Uma Avaliação das plataformas de denúncia de Phishing: uma análise da plataforma PhishTank

Lucas C. Teixeira[1], **Carlo M. R. da Silva**[1,2]

[1]Licenciatura em Computação – Universidade de Pernambuco (UPE)

[2]CIn – Universidade Federal de Pernambuco (UFPE)

marcelo.revoredo@upe.br, lucas.candeia.1@gmail.com

Abstract. *This article addresses some of the bottlenecks in major phishing reporting platforms. The purpose of the proposal is to evaluate behaviors present in the repositories of these platforms that may justify obstacles such as the plataform incident response and blacklist maintenance. As a result, in addition to the quantitative data, the study also performed a qualitative analysis of the behaviors. Given this, it is expected that the results obtained will reflect on this anti-phishing approach.*

1. Introdução

Apesar de inúmeras propostas na literatura que visam descartar o uso de listas negras (*black lists*), ainda sim, esse recurso é bastante presente em soluções *anti-phishing* [AlEroud and Zhou 2017]. Em termos de aplicabilidade, a lista negra é de baixa complexidade, além disso, a mesma pode ser alimentada por plataformas de denúncias. Comumente, os navegadores Web utilizam essas plataformas como um serviço externo que sincroniza periodicamente suas listas negras. A alimentação dessas listas pode ser realizada por diversas maneiras, mas, em sua maioria, é baseada em denúncias voluntárias da comunidade [Almomani 2018].

Contudo, soluções baseadas em lista negra tem entraves no combate de *phishing* recém-criados, denominados como *phishing zero-day*, já que propiciam a ocorrência de falsos negativos [AlEroud and Zhou 2017]. No contexto, a problemática se enviesa no momento em que o *phishing* é disponibilizado na Web até o instante em que o mesmo é registrado na lista negra. Tal intervalo representa uma janela de vulnerabilidade. Além disso, existe um considerável esforço na manutenabilidade das listas negras. Primeiramente, é preciso considerar o tempo de vida curto do *phishing*, a exemplo dos que atuam sobre redes *fast-flux* [Almomani 2018].

Em decorrência, os mantenedores de lista negra acabam por armazenar um amontoado de *phishing offline* em suas listas. Outro fator é que simples modificações na URL maliciosa fará da mesma desconhecida, representando assim um *bypass* e, consequentemente, a lista negra armazenará URL redundantes. Por fim, não é incomum a ocorrência indevida de sites genuínos em listas negras, resultando em um falso positivo pela denúncia equivocada, proposital ou não. O estudo tem como objetivo investigar lacunas existentes em plataformas de denúncia, analisando comportamentos que evidenciem os entraves quanto a resposta ao incidente e manutenabilidade desses mecanismos.

2. Plataformas de Denúncia

Atualmente, *PhishTank* [OpenDNS 2019][1], *SafeBrowsing*[2] e *SmartScreen*[3] são as principais plataformas de denúncias. A *PhishTank* é mantida pela *OpenDNS* e atuante no navegador *Opera*. Já a *SafeBrowsing* é mantido pela *Google* e atua nos navegadores *Chrome*, *Firefox* e *Safari*. Por fim, a *SmartScreen* é a solução da *Microsoft* para o *Internet Explorer* e *Edge*.

Além dessas, também foram observadas mais três plataformas, a saber: *OpenPhish*[4], *VirusTotal*[5] e *CaUMa*[6]. Contudo, inicialmente foi preciso checar a disponibilidade dos dados para extração de cada uma das plataformas, conforme descrito na Tabela 1. Foi possível observar que cada plataforma tem sua particularidade em relação a disponibilidade dos dados. Diante disso, algumas não disponibilizam seus dados e nem informações adicionais além da URL, o que inviabiliza o processo de investigação. Portanto, o estudo proposto tem como critério de inclusão os aspectos destacados em negrito na tabela, o que resultou no descarte de três plataformas, restando para análise a *PhishTank*, *OpenPhish* e *CaUMa*. A metodologia adotada para extração e análise dos registros foi uma avaliação do tipo *survey*. Como primeira análise, o estudo escolheu a plataforma *PhishTank* devido sua base ter maior disponibilidade e volume.

