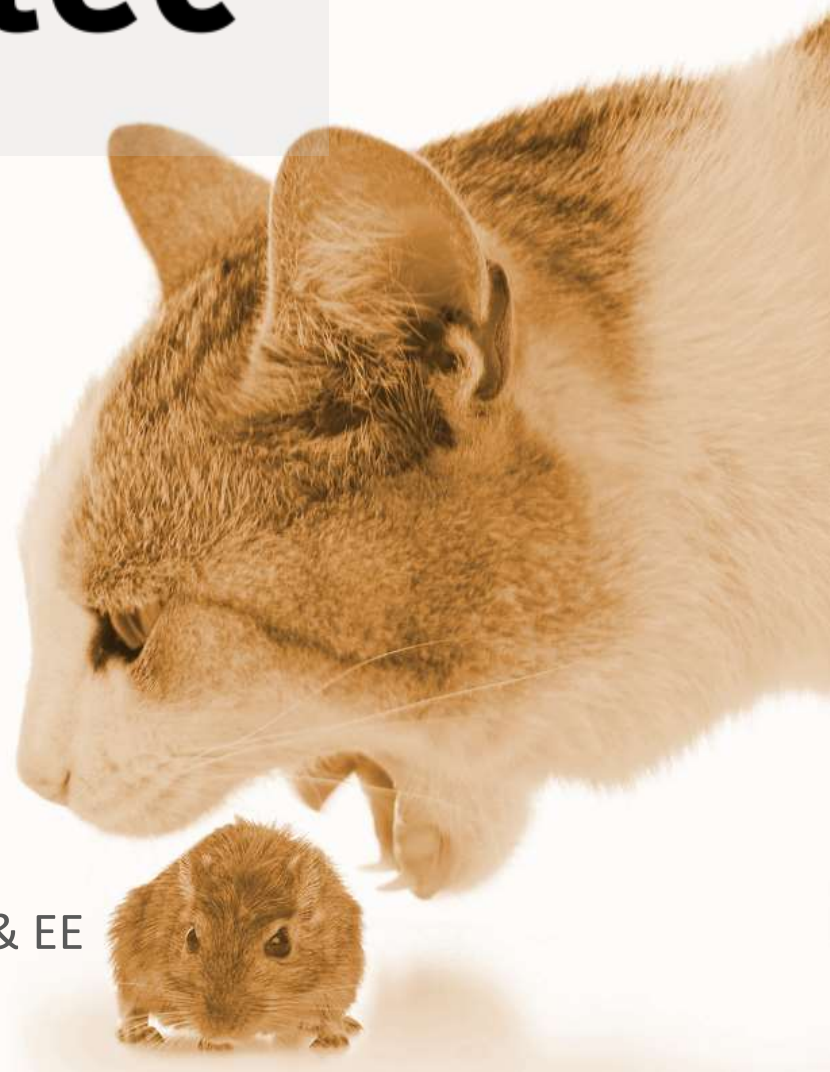
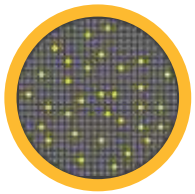
KATZ UND MAUS IM SANDKASTEN



Lukas Rist Sr. Software Engineer MA
Andre Engel Sr. System Engineer ATP DACH & EE

SYMANTEC
AT A GLANCE



175M endpoints
under protection

$4.6B annual
revenue

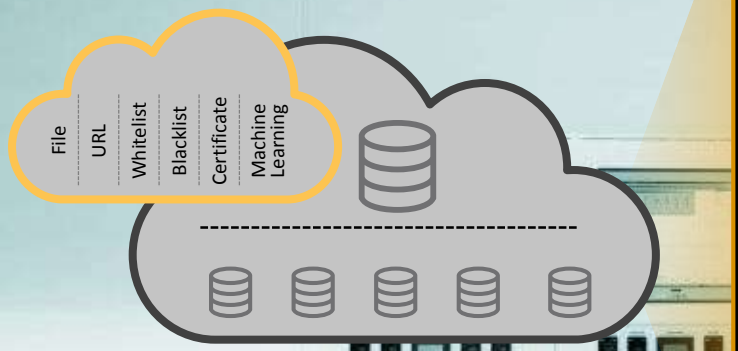
2123 patents

385,000
customers worldwide

3000+
R&D engineers

6 SOCs threat
response centers

SYMANTEC
WE FIGHT FOR THE USER



Discovered
430 million
new unique pieces
of malware last year

1B
malicious emails
stopped last year

100M
social engineering
scams blocked
last year

12,000+
Cloud applications
discovered and
protected

1 Billion websites
categorised each day

INTELLIGENCE SOURCED FROM:

1 Billion previously unseen web requests scanned daily

2 Billion emails scanned per day

175M Consumer and Enterprise endpoints protected

9 global threat response centers with
3,000 Researchers and Engineers


Managed PKI
VIP/ Identity
Encrypted Traffic Management
Data Protection
Information
Management & Compliance
Data Center
Endpoint Detection
Endpoint Protection
Users
Security Analytics
CASB
Content Analysis
Web Protection
Web
Encryption
Message Security
Anti-Phishing
Email Protection
Messaging
Symantec.
Integrated Cyber Defense

