pzgiestas@hotmail.com

Assunto: Violação de Privacidade e Intimidade do Consumidor - Informações e Arquivos - DIEBOLD E BANCOS BRASILEIROS

Anexos: EULA - Contrato de Licença do Usuário Final.pdf; Contestação - GAS-DIEBOLD.pdf; SERPRO NÃO PERMITE WARSAW PLUGIN.pdf; CLIENTES DA DIEBOLD.pdf; Relatório Americano de Violações Criminais - INFORMATIVO - Diebold Nixdorf.pdf

Prezados,

Sou advogado especialista em direito cibernético e o meu nome é **Dr. Phelippe Zanotti Giestas**.
Atualmente estamos com 5 processos de danos morais contra a DIEBOLD e a Caixa Econômica Federal.

Venho, nesta oportunidade, levar ao conhecimento da mídia para o público brasileiro e estrangeiro sobre a **VIOLAÇÃO DE PRIVACIDADE E INTIMIDADE OCASIONADA PELO MONITORAMENTO DE DADOS PESSOAIS ATRAVÉS DO MÓDULO DE PROTEÇÃO BANCÁRIA "WARSAW" DA FABRICANTE AMERICANA DIEBOLD** (mesma empresa fabricante das urnas eletrônicas no Brasil).

Apresento, através de documentos, provas indiscutíveis de que a empresa americana Diebold, fabricante dos "Módulo de Segurança Bancária" para acesso ao "Internet Banking" via um "computador", e fornecido de forma obrigatória por alguns bancos brasileiros, a exemplo da Caixa Econômica Federal, Banco do Brasil, Banestes, Banco da Amazônia, Banco de Brasília, Banco Itaú e entre outros, têm violado a privacidade e intimidade do consumidor correntista quando descobrimos que tal aplicativo bancário permanece ativo fora do acesso ao internet banking.

Em outras palavras, o **MONITORAMENTO DE DADOS PESSOAIS FORA DO INTERNET BANKING**, é uma verdadeira **VIOLAÇÃO DE PRIVACIDADE E INTIMIDADE AO CONSUMIDOR CORRENTISTA**, no qual passo a explicar em detalhes:

- **SOBRE O WARSAW – MÓDULO DE SEGURANÇA BANCÁRIA**

De acordo com as informações da fabricante DIEBOLD (GAS Tecnologia), o "módulo de proteção bancária" é o aplicativo "WARSAW", no qual se trata de uma solução de segurança desenvolvida pela "GAS", sendo uma empresa do grupo americano

Diebold Nixdorf, que tem como premissa proporcionar maior segurança aos dispositivos do usuário final, ajudando a prover confiabilidade e proteção durante o acesso ao Internet Banking, E-commerce, sites de governo e de instituições legítimas de que a GAS se reservar ao direito de ajudar a proteger.

A fabricante DIEBOLD explica em seu contrato que o "USUÁRIO" significa o utilizador final que opera o computador no qual o "módulo de segurança bancária" fora instalada.

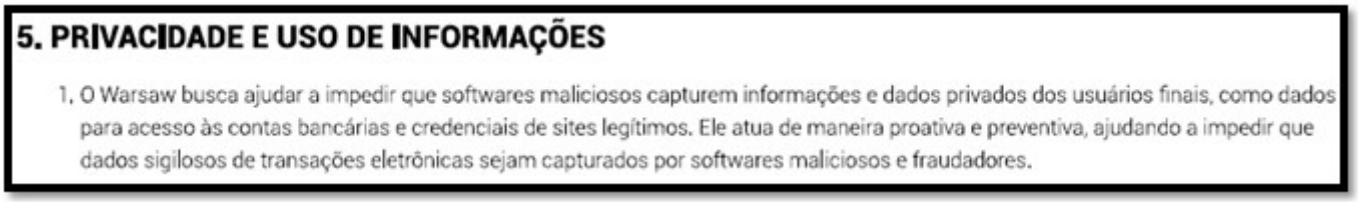
- **COMO É INSTALADO O WARSAW NO COMPUTADOR DO CORRENTISTA**

O correntista, através de seu computador, desejando acessar sua conta bancária, vai diretamente no endereço eletrônico de sua Instituição Financeira, como exemplo, o site da Caixa Econômica Federal (www.caixa.gov.br) e ao digitar sua agência e conta corrente, a proteção do banco fará uma pequena análise em seu computador e verificará se o "módulo de proteção bancária" já se encontra instalado, e caso seja negativo, o banco obrigará ao correntista para que instale tal programa, SEM ENTRAR EM DETALHES.

Após a instalação do "módulo de segurança bancária" ou seja, do WARSAW, o correntista consegue ter o seu acesso ao Internet Banking, MAS NÃO POSSUI NOÇÃO DE QUE O "WARSAW" PERMANECERÁ ATIVO NO SEU COMPUTADOR FORA DO ACESSO AO INTERNET BANKING EFETUANDO TODO O TIPO DE MONITORAMENTO DE DADOS PESSOAIS.

- **DA PROVA DE QUE O "WARSAW" PERMANECE ATIVO NO COMPUTADOR DO CORRENTISTA FORA DO INTERNET BANKING OU DO NAVEGADOR**

De acordo com a "*EULA – Contrato de Licença do Usuário Final*" da fabricante DIEBOLD (GAS Tecnologia), em sua cláusula "5", item "1", o "Warsaw" atua de maneira **PROATIVA** e **PREVENTIVA**, conforme imagem que segue:



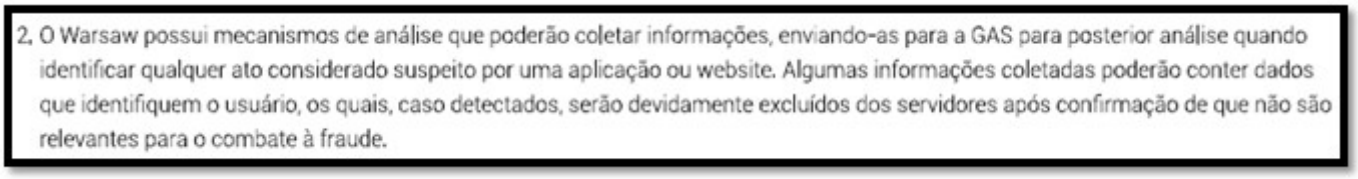
5. PRIVACIDADE E USO DE INFORMAÇÕES

1. O Warsaw busca ajudar a impedir que softwares maliciosos capturem informações e dados privados dos usuários finais, como dados para acesso às contas bancárias e credenciais de sites legítimos. Ele atua de maneira proativa e preventiva, ajudando a impedir que dados sigilosos de transações eletrônicas sejam capturados por softwares maliciosos e fraudadores.

