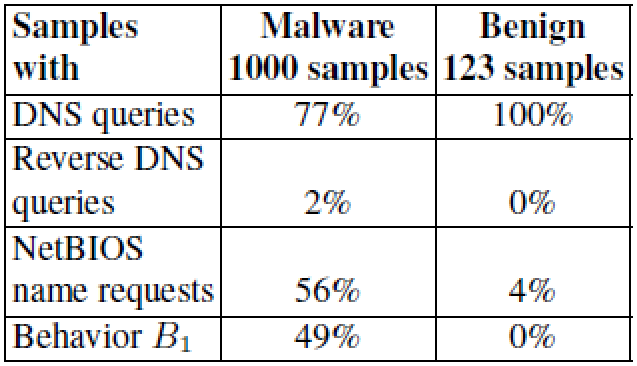
- B1: Process performs a NetBIOS name request on a domain name that is not part of a DNS or rDNS query
- B2: Failed connection attempt to an IP address obtained from a successful DNS query
- B3: Failed connection attempt to the input IP address of a successful rDNS query
- B4: Connection attempt to the input IP address of a failed rDNS query

7 Behaviors

- B5: ICMP only activity, ICMP echo requests for a specific non-local network IP address with no reply or a returned error message.
- B6: TCP/ICMP activity, TCP connection attempts to non-local IP addresses that received a successful reply to their ICMP echo requests
- B7: Network activity that is rarely occurring or implemented in an anomalous manner

Behavior B1

- Process performs a NetBIOS name request on a domain name that is not part of a DNS or rDNS query
- Table shows B1 occurring only in malware, benign NetBIOS used domain names previously used in a DNS query.
- Several domains in B1 known malicious by Malwareurl.com but others were not

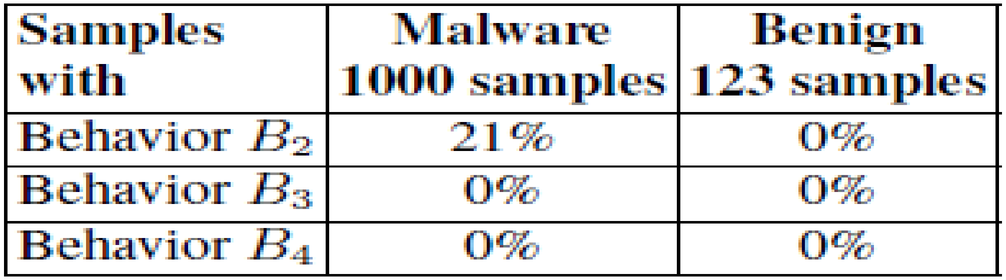


Samples with	**Malware 1000 samples**	**Benign 123 samples**
DNS queries	77%	100%
Reverse DNS queries	2%	0%
NetBIOS name requests	56%	4%
Behavior B_1	49%	0%

Table 3. Samples with DNS, NetBIOS, & B_1

Behaviors B2, B3 & B4

- DNS often used to acquire IP addresses
- Only B2 occurred, many malware DNS domain names and cannot connect with returned IP, either offline or shutdown, or newly registered and inactive
- B3, B4 no occurrence, possible less favored by malware authors

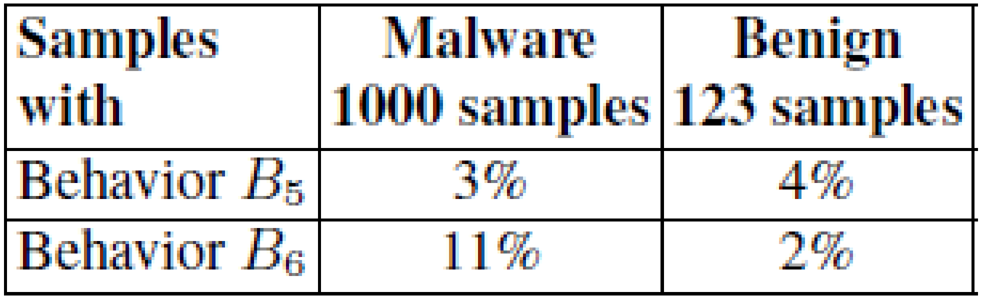


Samples with	Malware 1000 samples	Benign 123 samples
Behavior B_2	21%	0%
Behavior B_3	0%	0%
Behavior B_4	0%	0%

Table 4. Samples with behaviors B_2, B_3 & B_4

Behaviors B5 & B6

- ICMP used by malware (like PING) to acquire active IP addresses, these IPs not part of previous DNS, rDNS or NetBIOS → suspicious behavior. B6 dominant in malware
- B5 almost same in both, very similar to DNS behavior with no request reply

