Segurança Cibernética em Roteadores Wi-Fi: abordagem automatizada para Coleta e Análise de Firmware

Guilherme Müller Bertolino
Me. Francoa Taffarel
Prof. Dr. Lourenço Alves Pereira Júnior

Instituto Tecnológico de Aeronáutica (ITA)

Sumário

- Motivação;
- Metodologia proposta;
- Resultados;
- Conclusão;
- Trabalhos futuros.

Motivação: Segurança de Roteadores

Porque se preocupar?

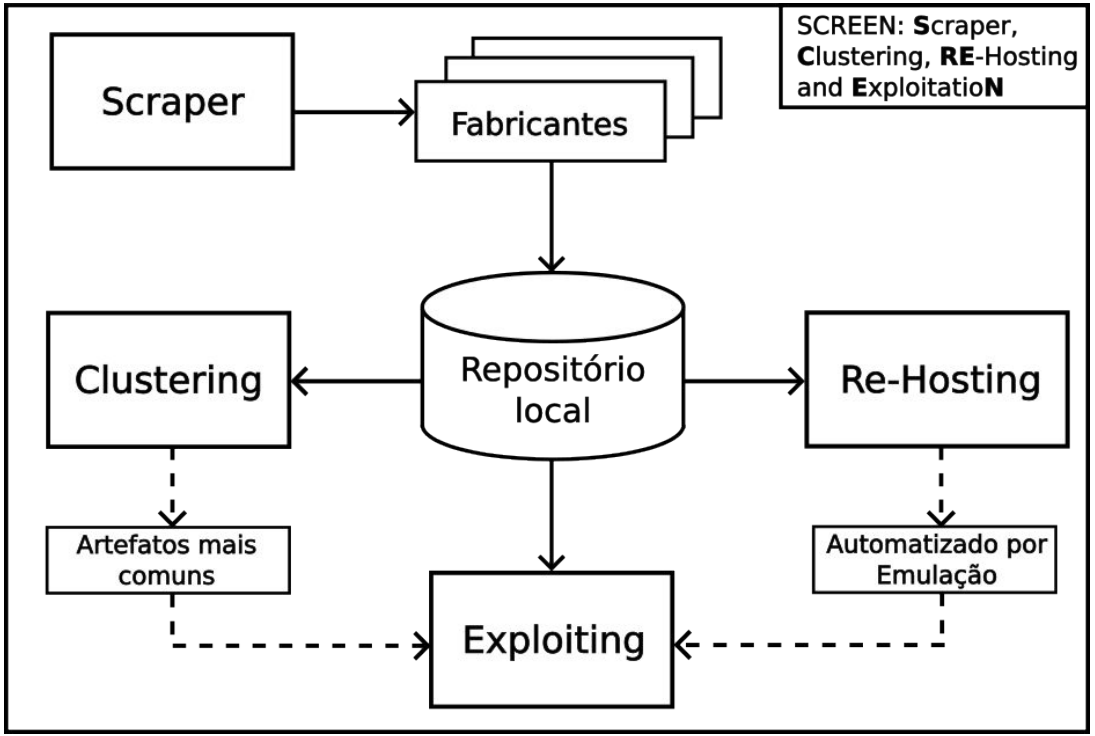
- *Gateway* de redes privadas;
- IoT e BotNets;
- *Home Office*.

Cenário atual:

- Ciclo de desenvolvimento deficiente;
- Poucos *updates*;
- *Firmware* vulnerável.

