

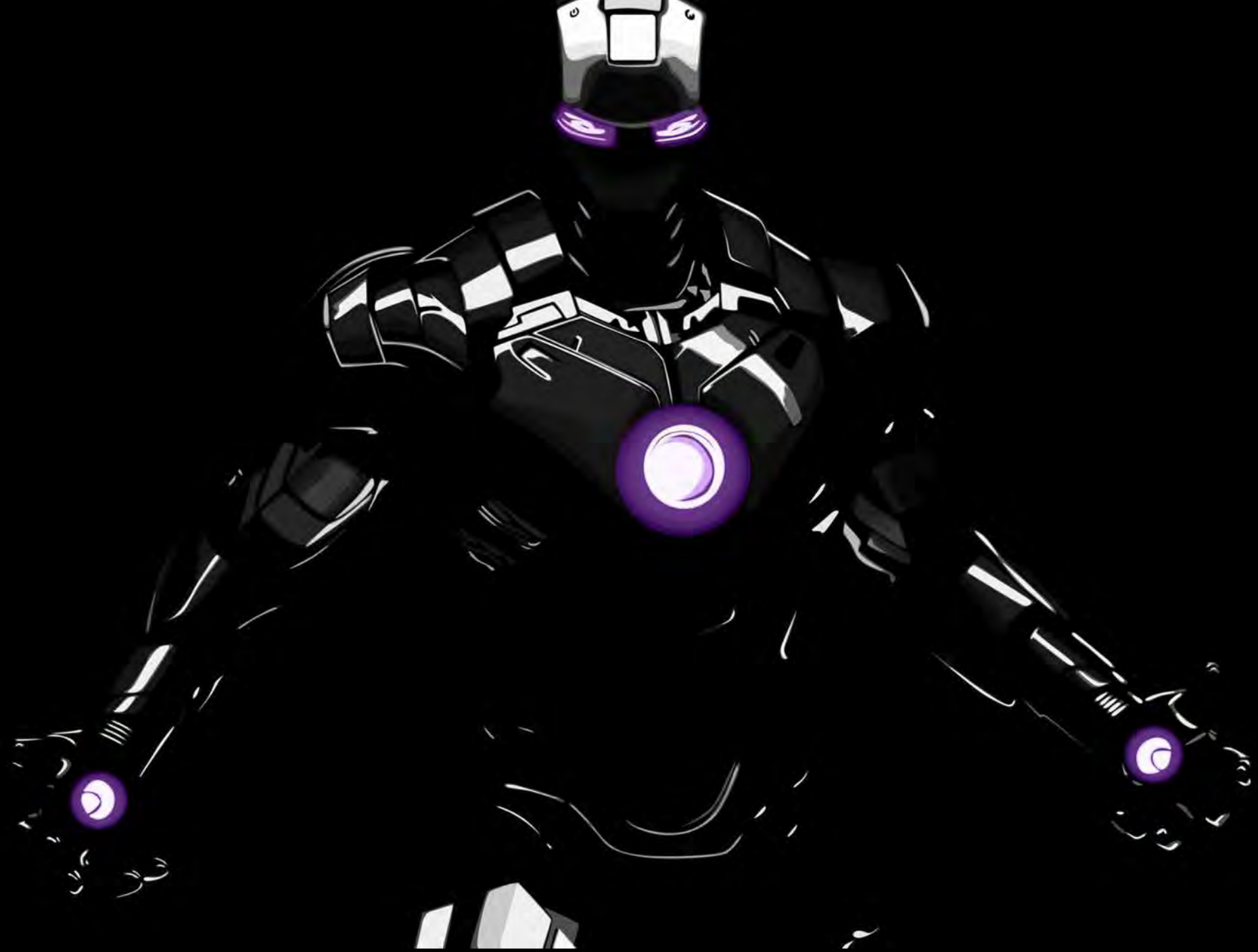


POSE A THREAT

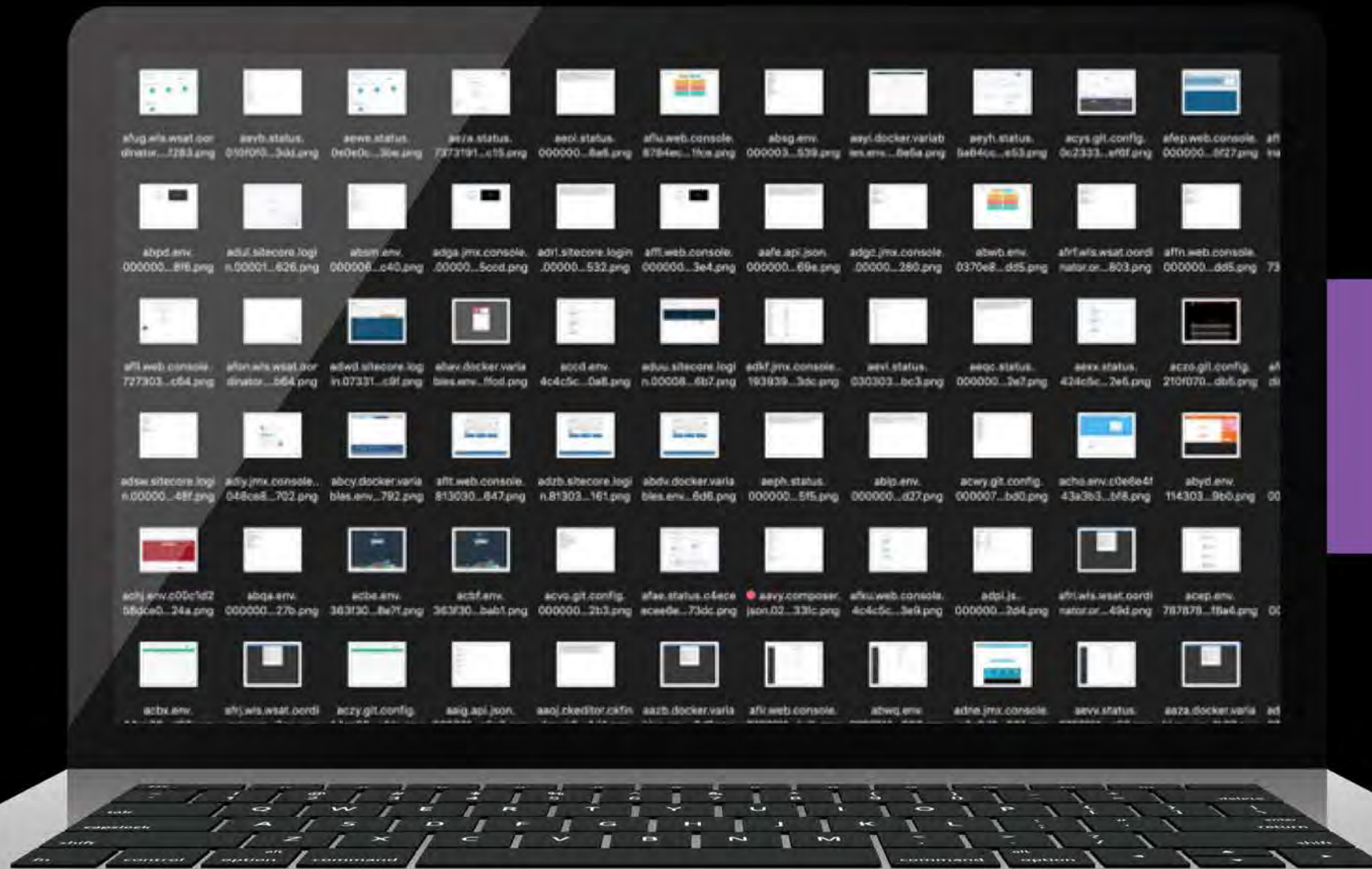
HOW PERCEPTUAL

ANALYSIS HELPS BUG HUNTERS

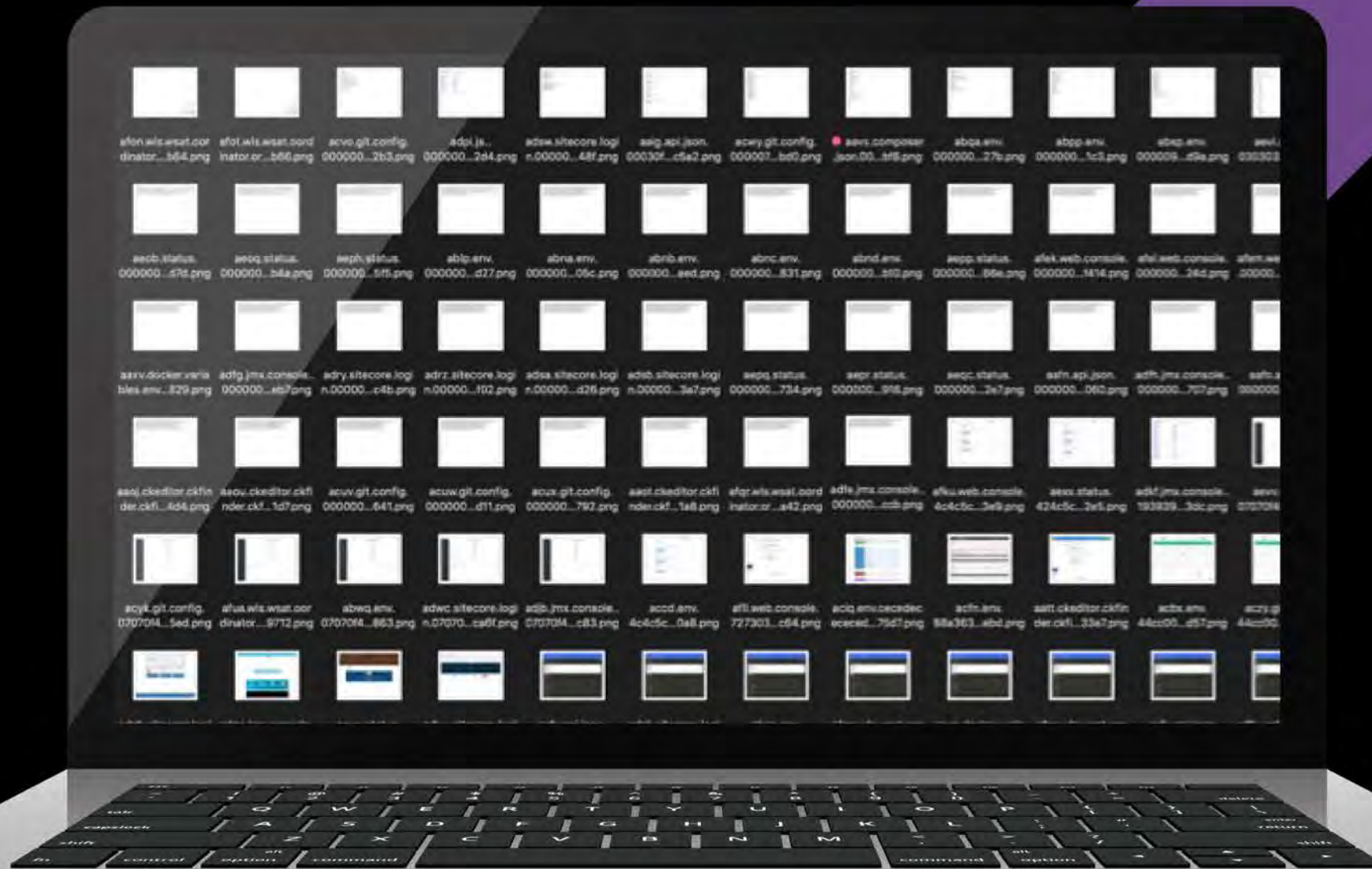
