



XXI
SBSeg
2021
Belém - PA

Freki

Uma Ferramenta para Análise Automatizada de Malware

Cristian Souza - IFRN

Felipe Dantas - IFRN

Agenda

- 1 – Introdução
- 2 – Objetivos
- 3 – O Freki
- 4 – Funcionalidades
- 5 – Demonstração
- 6 – Conclusão

Introdução



Global Windows malware detections increased by 13% on business endpoints



Rise in pre-installed malware and adware on Android devices



For the first time ever, Macs outpaced Windows PCs in number of threats detected per endpoint

- Infecções por *malware* continuam sendo uma das principais ameaças aos sistemas computacionais.
- Em 2020 foi constatado um aumento de 13% nas detecções de *malware* focado no setor corporativo.
- Atividades de *ransomware* estão sendo cada vez mais utilizadas por cibercriminosos.
- Infecções por *adwares* em dispositivos móveis cresceram significativamente.

Fonte: https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report-1.pdf

Introdução

- Visando entender o funcionamento do programa malicioso, são executadas análises estáticas e dinâmicas.
- Análise estática: coleta de informações sobre o binário sem executá-lo.
Exemplos: Tipo de arquivo, *hashes*, *strings*, cabeçalhos, seções...
- Análise dinâmica: execução do artefato em um ambiente controlado.
Exemplos: Requisições, arquivos baixados, arquivos criados, chamadas de sistema, processos...

Introdução

- Análise estática:

```
$ sha256sum mimikatz.exe
92804faab2175dc501d73e814663058c78c0a042675a8937266357bcfb96c50 mimikatz.exe
$ xxd mimikatz.exe | head -n 20
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ.....
00000010: b800 0000 0000 0000 4000 0000 0000 0000  .....@.....
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000030: 0000 0000 0000 0000 0000 0000 2001 0000  .....
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  .....!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode...$.
00000080: 34c8 d822 70a9 b671 70a9 b671 70a9 b671  4.."p..qp..qp..q
00000090: 79d1 2371 72a9 b671 79d1 3571 4fa9 b671  y.#qr..qy.5q0..q
000000a0: 79d1 3271 60a9 b671 79d1 2571 72a9 b671  y.2q`.qy.%qr..q
000000b0: 6b34 2a71 72a9 b671 1647 7d71 74a9 b671  k4*qr..q.G}qt..q
000000c0: eb42 7d71 72a9 b671 0634 db71 72a9 b671  .B}qr..q.4.qr..q
000000d0: 6efb 3271 72a9 b671 0634 cd71 5fa9 b671  n.2qr..q.4.q_.q
000000e0: 70a9 b771 0aab b671 576f c871 71a9 b671  p..q...qWo.qq..q
000000f0: 79d1 3f71 13a9 b671 79d1 2271 71a9 b671  y.?q..qy."qq..q
00000100: 79d1 2771 71a9 b671 5269 6368 70a9 b671  y.'qq..qRichp..q
00000110: 0000 0000 0000 0000 0000 0000 0000 0000  .....
00000120: 5045 0000 6486 0600 6339 5a5e 0000 0000  PE..d...c9Z^....
00000130: 0000 0000 f000 2200 0b02 0900 002c 0c00  ....."
```

- Análise dinâmica:

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	95.26	0 K	24 K		
System	4	0.21	184 K	1,664 K		
smss.exe	404		596 K	460 K		
csrss.exe	552	< 0.01	2,472 K	2,336 K		
wininit.exe	624		1,696 K	360 K		
services.exe	680		6,720 K	6,076 K		
svchost.exe	828		5,744 K	5,516 K	Host Process for Windows S...	Microsoft Corporation
explorer.exe	3104	0.03	88,424 K	85,188 K	Windows Explorer	Microsoft Corporation
Process Explorer Portable (P...	7832	< 0.01	37,960 K	1,992 K	Process Explorer Portable (P...	PortableApps.com
procexp.exe	7984		2,404 K	7,504 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64...	7840	0.41	15,292 K	28,200 K	Sysinternals Process Explorer	Sysinternals - www.sysinter...
WmiPrvSE.exe	7812		3,220 K	6,592 K		
svchost.exe	904	< 0.01	5,196 K	5,332 K	Host Process for Windows S...	Microsoft Corporation
MsMpEng.exe	964	0.05	80,024 K	64,300 K	Antimalware Service Execut...	Microsoft Corporation
atiesnox.exe	844		1,760 K	684 K	AMD External Events Servic...	AMD
atiecbox.exe	1512		2,768 K	1,048 K		
svchost.exe	980		21,372 K	12,628 K	Host Process for Windows S...	Microsoft Corporation
audiogd.exe	4948		18,704 K	14,396 K		
svchost.exe	1060	< 0.01	156,408 K	148,924 K	Host Process for Windows S...	Microsoft Corporation
WUDFHost.exe	2616		2,372 K	3,744 K		
dwm.exe	340	0.09	46,228 K	43,472 K	Desktop Window Manager	Microsoft Corporation
svchost.exe	1104	< 0.01	30,468 K	25,480 K	Host Process for Windows S...	Microsoft Corporation
UnsignedThemesSvc.exe	1140		1,816 K	544 K	Unsigned Themes Service	The Within Network, LLC
svchost.exe	1252	< 0.01	10,648 K	11,592 K	Host Process for Windows S...	Microsoft Corporation
svchost.exe	1424	< 0.01	18,384 K	10,264 K	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe	1588		6,628 K	3,748 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1620		21,372 K	11,648 K	Host Process for Windows S...	Microsoft Corporation
amsmvc.exe	1740		1,232 K	500 K	Adobe Acrobat Update Servi...	Adobe Systems Incorporated
...	1788	< 0.01	47,920 K	122,220 K

CPU Usage: 4.74% | Commit Charge: 48.27% | Processes: 75 | Physical Usage: 71.66%

Introdução

- Algumas ferramentas automatizadas existentes:



- Deficiências:

Plataformas fechadas.

Ausência de *deploy* local.

Exposição do arquivo analisado.

APIs limitadas.