Em outras palavras, o "WARSAW" permanece ATIVO NO COMPUTADOR, MONITORANDO OS DADOS PESSOAIS DO CORRENTISTA FORA DO ACESSO BANCÁRIO.

- **DO MONITORAMENTO DE DADOS PESSOAIS – INFORMAÇÕES CONTRATUAIS**

De acordo com a "*EULA – Contrato de Licença do Usuário Final*" da fabricante DIEBOLD (GAS Tecnologia), em sua cláusula "5", item "2", o "Warsaw" coleta informações pessoais que poderão conter dados (pessoais) que identifiquem o usuário, conforme imagem que segue:

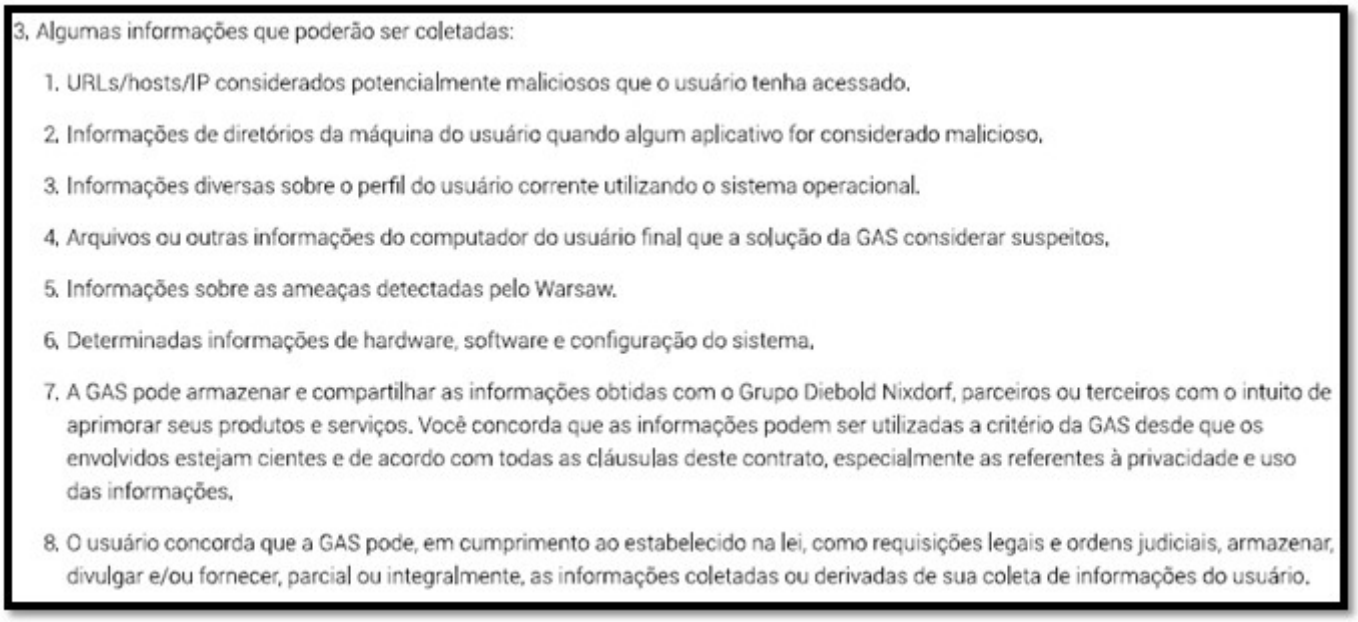

2. O Warsaw possui mecanismos de análise que poderão coletar informações, enviando-as para a GAS para posterior análise quando identificar qualquer ato considerado suspeito por uma aplicação ou website. Algumas informações coletadas poderão conter dados que identifiquem o usuário, os quais, caso detectados, serão devidamente excluídos dos servidores após confirmação de que não são relevantes para o combate à fraude.

Assim sendo, o próprio contrato da fabricante DIEBOLD (GAS Tecnologia) CONFESSA que o "WARSAW" – Módulo de Segurança Bancária PERMANECE ATIVO FORA DO INTERNET BANKING OU DO NAVEGADOR EFETUANDO O MONITORAMENTO DE DADOS PESSOAIS NO COMPUTADOR DO CORRENTISTA, ocorrendo assim a VIOLAÇÃO DE PRIVACIDADE E INTIMIDADE.

- **QUAIS AS INFORMAÇÕES SÃO COLETADAS / MONITORADAS PELO "WARSAW"**

De acordo com a "*EULA – Contrato de Licença do Usuário Final*" da fabricante DIEBOLD (GAS Tecnologia), em sua cláusula "5", item "3", [1 a 8], o monitoramento de dados e as coletas de informações no computador do correntista, fora do acesso bancário, ocorrem com endereço eletrônico de sites que são considerados potencialmente maliciosos pelo qual o consumidor tenha acessado; informações das pastas / diretórios do consumidor correntista quando algum aplicativo for considerado malicioso; informações diversas a respeito do perfil do consumidor correntista a respeito da utilização do sistema operacional (Windows, Linux, etc); todos os arquivos ou outras informações do computador do correntista pelo qual o "Warsaw" considerar suspeito; informações de ameaças que forem detectadas pelo "Warsaw"; algumas determinadas informações do computador (hardware), do

software (sistema operacional) e configuração do sistema; - Segue imagem do contrato da fabricante:



3. Algumas informações que poderão ser coletadas:

1. URLs/hosts/IP considerados potencialmente maliciosos que o usuário tenha acessado.
2. Informações de diretórios da máquina do usuário quando algum aplicativo for considerado malicioso.
3. Informações diversas sobre o perfil do usuário corrente utilizando o sistema operacional.
4. Arquivos ou outras informações do computador do usuário final que a solução da GAS considerar suspeitos.
5. Informações sobre as ameaças detectadas pelo Warsaw.
6. Determinadas informações de hardware, software e configuração do sistema.
7. A GAS pode armazenar e compartilhar as informações obtidas com o Grupo Diebold Nixdorf, parceiros ou terceiros com o intuito de aprimorar seus produtos e serviços. Você concorda que as informações podem ser utilizadas a critério da GAS desde que os envolvidos estejam cientes e de acordo com todas as cláusulas deste contrato, especialmente as referentes à privacidade e uso das informações.
8. O usuário concorda que a GAS pode, em cumprimento ao estabelecido na lei, como requisições legais e ordens judiciais, armazenar, divulgar e/ou fornecer, parcial ou integralmente, as informações coletadas ou derivadas de sua coleta de informações do usuário.

