Evolution of APT State of the Art

SANS Forensics & IR Summit 2010
APT Panel

Michael Cloppert
Intel Fusion lead
Lockheed Martin CIRT

whoami

Michael Cloppert

Intel Fusion Team Lead, LM-CIRT

Logged In Since: 6/1997, 6/2001, 9/2005

Formal education as engineer, scientist

- BS Computer Engineering, The University of Dayton
- MS Computer Science, The George Washington University

Industry certifications

- GCIA gold, GCFA gold, GREM
- Countless others (SCO?)

Industries include Financial Services, Fed Gov't, DoD

Constants Since 2006

Based on empirical evidence, beginning '04-'06:

Delivery: social engineering, highly targeted, user/wkstn

Exploits: ubiquitous app focus, used first in targeted attacks

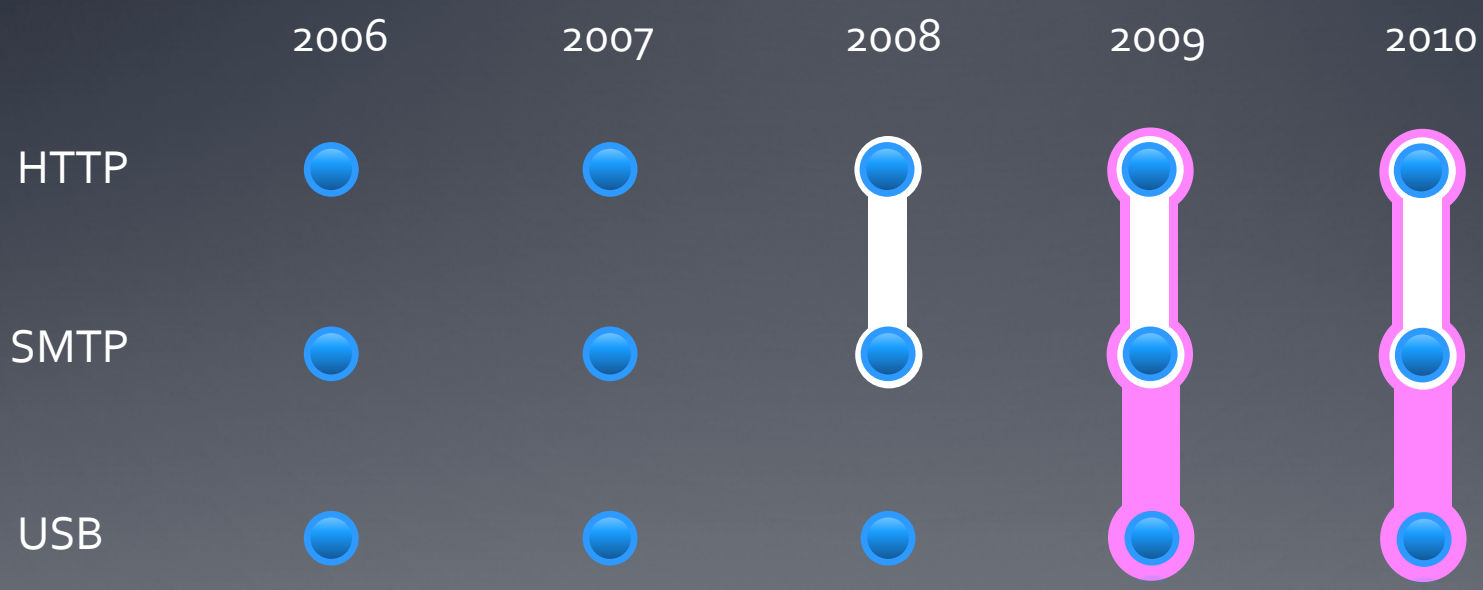
