

# App Armor

Will Chen

Gaba

2019.11.17

@GoHack 2019



# Threats

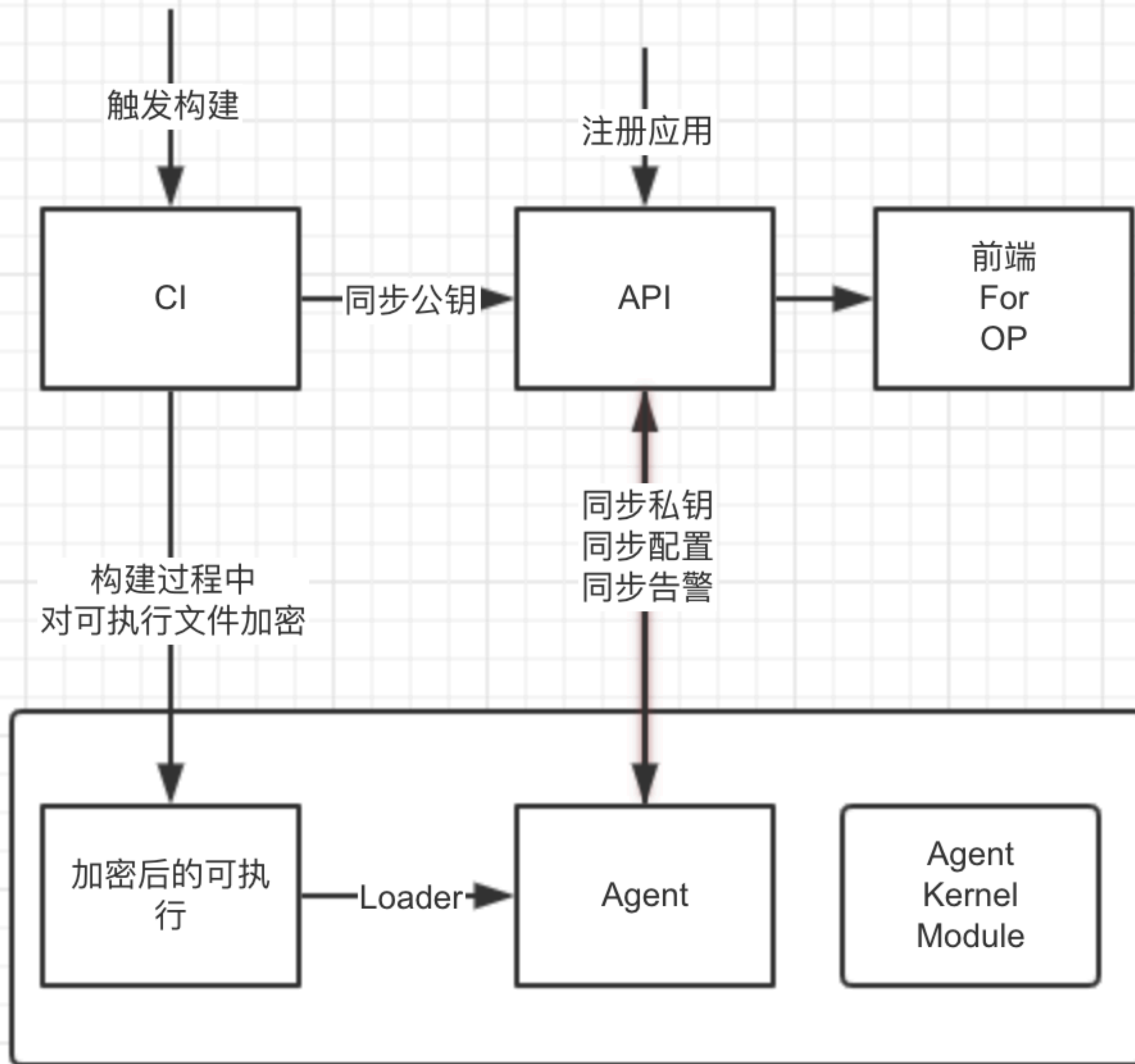
- A. 生产环境可执行文件窃取
- B. 非可靠生产环境
- C. 可执行文件被调试
- D. 过高的执行权限
- E. 可执行程序被篡改



