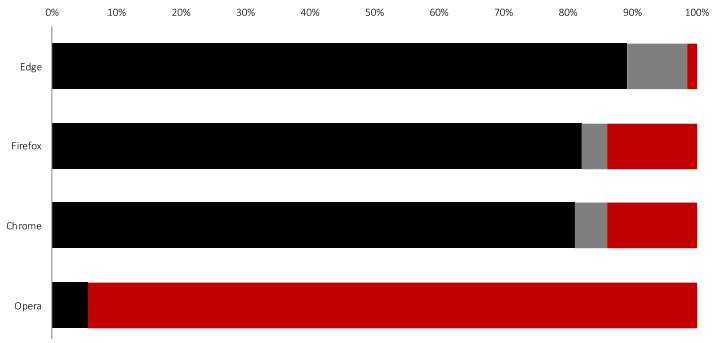
T2 2020 RELATÓRIO DE TESTE COMPARATIVO

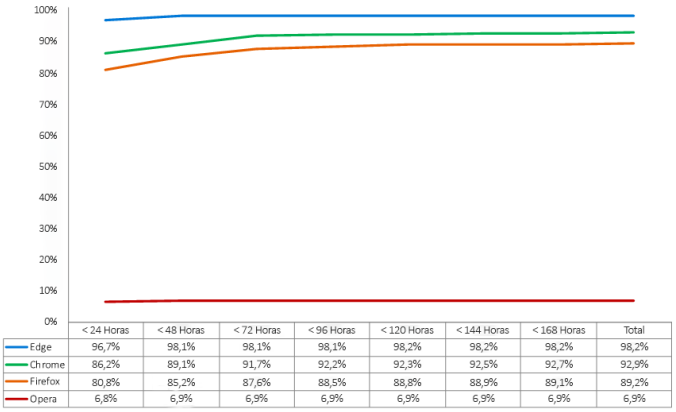
Descrição geral

Durante o 2.º trimestre de 2020, a NSS Labs efetuou um teste independente à proteção contra malware disponibilizada pelos browsers: 32.267 testes discretos (por browser) utilizando 1.065 amostras exclusivas ao longo de 34 dias. Para proteção contra malware, 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 a Yandex.

O Microsoft Edge ofereceu a maior proteção, bloqueando 98,5% do malware, proporcionando simultaneamente a taxa mais elevada de proteção automática (96,7%). O Firefox proporcionou a segunda proteção mais elevada, bloqueando uma média de 86,1%, seguido pelo Google Chrome com 86,0%. O Opera bloqueou 5,6%.



