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

-- Sun Tzu

./whoami

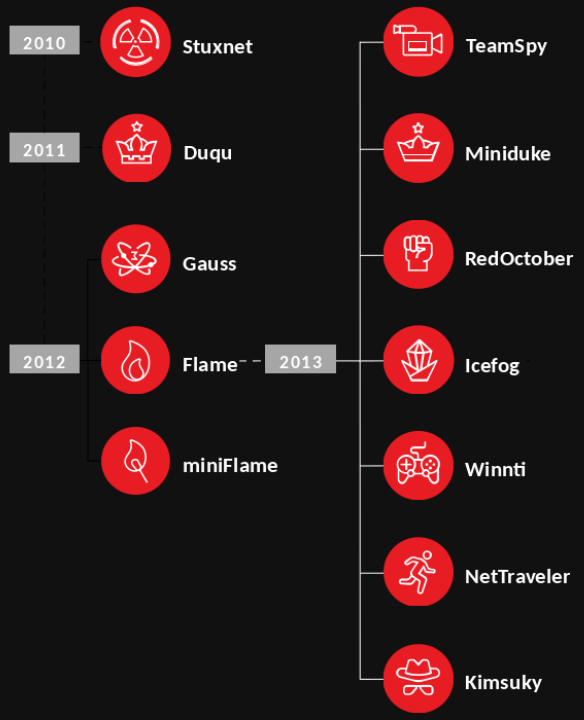
- MEng from Imperial College London in 2014
- Security Researcher @ Kaspersky Lab
- Threat Intelligence and Big Data

