

*"If you know the enemy and know yourself you need
not fear the results of a hundred battles."*

-- Sun Tzu

./whoami

- MEng from Imperial College London in 2014
- Security Researcher @ Kaspersky Lab
- Threat Intelligence and Big Data

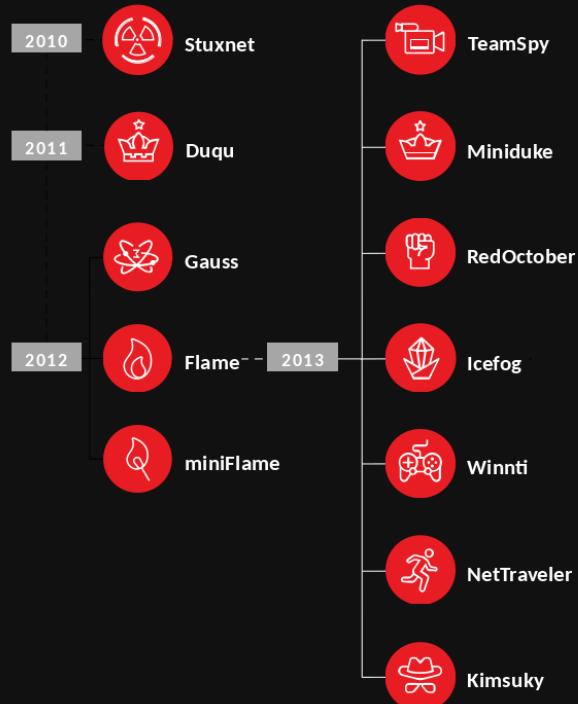
GReAT - Elite Threat Research

- Global Research and Analysis Team
- Founded 2008
- Threat intelligence, research and innovation leadership
- APTs, critical infrastructure threats, banking threats, targeted attacks, finding attacks using zero-days in popular OS'es and products

TARGETED ATTACKS

GREAT

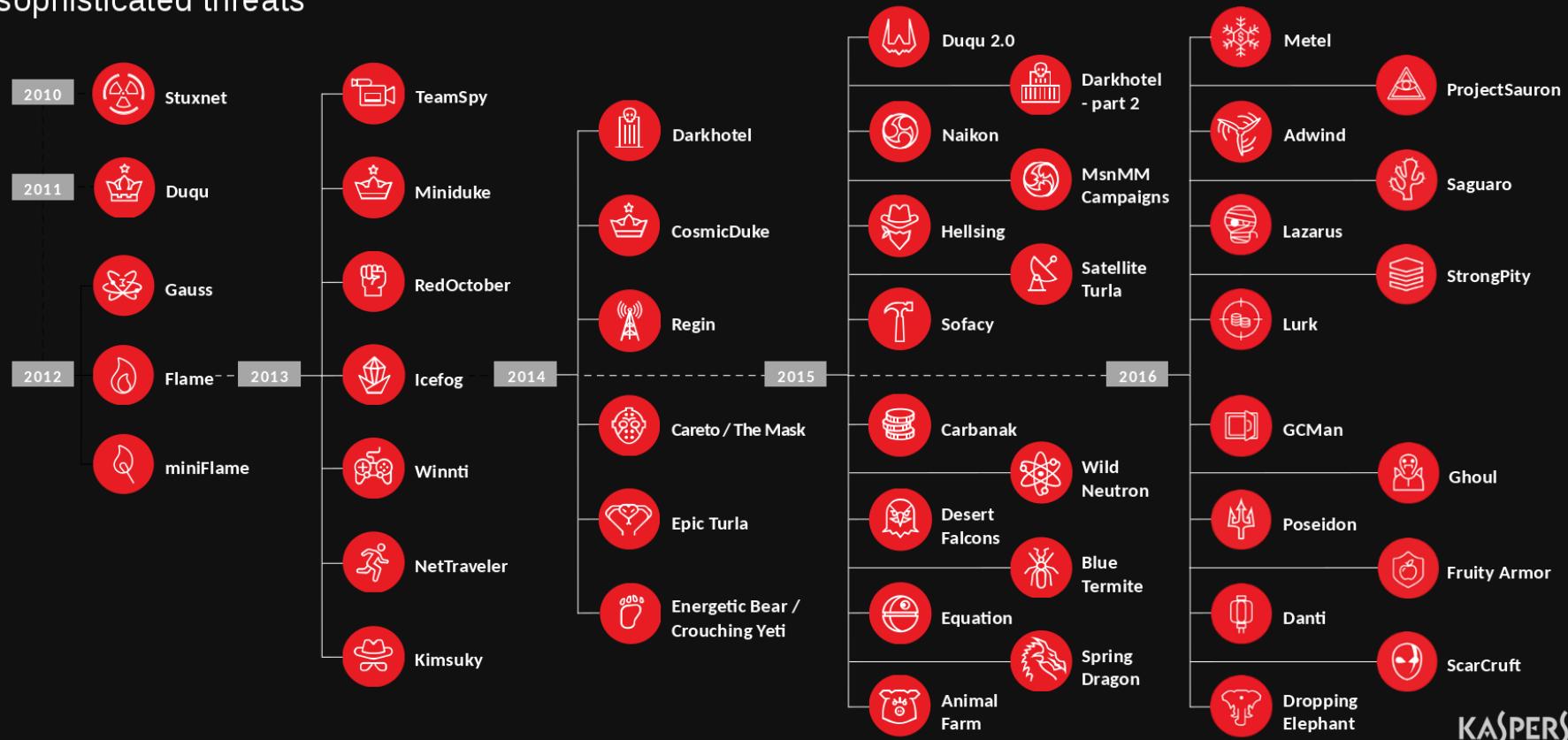
We discover and dissect the world's most sophisticated threats



