Malicious Linux Binaries: A Landscape

Lucas Galante, Marcus Botacin, André Grégio, Paulo Lício de Geus

SBSEG 2018

Agenda

Agenda

Are there Linux malware?

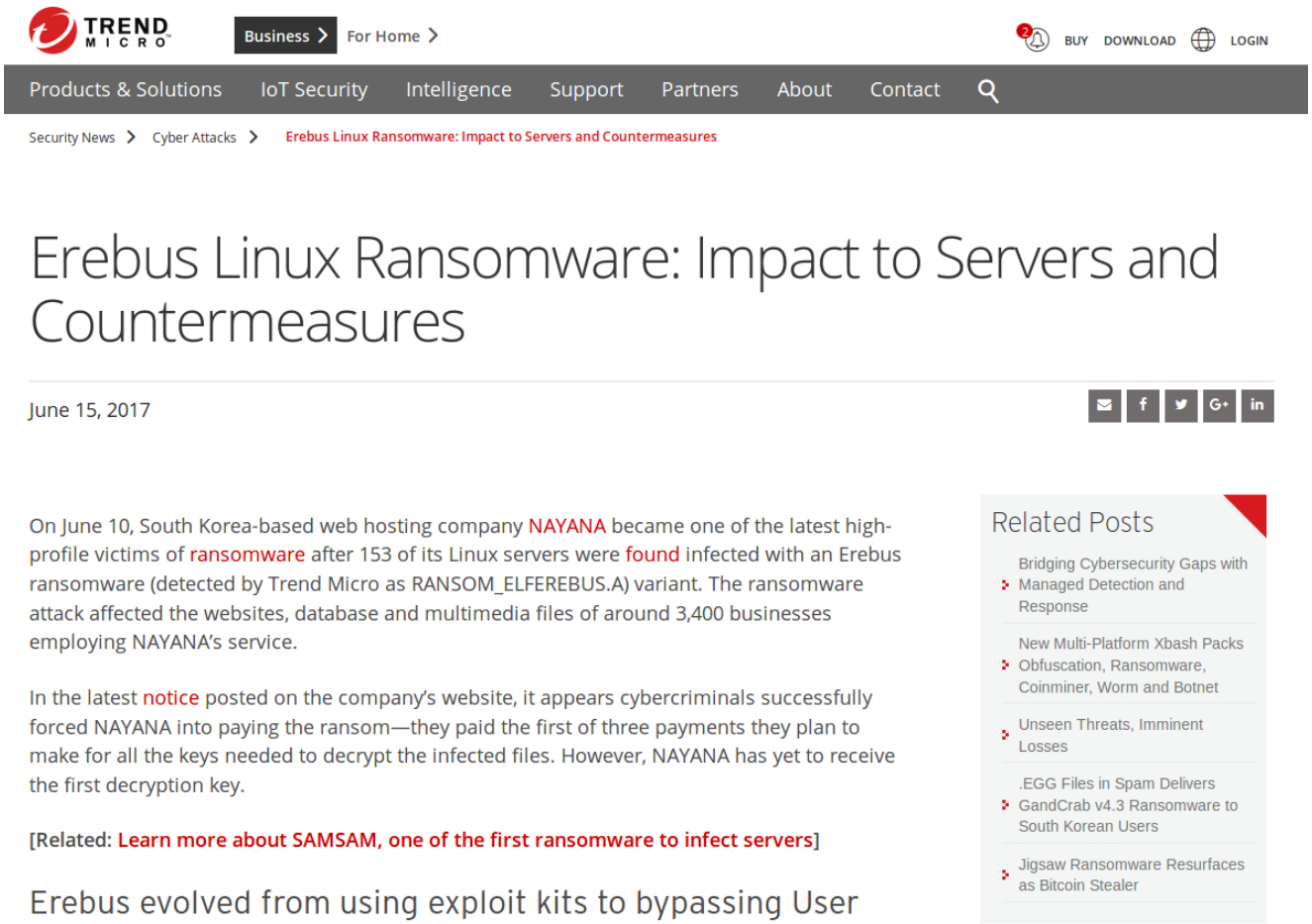

Figure: Erebus ransomware attacks South Korean internet provider.

Agenda

Binaries Architectures

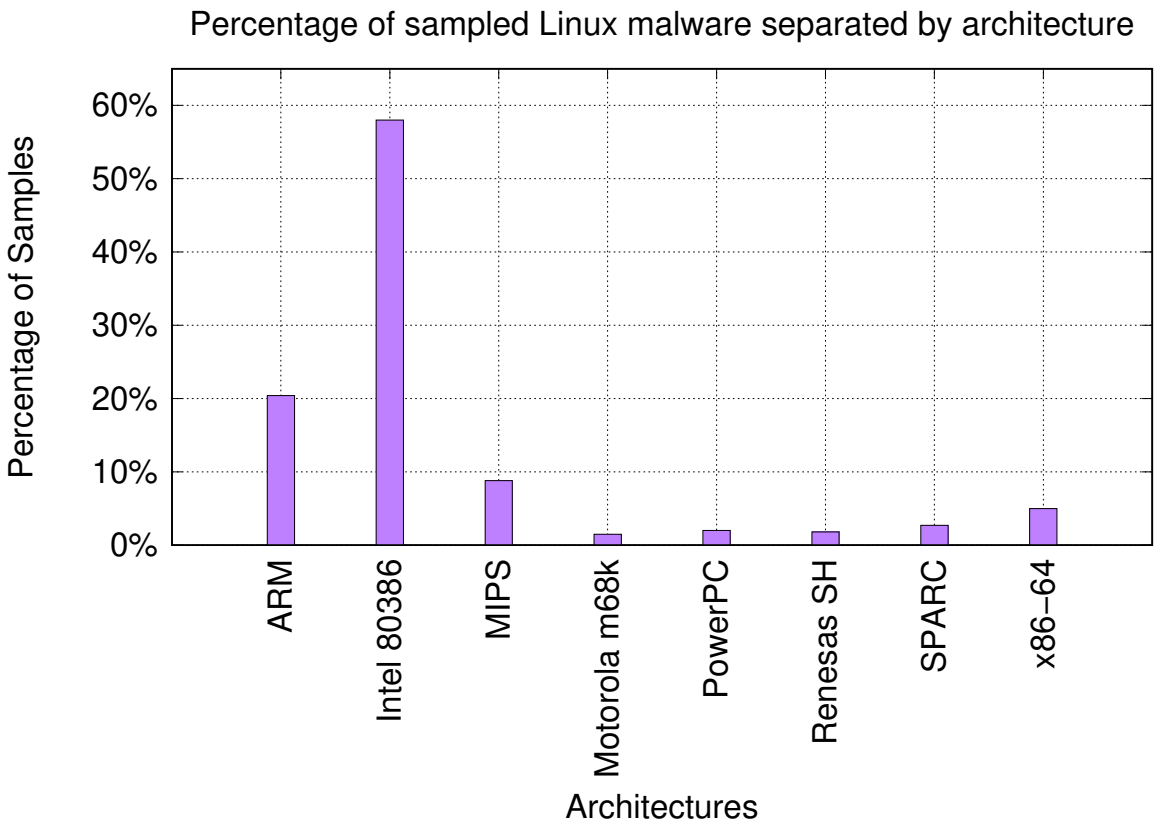

Figure: ELF binary samples distributed by architectures.

