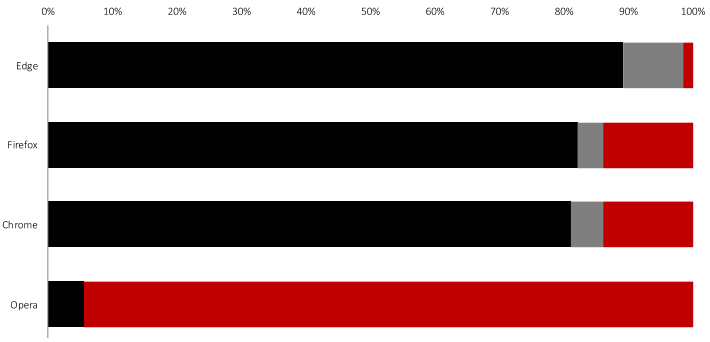
Q2 2020 비교 테스트 보고서

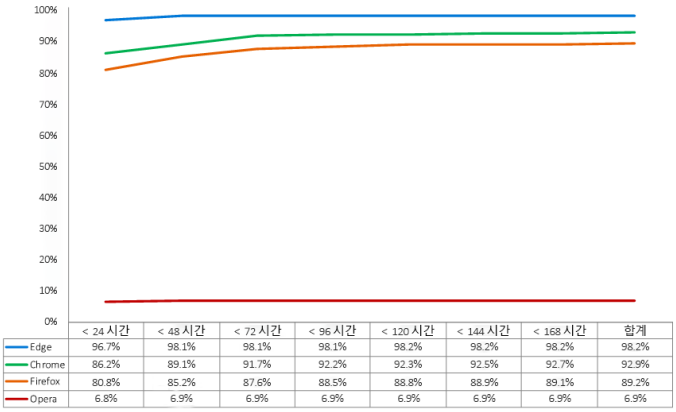
개요

2020 년 2 분기 동안 NSS Labs 는 웹 브라우저에서 제공하는 맬웨어 방지에 대한 독립적인 테스트를 수행했습니다. 34 일 동안 1,065 개의 고유 샘플을 사용하여 웹 브라우저당 32,267 개의 개별 테스트가 수행되었습니다. Microsoft Edge 는 맬웨어로부터 보호하기 위해 Microsoft Defender SmartScreen 을 사용합니다. Google Chrome 및 Mozilla Firefox 는 Google Safe Browser API 를 사용하고, Opera 는 Yandex 를 사용합니다.

Microsoft Edge 는 98.5%의 맬웨어를 차단하는 동시에 가장 높은 제로 시간 보호율(96.7%)을 제공함으로써 보호 기능이 가장 뛰어났습니다. Firefox 가 평균 86.1%를 차단함으로써 두 번째로 높은 보호 기능을 제공했으며, Google Chrome 이 86.0%로 그 뒤를 이었습니다. Opera 는 5.6%를 차단했습니다.