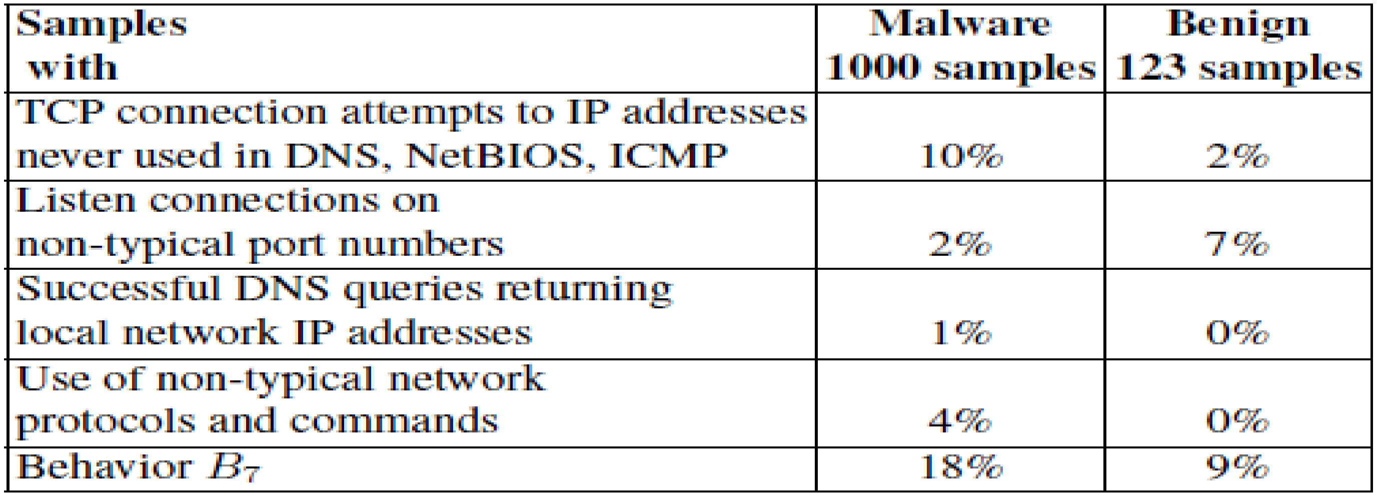


Samples with	**Malware 1000 samples**	**Benign 123 samples**
Behavior B_5	3%	4%
Behavior B_6	11%	2%

Table 5. Samples with behaviors B_5 & B_6

Behavior B7

- Considered suspicious but not necessarily malicious, behaviors were rarely occurring or implemented in non-conventional manner
- TCP connection attemps most prevalent, IP not acquired via DNS, NetBios or ICMP, possibly hardwired or dynamically generated



Samples with	Malware 1000 samples	Benign 123 samples
TCP connection attempts to IP addresses never used in DNS, NetBIOS, ICMP	10%	2%
Listen connections on non-typical port numbers	2%	7%
Successful DNS queries returning local network IP addresses	1%	0%
Use of non-typical network protocols and commands	4%	0%
Behavior B_7	18%	9%

Table 6. Samples with behavior B_7

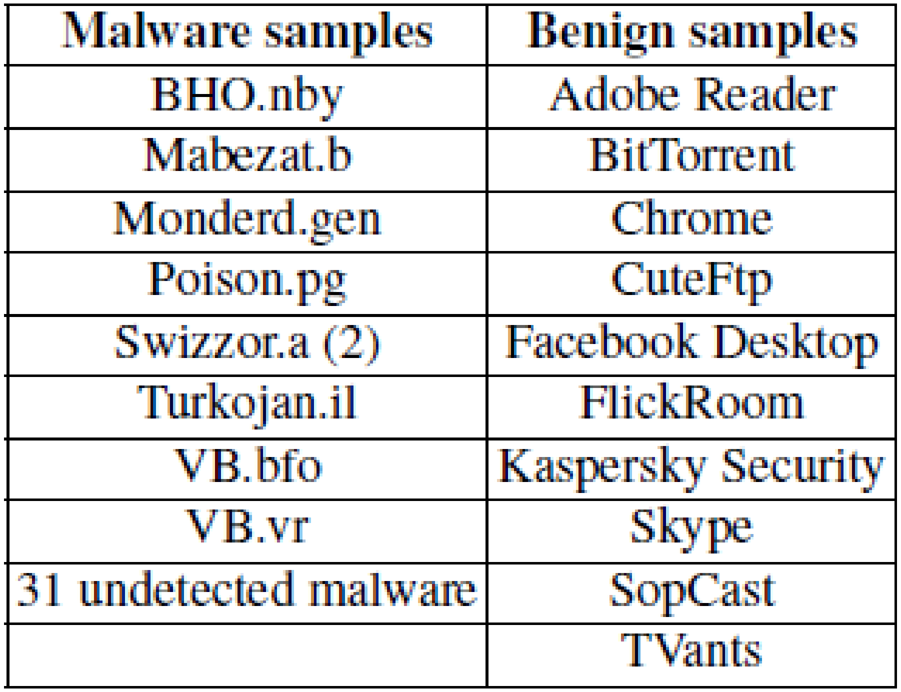
Behavior Evaluation

- 1000 malware samples from CWSandbox 27 October 2009 upload, diverse set, still active durng testing.
  - 31 samples from 31 March 2010 upload not detected by Virustotal.com (MD5 search) 1 April 2010
- 41 benign samples executed 3 times each = 123 total benign samples – FTP, RSS, socnet, P2P, AV, net tools
- Individual samples run for 10 minutes in VMWare (XP SP2) using Windows network monitor, proprietary netwok layer filters
- Results revealed behaviors differentiate malicious from benign including 31 unidentified malware