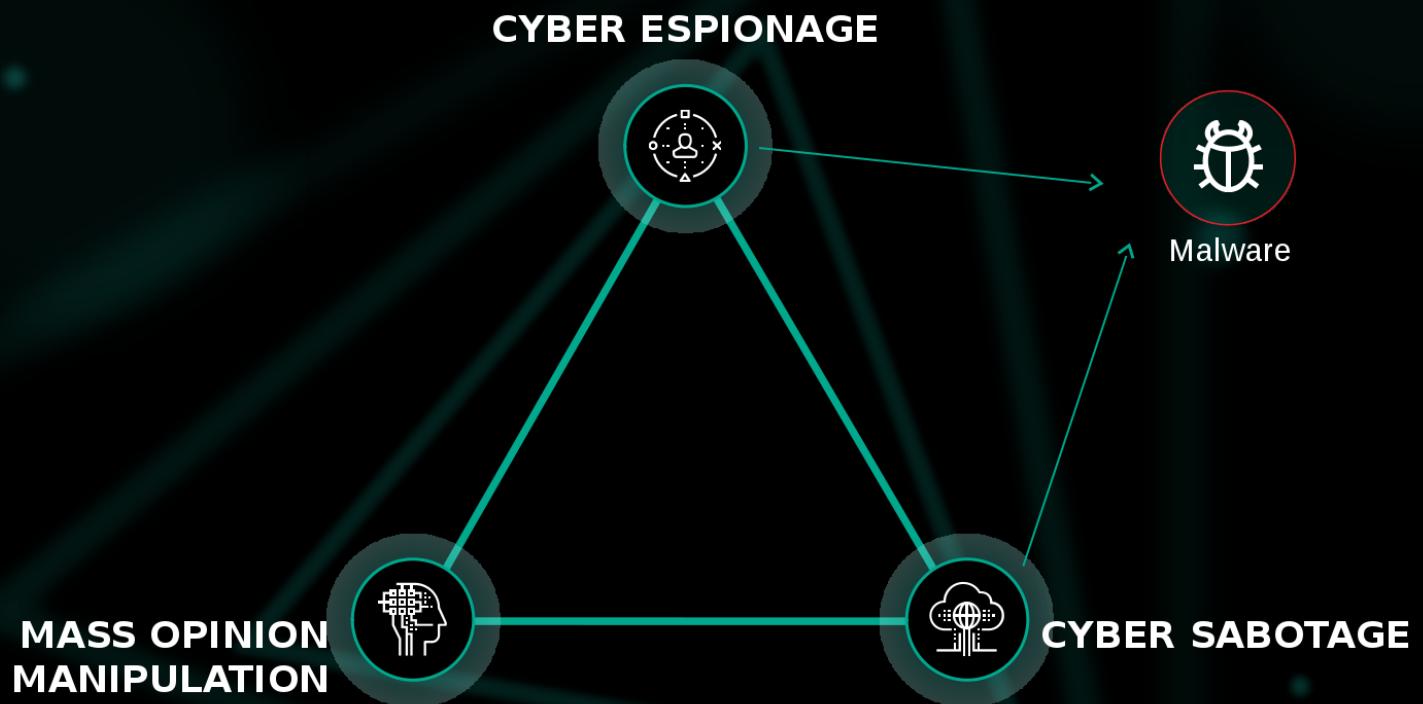
KASPERSKY

TARGETED ATTACKS

We discover and dissect the world's most sophisticated threats



The Information War



The Information War



Malware

KASPERSKY

Looks familiar?

```
rule ransomware_exPetr {
meta:
copyright      = "Kaspersky Lab"
description    = "Rule to detect PetrWrap ransomware samples"
hash          = "71B6A493388E7D0B40C83CE903BC6B04"

strings:
$a2 = ".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs."
$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CA"
$a4 = "wowsmith123456@posteo.net." fullword wide

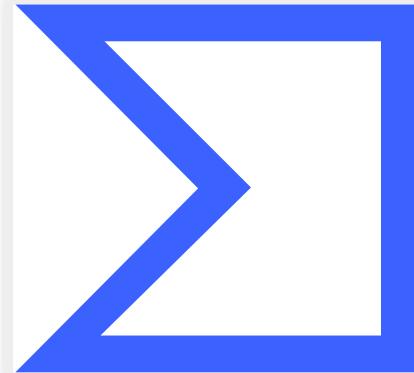
condition:
  (uint16(0) == 0x5A4D) and
  (any of them)
}
```




<https://virustotal.github.io/yara/>

A woman with blonde hair tied back, wearing a camouflage long-sleeved shirt and camouflage pants, stands in a desert environment. She is holding a bolt-action rifle with both hands, pointing it towards the right side of the frame. To her right is a dark-colored pickup truck. The background shows a vast, arid landscape under a clear blue sky.

