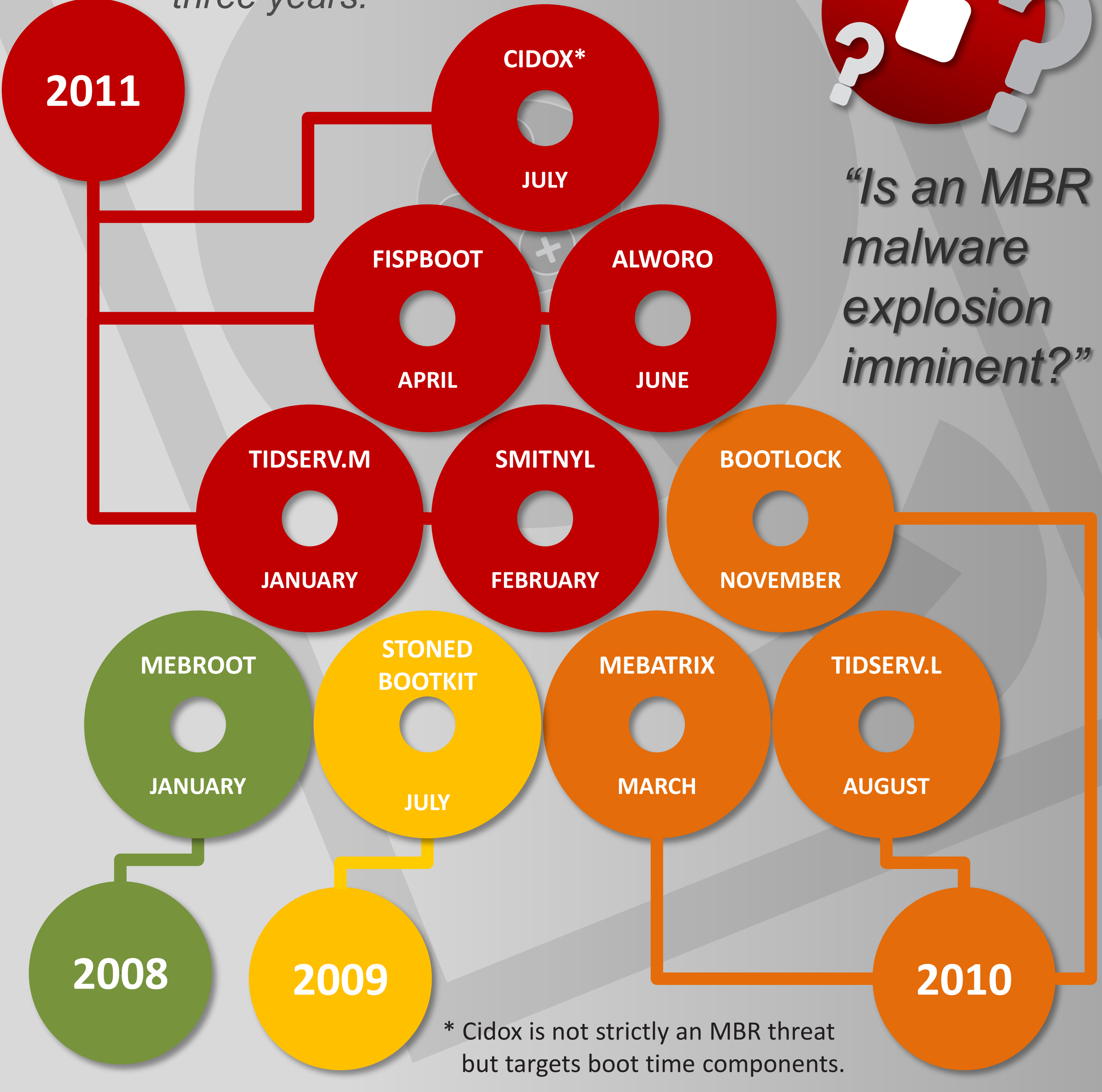
MBR Malware Back in Fashion

RETURN OF THE BOOTUP MALWARE

There has been as many new MBR threats found in the first seven months of 2011 as there were in all the previous three years.