- **DA CONFISSÃO DA FABRICANTE – PROCESSO JUDICIAL – DA PROVA DA ATIVIDADE DO "WARSAW" FORA DO INTERNET BANKING OU DO NAVEGADOR**

A resposta da fabricante, **DIEBOLD** (GAS Tecnologia), em sua contestação, em trâmite na 4ª Vara Federal Cível da Comarca de Vitória/ES, sob o processo nº **0015818-70.2016.4.02.5001, às fls. 400, (46, 47 e 48)**, **CONFESSA que o "warsaw" permanece ativo no computador do correntista fora do contexto do navegador e do acesso ao internet banking**.

ORAS, estamos falando aqui de um **MONITORAMENTO DE DADOS QUE OCORREM FORA DO ACESSO BANCÁRIO**, no qual significa que a fabricante DIEBOLD (GAS Tecnologia) permanece efetuando o monitoramento de todos os dados pessoais que ocorrem no computador do consumidor, tendo acesso aos arquivos, fotos, vídeos, mensagens particulares, visualização de e-mails, logins, senhas, enfim, todas as coisas que são efetuadas no computador que o "warsaw" esteja instalado, a empresa fabricante DIEBOLD está efetivamente monitorando, **VIOLANDO COMPLETAMENTE A PRIVACIDADE E INTIMIDADE DO CONSUMIDOR CORRENTISTA**. Segue imagem retirada da contestação da fabricante no processo supracitado:

46. Sendo um software que promove a segurança do acesso, pelos usuários, aos sistemas de Internet Banking, entre outros; o Warsaw possui tecnologias de proteção que impedem os mais diversos ataques aos computadores dos usuários, destacando-se proteções contra:

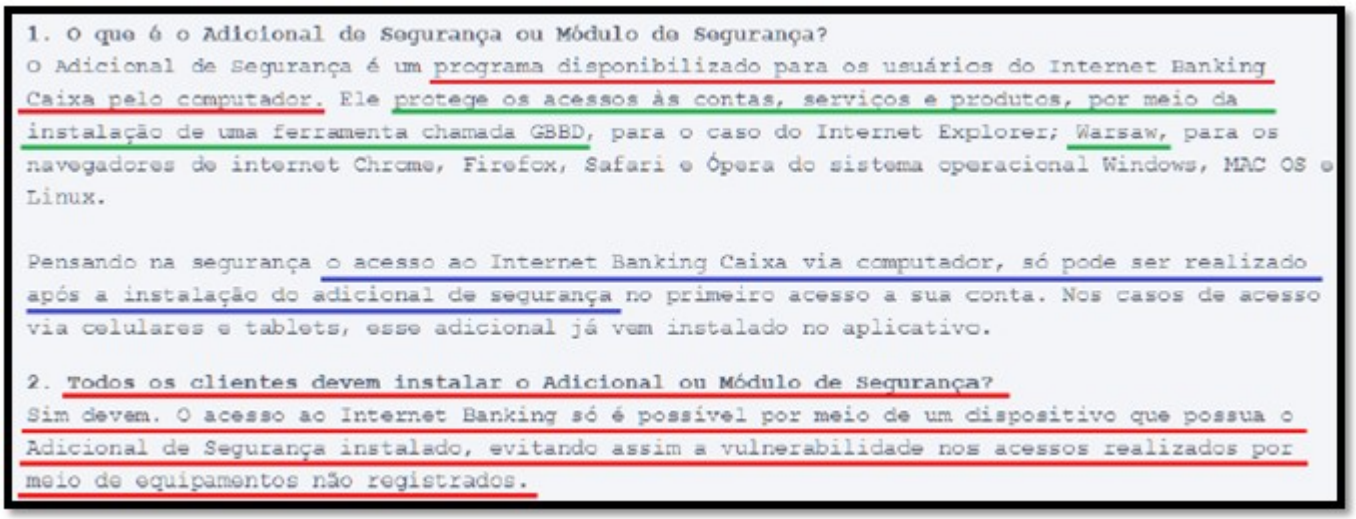
- *Malwares* que tentam capturar as credenciais dos usuários;
- Trojans que identificam o momento em que as páginas protegidas são abertas;
- Modificações em memória no código do browser para facilitar a captura das informações sigilosas dos usuários;
- Modificações de DNS que redirecionam o usuário para sites falsos;
- Digitação das credenciais do usuário em sites ou programas maliciosos;
- Acesso a páginas falsas da instituição protegida;
- Programas maliciosos carregados em memória.

47. Aliás, é por essa razão que o Warsaw permanece em atividade para fins de autoproteção e prevenção de ataques que ocorrem fora do contexto do navegador e do acesso ao Internet Banking.

48. De nada adiantaria manter-se inerte nesse período, permitindo a infecção da máquina para que, apenas quando do acesso ao Internet Banking, a proteção tornasse-se ativa. A eficiência do software pressupõe, justamente, a sua atividade constante, inclusive no que toca a proteção de agentes invasores que ingressam por outros sites para, ao final, atingirem os dados e operações do Internet Banking

- **DEMONSTRANDO O MÓDULO ADICIONAL DE SEGURANÇA DA CAIXA ECONÔMICA FEDERAL – AUSÊNCIA DE EXPLICAÇÕES AO CORRENTISTA**

Como exemplo, a seguir, iremos demonstrar o que é o "WARSAW" do Banco da Caixa Econômica Federal (CEF), demonstrando que O BANCO não informa para o correntista de que o software permanecerá monitorando seus dados pessoais fora do Internet Banking, senão vejamos:



1. O que é o Adicional de Segurança ou Módulo de Segurança?
O Adicional de Segurança é um programa disponibilizado para os usuários do Internet Banking Caixa pelo computador. Ele protege os acessos às contas, serviços e produtos, por meio da instalação de uma ferramenta chamada GBBD, para o caso do Internet Explorer; Warsaw, para os navegadores de internet Chrome, Firefox, Safari e Ópera do sistema operacional Windows, MAC OS e Linux.

Pensando na segurança o acesso ao Internet Banking Caixa via computador, só pode ser realizado após a instalação do adicional de segurança no primeiro acesso a sua conta. Nos casos de acesso via celulares e tablets, esse adicional já vem instalado no aplicativo.

2. Todos os clientes devem instalar o Adicional ou Módulo de Segurança?
Sim devem. O acesso ao Internet Banking só é possível por meio de um dispositivo que possua o Adicional de Segurança instalado, evitando assim a vulnerabilidade nos acessos realizados por meio de equipamentos não registrados.

Como podemos observar, no exemplo da Caixa Econômica Federal, o correntista é obrigado a instalar o "Módulo Adicional de Segurança da CAIXA" para poder ter acesso ao "Internet Banking", PORÉM, em nenhum momento o BANCO explica para o correntista que na verdade TAL APLICATIVO se trata de um programa chamado "WARSAW" que de forma abusiva, PERMANECERÁ ATIVO NO COMPUTADOR FAZENDO O MONITORAMENTO DE DADOS PESSOAIS FORA DO ACESSO AO INTERNET BANKING.

