

RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Twilight of Legacy AV Models

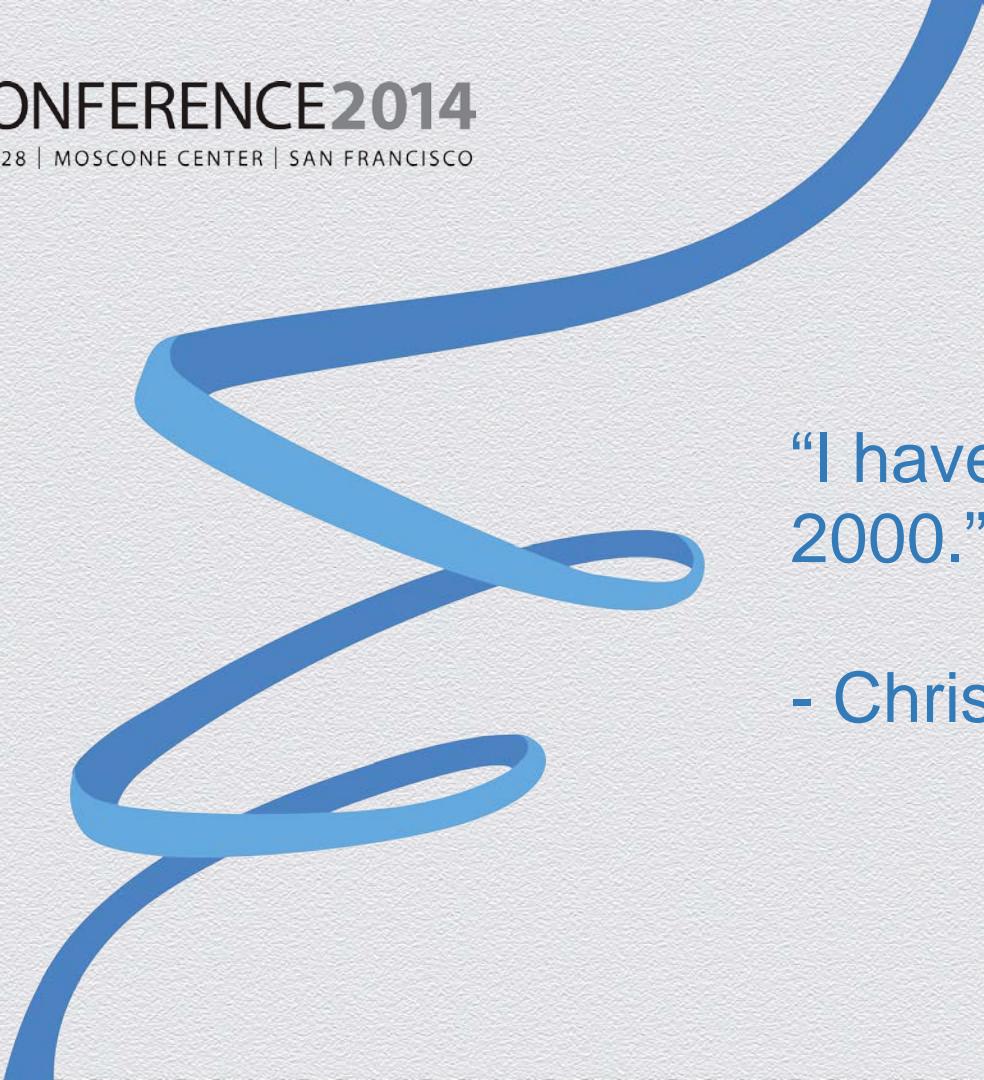
SESSION ID: SPO2-T07

Zheng Bu
FireEye Labs



RSA® CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



“I haven’t run AV since
2000.”

