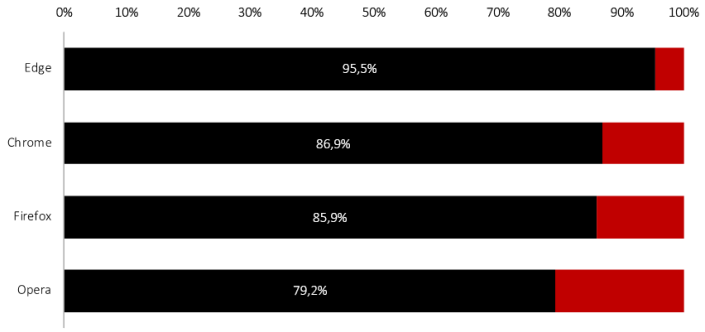
T2 2020 RELATÓRIO DE TESTE COMPARATIVO

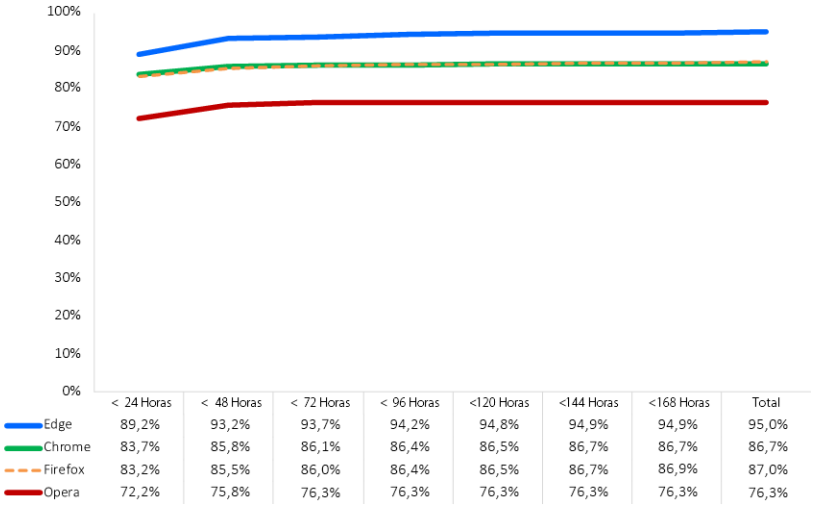
Descrição geral

Durante o 2.º trimestre de 2020, a NSS Labs efetuou um teste independente à proteção contra phishing disponibilizada pelos browsers: 47.274 testes discretos (por browser) utilizando 2.443 URLs de phishing exclusivos ao longo de 18 dias. Para proteção contra phishing, o Microsoft Edge utiliza o Microsoft Defender SmartScreen, o Google Chrome e o Mozilla Firefox utilizam a API Safe Browsing da Google e o Opera utiliza uma combinação de listas de bloqueios de terceiros.

O Microsoft Edge ofereceu a maior proteção, bloqueando 95,5% dos URLs de phishing, proporcionando simultaneamente a taxa mais elevada de proteção automática (89,2%). O Google Chrome proporcionou a segunda proteção mais elevada, bloqueando uma média de 86,9%, seguido pelo Mozilla Firefox com 85,9%. O Opera bloqueou 79,2%.



