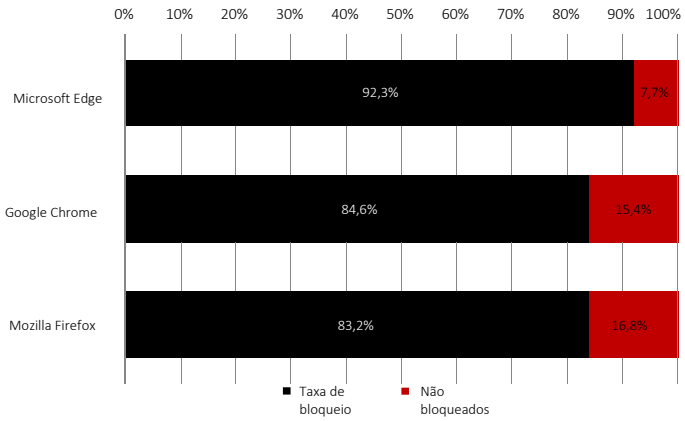
T2 2021 Navegadores da Web versus Phishing

Visão

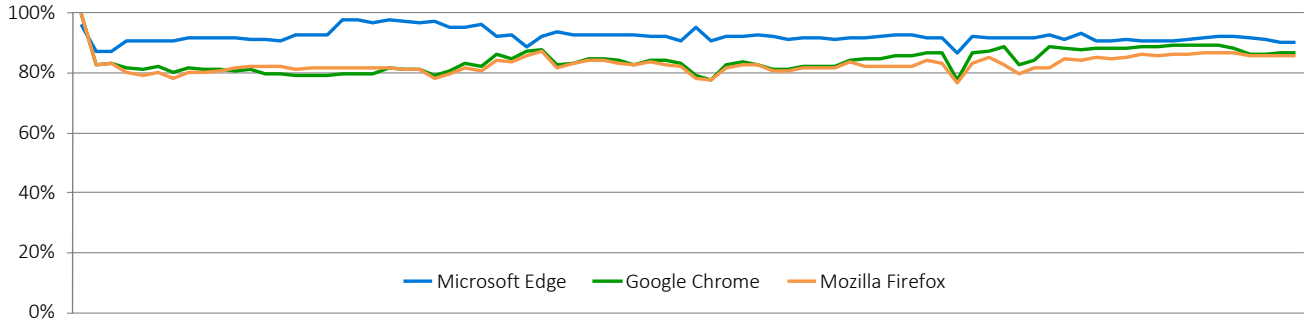
Durante o segundo trimestre de 2021, CyberRatings.org realizou um teste independente de proteção contra phishing oferecida por navegadores da Web. Os testes foram executados por 20 dias, com 80 execuções de teste discretas. Para se proteger contra phishing, o Microsoft Edge usa o Microsoft Defender SmartScreen; o Google Chrome e o Mozilla Firefox usam a API de navegação segura do Google. O Microsoft Edge ofereceu a maior proteção, bloqueando 92,3% das URLs de phishing e, ao mesmo tempo, proporcionando a maior taxa de proteção zero hora (93,5%). O Google Chrome forneceu a segunda maior proteção, bloqueando uma média de 84,6%, seguido pelo Mozilla Firefox com 83,2%.



Resumo de

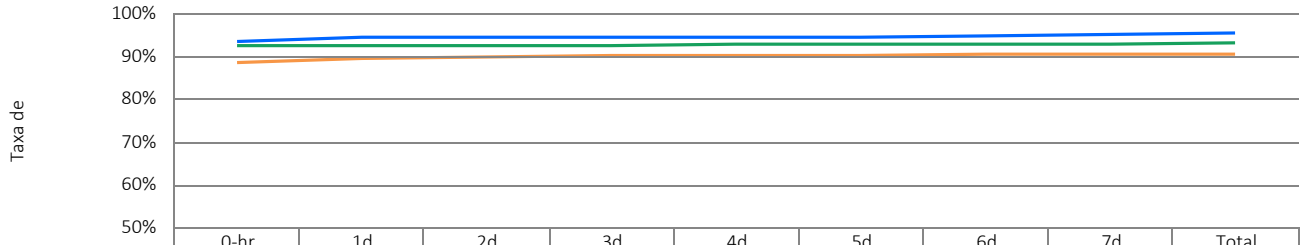
Os sistemas de reputação de URL reduzem o tempo que os invasores têm para atingir seus objetivos, evitando/avisando os usuários de que uma URL é um conhecido site de phishing. No entanto, como os usuários visitam uma ampla variedade de sites, muitos dos quais novos, os sistemas de reputação de URLs não podem simplesmente bloquear todas as novas URLs. Com isso em mente, as campanhas de phishing dos invasores estão em constante mudança, com a maior parte dos novos ataques ocorrendo nas primeiras horas após o lançamento de um ataque.

Proteção contra phishing ao longo do tempo



Durante o teste, novas URLs de phishing foram adicionados diariamente e as URLs que não estavam mais acessíveis ou que não entregavam mais ataques de phishing foram removidos. Cada ponto de dados representa proteção em um momento específico. Se uma URL foi bloqueada no início, melhorou a pontuação do navegador para a consistência da proteção ao longo do tempo. Como alternativa, se o navegador não bloqueou a URL, a pontuação diminuiu.