- Chris Jordan

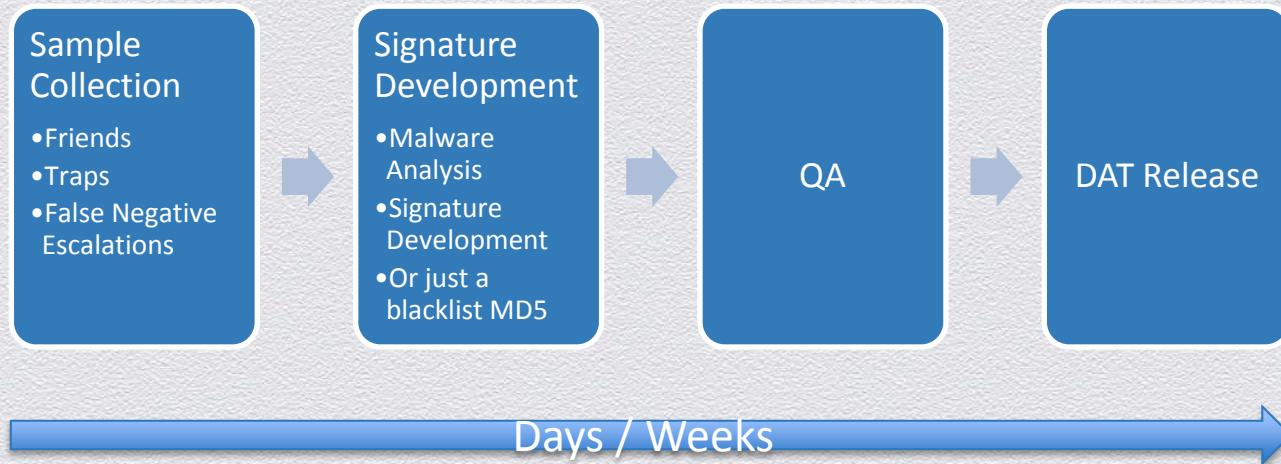
Agenda

- ◆ Malware Lifecycle
- ◆ AV reactive model
- ◆ Malware long tail / fat head distribution
- ◆ Advanced Attack Case Studies:
 - ◆ Operation DeputyDog
 - ◆ Operation Ephemeral Hydra
- ◆ Announcing FIX program
- ◆ Takeaways

Malware Development Life Cycle



AV Reactive Model



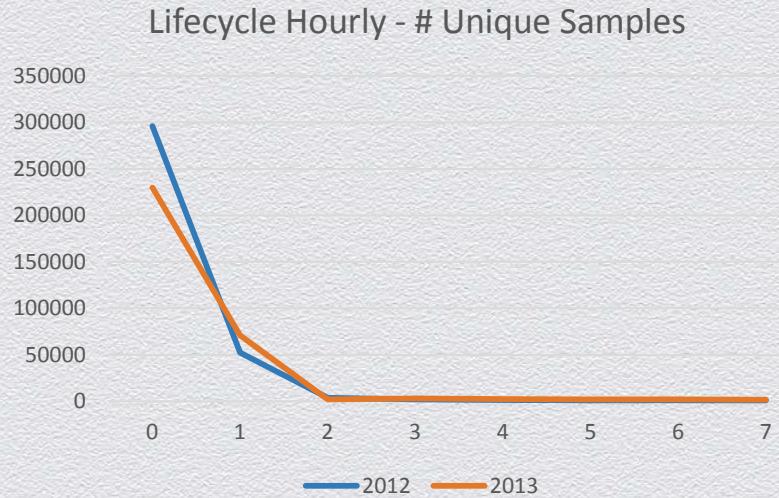
RSA® CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