Hunting in the wild

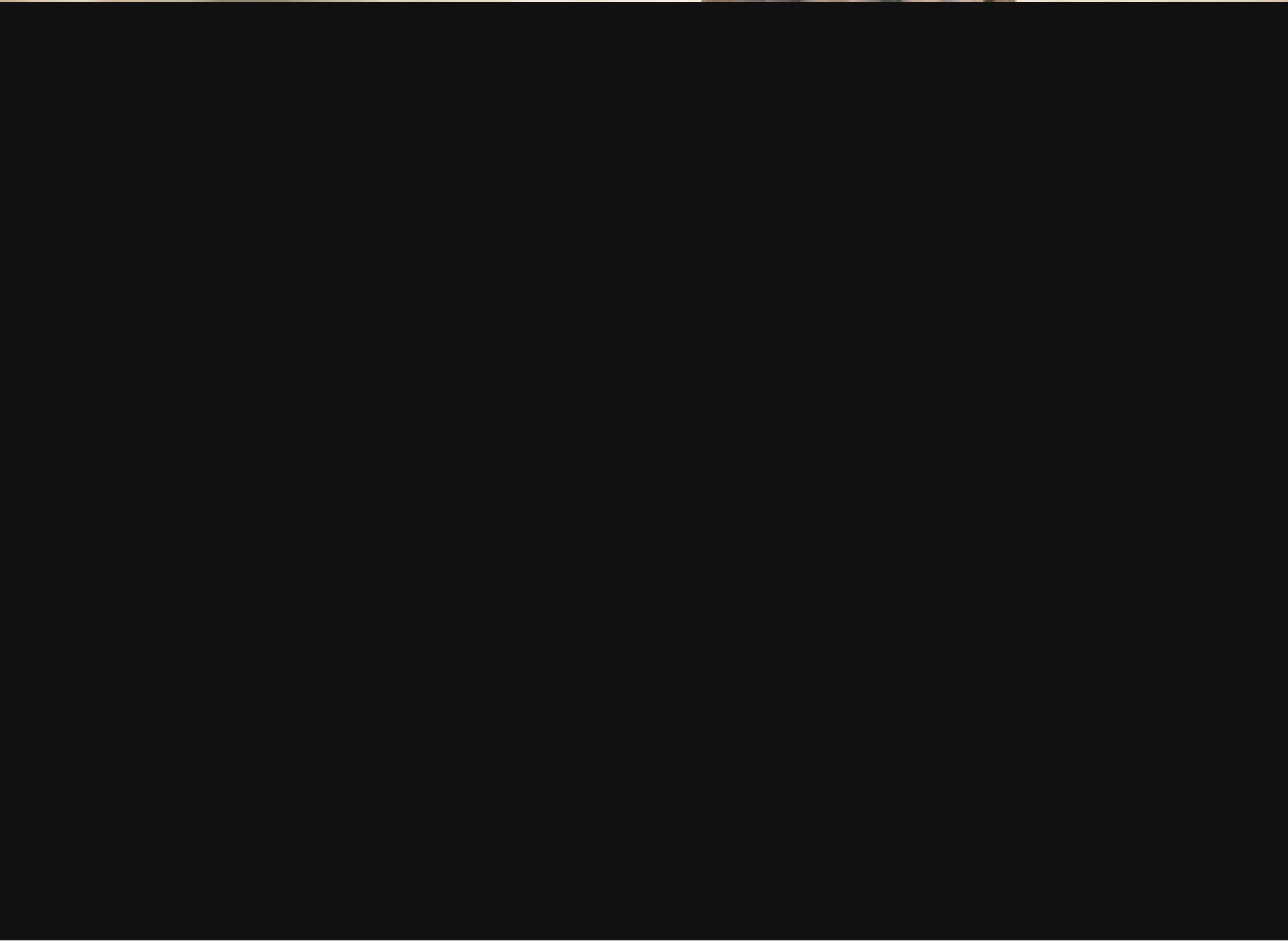


VirusTotal

<https://virustotal.com>

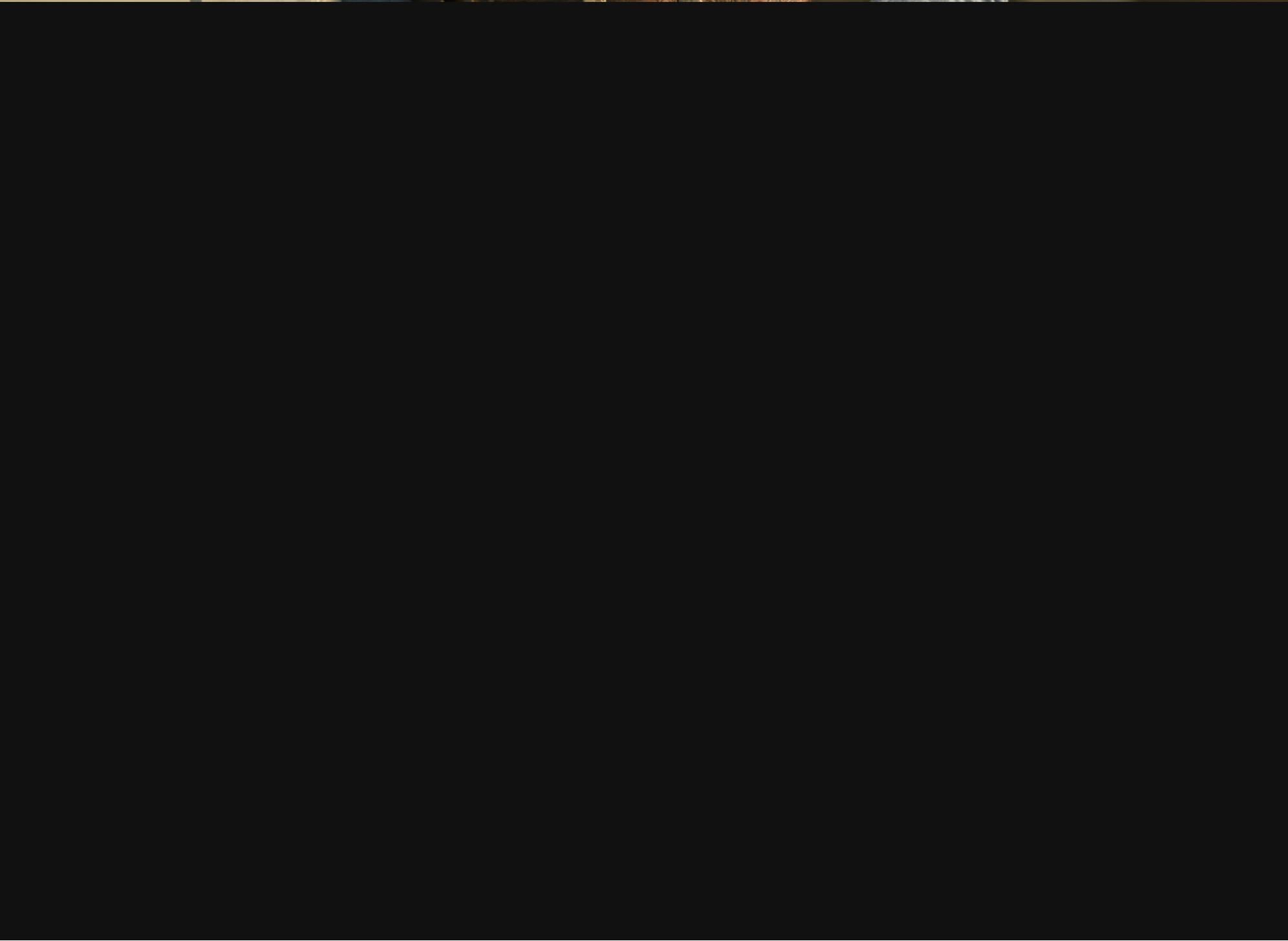
A cowboy wearing a wide-brimmed hat and a dark vest over a light shirt, holding a revolver. The background is a blurred outdoor setting.