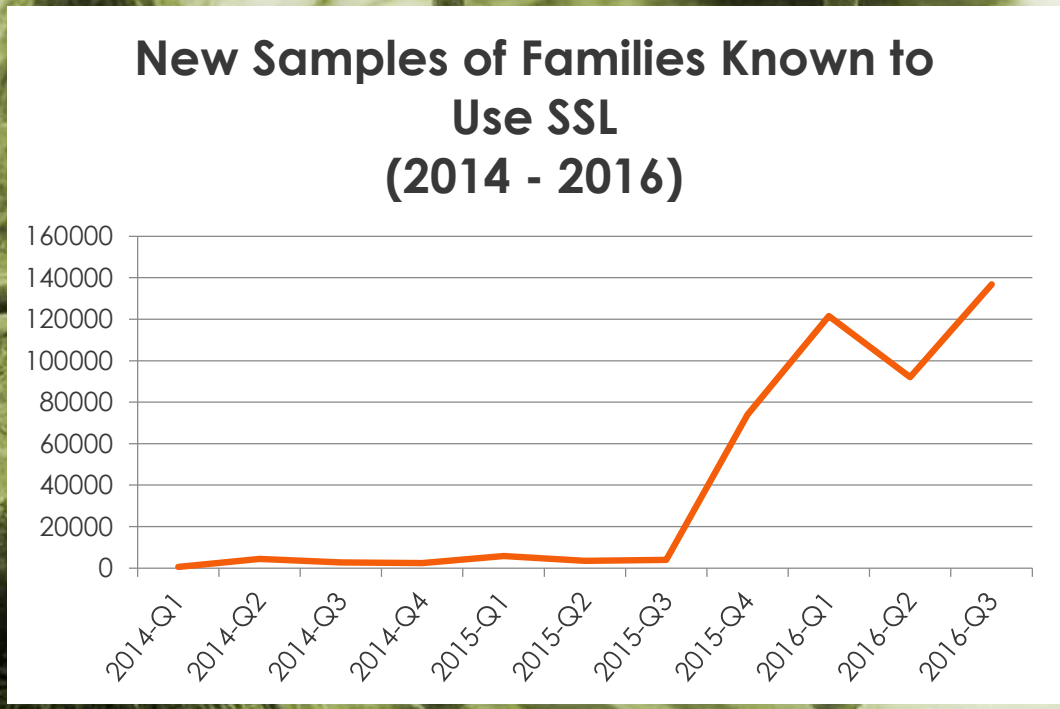
Increasing inflow from Families known to use SSL*

Malware based on **SSL Blacklist**† families spiked dramatically towards the end of 2015!

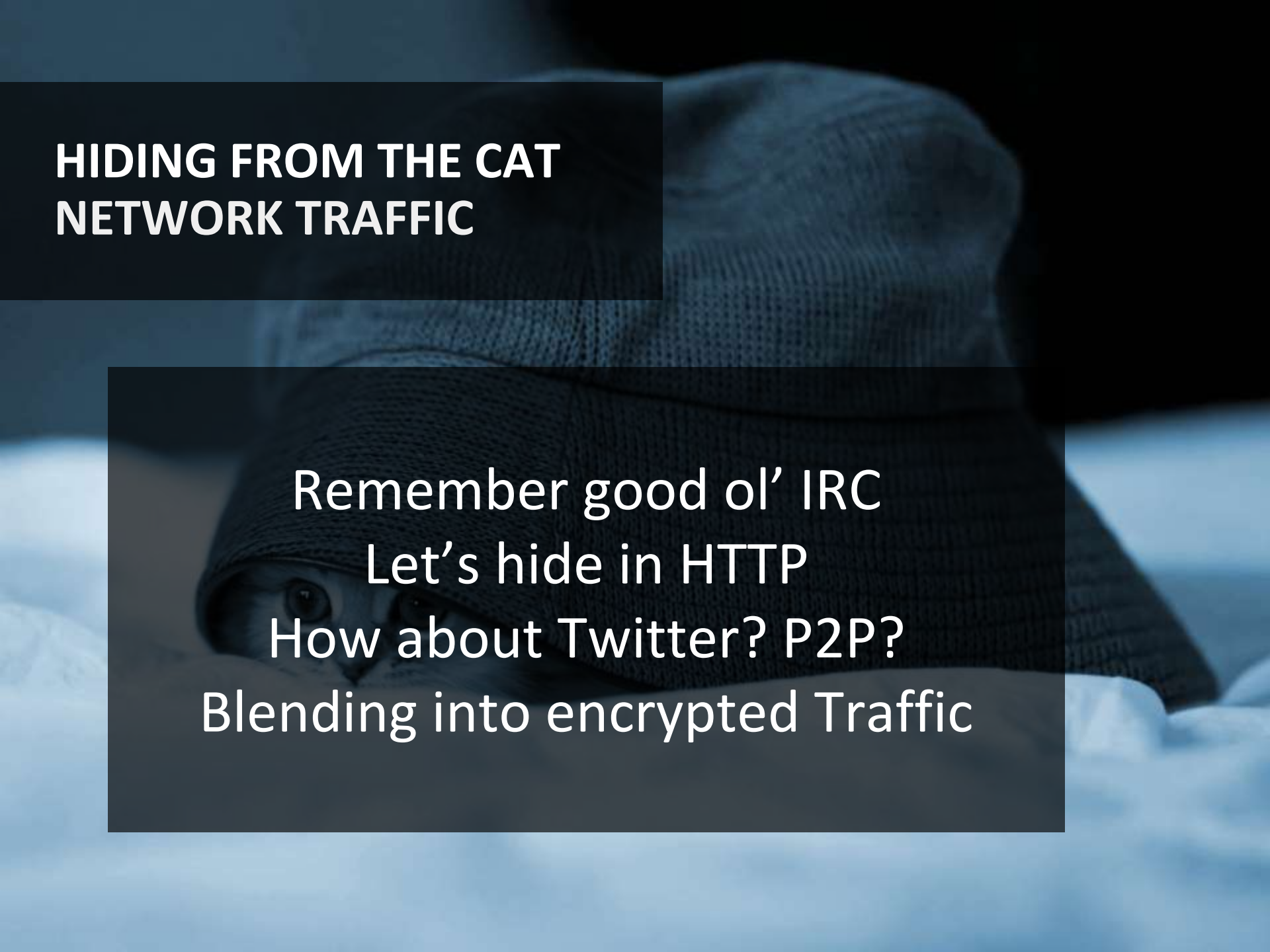
Dridex	**Spambot**	**Tinba**
KINS	**Retefe**	**Gozi**
Shylock	**TeslaCrypt**	**VMZeus**
URLzone	**CryptoLocker**	**Redyms**
TorrentLocker	**Bebloh**	**Qadars**
CryptoWall	**Gootkit**	**Vawtrack**
Upatre	**Geodo**	**Emotet**