결과 요약

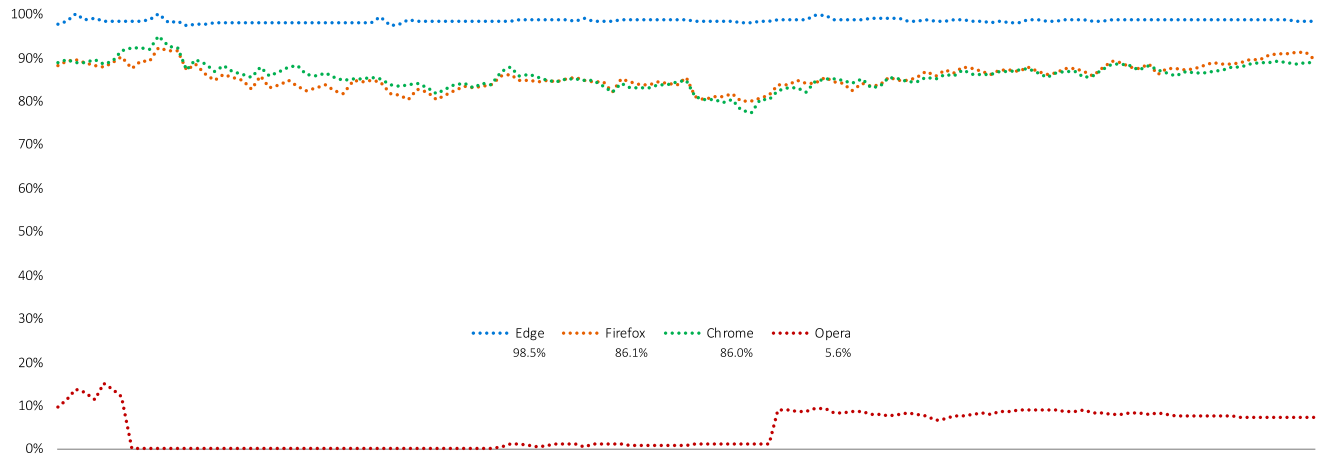


	< 24 시간	< 48 시간	< 72 시간	< 96 시간	< 120 시간	< 144 시간	< 168 시간	합계
Edge	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Chrome	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Firefox	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Opera	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

평판 시스템은 URL, 파일 또는 응용 프로그램을 방지하거나 이러한 것들이 위험하다는 것을 사용자에게 경고함으로써 공격자에게 주어지는 시간을 줄입니다. 하지만 사용자들은 끊임없이 새로운 웹 사이트를 방문하고, 파일을 다운로드하고, 응용 프로그램을 설치합니다. 평판 시스템이 새로운 모든 것을 다 차단할 수는 없습니다. 이를 알고 있는 공격자의 맬웨어 캠페인은 끊임없이 변화하고 있으며, 대부분의 공격은 캠페인 시작 후 처음 몇 시간 안에 발생합니다. 따라서 콘텐츠를 신속하게 분류하는 것이 성공적인 보호의 핵심입니다.

NSS Labs 는 인터넷에서 맬웨어를 발견하는 즉시 브라우저에서 맬웨어를 차단할 수 있는 기능을 평가했습니다. 6 시간마다 악성 URL, 파일 및 응용 프로그램을 계속 테스트하여 공급업체가 보호 기능을 추가하는 데 걸리는 시간을 파악했습니다.

시간 경과에 따른 맬웨어 방지



테스트 내내 새로운 맬웨어가 지속적으로 추가되었습니다. 더 이상 연결할 수 없거나 맬웨어를 호스트하지 않는 URL, 파일 및 응용 프로그램은 제거되었습니다. 각 데이터 점은 특정 시점에 기록된 측정값으로부터 계산됩니다. 맬웨어가 조기에 차단되면 브라우저의 시간 경과에 따른 보호 일관성 점수가 향상됩니다. 반면에 브라우저가 맬웨어를 차단하지 못하면 점수가 떨어집니다.

테스트는 Web Browser Test Methodology v4.0(www.nsslabs.com 에서 확인 가능)을 기반으로 했습니다.

배경 정보

SEM(Social Engineered Malware) 공격은 소셜 미디어, 하이재킹된 이메일 계정, 컴퓨터 문제에 대한 허위 알림 및 기타 잘못된 정보를 동적으로 결합하여 사용자가 맬웨어를 다운로드하도록 유도합니다. 사이버 범죄자는 하이재킹된 이메일을 사용하여 연락처 간의 암묵적 신뢰를 이용하고 피해자를 속여서 악성 파일에 대한 링크를 신뢰할 수 있는 링크로 믿게 만듭니다. 하이재킹된 소셜 미디어 계정은 하이재킹된 이메일 계정과 동일한 방식으로 사용됩니다. 하지만 소셜 네트워크의 경우 그 범위가 더 넓어집니다. 친구나 심지어 친구의 친구까지도 속을 위험이 있습니다.

소셜 엔지니어링 전술을 팝업 메시지를 사용할 수도 있습니다. 예를 들어 Adobe Flash Player 와 같은 응용 프로그램을 설치해야 하거나, 컴퓨터가 감염되었거나 업데이트가 필요한 것처럼 사용자에게 안내할 수 있습니다. 맬웨어가 설치되면 피해자는 신원 도용, 은행 계좌 손상 및 기타 심각한 잠재적 피해에 취약해집니다.

