UTSA Institute for Cyber Security
THE UNIVERSITY OF TEXAS AT SAN ANTONIO

4th International Conference on Malicious and Unwanted Software (Malware 2009)

October 13-14 2009 – Montreal, Canada

Analyzing DNS Activities of Bot Processes

Dr. Jose Andre Morales
Areej Al-Bataineh
Dr. Shouhuai Xu
Dr.Ravi Sandhu

Overview

- Attempt to detect bot processes based on a process's reaction to DNS activity, RD-behavior.
- Detect with host based approach that is process-specific
- Real-time data collection with post analysis
- Detects bots and non-bot malware
- Enhances results of some commercial solutions

Bots and DNS

- Bots need to join a botnet to be useful
- Botmasters provide several IPs or domains to connect with
- Brute force connection attempts have many failures
- DNS activities: DNS and reverse DNS (rDNS) used to lower the failure rate but produces failed DNS results

RD-behavior - 1

- RD-behavior: a process’s reaction to DNS response behavior
- Process will use DNS or rDNS queries for various tasks
  - How should a process react?
  - When should DNS result be ignored?
  - When should a DNS result be used?

RD-behavior - 2

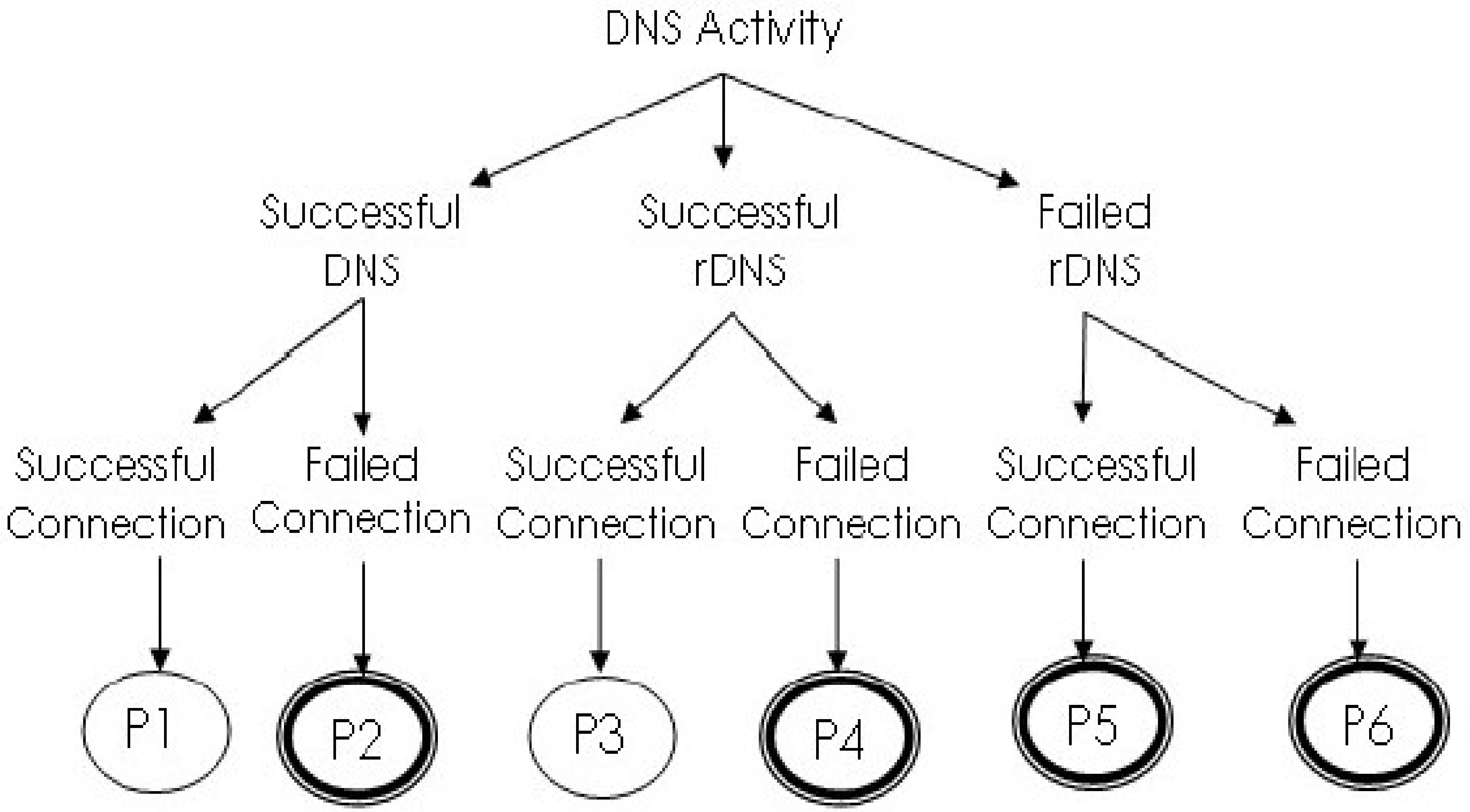
Expected RD-behavior

- An IP address that fails a rDNS query is not used in a connection attempt
- IP address used in a successful DNS activity should connect.

Anomalous (Suspicious) RD-behavior, SRDB

- An IP address that fails rDNS query is used in any connection attempt.
- IP address of a successful DNS activity is used in a unsuccessful connection attempt.