† *SSL Blacklist can be viewed at https://sslbl.abuse.ch*

* *Samples observed on VirusTotal*



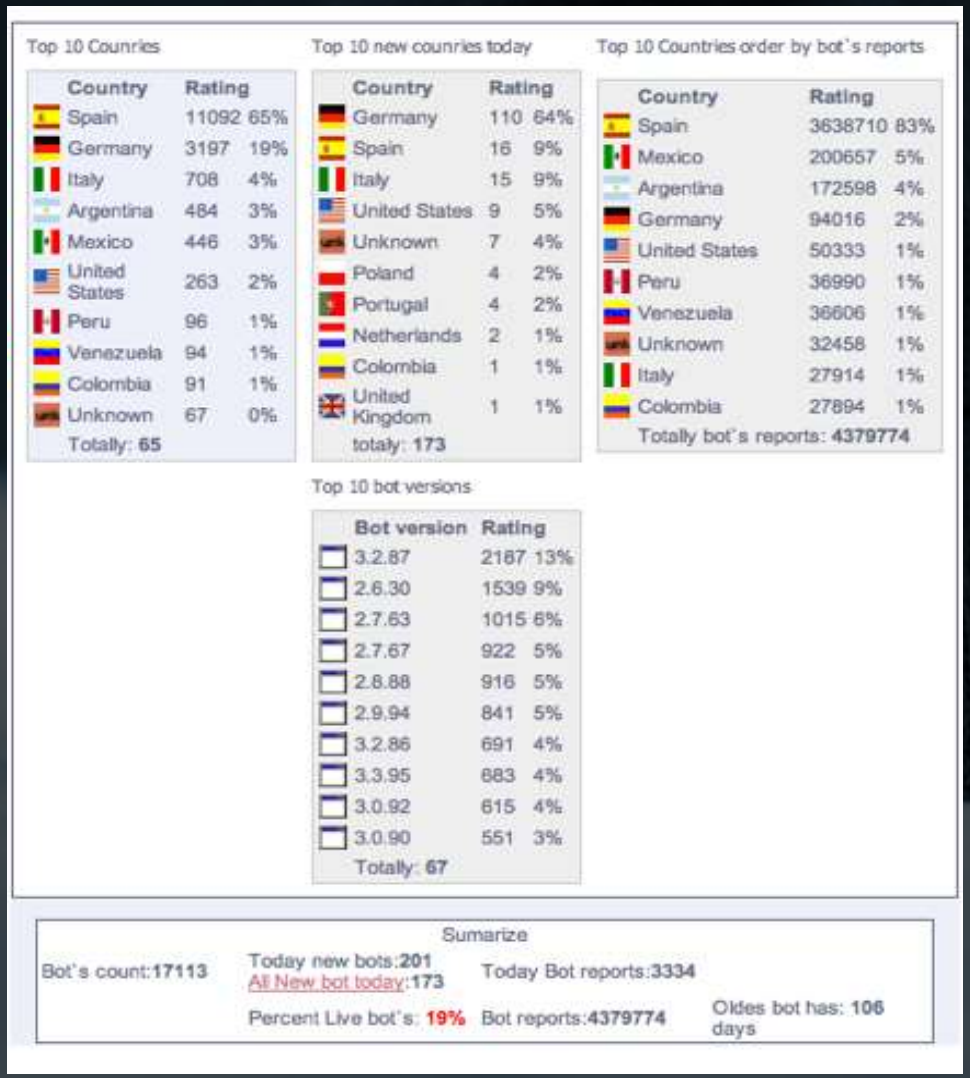

100% OF ALL SECURITY
SOLUTIONS HAVE WEAKNESSES
Protect Like an Onion
Network Protection
Antivirus
Sandbox
Weaknesses
Encryption
Packers/Polymorphic
VM Detection
Make It Hard
Make ‘em sweat
those tears...



