

Malicious Linux Binaries: A Landscape

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

SBSEG 2018

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

Are there Linux malware?

The screenshot shows the Trend Micro website. The header includes the Trend Micro logo, navigation links (Business, For Home), and user options (BUY, DOWNLOAD, LOGIN). The main navigation bar lists Products & Solutions, IoT Security, Intelligence, Support, Partners, About, and Contact. Below this is a breadcrumb trail: Security News > Cyber Attacks > Erebus Linux Ransomware: Impact to Servers and Countermeasures. The article title is 'Erebus Linux Ransomware: Impact to Servers and Countermeasures', dated June 15, 2017. The article text states that on June 10, NAYANA, a South Korea-based web hosting company, became a victim of ransomware. The ransomware was detected by Trend Micro as RANSOM_ELFEREBUS.A. The attack affected websites, databases, and multimedia files of approximately 3,400 businesses. A notice on the company's website mentioned that cybercriminals had successfully forced NAYANA to pay the ransom. A related post section on the right lists several other cybersecurity topics.

TREND MICRO Business For Home >

BUY DOWNLOAD LOGIN

Products & Solutions IoT Security Intelligence Support Partners About Contact

Security News > Cyber Attacks > Erebus Linux Ransomware: Impact to Servers and Countermeasures

Erebus Linux Ransomware: Impact to Servers and Countermeasures

June 15, 2017

On June 10, South Korea-based web hosting company **NAYANA** became one of the latest high-profile victims of **ransomware** after 153 of its Linux servers were **found** infected with an Erebus ransomware (detected by Trend Micro as RANSOM_ELFEREBUS.A) variant. The ransomware attack affected the websites, database and multimedia files of around 3,400 businesses employing NAYANA's service.

In the latest **notice** posted on the company's website, it appears cybercriminals successfully forced NAYANA into paying the ransom—they paid the first of three payments they plan to make for all the keys needed to decrypt the infected files. However, NAYANA has yet to receive the first decryption key.

[Related: [Learn more about SAMSAM, one of the first ransomware to infect servers](#)]

Erebus evolved from using exploit kits to bypassing User

Related Posts

- Bridging Cybersecurity Gaps with Managed Detection and Response
- New Multi-Platform Xbash Packs
- Obfuscation, Ransomware, Comminer, Worm and Botnet
- Unseen Threats, Imminent Losses
- .EGG Files in Spam Delivers
- GandCrab v4.3 Ransomware to South Korean Users
- Jigsaw Ransomware Resurfaces as Bitcoin Stealer

Figure: Erebus ransomware attacks South Korean internet provider.

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

Binaries Architectures

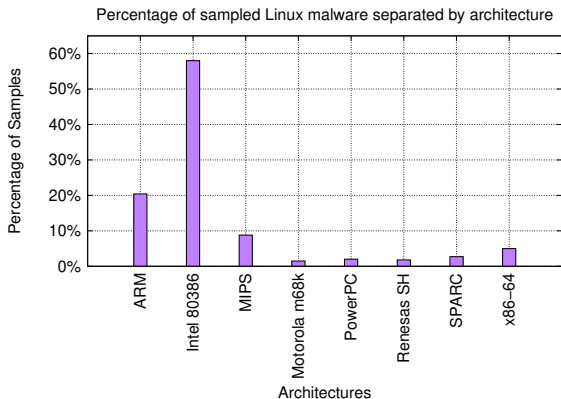


Figure: ELF binary samples distributed by architectures.

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

Analysis Techniques

Table: Adopted strategy to handle evasive samples.

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

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

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

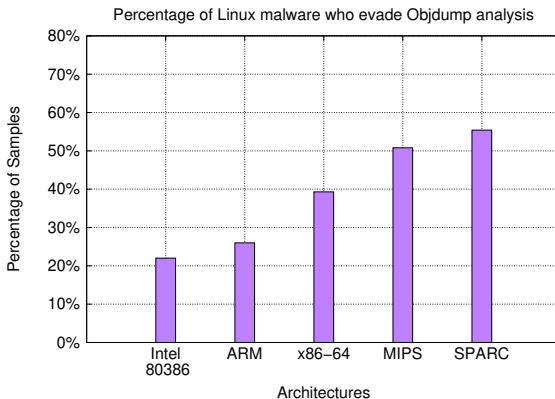


Figure: Percentage of malware that failed to dissassembly.

