

Keylogger detector

Michel Romancuk, Sebastian Lenzlinger

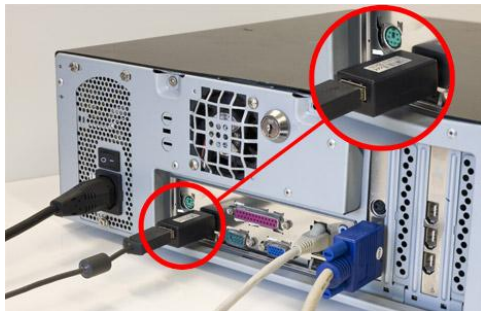
Topics

- What is a keylogger
- Our focus: Software Based Keylogger
 - Kernel based
 - API based
- Detecting keyloggers

what is a keylogger

a computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information

— — —



Hardware based

```
[root@fedora by-path]# pwd
/dev/input/by-path
[root@fedora by-path]# ll
total 0
lrwxrwxrwx. 1 root root 10 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.3:1.0-event-kbd -> ../event23
lrwxrwxrwx. 1 root root 10 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.3:1.1-event -> ../event26
lrwxrwxrwx. 1 root root 10 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.3:1.1-event-mouse -> ../event24
lrwxrwxrwx. 1 root root 9 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.3:1.1-mouse -> ../mouse4
lrwxrwxrwx. 1 root root 10 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.4:1.0-event-mouse -> ../event27
lrwxrwxrwx. 1 root root 9 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.4:1.0-mouse -> ../mouse5
lrwxrwxrwx. 1 root root 10 Apr 12 21:18 pci-0000:00:14.0-usb-0:3.4.4:1.1-event-kbd -> ../event28
lrwxrwxrwx. 1 root root 10 Apr 10 10:16 pci-0000:00:14.0-usb-0:8:1.0-event -> ../event11
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 pci-0000:00:15.0-platform-i2c_designware.0-event-mouse -> ../event7
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 pci-0000:00:15.0-platform-i2c_designware.0-mouse -> ../mouse2
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 platform-i8042-serio-0-event-kbd -> ../event4
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 platform-i8042-serio-1-event-mouse -> ../event5
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 platform-i8042-serio-1-mouse -> ../mouse0
lrwxrwxrwx. 1 root root 9 Apr 10 10:16 platform-INTC1051:00-event -> ../event9
lrwxrwxrwx. 1 root root 10 Apr 10 10:16 platform-pcspkr-event-spkr -> ../event10
```

Software based

- Keyloggers are not per se malicious.
- Your apps need to access Keyboard I/O too.
- It is malware when you're not aware of it, and if it is deployed with malintent.

Software Keyloggers

— — —

- Hypervisor Based
- Kernel Based
- API Based
- Various Script Injections in Userland

→ <https://github.com/cvc0rpion/micKeyDetector>, <https://github.com/kernc/logkeys>
countless others, especially Python API Based Keystroke loggers on Github.

Kernel Based:

- Logger obtains root access and hides in OS
- Intercepts Keystrokes passing through the Kernel

