

Analysis of Free Movies and Series Websites Guided by User Search Terms

Botconf 2016 - Lyon, France



Luis Alberto Benthin Sanguino, Martin Clauß
luis.alberto.benthin.sanguino@fkie.fraunhofer.de
martin.clauss@fkie.fraunhofer.de

CA&D | Cyber Analysis and Defense

- 1 Motivation**
- 2 Evaluation Method**
- 3 Results**
- 4 Conclusion**

- 1. Why do we analyse websites?**
- 2. Why a reduced subset of the web?**
- 3. Why Free Movies and Series (FMS) websites?**

1. Why do we analyse websites?

- Websites used by cybercriminals to infect users with malware

⇒ **Why do cybercriminals use websites as infection vector?**

- **Efficient**

- Massive number of possible victims

- **Effective**

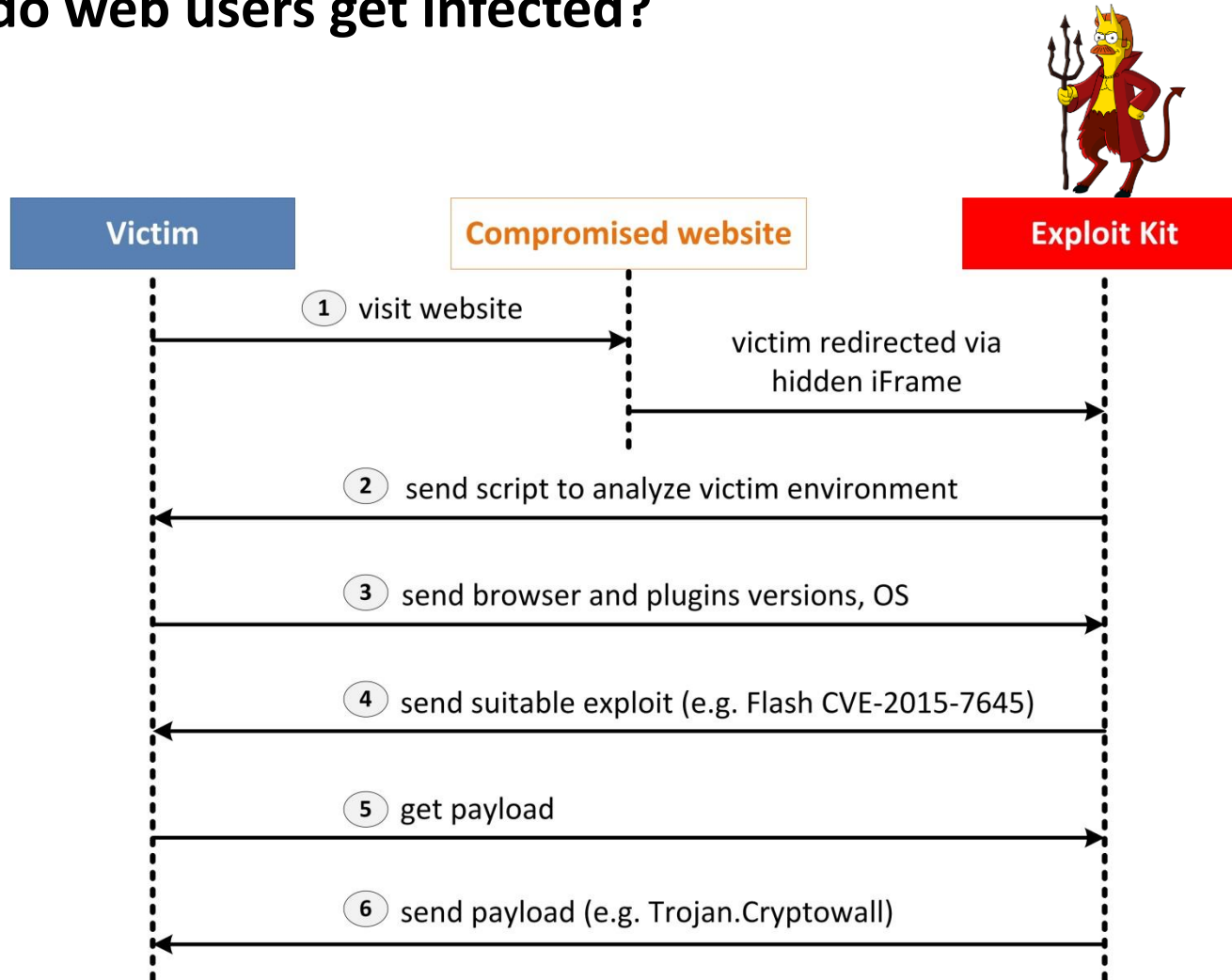
- **Server side** Legitimate websites can be compromised

