DOI: 10.5769/C2015012 or http://dx.doi.org/10.5769/C2015012

Um Levantamento sobre o Mercado de Exploração de Vulnerabilidades do Espaço Cibernético

Robson de Oliveira Albuquerque, Rafael Timóteo de Sousa Júnior e João Paulo C. Lustosa da Costa

Departamento de Engenharia Elétrica, Universidade de Brasília (UnB)
Campus Universitário Darcy Ribeiro – Asa Norte – 70910-900 – Brasília-DF – Brasil

robson@redes.unb.br, desousa@unb.br, joaopaulo.dacosta@ene.unb.br

***Resumo*— O espaço cibernético é a base de sustentação de múltiplos setores da economia, constituindo-se como fonte de geração de recursos e capitais, bem como a projeção de poder de vários Estados. Logo, se tornou comum explorar vulnerabilidades da informação neste ambiente. As ferramentas de exploração de vulnerabilidades encontram-se no centro de um processo de produção e comercialização que, com seus diversos atores, constituem um mercado a parte. É importante para o profissional de segurança da informação e combate ao cibercrime ter conhecimento desse mercado específico, no sentido de organizar proteções de sistemas de informação, e também realizar investigações de evidências do cibercrime. Neste artigo, apresentam-se as definições dos elementos básicos desse mercado, além de um levantamento de algumas das principais empresas participantes. As conclusões apontam a necessidade de forte planejamento para correta atuação nessa área.**

***Abstract* – Cyberspace is now essential to support multiple economy sectors, as it constitutes a source of resources and wealth, as well as representing the projection of power from multiple nations. Due to its characteristics, cyberspace has become a place where the exploitation of information vulnerabilities occurs continuously. Tools for vulnerability exploitation are in the middle of a production and trade process, which, with a variety of actors, form a specialized market, dealing with large amounts of money. For law and enforcement agencies that fights cybercrime it is very important to have knowledge of such market, not only to protect information systems, but to perform cybercrime investigation and forensics activities. In this paper, definitions are given for the basic elements that take part in this market and relevant concepts related to exploits, as well as a review of enterprises that operate in this market. The conclusions point that strategic planning is a critical requirement to approach this cyber security area.**

***Keywords* – Security, Vulnerabilities, Exploits, Exploit and Vulnerability Market.**

I. INTRODUÇÃO

No cenário atual, a Internet que integra o espaço cibernético não pode ser vista apenas como mais uma rede de computadores mundial, mas sim a base de sustentação de múltiplos setores da economia como, por exemplo, hardware, software, telecomunicações, redes sociais, sistemas financeiros, moedas virtuais, serviços de indexação, armazenamento massivo e jogos online. Em diversos aspectos o espaço cibernético é a fonte de geração de recursos e capitais, bem como a projeção de poder de vários Estados, através do controle de recursos tecnológicos que compõem tal espaço.

O espaço cibernético está em franca evolução, em função do desenvolvimento ininterrupto de novas tecnologias e consequente desenvolvimento de soluções que têm o objetivo de atender às demandas crescentes do mercado. Este processo evolutivo gera um volume cada vez maior de informações estratégicas, corporativas e pessoais e que, idealmente, deveriam ser acessadas apenas por aqueles que teriam a legitimidade de tratá-las. Entretanto, dependendo do valor da informação que estiver sendo tratada, outros integrantes desse ecossistema, que não deveriam ter acesso à informação, têm não só interesse em acessá-la, mas também de copiá-la, modificá-la e, eventualmente, destruí-la.

Nesse espaço cibernético, está inserida uma área particular e específica de segurança da informação, área esta que trata de exploração de vulnerabilidades e de falhas de segurança. As explorações são realizadas das mais variadas formas e com os mais variados tipos de meios e tecnologias. Normalmente são realizadas com o intuito de se obter vantagem estratégica e competitiva, e também para a obtenção de lucros.

Este ambiente de exploração de falhas cibernéticas tem três raízes principais: o crime organizado, atividades hacktivistas e as ações de nações-estado [1], [2], [3]. De comum, os três fazem uso de técnicas de exploração de falhas e desenvolvem de mecanismos técnicos de garantia de obtenção do dado ou da informação desejada para posterior uso. Para a consecução do objetivo relacionado ao acesso à informação privilegiada, um atacante ou intruso utiliza as mais variadas técnicas e processos, mas é possível destacar o emprego de ferramentas de software projetadas especificamente para tirar proveito de alguma falha em um sistema computacional, normalmente para fins danosos como o de instalar um código malicioso, em inglês, *malware*.

Tais tipos de ferramentas, formalmente denominadas de *exploits* em inglês, vêm sendo objeto de todo um mercado de desenvolvimento, comercialização, manutenção e suporte, voltado para o crime cibernético (*cybercrime*). Sob a ótica deste cenário, o mercado de *exploits* é uma atividade complexa, de alto nível técnico e profissional, amplamente competitiva entre os atores envolvidos, e altamente lucrativa sob o aspecto financeiro e estratégico, no sentido de obtenção de algum tipo de vantagem.

Em função desse contexto, o objetivo deste artigo é o de demonstrar um levantamento da situação desse mercado, em especial do ponto de vista daqueles serviços e produtos que se encontram disponíveis para utilização em diversas situações.

Os dados coligidos são importantes para que o profissional de segurança da informação e combate ao *cybercrime* tenha conhecimento desse mercado específico, no sentido de organizar proteções de sistemas de informação, e de realizar investigações tanto para prevenção de crimes cibernéticos quanto para a investigação de evidências da ocorrência desses crimes. Além disso, o artigo aponta a necessidade de planejamento focado e com objetivos bem definidos para a inserção nesse tipo de atividade.

De maneira geral, este artigo está organizado nas seguintes divisões. A Seção II explica o que são *exploits* e temas correlatos, assim como o processo básico de emprego dessas ferramentas. Na Seção III tem-se uma discussão que trata de como o mercado de *exploits* está estruturado. Já a Seção IV apresenta alguns dos principais atores envolvidos. Por fim, as conclusões do trabalho encontram-se na Seção V.