Objetivos

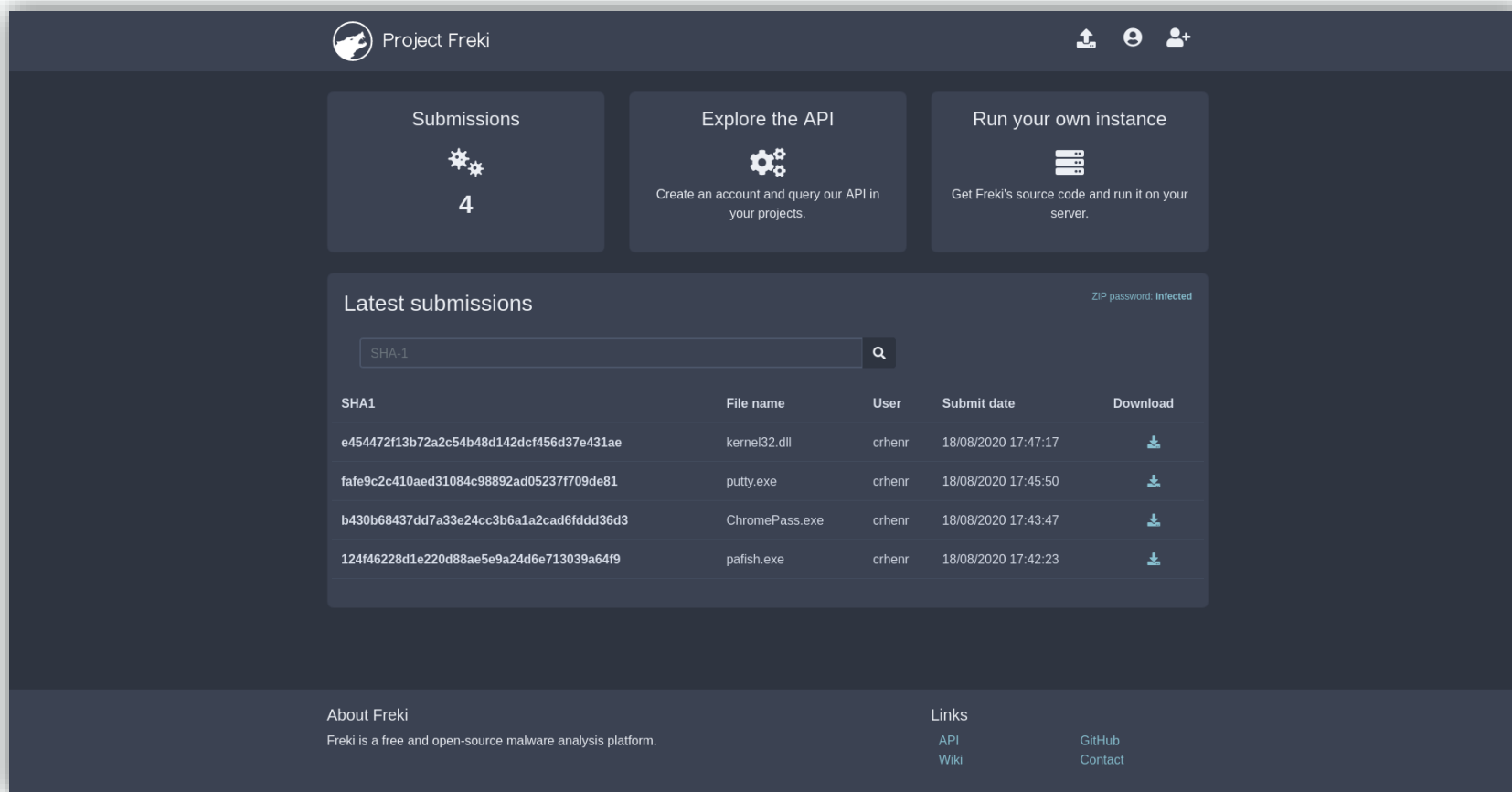
- Facilitar a análise de malware e engenharia reversa.
- Prover uma API de fácil utilização em diferentes projetos.
- Fácil implantação: Via Docker.
- Desenvolvimento de uma ferramenta *open-source*.

Novas funcionalidades podem ser facilmente adicionadas pela comunidade.

Licença AGPL.

Código fonte disponível em: <https://github.com/crhenr/freki>

- Plataforma *open-source* para análise de malware e engenharia reversa.