# Integration with CI/CD

在构建阶段对可执行文件进行重新打包

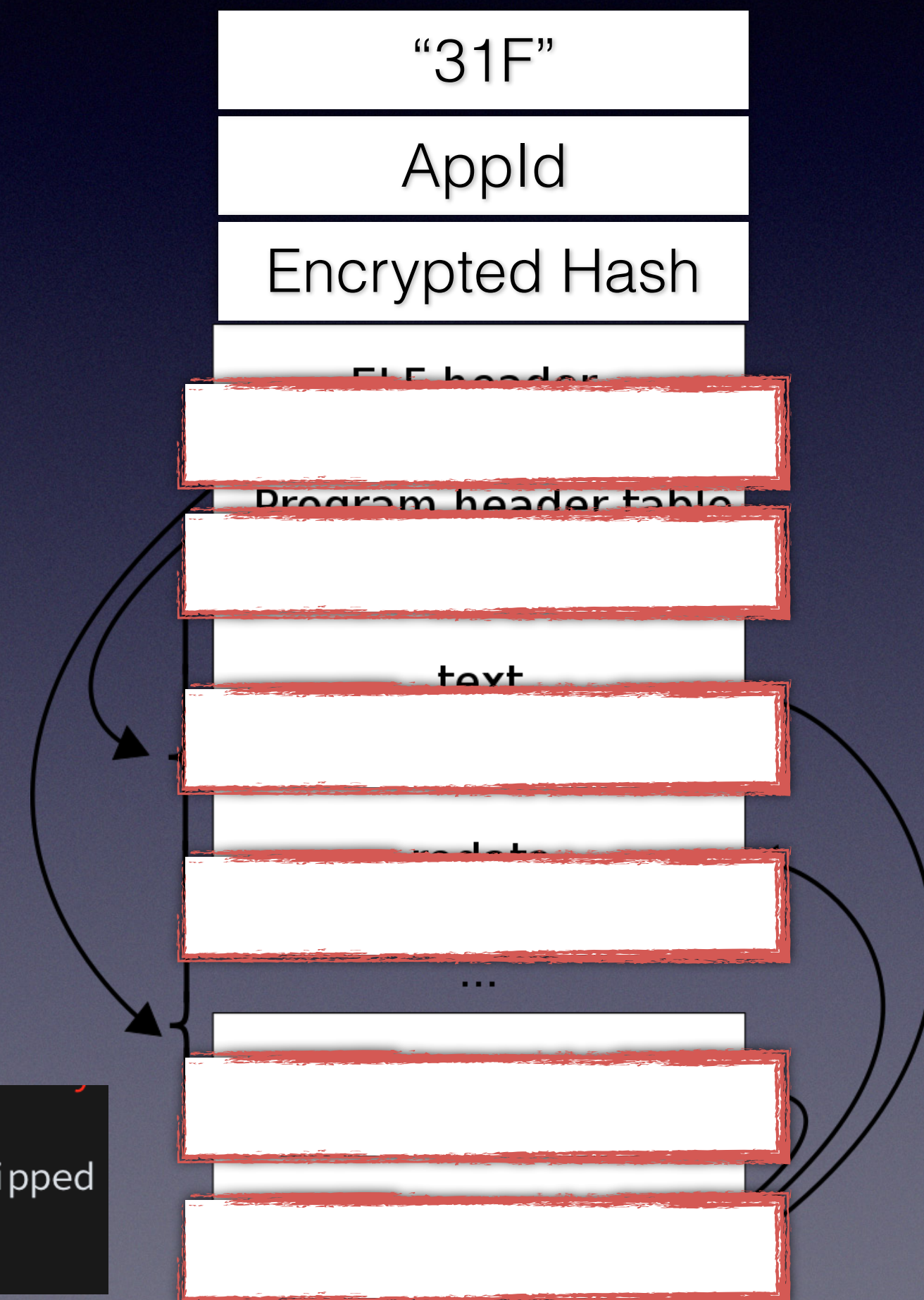