HIDING FROM THE CAT
NETWORK TRAFFIC

Remember good ol’ IRC
Let’s hide in HTTP
How about Twitter? P2P?
Blending into encrypted Traffic

HIDING FROM THE CAT
NETWORK TRAFFIC



Top 10 Counries

Country	Rating	
Spain	11092	65%
Germany	3197	19%
Italy	708	4%
Argentina	484	3%
Mexico	446	3%
United States	263	2%
Peru	96	1%
Venezuela	94	1%
Colombia	91	1%
Unknown	67	0%

Totaly: **65**

Top 10 new counries today

Country	Rating	
Germany	110	64%
Spain	16	9%
Italy	15	9%
United States	9	5%
Unknown	7	4%
Poland	4	2%
Portugal	4	2%
Netherlands	2	1%
Colombia	1	1%
United Kingdom	1	1%

totaly: **173**

Top 10 Countries order by bot`s reports

Country	Rating	
Spain	3638710	83%
Mexico	200657	5%
Argentina	172598	4%
Germany	94016	2%
United States	50333	1%
Peru	36990	1%
Venezuela	36606	1%
Unknown	32458	1%
Italy	27914	1%
Colombia	27894	1%

Totally bot`s reports: **4379774**

Top 10 bot versions

Bot version	Rating	
3.2.87	2167	13%
2.6.30	1539	9%
2.7.63	1015	6%
2.7.67	922	5%
2.6.88	916	5%
2.9.94	841	5%
3.2.86	691	4%
3.3.95	683	4%
3.0.92	615	4%
3.0.90	551	3%