- Via e.g. vulnerable CMS

- **Client side** Web users can be infected

- Via vulnerable versions of e.g. IE, Flash, PDF

■ How do web users get infected?



2. Why do we focus on a subset of the web?

- 5 billion pages and 1.1 billion websites [1, 2]
 - ⇒ Detection and analysis resources must be spent efficiently

3. Why Free Movies and Series (FMS) websites?

- Free entertainment content attract millions of web users
 - Why to pay, if it can be obtained for free?
- Cybercriminals use free services websites to expose users to malware
- Manual analysis showed that FMS websites try to trick users
 - Malicious Flash installer
 - Malicious video converter
 - Possible scam

[1] <http://www.worldwidewebsite.com>


[2] <http://www.internetlivestats.com/total-number-of-websites>

VEZI ONLINE Cauta filme, seriale, actori...

Home Filme Filme dupa gen Filme dupa ani Seriale Actori Film aleator Contact

NARCOS S02E10 – AL FIN CAYÓ! Like Share 6 people like this.

◀ Episodul anterior


Please click on this button to open this video

Sursa 1 Sursa 2 Sursa 3 Download

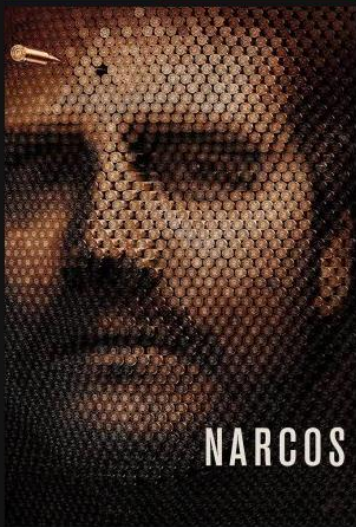
SINOPSIS NARCOS S02E10 – AL FIN CAYÓ!


Vezi Narcos S02E10 – Al Fin Cayó online subtitrat. Vizionare placuta!

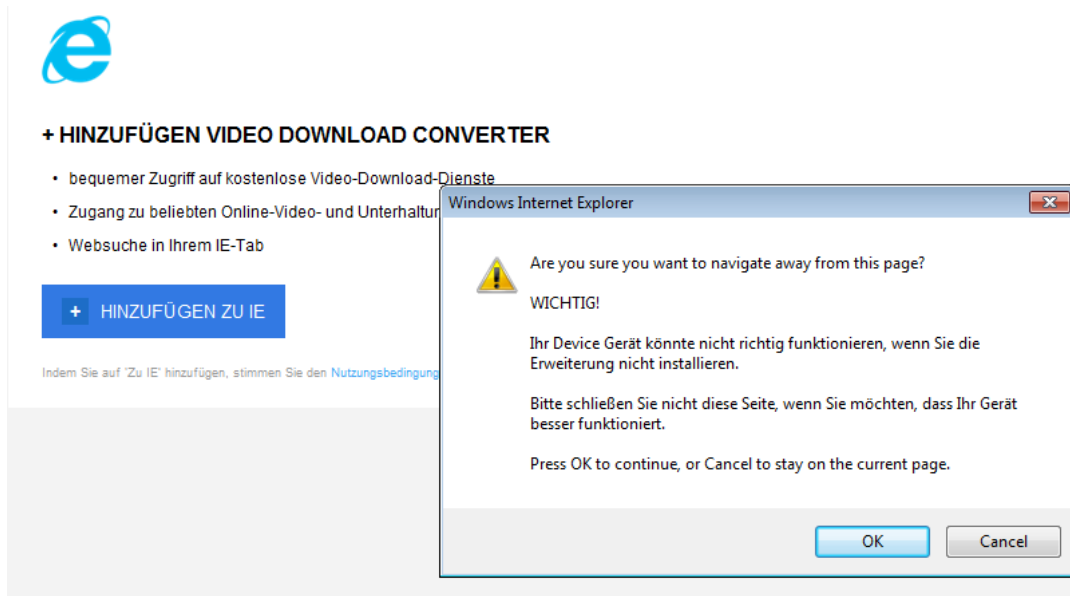
Twitter Facebook Google+ Comentarii

Lipseste episodul? Lasa-ne un mesaj in formularul de mai jos!
Episodul nu se incarca? Da play la episod si apoi pauza, asteapta cateva minute pentru a se incarca