맬웨어에 대한 웹 브라우저 보호

맬웨어로부터 보호하기 위해 브라우저는 악성 웹 사이트를 샅샅이 살펴본 다음 차단 목록이나 허용 목록에 추가하거나 공급업체의 접근 방식에 따라 점수를 할당함으로써 콘텐츠를 적절히 분류합니다.

이러한 분류 기법은 수동으로 또는 자동으로 수행될 수 있습니다. 맬웨어 방지의 두 번째 기능 구성 요소에는 웹 브라우저가 특정 URL, 파일 또는 응용 프로그램에 대한 클라우드 기반 평판 시스템에 평판 정보를 요청한 다음 맬웨어를 경고하거나 차단하는 기능이 포함됩니다.

맬웨어가 있다는 결과가 나타날 경우 웹 브라우저는 URL, 파일 또는 응용 프로그램이 악성이라는 경고 메시지를 사용자에게 리디렉션합니다. 일부 평판 시스템에는 추가적인 교육 콘텐츠도 포함되어 있습니다. 반대로, 콘텐츠가 "양호"한 것으로 확인될 경우 웹 브라우저는 아무런 조치도 취하지 않으며 사용자는 방금 브라우저가 보안 검사를 수행했다는 사실조차 알지 못합니다.

Google 과 Firefox 는 URL 평판을 위해 그리고 사용자가 특정 유형의 파일 다운로드하는 것을 차단하거나 경고하기 위해 Google Safe Browsing API 를 사용합니다. Microsoft Edge 는 응용 프로그램 평판 서비스를 비롯한 Microsoft Defender SmartScreen 을 사용하여 피싱 및 맬웨어 위협으로부터 보호합니다. Opera 는 Netcraft[1], PhishTank[2], Metamask[3]의 차단 목록과 Yandex[4]의 맬웨어 차단 목록을 함께 사용합니다.

또한 Microsoft Defender SmartScreen 은 2017 년 10 월 Windows 10 업데이트를 통해 OS 전체 기능으로 통합되었습니다. 운영 체제 버전의 SmartScreen 보호는 맬웨어에 대한 OS 보호의 일부로서 모든 브라우저, 이메일 클라이언트, USB 및 기타 응용 프로그램을 위한 후방 방어벽입니다. 따라서 사용자는 브라우저 URL 보호, 브라우저 응용 프로그램/파일 보호, 운영 체제 보호 등의 이점을 누릴 수 있습니다.

테스트 구성 요소 – 맬웨어 샘플

이 보고서의 데이터는 2020 년 4 월 21 일부터 2020 년 5 월 25 일까지 34 일의 테스트 기간에 걸쳐 있습니다. 모든 테스트는 텍사스주 오스틴에 위치한 NSS 테스트 시설에서 수행되었습니다. 테스트하는 동안 NSS 엔지니어는 테스트 대상 브라우저가 맬웨어 그리고 클라우드의 평판 서비스에 액세스할 수 있는지 확인하기 위해 정기적으로 연결 상태를 모니터링했습니다.

신선도에 중점을 두었기 때문에 결과적으로 최종 테스트 세트에 남아 있는 것보다 더 많은 수의 샘플이 평가되었습니다. 새로운 샘플이 지속적으로 테스트에 추가되고, 죽은 샘플은 제거되었기 때문입니다.

