São Paulo, Brazil
October 29-30, 2018

The Tenth International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2018007 or http://dx.doi.org/10.5769/C2018007

Anatomia do *Modus Operandi* de um *Cracker* - Perícia de um Caso Real de Fraudes pela Internet

Wilson Leite da Silva Filho[1]

(1) Instituto Geral de Perícias (IGP/SC), Email: wleitefilho@gmail.com

Resumo: Este artigo apresenta os resultados de uma perícia oficial de um caso de fraude realizada via Internet, que vitimava pessoas físicas e instituições financeiras. Além das questões técnicas referentes à fraude, serão apresentados o modus operandi do fraudador e de outros personagens que integravam toda uma organização criminosa. São discutidas questões importantes referentes à volatilidade da prova digital, técnicas antiforenses e os cuidados que devem ser tomados durante a busca e apreensão de casos similares. Além dessas questões, são analisados os artefatos digitais que proporcionavam a fraude e as demais evidências encontradas pela perícia.

Palavras-chave: Fraude digital, crimes informáticos, fraudes em Internet Banking, volatilidade da prova digital, cuidados com antiforense.

Abstract: This paper presents the results of an official forensic examination of a fraud committed thru the Internet. Besides the technical issues, the operational mode of the suspects will be presented. Important issues about the data volatility of the digital evidence, anti-forensic techniques and the precautions needed in the search and seizure operations of similar cases. Besides that, digital artefacts and other evidences related with the fraud will be analyzed.

Key words: Digital fraud, cybercrime, internet banking fraud, digital evidence volatility, precautions about anti-forensics.

I. Introdução

Serviços e movimentações financeiras realizadas por meio da tecnologia da informação trouxeram grande praticidade e comodidade às pessoas. Por meio de aplicativos de celular ou páginas Web é possível realizar todo tipo de transação financeira, desde pagamento de pequenos valores até transações mais volumosas. O comércio eletrônico teve grande expansão. Já não é mais necessário ir fisicamente às lojas para realizar compras. Basta acesso à Internet e um cartão de crédito.

Contudo, infelizmente, a criminalidade também acompanha o avanço tecnológico. Fraudes por meio da Internet se tornaram uma atividade bastante lucrativa. Estima-se que as perdas das instituições financeiras chegam a casa dos bilhões de reais por ano [3] [4] [5].

Segundo dados da F-Secure, o Brasil anualmente registra prejuízo da ordem de R$ 40 bilhões. O país também se destaca como quarto principal alvo de fraudes pela Internet, principalmente na modalidade pescaria de senhas ou phishing, figurando entre os cinco países que mais tiverem empresas hackeadas. Em relação ao combate a esse tipo de delito, pouco se faz por aqui. Uma situação oposta acontece nos Estados Unidos, onde o FBI convoca especialistas de segurança da informação para o que anuncia ser uma "guerra cibernética" [7].

A persecução penal desses ilícitos se faz cada vez mais necessária e a perícia criminal especializada se torna imprescindível para a produção de uma prova robusta.

II. Objetivo

O objetivo do trabalho é apresentar os procedimentos realizados em uma perícia de um caso de fraude envolvendo ambiente digital, discutir as melhores práticas segundo a literatura especializada e analisar os resultados alcançados.

O artigo tem como público alvo e visa apresentar informações úteis tanto para os especialistas da área de computação forense, como peritos, assistentes técnicos e pesquisadores, quanto para os operadores do direito interessados na persecução penal desse tipo de delito.

III. Considerações sobre a volatilidade da prova digital, técnicas antiforenses e suas implicações na busca e apreensão

A fraude retratada neste trabalho inicialmente foi detectada por uma das instituições financeiras lesadas, que comunicou à polícia o ocorrido. Uma vez ciente do delito, a autoridade policial instaurou inquérito policial, que foi conduzido por uma divisão especializada em fraudes da polícia judiciária. A investigação identificou um suspeito, sendo que após os procedimentos legais, foi emitido mandado de busca e apreensão pela Justiça.

Antes de proceder ao cumprimento do mandado, a autoridade policial entrou em contato com a perícia para acompanhamento das diligências, aconselhamento técnico sobre a área de crimes cibernéticos e medidas necessárias para a preservação da prova digital.