Agenda

Analysis Techniques

Table: Adopted strategy to handle evasive samples.

Technique	Tool	Evasion	Countermeasure
Static analysis	*objdump* *file* *strings*	obfuscation	Dynamic analysis
Dynamic analysis	*ltrace* *ptrace* *strace* *LD_PRELOAD*	Static compilation *ptrace* check Long *sleep* Injection blocking	*ptrace* step-by-step binary patching *LD_PRELOAD* Kernel *hooks*

Agenda

Malware Behavior Taxonomy

Table: Identified invoked system calls.

Network	Evasion	Environment	Removal	Timing	Memory	Modularity
socket	fork	gettimeofday	unlink	time	mmap	execve
connect	kill	access	rmdir	wait	munmap	fork
poll	ptrace	uname	kill	nanosleep	mprotect	clone
select		ioctl				exit
getsockname						getppid

Objdump

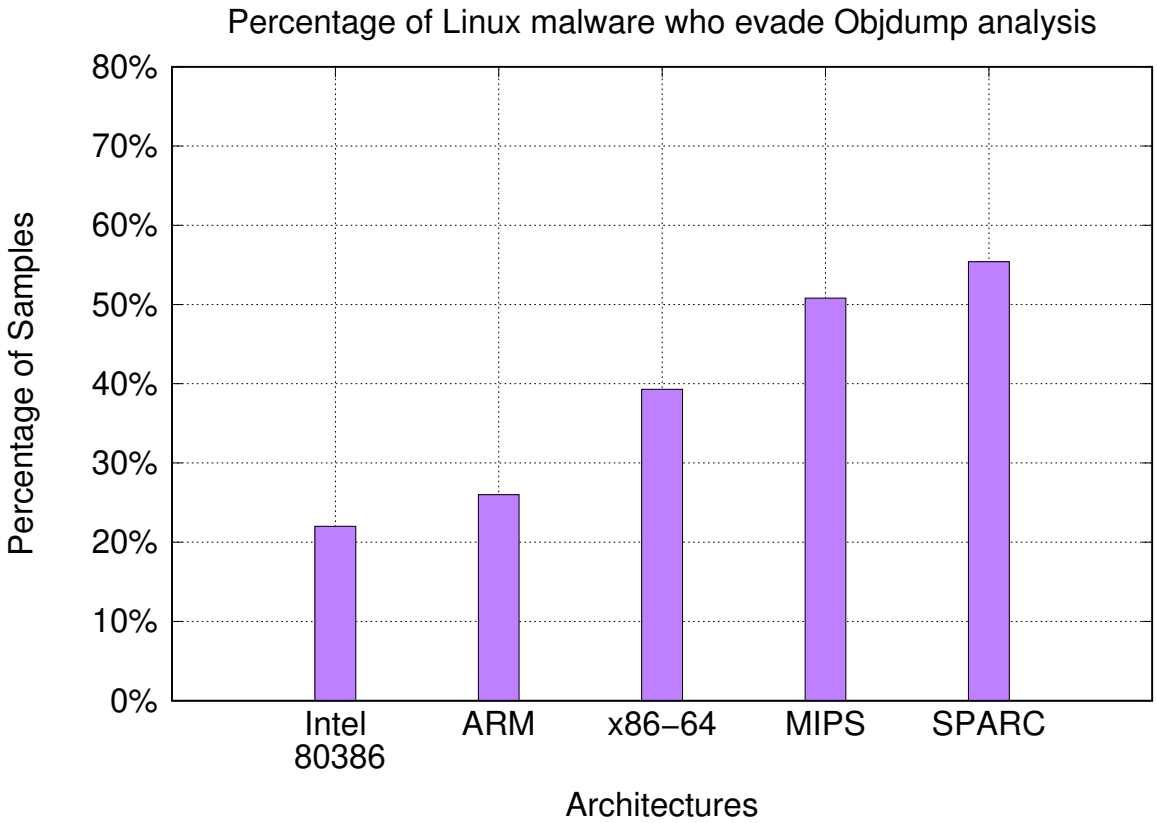

Figure: Percentage of malware that failed to dissasembly.

Static Functions

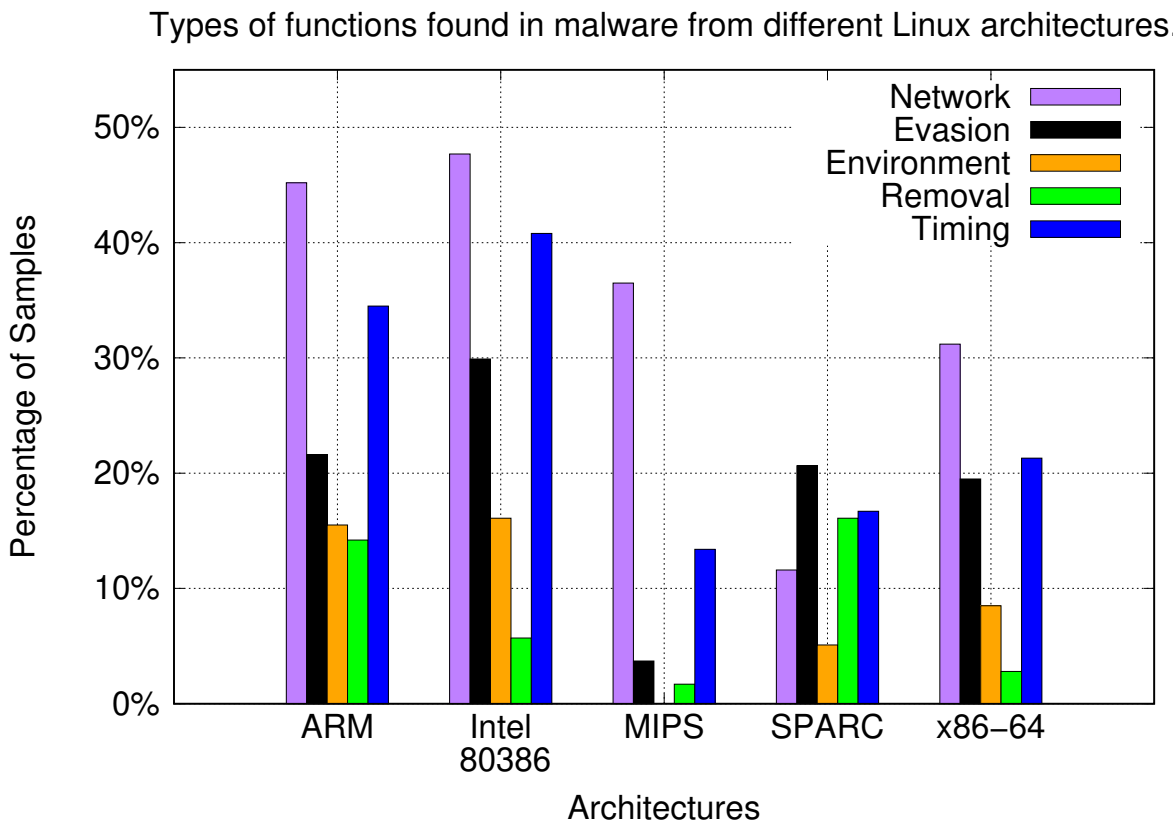

Figure: Malware behavior prevalence by malware architectures.