PRESENTED BY ROB RAGAN AND OSCAR SALAZAR



TURNING CHAOS



INTO ORDER



LET'S SEE SOME HANDS

WHO HERE IS
A PENTESTER?

QUESTION

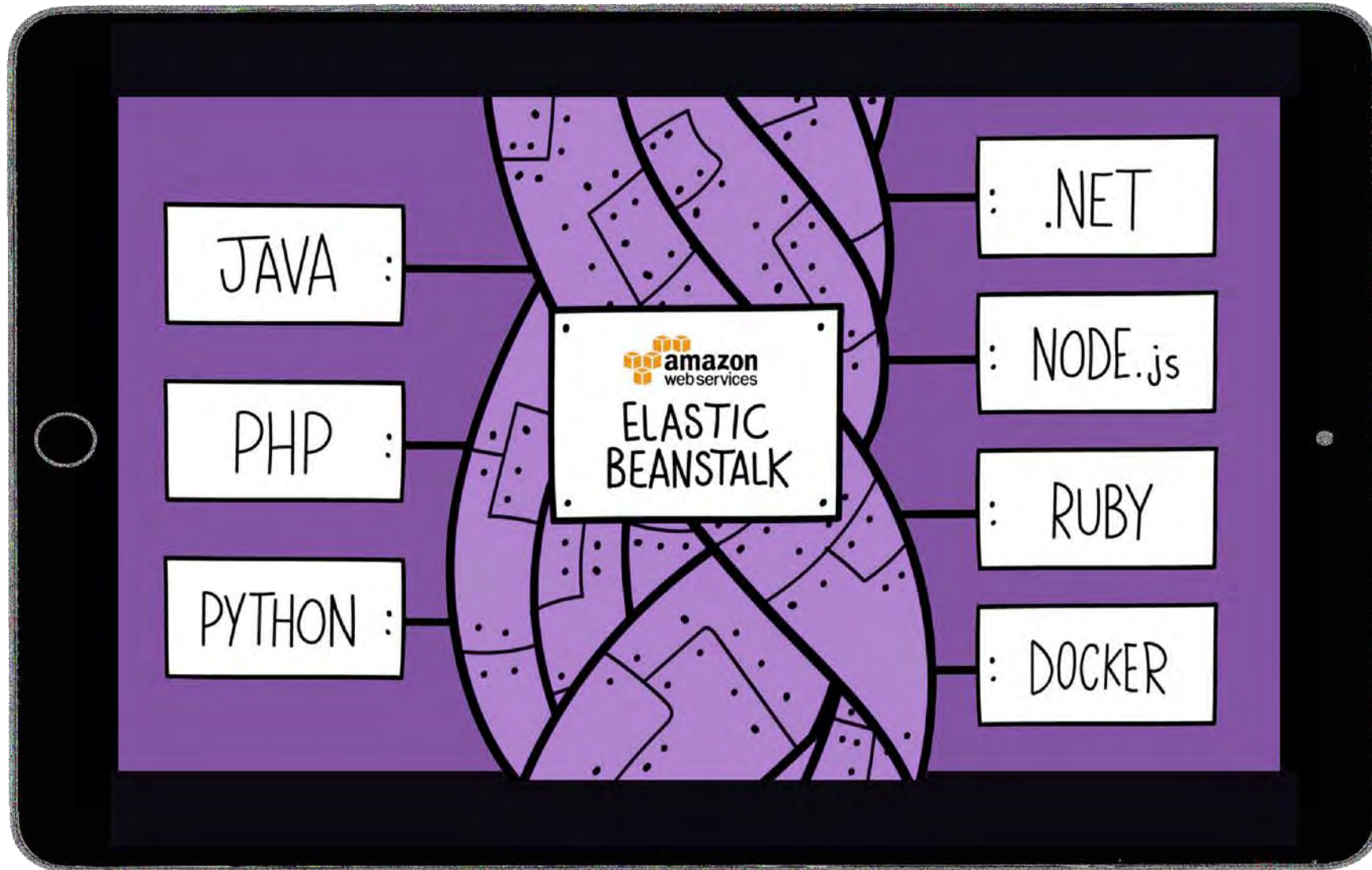
WHO HAS HAD THEIR AWS

CREDENTIALS

STOLEN?