Contatar a perícia previamente se mostrou uma atitude acertada. Há também respaldo na literatura sobre a importância de levar ao conhecimento do perito, com certa antecedência, o cenário provável que será encontrado no momento da diligência.

A norma ABNT BR ISO/IEC 27037 recomenda que seja feita uma seção formal de instrução para o entendimento do incidente, o que esperar e o que não esperar durante a investigação e um lembrete contra adulteração e espoliação. Convém que as instruções sejam suficientes para os envolvidos estarem bem preparados no desempenho de suas funções e responsabilidades; desse modo, assegurando a extração de todas as potenciais evidências digitais relevantes [1].

Deve-se sempre ter em mente que a prova digital é volátil, se não tratada de forma adequada. No caso concreto da perícia que este trabalho se relaciona, a autoridade policial informou ao perito sobre o cenário e sobre algumas das características do suspeito, que foi categorizado como um hacker pela autoridade policial.

Cabe aqui, parênteses sobre essa terminologia. O termo hacker, no contexto da investigação policial, foi usado com o significado usualmente empregado pela mídia, ou seja, de um cibercriminoso ou um criminoso com conhecimentos de informática. No entanto, na comunidade de segurança da informação, essa definição sempre foi contestada, sendo que um hacker pode ser uma pessoa que emprega seus conhecimentos para fins lícitos. O termo mais adequado para definir especialistas em burlar sistemas informáticos com fins ilícitos seria cracker. Esse termo começa a ser empregado

também no meio jurídico. O professor Damásio de Jesus ensina que são os crackers, e não os hackers – estes, pesquisadores de segurança da informação – que exploram as intimidades dos sistemas e também dos processos desenvolvidos sobre a tecnologia da informação para a prática de delitos [7].

Estando diante de um potencial cracker, surgiu, então, a preocupação de que o suspeito pudesse em poucos minutos se desfazer das provas digitais. Como era esperado que o alvo tivesse conhecimentos avançados de informática, foi trabalhado um cenário em que técnicas antiforenses pudessem ser aplicadas. Garfinkel define antiforense como uma técnica que usa métodos para remoção, ocultação ou subversão de evidências com o objetivo de mitigar os resultados de análises forenses [6]. Entre as técnicas de antiforense discutidas por Garfinkel, duas eram de especial preocupação da perícia: a sanitização dos dados (wipe) e a criptografia de volume ou disco completo. Causavam preocupação principalmente por poderem ser postas em prática muito rapidamente e por serem altamente eficientes em prejudicar ou até mesmo inviabilizar as análises periciais.

A sanitização dos dados consiste em apagá-los de forma segura, na qual as técnicas de recuperação de dados apagados usados pela perícia seriam ineficazes. Esse processo pode ser feito muito rapidamente em dispositivos móveis (smartphones), nos quais é disponibilizado pelos fabricantes opção de restaurar configuração de fábrica. A outra técnica antiforense consiste na criptografia de volume ou disco completo. Existem várias soluções de software para implementar essa técnica. Entre os mais famosos, pode-se citar o BitLocker do Windows, o FileVault da Apple, o TrueCrypt e o VeraCrypt. Se estivessem sendo usados, a melhor abordagem para a perícia seria chegar ao local e poder ter acesso aos computadores ainda ligados, tendo assim, a oportunidade de copiar os dados dos volumes montados (disponíveis para acesso) e realizar a cópia dos dados da memória volátil (RAM), em que técnicas periciais poderiam ser usadas para extrair as chaves criptográficas dessa memória. Porém, bastaria o suspeito puxar o fio da tomada dos computadores que todo esse processo seria inviabilizado e os dados poderiam se tornar inacessíveis se a senha de acesso não fosse fornecida.

Ciente desses pontos, a autoridade policial, junto com sua equipe, tomou todas as providências para que o suspeito fosse surpreendido e não tivesse tempo e nem oportunidade de pôr em prática a destruição das provas digitais.

A figura 1 ilustra os computadores do suspeito no momento da chegada dos agentes de polícia e peritos. É importante notar que os computadores estavam ligados e sem qualquer tipo de proteção que pudesse dificultar as análises iniciais ou posteriores. Esse cenário foi garantido pela rápida atuação da equipe policial e do esforço empreendido para a preservação do local de crime.