Network Strings

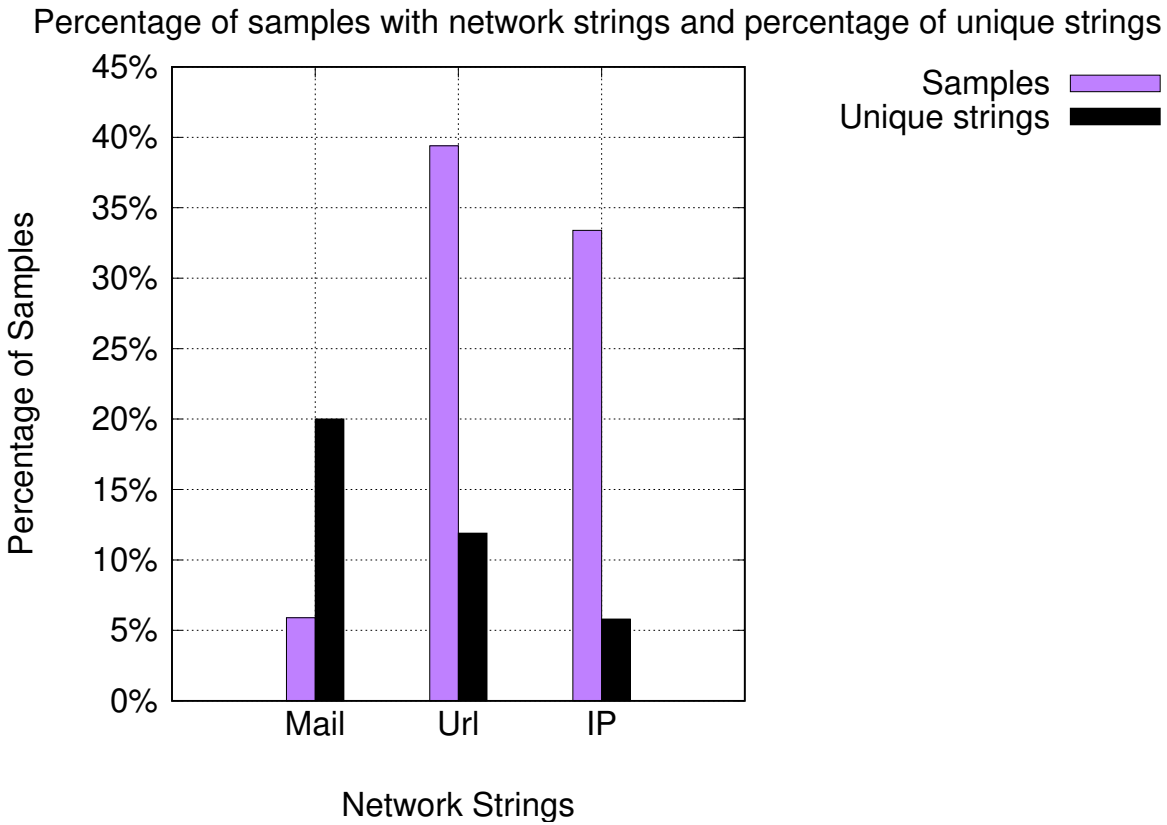

Figure: Network-Related Strings. Rate of samples with network related strings.

Packer

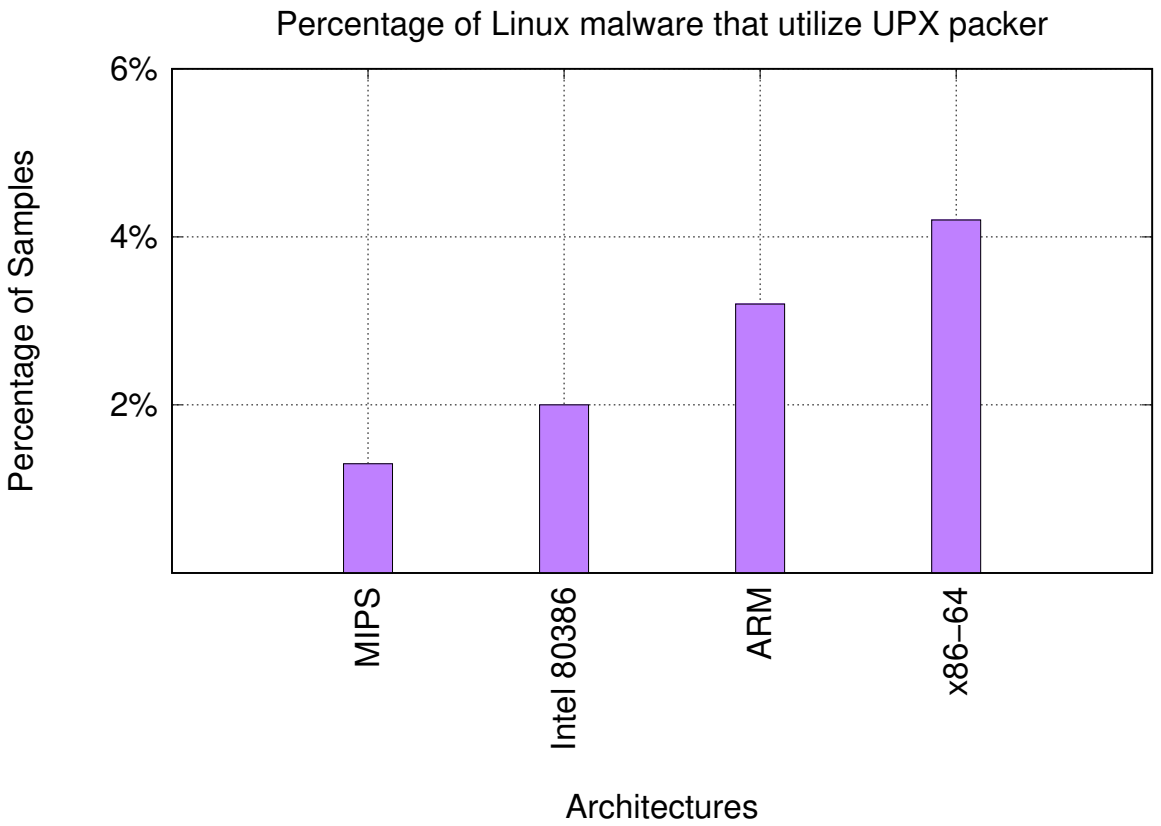

Figure: Rate of UPX-packed samples. Few samples are packed.