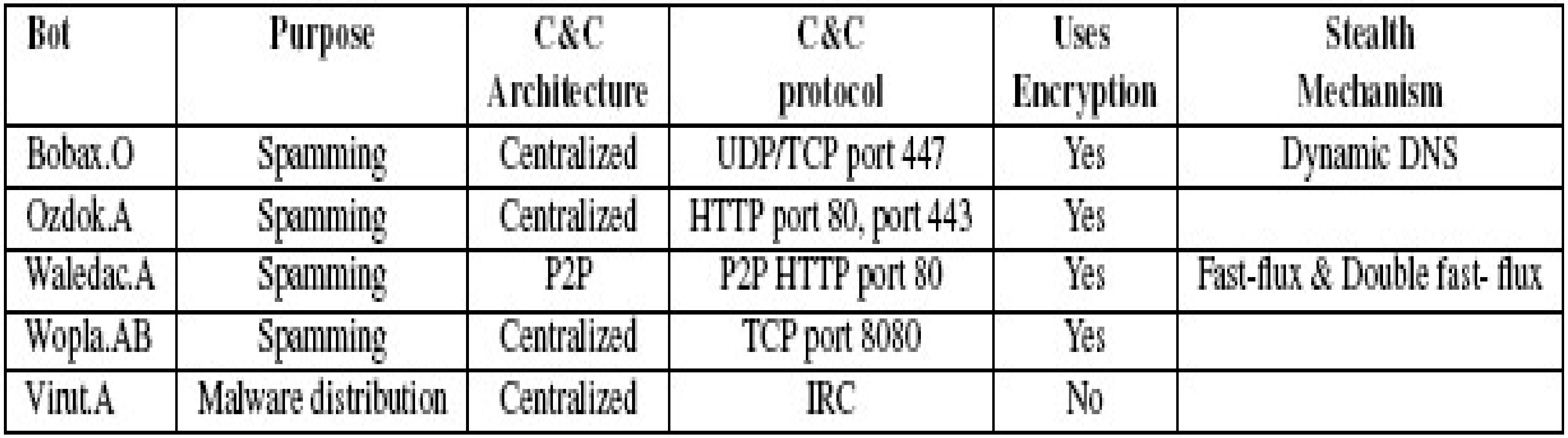
RD-behavior Tree with 6 paths



Experiments - 1

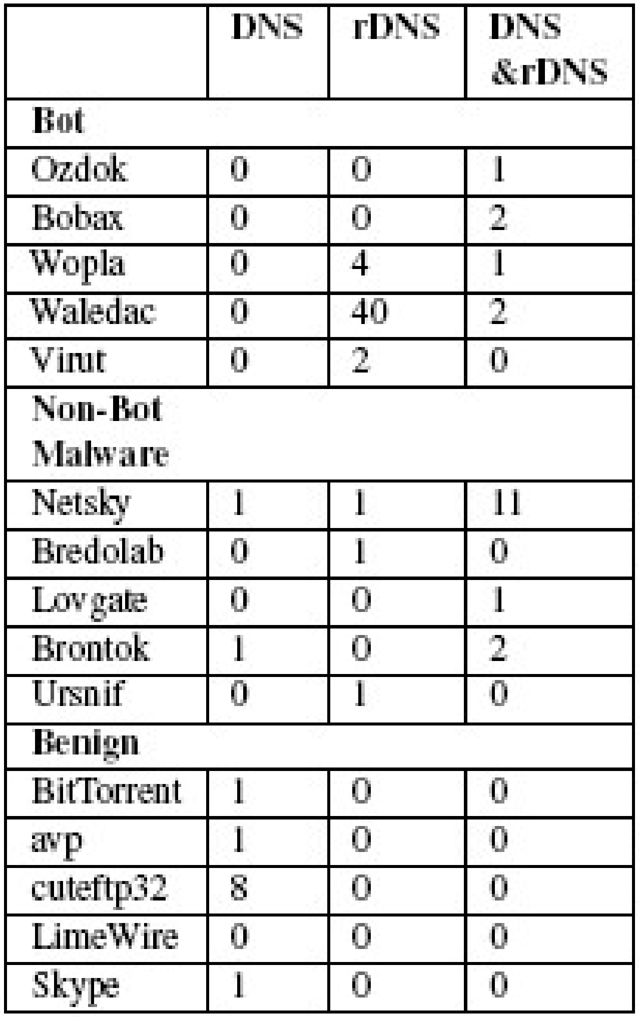
- Detection occurred after 1 instance of SRDB
  - 1 instance of P2,P4,P5,P6
- Tested three sets of processes for 1 hour period:
  - Non-bot malware: Netsky, Bredolab, Lovegate, Brontok, Ursnif
    - In the wild between January and May 2009
    - Worms, Trojan downloaders and Backdoors
  - Benign: BitTorrent, Kaspersky AV, Cute FTP, LimeWire and Skype
    - All network active

Bot Properties



Bot	Purpose	C&C Architecture	C&C protocol	Uses Encryption	Stealth Mechanism
Bobax.O	Spamming	Centralized	UDP/TCP port 447	Yes	Dynamic DNS
Ozdok.A	Spamming	Centralized	HTTP port 80, port 443	Yes	
Waledac.A	Spamming	P2P	P2P HTTP port 80	Yes	Fast-flux & Double fast- flux
Wopla.AB	Spamming	Centralized	TCP port 8080	Yes	
Virut.A	Malware distribution	Centralized	IRC	No	

