



Extracting Malware Intelligence

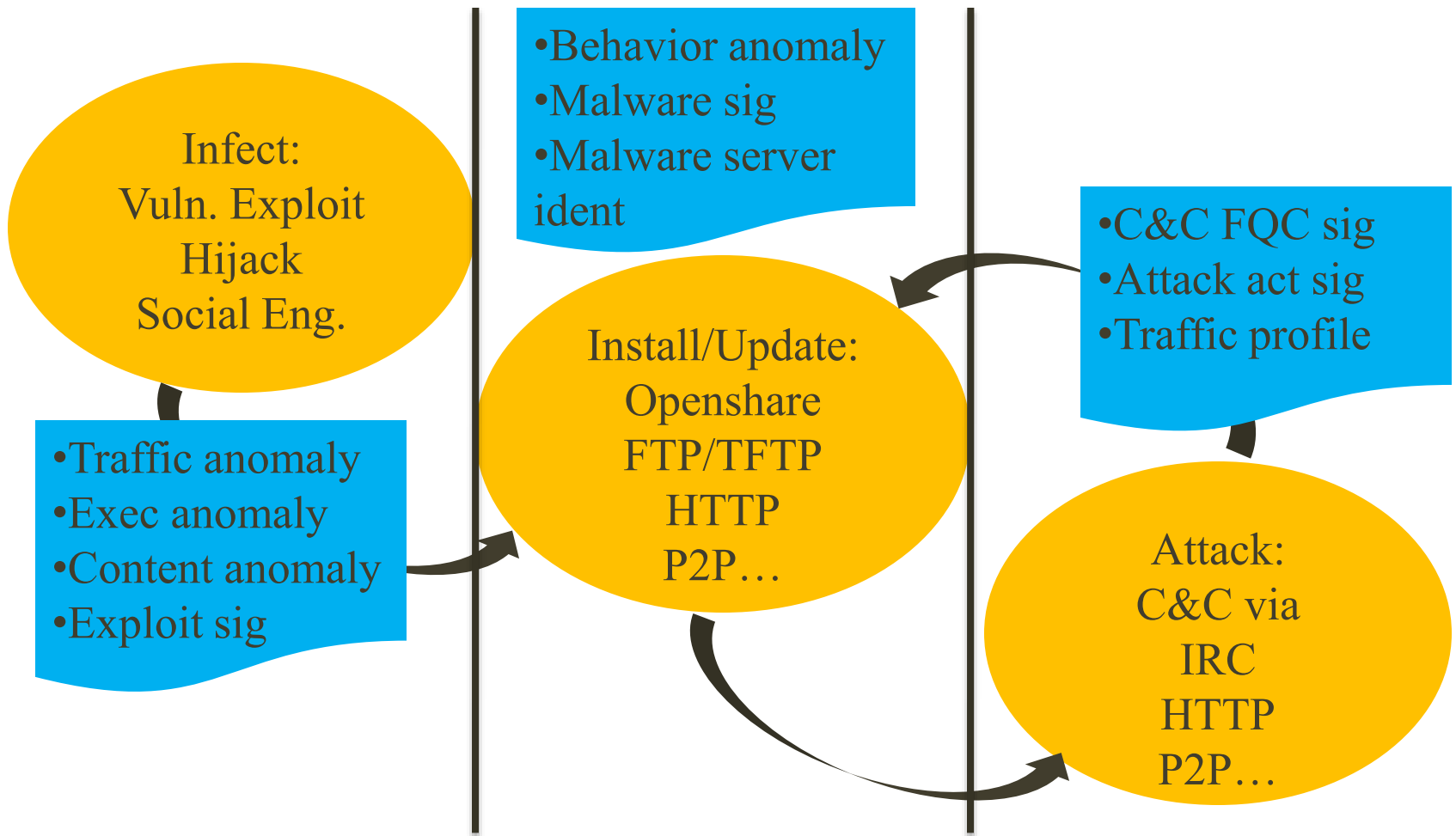
Supporting An Anti-Malware Ecosystem

Fengmin Gong
fgong@fireeye.com
Internet2 Spring Meeting 2008

- Observing botnet life cycle
- Best botnet fighting strategy
- Critical factor – malware/botnet intelligence
- VM-based extraction technology
- Building anti-malware ecosystem
- Examples



Botnet - Malicious But Not Invisible





Knowing The Enemy

- Botnets must be built - one bot at a time from infection to installation, and to joining the C&C network.
- Botnets utilize networked computers but also increase the exposure surface for detection.
- Botnets take time to “grow up” thus opening up a window of opportunity for control.
- Botnet is like a pandemic disease thus requiring pervasive countermeasures.
- More mature a botnet is, more severe & wide-spread the damage will be, thus proactive measures should be preferred.