Objective: specific data, CNE

Capability: 24x7, situational awareness

Prior to 2006

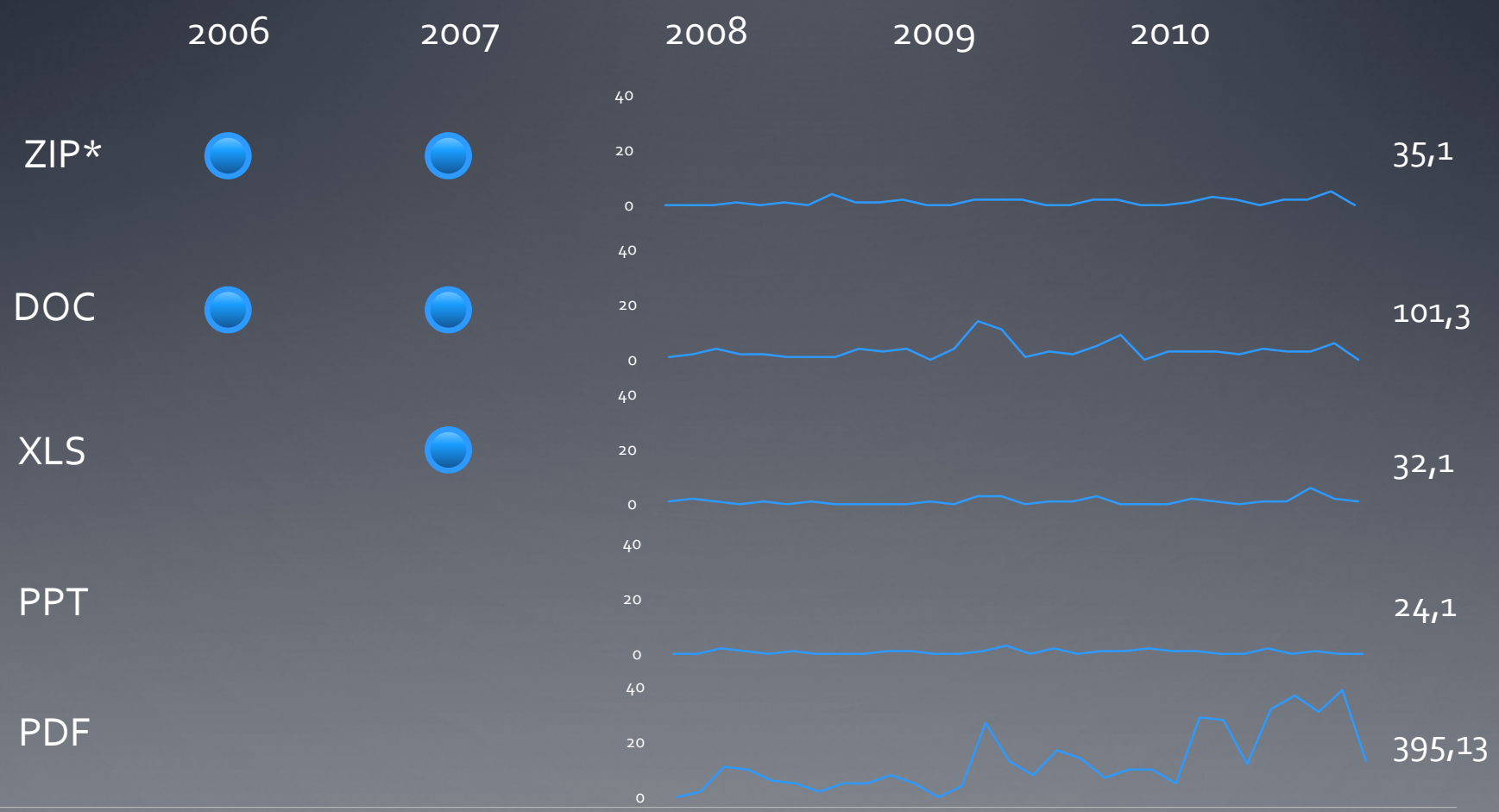
Classic intrusion methodology

Delivery Vector Evolution



Capability will persist and spread amongst adversaries once used

Exploit Trends



Activity observed; reliable measures unavailable

* - typically only exploit was social engineering

C2, Payload Obfuscation

Arms race:

- Base64
- Modified Base64
- XOR with keys increasing in size
- XOR with complex key scheduling
- SSL

Sleep tight…

No, you can't see the data (sorry)

Contact Info

mike@cloppert.org

Twitter: mikecloppert

Web:

- http://blog.cloppert.org
- https://blogs.sans.org/computer-forensics/author/mikecloppert/