Taxa de bloqueio de phishing ao longo do tempo



	0-hr	1d	2d	3d	4d	5d	6d	7d	Total
Microsoft Edge	93,5%	94,4%	94,5%	94,5%	94,5%	94,7%	94,9%	95,1%	95,4%
Google Chrome	92,4%	92,6%	92,7%	92,7%	92,8%	92,8%	92,8%	92,9%	93,2%
Mozilla Firefox	88,7%	89,7%	90,0%	90,4%	90,4%	90,4%	90,5%	90,6%	90,6%

Medimos a capacidade dos navegadores de bloquear URLs mal-intencionadas tão rapidamente quanto as encontramos na Internet. Isso continuou a cada seis horas para determinar quanto tempo levaria para um fornecedor adicionar proteção. A figura acima mostra o tempo de resposta de cada navegador para bloquear um site de phishing, depois que a ameaça foi introduzida no ciclo de teste.

Ataques de phishing

Phishing é um tipo de ataque de engenharia social que tenta persuadir a vítima a fornecer informações pessoais confidenciais ao invasor. Alguns exemplos de informações confidenciais são números de cartão de crédito, CPFs e login e senhas de contas bancárias. E-mail, mensagens instantâneas, mensagens SMS e links em sites de redes sociais são vetores de ataques de phishing. A página de destino de um site de phishing muitas vezes tenta explorar silenciosamente o computador de um visitante e instalar software mal-intencionado (também conhecido como exploit com ataque tipo drive-by).

Os ataques de phishing representam um risco significativo para indivíduos e organizações, pois ameaçam comprometer ou adquirir informações pessoais e corporativas confidenciais. O Anti-Phishing Working Group (APWG) relatou um total de 396.688 campanhas exclusivas de phishing por e-mail no quarto trimestre de 2020.[1]

Proteção de navegadores da Web contra phishing

A proteção contra phishing é fornecida por um aplicativo em um navegador da Web que solicita a reputação de uma URL de um serviço em nuvem que tem vasculhado a Internet para encontrar sites de phishing e adicioná-los a uma lista de bloqueio. Dessa forma, quando um navegador da Web tenta visitar uma URL, a proteção contra phishing do navegador (ou seja, Navegação segura, SmartScreen, etc.) redireciona o usuário para uma mensagem de aviso que explica que a URL é mal-intencionada. Alguns sistemas de reputação também incluem conteúdo educacional adicional. Por outro lado, se um site for considerado "bom", o navegador da Web não executará qualquer ação.

O Google e o Firefox usam a API de navegação segura do Google para reputação de URL e para avisar os usuários sobre o download de certos tipos de arquivos. O Microsoft Edge usa o Microsoft Defender SmartScreen, que fornece proteção contra ataques baseada em URL, por meio de um serviço integrado de reputação de URL baseada em nuvem, bem como reputação de aplicativo para bloqueio de arquivos mal-intencionados.

Número médio de amostras de URLs mal-intencionadas adicionadas por dia

Em média, 50 novas URLs validadas foram adicionadas ao conjunto de teste por dia; os números variaram em alguns dias, conforme a oscilação dos níveis de atividade criminosa.

Ambiente de teste

- Microsoft Windows 10 Pro, 21H1

Número total de URLs mal-intencionadas no teste

Foram testadas 26.976 URLs brutas não validadas várias vezes com cada navegador da Web, em um total de 80 ciclos de teste cada, sem interrupção por 480 horas (a cada 6 horas por 20 dias). Nossos engenheiros removeram amostras que não passaram nos critérios de validação, incluindo aquelas contaminadas por exploits (não fazem parte deste teste). No final das contas, 996 URLs de phishing válidas e exclusivas foram incluídas no conjunto final de 61.605 testes de phishing válidos e discretos (20.535 testes por navegador da Web), fornecendo uma margem de erro de 3,1 por cento (<3,1%) em um nível de confiança de 95%

Como testar a composição - URLs de phishing

Os dados neste relatório abrangem um período de teste de vinte (20) dias entre 11 de maio e 31 de maio de 2021. Durante o teste, nossos engenheiros monitoraram rotineiramente a conectividade para garantir que os navegadores em teste pudessem acessar as URLs de phishing, bem como os serviços de reputação de navegador na nuvem.

A ênfase estava na renovação, com novas URLs sendo constantemente adicionadas ao teste, e os sites inativos removidos.

Como avaliamos os resultados

Medimos a capacidade de cada navegador de bloquear as URLs mal-intencionadas com a mesma rapidez com que foram descobertas na Internet. Os engenheiros repetiam esses testes a cada seis horas, para determinar quanto tempo um fornecedor levaria para adicionar proteção, se o fizesse.

O desempenho de cada navegador foi medido continuamente, e a taxa geral de bloqueio de todas as URLs testadas com o navegador foi registrada. A taxa de bloqueio geral de cada navegador foi calculada como o número de bloqueios bem-sucedidos dividido pelo número total de casos de teste. Por exemplo, com testes realizados a cada 6 horas, uma URL que ficou online por 48 horas foi testada oito (8) vezes. Um navegador que a bloqueou em 6 (de um máximo de 8) execuções de teste atingiu uma taxa de bloqueio de 75%.

Produtos testados

- Google Chrome: Versão 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: Versão: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: Versão 88.0.1 - 88.0.1

[1] APWG Phishing Activity Trends Report

Autores

Thomas Skybakmoen, Vikram Phatak

Metodologia do teste

A Metodologia de teste de segurança do navegador da Web CyberRatings v1.0 está disponível em www.cyberratings.org

Informações de contato

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org