Tabela 1. As plataformas e seus respectivos recursos

	PhishTank	SafeBrowsing	SmartScreen	**OpenPhish**	VirusTotal	**CaUMa**
Disponibiliza acesso aos registros?	**Total**	**Nenhum**	**Nenhum**	**Parcial**	**Nenhum**	**Total**
Possui informações além da URL?	**Parcial**	**Nenhum**	**Nenhum**	**Parcial**	**Parcial**	**Parcial**
Possui API para checar URL?	Total	Total	Nenhum	Parcial	Total	Total
Disponibiliza download dos dados	Parcial	Nenhum	Nenhum	Parcial	Nenhum	Nenhum

A proposta do PhishTank é ser comunitária e gratuita onde qualquer pessoa pode enviar, verificar, rastrear e compartilhar dados de *phishing*. É importante salientar que a equipe da *PhishTank* não considera sua plataforma como uma medida de proteção, contudo, as informações fornecidas pela mesma servem de subsídio para mecanismos de resposta a incidente em diversas organizações. É tida como uma comunidade porque comporta usuários que colaboram entre si dados de *phishing*. Seu caráter colaborativo remete ao fato dos usuários popularem a base de dados de *phishing*. Cada registro de *phishing* é feito através de denúncias que analisam a **confirmação** e **disponibilidade**.

Em relação a confirmação, a *PhishTank* possibilita que um usuário submeta uma URL suspeita e os demais usuários realizem um sistema de votação para determinar o veredito sobre a denúncia, ou seja, considerar o *phishing* como **válido** ou **inválido**. Quanto a disponibilidade, a plataforma observa se o *phishing* está **online** ou **offline**. Importante frisar que um *phishing* indisponível significa que a requisição o retornou código HTTP 400 ou 500, ou seja, inacessível, assumindo o status "offline". O ciclo de vida entre o *phishing*, a plataforma e seus usuários está dividido em 5 etapas, conforme a Figura 1.

[1]https://www.phishtank.com/
[2]https://safebrowsing.google.com/
[3]https://support.microsoft.com/pt-br/help/17443/windows-internet-explorer-smartscreen-faq
[4]https://openphish.com/
[5]https://www.virustotal.com
[6]https://cauma.pop-ba.rnp.br/

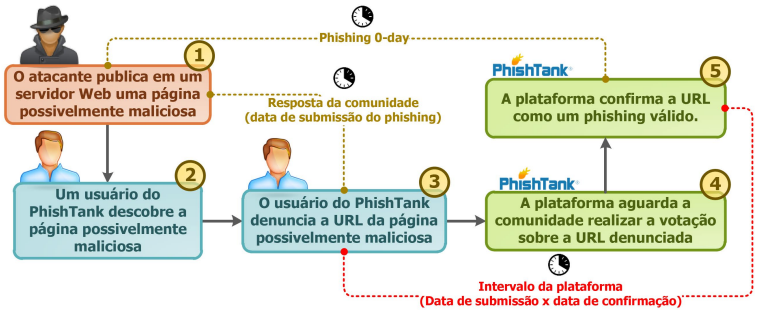

Figura 1. Ciclo de vida das denúncias de *phishing*

Na etapa 1 o atacante publica sua página maliciosa em um servidor web, disponibilizada para ser propagada pela Web. A etapa 2 remete ao descobrimento da URL maliciosa por um usuário. Posteriormente, o usuário acessa a *PhishTank* e denuncia a URL, realizando assim a etapa 3. Já a etapa 4 descreve o momento em que a plataforma aguarda as votações da comunidade sobre a URL recém denunciada. Por fim, a etapa 5 ocorre quando o sistema de votos recebe uma quantidade satisfatória para considerar a URL maliciosa ou não. Vale salientar que a quantidade "suficiente" de votos não é explicitada, a plataforma declara que pode variar de acordo com o histórico das denúncias.

3. Resultados parciais

Cada aspecto analisado é tido como uma característica que descreve um determinado comportamento que tem como causa ou consequência algum entrave sobre a resposta ao incidente da plataforma ou manutenabilidade da lista negra. No estado atual do estudo, foram detectadas 6 características, que serão descritas adiante.

C01. Atraso na Sincronização: Essa característica descreve falhas na sincronização entre a base de dados da plataforma e o respectivo navegador que utiliza a plataforma como apoio ao mecanismo de proteção. O motivo seria o atraso na sincronização da lista negra do navegador com os registros do respectivo repositório, evidenciando assim um problema crônico que merece ser investigado. Essa característica evidencia um entrave sobre a resposta ao incidente.