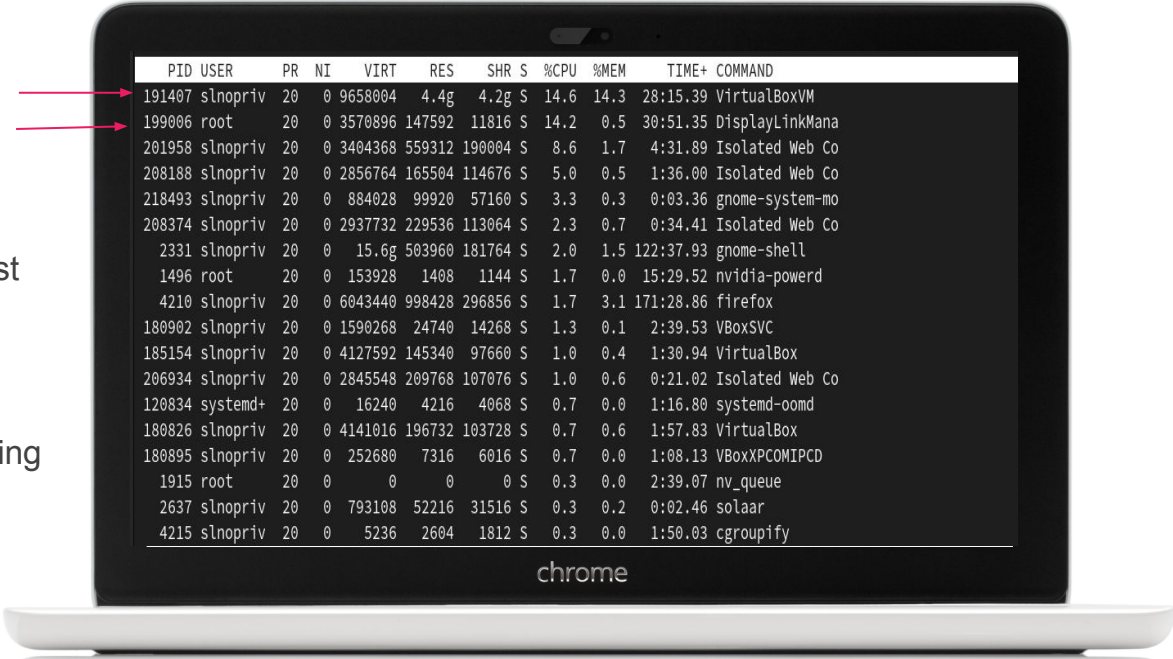
How do you detect a keylogger?

Aren't I/O Ops ubiquitous and plentiful?

Detection

That's a
lot of
processes

- Just wade through processes...
- Use list of known loggers → ok I'll just rename mine, thanks
- Signature Based
- Behavioural Analysis
- Main problem: what is good I/O reading behaviour, what not?



PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
191407	slnopriv	20	0	9658004	4.4g	4.2g	S	14.6	14.3	28:15.39	VirtualBoxVM
199006	root	20	0	3570896	147592	11816	S	14.2	0.5	30:51.35	DisplayLinkMana
201958	slnopriv	20	0	3404368	559312	190004	S	8.6	1.7	4:31.89	Isolated Web Co
208188	slnopriv	20	0	2856764	165504	114676	S	5.0	0.5	1:36.00	Isolated Web Co
218493	slnopriv	20	0	884028	99920	57160	S	3.3	0.3	0:03.36	gnome-system-mo
208374	slnopriv	20	0	2937732	229536	113064	S	2.3	0.7	0:34.41	Isolated Web Co
2331	slnopriv	20	0	15.6g	503960	181764	S	2.0	1.5	122:37.93	gnome-shell
1496	root	20	0	153928	1408	1144	S	1.7	0.0	15:29.52	nvidia-powerd
4210	slnopriv	20	0	6043440	998428	296856	S	1.7	3.1	171:28.86	firefox
180902	slnopriv	20	0	1590268	24740	14268	S	1.3	0.1	2:39.53	VBoxSVC
185154	slnopriv	20	0	4127592	145340	97660	S	1.0	0.4	1:30.94	VirtualBox
206934	slnopriv	20	0	2845548	209768	107076	S	1.0	0.6	0:21.02	Isolated Web Co
120834	systemd+	20	0	16240	4216	4068	S	0.7	0.0	1:16.80	systemd-oomd
180826	slnopriv	20	0	4141016	196732	103728	S	0.7	0.6	1:57.83	VirtualBox
180895	slnopriv	20	0	252680	7316	6016	S	0.7	0.0	1:08.13	VBoxXPCOMIPCD
1915	root	20	0	0	0	0	S	0.3	0.0	2:39.07	nv_queue
2637	slnopriv	20	0	793108	52216	31516	S	0.3	0.2	0:02.46	solaar
4215	slnopriv	20	0	5236	2604	1812	S	0.3	0.0	1:50.03	cgroupify

chrome

`/*TODOs*/`

Analyze
existing
keyloggers:
what
APIs/System
calls are
done?

who is
reading
/dev/input
/*?

Find processes
involved in
reading from I/O
and display them

Env:
Fedora 37,
Gnome,
Wayland

Unclear: Is
this a
Kernel
Module or
user App?

Merci

Michel Romancuk, Sebastian Lenzlinger

Questions ?

— — —

Hier könnte ihre Werbung
stehen