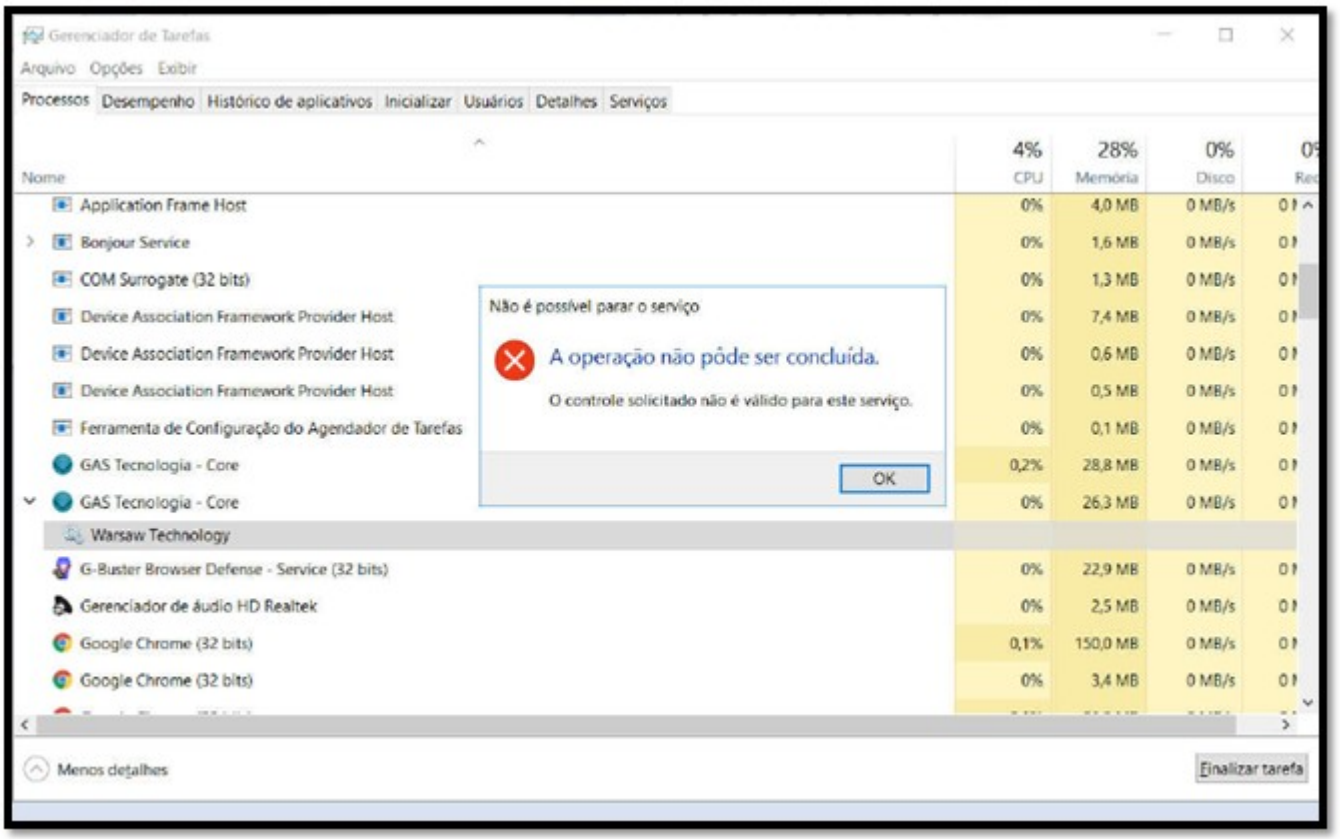
Com tal prova documental, já demonstramos que o consumidor correntista está tendo a sua privacidade e intimidade totalmente violada perante um monitoramento de dados pessoais que ocorrem fora do acesso bancário, invadindo por completo a vida privada do consumidor.

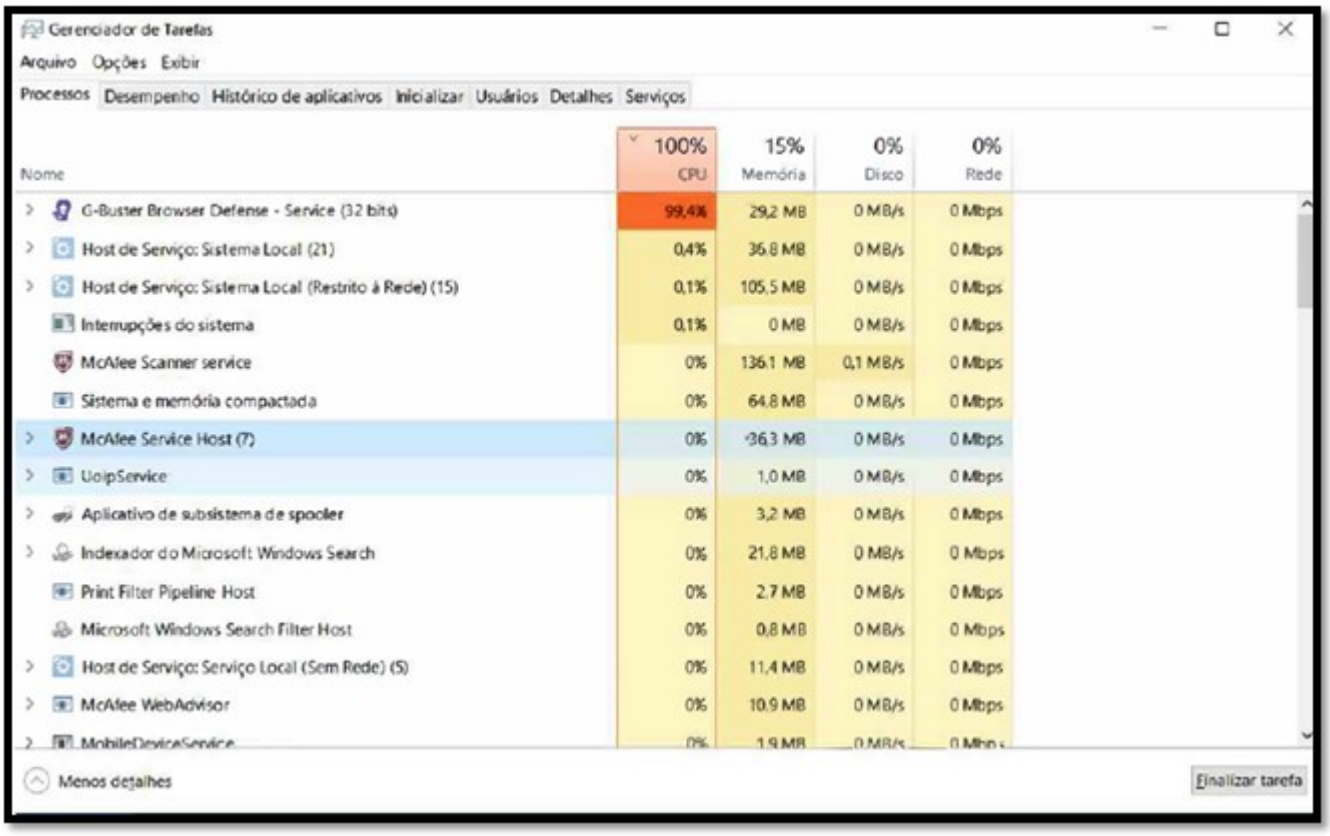
- **"WARSAW" POSSUI OUTROS NOMES – ATIVIDADE DE MONITORAMENTO É SEMELHANTE A UM ESPIÃO DE DADOS**