**Legacy AV Model can
NOT catch up any
more**

Malware Lifecycle – The New Fat Head Theory



Malware Lifecycle – The New Fat Head Theory

67%

85%

67% Malware Happened Only Once

85% Malware Never Appear after 1 Hour

RSA® CONFERENCE 2014

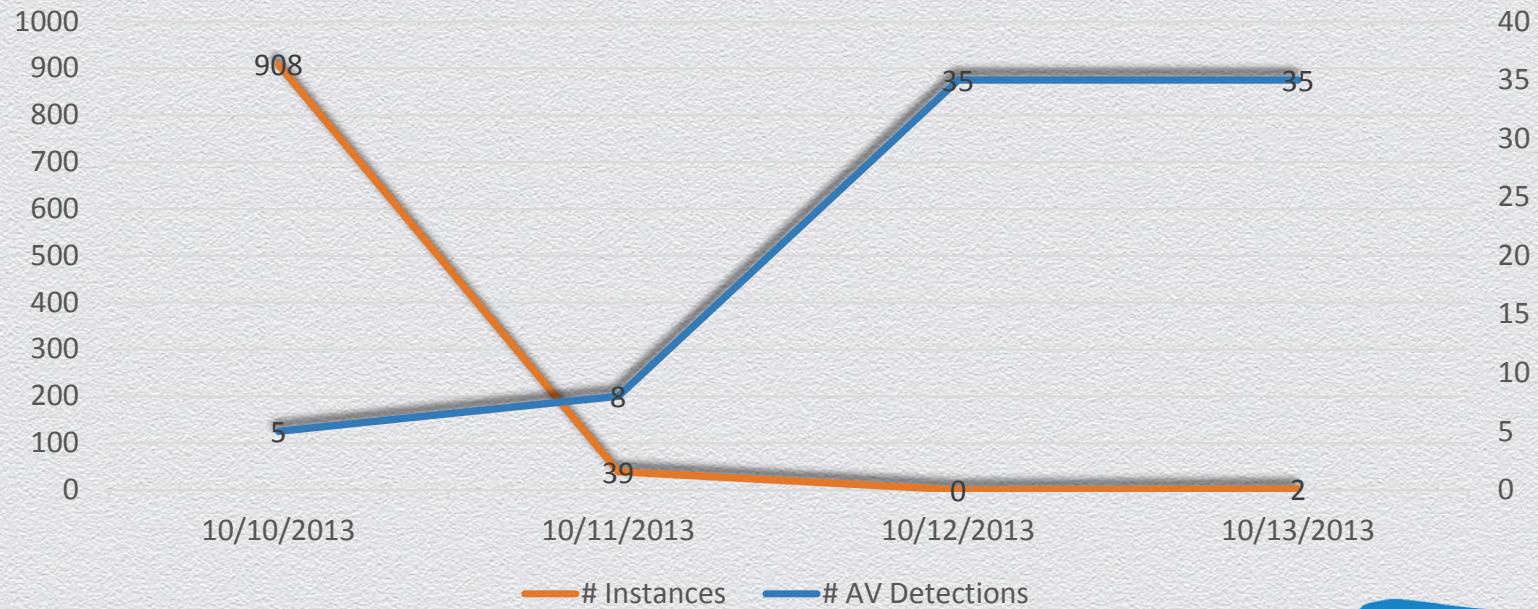
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