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

We discover and dissect the world's most sophisticated threats



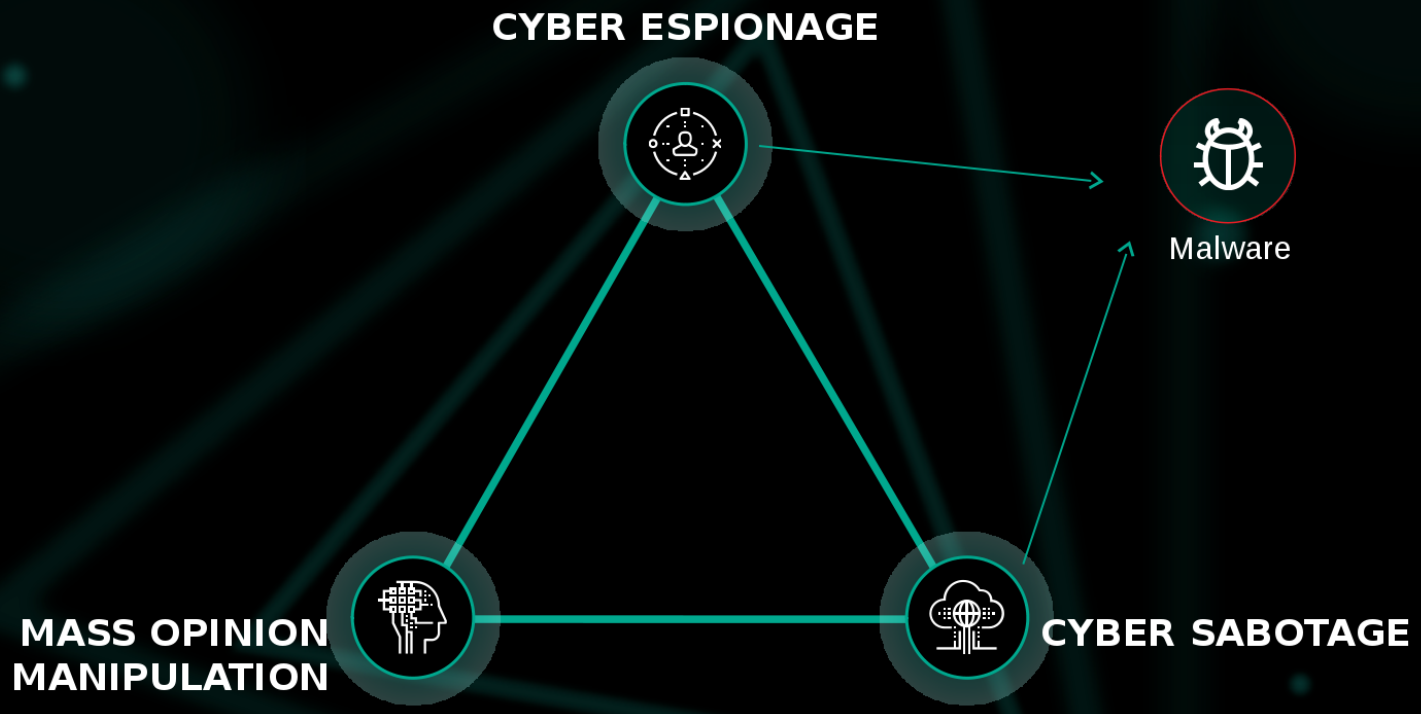
TARGETED ATTACKS

GREAT

We discover and dissect the world's most sophisticated threats

KASPERSKY lab

The Information War



KASPERSKY lab

The Information War

Malware

KASPERSKY lab

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/


Hunting in the wild

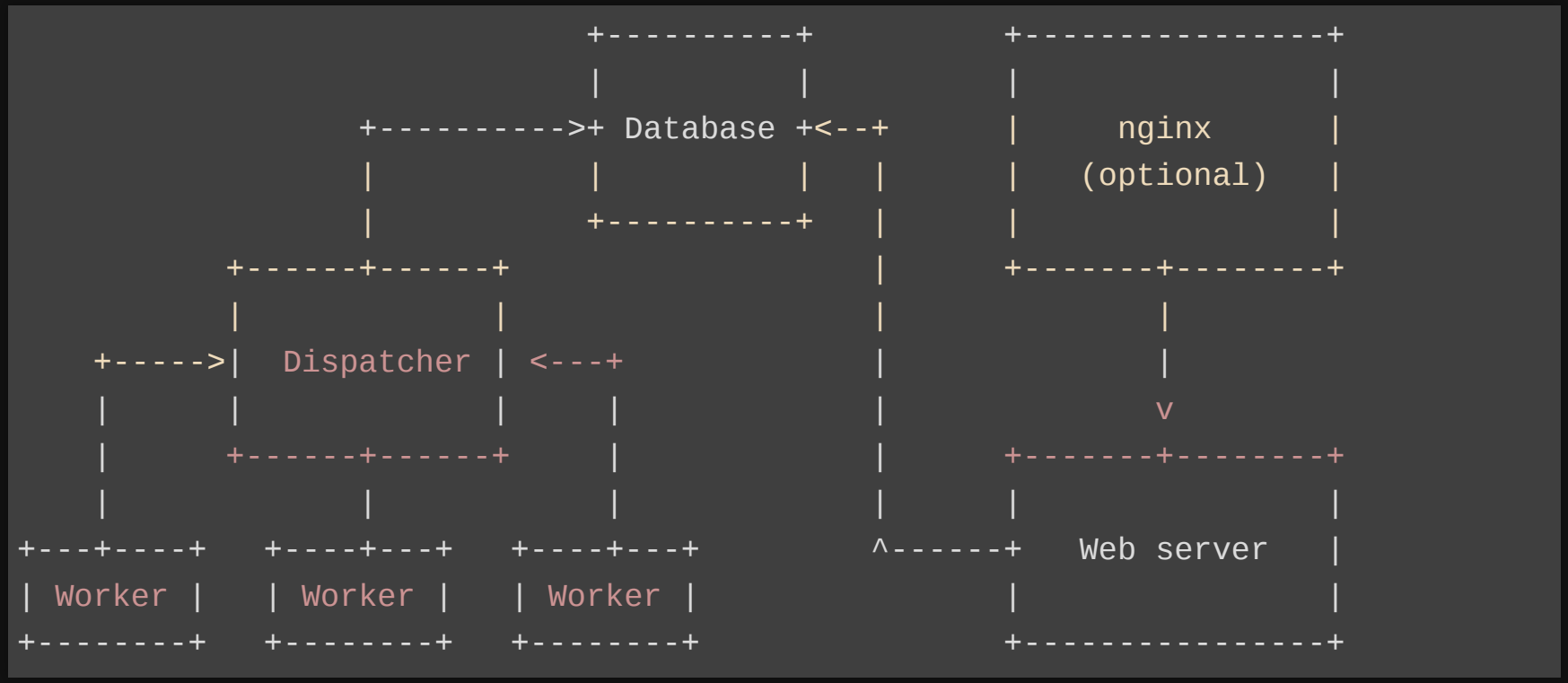
https://virustotal.com


Main issues


~~Dolores~~
Klara

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

- Python
- MariaDB
- Yara


Database
nginx
(optional)
Dispatcher
Worker
Worker
Worker
Web server

Our work philosophy

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

GReAT KLara Current jobs New job My profile Current quota: **1000** jobs - Logged in as klara - Group: Kaspersky Training [Logout]

Add a new job

Notify e-mail: user@example.com

Yara Rules

```
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 = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Repositories to scan

- [x] /sas
- [x] /_clean

Submit

GReAT KLara Current jobs New job My profile Current quota: **998** jobs - Logged in as klara - Group: Kaspersky Training [Logout]

Showing 1 to 2 of 2 entries **Show** 10 **entries** Previous 1 Next **Search:**

#	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	`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 = "UVODFRYSIHLNWPEJXQZAKCBGMT"`
	
	`  condition:`
	`  $a or $b or $c`
	`}`

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       |
+----+--------------------------------+
```

GReAT KLara Current jobs New job My profile Current quota: **1000** jobs - Logged in as klara - Group: Kaspersky Training [Logout]

Add a new job

Notify e-mail: user@example.com

Yara Rules

```
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 = "UVODFRYSIHLNWPEJXQZAKCBGMT"

    condition:
        $a or $b or $c
}
```

Repositories to scan

- [x] /sas
- [x] /_clean

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


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

Dan Demeter

@_xdanx

Search: Kaspersky Klara Github