Knowing Ourselves

- We have extensive deployment of all kinds of security solutions, we should leverage them for botnet fighting!
- Defenders should also advance our causes through open-source approach - sharing botnet intelligence.
- We can also turn the network to our advantage - building a global anti-botnet network.
- **Critical factor – accurate, timely, available, and complete malware intelligence**

- Real-time events
 - Infection attempts
 - C&C communications
 - Attack activities
- Infection intelligence
 - Coordinates of the infecting/infected
 - Infection (exploit) signatures
 - Malware signatures
 - OS changes
 - Infection trending



Botnet Intelligence – cont'd

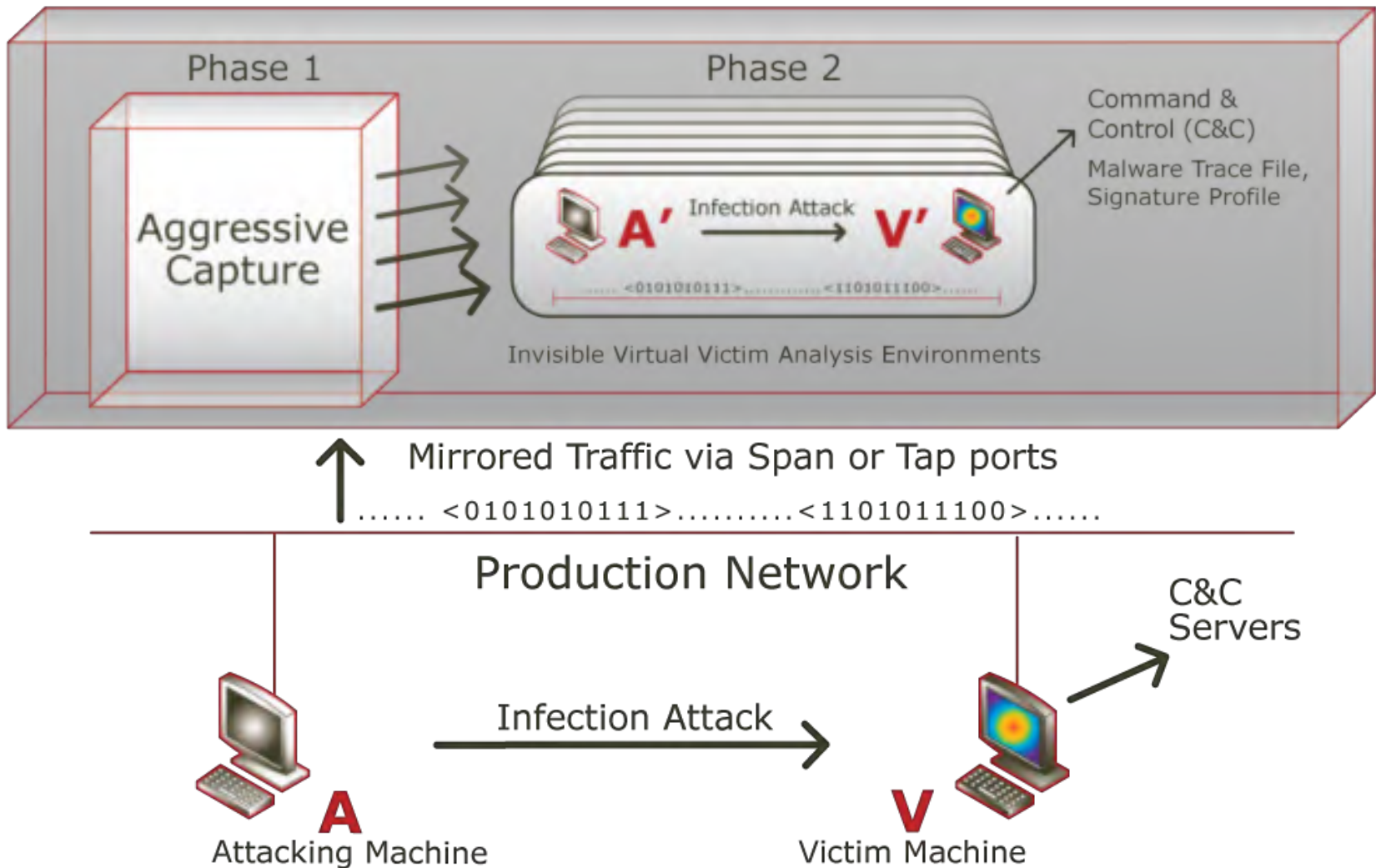
- Attack activity intelligence
 - Coordinates of C&C server, bot host
 - Coordinates of malware update server
 - Coordinates of data collection server
 - Fully qualified channel (FQC) signatures
 - Botnet threat trending
- Cyberspace risk intelligence
 - Incident-based rating - infection/botnet incident per Org/ISP/AS/Country
 - Fraud trending – SPAM/Phishing/DOS/DataTheft