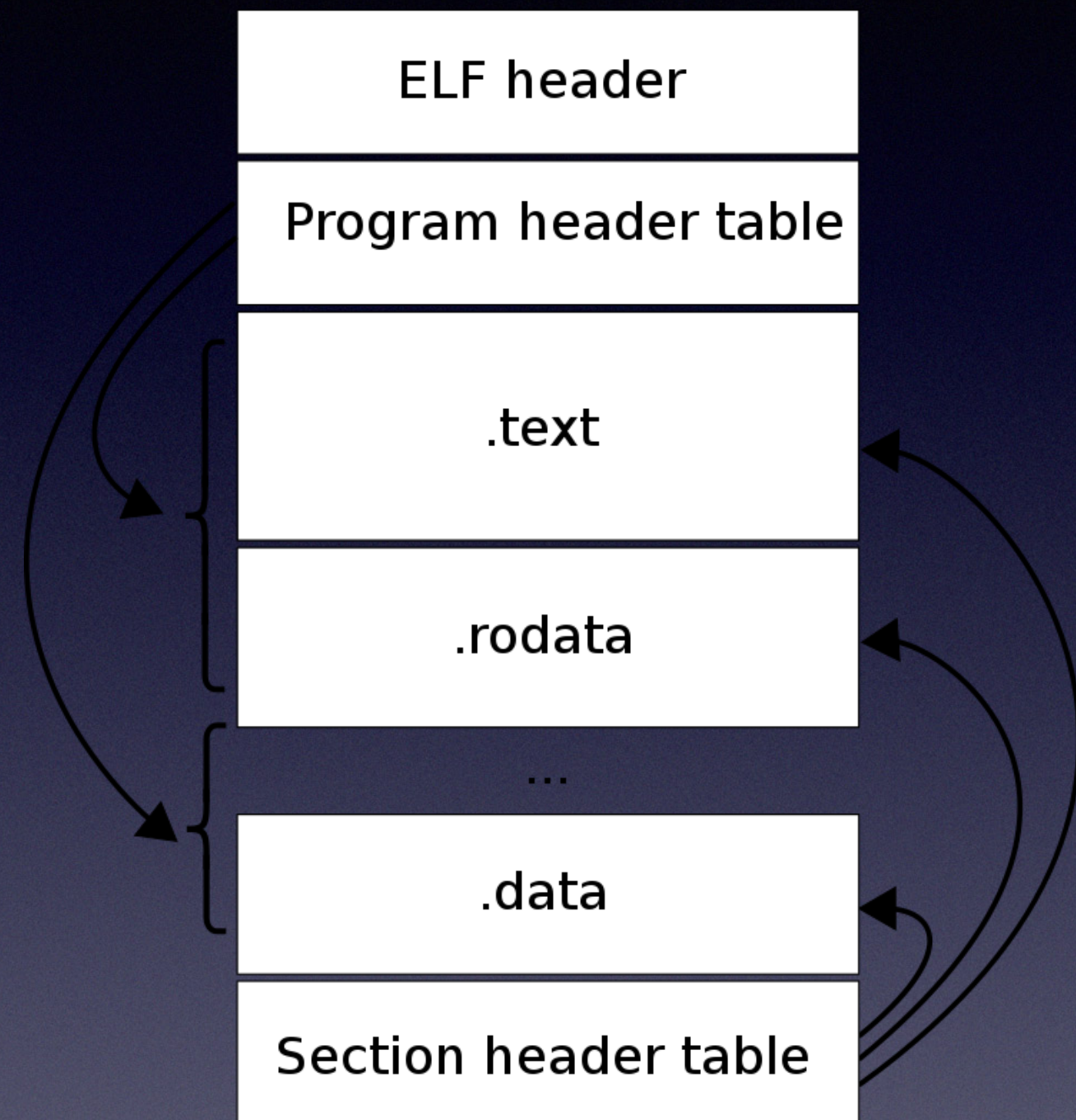
在执行前经过安全检查和加载