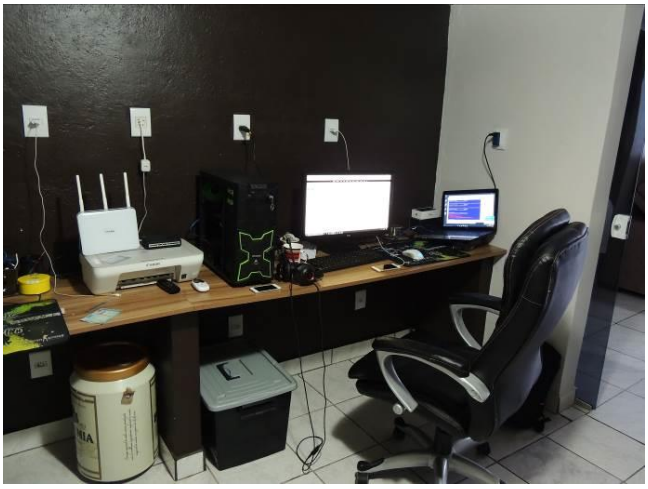

Figura 1. Computadores do suspeito.

A figura 2 ilustra um pendrive conectado ao computador do suspeito. A perícia descobriu que era nesse pendrive que estava a maioria dos códigos maliciosos responsáveis por parte da fraude. Se o suspeito de alguma forma tivesse conseguido ocultar ou destruir esse simples pendrive, parte importante das evidências teriam sido perdidas.

Figura 2. *Pendrive* com a maioria do código malicioso usado nas fraudes.

IV. Entendendo o modus operandi do cracker por meio das conversas encontradas

Tanto nos computadores como nos celulares periciados foi encontrada grande quantidade de conversas sobre fraudes pela Internet.

O suspeito participava de diversos grupos de aplicativos de mensagens e por meio desses grupos obtinha informações sobre como realizar ou aprimorar as fraudes. Também por meios desses aplicativos mantinha contato com partícipes dos crimes cometidos.

A abordagem pericial para a produção das provas elencadas no laudo iniciou-se pela análise de todas as conversas, compostas por milhares de mensagens. Por elas, foi possível adentrar na rotina, no dia a dia do suspeito e identificar o modo de operação do fraudador. Essa abordagem escolhida pareceu mais eficiente do que ir direto para a análise de milhares de arquivos contendo dados diversos. Dessa forma foi possível entender o modo de operação, estabelecer um roteiro de como os golpes eram aplicados e a partir desse ponto, buscar as evidências digitais que corroborariam ou não o modo de operação descoberto nas conversas.

Eram usados diversas gírias e abreviações de gírias que inicialmente tornavam o entendimento das conversas mais difícil. Com a análise do conteúdo de diversas mensagens foi possível entender o vocabulário próprio dos participantes do grupo. A tabela a seguir traz os principais termos usados e seus significados.

Termo ou Jargão	Significado
Spam	No contexto desse trabalho, o termo se refere a enviar uma grande quantidade de e-mails, na ordem de centenas de milhares ou milhões, contendo software malicioso, com objetivo de induzir as vítimas a fornecer dados bancários.
Spamar ou spama	Realizar spam.
Keylogger ou KL	Software malicioso, instalado no computador da vítima com objetivo de obter dados digitados pelos usuário, realizar captura de telas ou até mesmo promover o controle remoto total do computador alvo.
Info	Dados dos cartões bancários das vítimas. Pode incluir o número da conta, data de nascimento da vítima, telefone, número de cartão de crédito, entre outros necessários para realização das fraudes.
Lara	Abreviação de “laranja”. Pessoa usada para realização de saques bancários com os dados obtidos pela via cibernética.
Leto	Abreviação de boleto bancário.
Lotters	Termo que pode ser usado para comparsas que não cumprem com as obrigações financeiras acordadas (caloteiros) ou policiais infiltrados nos grupos de conversas sobre fraudes.
Infect	Software malicioso que infecta a máquina da vítima ou ato de infectar a máquina da vítima com software malicioso.
Coder	Programador. Pessoa com conhecimento para criar os softwares maliciosos que irão ser usados por outras pessoas no cometimento da fraude. Geralmente, não se envolve diretamente com a fraude. Obtém lucro vendendo ou alugando os programas criados para pessoas que irão efetivamente usá-los para cometimento da fraude.
Santa	Abreviação de Banco Santander.
Desco	Abreviação de Banco Bradesco.
Ita	Abreviação de Banco Itaú.
BB	Abreviação de Banco do Brasil.
Virar BB Virar Santa	O termo “virar” é usado para designar o processo de aproveitamento dos