II. DEFINIÇÕES E TERMINOLOGIA

O mercado de *exploits* pode ser analisado em uma perspectiva de consumidor (cliente) e fornecedor (especialista/empresa). Indiferente da perspectiva, para se abordar esse mercado é necessário planejamento, foco e objetivo concreto. É um mercado profissional que conta com desenvolvimento de técnicas e estudo de tecnologias em constante evolução, empregando pessoal técnico altamente capacitado.

A participação neste mercado como eventual gerador de necessidade não prescinde de um planejamento bem estruturado, de preferência com suporte e objetivo estratégico, que conte com infraestrutura própria e ferramentas específicas. Por consequente, tal participação requer recursos financeiros e técnicos para implementação de laboratórios avançados para testes de funcionalidades e técnicas de exploração, já que para se atender a uma necessidade, um objetivo claramente definido é fundamental.

Além disso, estes tipos de recursos técnicos e financeiros são aplicados de diversas formas. Por exemplo, para permitir a replicação das características técnicas e de ambiente de um alvo específico para testes de efetividade e exploração de uma oportunidade real. Note-se que esta atividade deve ser desenvolvida por pessoal qualificado na área de segurança cibernética. Esta área envolve diversas tecnologias e arquiteturas, tornado a atividade claramente multidisciplinar com viés técnico e especializado.

Assim sendo, podem ser considerados como requisitos mínimos para atuação neste tipo de mercado, o domínio e entendimento de tecnologias relacionadas a arquiteturas de hardware dos mais variados tipos, arquiteturas e plataformas de software para avaliação, desenvolvimento e testes funcionais, bem como domínio avançado de tecnologias e protocolos de redes de comunicação, sistemas operacionais, equipamentos de redes de comunicação, serviços de telecomunicação, entre outros requisitos.

Isso posto, um dos fundamentos básicos deste mercado é o *exploit* em si. Sob o aspecto de segurança, ele é o ponto de partida visando uma necessidade específica de emprego de recursos técnicos ligados a um objetivo concreto. É o *exploit* que oferece as condições mínimas de sucesso na exploração de falhas. Entretanto, para que o *exploit* obtenha sucesso, diversas etapas precisam ser entendidas corretamente.

Os tópicos a seguir detalham alguns aspectos de forma a explicar o que são vulnerabilidades *Zero-day*, o que são *exploits* e o processo básico de emprego dos mesmos. Para fins deste artigo, uma vulnerabilidade é um tipo de falha que permite ao atacante obter sucesso na exploração de um recurso tecnológico, seja ele na forma de um hardware ou de um software.

A. VULNERABILIDADES ZERO-DAY

Sob o aspecto de segurança da informação, uma vulnerabilidade *Zero-day* é um tipo de falha para a qual não existe defesa prévia eficiente devido ao fato de não existir uma correção ou uma atualização que a remova do produto sendo explorado. Isso permite a um atacante, considerando o seu objetivo e o nível de aprofundamento da exploração desejada, uma elevada taxa de sucesso na exploração da falha e, consequentemente, alcançar o objetivo desejado seja ele relacionado à obtenção de informações, seja ao controle do recurso explorado, seja à negação de serviço ao recurso por parte de outrem.

Relacionado ao desenvolvimento de produtos e aplicações na área de tecnologia e segurança da informação, um *Zero-day* é uma falha cujo responsável pelo produto ou aplicação não teve tempo hábil para correção antes de a falha ser explorada, seja por total desconhecimento prévio da falha, seja por inexistência de tempo hábil de publicação de correção antes de a falha ser conhecida e explorada.

Após a falha ser publicamente conhecida através de canais oficiais de divulgação, lista de segurança, entre outros, ela deixa de ser considerada uma vulnerabilidade *Zero-day* e passa a ser uma falha explorável em condições que atendam a versão que é atingida por determinada falha.

Devido as características de desenvolvimento de determinados sistemas, uma falha atinge uma única versão de um determinado produto, ou atinge múltiplos produtos em múltiplas versões. Exemplo disso é o caso da falha estar em uma biblioteca que é base de desenvolvimento de vários produtos.

B. EXPLOIT

Do ponto de vista técnico, um *exploit* [4] é um trecho de código de programa desenvolvido e compilado para uma arquitetura de hardware ou para uma arquitetura de software ou para um tipo de aplicativo. Este código é criado com o intuito de explorar uma vulnerabilidade associada a um recurso tecnológico, podendo inclusive ser para exploração de vulnerabilidade *Zero-day*.

Em um maior detalhamento, um *exploit* é um trecho de código que normalmente utiliza técnicas de linguagem de máquina de baixo nível, por meio de instruções de registradores em linguagem *assembly* que são capazes de manipular recursos de entrada e saída de memória e de recursos de processamento. Através deste tipo de manipulação, onde exista uma falha capaz de ser explorada em uma aplicação ou hardware, um *exploit* faz com que um conjunto arbitrário de instruções desejada pelo atacante sejam executadas, em detrimento do conjunto original de instruções que deveria ser executado na aplicação explorada.

Do ponto de vista de segurança da informação um *exploit* pode ser visto e entendido como uma arma cibernética. É um recurso tecnológico especializado que faz uso de técnicas específicas relacionadas à arquitetura de hardware e software, cujo efeito gera vantagem estratégica a um atacante e causa prejuízos variados a quem se torne alvo de uma arma deste tipo.

O *exploit* é um recurso técnico eficiente se bem empregado e se bem controlado, que permite o acesso não autorizado a recursos computacionais, possibilitando a escalação de privilégios ou realizando a negação de serviços. Caso um *exploit* seja mal empregado, ele se torna um recurso perdido. Uma vez utilizado fora do ambiente de controle, um *exploit* deixa de ter a eficiência desejada. Ainda, caso mal empregado, permite a implicação de autoria, e como consequência, de possíveis acusações envolvendo crime e espionagem cibernética.

Há basicamente dois tipos de *exploit* – local e remoto. Um *exploit* local é aquele onde o atacante já possui acesso a um determinando recurso computacional e executa localmente um determinado código com o intuito de aumentar suas permissões no recurso explorado, instalar determinadas ferramentas auxiliares ou permitir ainda que seja possível o controle remoto do recurso computacional mediante exploração de falhas. Um *exploit* remoto é aquele onde o atacante é capaz de executar um determinado código por meio de um canal de comunicação ou uma rede, permitindo a exploração de falha no recurso computacional, sendo possível o seu controle remotamente.