Totaly: **67**

Sumarize

Bot`s count:**17113**

Today new bots:**201**
All New bot today:**173**

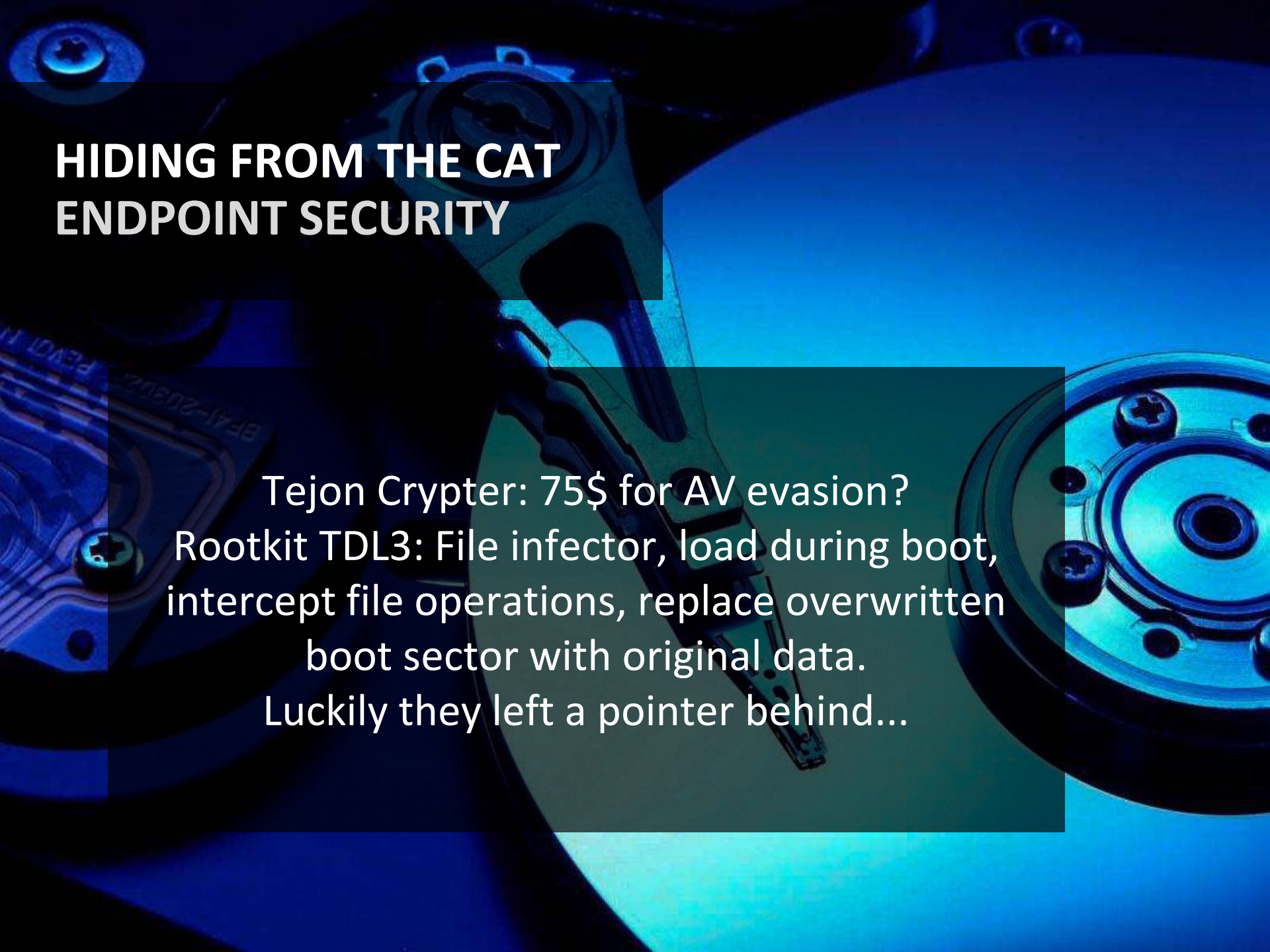
Today Bot reports:**3334**

Percent Live bot`s: **19%**

Bot reports:**4379774**

Oldes bot has: **106** days

HTTP/S



HIDING FROM THE CAT
ENDPOINT SECURITY

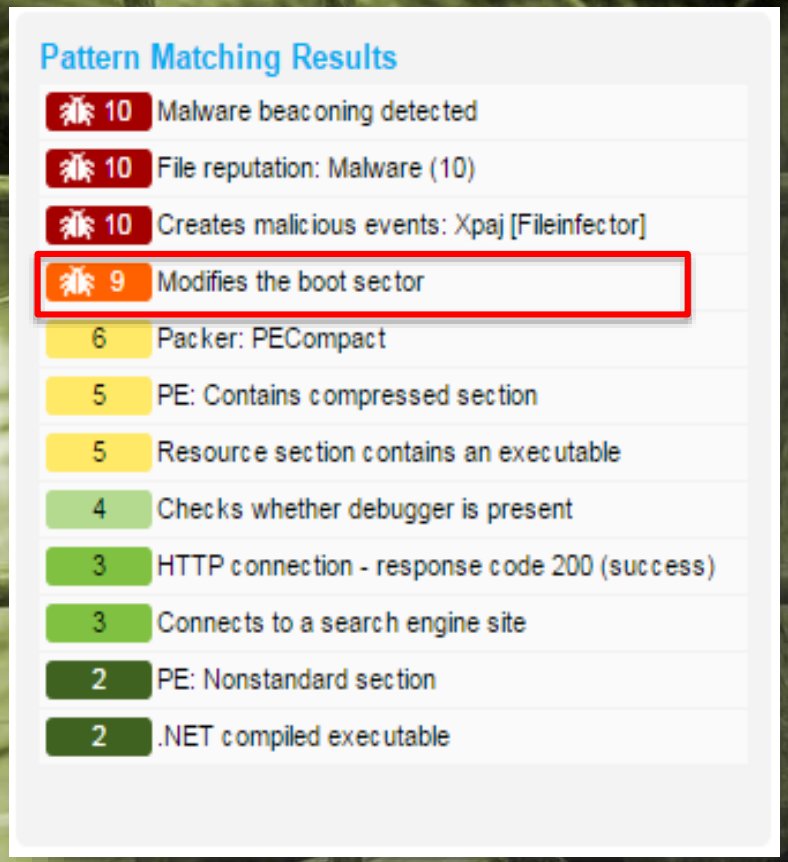
Tejon Crypter: 75$ for AV evasion?
Rootkit TDL3: File infector, load during boot, intercept file operations, replace overwritten boot sector with original data.
Luckily they left a pointer behind...

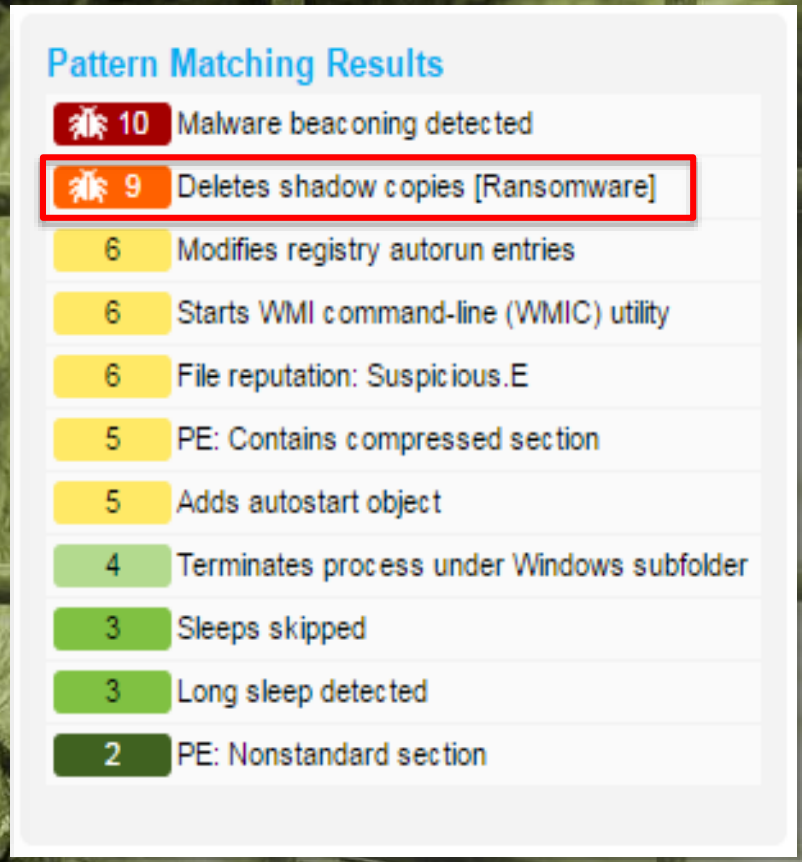
HIDING FROM THE CAT
SANDBOXING

Sandboxes are more than just run-time analysis:

- File, IP, domain reputation
- File properties
- Statistical analysis
- Detonation

➔ Small anti-virus lab on premise





Sandboxes show the behavior as on a real system
See the installation of a bootkit before it is on real system
See ransomware before it encrypts files on a user's system

HIDING FROM THE CAT SANDBOXING

Detecting discrepancies in the execution environment

Typically look for signs of being run in a sandbox, or any differences in the execution environment compared to what is expected on the target

HIDING FROM THE CAT SANDBOXING

Exhibit different behavior inside the sandbox than on a target system

Often means not running the ‘malicious part’ of the code, or simply crash

HIDING FROM THE CAT
SANDBOXING

```
push    large dword ptr fs:30h
pop     eax             ; eax now holds PEB (Process Environment Block)
mov     [esp+30h+PEB], eax
mov     eax, [esp+30h+PEB]
cmp     dword ptr [eax+64h], 2 ;  check number of processors
jnb     short continue  ; continue if 2 or greater
```

```
xor     eax, eax
pop     esi
mov     esp, ebp
pop     ebp
retn                    ;       returns to 406000 (intentional crash)
```

```
continue:
call    sub_4033C0
push    eax             ; lpProcName
push    offset aKernel32_dll_1 ; "kernel32.dll"
call    GetModuleHandleA
push    eax             ; hModule
call    GetProcAddress
```

HIDING FROM THE CAT
SANDBOXING

```
#define LONG_TIME 1200000  // 20 minutes specified in milliseconds

int malware()
{
    Sleep(LONG_TIME);

    // Do bad stuff
}
```

HIDING FROM THE CAT
SANDBOXING

```
ticks_before_sleep = GetTickCount();

Sleep(SOME_TIME);

ticks_after_sleep = GetTickCount();

// Check how much time has elapsed
if ( (ticks_after_sleep - ticks_before_sleep) >= EXPECTED_TICK_DIFFERENCE )
{
    // Do bad stuff
}
```


PROCESSING MALWARE
TO THE CLOUD!
Reduce maintenance and development cost
(fewer systems by providing a common platform)
Enable analysts to do efficient threat hunting
and MA pattern/signature development

PROCESSING MALWARE TO THE CLOUD!

Analyze large amounts of samples with different tools
Optimize the selection of samples to be analyzed in MA
Allow for easy deployment of additional workers into the flow
Configure the flow on the fly for custom needs
Elastic scaling of the resources used (micro services)