Static Functions

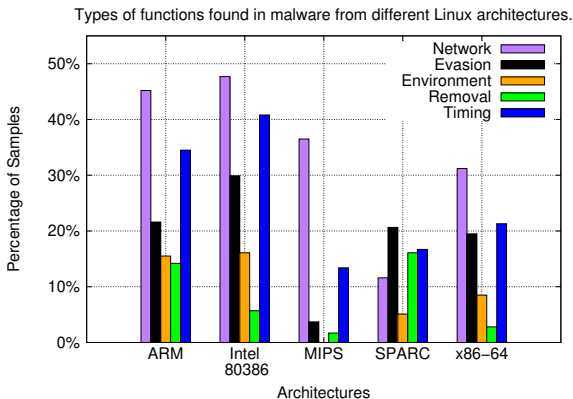


Figure: Malware behavior prevalence by malware architectures.

Network Strings

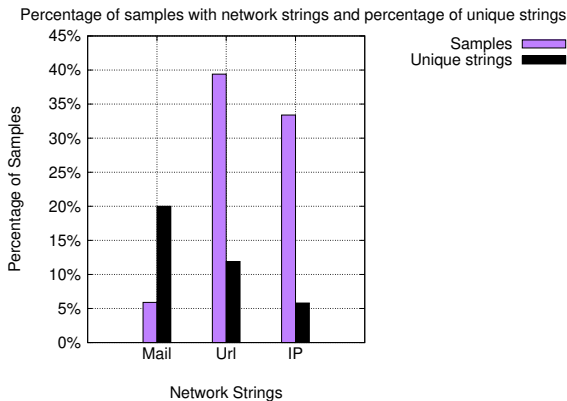


Figure: Network-Related Strings. Rate of samples with network related strings.

Packer

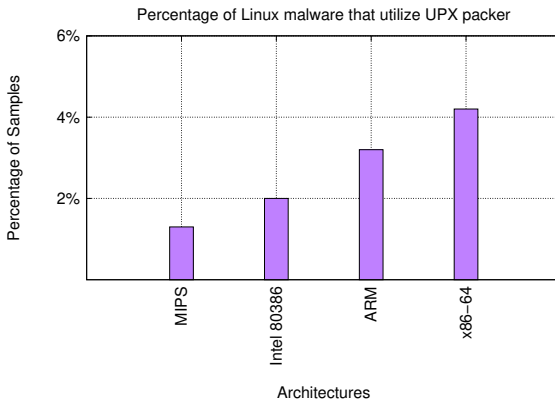


Figure: Rate of UPX-packed samples. Few samples are packed.

AV Labels

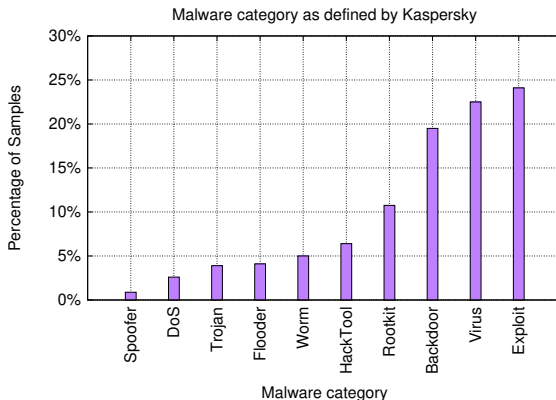


Figure: AV labels according Kaspersky AV. We observe a prevalence of exploits

Clusters

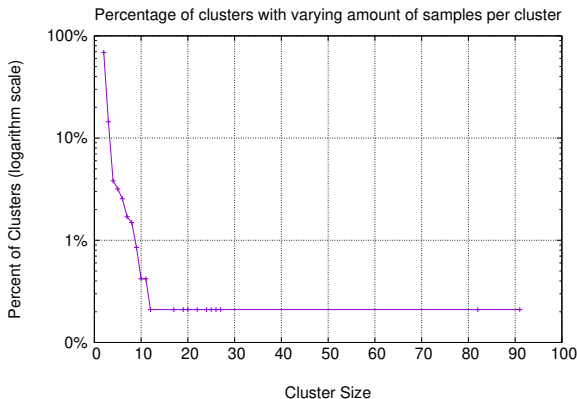


Figure: Samples variants clustering. Smaller clusters are prevalent.