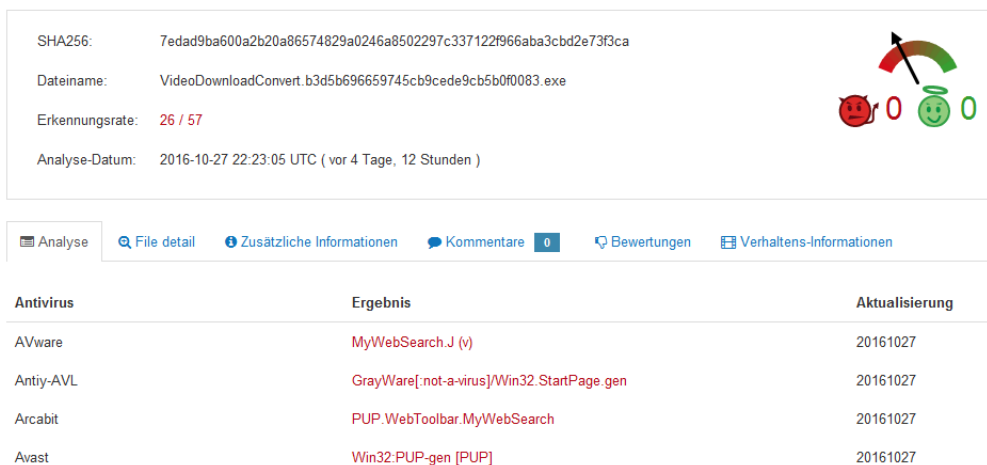
POSTER SERIAL


NARCOS


SEX AND THE CITY
DIAVOLITA
VIBRATOARE
DILDO
BUTT PLUG
STRAPON
BILE GHEISA
POMPE MARIRE



The screenshot shows a web browser window with a blue header bar. Below the header, there is a section titled "+ HINZUFÜGEN VIDEO DOWNLOAD CONVERTER". This section contains a list of bullet points: "bequemer Zugriff auf kostenlose Video-Download-Dienste", "Zugang zu beliebten Online-Video- und Unterhaltung", and "Websuche in Ihrem IE-Tab". Below the list is a blue button with a white plus sign and the text "HINZUFÜGEN ZU IE". Underneath the button, there is a small line of text: "Indem Sie auf 'Zu IE' hinzufügen, stimmen Sie den Nutzungsbedingung". Overlaid on the right side of the browser window is a Windows Internet Explorer warning dialog box. The dialog box has a yellow warning icon and the text: "Are you sure you want to navigate away from this page?", "WICHTIG!", "Ihr Device Gerät könnte nicht richtig funktionieren, wenn Sie die Erweiterung nicht installieren.", "Bitte schließen Sie nicht diese Seite, wenn Sie möchten, dass Ihr Gerät besser funktioniert.", and "Press OK to continue, or Cancel to stay on the current page." At the bottom of the dialog box are two buttons: "OK" and "Cancel".



The screenshot shows the VirusTotal analysis results for a file. The file name is "VideoDownloadConvert.b3d5b696659745cb9cede9cb5b0f0083.exe". The SHA256 hash is "7edad9ba600a2b20a86574829a0246a8502297c337122f966aba3cbd2e73f3ca". The detection rate is "26 / 57". The analysis date is "2016-10-27 22:23:05 UTC (vor 4 Tage, 12 Stunden)". To the right of the file information is a circular progress indicator with a red arrow pointing to the right, and two smiley face icons, one red and one green, with the number "0" next to each. Below the file information is a navigation bar with tabs: "Analyse", "File detail", "Zusätzliche Informationen", "Kommentare", "Bewertungen", and "Verhaltens-Informationen". Below the navigation bar is a table with three columns: "Antivirus", "Ergebnis", and "Aktualisierung". The table contains five rows of data:

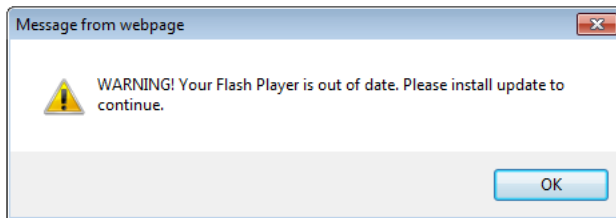
Antivirus	Ergebnis	Aktualisierung
AVware	MyWebSearch.J (v)	20161027
Antiy-AVL	GrayWare[.not-a-virus]/Win32.StartPage.gen	20161027
Arcabit	PUP.WebToolbar.MyWebSearch	20161027
Avast	Win32:PUP-gen [PUP]	20161027

Adobe Flash Player Update

Adobe Flash Player Update

The new version of "Adobe Flash Player" is ready to download.
This new version include the latest security features.

To use the new version, download and install now (Recommended)



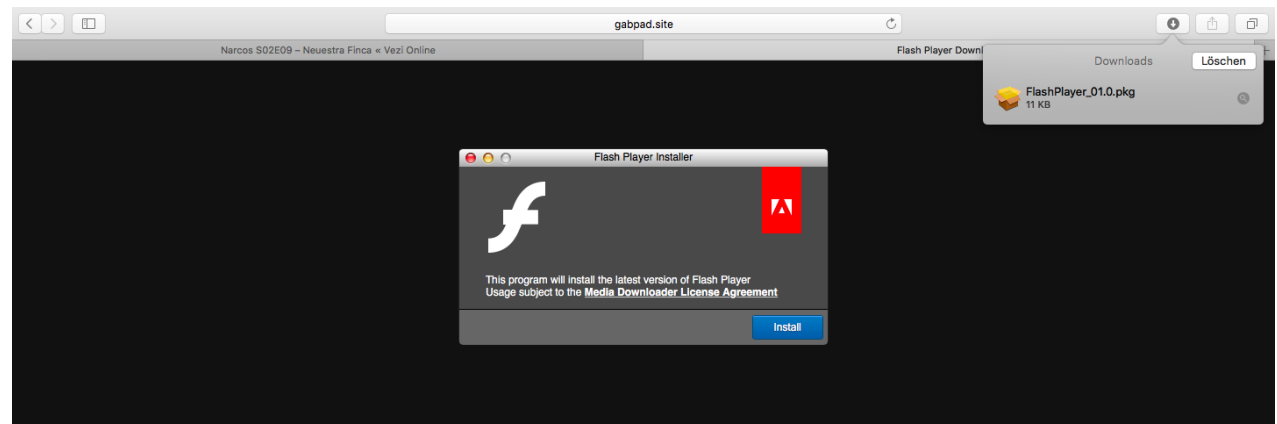
virustotal

SHA256: a785f4a2d12c8df69307ecea082074fa6cf0c068a2e732e73234c0301e35e0fe
Dateiname: adobe_flash_setup.exe
Erkennungsrate: 13 / 56
Analyse-Datum: 2016-11-01 10:41:14 UTC (vor 0 Minuten)




Analyse File detail Zusätzliche Informationen Kommentare Bewertungen


Antivirus	Ergebnis	Aktualisierung
AVG	Generic.F15	20161101
Antiy-AVL	GrayWare[Adware]/Win32.InstallCore.gena	20161101
Bkav	W32.HfsAdware.8CF1	20161031
CAT-QuickHeal	PUA.Oookod.Gen	20161101



appless.store/mk/22.php?c1=1467877&c2=General/Arts/Movies&c3=4&c4=0.005

es « Vezi Online VIRUS FOUND

 **VIRUS FOUND**

 Eine von Ihnen heute besuchte Webseite hat Ihr Gerät mit einer kompletter Systems캔 ist erforderlich, um gefährliche Dateien zu finden und von Ihrem Gerät zu entfernen.