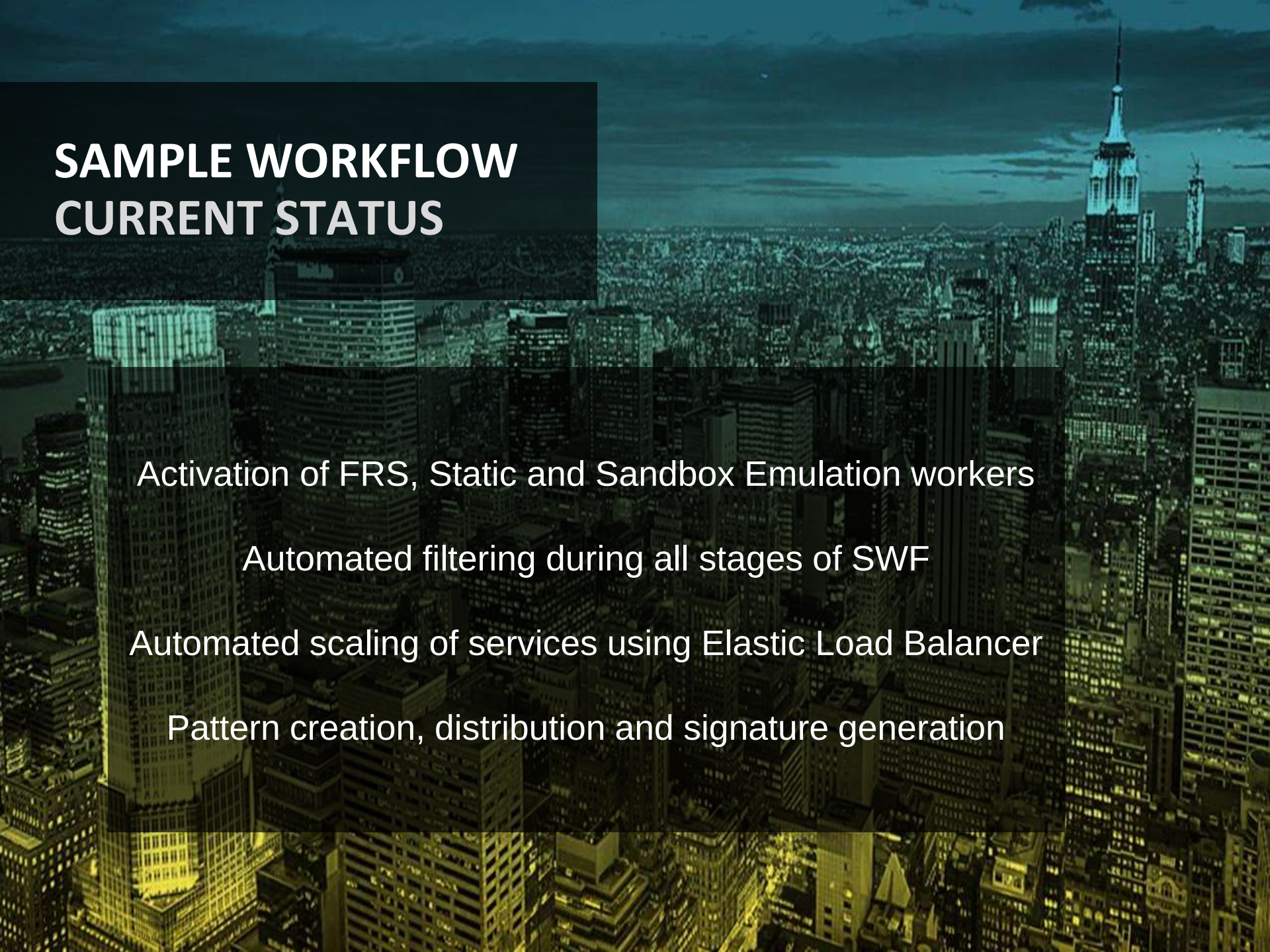
OPEN ANALYSIS PLATFORM
OVERVIEW

Open Analysis Platform 1/2
Sample intake/feeds
Patterns/Signatures/Updates

Open Analysis Platform 2/2
Sample Workflow (Elastic MA)
Analyst UI
Detection Backend

Malware Analysis Telemetry
File Reputation
Update Information

Data Sinks
VxDB
Global Intelligence Network
Analysts ;)