Main issues



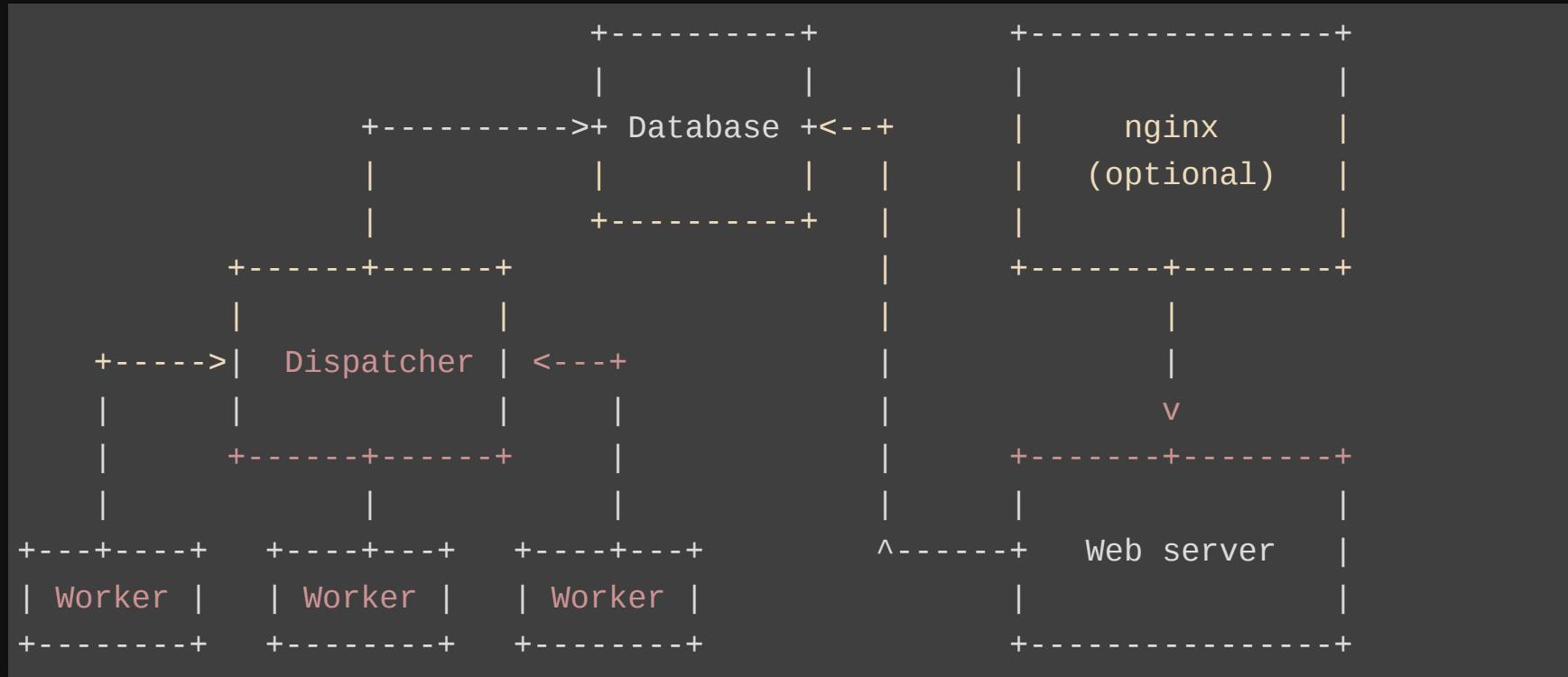


Dolores
Klara



- distributed YARA scanning
- web interface
- users groups
- e-mail notifications

- Python
- MariaDB
- Yara



Our work philosophy

 **Costin Raiu** 
@craiu Following ▾

Giving back to the community is part of our work philosophy. Today we open source KLARA, our [#yara](#) scanning framework. Props to [@_xdanx](#) who made this possible. Cc [@plusvic](#) [@JohnLaTwC](#)

 **KasperskyLab/klara**
Kaspersky's GReAT KLara. Contribute to klara development by creating an account on Github.
[github.com](https://github.com/KasperskyLab/klara)

2:57 PM - 9 Mar 2018

235 Retweets 354 Likes


Comment 5 Retweet 235 Like 354 Share

<https://github.com/KasperskyLab/klara>

Installing

<https://github.com/KasperskyLab/klara/tree/master/install>

- Ubuntu 16.04 / 18.04
- Dispatcher: Supervisor; Python + virtualenv
- Worker: Supervisor; Python + virtualenv; Yara
- DB: MariaDB / MySQL