Assim, um *exploit* é um recurso técnico que pode atingir qualquer usuário em qualquer ambiente cibernético, seja ele conectado ou isolado, sendo que, neste último caso, o *exploit* pode ser inserido no ambiente por meio de dispositivos removíveis. Normalmente, um *exploit* [5] pode alterar o funcionamento do hardware ou do software, permitindo que sejam instalados ou manipulados outros recursos de acordo com o objetivo do atacante.

C. Processo Básico de Emprego de um Exploit

Um *exploit* pode ser utilizado das mais variadas formas e técnicas. Por exemplo, pode ser um pequeno arquivo executável para uma plataforma de hardware e software, pode ser embutido em páginas na Internet, pode ser um arquivo anexo a uma mensagem de correio eletrônico, pode vir na forma de uma mensagem de texto em um celular, pode estar embutido em arquivos digitais com as mais variadas extensões.

Uma vez executado, o *exploit* permite ao atacante realizar ações no ambiente cibernético, como por exemplo, permitir o controle remoto de determinados dispositivos através de um canal de comunicação, ou causar falha ou interrupção de serviços computacionais e de sistema de controle de outrem. Para ser eficiente, um *exploit* faz uso de técnicas de exploração de falhas que permitem ao atacante a execução de instruções visando o controle do recurso computacional desejado.

O desenvolvimento de *exploits* passa por etapas específicas que variam de acordo com o recurso a ser explorado. Desta forma, para uma vulnerabilidade ser passível de exploração em tempo hábil é necessário, no mínimo, o domínio da tecnologia a ser explorada. Isto envolve a capacidade de entender ou replicar o ambiente a ser explorado. Entretanto, o *exploit* pode ser desenvolvido por meios próprios ou ser adquirido para um propósito particular, observada uma janela de oportunidade.

De maneira geral, o processo de emprego de um *exploit* segue um ciclo de vida, conforme a Figura 1, cujas etapas são explicadas na Tabela 1. Observa-se nessa figura que a janela de oportunidade, durante a qual o recurso está explorável, é variável em função de vários aspectos, como tempo de atualização, tempo de descobrimento, complexidade da falha, entre outras.

Conforme o estudo de Bilge e Dumitras [7], são conhecidos alguns detalhes da janela de oportunidade. Por exemplo, o tempo médio de detecção de um ataque utilizando uma vulnerabilidade *Zero-day* é de 300 dias após o recurso computacional já se encontrar em fase de exploração por um atacante. Nesse período, normalmente não estão disponíveis atualizações, assinaturas de antivírus ou sistemas de detecção de intrusão, o que faz com que a detecção seja mais difícil e complexa. Ainda em [7], encontra-se a informação de que a duração de ataques que exploram falhas *Zero-day* varia entre 19 dias e 30 meses.

Fig. 1. Processo Básico de Emprego de um *Exploit* (Adaptado de [6])

TABELA I. Etapas do Ciclo de Emprego de um *Exploit*

Etapa	Descrição
1 – Lançamento de um produto	Nesta etapa é disponibilizado um produto de um fabricante no mercado de tecnologia da informação. Este produto pode ser um *hardware* com *software* customizado, pode ser um *software* aplicativo, um sistema operacional, uma plataforma cliente-servidor ou qualquer recurso técnico que faça uso de algum recurso computacional.
2.1 – Descobrimento privado de vulnerabilidade	Nesta etapa, por meio de pesquisa e desenvolvimento, um determinado grupo, empresa ou pessoa, descobre uma determinada vulnerabilidade. Caso esta vulnerabilidade não seja divulgada publicamente, ela se torna uma vulnerabilidade *Zero-day*.
2.2 – Relatório Público de vulnerabilidade	É quando uma vulnerabilidade é descoberta e publicada na Internet, seja por um grupo de pesquisa, uma empresa, seja pelo próprio fabricante do produto. Nesta etapa, normalmente, o responsável pelo produto é previamente avisado para que desenvolva a respectiva correção do produto antes da divulgação em massa da falha. Vale observar que antes da correção, qualquer produto atingido pela vulnerabilidade é passível de exploração.
3 – Criação de Prova de Conceito (PoC)	Dado o conhecimento da vulnerabilidade, é desenvolvido um código prévio que demonstra a capacidade da exploração da vulnerabilidade. Normalmente a PoC é um passo para a criação de um *exploit* para o produto vulnerável.
4 – Desenvolvimento de atualização do produto	O fabricante é capaz de desenvolver uma nova versão do produto, de maneira a evitar que o *exploit* seja eficiente em termos de exploração da falha de segurança.
5 – Disponibilização de atualização	O responsável pelo produto torna público a sua atualização, de forma que os usuários desse produto possam fazer a respectiva atualização e consequentemente evitar que o produto seja explorado.
6 – Aplicação da atualização	Os usuários devem ter um processo de manutenção de atualização do produto, de forma a fazer com que o produto seja atualizado com uma versão que não seja explorada.

Cabe ressaltar que ataques que utilizam falhas *Zero-day* normalmente possuem alvos direcionados, o que os tornam

mais difíceis de detectar através de uso de técnicas convencionais, já que muitas vezes, quem é alvo de tais ataques não torna público o ataque e muito menos divulga detalhes do mesmo. O estudo [7] mostra ainda que tornar pública uma vulnerabilidade resulta em aumento significativo do número de sistemas atacados. Isso pode ser ainda confirmado atualmente conforme relatório de segurança da informação divulgado pela Verizon [8].

A respeito do processo de emprego de um *exploit*, observa-se que algumas etapas são fundamentais. Por exemplo, o atacante precisa conhecer no mínimo o recurso a ser explorado, ser capaz de desenvolver o código para a falha a ser explorada e observar, além da efetividade do código, o tempo efetivo de exploração, dentro da janela de oportunidade.