Virar Desco	dados obtidos nas “infos” de forma efetiva. Parte dos dados das “infos” não “viram”, ou seja, não podem ser aproveitados. Os principais motivos para as “infos” não “virarem” são o cancelamento dos dados do cartão por parte dos clientes ou pelo banco e mecanismos de segurança do sistemas dos bancos.
Upar	Fazer o *upload* de software para um servidor, ou seja, enviar os dados de um computador local para um servidor. *Upload* é o processo inverso ao *download*.
Resgate de chip	Processo de transferir a linha de telefonia celular de uma vítima para o chip/celular do fraudador. Dessa forma, o fraudador terá acesso aos códigos de segurança enviados pelo banco via SMS àquele número de celular. O resgate é realizado com a participação de funcionários de lojas de telefonia celular.
Phishing	É uma maneira desonesta que cibercriminosos usam para enganar as vítimas para que revelem informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. É feito pelo envio de e-mails falsos ou direcionando as vítimas a sites web forjados.
RL	Abreviação de *Real Life* (Vida Real, em português). Termo usado pelos cibercriminosos para se referirem à pessoas que realizarão alguma atividade fora do ambiente cibernético (na vida real).
Engenharia Engenharia Social	Refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgação de informações confidenciais. No caso em tela, consiste em enviar e-mails para as vítimas com alguma história, visando induzi-las a realizar algum procedimento, como a instalação de um software, clicar em um link que irá redirecioná-las para páginas de banco falsas ou qualquer outra atividade que envolva a apropriação de dados bancários e pessoais com objetivo de fraude. Refere-se, também, a criação de páginas falsas convincentes de instituições bancárias.
Chipeira	Equipamento para acoplar diversos chips de telefonia celular e enviar SMS em massa.

Tabela 1. Termos usados pelo suspeito em conversas

Pela análise das conversas, é possível descrever sinteticamente que se tratava de um esquema de realização de fraudes em sistemas bancários por meio da obtenção de dados dos cartões bancários e de crédito das vítimas. A fraude começava pelo envio massivo de e-mails. Eram enviados a cada vez, centenas de milhares ou até milhões de e-mails para vítimas localizadas em diversos Estados brasileiros. Esse processo é referenciado nas conversas pelo termo “spamar”. A especialidade técnica do suspeito era o processo de “spamar”. Existem várias técnicas implementadas nos servidores de e-mails para bloquear o envio indiscriminado de grandes quantidades de e-mails. Uma das técnicas é a criação de listas negras de máquinas que enviem spams. O suspeito se utiliza de máquinas virtuais recém-criadas em serviços de nuvem, tais como Amazon AWS, Microsoft Azure, Google, entre outros. O suspeito também usava como técnica para evitar que as máquinas fossem classificadas com geradoras de spam e entrassem nas listas negras, o acréscimo de intervalos ou atrasos pré-determinados entro os envios. Era comum que cada máquina configurada funcionasse por algumas horas ou poucos dias. Depois desse tempo elas eram bloqueadas e novas máquinas em novas contas dos provedores de serviço de nuvem precisavam ser configuradas. Os recursos financeiros para a compra dos serviços de nuvem vinham das próprias fraudes.

Caiu
minha azure duro 5h kk
se todas durasse isso tava perfeito
te mandar a tela aqui
tu deleto as win?
a pa tira grana do card na santa?
Saldo Disponível Total (D + E) 6.591,51
quanto nois consegue ranca dessa vagabunda

Tabela 2. Conversa sobre maquinas na nuvem (Azure)

Ao clicar nos links desses e-mails, as vítimas eram redirecionadas para servidores configurados pelo suspeito com páginas falsas de bancos brasileiros. As vítimas, ao entrarem com os dados bancários nas páginas falsas, tinham seus dados coletados e enviados ao suspeito. Essa parte da fraude é conhecida como pescaria de senha ou

phising. Cada agrupamento de dados de uma determinada vítima é denominado no esquema como “info”.