Add a new job	
Notify e-mail	user@example.com
Yara Rules	<pre>1 rule silent_banker : banker 2 { 3 meta: 4 description = "This is just an example" 5 threat_level = 3 6 in_the_wild = true 7 8 strings: 9 \$a = {6A 40 68 00 30 00 00 6A 14 8D 91} 10 \$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9} 11 \$c = "UVODFRYSIHLNWPEJXQZAKCBGMT" 12 13 condition: 14 \$a or \$b or \$c 15 }</pre>
Repositories to scan	<input checked="" type="checkbox"/> /sas <input checked="" type="checkbox"/> /_clean
	<input type="button" value="Submit"/>

#	Description	Repo name	Rule name	Matched files	Status and actions
21300	Agent info: N/A Owner: klara	/sas	silent_banker : banker	N/A	New Job Job Management
21299	Agent info: N/A Owner: klara	/_clean	silent_banker : banker	N/A	New Job Job Management

Showing 1 to 2 of 2 entries [Show 10 ▾ entries](#)

Previous

1

Next

Search:

Job ID: 21300	
Status	Finished
Owner	klara
Start time	2018-02-22 20:17:29
Finish time	2018-02-22 20:17:45
Execution time	8 second(s)
Matched files	0
Rules	<pre>rule silent_banker : banker { meta: description = "This is just an example" threat_level = 3 in_the_wild = true strings: \$a = {6A 40 68 00 30 00 00 6A 14 8D 91} \$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9} \$c = "UVODFRYSIHLNWPExJQZAKCBGMT" condition: \$a or \$b or \$c }</pre>
Fileset scan	/sas
Matched MD5s	N/A
Results	### Yara found no matches! ###

Understanding Users and Groups

```
> select * from users;  
+-----+-----+-----+-----+  
| username | desc          | auth | group_cnt | quota_searches |  
+-----+-----+-----+-----+  
| HITB-admin | Hello HITB 2018! |    16 |         1 |             0 |  
| HITB-user  | Hello HITB 2018! |     2 |         2 |        1000 |  
+-----+-----+-----+-----+
```


Understanding Users and Groups

```
> select * from users;
```

username	desc	auth	group_cnt	quota_searches
HITB-admin	Hello HITB 2018!	16	1	0
HITB-user	Hello HITB 2018!	2	2	1000

```
> select * from users_groups
```

cnt	name	scan_filesets_list	jail_users
1	admins	[1,3,5]	0
2	general	[1]	1

Understanding Groups and Scan Repositories

```
> select * from users_groups
+-----+-----+-----+-----+
| cnt | name      | scan_filesets_list | jail_users |
+-----+-----+-----+-----+
| 1   | admins    | [1,3,5]          | 0           |
| 2   | general   | [1]              | 1           |
+-----+-----+-----+-----+
> select * from scan_filesets
+-----+
| id | entry          |
+-----+
| 1  | /virustotal_samples |
| 3  | /clean_files      |
| 5  | /col_a + /col_b + /col_c |
+-----+
```


Add a new job	
Notify e-mail	user@example.com
Yara Rules	<pre>1 rule silent_banker : banker 2 { 3 meta: 4 description = "This is just an example" 5 threat_level = 3 6 in_the_wild = true 7 8 strings: 9 \$a = {6A 40 68 00 30 00 00 6A 14 8D 91} 10 \$b = {8D 4D B0 2B C1 83 C0 27 99 6A 4E 59 F7 F9} 11 \$c = "UVODFRYSIHLNWPEJXQZAKCBGMT" 12 13 condition: 14 \$a or \$b or \$c 15 }</pre>
Repositories to scan	<input checked="" type="checkbox"/> /sas <input checked="" type="checkbox"/> /_clean
	<input type="button" value="Submit"/>

Repository control file

github.com/KasperskyLab/klara/blob/master/install/README.md

Search: Setting up worker's scan repositories

Advanced features

github.com/KasperskyLab/klara/blob/master/install/features_advanced.md

Redirect Paths

```
cat /mnt/storage/virustotal_samples/repository_control.txt:  
{  
  
    "owner" : "John Doe",  
    "files_type" : "elf",  
    "repository_type" : "APT",  
    "redirect_paths" : [  
        "/mnt/nas/klara_bigger_collection/"  
    ]  
  
}
```