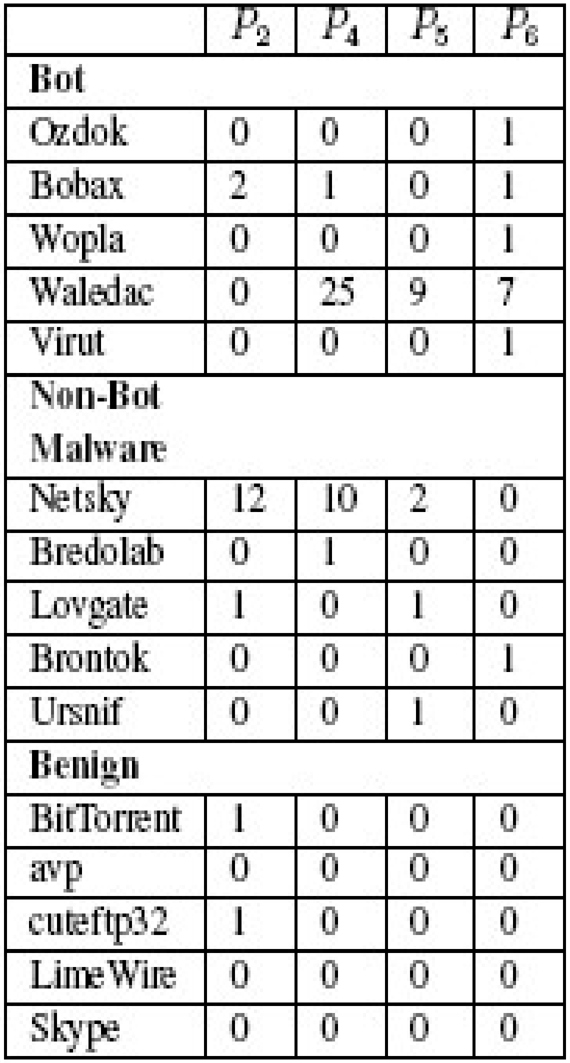
Experiments - 2



	DNS	rDNS	DNS &rDNS
Bot			
Ozdok	0	0	1
Bobax	0	0	2
Wopla	0	4	1
Waledac	0	40	2
Virut	0	2	0
Non-Bot Malware			
Netsky	1	1	11
Bredolab	0	1	0
Lovgate	0	0	1
Brontok	1	0	2
Ursnif	0	1	0
Benign			
BitTorrent	1	0	0
avp	1	0	0
cuteftp32	8	0	0
LimeWire	0	0	0
Skype	1	0	0

- Total # distinct IPs/domains in a DNS, rDNS or both and a connection attempt (successful and failed)
- Bots had the most, followed by non-bot malware and benign