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - **Dynamic Analysis**
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

Timeout Signals

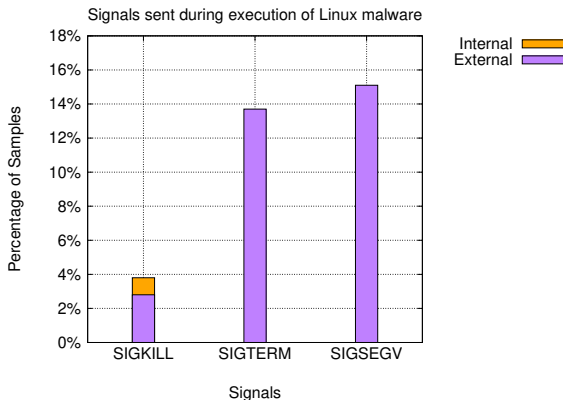


Figure: Observed Signals during execution.

Behavior

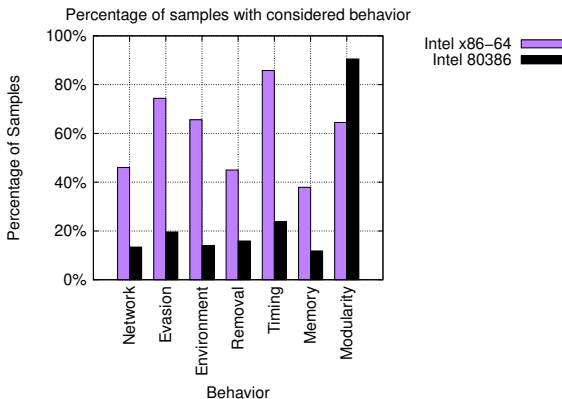


Figure: Malware behavior prevalence.

Accessed Files

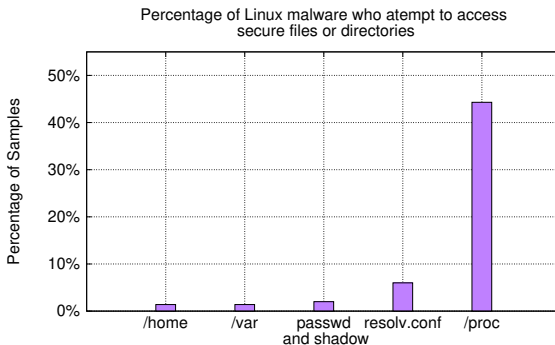


Figure: Accessed files and directories.

I/O Operations

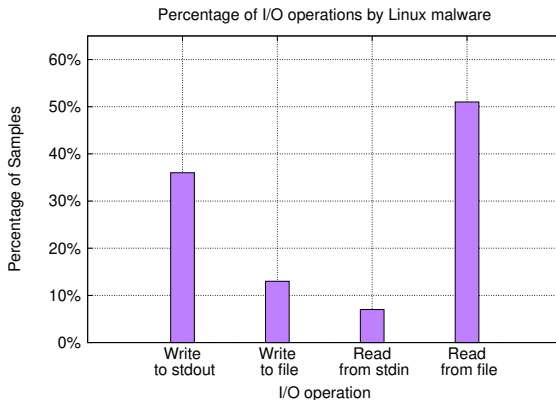


Figure: I/O operations. Most samples do not present direct user interaction.