WHAT IS **ELASTICBEANSTALK**




```
001tomacat8-env.2zbpvvy4i7.us-east-1.elasticbeanstalk.com
00-api-ib3alacarta-com.us-east-1.elasticbeanstalk.com
00ldrestdraj.us-west-2.elasticbeanstalk.com
0113t-pro.elasticbeanstalk.com
01test2-env.eu-west-2.elasticbeanstalk.com
03c9acbb-4d65-4544-bc3d-082aa04cc5b4.eu-west-1.elasticbeanstalk.com
05servicetest.us-east-2.elasticbeanstalk.com
07530960-a590-live-beeline-portal.eu-central-1.elasticbeanstalk.com
0f9b429-im-events-staging.us-west-2.elasticbeanstalk.com
1001-env.vj2paiqvay.us-west-2.elasticbeanstalk.com
100internal-env.4vuscgkmb.us-west-1.elasticbeanstalk.com
100internal-env.pinsu7bcza.us-west-2.elasticbeanstalk.com
100-million.us-east-1.elasticbeanstalk.com
101careers.eu-west-1.elasticbeanstalk.com
101-diy-master.ap-southeast-1.elasticbeanstalk.com
10d-idb-console-prod.eu-west-1.elasticbeanstalk.com
10d-idb-console-test.eu-west-1.elasticbeanstalk.com
10d-idb-prod.eu-west-1.elasticbeanstalk.com
10d-idb-test.eu-west-1.elasticbeanstalk.com
10d-tokens-console-prod.eu-west-1.elasticbeanstalk.com
10d-tokens-prod.eu-west-1.elasticbeanstalk.com
10dws-events-prod.eu-west-1.elasticbeanstalk.com
10e4.us-east-2.elasticbeanstalk.com
112-alex.us-east-1.elasticbeanstalk.com
:
```


5 AVENUES OF ATTACK

WEAK **PASSWORDS**

INSECURE
APPLICATIONS

SENSITIVE
INFO LEAKS

MISSING
PATCHES

SINGLE
MISCONFIGURATION



```
K2.ActionContext.container' ]).( #ognlUtil=#Container.getInstance(@com.opensymphony.xwork2.PackageNames().clear()).( #ognlUtil.getExcludedClasses().clear()).( #context.setMemberVletActionContext@getResponse()).( #res.addHeader('eresult','struts2_security_check'))/( #_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)?( #wr=#context[#parameters.0]content[0]),#wr.flush(),#wr.close()):xx.toString.json
/.env
/.ftpconfig
/.git/HEAD
/.git/config
/.git/info/refs
/.php
/.remote-sync.json
✓/.vscode/ftp-sync.json
/.well-known/security.txt
//
//.git/config
//.phpmyadmin/scripts/setup.php
///UE/welcome_login.html
//MyAdmin/scripts/setup.php
//PMA/scripts/setup.php
//PMA2005/scripts/setup.php
//_online_help.css
//_phpmyadmin/scripts/setup.php
//a2billing/customer/templates/default/footer.tpl
.:
```



QUESTION ONE

WHAT DID WE
OBSERVE?

QUESTION TWO

WHAT'S IN THE LIST
OF TARGETS?




```
DB_PASSWORD=
R1VVpaaUdLIt
MAIL_PASSWORD
CLOUDINARY_AI
GOOGLE_API_KI
REDIS_PASSWO
AMAZON_PASSW
AUTH_KEY='X^
APP_KEY=base
MAILCHIMP_AP
DB_PASSWORD=
MAIL_PASSWORD
NONCE_KEY='+
NOTIFICATION
TRP_FEEDBACK
MAIL_PASSWORD
DB_PASSWORD:
TWITTER_CONSI
DB_PASSWORD=
APP_KEY=UgFDI
GPG_API_PASSI
SQS_SECRET_KI
YMHdQSVRXZkl
WUifQ==
MAIL_PASSWORD
REDIS_PASSWO
GOOGLE_SERVEI
DB_PASSWORD=
MAIL_PASSWORD
APP_KEY=3H3Z
APP_KEY=DHQoi
DB_PASSWORD=
DB_PASSWORD=
DATABASE_PAS
GOOGLE_CAPTCI
DB_PASSWORD=
SECURE_AUTH_I
SQS_KEY=AKIA
AWS_ACCESS_KI
ORDER_MAIL_P
REDIS_PASSWO
WORDPRESS_DB
APP_KEY=iush
AWS_ACCESS_KI
APP_KEY=ejxVI
```