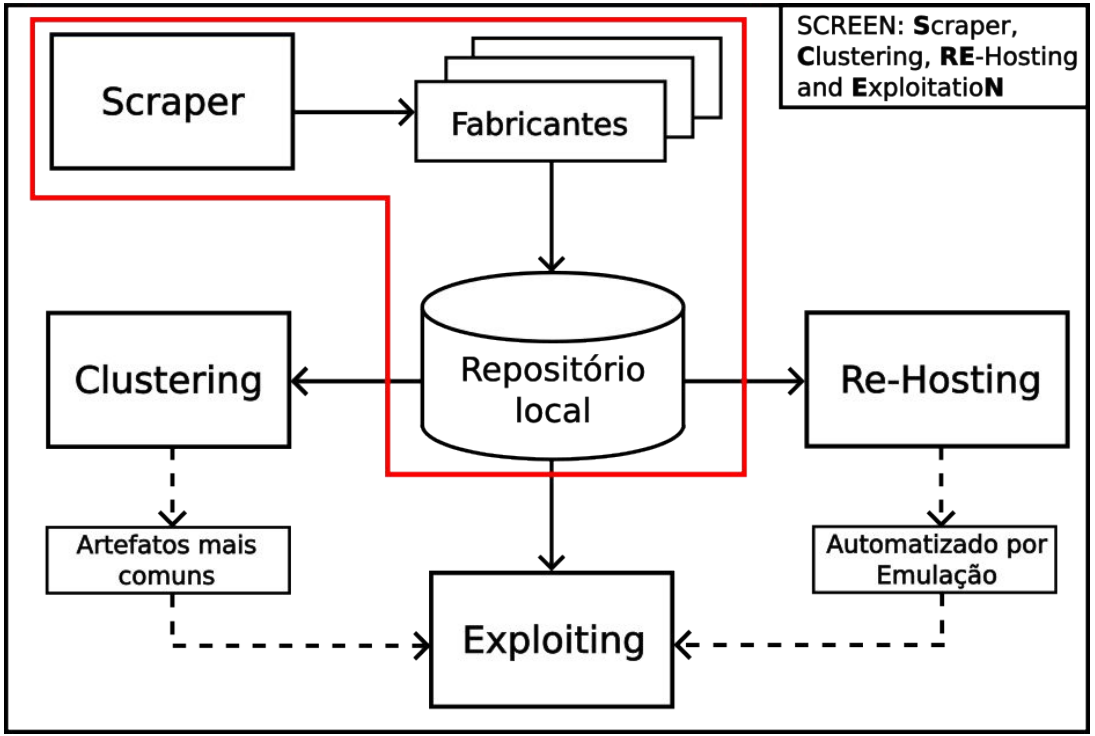
Motivação: SCREEN

- Inserido no SCREEN;
- Avaliação de SOHO;
- Larga escala;
- Automática.

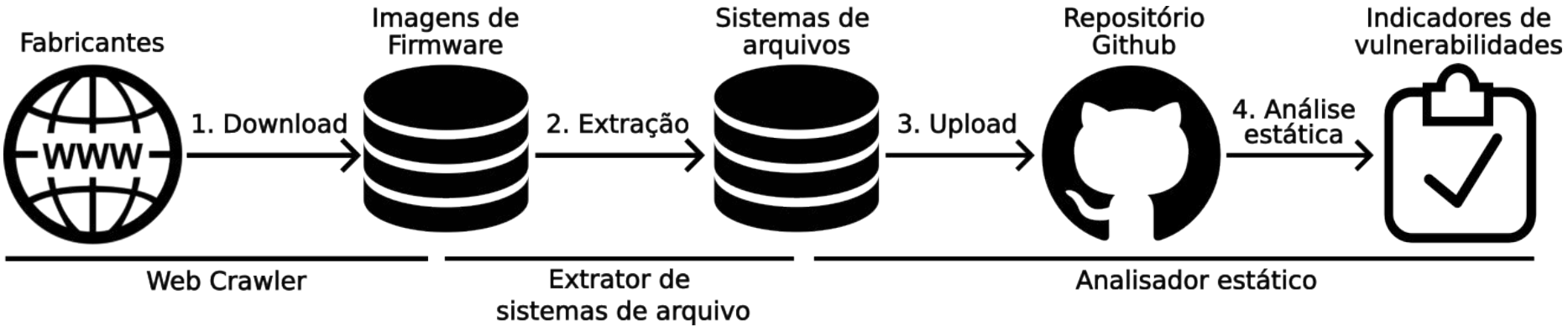


Motivação: SCREEN

- Necessidade de um Dataset;
- Crawlers desatualizados;
- Escopo Brasil.