Resumo dos Resultados

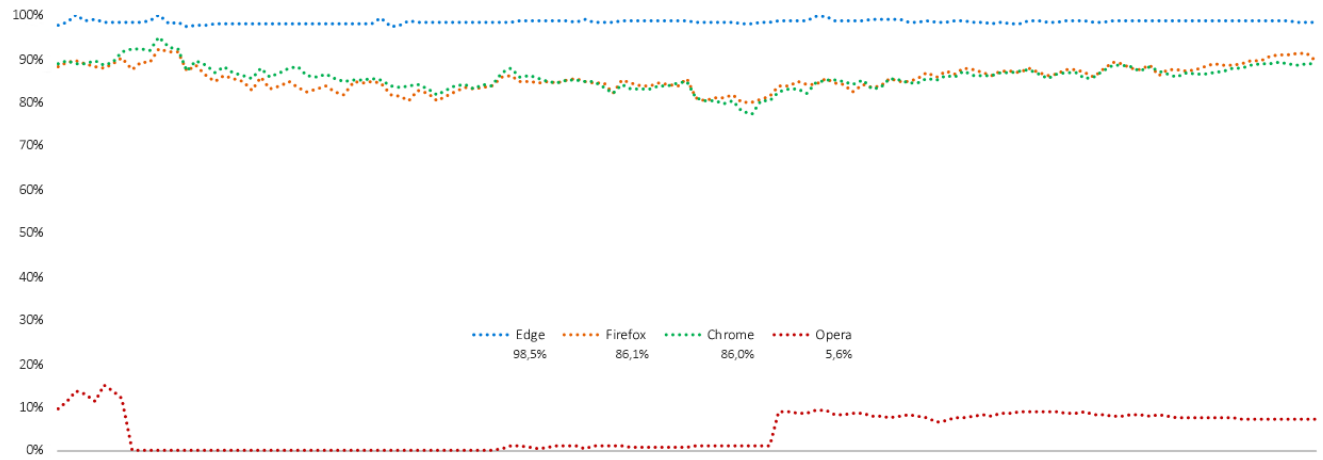


	< 24 Horas	< 48 Horas	< 72 Horas	< 96 Horas	< 120 Horas	< 144 Horas	< 168 Horas	Total
Edge	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Chrome	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Firefox	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Opera	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Os sistemas de reputação reduzem o tempo que os atacantes têm para atingir os seus objetivos, evitando ou avisando os utilizadores que um URL, uma aplicação ou um ficheiro é perigoso. No entanto, os utilizadores estão constantemente a visitar sites novos, a transferir ficheiros e a instalar aplicações. Os sistemas de reputação não podem pura e simplesmente bloquear tudo o que for novo. Sabendo disto, as campanhas de malware dos atacantes estão em constante mudança e a maior parte de todos os ataques ocorrem nas primeiras horas após o lançamento de uma campanha. Consequentemente, a classificação dos conteúdos de forma exata e rápida é crucial para o êxito da proteção.

A NSS Labs avaliou a capacidade dos browsers bloquearem malware à mesma velocidade a que este é detetado na Internet. Continuámos a testar os URLs, aplicações e ficheiros maliciosos 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 Malware ao Longo do Tempo



Foi constantemente adicionado malware novo ao longo do teste. Os URLs, ficheiros e aplicações que já não estavam contactáveis ou que já não estavam a alojar malware foram removidos. Cada ponto de dados é calculado através de medições registadas num ponto específico no tempo. Se o malware 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 malware, a pontuação diminuía.

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

Antecedentes

Os ataques de malware por engenharia social (SEM) utilizam uma combinação dinâmica de redes sociais, contas de e-mail acedidas ilicitamente, notificações falsas de problemas informáticos e outros logros para encorajar os utilizadores a transferirem malware. Os cibercriminosos utilizam contas de e-mail acedidas ilicitamente para tirarem partido da confiança implícita entre contactos, levando as vítimas a acreditar que as ligações para ficheiros maliciosos são fidedignas. Para a mesma finalidade são também utilizadas contas de redes sociais acedidas de forma ilícita. No entanto, o círculo é mais alargado no caso das redes sociais: amigos e até mesmo amigos de amigos correm o risco de serem lograd os.

As táticas de engenharia social podem utilizar mensagens de pop-up: por exemplo, para avisar os utilizadores de que é necessário instalar uma aplicação (como o Adobe Flash Player) ou que os respetivos computadores estão infetados ou necessitam de uma atualização. Após a instalação do malware, as vítimas ficam vulneráveis a roubo de identidade, compromisso de contas bancárias e outras consequências potencialmente devastadoras.

Proteção dos Browsers contra Malware

Para proteção contra malware, os browsers utilizam sistemas de reputação baseados na cloud que percorrem a Internet à procura de sites maliciosos e categorizam os conteúdos em conformidade, adicionando-os a listas de bloqueio ou permissão ou atribuindo-lhes uma pontuação (consoante a abordagem do fornecedor).

Estas técnicas de categorização podem ser efetuadas de forma manual ou automática. O segundo componente funcional da proteção contra malware envolve o browser solicitar informações de reputação de URLs, aplicações ou ficheiros específicos aos sistemas de reputação baseados na cloud e, em seguida, emitir um aviso ou bloquear o malware.