# ELF 粉碎加密

区间块加密，降低文件体积  
无法手动恢复的ELF




```
/o/youzu ➤ file main main.enc
main:      ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, not stripped
main.enc: data
/o/vouzu ➤
```



# Loader in Go

解密可执行文件  
调用memfd\_create进行无文件执行

```
func CreateMemfd(name string) *MemFD {  
    fd, _, _ := syscall.Syscall(MFD_CREATE, uintptr(unsafe.Pointer(&name)), uintptr(MFD_CLOEXEC), 0)  
    return &MemFD{  
        os.NewFile(fd, name),  
    }  
}  
  
func (self *MemFD) Write(bytes []byte) (int, error) {  
    return syscall.Write(int(self.Fd()), bytes)  
}  
  
func (self *MemFD) Path() string {  
    return fmt.Sprintf("/proc/self/fd/%d", self.Fd())  
}  
  
func (self *MemFD) ExecuteWithAttributes(procAttr *syscall.ProcAttr, arguments ...string) (int, uintptr, error) {  
    return syscall.StartProcess(self.Path(), append([]string{self.Name()}, arguments...), procAttr)  
}
```






# Loader in Go

无文件，不落盘

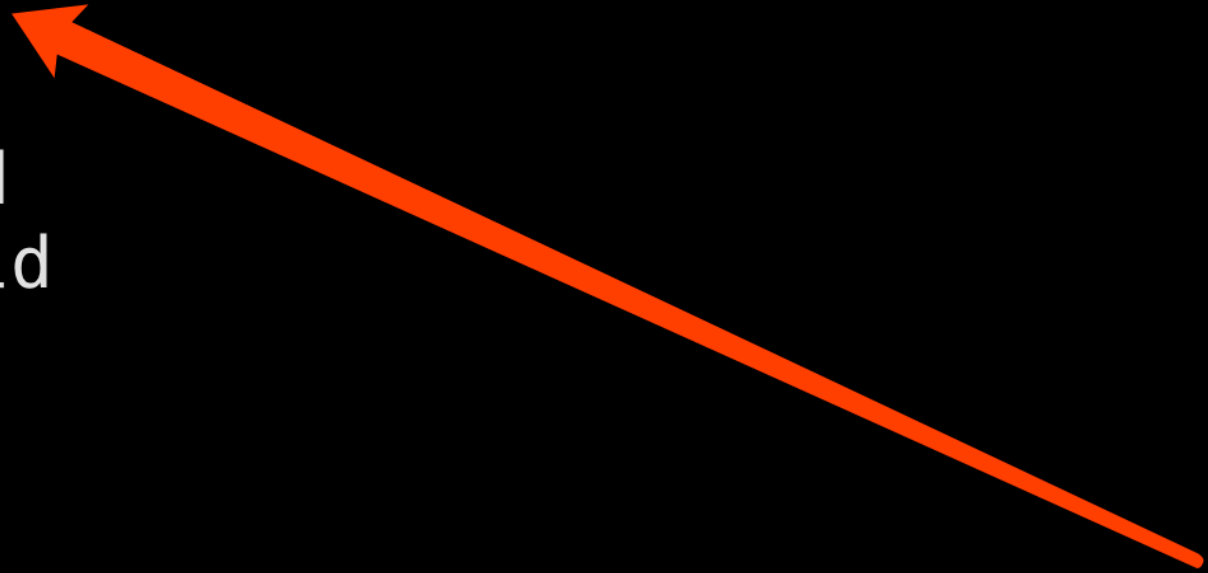
```
root@10-6-24-60-aq ~/g/s/i/b/agent# cd /proc/10569/
root@10-6-24-60-aq /p/10569# ll -a
total 0
dr-xr-xr-x    9 nobody nobody 0 Nov 17 09:17 ./
dr-xr-xr-x 470 root    root    0 May  9 2019 ../
dr-xr-xr-x    2 nobody nobody 0 Nov 17 09:18 attr/
-rw-r--r--    1 nobody nobody 0 Nov 17 09:18 autogroup
-r-----    1 nobody nobody 0 Nov 17 09:18 auxv
-r--r--r--    1 nobody nobody 0 Nov 17 09:18 cgroup
--w-----    1 nobody nobody 0 Nov 17 09:18 clear_refs
-r--r--r--    1 nobody nobody 0 Nov 17 09:17 cmdline
-rw-r--r--    1 nobody nobody 0 Nov 17 09:18 comm
-rw-r--r--    1 nobody nobody 0 Nov 17 09:18 coredump_filter
-r--r--r--    1 nobody nobody 0 Nov 17 09:18 cpuset
lrwxrwxrwx    1 nobody nobody 0 Nov 17 09:17 cwd -> /root/go/src/improved-octo-giggle/
bin/agent/
-r-----    1 nobody nobody 0 Nov 17 09:18 environ
lrwxrwxrwx    1 nobody nobody 0 Nov 17 09:17 exe -> /memfd:???Y?? (deleted)
dr-x-----    2 nobody nobody 0 Nov 17 09:17 fd/
dr-x-----    2 nobody nobody 0 Nov 17 09:18 fdinfo/
-rw-r--r--    1 nobody nobody 0 Nov 17 09:18 gid_map
```