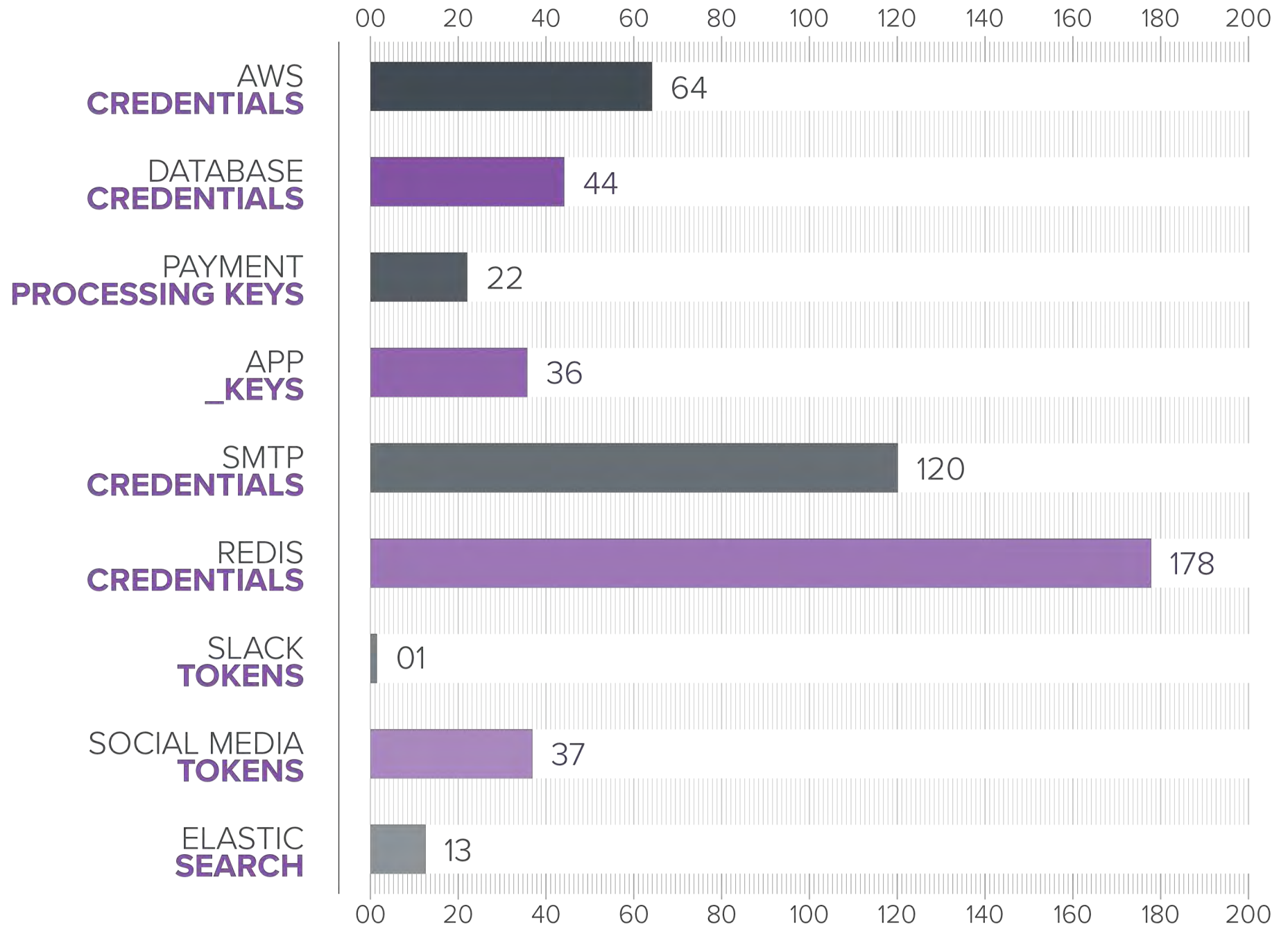
REDACTED



APIKEY=75177
DB_PASSWORD=
APP_KEY=FUxn
MSQC_PASSWORD
APP_KEY=base
MAIL_PASSWORD
LOGGED_IN_KEY
PUSHER_APP_K
PS_COOKIE_KEY
DB_PASSWORD=
AWS_KEY='AKI
GCM_KEY=AAAA
Ofc4dUj7L00U
APIKEY=40800
GOOGLE_API_K
MAIL_PASSWORD
FIREBASE_KEY
DB_PASSWORD=
APP_KEY=base
DB_PASSWORD=
DB_PASSWORD=
AWS_ACCESS_K
APP_KEY=base
DB_PASSWORD=
AWS_S3_KEY=A
APP_KEY=base
APP_KEY=base
APP_KEY=1X5e
APP_KEY=base
API_KEY="AIz
DB_PASSWORD=
DB_PASSWORD=
MAIL_PASSWORD
DB_PASSWORD=
GOOGLE_CAPTCH
APP_FCM_KEY=
M0setHPWZQBS
MAIL_PASSWORD
MAIL_PASSWORD
FB_API_KEY=1
APP_GCM_KEY=
MAIL_PASSWORD
AWS_KEY=AKIA
APP_KEY=base
MAIL_PASSWORD

REDACTED

ELASTICBEANSTALK LOOT



SOURCE CODE LEAK

CRITICAL EXPOSURE

`/.git/config`

Source Code Contains

Encryption Keys

DB Passwords

API Tokens

Internal Systems

Application Vulnerabilities

```
[OK] system/database/drivers/mssql/mssql_driver.php
[OK] system/database/drivers/mssql/mssql_forge.php
[OK] system/database/drivers/mssql/mssql_result.php
[OK] system/database/drivers/mysql/index.html
[OK] system/database/drivers/mssql/mssql_utility.php
[OK] system/database/drivers/mysql/mysql_forge.php
[OK] system/database/drivers/mysql/mysql_driver.php
[OK] system/database/drivers/mysql/mysql_result.php
[OK] system/database/drivers/mysql/mysql_utility.php
[OK] system/database/drivers/mysqli/index.html
[OK] system/database/drivers/mysqli/mysqli_forge.php
[OK] system/database/drivers/mysqli/mysqli_driver.php
[OK] system/database/drivers/mysqli/mysqli_result.php
[OK] system/database/drivers/mysqli/mysqli_utility.php
[OK] system/database/drivers/oci8/index.html
[OK] system/database/drivers/mysqli/mysqli_utility.php
[OK] system/database/drivers/oci8/oci8_driver.php
[OK] system/database/drivers/oci8/oci8_forge.php
[OK] system/database/drivers/odbc/index.html
[OK] system/database/drivers/oci8/oci8_utility.php
[OK] system/database/drivers/oci8/oci8_result.php
[OK] system/database/drivers/odbc/odbc_driver.php
[OK] system/database/drivers/odbc/odbc_forge.php
[OK] system/database/drivers/odbc/odbc_result.php
[OK] system/database/drivers/odbc/odbc_utility.php
[OK] system/database/drivers/pdo/index.html
[OK] system/database/drivers/pdo/pdo_driver.php
[OK] system/database/drivers/pdo/pdo_forge.php
[OK] system/database/drivers/pdo/pdo_result.php
[OK] system/database/drivers/pdo/pdo_utility.php
[OK] system/database/drivers/pdo/subdrivers/index.html
[OK] system/database/drivers/pdo/subdrivers/pdo_4d_driver.php
[OK] system/database/drivers/pdo/subdrivers/pdo_4d_forge.php
[OK] system/database/drivers/pdo/subdrivers/pdo_cubrid_driver.php
[OK] system/database/drivers/pdo/subdrivers/pdo_cubrid_forge.php
[OK] system/database/drivers/pdo/subdrivers/pdo_dblib_driver.php
[OK] system/database/drivers/pdo/subdrivers/pdo_dblib_forge.php
[OK] system/database/drivers/pdo/subdrivers/pdo_firebird_driver.php
[OK] system/database/drivers/pdo/subdrivers/pdo_firebird_forge.php
[OK] system/database/drivers/pdo/subdrivers/pdo_ibm_driver.php
[OK] system/database/drivers/pdo/subdrivers/pdo_ibm_forge.php
[OK] system/database/drivers/pdo/subdrivers/pdo_informix_driver.php
```