Se os resultados indicarem que está presente malware, o browser redireciona o utilizador para uma mensagem de aviso que explica que o URL, aplicação ou ficheiro é malicioso. Alguns sistemas de reputação também incluem conteúdos educativos adicionais. Por outro lado, se o conteúdo 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.

O Google e o Firefox utilizam a API Safe Browsing da Google para reputação de URLs e para avisar ou impedir que os utilizadores transfiram determinados tipos de ficheiros. 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,[1] PhishTank[2] e Metamask[3], juntamente com uma lista de bloqueio de malware da Yandex[4].

Além disso, o Microsoft Defender SmartScreen foi incorporado como funcionalidade ao nível do sistema operativo na atualização de outubro de 2017 do Windows 10. A versão da proteção do SmartScreen ao nível do sistema operativo engloba todos os browsers, clientes de e-mail, unidades USB e outras aplicações, no âmbito da proteção contra malware do sistema operativo. Consequentemente, os utilizadores beneficiam da proteção de URLs, aplicações e ficheiros do browser, juntamente com a proteção do sistema operativo.

Composição do Teste – Amostras de Malware

Os dados incluídos neste relatório dizem respeito a um período de teste de 34 dias, decorrido entre 21 de abril de 2020 e 25 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 ao malware e aos serviços de reputação na cloud.

Concentrámos a nossa atenção na atualização. Consequentemente, avaliámos um número de amostras maior do que aquele que acabou por ser incluído no conjunto de teste final: foram constantemente adicionadas novas amostras ao teste, ao mesmo tempo que as amostras inativas eram removidas.

Número Total de Amostras Maliciosas Incluídas no Teste

Um total de 1.844 amostras não processadas e não validadas foi testado várias vezes em cada browser, perfazendo um total de 182.676 testes discretos realizados sem interrupção ao longo de 822 horas (a intervalos de 6 horas durante 34 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, 1.065 amostras de malware exclusivas e válidas foram incluídas em 129.068 testes discretos de malware válidos (32.267 por browser), proporcionando uma margem de erro inferior a 2 por cento (<2%), com um intervalo de confiança de 95%.

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

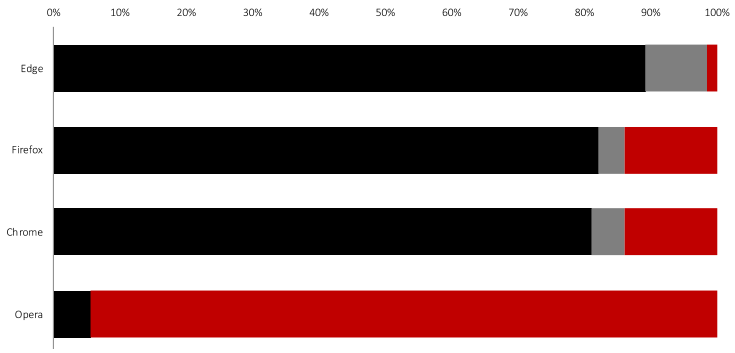
[2] http://www.phishtank.com/

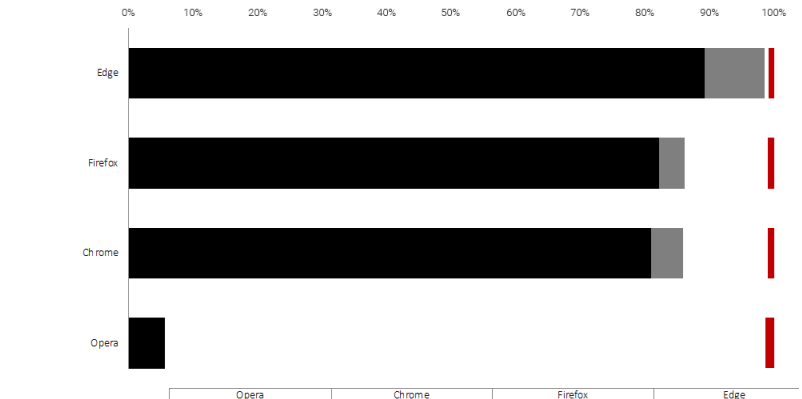
[3] https://github.com/metamask/eth-phishing-detect

[4] https://yandex.com

Taxa de Bloqueio de Malware

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 a ataques de malware por engenharia social. Visto que os sites de malware 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. Consequentemente, 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 malware nas primeiras 24 horas após a deteção do que após este período de tempo.