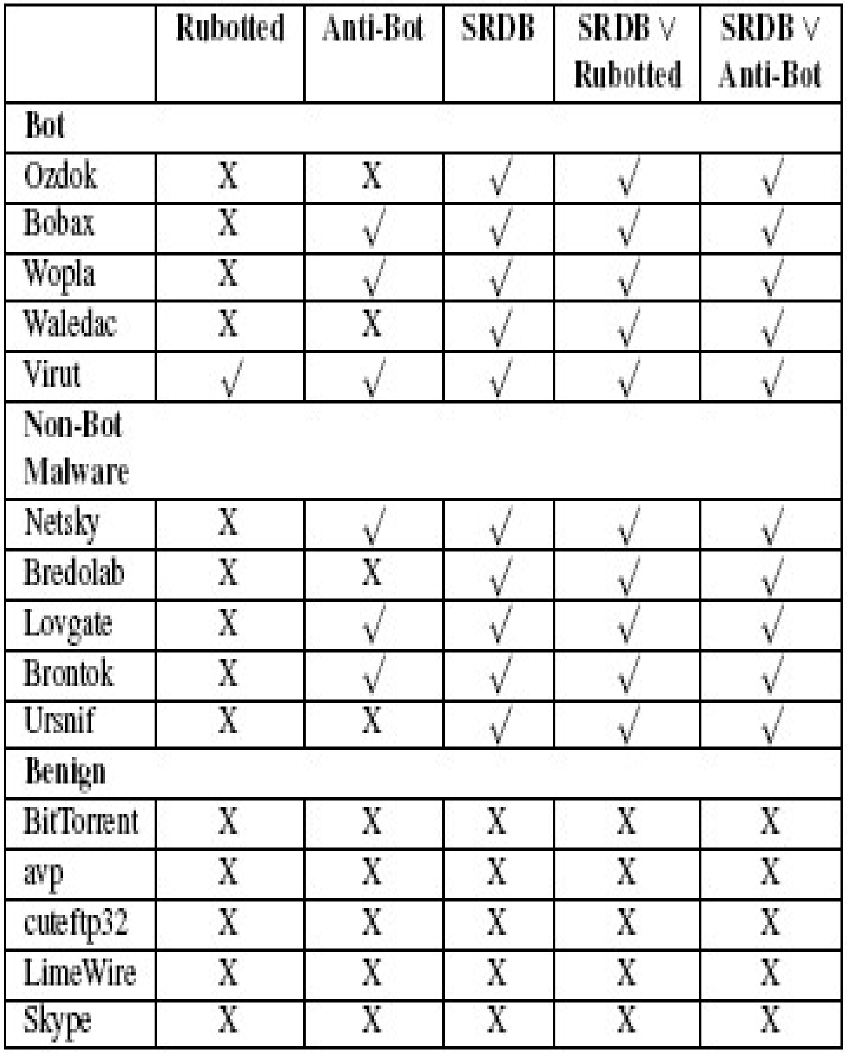
Experiments - 3



	P_2	P_4	P_5	P_6
Bot				
Ozdok	0	0	0	1
Bobax	2	1	0	1
Wopla	0	0	0	1
Waledac	0	25	9	7
Virut	0	0	0	1
Non-Bot Malware				
Netsky	12	10	2	0
Bredolab	0	1	0	0
Lovgate	1	0	1	0
Brontok	0	0	0	1
Ursnif	0	0	1	0
Benign				
BitTorrent	1	0	0	0
avp	0	0	0	0
cuteftp32	1	0	0	0
LimeWire	0	0	0	0
Skype	0	0	0	0

- Every P2 instance has at least one instance of P4-P6
- P2 assumed anomalous but not suspicious and is pruned
- Benign had no paths P4-P6
- Malware had instances of paths P4-P6
- P6 most dominant in bots

Experiments - 4



	Rubotted	Anti-Bot	SRDB	SRDB ∨ Rubotted	SRDB ∨ Anti-Bot
Bot					
Ozdok	X	X	√	√	√
Bobax	X	√	√	√	√
Wopla	X	√	√	√	√
Waledac	X	X	√	√	√
Virut	√	√	√	√	√
Non-Bot Malware					
Netsky	X	√	√	√	√
Bredolab	X	X	√	√	√
Lovgate	X	√	√	√	√
Brontok	X	√	√	√	√
Ursnif	X	X	√	√	√
Benign					
BitTorrent	X	X	X	X	X
avp	X	X	X	X	X
cuteftp32	X	X	X	X	X
LimeWire	X	X	X	X	X
Skype	X	X	X	X	X

Two commercial bot detectors
Rubotted: 9 false negative
Anti-bot: 4 false negatives

SRDB (RD-behavior): 0 false negatives

Combining SRDB with the two commercial bot detectors improved their detection accuracy.