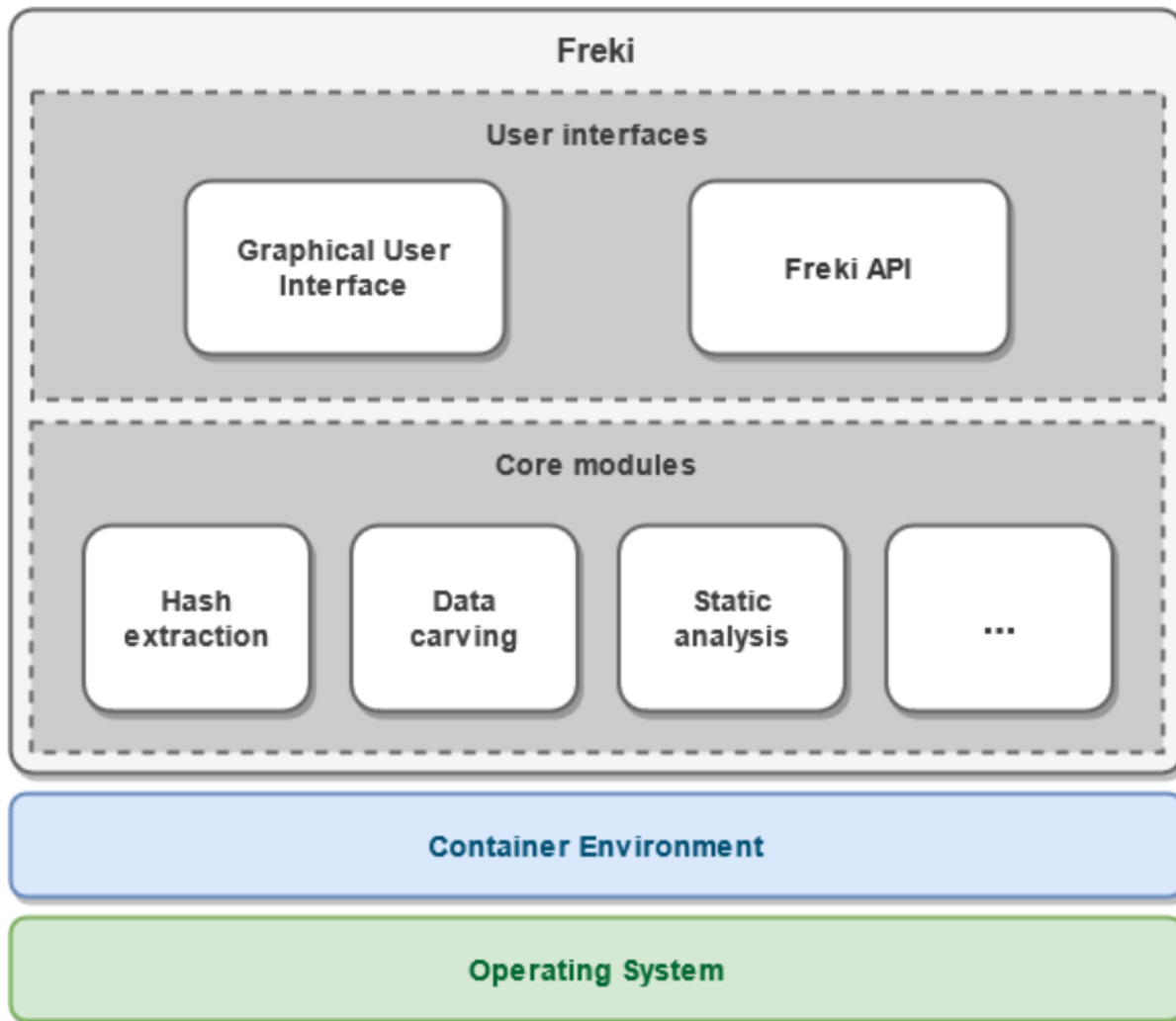


The screenshot displays the Project Freki web interface. At the top, there is a navigation bar with the Project Freki logo and icons for upload, search, and user profile. Below the navigation bar, there are three main action cards: 'Submissions' with a gear icon and the number '4', 'Explore the API' with a gear icon and the text 'Create an account and query our API in your projects.', and 'Run your own instance' with a server rack icon and the text 'Get Freki's source code and run it on your server.' Below these cards is a 'Latest submissions' section with a search bar labeled 'SHA-1' and a magnifying glass icon. To the right of the search bar, it says 'ZIP password: infected'. Below the search bar is a table with the following columns: SHA1, File name, User, Submit date, and Download. The table contains four rows of submission data.

SHA1	File name	User	Submit date	Download
e454472f13b72a2c54b48d142dcf456d37e431ae	kernel32.dll	crhenr	18/08/2020 17:47:17	Download
fafe9c2c410aed31084c98892ad05237f709de81	putty.exe	crhenr	18/08/2020 17:45:50	Download
b430b68437dd7a33e24cc3b6a1a2cad6fddd36d3	ChromePass.exe	crhenr	18/08/2020 17:43:47	Download
124f46228d1e220d88ae5e9a24d6e713039a64f9	pafish.exe	crhenr	18/08/2020 17:42:23	Download

At the bottom of the interface, there is a footer section with 'About Freki' (Freki is a free and open-source malware analysis platform.), 'Links' (API, Wiki), and 'GitHub' (Contact).