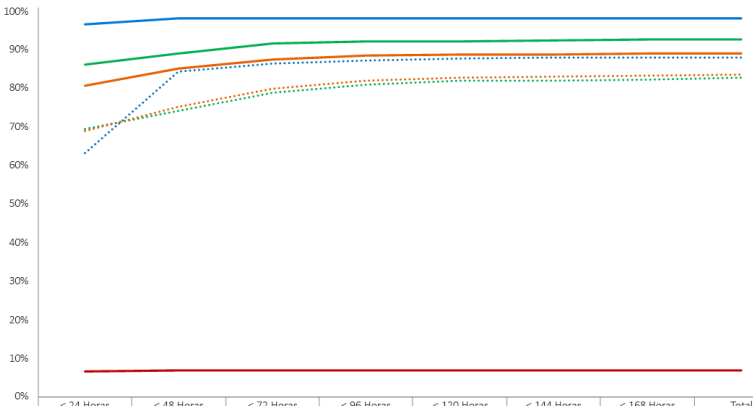
	Opera	Chrome	Firefox	Edge
Reputação de URLs	5,6%	80,9%	82,1%	89,2%
Reputação de URLs + Aplicações	0,0%	5,0%	4,0%	9,3%
Reputação de URLs + Aplicações + SO	93,1%	13,1%	13,0%	0,7%
Falhas	1,4%	0,9%	0,9%	0,8%

A tecnologia de proteção central do Microsoft Edge é o SmartScreen, que proporciona proteção contra ataques baseada em URLs através de um serviço de reputação de URL integrado baseado na cloud, aliado a um sistema de reputação de aplicações para bloqueio de ficheiros maliciosos. O SmartScreen com reputação de aplicações bloqueou 98,5% no Edge. O Mozilla Firefox e o Google Chrome utilizam a API Safe Browsing. O Firefox bloqueou 86,1%. O Google Chrome bloqueou 86,0%. O Opera, que utiliza uma combinação de listas de bloqueio de várias origens, bloqueou 5,6%.

Além disso, o Microsoft Defender SmartScreen bloqueou uma percentagem adicional de ficheiros maliciosos de 93,1% no Opera, 13,1% no Chrome, 13,0% no Firefox e 0,7% no Edge quanto tentámos executá-los.

Histograma da Proteção contra Malware

A proteção imediata contra novo malware é crucial. Os sites que alojam malware 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 mostra o tempo que cada browser demorou a bloquear malware após a amostra 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.