Cabe ressaltar que, para uma determinada falha para ser explorada, é precisa haver um objetivo bem definido, incluindo a especificação do recurso a ser explorado, e os processos de análise da falha e de desenvolvimento do método e das ferramentas de exploração. Por exemplo, explorar uma falha para controlar remotamente o dispositivo computacional, em termos de código, é totalmente diferente de copiar dados do ou para o recurso, que por sua vez é diferente do código que altera a funcionalidade do recurso, e assim por diante. Além disso, uma falha é explorável dentro de uma janela de oportunidade, que é variável.

III. LEVANTAMENTO SOBRE MERCADO DE *EXPLOITS*

O que determina um mercado comercial é basicamente a lei da oferta e da demanda. No espaço cibernético existem diversas fontes relacionadas à negociação de *exploits*, seja na forma de comércio entre pessoas, entre empresas e pessoas, entre empresas, entre empresas e governo. Isto é variável e normalmente é dependente da necessidade de cada um que esteja envolvido em tal processo.

O fato é que existe tal mercado. Muitas vezes ele é considerado legal, uma vez que existe a negociação lícita, dentro do que rege a lei, sendo negociado a cifras elevadas por entidades e governos. Entretanto, ele também pode se caracterizar como ilegal em muitos aspectos, já que há também produtos adquiridos por meio de fóruns eletrônicos sem nenhum tipo de controle e com as mais variadas formas de pagamento, inclusive relacionadas a atividades de crimes cibernéticos, encontrando-se até mesmo definidos na legislação em diversos países. Diante dessa situação, caracteriza-se como uma necessidade social o estabelecimento de processos e técnicas forenses relativas a tais ambientes.

O mercado de *exploits* é incentivado pelo descobrimento de falhas de segurança em sistemas computacionais que não são reportadas ao fabricante desses sistemas para a devida correção. Assim, os responsáveis pelo descobrimento têm a possibilidade de vender a falha, havendo casos de valores de venda substanciais, como U$ 500.000,00, segundo reportagem da revista Forbes [9]. Constata-se que os valores são variáveis dependendo da utilidade e efetividade do *exploit* sob o ponto de vista do interesse do comprador, da abrangência da falha ou da dificuldade de exploração de um determinado recurso.

O mercado de *exploits* também está ligado ao mercado do crime cibernético. Um estudo realizado pela empresa Hewlett-Packard (HP) aponta que existe um crescimento do impacto financeiro relacionado à segurança da informação da ordem de 40% [10]. Esse estudo também aponta que, em uma análise de organizações dos EUA, o custo médio do crime cibernético para essas organizações foi da ordem de U$ 8.900.000,00 em 2012. Esta cifra representa um aumento de 6% quando comparado aos dados de 2011 e 38% quando comparado a 2010. O estudo apontou que em 2012 houve aumento de 42% no número de ataques cibernéticos, com as organizações passando por uma média de 102 ataques com sucesso por semana, com custo médio de solução na ordem de valores de U$ 591.780,00.

Se uma organização é alvo de um ataque cibernético furtivo mediante uso de falhas *Zero-day*, é provável que ela não descubra o efeito desse ataque antes de a falha se tornar pública e, muitas vezes, antes que o fabricante tenha disponibilizado uma correção. Neste caso, o prejuízo pode ser incalculável sob os mais diversos aspectos, gerando diversas formas de perdas para a empresa.

Outro estudo, este da empresa Symantec Labs [11], lista dados do ano de 2013 que revelam características do mercado de *exploits*:

- Houve 91% de aumento em campanhas de ataques direcionados a um alvo específico;
- Aumento de 62% no número de falhas de segurança;
- Mais de 552 milhões de identidades foram expostas;
- Pelo menos 23 falhas *Zero-day* descobertas;
- Cerca de 38% de usuários de plataformas móveis experimentaram problemas com crimes cibernéticos;
- Aumento de 66% no volume de mensagens não solicitadas; e
- 1 em cada 392 e-mails continha ataques de roubo de senhas.

De acordo com um estudo conduzido por Goncharov [12], da empresa Trend Micro, há no mercado cibernético Russo um submundo que é ativo de maneira organizada desde 2004 e é utilizado como mercado para troca de informações sobre vulnerabilidades e *exploits*. Nesse caso, alguns dos atores, como zloy.org, DaMaGeLab e XaKePoK.NeT, são bastante utilizados e constituem a bastante tempo focos de atividades relacionadas ao mercado de crimes cibernéticos em geral. Também existem diversos outros casos mais recentes, tais como o 1337Day para *exploits*, e, em um domínio diverso mas aparentado pela suscetibilidade ao crime organizado, os casos SILKROAD e AGORA para drogas.

A. *ASPECTOS ESTRATÉGICOS*

O ponto chave do estudo de Goncharov [12] é a descrição do alto nível de especialização de muitas partes do mercado de crime cibernético russo. O relatório analisado deixa claro que um *hacker* com uma boa cadeia de relacionamentos e contatos não precisa mais criar todas as suas armas cibernéticas. Tais armas simplesmente podem ser compradas de outro *hacker*, ou se pode alugar uma plataforma de negação de serviço, ou terceirizar determinadas funções. Nesse mercado, existem especialistas para qualquer tipo de atividade no espaço cibernético, incluindo cifração, ataques de negação distribuídos, redirecionamento de tráfico, serviços de *Pay-Per-Install* (Pague por instalação de *malware*), entre outros.

O estudo ainda apontou que houve depreciação em valores de acordo com o tipo de serviço. Por exemplo, a Tabela II aponta que no caso do furto de cartões de crédito, em vários países, o preço unitário encontra-se em queda desde 2011.

TABELA II. PREÇO (US$) PARA DADOS DE CARTÕES DE CRÉDITOS FURTADOS (FONTE: TREND MICRO [12])

País	2011	2012	2013
Austrália	7	5	4
Canadá	5	5	4
Alemanha	9	5	6
Reino Unido	7	6 – 8	5
Estados Unidos	3	1	1

No que se refere a contas de serviços de e-mails e redes sociais, conforme dados da Tabela III, o estudo aponta que o preço médio de sequestro de contas está em declínio. De maneira geral, os dados mostram que, dependendo do tipo de atividade, o custo tem diminuído em função do aumento da oferta por esses serviços no mercado russo.