Result Analysis

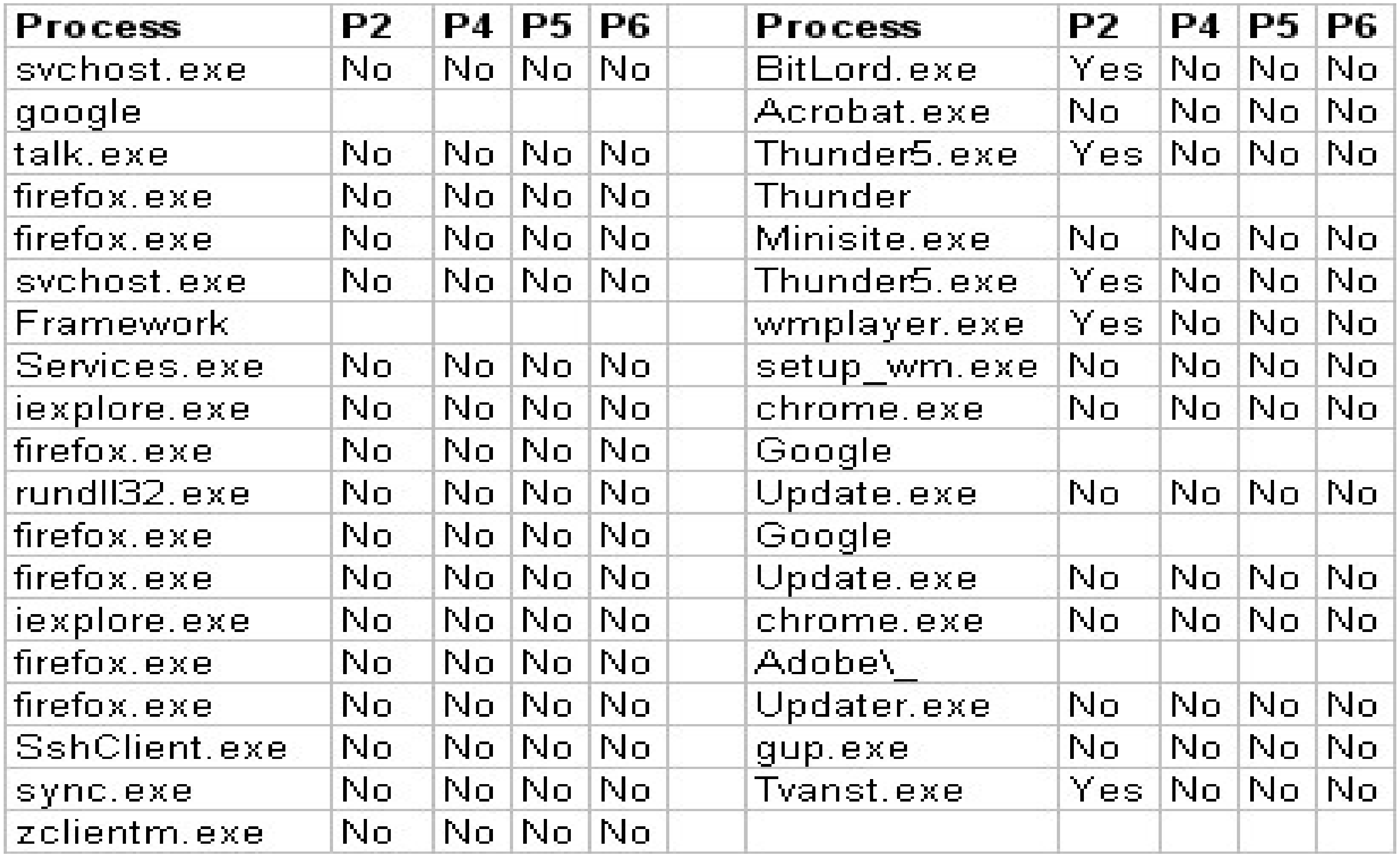
- Benign tend to follow expected RD-behavior

- Bots follow expected and SRDB
  - Especially bots with a pool of domains/IPs to choose from
- Non-bot malware exhibit SRDB behavior
  - Encouraging, results suggest technique can be extended to detect other malware classes
- All results acquired in first 7minutes of execution
  - Early detection mitigates damage and distribution

Limitations

- Kernel mode bots
- Paths P1, P3
- Beyond join phase
- Only TCP traffic
- Web 2.0, socnet bots (Twitterbot)