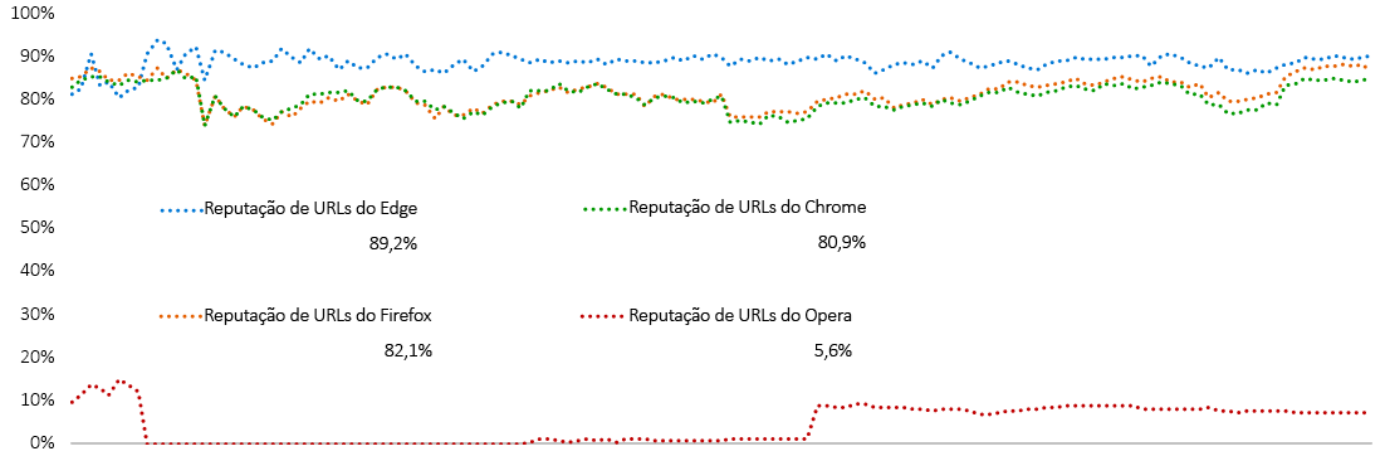
	< 24 Horas	< 48 Horas	< 72 Horas	< 96 Horas	< 120 Horas	< 144 Horas	< 168 Horas	Total
Edge c/ Reputação de Aplicações	96,7%	98,1%	98,1%	98,1%	98,2%	98,2%	98,2%	98,2%
Edge c/ Reputação de Aplicações	63,4%	84,5%	86,5%	87,3%	87,8%	88,1%	88,1%	88,1%
Chrome c/ Reputação de Aplicações	86,2%	89,1%	91,7%	92,2%	92,3%	92,5%	92,7%	92,9%
Chrome c/ Reputação de Aplicações	69,7%	74,4%	79,0%	81,0%	82,0%	82,2%	82,4%	82,7%
Firefox c/ Reputação de Aplicações	80,8%	85,2%	87,6%	88,5%	88,8%	88,9%	89,1%	89,2%
Firefox c/ Reputação de Aplicações	69,1%	75,3%	80,0%	82,1%	82,9%	83,0%	83,4%	83,6%
Opera c/ Reputação de Aplicações	6,8%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%	6,9%

Ao longo do teste, o Microsoft Edge demonstrou uma taxa de proteção inicial de 96,7% contra malware. O Google Chrome e o Mozilla Firefox alcançaram uma taxa de proteção inicial de 86,2% e 80,8%, respetivamente. A taxa de proteção inicial do Opera foi de 6,8%. No final do sétimo dia de testes, todos os browsers registaram um aumento na proteção. O Microsoft Edge registou um aumento de 4,5%, para 98,2%. O Google Chrome registou um aumento de 6,7%, para 92,9%; o Mozilla Firefox registou um aumento de 8,4%, para 89,2%; o Opera registou um aumento de 0,1%, para 6,9%