AV Labels

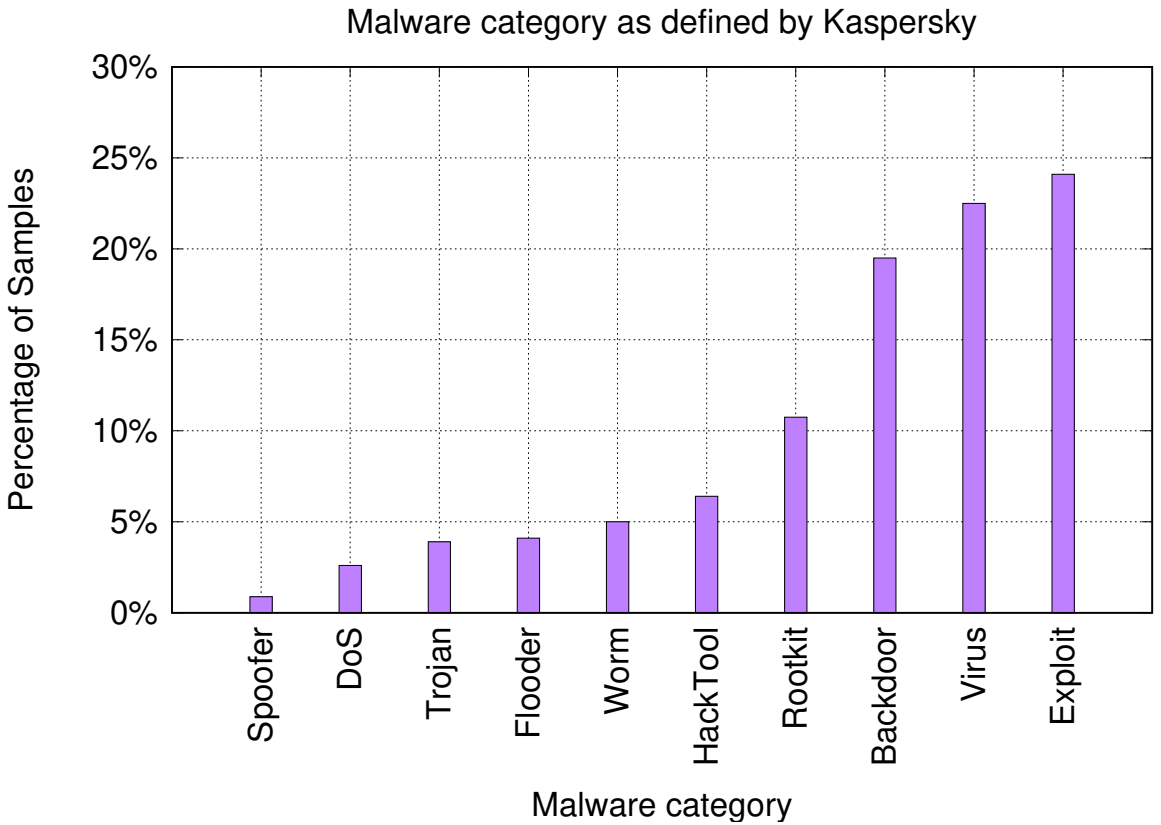

Figure: AV labels according Kaspersky AV. We observe a prevalence of exploits

Clusters

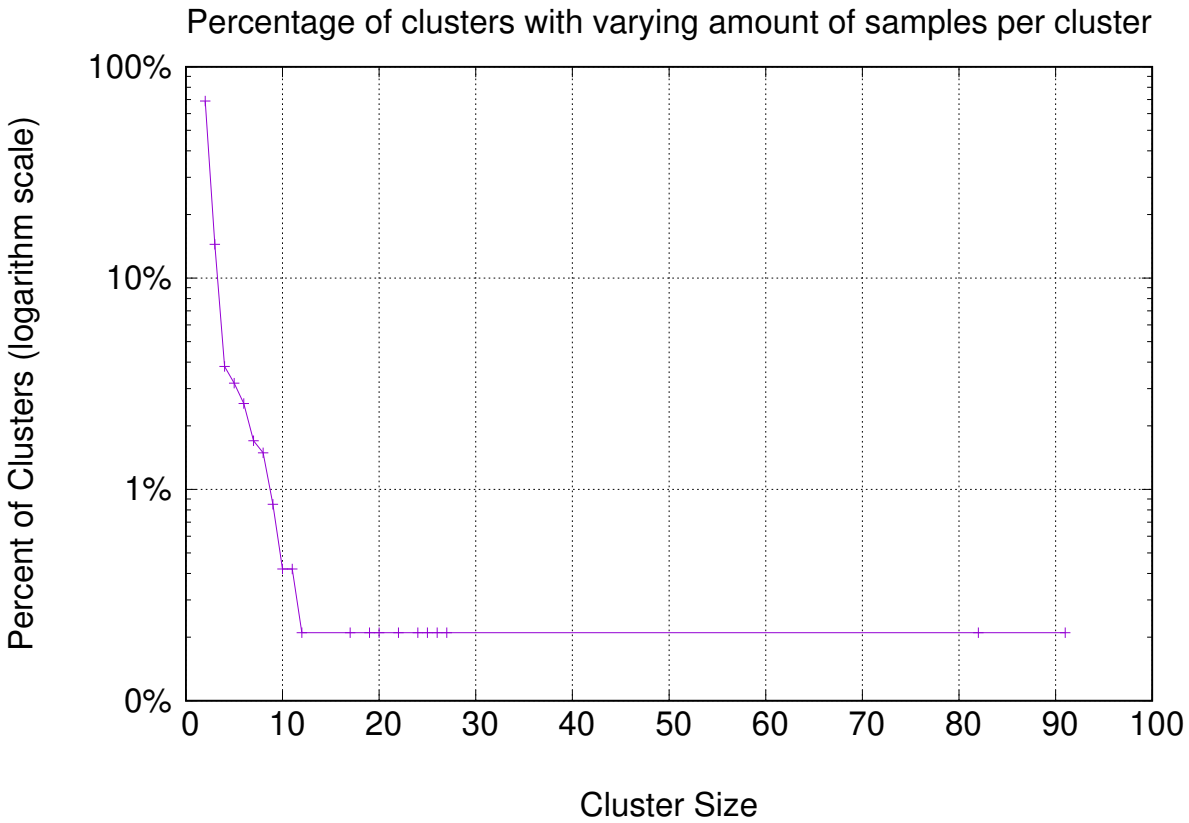

Figure: Samples variants clustering. Smaller clusters are prevalent.