Resumo dos Resultados

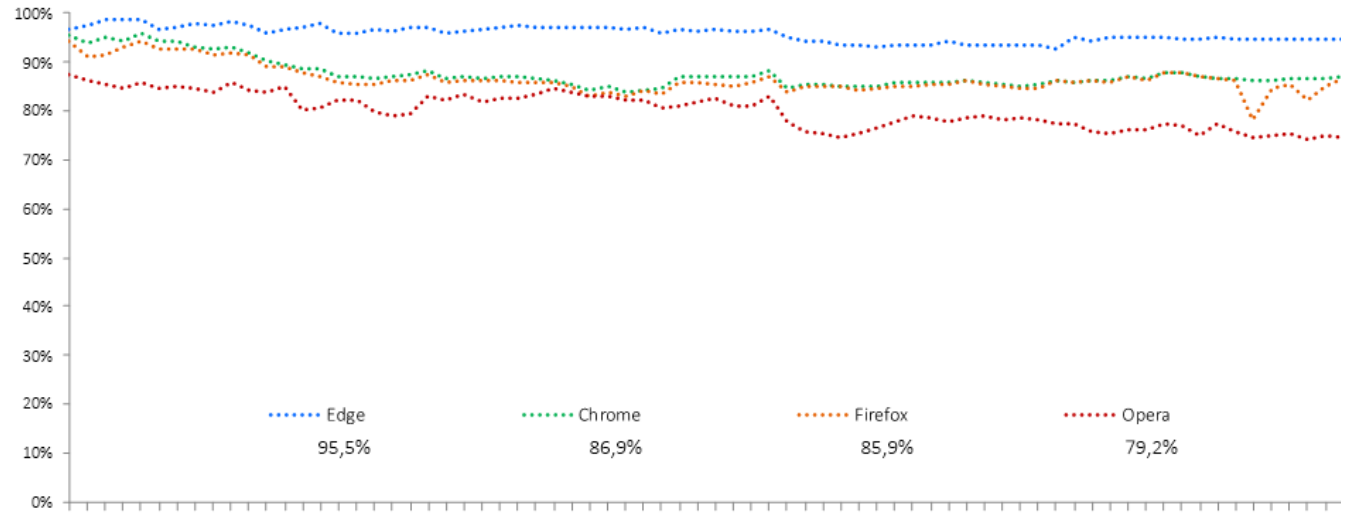


	< 24 Horas	< 48 Horas	< 72 Horas	< 96 Horas	<120 Horas	<144 Horas	<168 Horas	Total
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

Os sistemas de reputação de URLs reduzem o tempo que os atacantes têm para atingir os seus objetivos, evitando/avisando os utilizadores que um URL é um site de phishing conhecido. No entanto, visto que os utilizadores visitam uma vasta gama de sites, muitos dos quais são novos, os sistemas de reputação não conseguem bloquear todos os URLs novos. Sabendo disto, as campanhas de phishing dos atacantes estão em constante mudança e a maior parte dos novos ataques ocorrem nas primeiras horas após o lançamento de um ataque.

A NSS Labs avaliou a capacidade dos browsers bloquearem URLs maliciosos à mesma velocidade a que estes são detetados na Internet. Continuámos a testá-los a intervalos de seis horas, para determinarmos quanto tempo é que cada fornecedor demorou a adicionar a proteção, se é que chegou a fazê-lo.

Proteção Contra Phishing ao Longo do Tempo



Ao longo do teste foram adicionados diariamente novos URLs de phishing; simultaneamente, os URLs que já não estavam contactáveis ou que já não estavam a gerar ataques de phishing foram removidos. Cada ponto de dados representa a proteção num ponto específico no tempo. Se um URL era bloqueado logo no início, a pontuação do browser relativa à consistência da proteção ao longo do tempo melhorava. Alternativamente, se o browser não bloqueava o URL, a pontuação diminuía.

Os testes foram baseados na Metodologia de Teste de Browsers v4.0 (disponível em www.nsslabs.com).

Antecedentes

O phishing é um tipo de ataque de engenharia social que tenta convencer a vítima a fornecer informações pessoais confidenciais ao atacante. Alguns exemplos de informações confidenciais são números de cartões de crédito, números de identificação fiscal e as informações de início de sessão e palavras-passe de contas bancárias. E-mail, mensagens instantâneas, mensagens SMS e ligações em sites de redes sociais são vetores para ataques de phishing. Frequentemente, a página de destino de um site de phishing também tenta explorar silenciosamente o computador do visitante e instalar um software malicioso (operação também conhecida pela expressão inglesa "drive-by exploit").

Os ataques de phishing constituem um risco significativo para pessoas individuais e empresas, ameaçando comprometer ou adquirir informações confidenciais pessoais e empresariais. O Anti-Phishing Working Group (APWG) comunicou um total de 165.772 campanhas de phishing por e-mail exclusivas no primeiro trimestre de 2020[1]. Os ataques de phishing têm vindo a tornar-se cada vez mais complexos e sofisticados, o que os torna mais difíceis de detetar e prevenir.

Proteção dos Browsers contra Phishing

A proteção contra phishing é fornecida por uma aplicação existente no browser, que solicita a reputação de um URL a um servidor de reputação localizado na cloud. O servidor de reputação percorre a Internet para localizar sites de phishing e, em seguida, atribui uma pontuação a cada URL e adiciona-o a uma lista de bloqueio. Desta forma, quando é pedido a um browser para visitar um URL, a proteção contra phishing do browser (ou seja, o Safe Browsing, o SmartScreen, etc.) solicita a reputação do URL ao servidor de reputação baseado na cloud. Se o resultado indica que um site é "mau", o browser redireciona o utilizador para uma mensagem de aviso que explica que o URL é malicioso. Alguns sistemas de reputação também incluem conteúdos educativos adicionais. Por outro lado, se um site é identificado como "bom", o browser não realiza qualquer ação e o utilizador não se apercebe de que este acabou de efetuar uma verificação de segurança.

