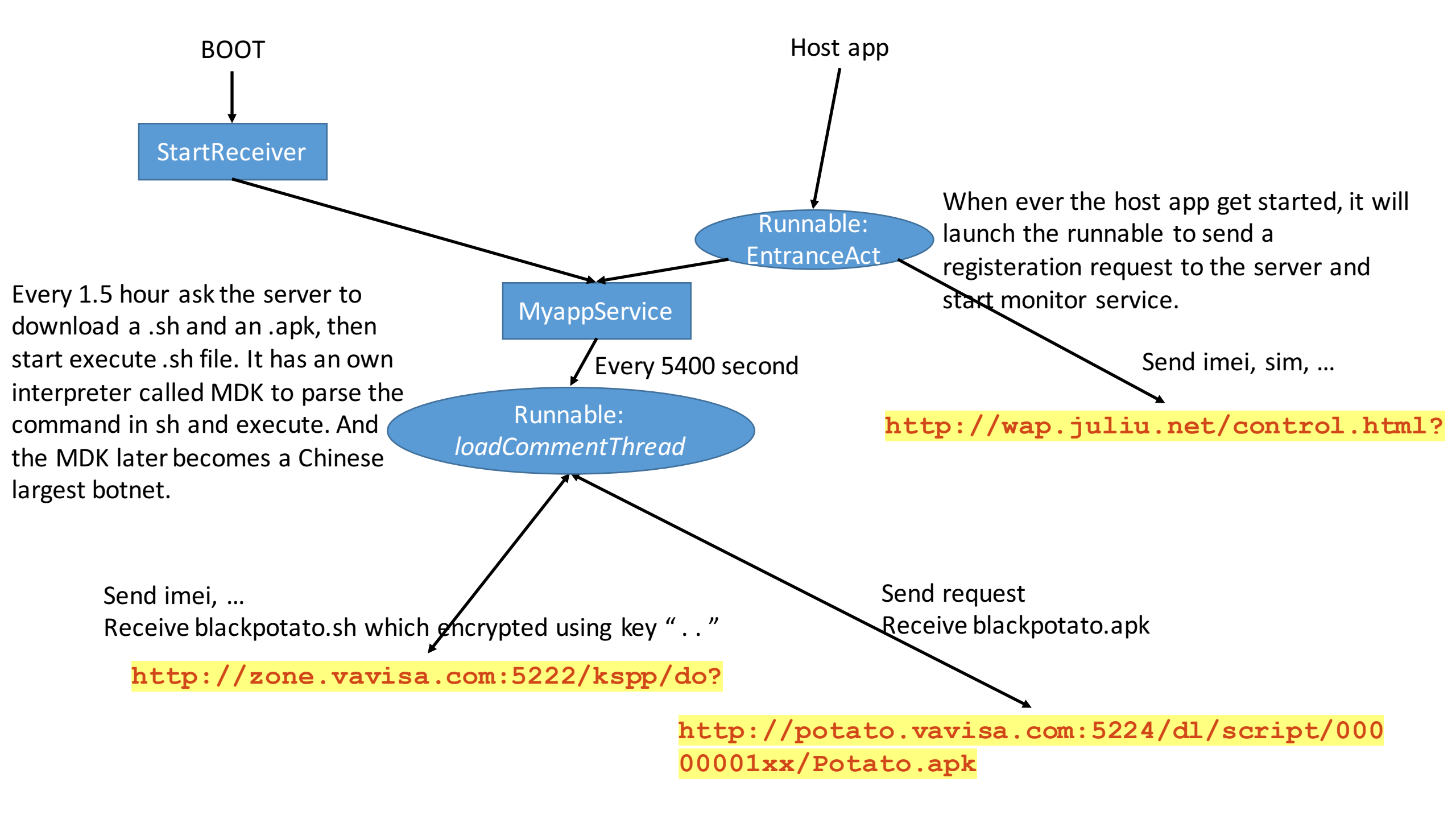
Ksapp Variety1


BOOT
Host app
StartReceiver
Runnable:
EntranceAct
When ever the host app get started, it will launch the runnable to send a registeration request to the server and start monitor service.
Every 1.5 hour ask the server to download a .sh and an .apk, then start execute .sh file. It has an own interpreter called MDK to parse the command in sh and execute. And the MDK later becomes a Chinese largest botnet.
MyappService
Every 5400 second
Send imei, sim, …
http://wap.juliu.net/control.html?
Runnable:
loadCommentThread
Send imei, …
Receive blackpotato.sh which encrypted using key " . . "
http://zone.vavisa.com:5222/kspp/do?
Send request
Receive blackpotato.apk
http://potato.vavisa.com:5224/dl/script/00000001xx/Potato.apk

MDK analysis

- It’s an interpreter which has a Lexer and Parser.
- The Lexer allows token, like:
  - if, then, endif, elseif, else
  - while, endwhile
  - func, endfunc
  - Basic java types
  - ID
  - Etc.
- Parser will then parse the .sh file line by line and generate a func list and var list.
- MDK controller will start from “start” func, and eval line by line to do the task. It has the type mappers to map from MDK type to java type. And if eval call statement, it will issue call in JVM via reflection.

- For this kind of malware, I consider it can do anything allowed by the apk’s permission.