TABELA III. PREÇO (US$) PARA CONTAS HACKEADAS (ADAPTADO DE TREND MICRO [12])

Serviço	2011	2012	2013
Facebook	200	160	100
Gmail	117	120	100
Hotmail	107	100	100
Mail.ru	74	70	50
Twitter	167	40	--

Além disso, o relatório aponta que a oferta excessiva também tem influenciado na qualidade da oferta. Já que a competitividade é alta, a qualidade dos produtos ofertados muitas vezes é duvidosa e estes não fazem a função para a qual foram comprados. Este aspecto apenas reforça a necessidade de entender-se o que está sendo negociado, o que torna fundamental a capacidade de verificação técnica, para obter uma exata caracterização do produto comercializado.

Um aspecto a ser observado é que a questão vai além do preço de produtos, sendo importante se observar quem é que está pagando por *exploits Zero-day*. Em uma reportagem da revista Forbes [9], um negociador intermediador (*broker*), conhecido pelo codinome Grugq, relata que a maior parte dos clientes é de governos ocidentais, tipicamente EUA e Europa, simplesmente pelo fato de que eles pagam mais do que russos e chineses, por exemplo.

Na entrevista realizada [9], o citado *broker* reportou que vender determinados produtos para a máfia russa é mau negócio, porque além de pagar pouco, há grande chance de que o produto tenha pouca utilidade em poucos dias, caso seja um *exploit*. Além disso, há na Rússia muitos criminosos cibernéticos, o que faz com que o preço deste tipo de produto derive da alta competitividade e custo muito baixo. Isso ainda é agravado pelo fato de haver muita desonestidade na negociação de produtos versus sua real efetividade no mercado russo.

Ainda segundo o entrevistado em [9], no caso do mercado chinês, que também possui um número elevado de *hackers*, a venda de armas cibernéticas por *hackers* chineses é exclusiva para o governo chinês, e o preço é muito baixo. A reportagem [9] ainda aponta que outros mercados de artefatos cibernéticos, como Oriente Médio e Ásia não superam o preço ofertado pelos países ocidentais.

B. MERCADO CIRCUNSCRITO

O mercado de *exploits* apresenta um agravante por se constituir um mercado circunscrito, muito particular e fechado. Em consequência de ser um mercado reservado, nele existem vulnerabilidades que são conhecidas apenas por grupos privilegiados e restritos. Nesse cenário, estão inseridos criminosos cibernéticos específicos e *brokers*, que normalmente possuem uma rede privilegiada de contatos.

Além disso, agências de diversos governos também estão inseridas neste mercado restrito, tanto no papel de consumidores quanto de membros ativos. A atuação de agências de governo se concretiza influenciando na criação de produtos com falhas de segurança. Também ocorre pela interferência na criação de padrões de mercado com dificuldades técnicas que proporcionam vantagens para agências de inteligência dotadas de recursos técnicos e alta capacidade de processamento e armazenamento.

Reitera-se que, por compreende elevada capacidade técnica e recursos financeiros significativos para investimento em pesquisa de novas vulnerabilidades e desenvolvimento de novos *exploits*, mercado circunscrito representa um alto risco para quem lida diretamente com desenvolvimento de software e para fabricantes que possuem produtos na lista de interesse da comunidade de inteligência, tais como sistemas operacionais, hardware para comutadores de rede, roteadores, memórias de computadores, soluções de segurança da informação, entre outros.

Um dos pontos fundamentais desse mercado circunscrito reside no fato de que os grupos participantes têm acesso à informação crítica, o que permite que eles possam comprometer sistemas vulneráveis sem que o público jamais conheça essas ameaças.

Nesse aspecto, um estudo de 2013 da NSS Labs [13] analisou uma série com dados de diversos anos de dois grandes programas de vulnerabilidades e os resultados apontaram que nos últimos 3 anos anteriores ao estudo, em qualquer dia, grupos privilegiados tinham acesso a pelo menos 58 vulnerabilidades, tendo como alvo sistemas de empresas como Microsoft, Apple, Oracle ou Adobe. Além disso, essas vulnerabilidades continuaram privadas por uma média de 151 dias. Neste caso, a janela de oportunidade (vide Figura 1) é da ordem de meses para os detentores de tais armas cibernéticas que nesse intervale tiveram a oportunidade de fazer uso de técnicas de infiltração, exfiltração de dados, controle remoto, vigilância cibernética, entre outras, virtualmente sem serem detectados ou combatidos.

C. CUSTOS DE EXPLOITS

É muito difícil definir o real custo de um *exploit*, haja vista a necessidade de empregar vários critérios de análise, além do tipo do *exploit*. Normalmente, características como a complexidade ou facilidade do uso, a efetividade, a especificação do alvo, a janela de oportunidade, localização do alvo, dificuldade de penetração, etc., são fatores que influenciam na composição do preço final de uma arma cibernética.

Na citada reportagem da Forbes [9], alguns números puderam ser correlacionados ao tipo de produto do mercado de tecnologia da informação afetado eventualmente por um *exploit* para uma vulnerabilidade *Zero-day*, conforme resumo na Tabela IV.

Em um levantamento específico para este artigo, atualizado com valores para 2015, algumas ferramentas com uso direcionado e de maneira restrita foram encontradas oferecidas por um único *hacker* (http://apt0.no-ip.biz/). A Tabela V indica alguns valores para produtos específicos, embora os dados não se adequem a uma comparação de preços nem a uma análise de depreciação. Entretanto, indicam que, uma vez que um determinado *Exploit* funcione em uma determinada versão do sistema alvo, os interessados em adquirir tal produto podem pagar um valor que depende de fatores que são inerentes ao

próprio *Exploit* (eficiência, por exemplo). Vale observar que a Tabela V não contempla *exploits Zero-day*.