Metodologia proposta

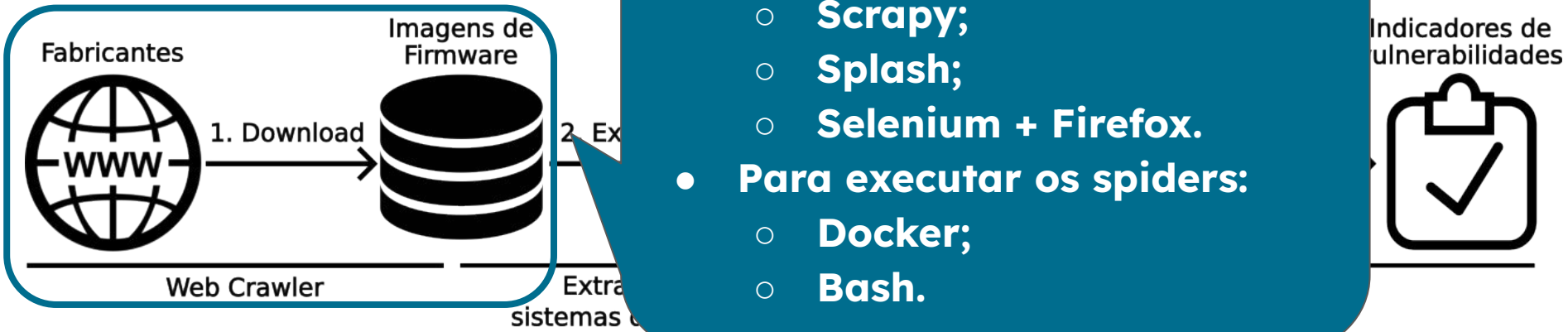


Metodologia proposta

Extração das imagens de:

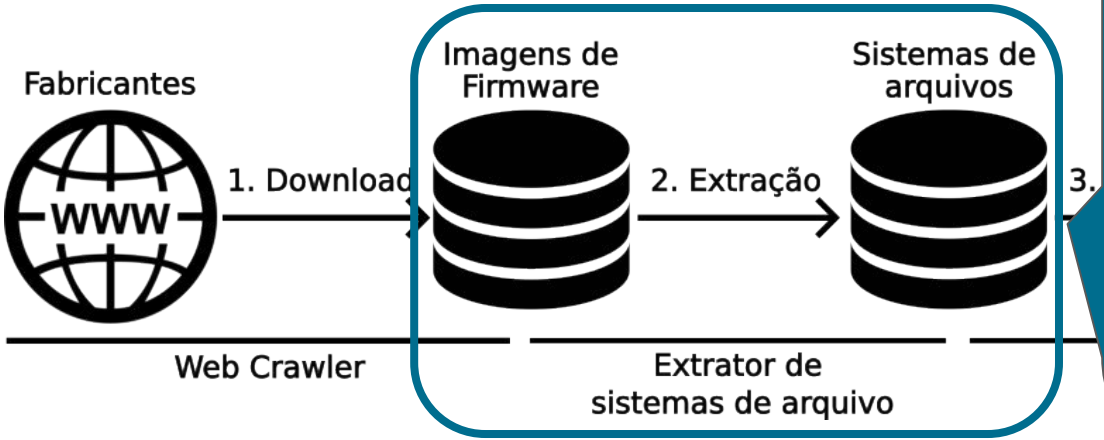
- **Fabricantes com maior Market Share;**
- **Roteadores vendidos no Brasil;**
- **Versão mais recente.**

Metodologia proposta



- **Ferramentas de *Crawling* :**
  - **Scrapy;**
  - **Splash;**
  - **Selenium + Firefox.**
- **Para executar os spiders:**
  - **Docker;**
  - **Bash.**