HISTORY
CONTENT DISCOVERY
OF YESTERYEARS

CONTENT DISCOVERY 10 YEARS AGO

EVOLVING OLD WAYS

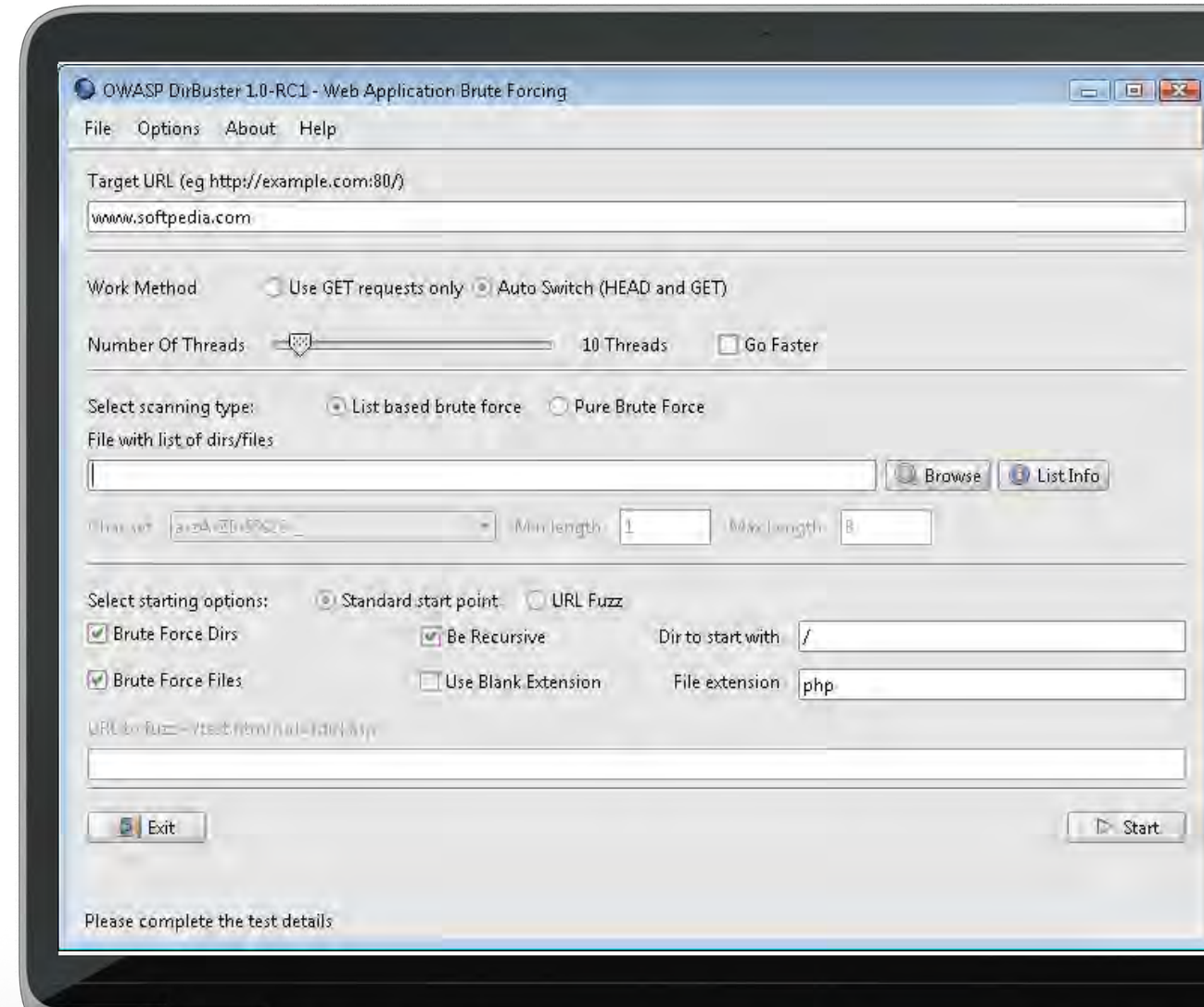
OWASP DirBuster (2008)

Multi-threaded Crawling

Wordlist Path Brute-forcing

Directory

File



Wednesday, January 23, 2019
06:25:40
198.23.249-

CSS

Script

Images

00045247

CONTENT DISCOVERY FAILS

EVOLVING OLD WAYS

/thisdefinitelydoesnotexist

Use “Fail Cases”

Soft 404 Checking

DOM Difference Analysis

Content Length



Great shot, kid. That was one in a million.

Let's get you [back](#).



CONTENT DISCOVERY FAILS

PAINFUL + TIME CONSUMING

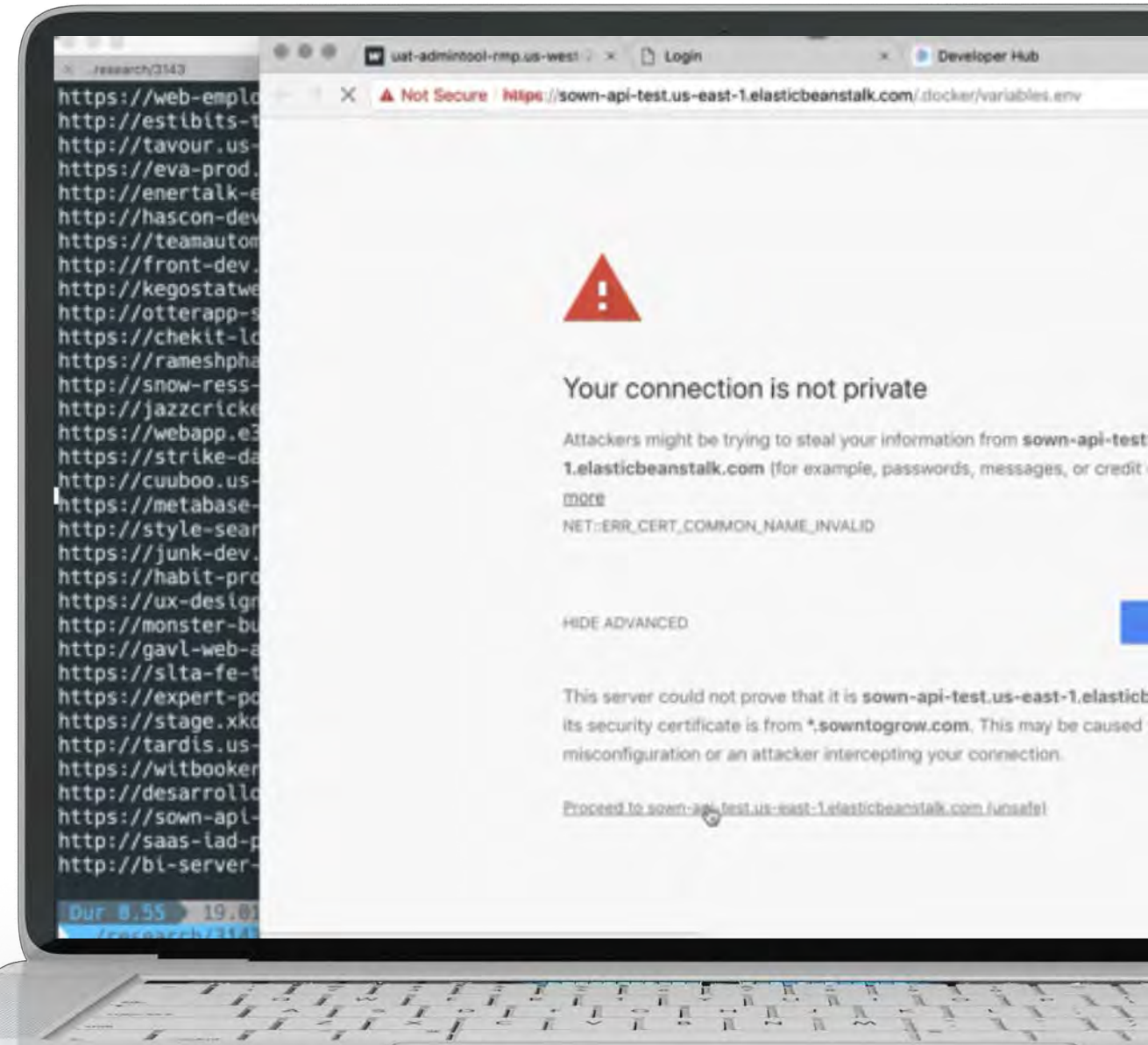
`/.docker/variables.env`

Manual Review

Load Times

SSL Errors

Human Errors



LIKE FINDING A
NEEDLE IN A
HAYSTACK



PROCESS PROBLEMS

CONTENT DISCOVERY 2008 - 2018

INCONSISTENCY – Actions performed pertaining to content discovery during assessments are inconsistent despite the value proposition. It's not feasible to run large-scale comprehensive dictionaries on every target in a small time window using traditional techniques.