TABELA IV. PREÇO (US$) MÉDIO DE UM *EXPLOIT ZERO-DAY* (ADAPTADO DE TREND MICRO [12])

Produto	Preço Estimado
Adobe Reader	5.000 – 30.000
Mac OSX	20.000 – 50.000
Android	30.000 – 60.000
Flash ou Plugins Java para Navegadores	40.000 – 100.000
Microsoft Word	50.000 – 100.000
Windows	60.000 – 120.000
Firefox ou Safari	60.000 – 150.000
Chrome ou Internet Explorer	80.000 – 200.000
IOS	100.000 – 250.000

TABELA V. PREÇOS (US$) DE *EXPLOITS ENCONTRADOS EM 2015*

Ferramenta	Sistema Alvo	Preço
Exploits, *Kits* de teste de penetração, infeção silenciosa	Firefox 22-27	200 (reduzido)
Mozilla Firefox *Bootstrapped Code Execution*	Firefox addon (Windows 7, Windows XP, Window 8.1)	400 (reduzido)
OLE automation array remote code execution	Internet Explorer <= 11	800
WolfPack	Java 1.6.0* Java 1.7.0_06 Java 1.7.0_10 Java 1.7.0_17 Java Applet (Windows 7, Windows XP, Window 8.1)	1000
Exploits, *Kits* de teste de penetração, infeção silenciosa	Firefox 31-34 (Windows 7)	800
Polymorphism IE11 Exploit Source Code	Internet Explorer 11 (Windows 7)	1200
Polymorphism Firefox 31-34 Exploit Source Code	Firefox 31-34 (Windows 7)	1000
Insanity - Infection Kit	Locação de infraestrutura para testes de penetração em sistemas	2000 (por mês)

D. PROGRAMAS DE RECOMPENSA PARA DESCOBERTA DE FALHAS

E. PREÇO MÉDIO (US$) PAGO POR *BUG BOUNTY PROGRAMS* (ADAPTADO DE FREI [13])

Empresa	Preço (US$)	Descrição
Google	~ 580.000	Preço médio durante 3 anos por 501 vulnerabilidades descobertas no navegador Chrome. Equivale a 28% de atualizações no mesmo período.
Mozilla	~ 570.000	Preço médio durante 3 anos por 190 vulnerabilidades no navegador Firefox. Equivale a 24% de atualizações no mesmo período.
Facebook	~ 1.000.000	Preço médio pago desde 2011 em seu programa de vulnerabilidades.
Microsoft	~ 130.000	Preço médio desde 2013 para programa de reporte de novas técnicas de exploração de falhas.

Além do setor de mercado de produtos e infraestrutura, verifica-se um setor de programas de recompensa para descoberta de falhas (*Bug Bounty programs*), cujos dados encontram-se na Tabela VI, conforme o estudo conduzido pela NSS Labs [13].

F. FORMA DE COMERCIALIZAÇÃO

Verifica-se um aumento do número de empresas que oferecem *exploits Zero-day* para os clientes, em um modelo de venda por assinaturas. Tais empresas normalmente não revelam seus clientes. Entretanto, grandes compradores incluem agências de governo. Neste caso, algumas empresas oferecem 25 *exploits Zero-day* por ano, ao custo de US$ 2.500.000,00 (preço de 2010) [9].

Outros dados disponíveis na Internet apontam que o preço médio da assinatura está entre US$ 40.000,00 e US$ 160.000,00 para clientes restritos de determinados países (explicitamente, Estados Unidos e Europa), relativamente a uma média de 100 *exploits* exclusivos por ano.

Existem ainda plataformas de desenvolvimento e de distribuição de *exploits* com vulnerabilidades *Zero-day*. Uma delas, amplamente conhecida para técnicas de exploração e comando e controle, é o Metasploit [14], disponibilizada tanto em versão pública como em versão comercial, sendo ambas as versões coordenadas e mantidas por uma empresa americana.

Outra plataforma, menos difundida, mas aparentemente muito conhecida no mercado de segurança cibernética, é conhecida como *Elderwood Project*, tendo sido reportada publicamente pela equipe de segurança da empresa Symantec [15]. Tal plataforma, relacionada a um grupo específico de *hackers*, permite a criação de vetores de ataques e códigos para vulnerabilidades em sistemas Adobe Flash e navegadores Internet Explorer, por exemplo.

Existem dados em fontes abertas que apontam o uso desta plataforma em ataques conhecidos como a "Operação Aurora". Também existem relatos de arquivos de *malware* relacionados ao *Elderwood Project* em países como Estados Unidos, Canadá, China, Austrália, Hong Kong, entre outros. Uma característica marcante do grupo relacionado ao *Elderwood Project* é que o seu foco de ataque são empresas que atuam como fornecedores de equipamentos eletrônicos, cujos principais clientes são grandes empresas da área de defesa.

IV. EMPRESAS ESPECIALIZADAS

Conforme o mercado se movimenta, existem empresas que fornecem serviços especializados na área de *exploits*. A seguir, são apresentadas algumas dessas empresas cujos dados estão disponíveis na Internet.

A. VUPEN

A Vupen é uma empresa francesa que participa ativamente do mercado de *exploits* e *bug bounty programs*. Segundo dados da própria empresa, todas as vulnerabilidades da Vupen são de desenvolvimento próprio e permitem a agências de governo e à comunidade de inteligência a condução de operações de rede em suas missões cibernéticas.

Segundo dados oriundos de fontes abertas [16], a lista de clientes da Vupen inclui governos, empresas de segurança em geral, empresas financeiras, de saúde, seguros, manufatura, tecnologia entre outros. Entre os clientes, a lista inclui países-membro da Organização do Tratado do Atlântico Norte (OTAN). Algumas fontes abertas [17] inclusive reportam que a estadunidense National Security Agency (NSA) comprou *exploits Zero-day* fornecidos pela Vupen.

B. REVULN

A ReVuln é uma empresa europeia situada em Malta. Segundo dados da própria empresa, seus serviços estão no estado da arte de pesquisa em segurança cibernética e em

soluções de segurança para clientes pelo mundo. É uma empresa especializada em pesquisa de vulnerabilidades para medidas ofensivas e defensivas em segurança cibernética.

Alguns relatos de fontes abertas [18] apontam que a ReVuln atuou na geração de códigos para serem explorados em usuários de redes de jogos online e que a lista de clientes inclui a NSA e adversários americanos como o grupo Guardas Revolucionários do Irã.