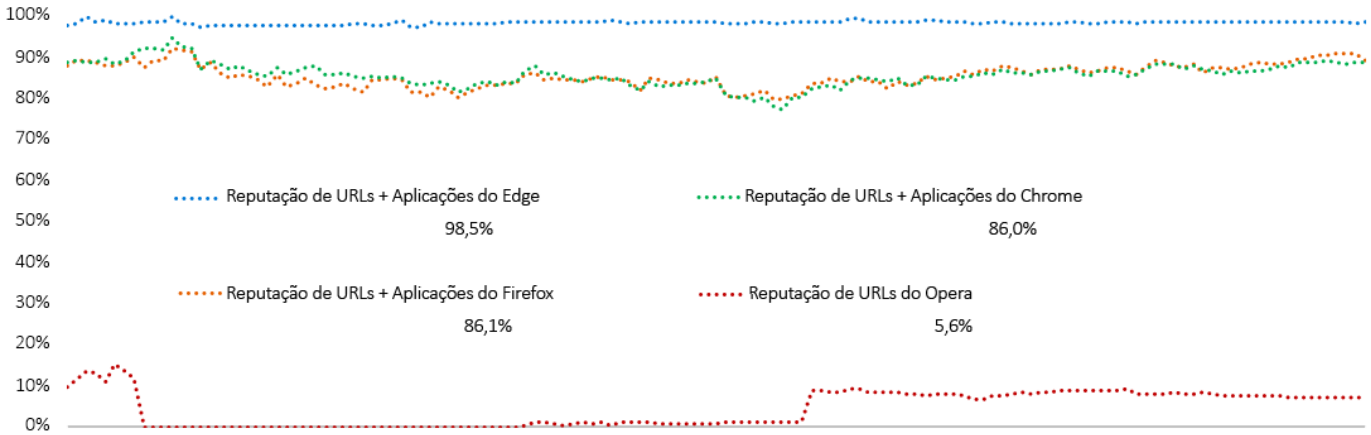
Consistência da Proteção ao Longo do Tempo

Foi constantemente adicionado malware novo ao longo do teste. Os URLs, ficheiros e aplicações que já não estavam contactáveis ou que já não estavam a alojar malware foram removidos. Cada ponto de dados é calculado através de medições registadas num ponto específico no tempo. Se o malware 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 malware, a pontuação diminuía.

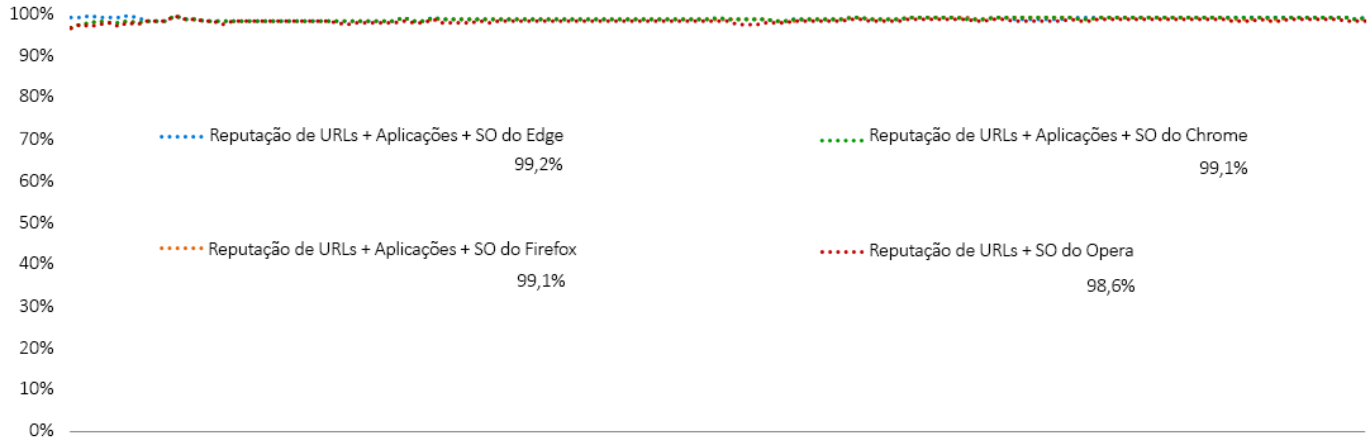
Os testes revelaram três camadas de proteção: reputação de URLs, reputação de aplicações no browser e reputação de aplicações no sistema operativo. A reputação de URLs proporcionou uma proteção razoavelmente boa.



A aplicação da camada de reputação de aplicações aumentou a proteção.



A reputação ao nível do sistema operativo proporcionou proteção adicional. Em circunstâncias ideais, o browser bloqueia o malware de forma a que este nunca alcance o sistema operativo. No entanto, os testes indicaram que a reputação ao nível do sistema operativo era extremamente eficaz.



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 – 84.0.516.1
- 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