DIVERGENCE – Information storage is disparate as new targets are discovered throughout an assessment. Penetration testers often work off of separate datasets and ensuring all targets were reviewed the same way is problematic.

EFFICIENCY – Results validation is time consuming when false positives are too numerous. Too much noise and not enough signal. Dictionaries that are used are often outdated or inefficiently utilized.



CONTENT DISCOVERY + SCREENSHOTS

EVOLVING OLD WAYS

Pre-render Applications

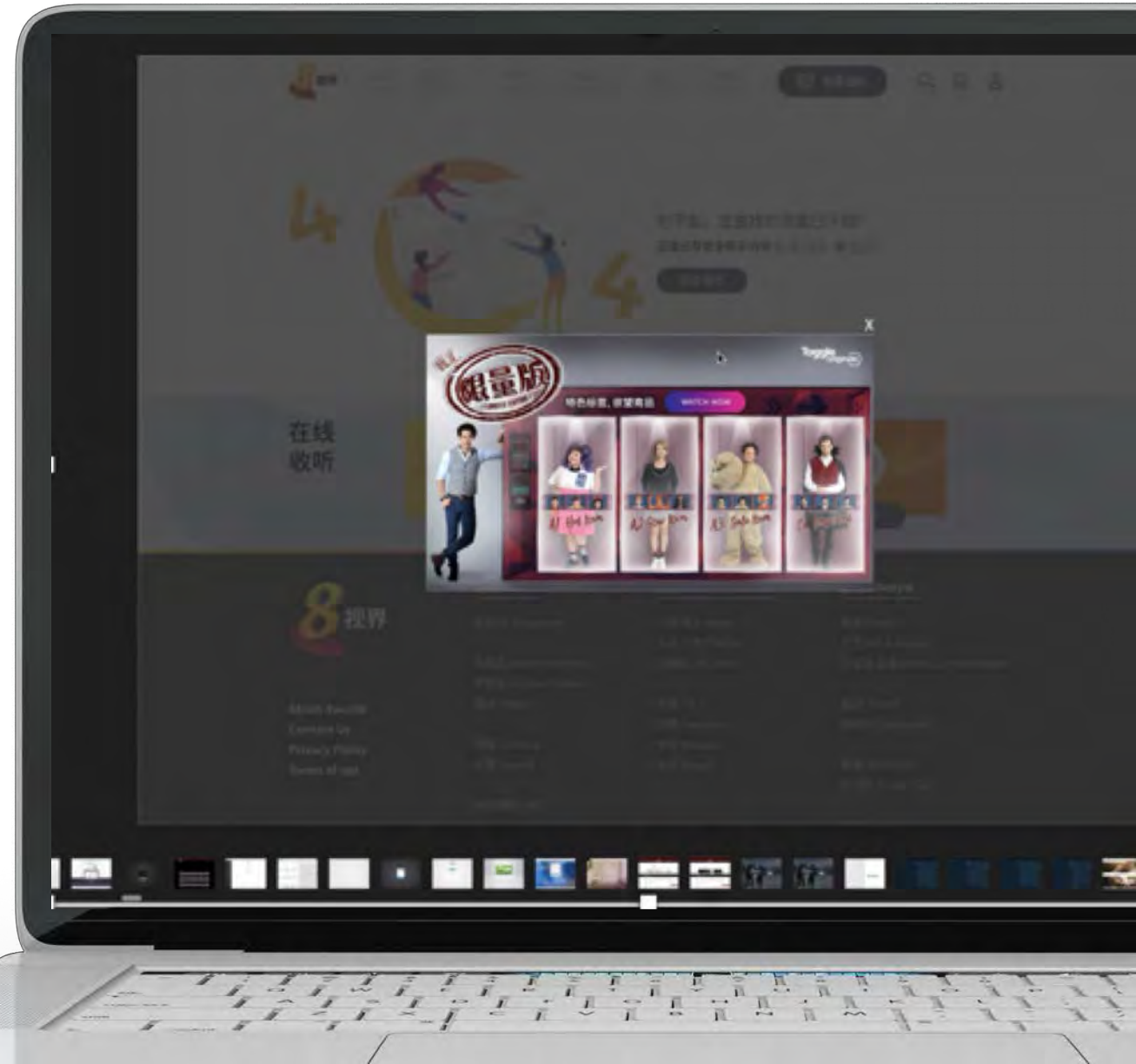
Approximately 100 per minute

Tag for further review

Goal

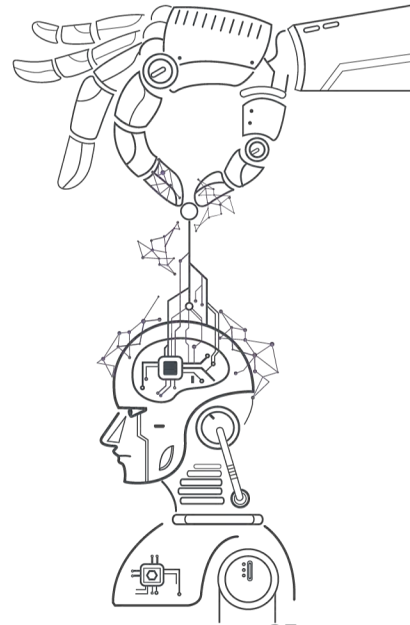
Find Content to Attack

Sensitive Information





HUMANS
ARE NOT THE
SOLUTION



WHAT IF THERE WERE A WAY
TO GET THE
SAME RESULTS...

...WITHOUT HAVING TO DO

404 CHECKING & SIGNATURES...

QUESTION

...AT
SCALE?