New Results 1 – Sept-Oct 2009 Benign Processes

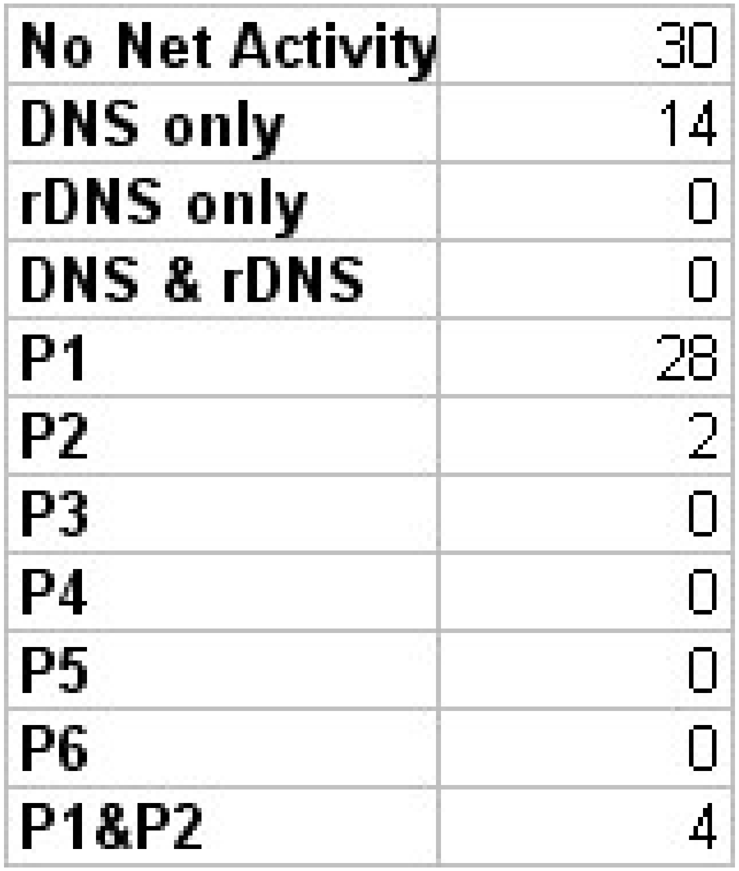


Process	P2	P4	P5	P6		Process	P2	P4	P5	P6
svchost.exe	No	No	No	No		BitLord.exe	Yes	No	No	No
google						Acrobat.exe	No	No	No	No
talk.exe	No	No	No	No		Thunder5.exe	Yes	No	No	No
firefox.exe	No	No	No	No		Thunder				
firefox.exe	No	No	No	No		Minisite.exe	No	No	No	No
svchost.exe	No	No	No	No		Thunder5.exe	Yes	No	No	No
Framework						wmplayer.exe	Yes	No	No	No
Services.exe	No	No	No	No		setup_wm.exe	No	No	No	No
iexplore.exe	No	No	No	No		chrome.exe	No	No	No	No
firefox.exe	No	No	No	No		Google				
rundll32.exe	No	No	No	No		Update.exe	No	No	No	No
firefox.exe	No	No	No	No		Google				
firefox.exe	No	No	No	No		Update.exe	No	No	No	No
iexplore.exe	No	No	No	No		chrome.exe	No	No	No	No
firefox.exe	No	No	No	No		Adobe_				
firefox.exe	No	No	No	No		Updater.exe	No	No	No	No
SshClient.exe	No	No	No	No		gup.exe	No	No	No	No
sync.exe	No	No	No	No		Tvanst.exe	Yes	No	No	No
zclientm.exe	No	No	No	No						

New Results 1 – Sept-Oct 2009 Malware Processes

- 78 samples from CWSandbox malware repository 09-10-2009
- Very diverse, adware, scareware, bots(zbot,harebot), PWS, backdoors, Trojans(all types), Packed Win32 Vxs.
- Virustotal, 4 not detected

New Results 2 – Sept-Oct 2009
Malware Processes



No Net Activity	30
DNS only	14
rDNS only	0
DNS & rDNS	0
P1	28
P2	2
P3	0
P4	0
P5	0
P6	0
P1&P2	4

- P2: 6 instances, P1: 28 instances, No P3 – P6,
- Malware observations
  - DNS many domain names
  - Each Domain DNS’d many times
  - Unusual, never seen domain names: .kr,.cn,.NU, etc…

Detection Enhancements

- In addition to detecting RD-Behavior
- User/machine-based whitelist of commonly visited domain names
- Process-based
  - total domain names DNS’d per execution
  - total DNS of one domain name
- DNS success/failure rate
- Combining can produce better results
- GOAL: exploit DNS maximally to detect malware (not just bots), usable as one component of bigger detection strategy
- Research currently underway

Conclusion and Future Work

- Combining DNS & connection attempts very useful in bot detection
- rDNS key element of bots
- Several bots (non-bot malware) do not follow DNS rules of expected behavior
- Benign use DNS activities in expected ways
- Future Work

  -Kernel bot detection

  - More malware, benign processes
  - Diversity of protocols
  - Detection Enhancements presented here

Questions?

¿Preguntas?

質問

Вопросы

Sawaal

Domande

Soru

Ερωτήσεις

問題

kyseessä

pytanie