O Freki: Arquitetura



- Principais componentes:

1 - User Interface (UI).

2 - REST API.

3 - Core Modules:

Extração de hashes.

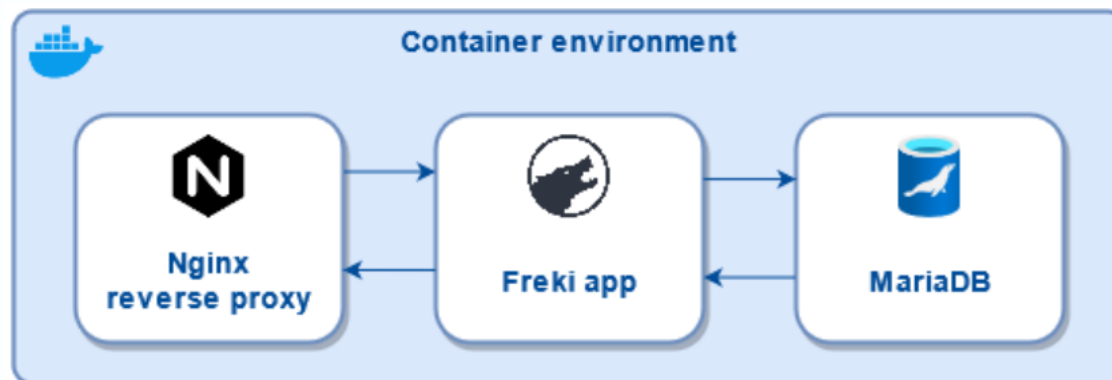
Consultas ao VirusTotal.

Análise estática.

Data carving.

Classificação do binário.

O Freki: Arquitetura



Funcionalidades

- Extração de *hashes*: MD5, SHA-1, SHA-256, SHA-384, SHA-512, CRC32 e SSDEEP.
- Consultas ao VirusTotal: Resultados das análises providas pela ferramenta.
- Análise estática de arquivos PE: Cabeçalhos, seções, importações, capacidades e *strings*.
- Identificação de padrões via Yara.
- Download de artefatos.
- Gerenciamento de usuários e comentários da comunidade.

Funcionalidades

- *Deploy* via Docker:
 1. `git clone https://github.com/crhenr/freki.git`
 2. Configure as credenciais no arquivo `.env` localizado na raiz do projeto
 3. É recomendável habilitar o HTTPS copiando o certificado e a chave privada no diretório `docker/nginx/certs`
 4. Execute a ferramenta: `make run` ou `docker-compose up -d`

Funcionalidades

```
$ git clone https://github.com/crhenr/freki.git
Cloning into 'freki'...
remote: Enumerating objects: 939, done.
remote: Counting objects: 100% (19/19), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 939 (delta 7), reused 10 (delta 4), pack-reused 920
Receiving objects: 100% (939/939), 14.10 MiB | 2.96 MiB/s, done.
Resolving deltas: 100% (262/262), done.
$ cd freki
$ docker-compose up -d
Creating network "freki_frekinet" with driver "bridge"
Creating freki_db ... done
Creating freki ... done
Creating freki_nginx ... done
$ docker container ls
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                                                                 NAMES
bd0867025782   freki_nginx   "/docker-entrypoint..." 10 seconds ago Up 8 seconds  0.0.0.0:80->80/tcp, :::80->80/tcp, 0.0.0.0:443->443/tcp, :::443->443/tcp  freki_nginx
3c9bel16a638c   freki_freki   "bash -c '/freki/wai..." 12 seconds ago Up 9 seconds  8000/tcp                                               freki
f7cd7cf3ac90   freki_db      "/scripts/startup.sh"    15 seconds ago Up 12 seconds  3306/tcp                                               freki_db
```