# Anti Debug/Permission protected

```
X ./.agent /root/go/src/improved-octo-giggle/bin/agent (ssh)
root@10-6-24-60-aq ~/g/s/i/b/agent# ls
agent* agent.go
root@10-6-24-60-aq ~/g/s/i/b/agent#
./agent -path /root/gohack/test.enc -host localhost:5000
Hello World
pHello World
s Hello World
Hello World
Hello World
Hello World
Hello World
Hello World
Hello World
Hello World
Hello World
Hello World
```



```

root@10-6-24-60-aq ~/g/s/i/b/agent# ps aux | grep test
root      10557  2.5  0.0 606020  9104 pts/1    Sl+  09:17
           0:00 ./agent -path /root/gohack/test.enc -host localhost
           :5000
nobody    10569  0.0  0.0   4212   348 ?        Ss   09:17
           0:00 /root/gohack/test.enc
root      10605  0.0  0.0 112676   728 pts/3    S+   09:17
           0:00 grep --color=auto test
root@10-6-24-60-aq ~/g/s/i/b/agent# strace -p 10569
strace: attach: ptrace(PTRACE_ATTACH, ...): Operation not
permitted
root@10-6-24-60-aq ~/g/s/i/b/agent#

```

```
func DenyPtrace(pid int) (err error) {
    _, _, e := syscall.Syscall6(PTRACE, uintptr(PTRACE_SEIZE), uintptr(pid), uintptr(0), uintptr(0), uintptr(0), uintptr(0))
    if e != 0 {
        err = syscall.Errno(e)
        return err
    }
    return
}
```



# Base Line Check

同时保证可执行程序在安全的环境中执行：

- A. DNS
- B. /proc protect
- C. System Vuln Patch



Alert List

Appid	DNS	AbsPath	Argv	Envv	Ptrace	UserName
35097736-fb36-4c7e-9217-61794e9299dc		/tmp/test			false	
9dc958b3-2db3-4b9b-b087-4429604b2aca	10.6.48.128	/tmp/test			false	
b8a2b9c0-fc69-402a-9691-f648cfe1f7c4	10.6.48.128	/tmp/test			false	
b8f8377d-c968-4e66-b9ce-5b79c23a570f	10.6.48.128	/tmp/test			false	



← → ↺ ⓘ Not Secure   2smith:8088/alertlist.html							🔍 ☆ 🔄 🌐 🐞 📄 📡   🧑		
📁 Apps 📁 security 📁 software 📁 tools 📁 blog/forum 📁 杂 📁 study									
10	2019-11-17T00:35:11.492418195+08:00	2019-11-17T00:35:11.492418195+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				
11	2019-11-17T00:53:54.476128342+08:00	2019-11-17T00:53:54.476128342+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				
13	2019-11-17T00:56:17.505620566+08:00	2019-11-17T00:56:17.505620566+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				
14	2019-11-17T00:56:32.730327668+08:00	2019-11-17T00:56:32.730327668+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	danger	file watcher	File Writed			
15	2019-11-17T00:56:45.298015679+08:00	2019-11-17T00:56:45.298015679+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	danger	file watcher	File Writed			
16	2019-11-17T00:56:45.303592034+08:00	2019-11-17T00:56:45.303592034+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	danger	file watcher	File Writed			
17	2019-11-17T01:00:13.651975522+08:00	2019-11-17T01:00:13.651975522+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				
18	2019-11-17T01:14:05.8011897+08:00	2019-11-17T01:14:05.8011897+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				
19	2019-11-17T01:14:18.713871711+08:00	2019-11-17T01:14:18.713871711+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	danger	file watcher	File Writed			
20	2019-11-17T01:14:18.719374395+08:00	2019-11-17T01:14:18.719374395+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	danger	file watcher	File Writed			
21	2019-11-17T01:28:02.224500045+08:00	2019-11-17T01:28:02.224500045+08:00	b8f8377d-c968-4e66-b9ce-5b79c23a570f	success	runtime				