Jetzt scannen

weekly-prizes.co

Pepes « Vezi Online VIRUS FOUND

MediaMarkt Kunden Geschenke

Herzlichen Glückwunsch Desktop-Nutzer! Ihr Desktop hat einen Preis MediaMarkt gewonnen!
November 01, 2016
Nur heute, an diesem Dienstag, vergeben wir fünf Preise (im Wert von bis zu € 749) an zehn glückliche Kunden.
Wenn Sie vier Fragen in zwei Minuten korrekt beantworten, erhalten Sie Ihren!
Beileitung, zwei Nutzer haben ihren Preis bereits erhalten, nur (3) sind noch übrig.
Sie haben **1 Minuten 59 Sekunden** um die Fragen zu beantworten, bevor jemand anders Ihren Platz einnimmt. Viel Glück!

Herzlichen Glückwunsch Desktop Nutzer!

Sie wurden von MediaMarkt ausgewählt und sind einer der wenigen erste ein iPhone 7 oder andere MediaMarkt Preise gewinnen!! Dieses Geschenk ist exklusiv und nur für Desktop treuen Nutzern Germany.


Bitte bestätigen Sie, dass Sie der Besitzer dieses Desktop Handy sind, indem Sie auf OK.

Schließen

ad.fun-chat.com

narcoes « Resultate durch « Vezi Online FUNCHAT

Finde nette
**Girls, Boys
und Paare**
aus deiner
**Umgebung
im Live-Chat**



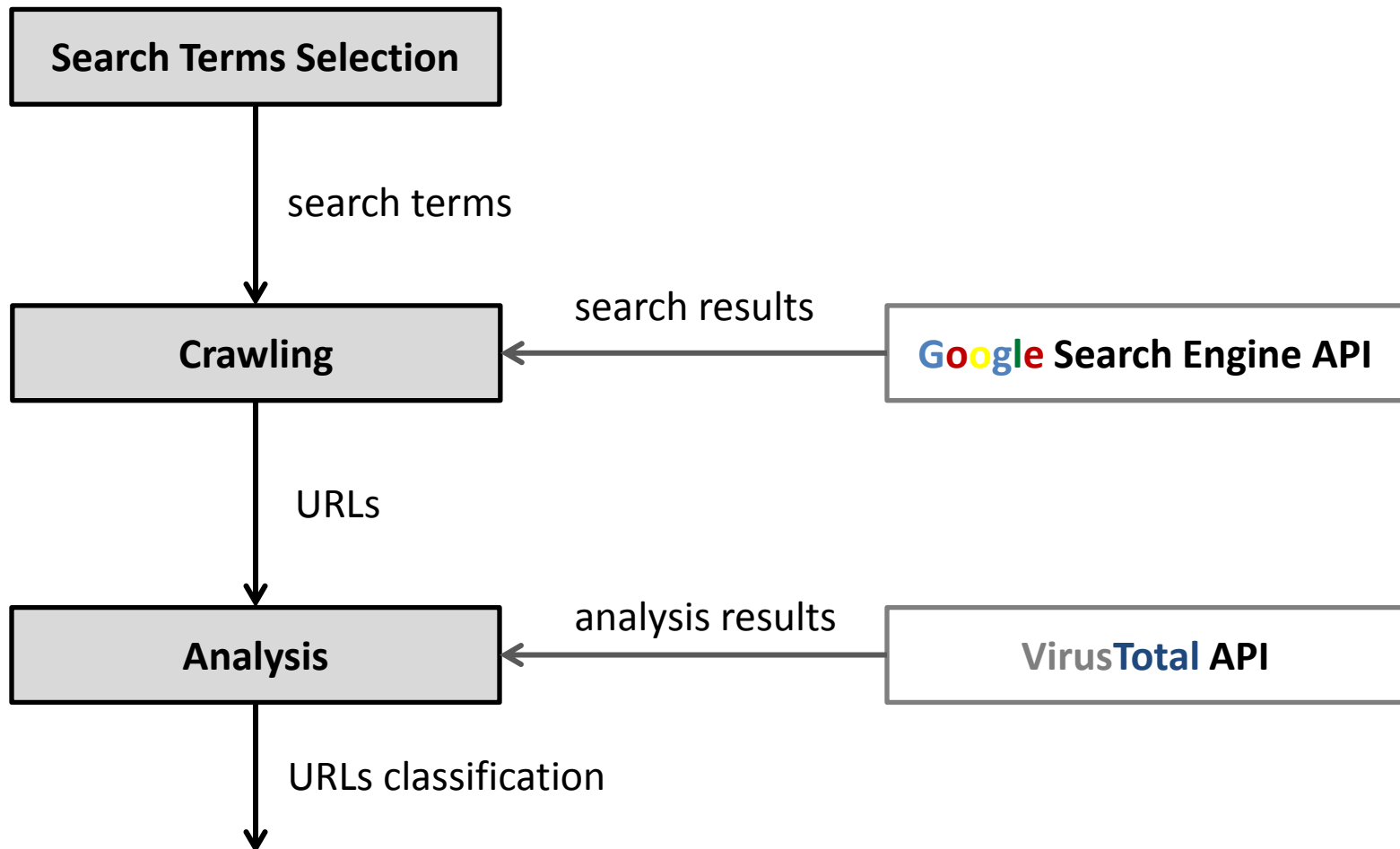
JETZT STARTEN

2013 Fun-chat - All Rights Reserved

Goals of our research
















1. **Hypothesis:** FMS websites are more dangerous than other web categories
2. Approach to analyze potentially malicious websites categories guided by **user search terms**
3. Easy-to-implement infrastructure to analyze website categories

3-Phase method



Search terms selection – FMS category

1. Native speaker search terms

	filme kostenlos		
	watch series online		
	películas con subtítulos en español		
	vezi filme online cu Subtitrari		
	смотреть сериалы онлайн бесплатно		

- **Output 25 search terms**

Search terms selection – FMS category

2. Google Trends



- **Output** 50 search terms

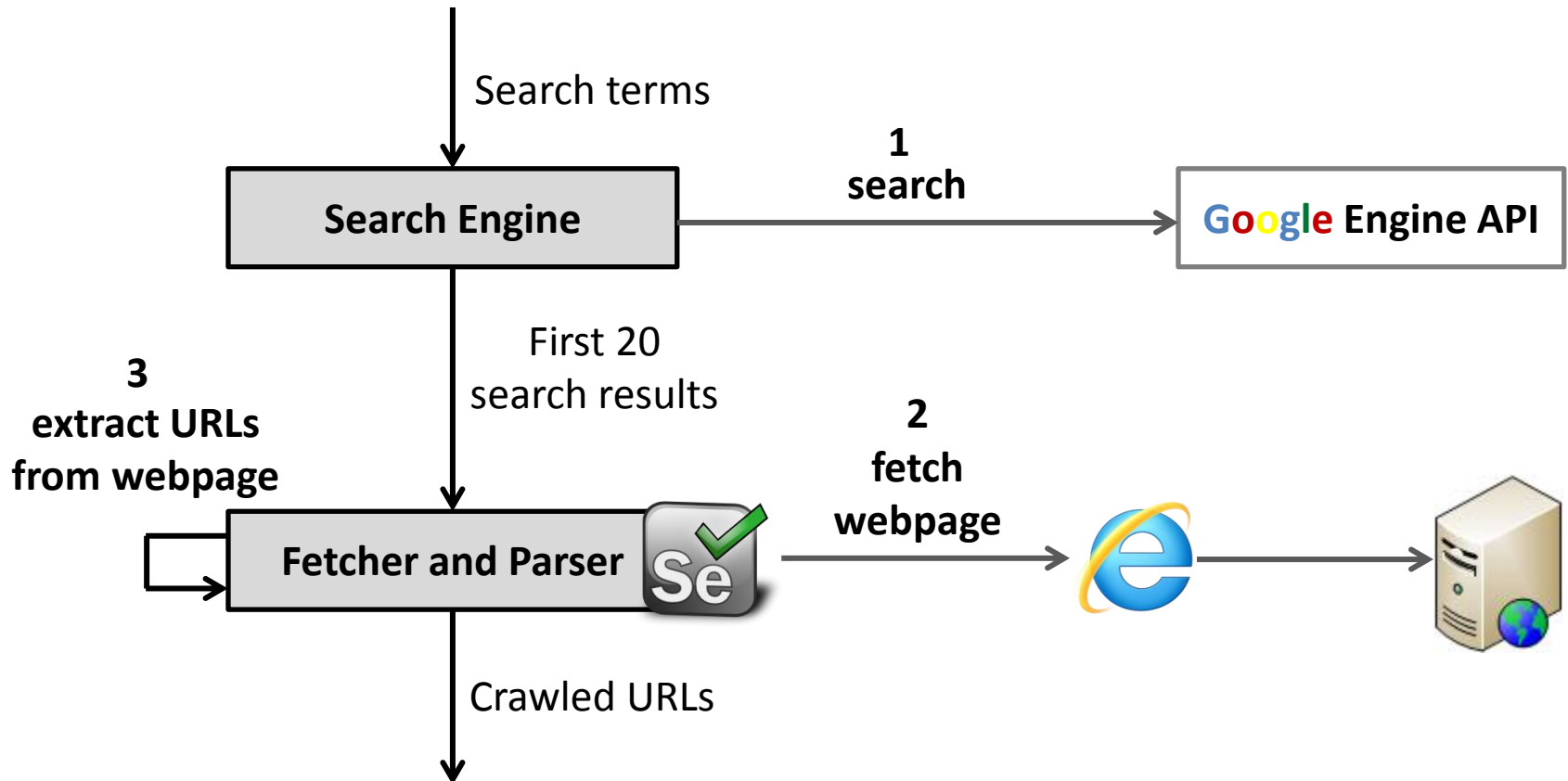
Search terms selection – Other categories