Para ser mais exato, o "Warsaw" também possui outras denominações, e como sua atividade é o ato de MONITORAR DADOS PESSOAIS SEM QUE O CONSUMIDOR CORRENTISTA TENHA CONHECIMENTO, sua existência se compara exatamente com softwares espiões, como "*spywares*", "*malware*" e "*keylogger*", tendo em vista que o "Warsaw" permanece ativo no computador, fora do acesso bancário, monitorando todos os arquivos e dados pessoais, praticamente, tudo o que é feito no computador.

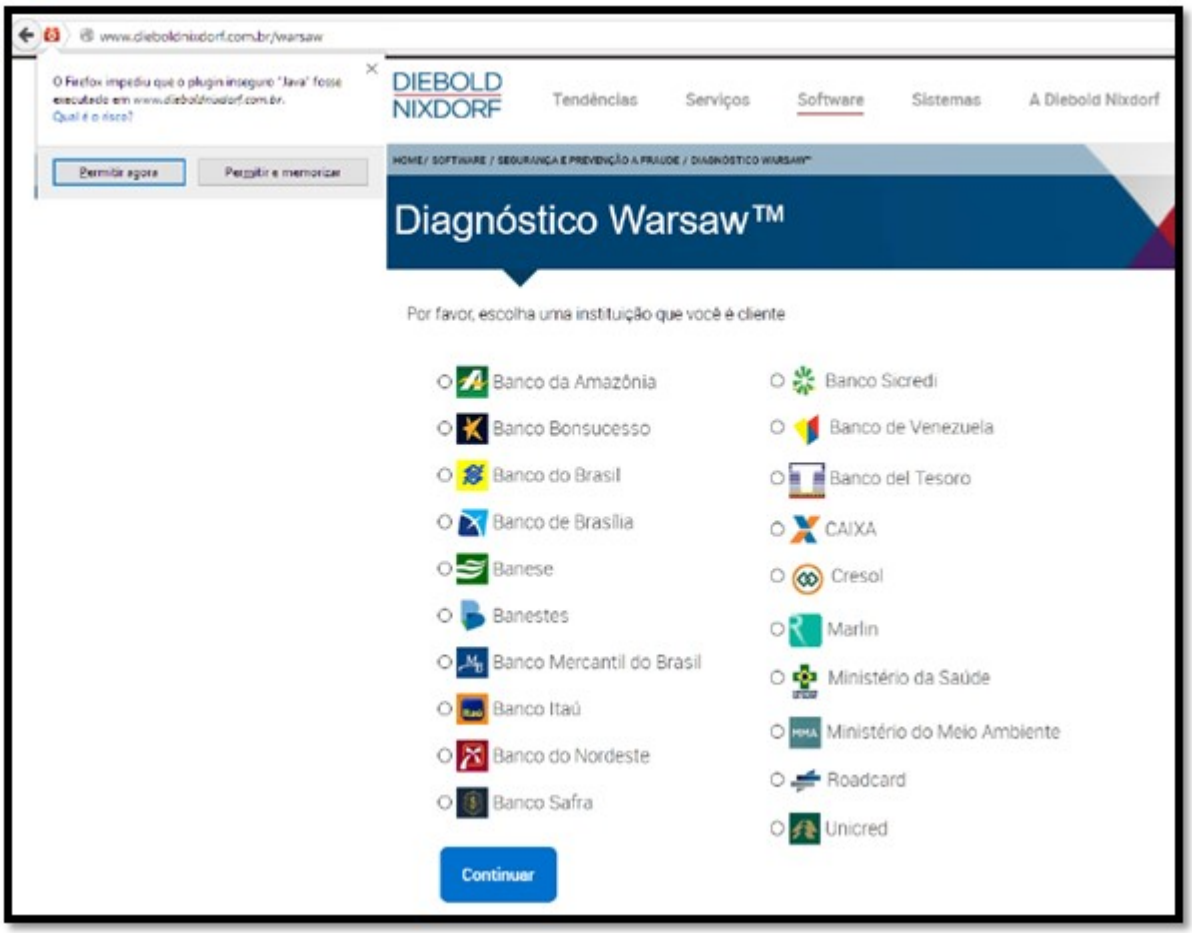
O "WARSAW", também possui outros nomes como: "G-Buster Browser Defense"; "GAS Tecnologia – Core" e "Gbplugin".

Segue imagem abaixo como exemplo para confirmar o que estamos alegando acima:





- **CLIENTES / BANCOS QUE UTILIZAM O "WARSAW"**



Conforme demonstrado na foto acima, esta é a lista dos clientes / bancos que fazem uso do software / plugin "WARSAW" – Módulo de Segurança Bancária.