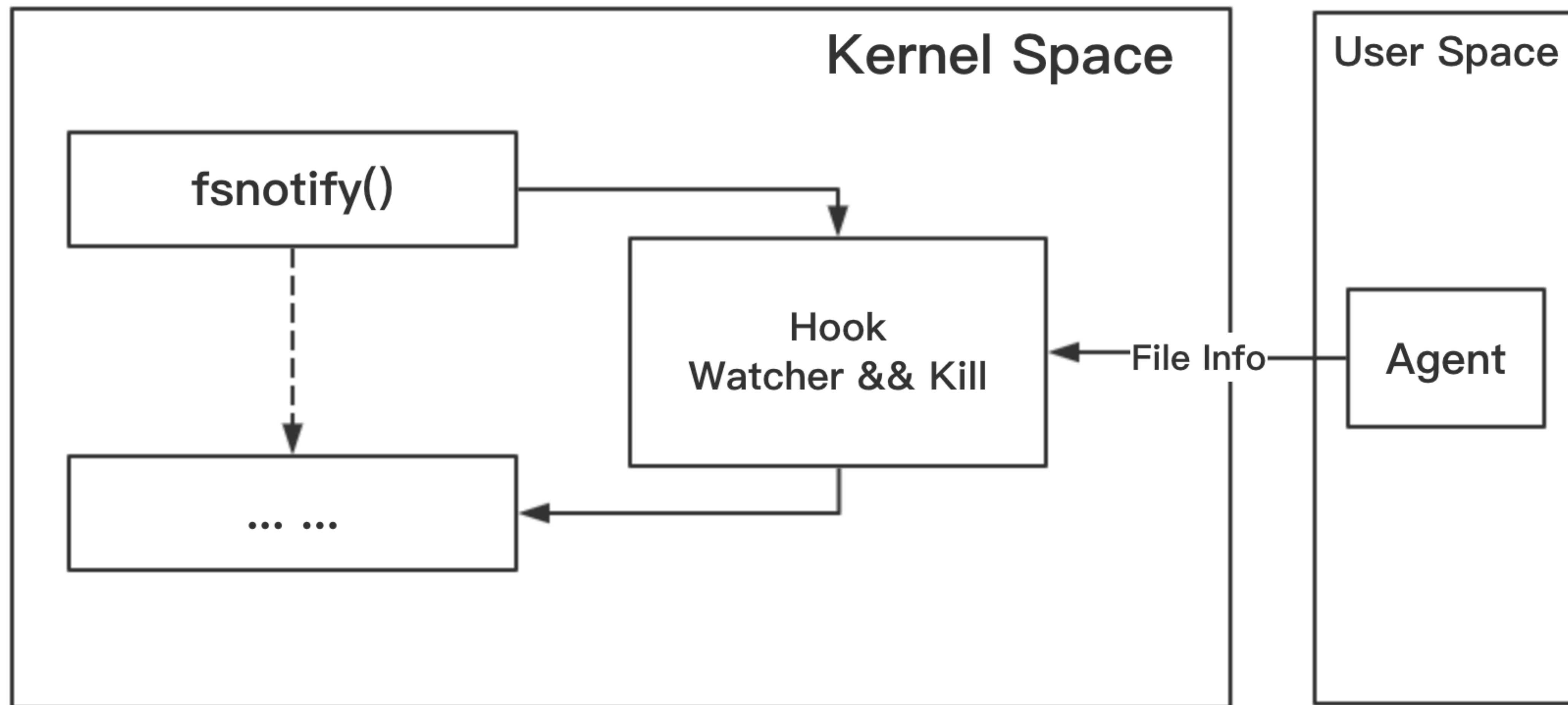
**DEMO**



ELF Encrypt?  
Anti Ptrace()?



# 彩蛋

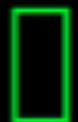




```
root@test ~/g/lkm# echo "+/2589/" > /dev/smith
root@test ~/g/lkm# cat /proc/2589/comm
fish: 'cat /proc/2589/comm' terminated by signal SIGKILL (Forced quit)
root@test ~/g/lkm#
```

```
[ 6.392760] IPv6: ADDRCONF(NETDEV_CHANGE): ens3/: link becomes ready
[ 7.730982] floppy0: no floppy controllers found
[ 7.731088] work still pending
[ 76.966984] smith: loading out-of-tree module taints kernel.
[ 76.967045] smith: module verification failed: signature and/or requ
[ 76.968916] [SMITH] init_share_mem success
```

```
[ 120.317702] [*] Add Protect List: /2589/
[ 126.959148] [!!!] Don't Touch Me(/2589/comm) 0|2703!
```





Open Source Today:

<https://github.com/AlkenePan/KAP>