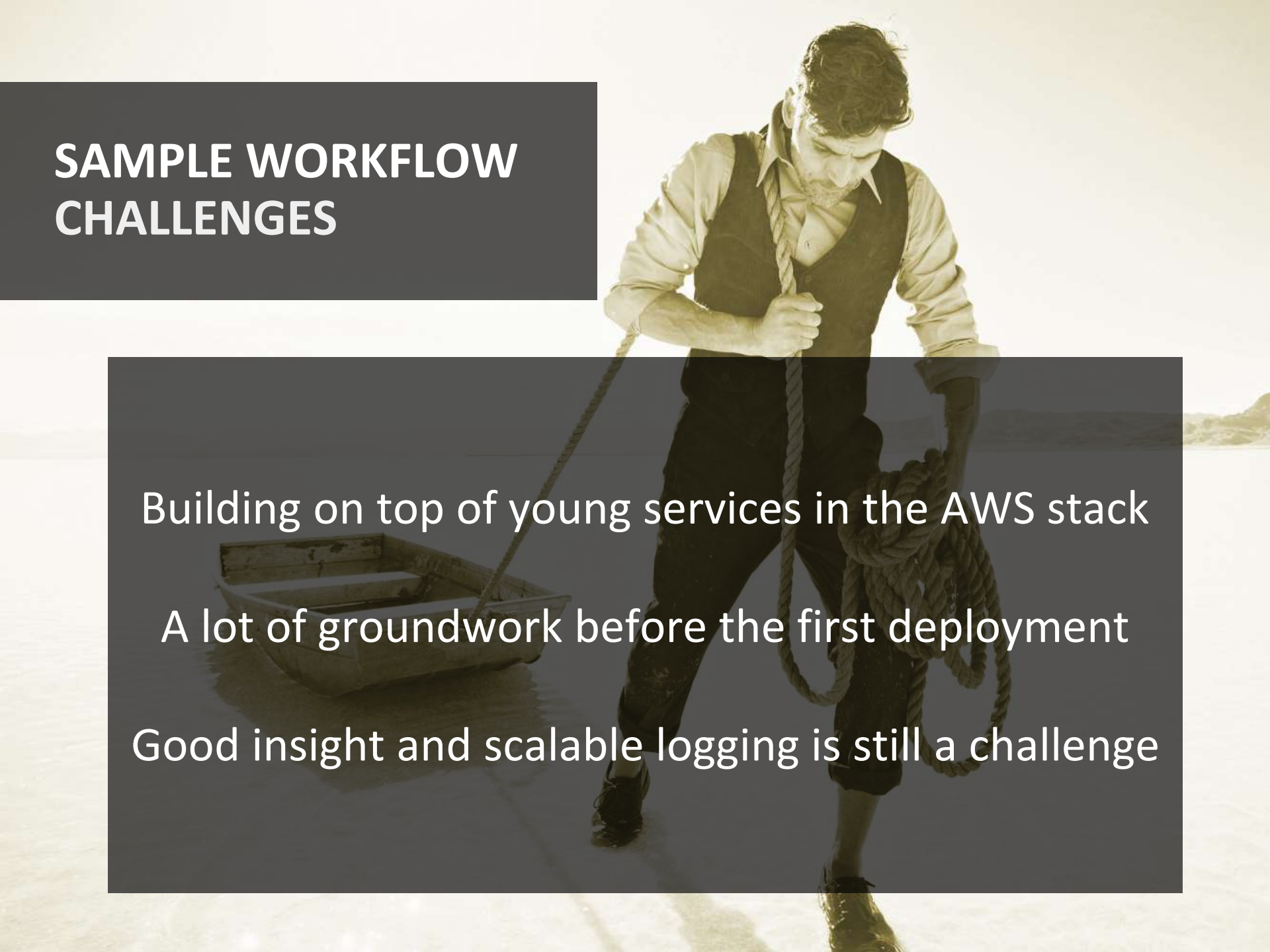
SAMPLE WORKFLOW CURRENT STATUS

Activation of FRS, Static and Sandbox Emulation workers

Automated filtering during all stages of SWF

Automated scaling of services using Elastic Load Balancer

Pattern creation, distribution and signature generation



SAMPLE WORKFLOW CHALLENGES

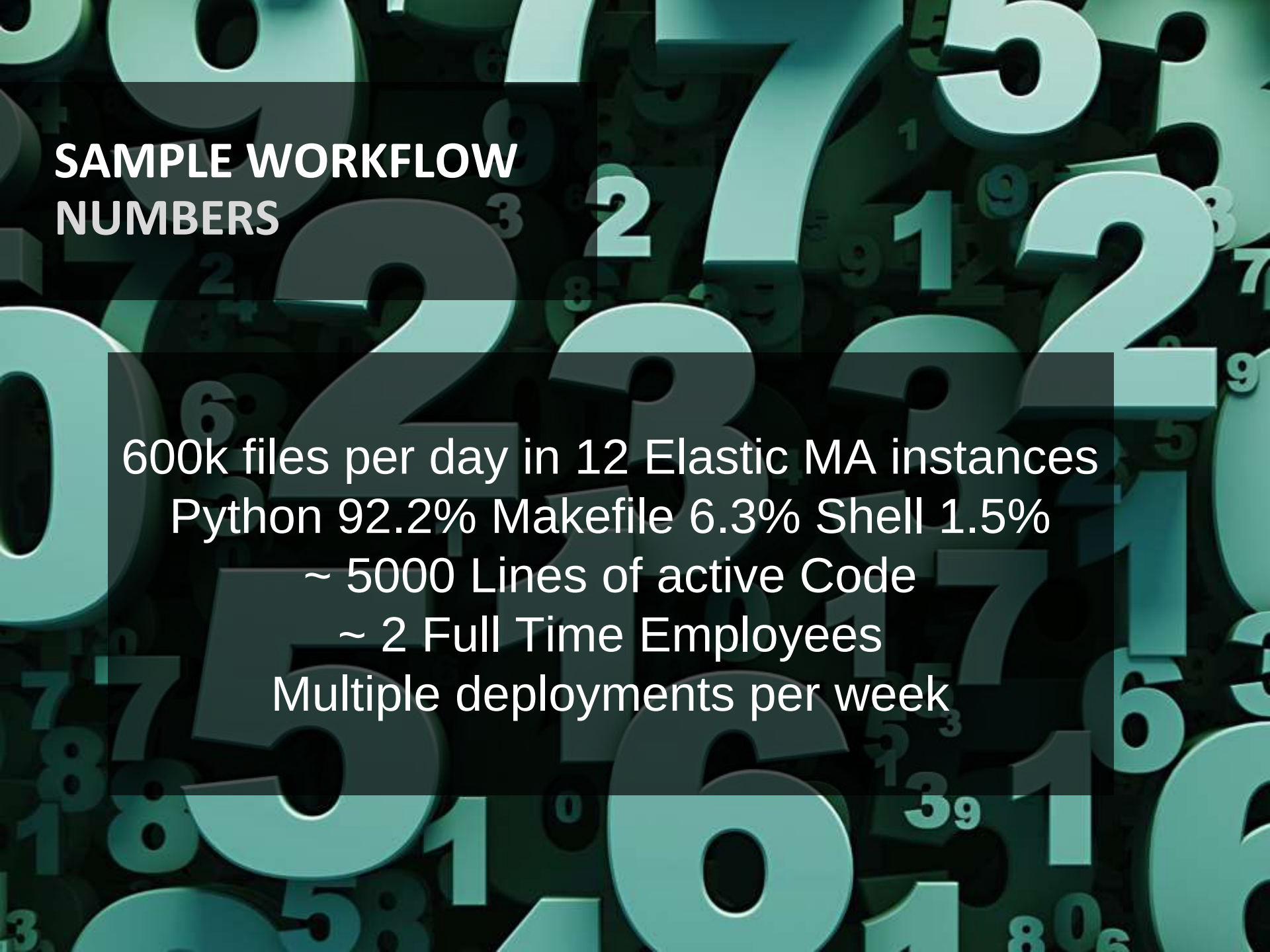
Building on top of young services in the AWS stack

A lot of groundwork before the first deployment

Good insight and scalable logging is still a challenge

SAMPLE WORKFLOW AWS SERVICES

Storage: S3
Databases: Aurora, DynamoDB
Computation: EC2/ECS+ECR
Networking: VPC, Route 53
Application Service: SQS, ELB/ALB



SAMPLE WORKFLOW NUMBERS

600k files per day in 12 Elastic MA instances
Python 92.2% Makefile 6.3% Shell 1.5%
~ 5000 Lines of active Code
~ 2 Full Time Employees
Multiple deployments per week

DANKE!

Lukas Rist Sr. Software Engineer MA
Andre Engel Sr. System Engineer ATP DACH & EE