Redirect Paths

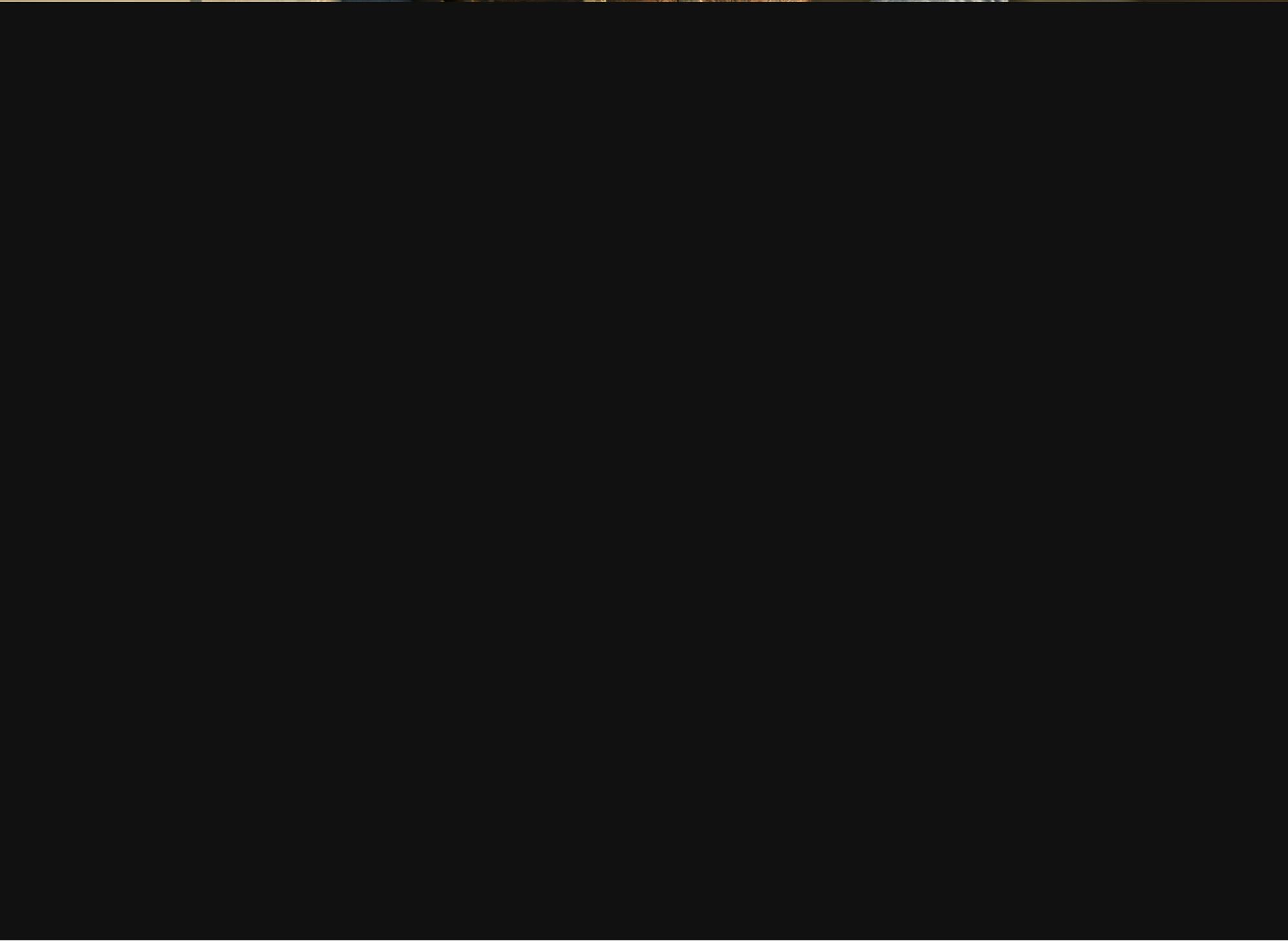
```
cat /mnt/storage/virustotal_samples/repository_control.txt:  
{  
  
    "owner" : "John Doe",  
    "files_type" : "elf",  
    "repository_type" : "APT",  
    "redirect_paths" : [  
        "/mnt/nas/klara_bigger_collection/"  
    ]  
  
}  
  
/mnt/storage/virustotal_samples/ => /mnt/nas/klara_bigger_collection/
```


Advanced features

- Redirect paths
- Rewrite paths
- Hash searches
- Shareable links



Dolores
Klara



A woman with long blonde hair tied back, wearing a light-colored tank top and jeans, stands outdoors in a rugged, mountainous landscape. She is holding a rifle with a dark leather bandolier across her chest. She is looking towards the camera with a slight smile. The background shows rolling hills and mountains under a clear sky.