Funcionalidades

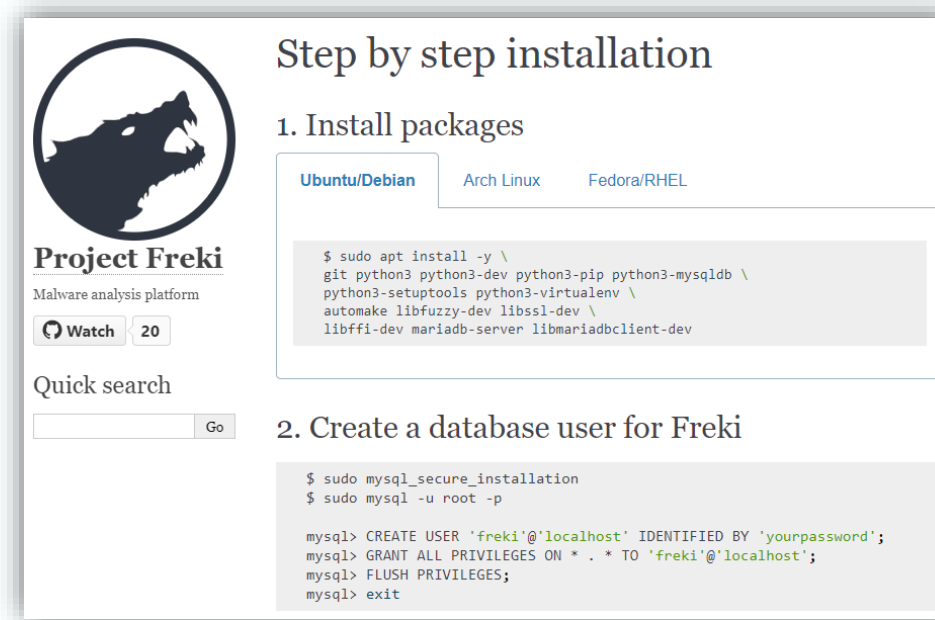
- Também é possível realizar a instalação nativa da ferramenta.
- Mais detalhes em: <https://crhenr.xyz/freki/admin/run-steps.html>.

- Distribuições testadas:

Ubuntu/Debian

Arch Linux

Fedora/RHEL



The screenshot shows the Project Freki installation guide. On the left, there is a circular logo of a wolf's head and the text 'Project Freki' and 'Malware analysis platform'. Below this is a 'Watch' button with '20' and a 'Quick search' input field with a 'Go' button. The main content area is titled 'Step by step installation' and has three tabs: 'Ubuntu/Debian' (selected), 'Arch Linux', and 'Fedora/RHEL'. Under the 'Ubuntu/Debian' tab, there are two sections: '1. Install packages' with a code block containing terminal commands for installing dependencies, and '2. Create a database user for Freki' with a code block containing terminal commands for creating a user and granting privileges.

```
$ sudo apt install -y \
git python3 python3-dev python3-pip python3-mysqldb \
python3-setuptools python3-virtualenv \
automake libfuzzy-dev libssl-dev \
libffi-dev mariadb-server libmariadbclient-dev
```

```
$ sudo mysql_secure_installation
$ sudo mysql -u root -p

mysql> CREATE USER 'freki'@'localhost' IDENTIFIED BY 'yourpassword';
mysql> GRANT ALL PRIVILEGES ON * . * TO 'freki'@'localhost';
mysql> FLUSH PRIVILEGES;
mysql> exit
```

Demonstração

<https://www.youtube.com/watch?v=brvNUPgw7ho>

Conclusão

- Freki é uma ferramenta livre para análise automatizada de malware e engenharia reversa.
- Sua arquitetura é bastante modular, permitindo a adição de novos recursos com grande facilidade.
- Seu *deploy* via Docker permite a criação de um ambiente para análise de forma simples e rápida.
- Trabalhos futuros:
 - Análise estática de outros tipos de arquivos: ELF, PDF, APK...
 - Criação de um ambiente para análise dinâmica.
 - Criação de um executável *standalone*.
 - Melhorias gerais no código fonte.