Composição do Teste – URLs de Phishing

Os dados incluídos neste relatório dizem respeito a um período de teste de 18 dias, decorrido entre 21 de abril de 2020 e 8 de maio de 2020. Todos os testes foram realizados nas instalações de teste da NSS em Austin, no Texas (E.U.A.). Durante o teste, os engenheiros da NSS monitorizaram periodicamente a conectividade para garantir que os browsers testados conseguiam aceder aos URLs de phishing e aos serviços de reputação na cloud.

Concentrámos a nossa atenção na atualização. Consequentemente, avaliámos um número de sites maior do que aquele que acabou por ser incluído no conjunto de teste final: foram constantemente adicionados novos URLs ao teste, ao mesmo tempo que os sites inativos eram removidos.

Número Total de URLs Maliciosos Incluídos no Teste

Um total de 4.020 URLs não processados e não validados foi testado várias vezes em cada browser, perfazendo um total de 222.527 testes discretos realizados sem interrupção ao longo de 430 horas (a intervalos de 6 horas durante 18 dias). Os engenheiros da NSS removeram amostras que não passaram nos critérios de validação incluindo as que foram contaminadas por exploits (que não faziam parte deste teste). Finalmente, 2.443 URLs de phishing exclusivos e válidos foram incluídos em 189.096 testes discretos de phishing válidos (47.274 por browser), proporcionando uma margem de erro inferior a 2 por cento (<2%), com um intervalo de confiança de 95%.

Número Médio de URLs Maliciosos Adicionados por Dia

Em média, foram adicionados diariamente 136 novos URLs validados ao conjunto de teste; este número variou em alguns dias consoante a flutuação dos níveis de atividade criminosa.

Bloqueio de URLs de Phishing

A NSS avaliou a capacidade dos browsers bloquearem URLs maliciosos à mesma velocidade a que estes eram detetados na Internet. Os engenheiros repetiram estes testes a intervalos de seis horas, para determinarem quanto tempo é que cada fornecedor demorou a adicionar a proteção, se é que chegou a fazê-lo.

O novo Microsoft Edge é baseado no Chromium e foi lançado em 15 de janeiro de 2020. Este browser é compatível com todas as versões suportadas do Windows e macOS. A transferência do browser substitui a versão legada do Microsoft Edge em PCs Windows 10.

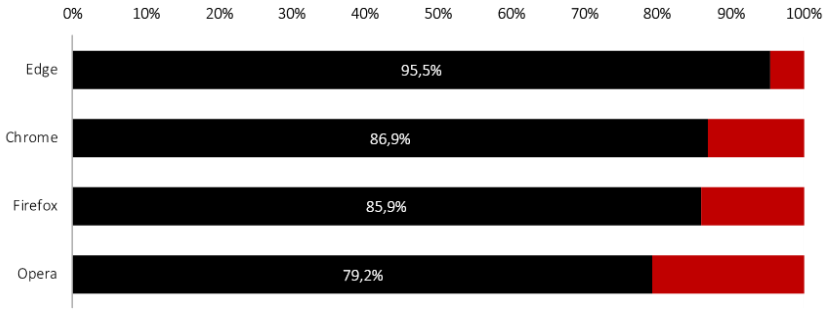
https://support.microsoft.com/pt-pt/help/4501095/download-the-new-microsoft-edge-based-on-chromium