- **DEMONSTRAÇÃO EM VÍDEO DA ATIVIDADE DO MONITORAMENTO DE DADOS PESSOAIS DO "WARSAW" – MÓDULO DE SEGURANÇA BANCÁRIA – NO COMPUTADOR DO CORRENTISTA**

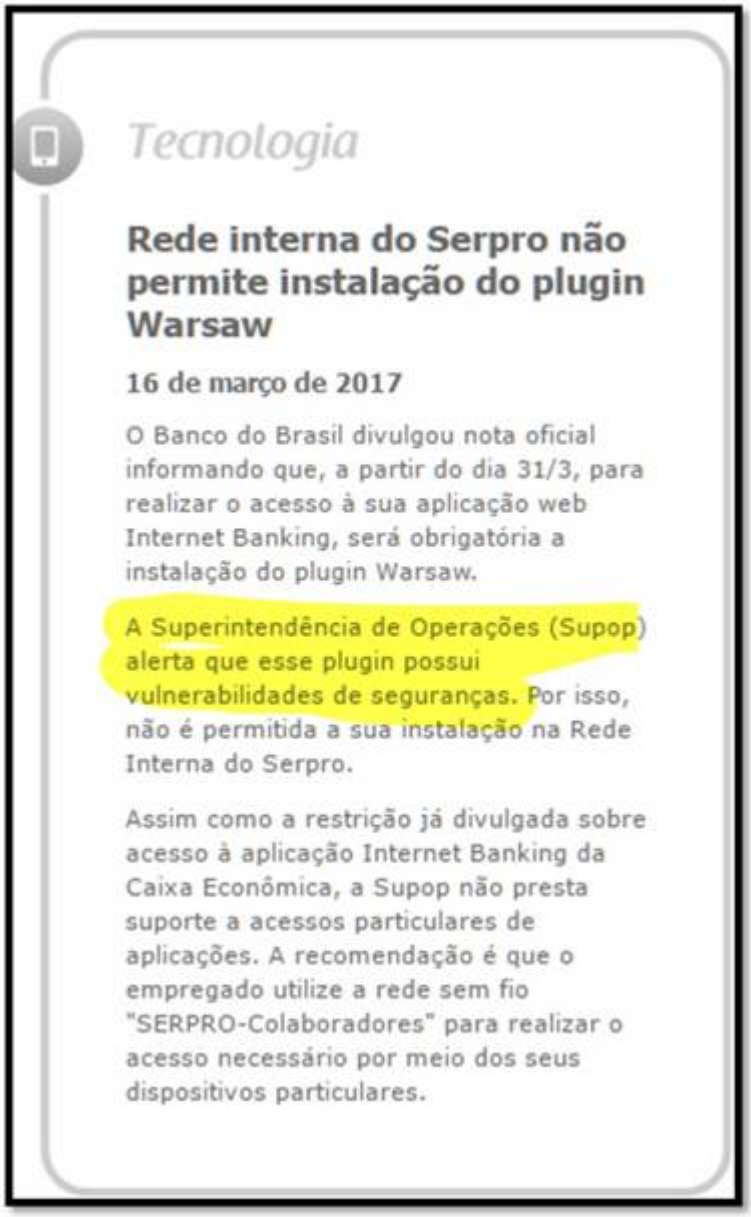
No "Youtube", link: https://www.youtube.com/watch?v=nlCJgKbzVHs, nós demonstramos, como PROVA, a metodologia e forma de como ocorre a atividade do "WARSAW" - "módulo de segurança bancária".

RESUMINDO: O "módulo de segurança bancária" (WARSAW) **NÃO DEVERIA ESTAR ATIVO FORA DO ACESSO AO INTERNET BANKING**.

Uma vez que finalidade do "Warsaw" é monitorar dados pessoais, estando o mesmo ativo fora do acesso bancário ou do navegador, este passa a VIOLAR A PRIVACIDADE E INTIMIDADE DO CONSUMIDOR CORRENTISTA.

- **A SUPOP – SUPERINTENDÊNCIA DE PRODUTOS E SERVIÇOS E OPERAÇÕES - (SERPRO NÃO AUTORIZA O USO DO "WARSAW" EM SUA REDE)**

Como podemos observar, a própria SUPOP – Superintendência de Produtos e Serviços e Operações, em **16/03/2017**, lançou uma nota informando que o "plugin" "WARSAW" possui vulnerabilidades de seguranças, em conformidade ao que fora divulgado pelo Banco do Brasil, no qual destacou que após o dia 31/03/2017, para realizar o acesso ao Internet Banking, **será obrigatória a instalação do plugin "Warsaw"**.



Tecnologia

Rede interna do Serpro não permite instalação do plugin Warsaw

16 de março de 2017

O Banco do Brasil divulgou nota oficial informando que, a partir do dia 31/3, para realizar o acesso à sua aplicação web Internet Banking, será obrigatória a instalação do plugin Warsaw.

A Superintendência de Operações (Supop) alerta que esse plugin possui vulnerabilidades de seguranças. Por isso, não é permitida a sua instalação na Rede Interna do Serpro.

Assim como a restrição já divulgada sobre acesso à aplicação Internet Banking da Caixa Econômica, a Supop não presta suporte a acessos particulares de aplicações. A recomendação é que o empregado utilize a rede sem fio "SERPRO-Colaboradores" para realizar o acesso necessário por meio dos seus dispositivos particulares.

VEJAMOS... – Documentalmente e confessada pela fabricante DIEBOLD, o "Warsaw" é um programa espião de dados, no qual **PERMANECE ATIVO NO COMPUTADOR DO CORRENTISTA, FORA DO INTERNET BANKING, EFETUANDO O MONITORAMENTO DE DADOS PESSOAIS DE FORMA TOTALMENTE INVISÍVEL E AINDA POSSUI VULNERABILIDADES DE SEGURANÇAS ???**

ASSIM, PODEMOS CONCLUIR... – A própria **SERPRO**, através da "SUPOP", **PROÍBE A INSTALAÇÃO DO MÓDULO DE SEGURANÇA BANCÁRIA – WARSAW**, diante da sua vulnerabilidade de segurança e também decorrente da sua atuação de monitoramento fora do acesso bancário, ou seja, **O PRÓPRIO GOVERNO NÃO CONFIA NO MÓDULO DE PROTEÇÃO BANCÁRIA, NÃO AUTORIZANDO A SUA INSTALAÇÃO EM SUA REDE INTERNA DO SERPRO**.

- **O "WARSAW" NÃO POSSUI INTERAÇÃO COM O CONSUMIDOR COMO OCORREM COM OUTROS PROGRAMAS, ANTIVÍRUS OU FIREWALL**

Por fim, cabe ressaltar ainda que, diferente de um software de proteção, como o "Antivírus" ou um "Firewall", o consumidor, após instalar o "Warsaw" – Módulo de Segurança Bancária, NÃO POSSUI NENHUM ACESSO AO PROGRAMA, no qual o mesmo permanece ativo, monitorando os dados pessoais fora do Internet Banking e SEM QUE O CONSUMIDOR TENHA AUTONOMIA SOBRE O PROGRAMA, não sendo sequer permitido ao mesmo desabilitar o "Warsaw" no sistema operacional.

Cabe esclarecer ainda que o "Warsaw" NÃO É CLASSIFICADO COMO ANTIVÍRUS, bem como NÃO É CLASSIFICADO COMO FIREWALL.