Clustering & Classification - 01

- Weka data mining software
- Clustering used complete malware and benign data set
- Classification training set used 1st 700 malware samples and 40 benign, testing used the remaining samples
- 31 unknown samples not part of training set

Clustering & Classification - 02

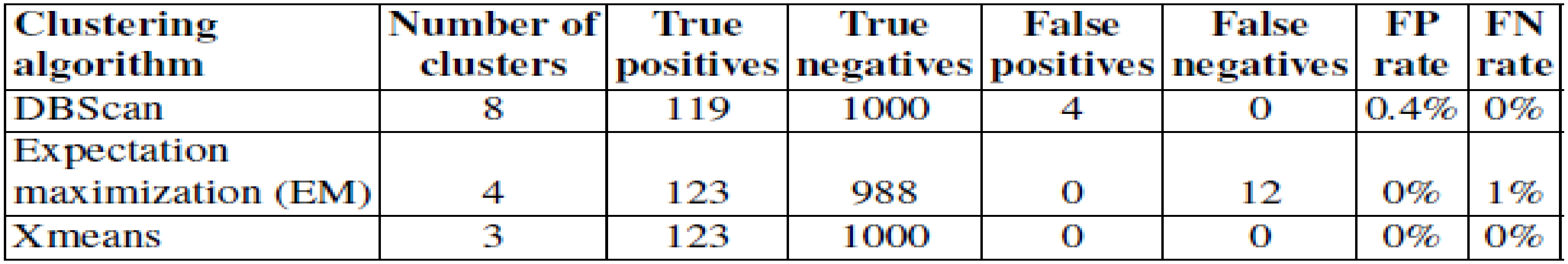


Malware samples	Benign samples
BHO.nby	Adobe Reader
Mabezat.b	BitTorrent
Monderd.gen	Chrome
Poison.pg	CuteFtp
Swizzor.a (2)	Facebook Desktop
Turkojan.il	FlickRoom
VB.bfo	Kaspersky Security
VB.vr	Skype
31 undetected malware	SopCast
	TVants

Table 7. Some of the malware and benign samples in test set and not in training set

Clustering Results

- If majority of cluster was malware then benign samples assumed FP, If majority of cluster was benign then malware samples assumed FN
- Xmeans perfect, DBScan & EM encouraging
    - All 31 unknown malware correctly identified
- FP video streamers known to be unreliable networks
- EM FN mostly malware downloaders

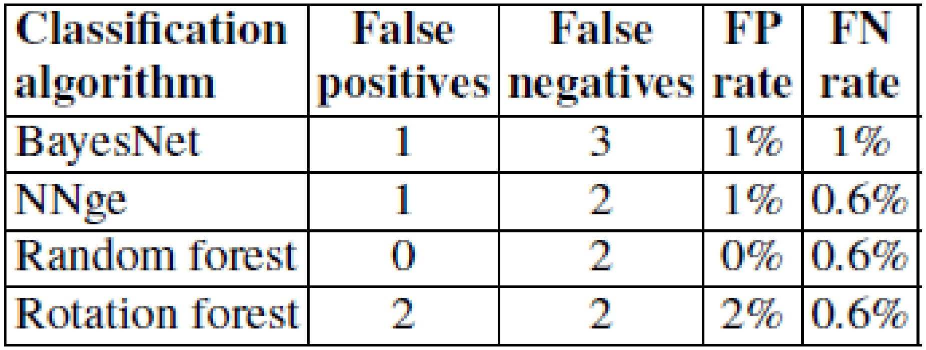


Clustering algorithm	Number of clusters	True positives	True negatives	False positives	False negatives	FP rate	FN rate
DBScan	8	119	1000	4	0	0.4%	0%
Expectation maximization (EM)	4	123	988	0	12	0%	1%
Xmeans	3	123	1000	0	0	0%	0%

Table 8. Top three clustering results with 1000 malware and 123 benign samples

Classification Results

- FN and FP very low, 2 malware flagged as FN by all 4, only 2 video streams flagged as FP
- 29 unknown malware correctly identified by all 4



Classification algorithm	False positives	False negatives	FP rate	FN rate
BayesNet	1	3	1%	1%
NNge	1	2	1%	0.6%
Random forest	0	2	0%	0.6%
Rotation forest	2	2	2%	0.6%

Table 9. Top four classification test set results with 300 malware and 83 benign samples

Discussion

- B1, B2 & B7 most dominant behaviors
- B1,B5 & B6 considered novel behaviors used by malware to find active remote hosts
- Classification & clustering produced excellent results with minimal FN & FP
- 31 malware not identified by virustotal.com on 1 April 2010 were correctly detected with minimal exceptions

Conclusions

- Network behaviors can be exploited to differentiate between malicious and benign
- Discovered 3 novel network behaviors
- Our approach can be combined with other perspectives to enrich detection accuracy
- The behaviors detected a diverse set of malware inlcuding 31 unknown samples with minimal FP and FN