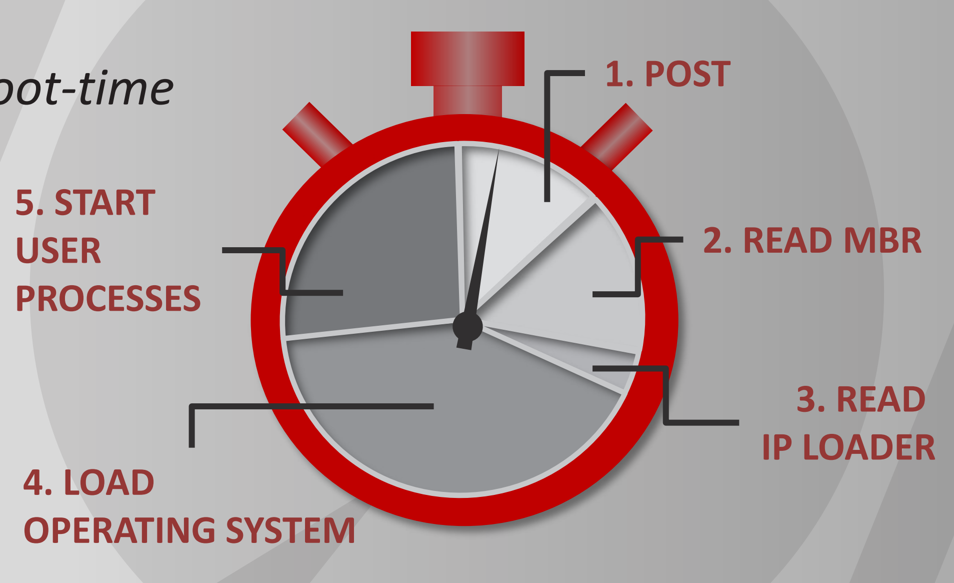
"Is an MBR malware explosion imminent?"

* Cidox is not strictly an MBR threat but targets boot time components.

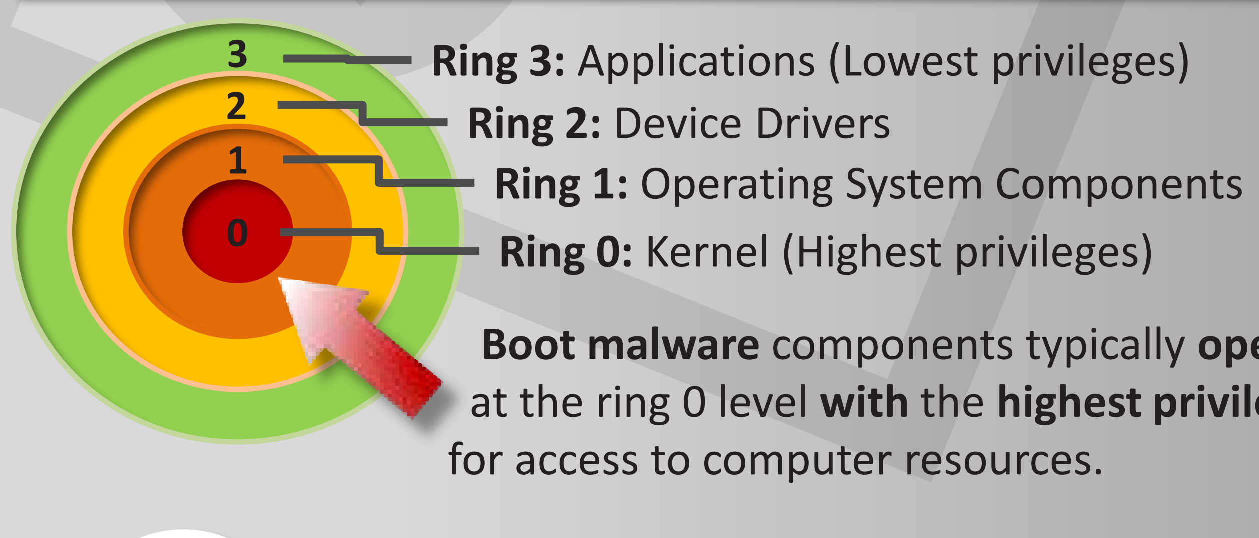
THE GOAL OF MBR/BOOT TIME MALWARE

"... get in quick ..."

"The goal of boot-time infection is to get the malware loaded onto the computer before the operating system does. Whatever gets loaded first ultimately calls the shots."