Agenda

Timeout Signals

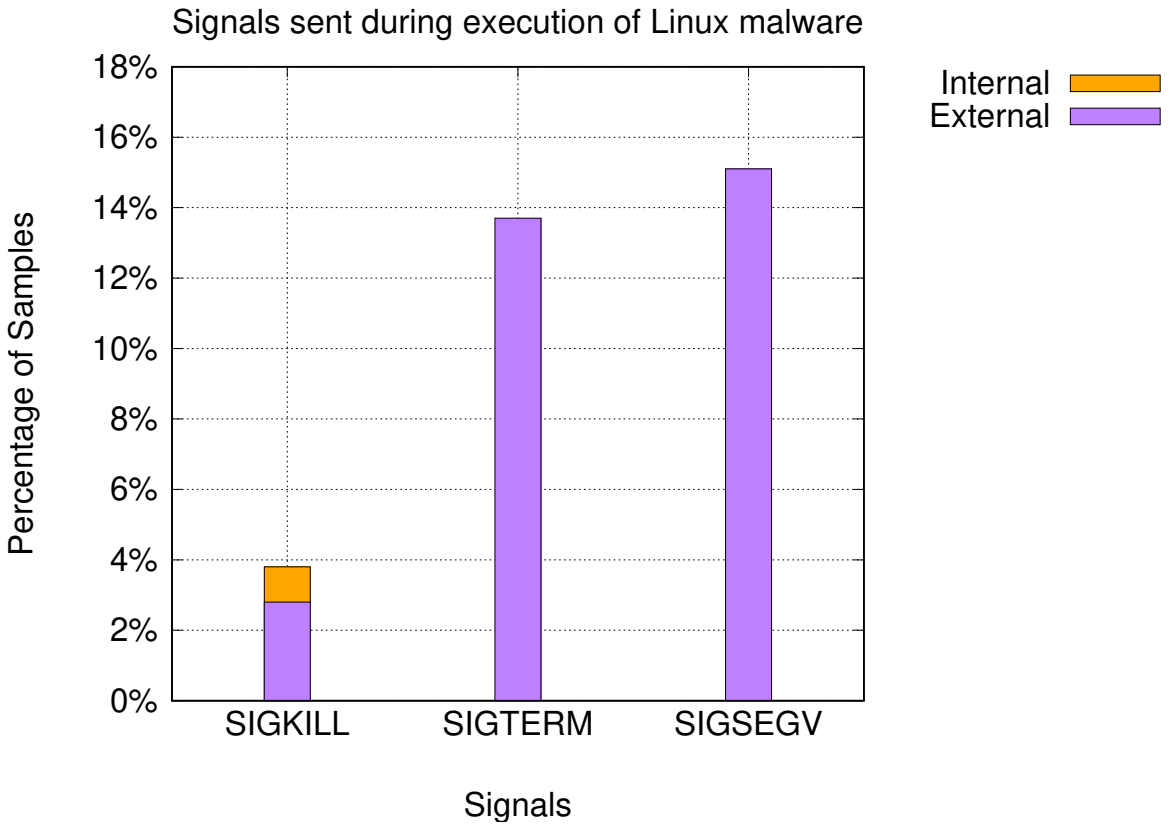

Figure: Observed Signals during execution.

Behavior

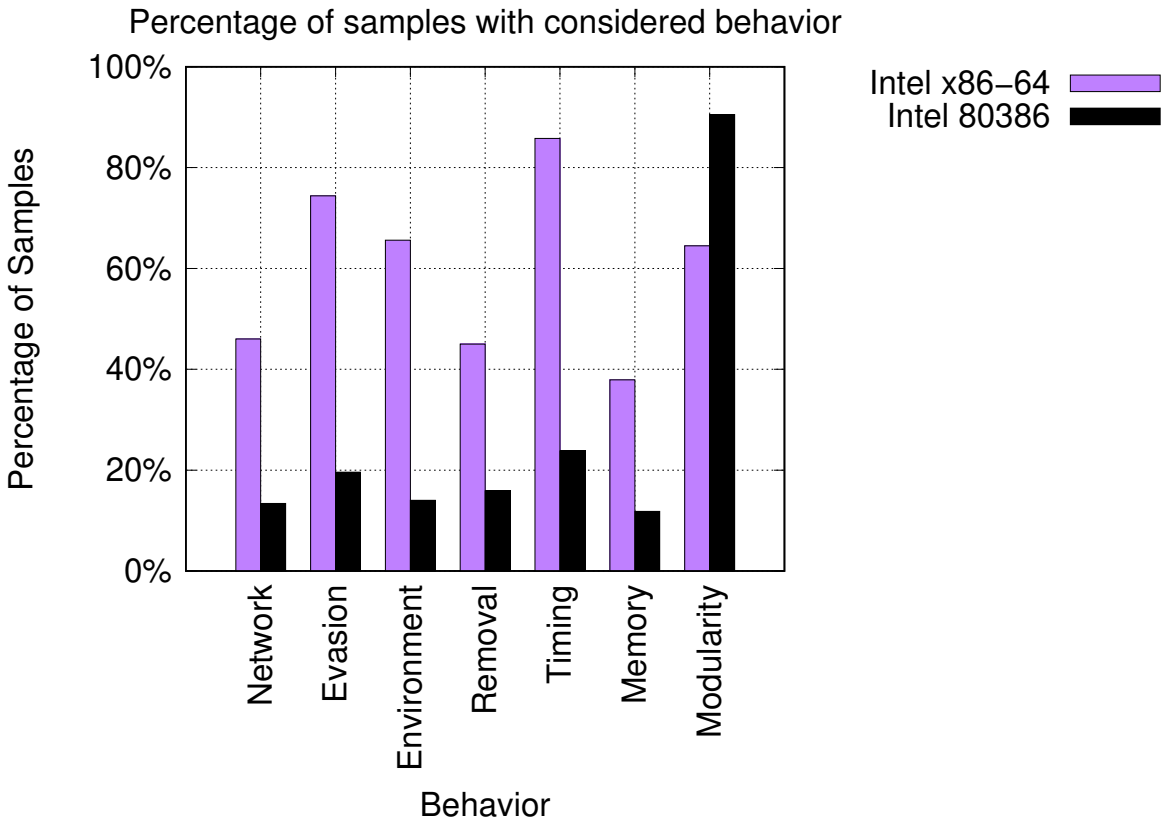

Figure: Malware behavior prevalence.

