Não sei

Alexandre Yuji Kajihara

2017

1 Introdução

O ataque de *zero-day* é um ataque cibernético que explora uma vulnerabilidade que não foi divulgada publicamente, e com isso não há defesa contra esse ataque, consequentemente não o *software* não pode ser corrigido e os antivírus não detectam devido a não ter assinatura [**?**]. Alguns tipos de ataques zero-day, permanecem desconhecidos até por 2,5 anos [**?**]. Quando as vulnerabilidades são descobertas ou são descritas em aviso público, os fornecedores de *software* lançam atualizações [**?**]. Além do que, um dos problemas é que depois de se lançados as atualizações, os usuários atrasam suas atualizações [**?**]. O preço das bulnerabilidades como a de plataformas, (Windows, iOS, principais navegadores) pode execeder mais de 100.000 dólares, dependendo da complexidade [**?**]. Atualmente, as explorações são incorporadas em arquivos não executáveis, como *.pdf, *.doc, *.xlsx [**?**]. Usuários que utilizam o antivírus podem ter mais cuidados com a segurança de seus computadores, e podem ser menos expostos aos ataques [**?**]. Ataques *zero-day* são ataques chamados de ataques específicos já que que visam um número limitado de organizções que possuem informações confidenciais que podem ser roubadas [**?**]. Além disso, os fornecedores de software dão preferência de corrigir vulnerabilidades que foram divulgadas ou estão prestes a declarar [**?**].

Os defensores da redes estão sempre a dois passos de trás dos invasores, já que devem se defender de falhas que não foram descobertas ou foram descobertas por atacantes [**?**]. A única vantagem é que os defensores sabem a localização provável e gravidade dessse ataque [**?**]. Uma maneira de se prevenir seria implementar sensores ou defesas cibernéticas, como *firewall* [**?**].

Os ataques de zero-day contra aplicações Web aumentaram [**?**]. Além disso, existem testes como o de *Web Application Penetration Testing* (WAPT), em que se as suas organizações não testam e não protegem de maneira adequadamente, terá seu aplicativo comprometido, ter dados roubados e danificar o desempenho da sua aplicação [**?**]. È díficil de prevenir, porque a informação só estará disponível quando o ataque tiver sido concluído [**?**]. Essas vulnerabilidades são muito desejadas por agências convernamentais, cibercriminosos e empresas de software [**?**]. Essas falhas podem ser em software ou sites [**?**]. As maneira para evitar os ataques *zero-day* seria utilizando 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. Atualizar suas aplicações, em que se houver notificação de atualização de *software* atualize. Usar navegadores somente atualizados já que todos os navegadores empurram atualizações periódicas [**?**].

O crime cibernético é uma forma de crime que inclui crimes que são cometidos através do uso da Internet ou de outras redes informáticas [**?**]. O aumento da dissemniação de crimes por computador deve se a um *Return On Investement* (ROI) derivado desse tipo de atividade criminosa [**?**]. As pessoas envolvidas em cibercrimes não entendem as ações ilegais realizadas com o auxílio de equipamentos de TI, e os mesmos se sentem que estão em um ambiente seguro com regras soltas [**?**]. As informaços pessoais e corporativas representam um grande valor para os criminosos [**?**]. Acredita-se que o período em que provavelmente ocorreram as primeiras vulnerabilidades de *zero-day*aconteceram nos anos 80 [**?**]. Para atacar um sistema, é essencial estudar, compreender sua estrutura, identificar o tipo de proteção instalada e o sistema operacional, par aassim identifcar as vulnerabilidades [**?**]. Além disso, os valores dessas vulnerabilidades elas mudam no qual o no segundo ela vale um quarto do que do que *zero-day*, e dez dias depois o valor dessa vulnerabilidade 1/1000 [**?**]. Existem fábricas de malware, na qual empresas criam malwares sob demanda em troca de uma taxa [**?**]. Existem três tipos de mercados. 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. Já 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. Por fim, o último mercado é o mercado cinza ou mercado governamental. O governo americano comprar 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, retaliar usando técnicas de hacking. Além do que, o governo incentiva os jovens talentosos a entrar em um programa para proteger o país [**?**].

A atividade de negociar explorações possui uma longa história, em que os criminosos utilizam cada vez mais disso para próprio benefício econômico [**?**]. Há prejuízos para a sociedade nos mercados de *zero-day*, pois motivam os criminosos venda privada dessas falhas [**?**]. Além disso, existem os *Zero-Day Market* em que é a venda de detalhes de exploração ou bug e o Vulnerability Rewards Program esao ganhando muita popularidade, em que é um programa pelo qual um fornecedor de software paga um pesquisador divulgar detalhes de um software relacionado à segurança, em que existem casos em que esses pesquisadores são contratados pelos fornecedores [**?**].Além disso, existem mercado de vulnera-

bilidades, em que os *Hackers* são pagos pela sua fama e notoriedade [**?**]. Esses mercados criam, incentivos atrativos para que pessoas mais inteligentes passem tempo procurando vulnerabilidades, já que quanto mais você olha, mais *bugs* você encontrará [**?**]. Além do que, *software* que são código aberto, ou de manutenção comunitária não existem fornecedores que estão dispostos a pagar pelas vulnerabilidades [**?**]. Existem vendedores de vulnerabilidades que vendem para prejudicar um fabricante do software [**?**].

Ataques do tipo *zero-day* são díficieis de analisar, porque em geral os dados não estão disponíveis de um ataque ser descoberto [**?**]. O mercado de nova vulnerabilidade varia entre 5.000 e 250.000 dólares. Ataques de *zero-day* foram o *trojan* Hydraq e Aurora [**?**]. Um ataque do tipo *zero-day* duram em média 312 dias e podem permanecer desconhecidos por até 2.5 anos [**?**]. Esse tipo de ataque começa com erros de programação [**?**]. Além do que, existem fornecedores que aprendem uma vulnerabilidades antes dela serem exploradas e consideram baixa prioridade [**?**]. Um problema que acontece é quando os fornecedores disponibilizam as atualizações, mas os usuário atrasam ela [**?**]. Nos últimos anos, a maiorida das explorações são incorporadas em arquivos não executáveis como .pdf .doc. .xlsx [**?**]. Usuários que instalam o antivírus podem ter mais cuidados com a segurança de seus computadores, sendo menos expostos aos ataques [**?**]. São ataques específicos, em que visam um número limitado de organizações que possuem informações confidenciais que podem ser roubadas [**?**]. Enquanto o software tenha erros para novas vulnerabilidaes será um atividade lucrativa, e estaremos expostos a ataques de *zero-day* [**?**].

Referências

[1] Angelo Ciampa, Corrado Aaron Visaggio, and Massimiliano Di Penta. A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications. In *2010 ICSE Workshop on Software Engineering for Secure Systems - SESS*. ACM, 2010.

[2] Marco Vieira, Nuno Antunes, and Henrique Madeira. Using web security scanners to detect vulnerabilities in web services. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, jun 2009.