What Makes It Actionable

- Accuracy
 - Verifiable infection
 - Verifiable activities
 - Material OS changes
- Timeliness
 - Best to kill a botnet in its infancy
 - Rapid dissemination is the key
- Availability
 - Arm every able body – anti-malware ecosystem
- Completeness
 - Cover all infection vectors including social engineering
 - Cover every stage of botnet development

VM-Based Detection Technology





Aggressive Capture

- Traffic anomaly detection
 - Captures all suspicious traffic flows exploiting service vulnerabilities
 - Adaptive capturing heuristics, service & connection aware
- Bayesian Web payload analysis
 - Captures all suspicious URLs delivering questionable payloads
 - Stateful tracking of redirects with obfuscation
 - Covers web-client exploitation & social engineering

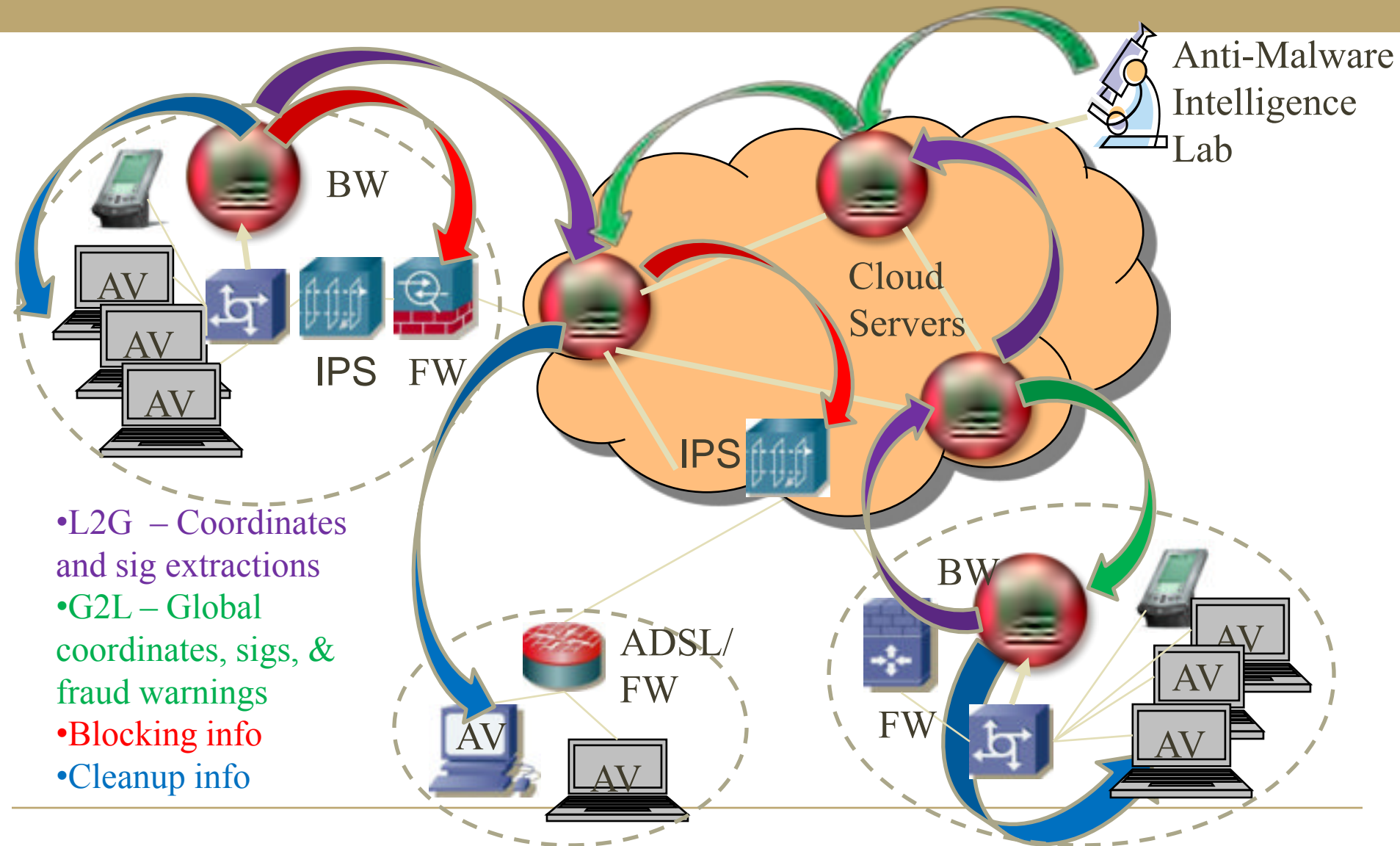


VM-Based Confirmation

- Seeing is believing
 - Instrumented virtual victim machines
 - Adaptive replay of captured traffic flows
 - Confirms malicious behavior/effect w/o signature
- Extract further intelligence
 - Extracts exploit signature for 0-day
 - Intercepts all outbound communications
 - Extracting target coordinates
 - Extracting communication signatures
 - Captures malware images
 - Captures OS changes
- Provide reliable linkage: **infection-malware-attack**



Anti-Malware Ecosystem





Examples: Rbot Infection

- 12/19/07 22:38:47.30 victim receives ping
 - Welchia/Nachi worm like scan behavior
- 12/19/07 22:38:47.69 receives DCE RPC request delivering BO exploit
 - RPC DCOM vulnerabilities MS03-026, MS03-39 (MS04-12 super patch)
- 12/19/07 22:38:55.24 compromised host TFTP **wiit.exe** from the infecting host
 - Malware image associated with spy bot W32/Rbot-AMS (first discovery 2005)



Rbot – cont'd

- 12/19/07 22:39:49.80 new bot attempts to resolve **irc.creativemindsircd.info**
- 12/19/07 22.39.50.92 new bot attempts to report to C&C server on **TCP/5598**:
 - *NICK USA|60742*
 - *USER xjhmfw 0 0 :USA|60742*