Acessed Files

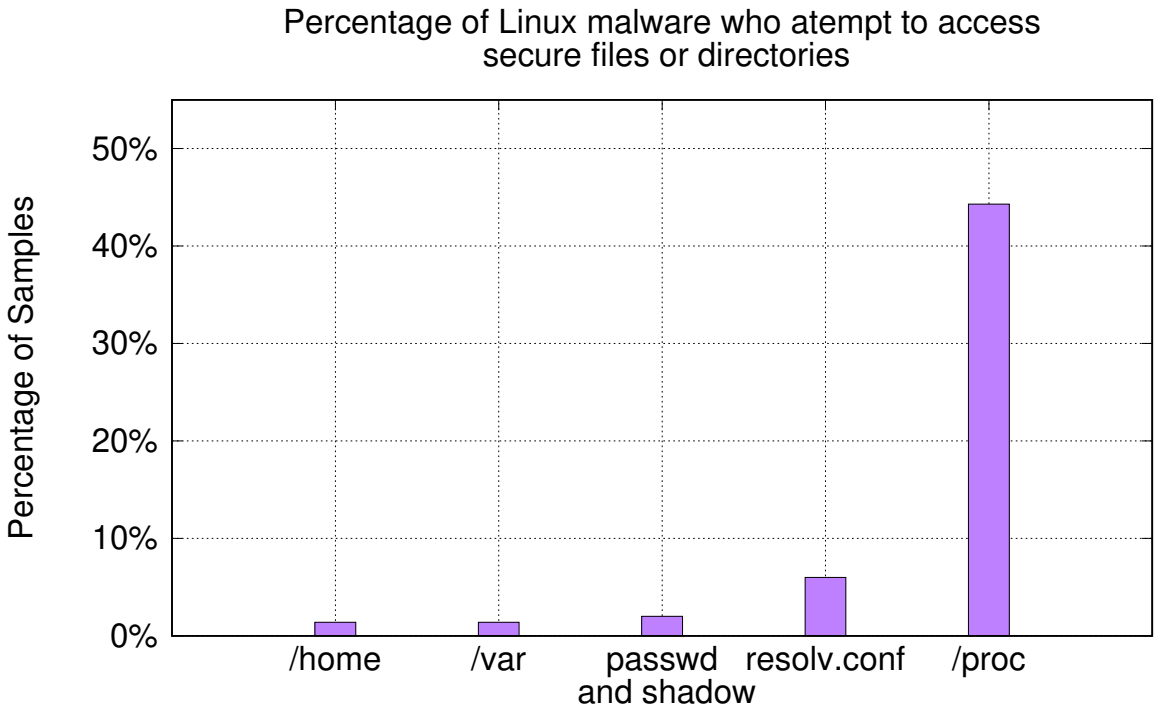

Figure: Accessed files and directories.

I/O Operations

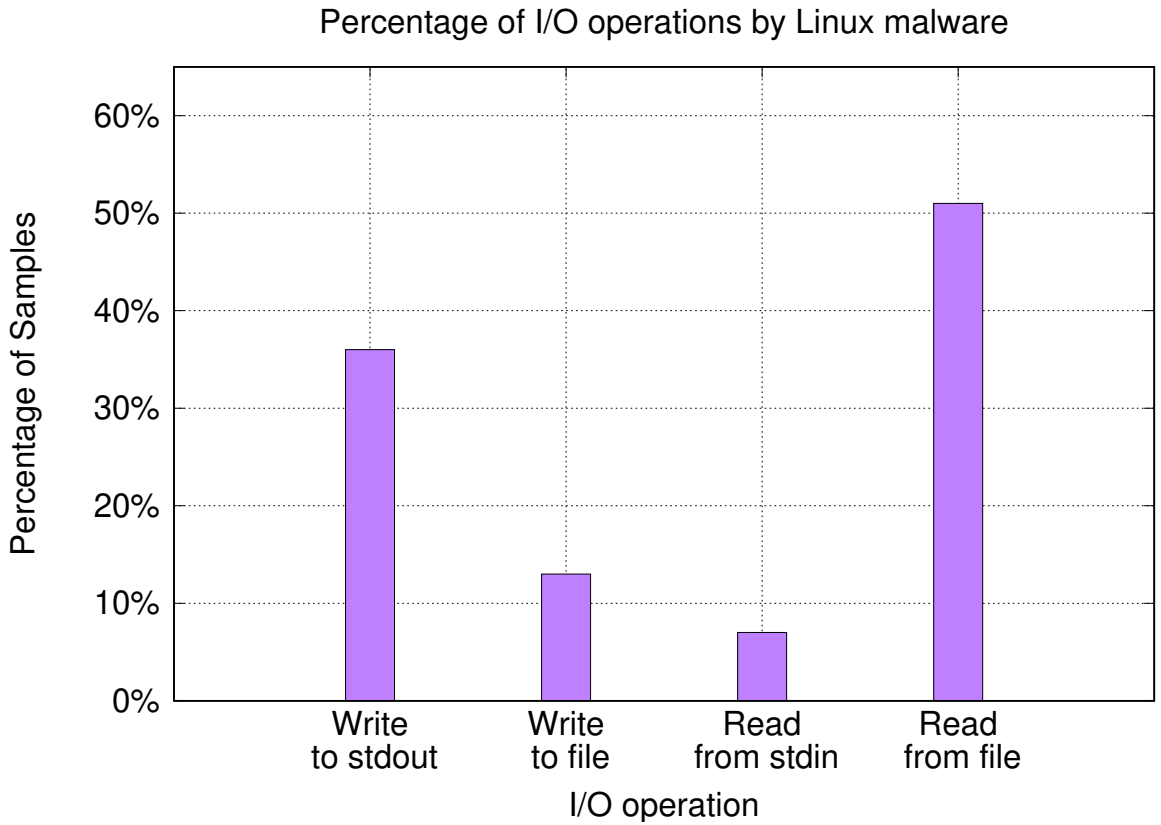

Figure: I/O operations. Most samples do not present direct user interaction.