De posse das “infos”, o esquema consistia em configurar computadores remotos para acesso às constas bancárias das vítimas via Internet Banking e tentar de alguma forma se apropriar do dinheiro contido nessas contas. A forma de fazer essa apropriação, segundo as conversas, variava dependendo da instituição. Uma das formas era realizar o pagamento de boletos bancários de terceiros usando as contas bancárias das vítimas, obtendo uma compensação financeira pela operação. Outra forma, era repassar esses dados a comparsas para que estes pudessem confeccionar cartões bancários falsos e, com a utilização de “laranjas” ou “laras”, pudessem ir até as instituições financeiras para realizar o saque de valor em espécie. Uma terceira forma consistia na aquisição de produtos por meios de sites de comércio eletrônico usando os dados bancários e de cartão de crédito das vítimas.

Nota-se, também, que os cartões de crédito e recursos advindos do esquema fraudulento eram usados para financiar infraestrutura de informática para a prática de novas fraudes, numa espécie de círculo de movimentação de recursos que alimentava o esquema.

A tabela 3 ilustra um trecho de conversa entre o suspeito e um comparsa.

P#!##! eu falo direto vamos roubar o sistema não nós mesmo aff
por isso a net fica desse jeito o cara passa um parceiro pra tras e os outros ficao desacreditados
tem bradesco - santander - itau - caixa - e entre outros esses banco tem dinheiro demais então vamos é roubar dele meu sonho é topar uma conta de um politico
<ss type="laugh">:D</ss>
alguem que nao e pilantra tem SCAM de SMTP ai ?

Tabela 3. Conversa entre o suspeito e comparsa.

Ficou claro que o *modus operandi* envolve um grupo de pessoas, cada qual exercendo função especializada que, integradas, permitem aos fraudadores obterem os ganhos financeiros ilícitos.

Podemos classificar os integrantes desses grupos em três categorias. Os especialistas em desenvolvimento de código malicioso, também conhecidos entre eles como *coders*; os implementadores da fraude, que fazem uso, personalizam e criam os ambientes informáticos para uso dos códigos maliciosos desenvolvidos pelos *coders*; e os laranjas, que possuem pouco conhecimento técnico e são os que geralmente atuam fora do mundo digital, ou *real life* (vida real), como é referenciado no meio.

Os *coders* são os que detém o maior conhecimento técnico e geralmente não realizam as fraudes e os ataques às vítimas diretamente. Eles lucram vendendo ou alugando seus códigos maliciosos para os implementadores da fraude. Estes possuem um conhecimento de intermediário a avançado. São a força motriz de todos o esquema. Usam uma coleção de *malwares* obtidos de diversas fontes, e os integram em um ambiente que permite a fraude. É nessa categoria que o suspeito alvo da operação relacionada a esse trabalho se enquadra. Os laranjas ou laras, como são também chamados, possuem pouco conhecimento técnico. Geralmente são responsáveis por retirar os recursos financeiros do mundo digital (*cash out*). Muitos emprestam seus nomes para criação de contas bancárias para as transferências de valores das contas das vítimas, em troca de um pequeno percentual nos ganhos obtidos da fraude.

V. Busca por *malware* e outros artefatos criminosos

Tendo-se descoberto o modo de operação do suspeito por meio da análise das mensagens, a perícia passou a procurar por evidências digitais que corroborassem esse modo de operação.

As cópias forenses dos computadores foram submetidas a ferramentas de indexação e análise.

Foram encontrados centenas de milhares de endereços de *e-mails*. Esses endereços eram usados na geração de *spam* (envio de *e-mails* em massa), consistindo de mensagens que visavam ludibriar as vítimas a clicar no *link* do *e-mail*, que as redirecionava para páginas falsas de instituições financeiras.