C02. Caminho duplicado na URL: Essa característica avalia casos em que a URL denunciada vem com um *path* vazio, ou seja, os caracteres "//" na URL. Diante disso, em alguns casos, a exemplo de aplicações que não são *RESTful*, o navegador redireciona o usuário desprezando o path "vazio", burlando assim a lista negra, já que a URL sem o *double slash* teria um *hash* diferente, resultando em um *bypass*. Essa característica evidencia um entrave de manutenibilidade.

C03. Denúncia duplicada: Essa característica remete a duplicidade de uma mesma URL durante uma denúncia. O intuito é evidenciar as ocorrências de votações desnecessárias para uma determinada URL, uma vez que a mesma já tenha sido submetida a uma votação. Além disso, também pode representar que uma determinada URL que anteriormente recebeu um veredito indevido, está novamente sendo submetida para uma possível retificação. Essa característica evidencia um entrave sobre a manutenibilidade.

C04. Exposição da porta padrão na URL: Alguns mecanismos realizam a filtragem com base no *hash* dos caracteres da URL. Ou seja, se o usuário realiza a denúncia da

URL com a porta padrão em seus caracteres, a exemplo de ":80" ou ":443", fará com que o *hash* resultante seja diferente de um *hash* calculado sobre uma URL que não possui as portas. Portanto, ao acessar uma URL com portas padrões especificadas, o navegador irá remover as portas e informar ao mecanismo de filtragem a URL sem as portas, resultando em *bypass*. Essa característica evidencia um entrave sobre a manutenibilidade.

C05. Precisão da comunidade: O intuito é avaliar a comunidade em relação a falsos positivos das URL que são denunciadas. Esse aspecto é importante para a plataforma, uma vez que representa a precisão com relação aos *phishing* válidos e inválidos. Essa característica evidencia um entrave sobre a resposta ao incidente.

C06. Resposta da plataforma: Conforme as denúncias e votações, a diferença entre a data de submissão e de confirmação possibilita analisar o tempo de resposta da plataforma. Essa característica evidencia um entrave sobre a resposta ao incidente. O fluxo do tempo de resposta está ilustrado na Figura 1, nas etapas 3, 4 e 5. Através do domínio, existem marcos importantes a serem analisados, como o intervalo entre as etapas 1 e 3, que seriam a janela da publicação do *phishing* na Web até o momento em que o mesmo foi denunciado na plataforma, estimando assim o tempo médio de denúncia. Na mesma linha, o intervalo entre as etapas 1 e 5 que seriam o período do *phishing* 0-day, ou seja, o tempo médio que um *phishing* fica imune da lista negra.

4. Conclusão

Foi evidenciado que 38.05% de *phishing* confirmados não foram reconhecidos como uma ameaça quando acessados através do navegador Opera, ou seja, um problema de sincronização foi detectado (C01). Além disso, o sistema de votação, por não possuir um prazo estimado e nem informar a quantidade de votos para conclusão, apresenta um atraso quanto a conclusão do veredito, em que 49.80% dos registros levaram entre 1 a 7 dias, evidenciando uma janela de vulnerabilidade (C06). Não obstante, grande parte dos *phishing* confirmados não duram o tempo de vida suficiente para receberem o veredito final sobre a confirmação de sua denúncia na plataforma. Ou seja, em muitos casos, a denúncia acaba por receber um veredito quando a URL da mesma já encontra-se *offline*.

Também foi possível observar que 12.15% dos *phishing* válidos levam entre 7 e 15 dias para serem confirmados. Todavia, o estudo evidenciou que 24.87% dos *phishing* válidos possuem um tempo de atividade entre 15 dias a 1 mês (C05). Diante disso, seria interessante a adoção de melhores estratégias na plataforma de denúncias no intuito de evitar votações desnecessárias, como os casos de duplicidade (C03) que foram observados e outras características que acarretam em duplicidades (C02 e C04). O próximo passo da pesquisa será investigar as características identificadas na *PhishTank* nas demais plataformas e observar a existência de outras. De posse desses dados, será realizada uma análise de agrupamento no intuito de observar similaridades e dissimilaridades.

Referências

[AlEroud and Zhou 2017] AlEroud, A. and Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*.

[Almomani 2018] Almomani, A. (2018). Fast-flux hunter: A system for filtering online fast-flux botnet. *Neural Comput. Appl.*, 29(7):483–493.

[OpenDNS 2019] OpenDNS (2019). Phishtank. *Available at: https://www.phishtank.com/*.