Evasion

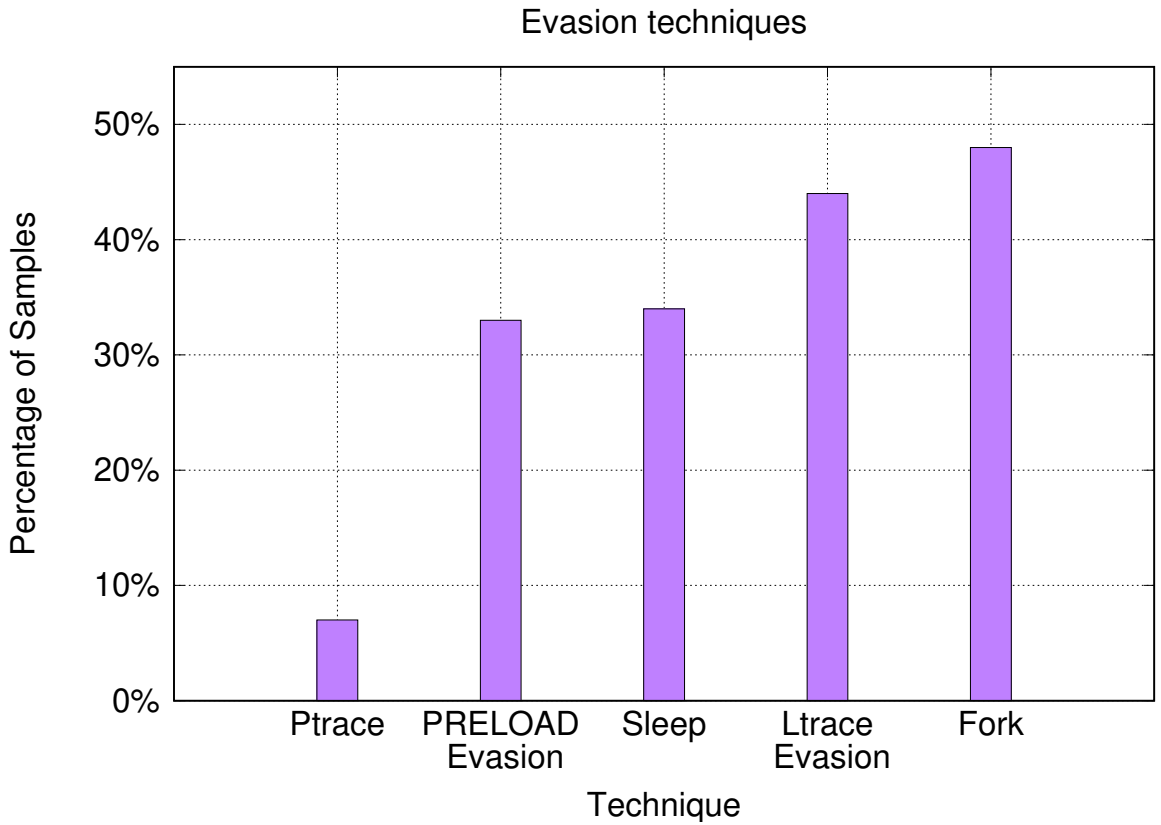

Figure: Evasion Techniques. Samples present diversified evasion methods.

Network

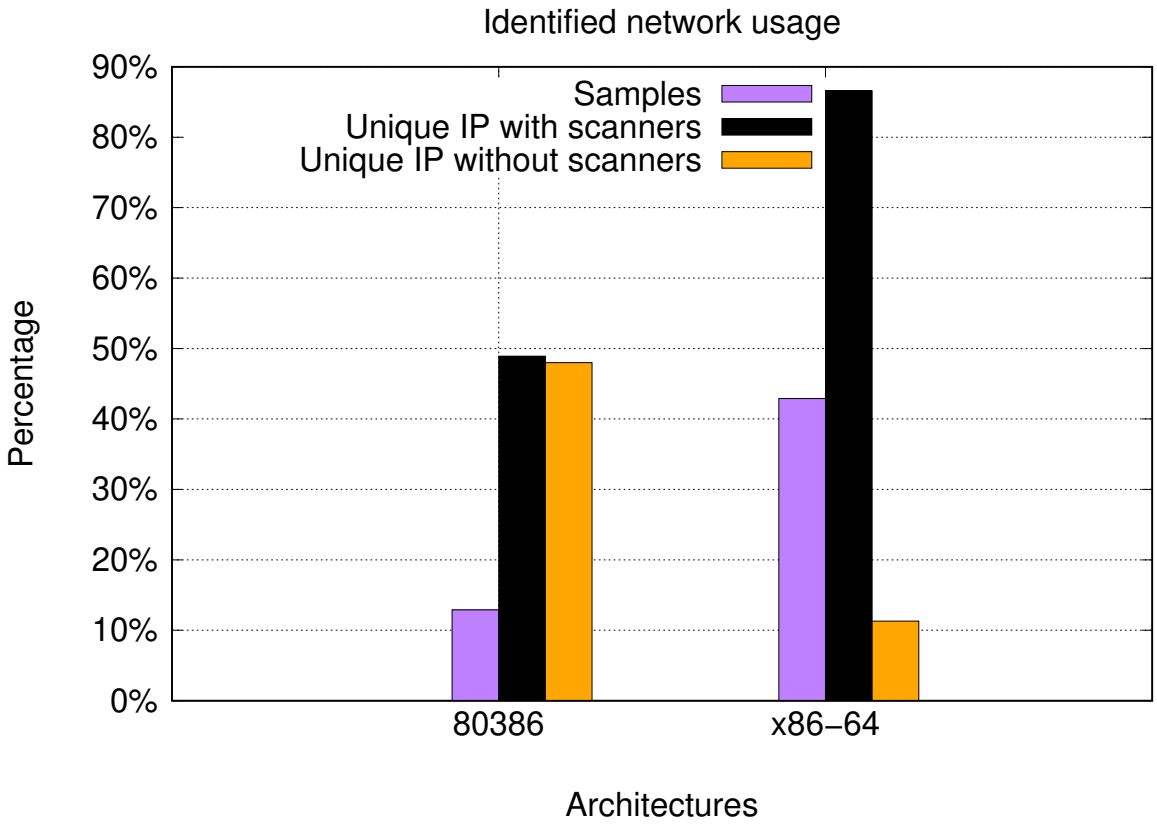

Figure: Identified network usage. Scanners dominate unique IP rate.

Domains

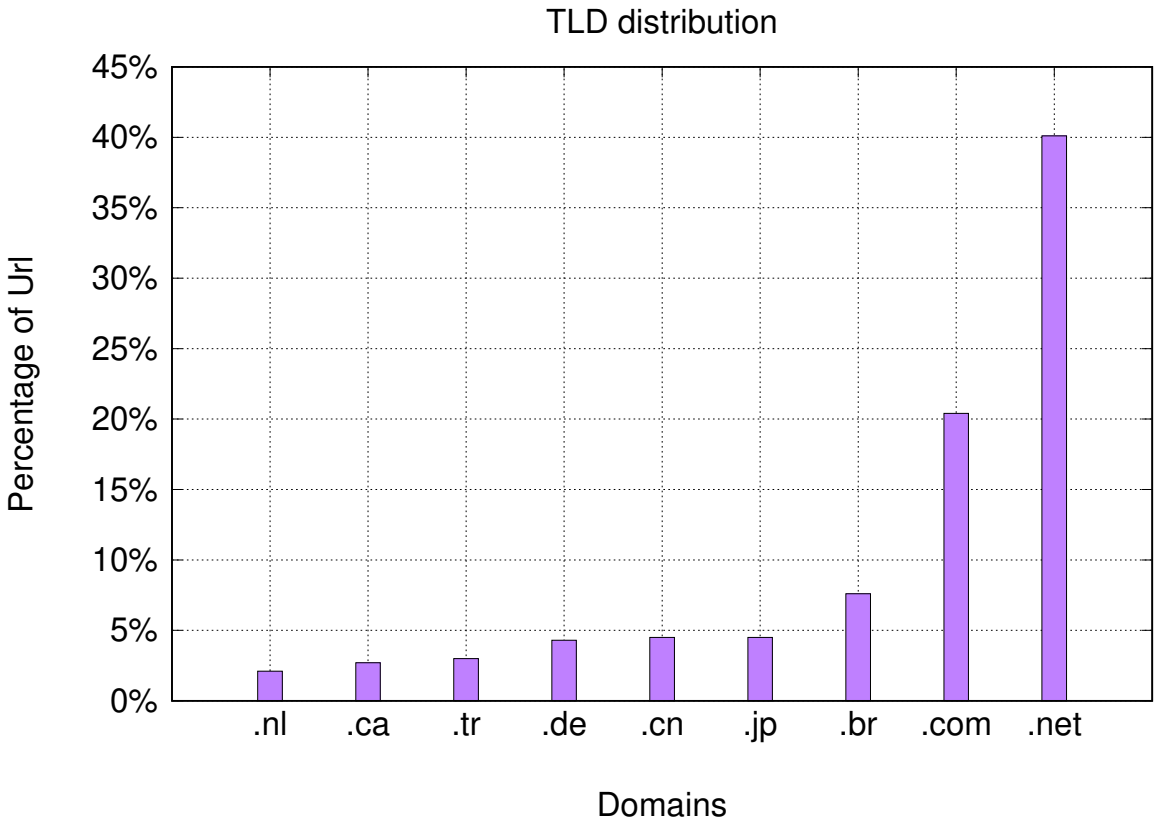

Figure: TLD distribution. Global domains are prevalent. Local domains are present due to scanners enumeration.