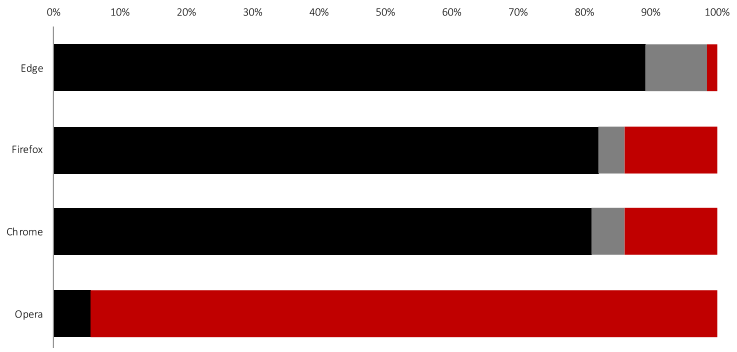
테스트한 전체 악성 샘플 수

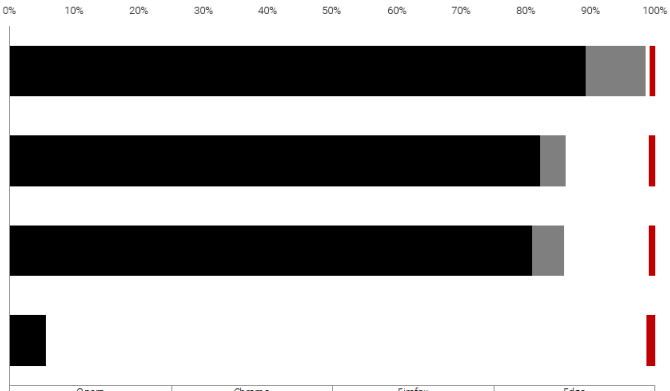
총 1,844 개의 검증되지 않은 원시 샘플이 각 웹 브라우저에서 여러 번 테스트되었으며, 총 182,676 개의 개별 테스트가 822 시간(34 일 동안 6 시간씩) 동안 중단 없이 수행되었습니다. NSS 엔지니어는 익스플로잇에 의해 오염된 샘플(이 테스트에 포함되는 부분이 아님)을 비롯하여 검증 기준을 통과하지 못한 샘플들을 제거했습니다. 최종적으로 1,065 개의 고유하고 유효한 맬웨어 샘플이 129,068 개의 유효한 개별 맬웨어 테스트(웹 브라우저당 32,267 개)에 포함되었으며 신뢰 수준은 95%로 2% 미만(<2%)의 오차 한계를 보였습니다.

[1] http://www.netcraft.com/
[2] http://www.phishtank.com/
[3] https://github.com/metamask/eth-phishing-detect
[4] https://yandex.com

맬웨어 차단율

악성 웹 사이트에 들어가려 한다는 것을 잠재적 피해자에게 경고하는 기능을 갖춘 웹 브라우저는 소셜 엔지니어링 맬웨어와의 싸움에서 유리한 위치를 차지하게 됩니다. 맬웨어 사이트는 수명이 짧기 때문에 사이트를 최대한 빨리 검색, 검증, 분류하여 평판 시스템에 추가하는 것이 중요합니다. 따라서 우수한 평판 시스템은 높은 탐지율을 실현하기 위해 정확하고 빨라야 합니다. 브라우저 개발자는 이러한 관계를 명확하게 이해하고 있으며, 발견 후 24 시간 이내에 차단되는 맬웨어가 그 이후 차단되는 맬웨어보다 훨씬 많습니다.





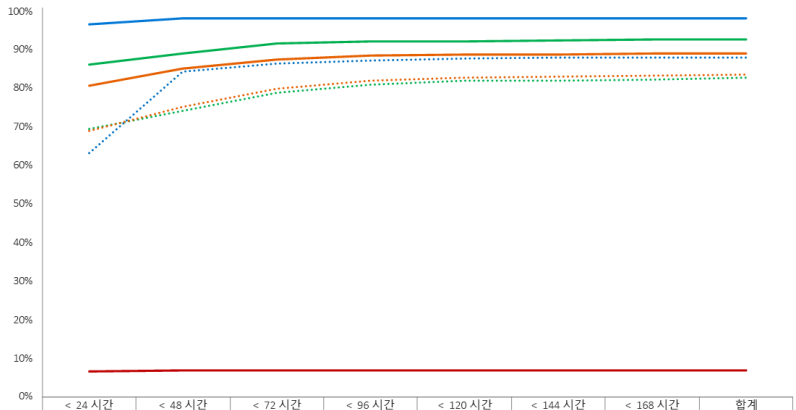
	Opera	Chrome	Firefox	Edge
URL 평판	5.6%	80.9%	82.1%	89.2%
URL + 앱 평판	0.0%	5.0%	4.0%	9.3%
URL + 앱 + OS 평판	93.1%	13.1%	13.0%	0.7%
누락	1.4%	0.9%	0.9%	0.8%