Angry Klara

Performance

- 8x 2Tb SAMSUNG enterprise SSDs
- RAID 5
- XFS Filesystem
- Supermicro - 2x Xeon E5-2690V3, 64GB Ram

2 GB/second



Our stats

- 10 TB - 40 min
- 30k Klara jobs
- Yara training

Some filesystem optimisations

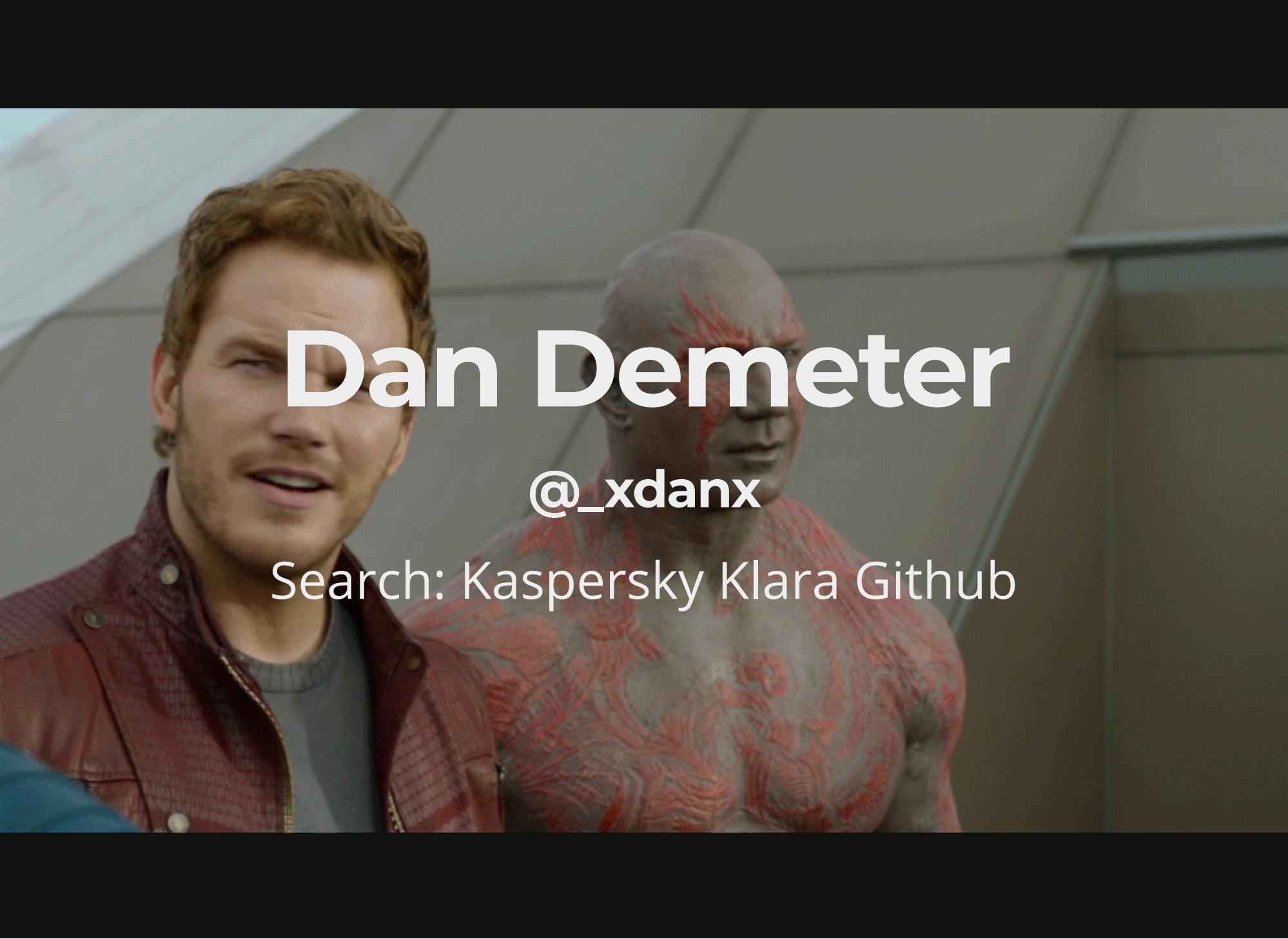
```
# mkfs.xfs:  
mkfs.xfs -f -d su=256k,sw=7,agcount=24 -l version=2,su=256 -i size=512 \  
/dev/sda1  
  
# mount xfs:  
mount -o noatime,nodiratime,nobarrier,largeio,inode64,swalloc, \  
logbufs=8,logbsize=256k,allocsize=131072k \  
/dev/sda
```


Future plans

Out gift for you!

*"If you know the enemy and know yourself you need
not fear the results of a hundred Yara scans."*

-- Sun Tzu about Klara

A promotional image for the movie Guardians of the Galaxy. It features Chris Pratt as Peter Quill/Damian Quill on the left, looking towards the right with a slight smile. On the right, Baby Groot, the tree-like alien, is shown from the chest up, looking directly at the camera with a neutral expression. The background is a metallic, industrial-looking interior.

Dan Demeter

@_xdanx

Search: Kaspersky Klara Github