Agenda

SSH Backdoor

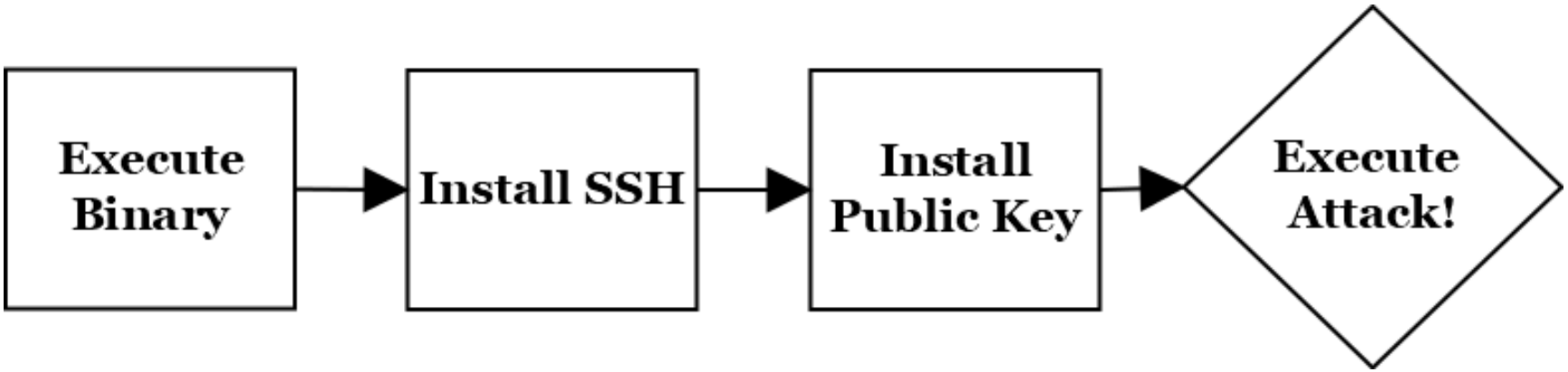

Figure: Execution flow of backdoor malware with SSH injection.

SSH Backdoor

Listing 1: Backdoor sample in action. It drops attacker key into the system, thus granting remote access.

```
1 malloc(381) = 0x2083c60
2 strlen("PPK\016QPB\003bbbba\020mYB‘\022Z@\021
      fbbbbgbrba"...)
3 strcat("", "ssh-rsa  AAAAB3NzaC1yc2EAAAADAQAB"...)
```

Erebus

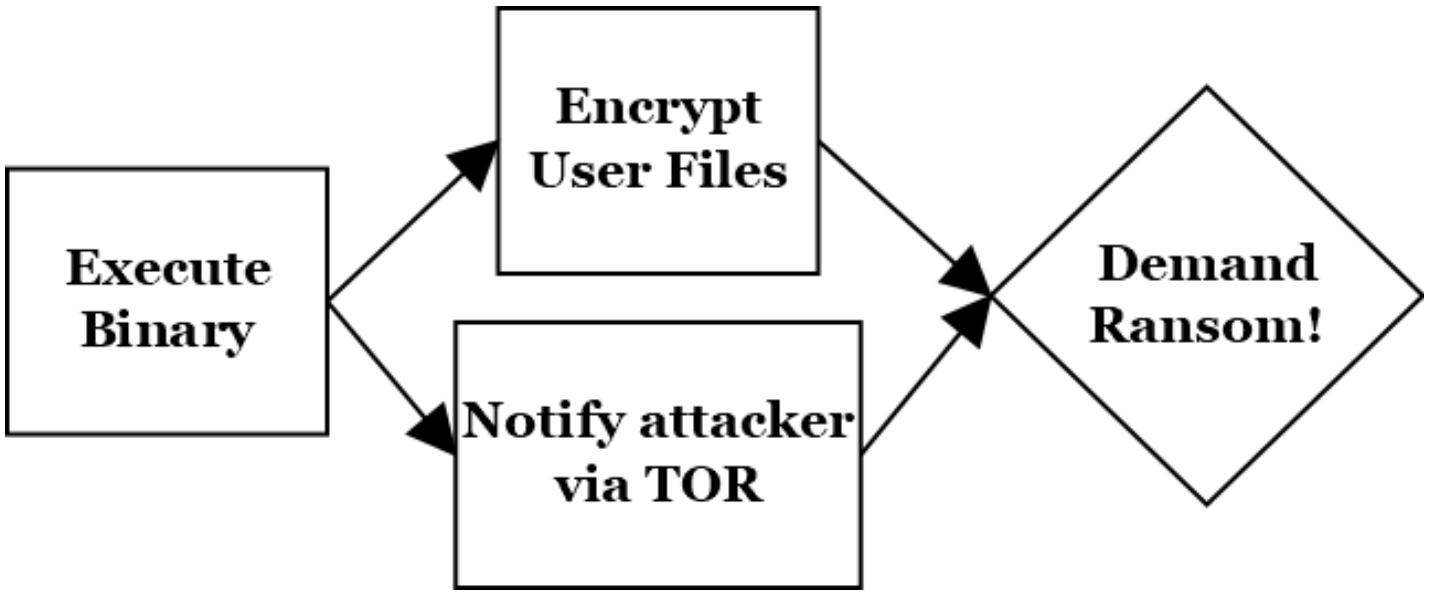

Figure: Execution flow of Erebus ransomware.

Erebus

Listing 2: Erebus Execution. It connects to runtime-generated IP addresses and to TOR-based hidden services and onion domains.

```
1 strncmp(""------BEGIN PUBLIC KEY------\\nMII"..., "
    null", 4)
2 strncmp("3,"tg":"216.126.224.128\\/24","bu"..., "
    null", 4)
3 strncmp(""7fv4vg4n26cxleel.hiddenservice."..., "
    null", 4)
4 strncmp(""qzjordhlw5mqhcn7.onion.to","qzj"..., "
    true", 4)
```

Agenda

Conclusion

- The threat of Linux malware is real.
- Ability to infect multiple systems.
- High use of network.
- Diverse evasion techniques.

Questions, Critics and Sugestions.

Contact

- **galante@lasca.ic.unicamp.br**

Complete version

- `https://github.com/marcusbotacin/Linux.Malware`