Evasion

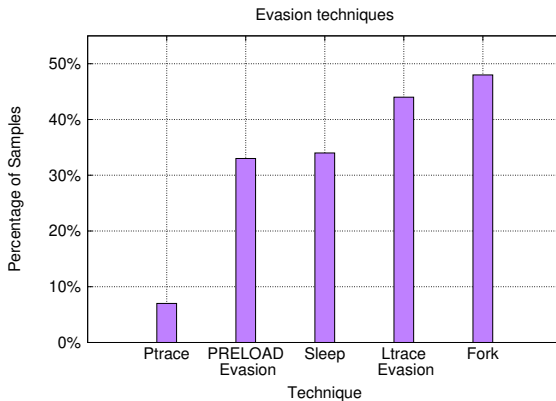


Figure: Evasion Techniques. Samples present diversified evasion methods.

Network

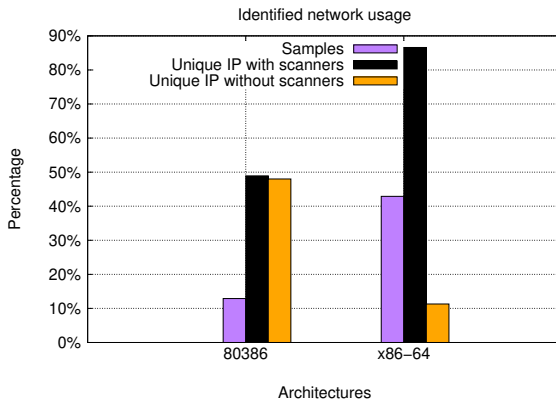


Figure: Identified network usage. Scanners dominate unique IP rate.

Domains

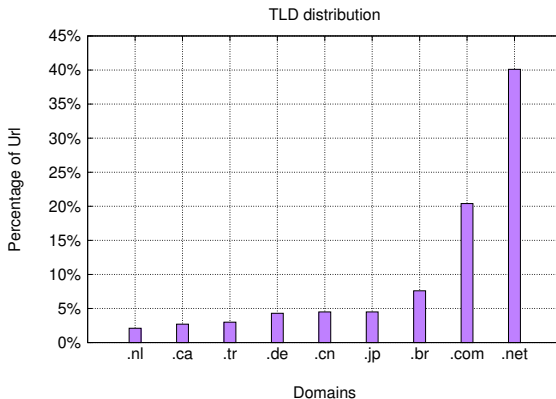


Figure: TLD distribution. Global domains are prevalent. Local domains are present due to scanners enumeration.

Agenda

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

SSH Backdoor

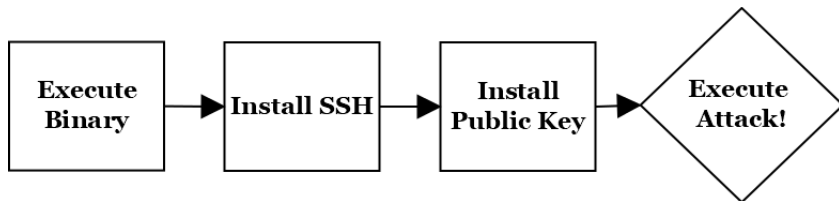


Figure: Execution flow of backdoor malware with SSH injection.

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\003bbbbba\020mYB'\022Z@\021
   fbbbbgbrba"... )
3 strcat("", "ssh-rsa AAAAB3NzaC1yc2EAAAADAQAB"...)
```

Erebus

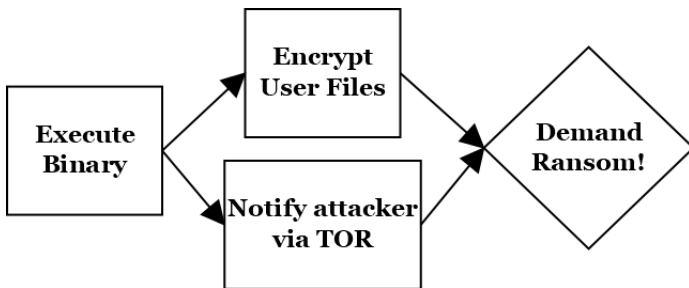


Figure: Execution flow of Erebus ransomware.

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

- 1 Motivation
 - Motivation
- 2 Dataset Description
 - Dataset Description
- 3 Methodology
 - Methodology
- 4 Analysis
 - Static Analysis
 - Dynamic Analysis
- 5 Case Studies
 - Case Studies
- 6 Conclusion
 - Conclusion

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>