EXPLORING
SOLUTIONS FOR
HUMANS



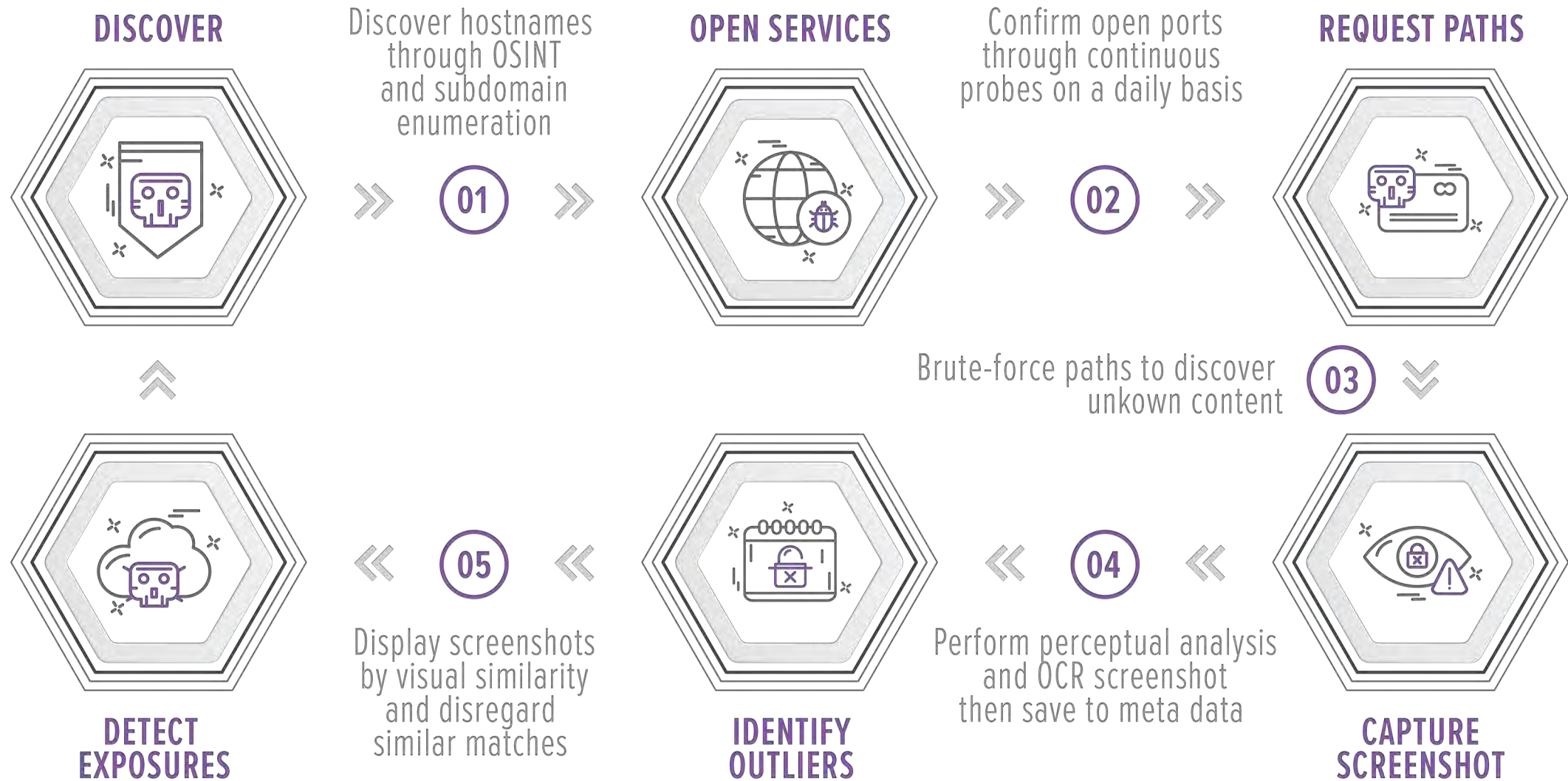
GOAL

MAKE IT EASY
FOR HUMAN

TO GET EYES ON
INTERESTING SCREENSHOTS
FROM URL PATH BRUTE-FORCE

HOW PERCEPTUAL ANALYSIS HELPS BUG HUNTERS

AUTOMATED TRIAGE



TARGET DISCOVERY 2018

DOZENS OF SOURCES

OWASP Amass (2018)

Open Source Intelligence (OSINT)

Scrape web pages with DNS dragnet data

Aggregate Passive DNS API data

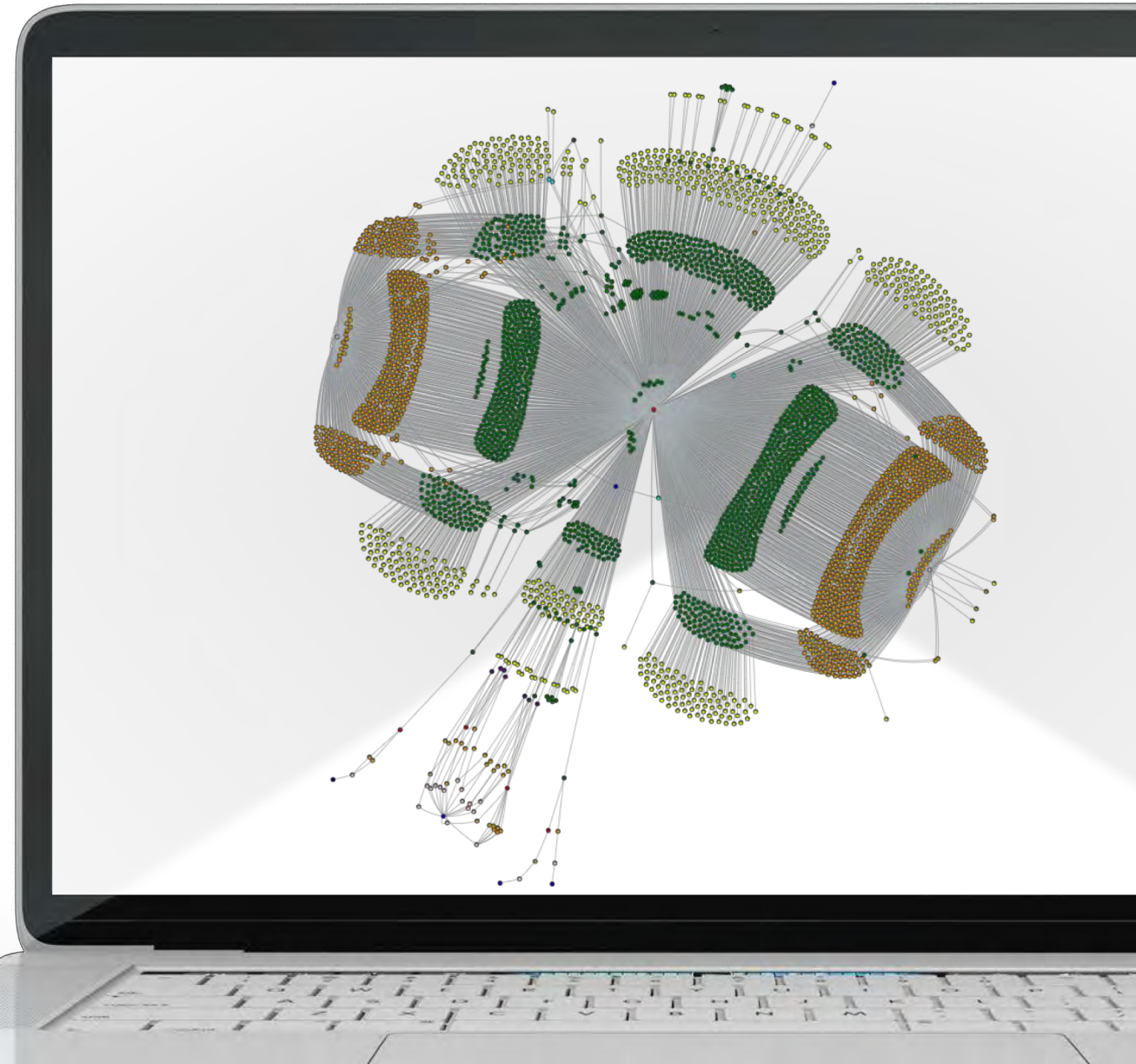
Crawling internet archives

Recursive brute-forcing subdomains

Permutations/alternative character substitutions

Reverse DNS lookups

Querying ASNs and netblocks



TARGET DISCOVERY 2018

DOZENS OF SOURCES

OWASP Amass (2018)

Open Source Intelligence (OSINT)