A mensagem do *e-mail* usava de engenharia social, ou seja, tentava convencer as vítimas que se tratava realmente de *e-mails* verdadeiros das instituições financeiras. Uma vez clicado no *link*, o usuário era direcionado a *sites* falsos. A figura 3 ilustra uma dessas páginas.

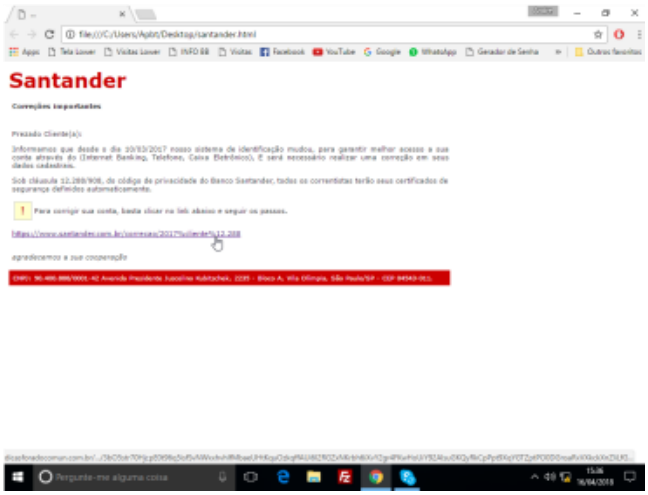

Figura 3. Página falsa de instituição financeira.

Prosseguindo nos exames, foram encontrados diversos dados das potenciais vítimas. Milhares de “infos”, como é conhecido o conjunto de dados cadastrais e de cartão de crédito das vítimas.

A figura 4 ilustra uma dessas “infos”. Os dados originais foram alterados para preservar a vítima.

```
######################################################################
IP: 191.251.xxx.xxx | DATA: 08/02/2017 | PC NAME: 191.251.xxx.xxx.dynamic.adsl.gvt.net.br
----------------------------------------------------------------------
NOME...................: LILIAN CARLA xxxxxx
EMAIL..................: financeiro@xxxxxxx.com.br
CPF....................: xxx.xxx.xxx-xx
NASCIMENTO.............: 29/08/1978
NOME CARD..............: lilian carla xxxxxx
NUMERO CARD............: 5140 xxxx xxxx xxxx
CVV....................: 7xx
VALIDADE...............: 01/20
----------------------------------------------------------------------

######################################################################
IP: 191.251.xxx.xxx | DATA: 08/02/2017 | PC NAME: 191.251.xxx.xxx.dynamic.adsl.gvt.net.br
----------------------------------------------------------------------
NOME...................: LILIAN CARLA xxxxxx
EMAIL..................: financeiro@xxxxxxx.com.br
CPF....................: xxx.xxx.xxx-xx
NASCIMENTO.............: 29/08/1978
NOME CARD..............: lilian carla xxxxxxx
NUMERO CARD............: 5443 xxxx xxxx xxxx
CVV....................: 6xx
VALIDADE...............: 08/17
----------------------------------------------------------+---------
```

Figura 4. “Infos” com os dados financeiros das potenciais vítimas

VI. Testando a eficiência do código malicioso

Nessa seção é apresentado o resultado na análise minuciosa que foi realizada em um dos softwares maliciosos encontrados no pendrive que estava conectado a máquina do suspeito.

Um dos objetivos dessa parte da perícia foi comprovar a eficácia de tal código, fornecendo material técnico para que os operadores do direito possam avaliar o fato da existência desse tipo de artefato digital e sua valoração legal.

A importância de se determinar a eficácia ou não de um malware é discutida pelo Professor Damásio de Jesus, na análise da Lei 12.737/2012 que tipifica algumas condutas como crimes informáticos: poderá haver situações em que se caracterize o crime impossível, tendo em vista a impropriedade do objeto, eis que, tal como não se mata um morto, não se invade o que está aberto. Até mesmo pela ineficácia do meio, o crime impossível poderá ocorrer, como no caso de agente que tenta invadir sistema bancário com software absolutamente ineficaz, comprovado por perícia técnica [7].