C. NETRAGARD

A Netragard é uma empresa americana que atua no mercado de segurança, com desenvolvimento de *exploits* e testes de penetração. A empresa trabalha com uma plataforma proprietária denominada *Real Time Dynamic Testing*, que segundo a própria empresa é diferente de produtos comuns e ferramentas automatizadas. A empresa mantém times permanentes de pesquisa em vulnerabilidades e desenvolvimento de *exploits*.

Segundo algumas fontes abertas [19] a lista de clientes desta empresa é restrita aos Estados Unidos.

D. ENDGAME SYSTEMS

A *Endgame Systems* é uma empresa americana que lida com inteligência em segurança da informação e análise de dados. Segundo dados da própria empresa, os produtos ofertados permitem uma visibilidade em tempo real em seus domínios digitais e através de uma variedade de aplicações que permitem resolver a mais variada gama de problemas digitais.

Segundo relatos de fontes abertas [20], a lista de clientes inclui a NSA, a Marinha e a Força Aérea Americanas, além da CIA, Inteligência Britânica e Comando Cibernético Americano.

E. EXODUS INTELLIGENCE

A *Exodus Intelligence* é uma empresa americana que lida com pesquisa e desenvolvimento de soluções de segurança cibernética. Sua missão institucional é prover aos clientes informações confiáveis e relacionadas a um contexto para suas vulnerabilidades e *exploits Zero-day* exclusivas.

Entre a lista de parceiros estratégicos desta empresa estão o Departamento de Defesa Americano, a DARPA, o NSSLabs, a Fortinet, entre outros.

F. HACKING TEAM

Hacking Team é uma empresa italiana que provê tecnologias ofensivas de comando e controle para agências de inteligência e de segurança. Seu principal produto faz uso de *exploits* e vulnerabilidades, para ser capaz de permitir controle remoto de diversas plataformas.

Existem relatos em fontes abertas [21] que apontam o uso de produtos desta empresa em pelo menos 30 países, incluindo Sudão, Azerbaijão, Arábia Saudita, Marrocos e Emirados Árabes.

G. AGT

A *Advanced German Technology* (AGT) é uma empresa alemã que oferece diversos produtos e soluções. Entre elas, é ofertado um sistema de comando e controle com técnicas avançadas de furtividade e exploração de vulnerabilidades para controle remoto de diversos dispositivos.

A lista de clientes da AGT inclui agências de segurança e forças da lei.

H. RAPID7

A Rapid7, uma empresa americana, é o braço comercial do *framework* de exploração de falhas *opensource* conhecido como Metasploit [14]. A empresa possui diversos produtos e serviços que variam de gerenciamento de vulnerabilidades até exploração de falhas e desenvolvimento de *exploits*.

A lista de clientes da Rapid7 inclui governos, agências de saúde, de telecomunicação, de energia, de finanças, entre outros.

I. IMMUNITYSEC

A *ImmunitySec* é uma empresa americana que trabalha com plataforma de comando e controle, desenvolvimento e implementação de *exploits*. A empresa possui aplicações e diversos *exploits* que são amplamente testados antes da sua disponibilização a seus clientes.

J. COREIMPACT

A CoreImpact é uma empresa americana que oferta sistemas de comando e controle e *exploits* para sistemas com o intuito de realizar testes de penetração em diversos cenários, plataformas e dispositivos.

K. GFI

A Gfi é uma empresa americana que oferta serviços na área de gerenciamento de vulnerabilidades para redes de comunicação e aplicação de atualizações de segurança contra falhas exploradas remotamente e localmente.

L. BEYONDTRUST

A BeyondTrust é uma empresa americana que provê soluções para o gerenciamento de vulnerabilidades. Seus produtos lidam com a identificação e resposta a vulnerabilidades de ataques cibernéticos.

M. BLUECOAT

A BlueCoat é uma empresa americana que provê soluções na área de *Advanced Persistent Threats* (APTs), análise de *malware* e soluções de análise de vulnerabilidades dos mais variados tipos. Os produtos são voltados para o mercado de segurança cibernética e possuem as mais diversas aplicações.

N. FINFISHER

A *FinFisher* é uma empresa alemã que atua no segmento de segurança cibernética oferecendo soluções para agências governamentais de segurança, comunidade de inteligência e governos. Seu foco de atuação está voltado principalmente ao combate a atividades criminosas no espaço cibernético. Ela atua em pesquisa e desenvolvimento e intrusão em sistemas de tecnologia da informação, segundo dados da própria empresa.

V. CONCLUSÕES

A inserção de uma instituição, ou mesmo de um profissional individual, na área de monitoração do mercado de vulnerabilidades, assim como no domínio geral da segurança cibernética, requer capacidades de análise, de acompanhamento constante, empregando pessoal técnico com formação avançada e treinamentos atualizados. Por sua importância nos domínios de segurança da informação, seja ela pública ou privada, é importante que a atuação nessa área venha provida de forte presença com competência e capacidade técnica, o que requer necessariamente investimento e planejamento de longo prazo.

Um planejamento estratégico definido é fator crítico de sucesso para atuação no mercado de vulnerabilidades, assim

como é fundamental para a correta atuação e inserção na área de segurança cibernética, mais especificamente para investigação no mercado de vulnerabilidades de sistemas computacionais, seja ela com o intuito de trabalho forense, seja ela para atuação contra o crime cibernético.

Do levantamento apresentado neste artigo, conclui-se que essa atuação parece ser considerada por diversos países como atividade sistemática, contínua, merecedores de alocação de recursos humanos, tecnológicos e financeiros, caracterizando-se, portanto, como estratégica para tais países. Vale ressaltar que a área cibernética não é um espaço para ações estanques e isoladas, sem foco e muito menos sem objetivo concreto. Assim, é estratégica também a geração de conhecimento específico sobre os processos e tecnologias de produção de *exploits*, o que é fundamental para a consecução do entendimento e avanço da análise de ameaças cibernéticas.