Scrape web pages with DNS dragnet data

Aggregate Passive DNS API data

Crawling internet archives

Recursive brute-forcing subdomains

Permutations/alternative character substitutions

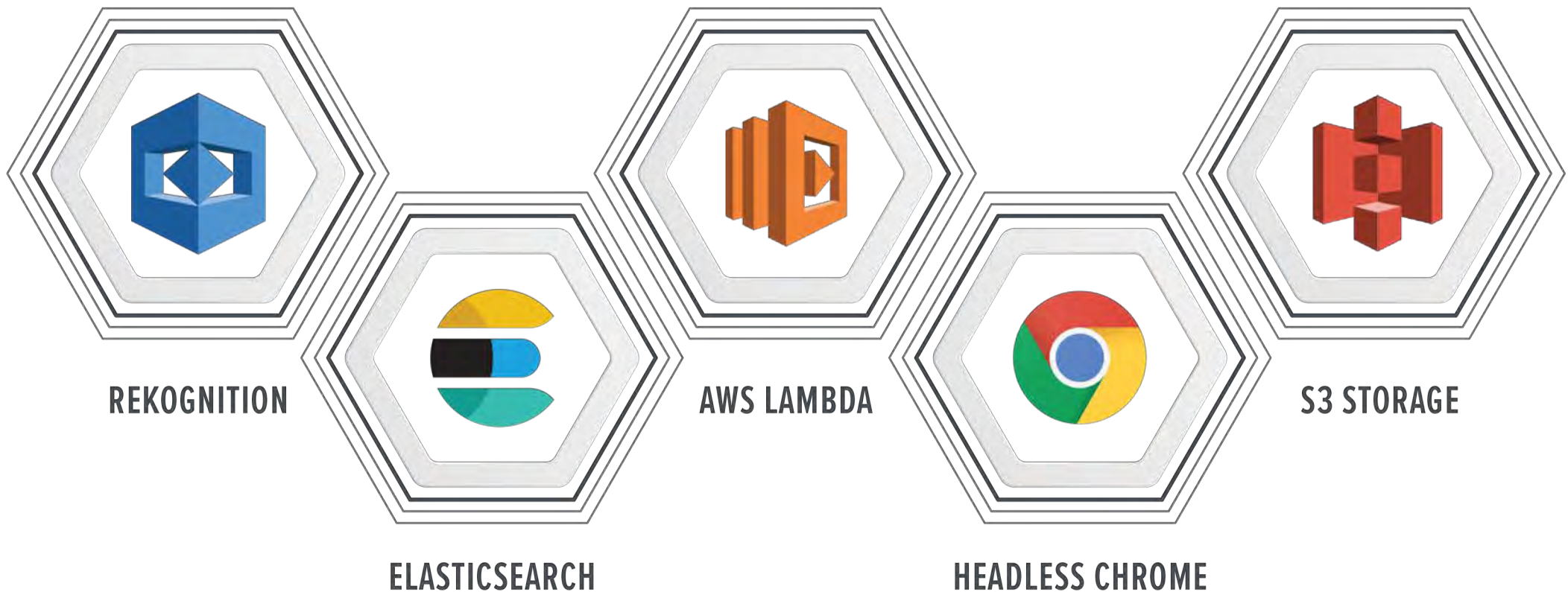
Reverse DNS lookups

Querying ASNs and netblocks

```
001tomacat8-env.2zbpvvy4i7.us-east-1.elasticbeanstalk.com
00-api-ib3alacarta-com.us-east-1.elasticbeanstalk.com
00ldrestdraj.us-west-2.elasticbeanstalk.com
0113t-pro.elasticbeanstalk.com
01test2-env.eu-west-2.elasticbeanstalk.com
03c9acbb-4d65-4544-bc3d-082aa04cc5b4.eu-west-1.elasticbeanstalk.com
05servicetest.us-east-2.elasticbeanstalk.com
07530960-a590-live-beeline-portal.eu-central-1.elasticbeanstalk.com
0f9b429-im-events-staging.us-west-2.elasticbeanstalk.com
1001-env.vj2paiqvay.us-west-2.elasticbeanstalk.com
100internal-env.4vuscgkmb.us-west-1.elasticbeanstalk.com
100internal-env.pinsu7bcza.us-west-2.elasticbeanstalk.com
100-million.us-east-1.elasticbeanstalk.com
101careers.eu-west-1.elasticbeanstalk.com
101-diy-master.ap-southeast-1.elasticbeanstalk.com
10d-idb-console-prod.eu-west-1.elasticbeanstalk.com
10d-idb-console-test.eu-west-1.elasticbeanstalk.com
10d-idb-prod.eu-west-1.elasticbeanstalk.com
10d-idb-test.eu-west-1.elasticbeanstalk.com
10d-tokens-console-prod.eu-west-1.elasticbeanstalk.com
10d-tokens-prod.eu-west-1.elasticbeanstalk.com
10dws-events-prod.eu-west-1.elasticbeanstalk.com
10e4.us-east-2.elasticbeanstalk.com
112-alex.us-east-1.elasticbeanstalk.com
```



TECHNOLOGY STACK







PERCEPTUAL ANALYSIS

WHAT IS IT?

APPROACH

- Reduce size. Shrink the image to a constant in order to ignore size differences
- Reduce color. Convert to grayscale to reduce colors
- Compute difference. Observe difference between adjacent pixels to identify gradient direction and store difference in bits.
- Assign bits. Each bit represents if the left pixel is brighter than the right pixel.

STEPS

- Shrink to 9x8 or 72 pixels
- Convert to 72 colors
- Compute 9 pixel differences or 8 differences per row which becomes 64 bits
- Assign 1 if $P[x] < P[x+1]$ else 0

 =  = 3a6c6565498da525

 <http://api.america.gov>
<http://adrc-tae.acl.gov>
<http://bp.1940census.archives.gov>
<http://dev.my.rd.usda.gov>
<http://dqwiki.arm.gov>
<http://epfup-cat.usps.gov>
<http://epfup.usps.gov>
<http://epfws-cat.usps.gov>
<http://epfws.usps.gov>
<http://external.nmfs.noaa.gov>

Show 41 more URLs

 <https://preview.catalog.usmint.gov>
<https://sso-east.csp.noaa.gov>
<https://sso-north.csp.noaa.gov>
<https://sso-pac.csp.noaa.gov>
<http://azwg.cap.gov>
<http://dev.challenge.gov>
<http://doj.wta.nfc.usda.gov>
<http://fehxd.bea.gov>
<http://fireeye-hxd.bbg.gov>
<http://intranet.lbl.gov>

Show 36 more URLs

 <http://beta.cpsc.gov>
<http://crowd.cms.gov>
<http://dcmstg.sec.gov>
<http://dev.edit.cms.gov>
<http://dev1.cms.gov>
<http://dev2.cms.gov>
<http://edit-beta.tsa.gov>
<http://edit.cbp.gov>
<http://edit.osha.gov>
<http://edit.tsa.gov>

Show 38 more URLs



<http://access.nsf.gov>
<http://accessdev.nsf.gov>
<http://entry.eiavpngw.eia.gov>
<http://remote.pnl.gov>
<http://remote.pnnl.gov>
<http://remote1.pnl.gov>
<http://vpn.llnl.gov>
<http://vpna.llnl.gov>
<http://vpnb.llnl.gov>
<http://vpndev1.llnl.gov>

Show 38 more URLs

FUTURE ENHANCEMENTS

OCR OF SCREENSHOTS

- To perform inclusive AND exclusive filtering based on text

ML

- To perform unsupervised categorization of screenshots and supervised training for valid consumer facing

COLLABORATIVE FILTERING

- To manage human analysis in real-time & centralize results





CONCLUSION

THANK YOU
FOR YOUR TIME