By the time AV
vendors release a
new signature,
Malware is long gone

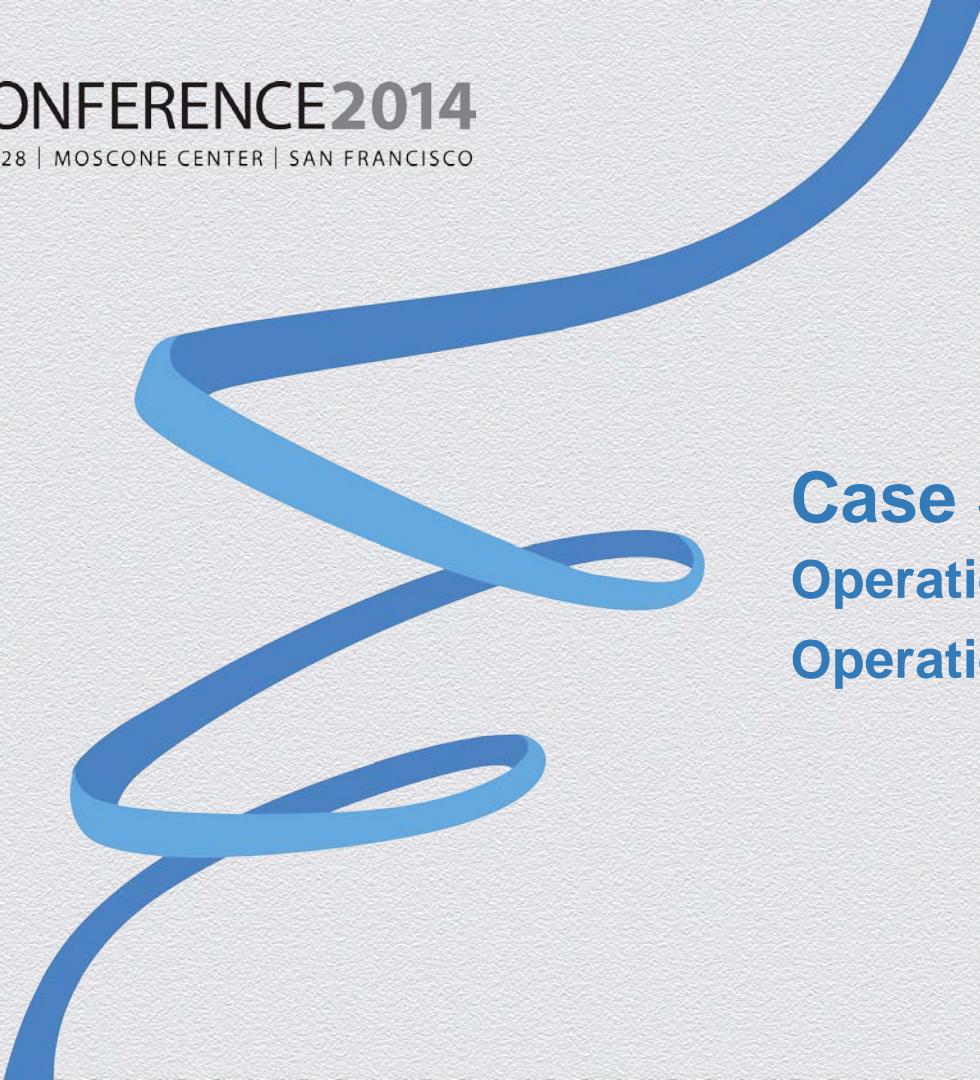
Malware Lifecycle and AV coverage

A ZBOT PDF Exploit



RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



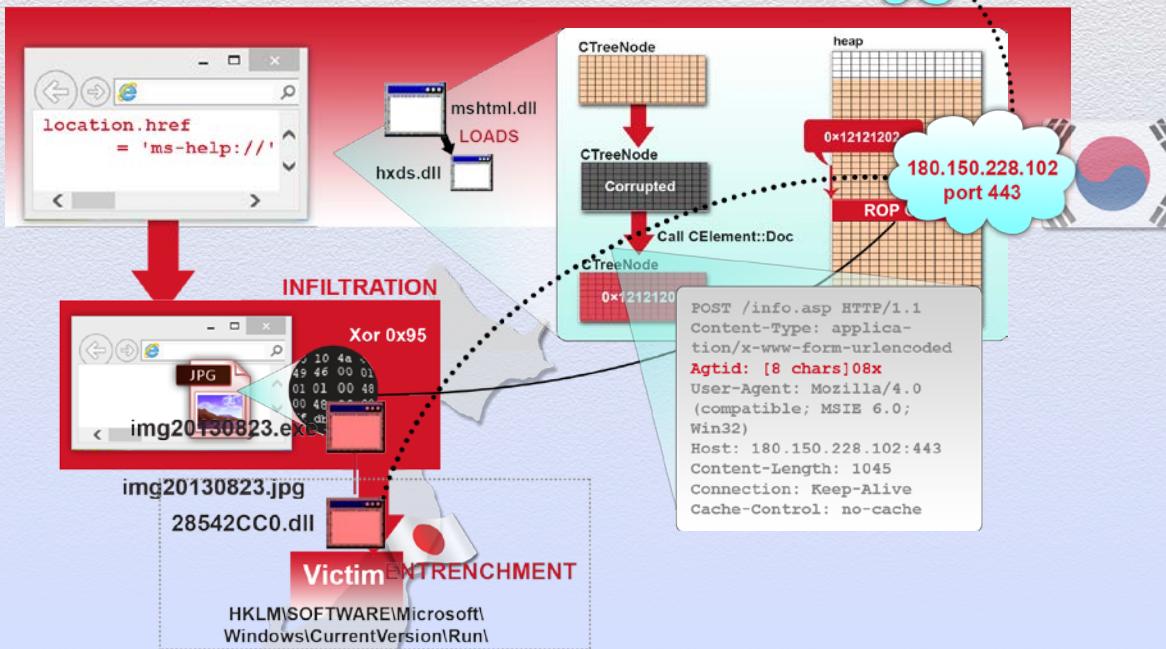
Case Study:

Operation DeputyDog

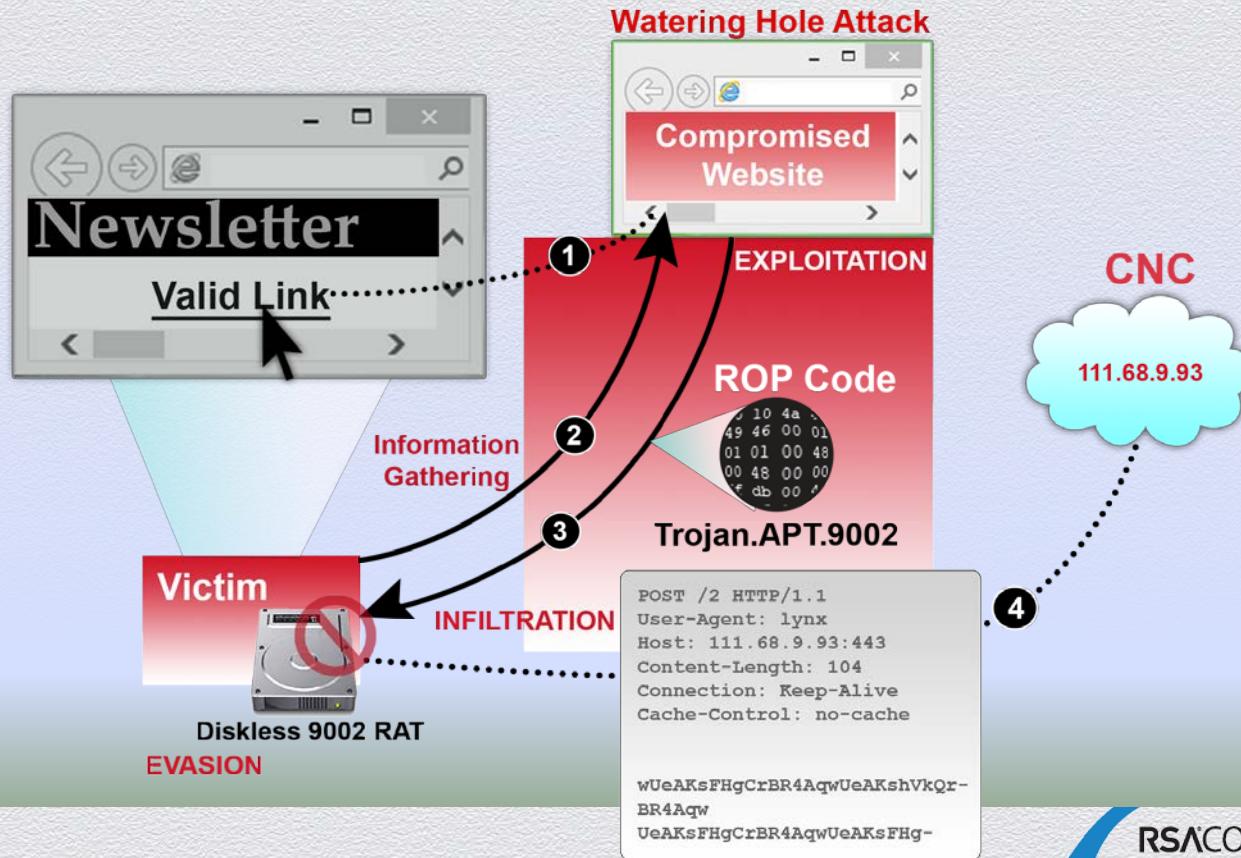
Operation Ephemeral Hydra

Operation DeputyDog

EXPLOITATION



Operation: Ephemeral Hydra



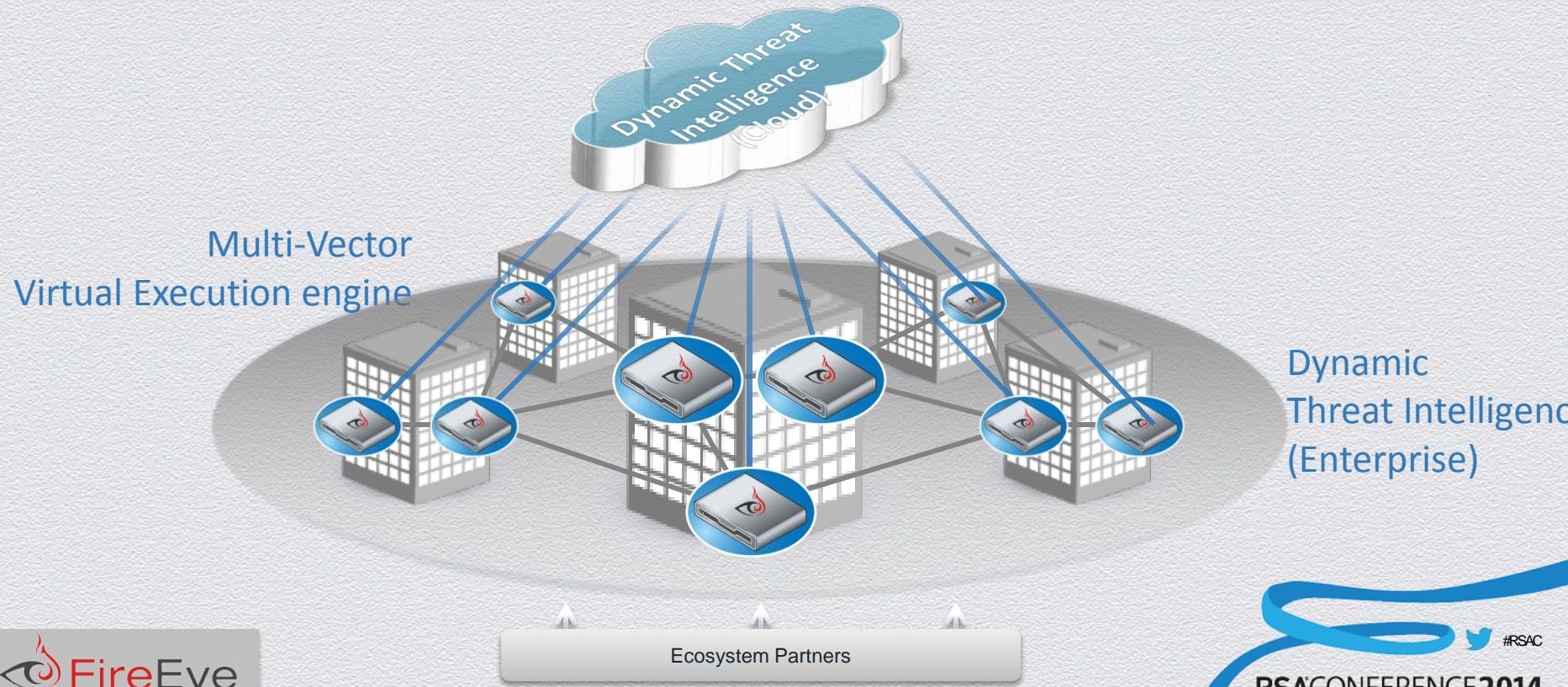
RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



New Prevention
Technology for
**Unknown Threats in
Real Time**

New Architecture: VMs at all points of attack + Integrated Threat Intelligence



RSA®CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Threat Intelligence Sharing

FIX Program

- ◆ Fireeye threat Intelligence eXchange Program (FIX)
 - ◆ Exploits, APT Campaigns
 - ◆ Detailed Threat Analysis
 - ◆ IOCs: emails, files, pages
 - ◆ C&C information, protocol analysis, domains
 - ◆ Threat Actor information
- ◆ CERT Organizations, Partners, Security Orgs
- ◆ Support OpenIOC Soon(<http://openioc.org>)

Takeaways

- ◆ Reactive AV model can not catch up with the new threat landscape
- ◆ New technology is needed for Unknown Threat prevention in Real Time
- ◆ Security Community should work together and share threat intelligence for faster mitigation
- ◆ Join our Intel Sharing by email fix@fireeye.com