Pela perícia, pôde-se observar que o software malicioso encontrado era composto por arquivos HTML, Javascript e PHP, que são linguagens de programação para ambiente Web. Para a análise da eficácia, o malware foi executado em ambiente

controlado, utilizando-se virtualização, e sobre o escrutínio de um depurador de software (EclipsePHP). Essa técnica de perícia é denominada de análise dinâmica de malware. Esta análise consiste no estudo do funcionamento do software com o programa em execução, isto é, com o malware alocado em memória e consumindo recursos da CPU [2].

Dessa forma, o malware foi executado e com auxílio do depurador de código foi observada a execução e a intenção de cada linha de programação do software malicioso. O software criava páginas falsas do Internet Banking do Banco do Brasil, em que a cada página acessada, solicitava informações bancárias, pessoais e senhas de acesso das vítimas (figuras 5 e 6).
Após coletadas essas informações, elas eram compiladas em "infos". Essa "info" era então enviada para um e-mail específico. A figura 8 exibe um trecho do código PHP da página falsa do Banco do Brasil, sendo analisado com auxílio de um depurador (debugger). Esse trecho de código era responsável por montar a "info" e enviá-la por e-mail.

Por fim, era exibida a página da figura 7 e após alguns segundos, a vítima era redirecionada para a página real do Banco do Brasil. Esse redirecionamento é mais uma estratégia para ludibriar o usuário. Tendo acesso ao site real e prosseguindo no acesso normalmente, diminui a chance de o usuário perceber de imediato que teve seus dados furtados.

Por essa análise, ficou comprovado que o software malicioso era eficaz. As "infos" de diversas vítimas, encontradas no computador do suspeito, tinham o formato compatível com as geradas pelo programa malicioso analisado, demonstrando a efetiva utilização do programa.
Além do apresentado até aqui, as análises periciais encontraram mais uma série de evidências, compostas por: imagens de documentos de identificação de diversas pessoas, fotografias de diversos cartões bancários e de crédito, imagens de boletos bancários e outras contas, milhares de números de cartões de crédito. A perícia também conseguiu relacionar a identificação de um dos celulares do suspeito com os registros de fraude do setor de inteligência de uma das instituições financeiras lesadas.

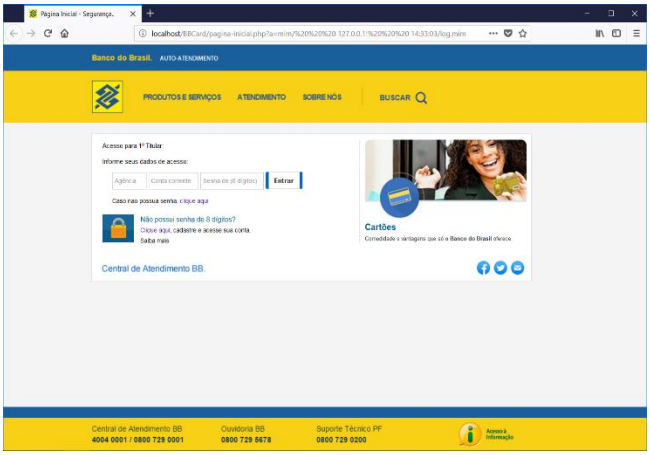

Figura 5. Página falsa do Banco do Brasil.

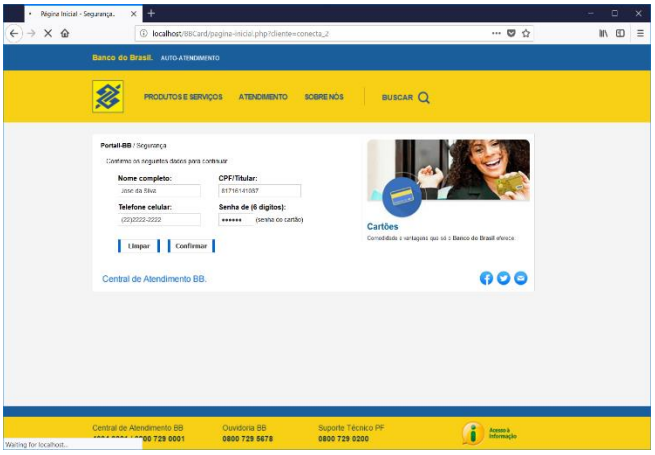

Figura 6. Entrada de dados na página falsa.