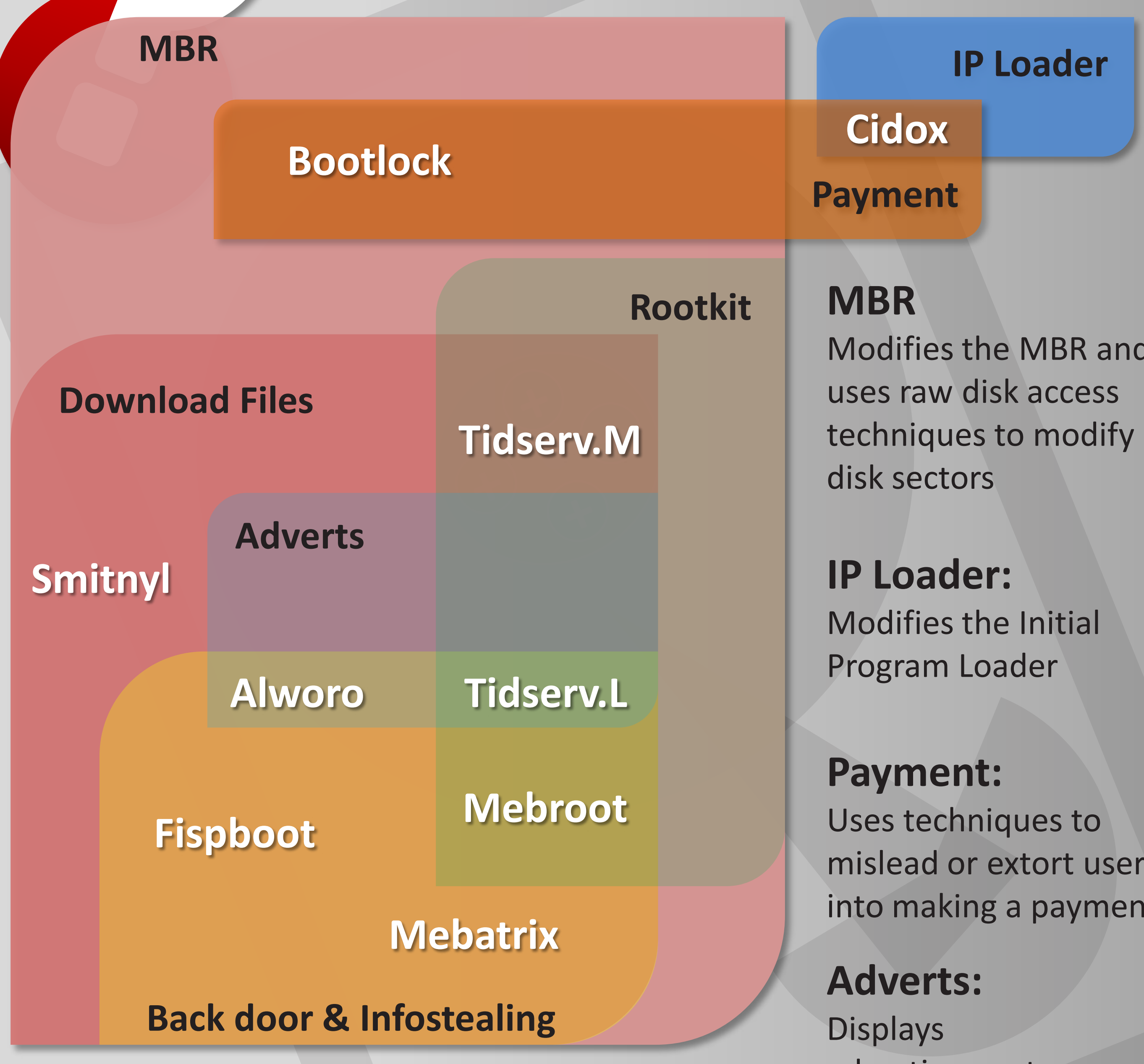
PROTECTION RING SECURITY ARCHITECTURE



Ring 3: Applications (Lowest privileges)
Ring 2: Device Drivers
Ring 1: Operating System Components
Ring 0: Kernel (Highest privileges)

Boot malware components typically **operate** at the ring 0 level **with** the **highest privileges** for access to computer resources.

WHAT THEY DO



MBR
Modifies the MBR and uses raw disk access techniques to modify disk sectors

IP Loader:
Modifies the Initial Program Loader

Payment:
Uses techniques to mislead or extort users into making a payment

Adverts:
Displays advertisements

Rootkit: Uses techniques to hide its presence

Back door: Opens a back door allowing remote communications

Download Files: Download files from a remote location

Infostealing: Collects information and uploads it to a remote location

A BRIEF HISTORY OF BOOT MALWARE

"Boot infection is not a new idea..."

2000
Boot sector viruses such as **Stoned.Michealangelo** were all the rage

2005
eEye researchers present **BootRoot** project at BlackHat

2007
Researchers at NVLabs present **Vbootkit** at BlackHat

*"Many boot malware including **Mebroot** and **Fispboot** are based on **BootRoot** code"*

2007/2008
Mebroot makes its debut

2009
StonedBootkit appears, **Vbootkit** becomes open source

2010
Mebatrix, **Tidserv.L**, and **Bootlock** debut

2011
Tidserv.M, **Smitnyl**, **Fispboot**, **Alworo**, and **Cidox**

"What's in store for the rest of 2011?"

Sources:
http://www.symantec.com/connect/blogs/mbr-rootkit-paper-vb2008
http://www.symantec.com/connect/blogs/bootroot-trojanmebroot-rootkit-your-mbr
http://www.blackhat.com/presentations/bh-usa-05/bh-us-05-soeder.pdf
http://www.nvlabs.in/?q=node/16

Symantec.