 - *:botserver 001 USA|60742 :Welcome to the x.y.z.w
USA|60742!xjhmfw@10.0.0.33*
 - *USERHOST USA|60742*
 - *MODE USA|60742 -x-i*
 - ***JOIN #g5 fuk***



Examples: ss.MEMEHEHZ.INFO Infection

- 2/1/08 00:43:26.72 code execution via **BO** in **ObjectName, DCOM IRemoteActivation** (Infection)
- 2/1/08 00:43:31.02 compromised host fetches **sgkcs.exe** from the infecting host on **TCP/52922** (Malware install)
- 2/1/08 00:46:21.51 new bot attempts to resolve **ss.MEMEHEHZ.INFO**
- 2/1/08 00:46:22.20 new bot attempts to report to C&C IRC server1 on **TCP/8080** (C&C connect)
- 2/1/08 00:46:28.75 new bot attempts to resolve **ss.nadnadzzz.info**
- 2/1/08 00:46:28.87 new bot attempts to report to C&C IRC server2 on **TCP/5190**



ss.MEMEHEHZ.INFO – cont'd

- 2/1/08 00:46:36.29 new bot attempts to resolve **ss.ka3ek.com**
- 2/1/08 00:46:36.53 new bot attempts to report to C&C IRC server3 on **TCP/10324**
 - *USER yikqx yikqx yikqx :mbecucphgblnvhp*
 - *NICK HdBeAoYM*
 - *:botserver 001 HdBeAoYM :Welcome to the x.y.z.w HdBeAoYM!yikqx@169.254.100.133*
 - *MODE HdBeAoYM +xi*
 - ***JOIN #kok6***



Examples: FQC Signatures For SNORT

- HTTP C&C @8.15.231.109:80

```
alert tcp any any -> 8.15.231.109 80 (sid:99002752;  
rev:1; msg:"503 HTTP_Botnet_Get_Update  
FEDefault"; content:"GET|20|/cgi-  
bin/bot/get.cgi?data="; depth: 250; nocase; )
```

- HTTP C&C @69.42.70.12:80

```
alert tcp any any -> 69.42.70.12 80 (sid:99002753;  
rev:1; msg:"503 IRC_Botnet_Report2Server  
FEDefault"; content:"GET|20|/checkin.php?affid=";  
depth: 250; nocase; )
```



FQC Signatures For SNORT – cont'd

- IRC C&C @ 206.63.81.89:6667
alert tcp any any -> 206.63.81.89 6667
(sid:99002593; rev:1; msg:"503
IRC_Botnet_JOIN_Channel FEDefault";
content:"JOIN|20|##boo##|20|.ghostman.|0d 0a|";
depth: 250; nocase;)
- IRC C&C @ 214.130.12.240:8080
▪ alert tcp any any -> 213.130.12.240 8080
(sid:99002655; rev:1; msg:"503
IRC_Botnet_JOIN_Channel FEDefault";
content:"JOIN|20|#*#|20|*!*!*!*|0d 0a|"; depth: 250;
nocase;)



Thank you!

Q & A