A SUA CLASSIFICAÇÃO ESTÁ EM SER UM PROGRAMA DE MONITORAMENTO DE DADOS PESSOAIS (ESPIÃO) QUE ATUA FORA DO ACESSO BANCÁRIO, EM TEMPO INTEGRAL, VIOLANDO A PRIVACIDADE E INTIMIDADE DO CONSUMIDOR CORRENTISTA QUE É OBRIGADO A INSTALAR O PROGRAMA EM SEU COMPUTADOR PARA CONSEGUIR ACESSO AO INTERNET BANKING.

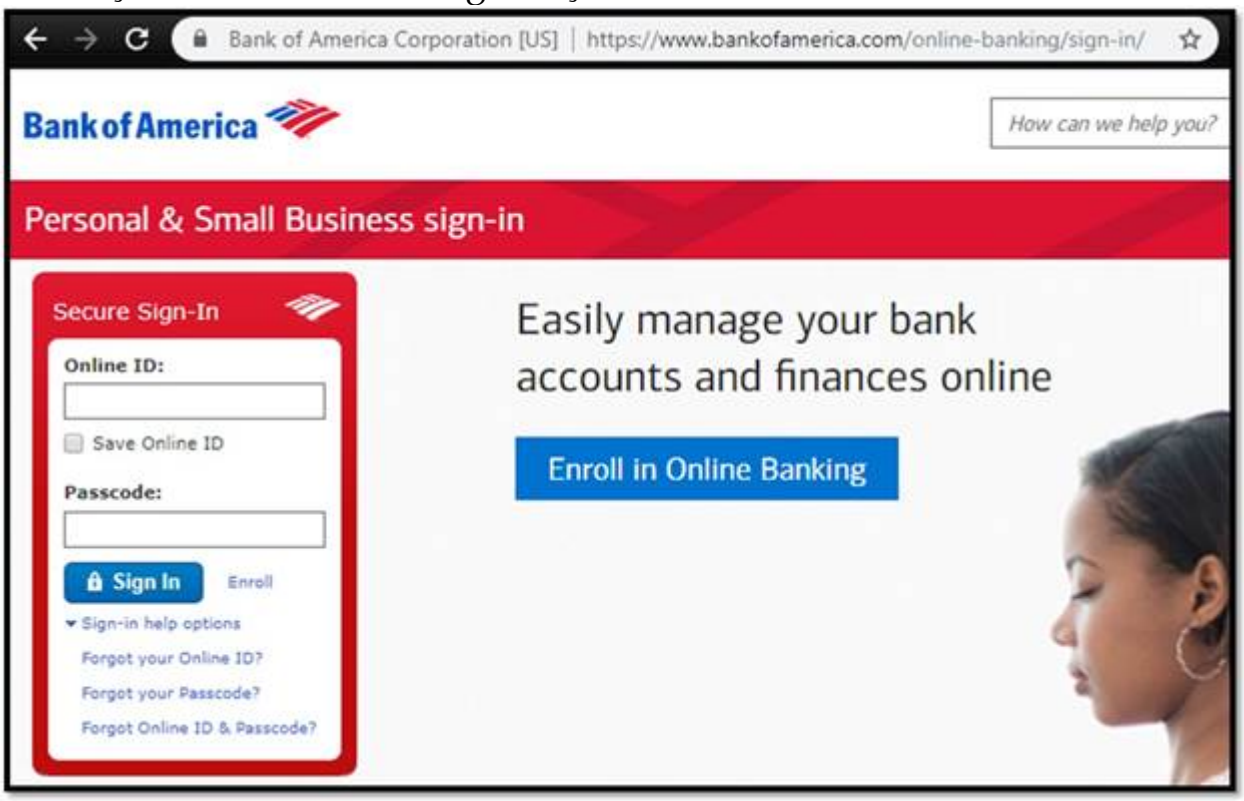
- **BANCOS ESTRANGEIROS UTILIZAM OUTRAS FORMAS DE SISTEMA DE PROTEÇÃO E NÃO FAZEM USO DO "WARSAW" – DEMONSTRAÇÃO DE ALTERNATIVAS PROTETIVAS – DA DIFERENÇA DA PUBLICIDADE E INFORMAÇÃO DE UM BANCO ESTRANGEIRO PARA UM BANCO BRASILEIRO**

Primeiramente, cabe deixar destacado que os Bancos Estrangeiros (Norte Americanos e Europeus), NÃO FAZEM UTILIZAÇÃO DO "WARSAW", justamente porque a sua atuação é uma violação de privacidade e intimidade.

ORAS, o que seria a "Criptografia SSL"? – O protocolo SSL é o mesmo utilizado por todos os bancos estrangeiros e sites de E-commerce, no qual podemos identificar esta característica visualizando o "CADEADO FECHADO" ao lado do endereço do site e também através da sigla "HTTPS" antes do endereço do site bancário.

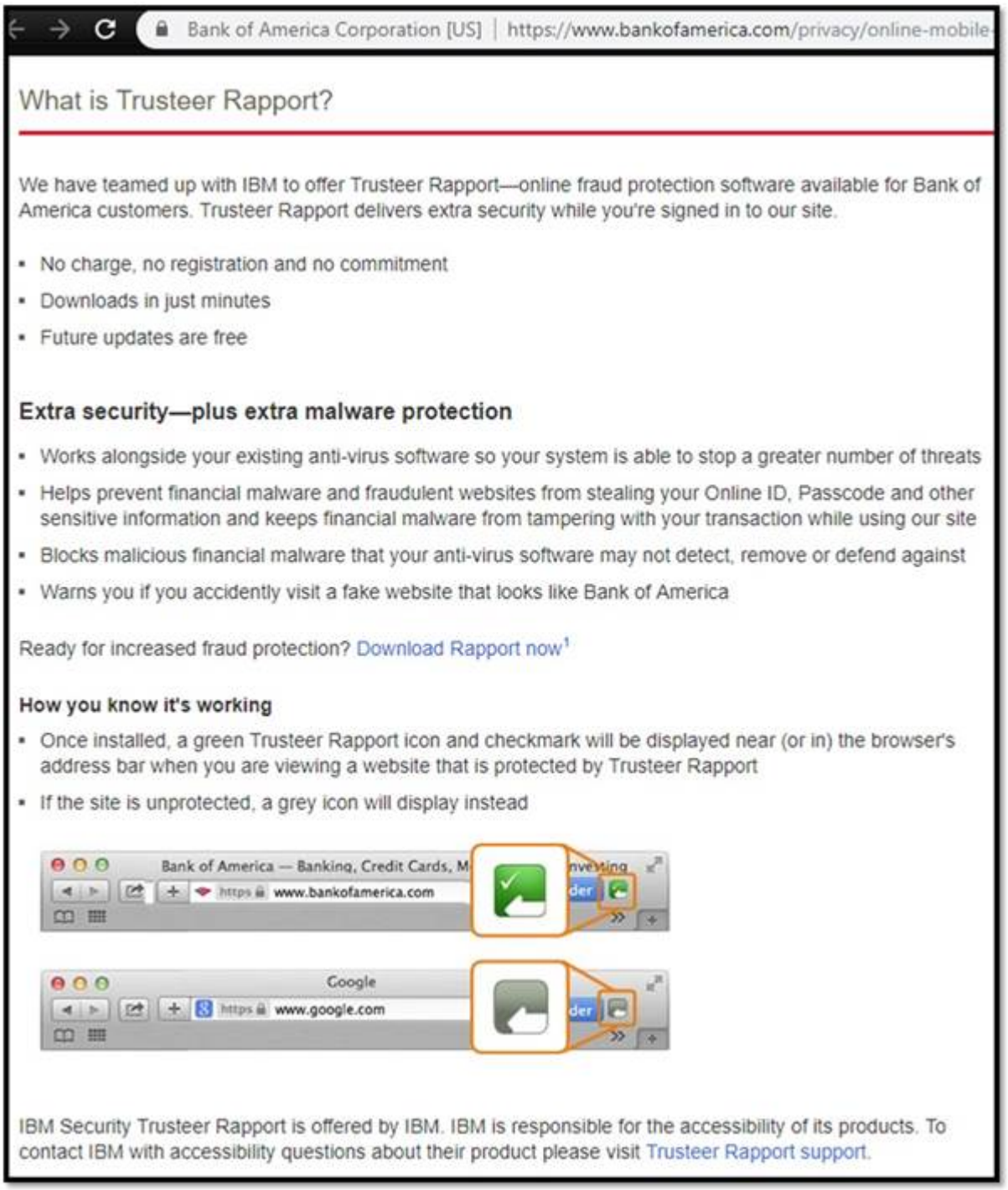
A proteção bancária existente fora do Brasil, ocorrem em outras plataformas e metodologias de segurança tecnológicas que não obrigam ao correntista a ter de instalar em seu computador um programa espião de dados.