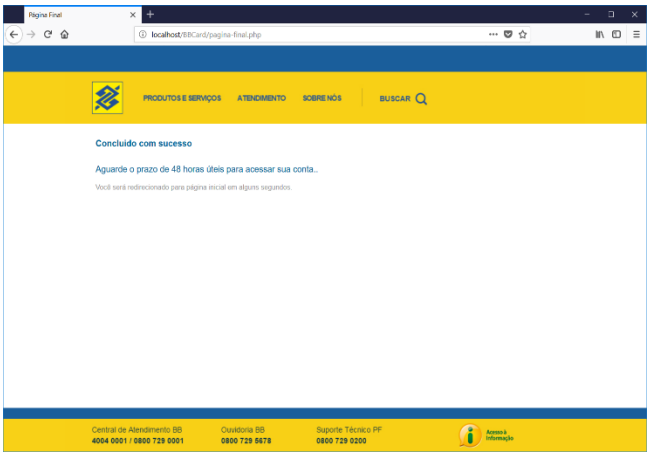

Figura 7. Conclusão da coleta dos dados das vítimas.

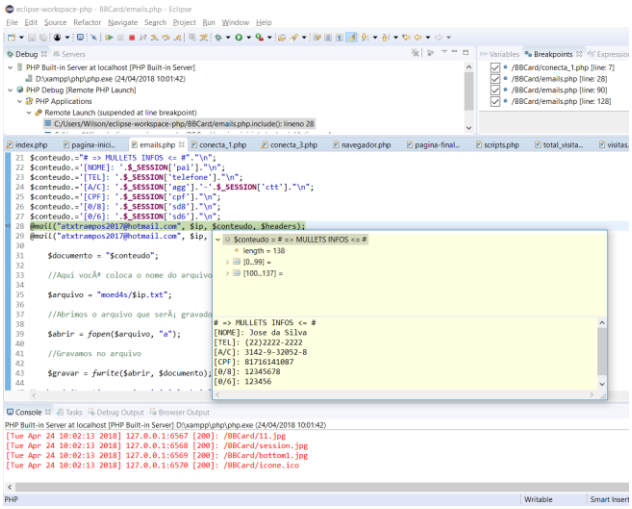

Figura 8. Depuração do código malicioso.

VII. Conclusão

Este artigo apresentou uma perícia realizada em um caso de fraude via Internet.

Foram analisadas questões desde as diligências de busca e apreensão até os exames dos artefatos maliciosos encontrados. Os cuidados tomados na busca e apreensão foram importantes para mitigar os riscos inerentes à destruição das evidências digitais pelo suspeito e garantir a preservação do local de crime. A análise das conversas dos computadores e celulares permitiu determinar o modus operandi do suspeito e os atores envolvidos nesse tipo de fraude.

A análise dos artefatos digitais permitiu corroborar o modus operandi e apresentar evidências digitais robustas em relação ao caso.

Espera-se que trabalhos desse tipo possam contribuir para a diminuição da impunidade deste tipo de delito.

Referências

[1] ABNT BR ISO/IEC 27037 – Tecnologia da Informação – Técnicas de Segurança – Diretrizes para Identificação, coleta, aquisição e preservação de evidência digital.

[2] Velho, Jesus Antonio; et al – Tratado de Computação Forense – Millenium Editora; São Paulo, 2016

[3] https://economia.uol.com.br/noticias/reuters/2018/03/21/pf-desarticula-grupo-responsavel-por-r10-mi-em-fraudes-bancarias-pela-internet.htm, acessado em 21/09/2018.

[4] http://tiinside.com.br/tiinside/seguranca/mercado-seguranca/13/06/2018/perdas-com-fraudes-bancarias-podem-chegar-a-us-93-bilhoes/, acessado em 21/09/2018.

[5] https://link.estadao.com.br/noticias/cultura-digital,cibercrime-faz-bancos-perderem-r-18-bilhao,10000028721, acessado em 21/09/2018.

[6] Garfinkel, Simon - Anti-forensics: techniques, detection and countermeasures, in: 2nd International Conference on i-Warfare and Security, 2007

[7] Jesus, Damásio E. de; Milagre, José Antônio - Manual de Crimes Informáticos – Editora Saraiva; 2016