[1] Relatório de Tendências da Atividade de Phishing do APWG

Taxa de Bloqueio de Phishing

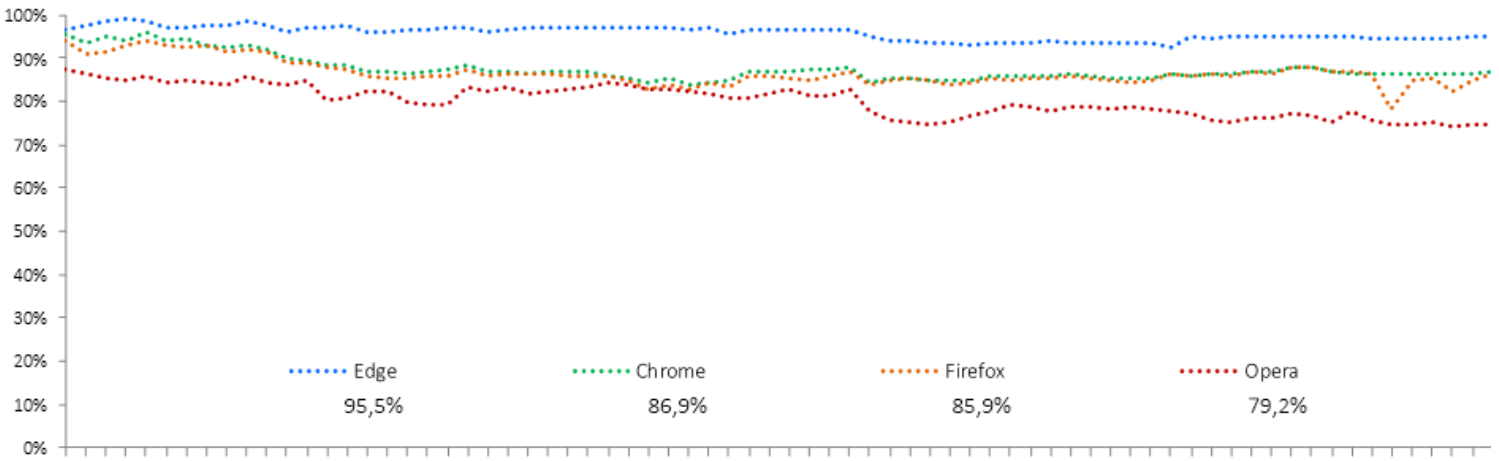
O Google Chrome e o Mozilla Firefox utilizam a API Safe Browsing da Google. O Microsoft Edge utiliza o Microsoft Defender SmartScreen (que inclui o serviço de reputação da aplicação) para proporcionar proteção contra ameaças de phishing e malware. O Opera utiliza uma combinação de listas de bloqueio da Netcraft,[2] PhishTank[3] e Metamask[4], juntamente com uma lista de bloqueio de malware da Yandex[5].

A capacidade de avisarem potenciais vítimas de que estão prestes a aceder a um site malicioso coloca os browsers numa posição privilegiada para o combate ao phishing e outras atividades criminosas. Visto que os sites de phishing têm um ciclo de vida reduzido, é essencial que cada site seja detetado, validado, classificado e adicionado ao sistema de reputação o mais rapidamente possível. Isto explica a correlação entre o tempo médio de bloqueio e a taxa de captura. Para atingir uma taxa de captura elevada, um bom sistema de reputação tem de ser simultaneamente exato e rápido. Os programadores dos browsers compreendem claramente esta relação: é bloqueado um número substancialmente superior de sites de phishing nas primeiras 24 horas após a deteção do que após este período de tempo.



O desempenho de bloqueio individual de cada browser foi medido continuamente, sendo registada a taxa de bloqueio geral de todos os URLs testados por browser. A taxa de bloqueio geral de um browser é obtida através da divisão do número de bloqueios com êxito pelo número de casos de teste. Por exemplo: visto que os testes eram realizados a intervalos de 6 horas, um URL que estivesse online durante 48 horas seria testado 8 vezes. Um browser que o bloqueasse em 6 execuções do teste (num máximo de 8) alcançaria uma taxa de bloqueio de 75%.

Consistência da Proteção ao Longo do Tempo



Ao longo do teste foram adicionados diariamente novos URLs de phishing; simultaneamente, os URLs que já não estavam contactáveis ou que já não estavam a gerar URLs de phishing foram removidos. Cada ponto de dados representa a proteção num ponto específico no tempo. Se um URL era bloqueado logo no início, a pontuação do browser relativa à consistência da proteção ao longo do tempo melhorava. Alternativamente, se o browser não bloqueava o URL, a pontuação diminuía.