A oferta de *exploits* por parte de empresas ou grupos é uma realidade efetiva que pode talvez levar ao entendimento de que a exploração de vulnerabilidades se trataria apenas de comprar *exploits* de prateleiras e empregá-los contra determinados alvos. Em uma perspectiva de monitoração, atuação preventiva contra crimes, investigação forense, e atividades correlatas, requisita-se um entendimento mais abrangente, que inclua o esclarecimento de questões como: existência de alvo claramente definido; capacidade técnica, em termos de pessoas e recursos técnicos, suficiente para a definição e avaliação de ferramentas a serem adquiridas; diferentes implicações quando da aplicação de eventuais ferramentas, que podem ser usadas tanto para ofender e atacar, quanto para prevenir e defender; necessidade de atribuição de origem de manobras consideradas ofensiva no espaço cibernético; as medidas que devem ser tomadas em função do sucesso ou insucesso no emprego de determinada ferramenta; etc.

Algumas dessas questões têm, não somente implicações estratégicas, mas devem muitas vezes ser detalhadas em seus aspectos táticos e operacionais, de acordo com o nível de ação que se deseje empreender no mercado de vulnerabilidades. Por outro lado, visto que muitas das ferramentas aí disponíveis são usadas também no sentido de contribuir com medidas de proteção de sistemas cibernéticos, é importante ressaltar que utilizar dessa forma tais ferramentas requer preparação, não apenas adquiri-las, mas, principalmente, para ter um planejamento claro e definido do seu emprego, bem como ter capacidade de analisá-las, seja na perspectiva forense, seja na perspectiva de crime cibernético.

O presente trabalho, de caráter exploratório, apresenta atividades que têm a possibilidade de, ao menos parcialmente, ser objeto de automação, seja no levantamento, nas análises e na aquisição de conhecimentos, reunindo tecnologias de mineração de dados, filtragem, descoberta de padrões, representação de ontologias de segurança na área cibernética, etc., assuntos que constituem possíveis trabalhos futuros.

AGRADECIMENTOS

Os autores agradecem às Agências brasileiras de pesquisa e inovação CAPES (Projeto FORTE, Edital CAPES Ciências Forenses 25/2014) e FINEP (Convênio RENASIC/PROTO 01.12.0555.00), pelo suporte a este trabalho.

REFERÊNCIAS

[1] Clarke, Richard A.; Knake, Robert K.; “Cyber war”. Tantor Media, Incorporated, 2014.

[2] Shackelford, Scott J.; “Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace.”; Cambridge University Press, 2014.

[3] Hyppönen, Mikko H. "Information Security"; Proceedings of the IATUL Conferences 2014; Purdue University; Purdue e-Pubs; Disponível em http://docs.lib.purdue.edu/iatul/2014/keynotes/1/.

[4] Wu, J.; Arrott, A.; Colon Osorio, F.C., "Protection against remote code execution exploits of popular applications in Windows," Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on, vol., no., pp.26-31, 28-30 Oct. 2014; DOI: 10.1109/MALWARE.2014.6999416.

[5] Mahaffey, Kevin, John G. Hering, and James Burgess. "Security Status and Information Display System." U.S. Patent No. 20,140,373,162. 18 Dec. 2014.

[6] Tiedata. “What are Web Based *Exploits*?” Disponível em: http://www.tiedata.com/web*exploits*.asp. Acessado em maio de 2014.

[7] Bilge, Leyla; Dumitras, Tudor; “Before We Knew It - An Empirical Study of *Zero-day* Attacks In The Real World”. Symantec Research Labs. Outubro de 2012.

[8] Verizon Report. “The 2015 Data Breach Investigations Report (DBIR)”; 2015. Disponível em http://www.verizonenterprise.com/DBIR/2015/.

[9] Revista Forbes; “Shopping For *Zero-day*s: A Price List For Hackers' Secret Software *Exploits*”. Edição de 23 de março 2012.

[10] HP Research. “Cybercrime Costs Rise Nearly 40 Percent, Attack Frequency Doubles”. Publicado em 08 de outubro de 2012.

[11] Symantec Labs. “2014 Internet Security Threat Report”. Volume 19. Publicado em Abril de 2014.

[12] Goncharov, Max; “The Russian Underground, Revisited”. Cybercriminal Underground Economy Series. A Trend Micro Research Paper. Publicado em 28 de abril de 2014. Disponível em http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf.

[13] Frei, Stefan; “The Known Unknowns: Empirical Analysis of Publicly Unknown Security Vulnerabilities”; Analyst Brief; NSS Labs; 05 de Dezembro de 2013.

[14] Metasploit; “The Metasploit Project”; Rapid7, 2015. Disponível em http://www.metasploit.com/.

[15] O’Gorman, Gavin; McDonald, Geoff. “The Elderwood Project”. Symantec Security Response. 06 Sep 2012.

[16] Fidler, Mailyn; “Anarchy or Regulation: Controlling the Global Trade in Zero-Day Vulnerabilities”; Thesis submitted to the Interschool Honors Program in International Security Studies; Center for International Security and Cooperation Freeman Spogli Institute for International Studies; Stanford University; May 2014.

[17] Walker, Danielle; “NSA sought services of French security firm, zero-day seller Vupen”; SC Magazine; September 18, 2013. Disponível em http://www.scmagazine.com/nsa-sought-services-of-french-security-firm-zero-day-seller-vupen/article/312266/.

[18] Perlroth, Nicole; Sangerjuly, David E. “Nations Buying as Hackers Sell Flaws in Computer Code”; New York Times, July, 2013.

[19] Ungerleider, Neal; “How Spies, Hackers, and the Government Bolster a Booming Software Exploit Market”; Disponível em http://www.fastcompany.com/3009156/the-code-war/how-spies-hackers-and-the-government-bolster-a-booming-software-exploit-market.

[20] Harris, Shane; “The Mercenaries. Ex-NSA hackers and their corporate clients are stretching legal boundaries and shaping the future of cyberwar”. Disponível em http://www.slate.com/articles/technology/future_tense/2014/11/how_corporations_are_adopting_cyber_defense_and_around_legal_barriers_the.html.

[21] Reporters without borders; “The Enemies of Internet Special Edition: Surveillance”; Disponível em http://surveillance.rsf.org/en/hacking-team/.