Como um bom exemplo de um dos maiores bancos do mundo, o "*Bank of America*" – (https://www.bankofamerica.com), que em seu site, na área do "Internet Banking", apresenta ao correntista para digitar "login" e "senha", não obriga nenhuma instalação de "módulo de segurança bancária".



Por sua vez, **OBSERVE QUE**, caso o correntista deseje "transacionar dentro do Internet Banking", o banco "*Bank of America*" não obriga a utilização de um "módulo de segurança bancária", que no caso, é da fabricante **IBM – Trusteer Rapport**, no qual, **DIFERENTE DOS BANCOS BRASILEIROS**, o próprio "*Bank of America*" informa ao correntista, explicando que o aplicativo "*Trusteer Rapport*" é um "módulo de segurança bancária" criado pela "IBM" no qual provê proteção online contra ataques "*malwares*", apresentando que os correntistas (clientes do banco) podem utilizar o "Trusteer Rapport" para aumentar a segurança em seus navegadores (browsers), como exemplo o "Google Chrome; Internet Explorer; Firefox..." quando estiverem acessando qualquer website que contenham informações pessoais ou financeiras. Destacando que o "*Trusteer Rapport*" mantém o seu computador protegido de "keyloggers" e entre outras situações.

EM OUTRAS PALAVRAS, ALÉM DO BANCO ESTRANGEIRO INFORMAR SOBRE O APLICATIVO, DEIXA CLARO QUE TAL PROGRAMA NÃO É OBRIGATÓRIO E INFORMA DETALHADAMENTE A SUA FUNÇÃO, NO QUAL O PRÓPRIO CORRENTISTA POSSUI A INTERAÇÃO COM SUA FUNÇÃO, CONFORME PODE SER OBSERVADO NA IMAGEM QUE SEGUE:



Assim sendo, voltando ao assunto sobre o "WARSAW" – Módulo de Segurança Bancária, DIFERENTE DO SISTEMA DA "IBM", o Correntista quando faz a instalação do programa "WARSAW" da fabricante DIEBOLD, sob a obrigatoriedade de seu banco para ter acesso ao Internet Banking, **ESTE NÃO POSSUI NENHUMA OUTRA INFORMAÇÃO, NÃO CONSEGUE INTERAGIR COM O PROGRAMA, NO QUAL O MESMO PERMANECE ATIVO NO COMPUTADOR, FORA DO INTERNET BANKING E DO NAVEGADOR, FAZENDO O MONITORAMENTO DE TODOS OS DADOS PESSOAIS NO COMPUTADOR, DE FORMA INVISÍVEL E SEM PERMITIR QUALQUER TIPO DE CONTROLE POR PARTE DO CONSUMIDOR**.

Ademais, como podemos observar, o que ocorre de fato é que o software "Warsaw", ao invés de monitorar os dados pessoais do correntista somente quando do acesso ao Internet Banking e ou da página de seu banco, **ESTE PERMANECE ATIVO FORA DO INTERNET BANKING OU DO NAVEGADOR – EFETUANDO O MONITORAMENTO DE DADOS PESSOAIS NO COMPUTADOR DO CORRENTISTA EM TEMPO INTEGRAL**.

Tal atividade de monitoramento de dados, sem autorização do consumidor correntista, é uma verdadeira VIOLAÇÃO DE PRIVACIDADE E INTIMIDADE, e deve ser levado ao conhecimento do público, das autoridades.

Por fim, repito, que não estamos falando sobre haver ou não "vazamento de dados", MAS DE UM **MONITORAMENTO DE DADOS PESSOAIS NÃO AUTORIZADOS QUE OCORREM FORA DO INTERNET BANKING OU DO NAVEGADOR**.

ARQUIVOS ANEXOS:

EULA – Contrato de Licença do Usuário Final.pdf – (Contrato da DIEBOLD);

Contestação – GAS – DIEBOLD.pdf – (Processo Federal nº 0015818-70.2016.4.02.5001);

Relatório Americano de Violações Criminais - INFORMATIVO - Diebold Nixdorf.pdf – (Reputação da DIEBOLD nos Estados Unidos);

SERPRO NÃO PERMITE WARSAW PLUGIN.pdf – (SUPOP/SERPRO alerta sobre WARSAW);

CLIENTES DA DIEBOLD.pdf – (Lista dos bancos que utilizam o WARSAW);

(Gentileza confirmar o recebimento)

Giestas & Reis
Advogados Associados

Phelippe Zanotti Giestas – (OAB/ES 24.603)
Manoel Amorim de Almeida Reis – (OAB/ES 14.692)

E-mail: PZGIESTAS@hotmail.com
Telefone: (27) 99725-6906 - (VIVO) – (27) 3049-1566
Escritório: Rua Cassiano Castelo, nº 36, 2º Andar, SL. 202, Centro, Colatina/ES