[2] http://www.netcraft.com/

[3] http://www.phishtank.com/

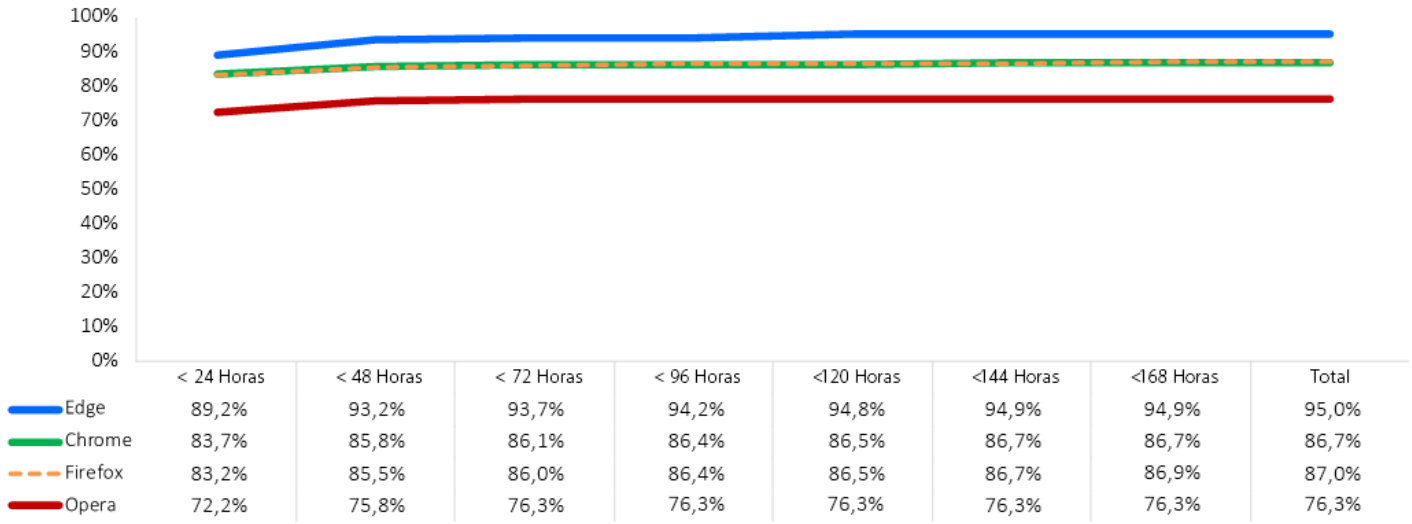
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Histograma da Proteção contra Phishing

A proteção imediata contra novos URLs de phishing é crucial. Os sites de phishing são frequentemente desativados num curto período de tempo após serem detetados. Os produtos que não adicionarem proteção atempadamente poderão ser ineficientes para deter uma ameaça. O histograma abaixo mostra o tempo que cada browser demorou a bloquear um site de phishing após a ameaça ser introduzida no ciclo de teste. Durante a janela de sete dias, as taxas de proteção cumulativa foram calculadas diariamente até que as ameaças fossem bloqueadas.

Ao longo do teste, o Microsoft Edge demonstrou uma taxa de proteção inicial de 89,2% contra ataques de phishing. O Google Chrome e o Mozilla Firefox alcançaram uma taxa de proteção inicial de 83,7% e 83,2%, respetivamente. A taxa de proteção inicial do Opera foi de 72,2%. No final do sétimo dia de testes, todos os browsers registaram um aumento na proteção.
O Microsoft Edge registou um aumento de 5,7%, para 94,9%.
O Mozilla Firefox registou um aumento de 3,7%, para 86,9%;
o Google Chrome registou um aumento de 3%, para 86,7%.
O Opera registou um aumento de 4,1%, para 76,3%



	< 24 Horas	< 48 Horas	< 72 Horas	< 96 Horas	<120 Horas	<144 Horas	<168 Horas	Total
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

Ambiente de Teste

- BaitNET™ (Ambiente Proprietário da NSS Labs)
- Microsoft Windows 10 Pro de 64 bits (versão 1909 Compilação: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel versão 4.19.0-kali5-amd64)
- VMware vCenter (Versão 6.7u2 Compilação 6.7.0.30000)
- VMware vSphere (Versão 6.7.0.20000)
- VMware ESXi (Versão 6.7u3 Compilação 14320388)
- VMware Tools 10.3.5
- Wireshark versão 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (Compilação 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Produtos Testados

- Google Chrome: Versão 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: Versão 83.0.478.10 – 84.0.502.0
- Mozilla Firefox: Versão 75.0 – 76.0.1
- Opera: Versão: 67.0.3575.137 – 68.0.3618.125

Autores

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Metodologia de Teste

A Metodologia de Teste v4.0 de Segurança de Browsers (WBS) da NSS Labs está disponível em www.nsslabs.com.

Informações de Contacto

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com