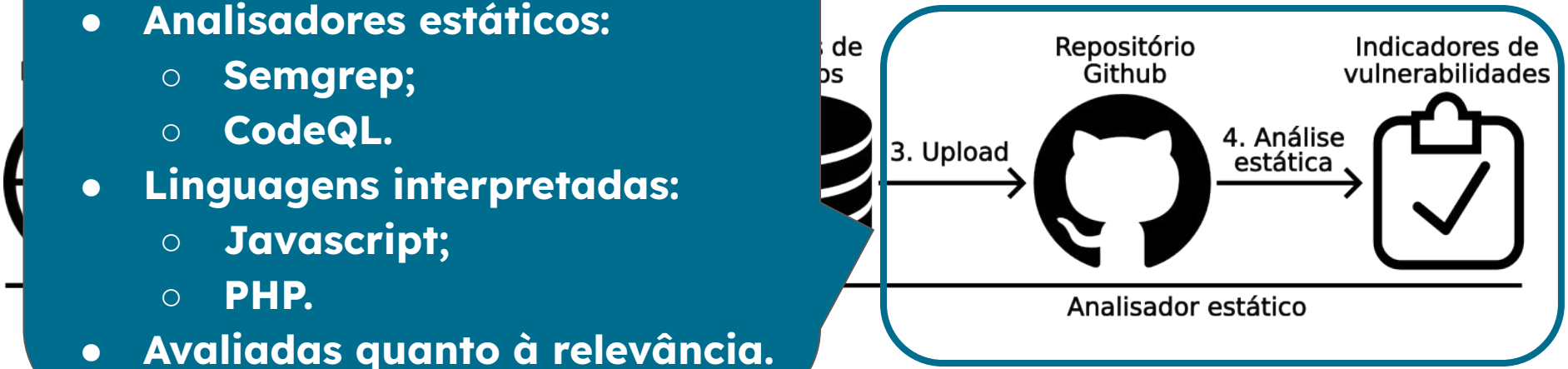
Metodologia proposta



- **Binwalk, sistemas de arquivos UNIX;**
- **Heurística: 4 ou mais diretórios UNIX;**
- **Estruturas em árvore;**
- **DFS no binário;**
- **BFS na extração.**

Metodologia proposta

- Github Actions;
- Analisadores estáticos:
  - Semgrep;
  - CodeQL.
- Linguagens interpretadas:
  - Javascript;
  - PHP.
- Avaliadas quanto à relevância.



Resultados: Crawler e Extrator

Fabricante	Imagens coletadas	Sistemas de arquivo extraídos	Porcentagem de sucesso
Tplink	87	57	66%
Intelbras	48	29	60%
Netgear	26	15	58%
Dlink	25	3	12%
Multilaser	18	5	28%
Ubiquiti	17	16	94%
Asus	14	14	100%
Tenda	13	2	15%
Mercusys	8	0	0%
Trendnet	6	0	0%
Total	262	141	54%

Resultados: Crawler e Extrator

Fabricante	Imagens coletadas	Sistema arquivo ex	
Tplink	87	57	
Intelbras	48	29	
Netgear	26		
Dlink	25	3	
Multilaser	18	5	28%
Ubiquiti	17	16	94%
Asus	14	14	100%
Tenda	13	2	15%
Mercusys	8	0	0%
Trendnet	6	0	0%
Total	262	141	54%

Escalabilidade:

- **Outras regiões;**
- **Outros fabricantes.**

Resultados: Crawler e Extrator

Problemas na extração:

- **Encriptação;**
- **Imagem parcial;**
- **Formatos não UNIX.**

	Imagens letadas	Sistemas de arquivo extraídos	Porcentagem de sucesso
	87	57	66%
	48	29	60%
	26	15	58%
	25	3	12%
		5	28%
		16	94%
	14	14	100%
Tenda	13	2	15%
Mercusys	8	0	0%
Trendnet	6	0	0%
Total	262	141	54%

Resultados: Análise estática

Ferramenta	Resultados totais	Alta severidade
Semgrep	7257	1871
CodeQL	3892	1427

- **Indicadores de vulnerabilidades (IoV);**
- **Usados para criar *exploits*;**
- **Validação posterior.**

Conclusão

- Crawler cumpre seu papel, criando um dataset para o SCREEN;
- Escalabilidade e portabilidade;
- IoVs úteis para o SCREEN;
- Repositório aberto.

Trabalhos futuros

- Expandir o Crawler;
- Melhorar extração de sistemas de arquivos;
- Extração de Bootloader e Kernel;
- Melhor avaliação da análise estática.

Obrigado!

- Autores:
  - Guilherme Bertolino;
  - Francoa Taffarel;
  - Lourenço Pereira Júnior.
- Contatos:
  - guilhermegmb@ita.br;
  - taffarel@ita.br;
  - ljr@ita.br.