- **Google Trends (GT15) 2015 report**

Category	Search term e.g.	Category	Search term e.g.
1. Music Artists	Adele	4. Loss	Bobbi Kristina
2. Global News	Charlie Hebdo	5. Consumer Tech	iPhone 6S
3. Sporting Events	Copa America	6. People	Lamar Odom

- **Output 60 search terms**

Phase 2: Crawling



 **Selenium:** web browser automation tool, <http://docs.seleniumhq.org/>.

Phase 3: Analysis



Interpretation of VirusTotal Results

- **Positives**

- Number of scanners that classified a URL as:
 - malicious site
 - malware site
 - phishing site

- **Positive URL**

- positives > 0

- **Positive Rate**

- Percent of positive URLs in relation with the number of analyzed URLs

FMS Category

	Scanned	# Positives	Positive Rate (%)
URLs	18110	1261	6.96
Domains	1157	117	10.11

URLs

Lang.	Positive Rate (%)
ES	11.35
RO	9.25
EN	8.16
RU	3.66
DE	0.34

Domains

Lang.	Positive Rate (%)
ES	13.27
RO	13.13
RU	11.64
EN	11.11
DE	3.36

GT15 Categories

	Scanned	# Positives	Positive Rate (%)
URLs	34793	178	0.51
Domains	3103	33	1.06

URLs

Category	Positive Rate (%)
Music artists	1.89
Consumer tech	0.79
Sporting events	0.21
People	0.19
Loss	0.14
Global news	0.11

Domains

Category	Positive Rate (%)
Consumer tech	3.10
Music artists	1.55
Global news	1.18
Sporting events	1.09
Loss	0.84
People	0.60

FMS category vs. GT15 categories

URLs

Category	Positive Rate (%)
FMS	6.96
GT15	0.51

Domains

Category	Positive Rate (%)
FMS	10.11
GT15	1.06

Positive Domain Geolocation - FMS Category

- **38 % hidden** behind **CloudFlare** [3] DNS service
 - We uncovered 57 % using **CrimeFlare** [4] database
- EU 36 %
- USA 32 %
- Russia 9 %

[3] <https://www.cloudflare.com>

[4] <http://www.crimeflare.com>

Conclusions

- ✓ FMS category more malicious than GT15 categories
 - Hypothesis proven
- ✓ Analysis based on real user search terms
 - Analyzed websites are likely to be visited by web users
- ✓ Spanish search terms with the highest positive rate
- ✓ Proposed method requires low-computational costs to be implemented

Future work

- Determine the causes why FMS websites were classified as malicious
- Why ES search terms have the highest positive rate?

Thank you!



Luis Alberto Benthin Sanguino, Martin Clauß
luis.alberto.benthin.sanguino@fkie.fraunhofer.de
martin.clauss@fkie.fraunhofer.de

CA&D | Cyber Analysis and Defense