# Prevenção de ataques *zero-day* por meio de vulnerabilidades divulgadas

Alexandre Yuji Kajihara

2017

## 1 Introdução

O crime cibernético é uma forma de crime que inclui crimes que são cometidos através do uso da Internet ou de outras redes de informáticas [1]. O aumento da disseminação de crimes por computador deve se a *Return On Investement* (ROI) derivado desse tipo de atividade criminosa [1]. Existem vulnerabilidades que podem valer mais de 100.000 dólares, dependendo da sua complexidade [2], um exemplo que podemos citar é as vulnerabilidades do tipo *zero-day*, que iremos explicar o que elas são logo abaixo, em que devido a esse retorno de investimento os valores variam, na qual no segundo dia ela pode valer um quarto do que valia no *zero-day* e no décimo dia o valor dela vale 1/1000 [1]. Além do que, essas vulnerabilidades são muito desejadas por agências governamentais, cibercriminosos e empresas de software [3].

Um dos tipos de ataque existente é o ataque de *zero-day*, em que acredita-se que o período em que provavelemnte ocorreram as primeiras vulnerabilidades de *zero-day* aconteceram nos anos 80 [1]. Esse ataque cibernético que explora uma vulnerabilidade que não foi divulgada publicamente, e esse ataques visam um número de organizações que possuem informações confidenciais que podem ser roubadas [2]. Essas vulnerabilidades permanecem desconhecidas até por 2.5 anos [2]. Enquanto a vulnerabilidade permanece desconhecida, o software obtido não pode ser corrigido e os produtos antivírus não conseguem detectar o ataque através da verificação baseada em assinatura [2].

Uma maneira de prevenção é a implementação de sensores ou defesas cibernéticas, *firewall* [4]. Outras maneiras de prevenção seria por meio de *Host Intrusion Protected Software* (HIPS), em que não se depende de assinaturas, já que há um monitoramente das atividades da máquina, usar um bom antivírus protegendo de ataques conhecidos e desconhecidos e atualizar suas aplicações sempre que houver notificação de atualização de *software* [3]. Usuários que utilizam o antivírus podem ter mais cuidados com a segurança de seus computadores, e podem ser menos expostos aos ataques [2]. Existem testes de penetração como o *Web Application Penetration Testing* (WAPT) [3]. Apesar de todas essas maneiras de prevenir é díficil, porque a informação só estará disponível quando o ataque tiver sido concluído [3]. Além disso, os fornecedores

de *software* dão preferência de corrigir vulnerabilidades que foram divulgadas ou estão prestes a declarar [2].

Como foi dito anteriormente, essas vulnerabilidades tem interessado pessoas, governos e empresas de software. No caso, dos ataques do tipo *zero-day* existem três tipos de mercados que vendem vulnerabilidades de *zero-day*, que no caso são o mercado negro, cinza e branco. O mercado branco é um mercado legal que não está escondido, em que as empresas de tecnologia pagam aos pesquisasdores dispostos a vender uma vulnerabilidade de *zero-day* que descobriram. Empresas como o Google lançaram um programa para compra de vulnerabilidades de seus produtos [1].

O mercado negro, é um mercado de bens e serviços ilegais, onde as operações ocorrem através de contatos e vendas on-line, e fisicamente através de reuniões entre criminosos que compram. As vulnerabilidades *zero-day* são vendidas no mercado negro em uam parte mais oculta. Um exemplo de um mercado negro é o *Russian Business Network* sediada em São Petersburgo, na Rússia.

O último mercado é o mercado cinza ou mercado governamental. O governo americano compra vulnerabilidades de *zero-day* não para se proteger, mas sim para atacar. Na China, os alunos talentosos em ciência da computação e matemática são ensinados a espionagem industrial contra governos estrangeiros. Já na Índia, existe uma organização chamada *National Technical Research Organization*, que uma lei autoriza, em caso de ataque, permite retaliar usando técnicas de *hacking*. Além do que, o governo incentiva os jovens talentosos a entrar em um programa para proteger o país [1].

# Referências


[1] Marco Cremonini Paolo Foti, Jart Armin, editor. *0-Day Vulnerabilities and Cybercrime*. IEEE, 2015.

[2] Tudor Dumitras Leyla Bilge, editor. *Before we knew it: an empirical study of zero-day attacks in the real world*. ACM, 2012.

[3] Ravi K. Sheth Pratap Kumar. A review on 0-day vulnerability testing in web application. *2nd International Conference on Information and Communication Technology for Competitive Strategies*, 141, 2016.

[4] David Last. Forecasting zero-day vulnerabilities. *11th Annual Cyber and Information Security Research Conference*, 13, 2016.