Edge 의 핵심 보호 기술은 SmartScreen 입니다. SmartScreen 은 통합 클라우드 기반 URL 평판 서비스를 통해 공격에 대한 URL 기반 보호를 제공할 뿐만 아니라 악성 파일 차단을 위한 응용 프로그램 평판도 제공합니다. 응용 프로그램 평판을 제공하는 SmartScreen 은 Edge 에서 98.5%를 차단했습니다. Mozilla Firefox 와 Google Chrome 은 Safe Browsing API 를 사용합니다. Firefox 는 86.1%를 차단했습니다. Google Chrome 은 86.0%를 차단했습니다. 여러 소스의 차단 목록을 조합하여 사용하는 Opera 는 5.6%를 차단했습니다.

또한 Microsoft Defender SmartScreen 은 악성 파일을 실행하려고 시도할 때 Opera 에서 93.1%, Chrome 에서 13.1%, Firefox 에서 13.0%, Edge 에서 0.7%의 악성 파일을 추가적으로 차단했습니다.

맬웨어 방지 히스토그램

새로운 맬웨어는 즉각적으로 보호하는 것이 중요합니다. 맬웨어를 호스트하는 사이트는 발견 후 비교적 짧은 시간 안에 제거되는 경우가 많습니다. 적시에 보호를 추가하지 못하는 제품은 위협에 대응하기에 너무 늦을 수 있습니다. 히스토그램에서는 샘플이 테스트 주기에 들어온 후 각 브라우저가 맬웨어를 차단하는 데 걸린 시간을 보여줍니다. 7 일 기간 동안 위협이 차단될 때까지 매일 누적 보호율이 계산됩니다.



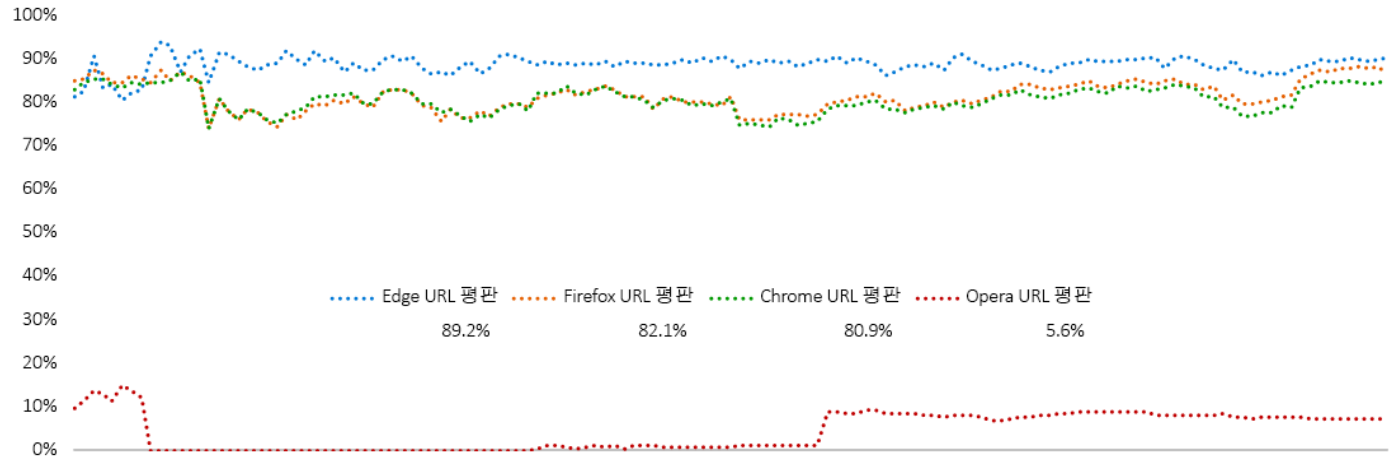
	< 24 시간	< 48 시간	< 72 시간	< 96 시간	< 120 시간	< 144 시간	< 168 시간	합계
Edge 및 앱 평판	96.7%	98.1%	98.1%	98.1%	98.2%	98.2%	98.2%	98.2%
Edge 및 URL 평판	63.4%	84.5%	86.5%	87.3%	87.8%	88.1%	88.1%	88.1%
Chrome 및 앱 평판	86.2%	89.1%	91.7%	92.2%	92.3%	92.5%	92.7%	92.9%
Chrome 및 URL 평판	69.7%	74.4%	79.0%	81.0%	82.0%	82.2%	82.4%	82.7%
Firefox 및 앱 평판	80.8%	85.2%	87.6%	88.5%	88.8%	88.9%	89.1%	89.2%
Firefox 및 URL 평판	69.1%	75.3%	80.0%	82.1%	82.9%	83.0%	83.4%	83.6%
Opera 및 URL 평판	6.8%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%	6.9%

테스트 중에 Microsoft Edge 는 맬웨어에 대한 초기 보호율이 96.7%로 나타났습니다. Google Chrome 과 Mozilla Firefox 는 각각 86.2%, 80.8%의 초기 보호율을 달성했습니다. Opera 의 초기 보호율은 6.8%였습니다. 테스트 7 일째가 끝나는 시점에서 모든 웹 브라우저는 보호율이 상승했습니다. Microsoft Edge 는 4.5% 상승하여 98.2%가 되었습니다. Google Chrome 은 6.7% 상승한 92.9%, Mozilla Firefox 는 8.4% 상승한 89.2% Opera 는 0.1% 상승한 6.9%였습니다.

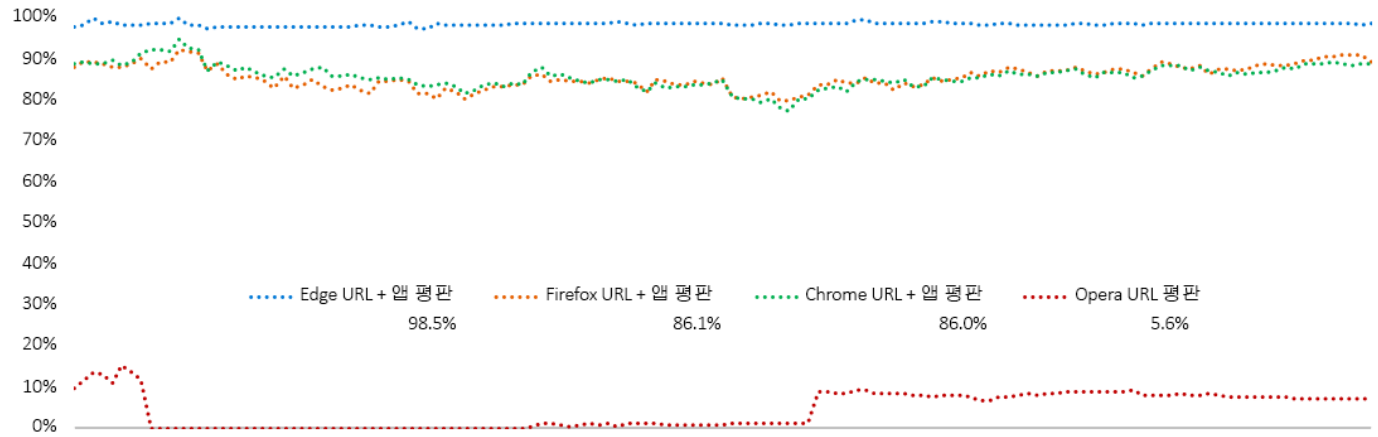
시간 경과에 따른 보호 일관성

테스트 내내 새로운 맬웨어가 지속적으로 추가되었습니다. 더 이상 연결할 수 없거나 맬웨어를 호스트하지 않는 URL, 파일 및 응용 프로그램은 제거되었습니다. 각 데이터 점은 특정 시점에 기록된 측정값으로부터 계산됩니다. 맬웨어가 조기에 차단되면 브라우저의 시간 경과에 따른 보호 일관성 점수가 향상됩니다. 반면에 브라우저가 맬웨어를 차단하지 못하면 점수가 떨어집니다.

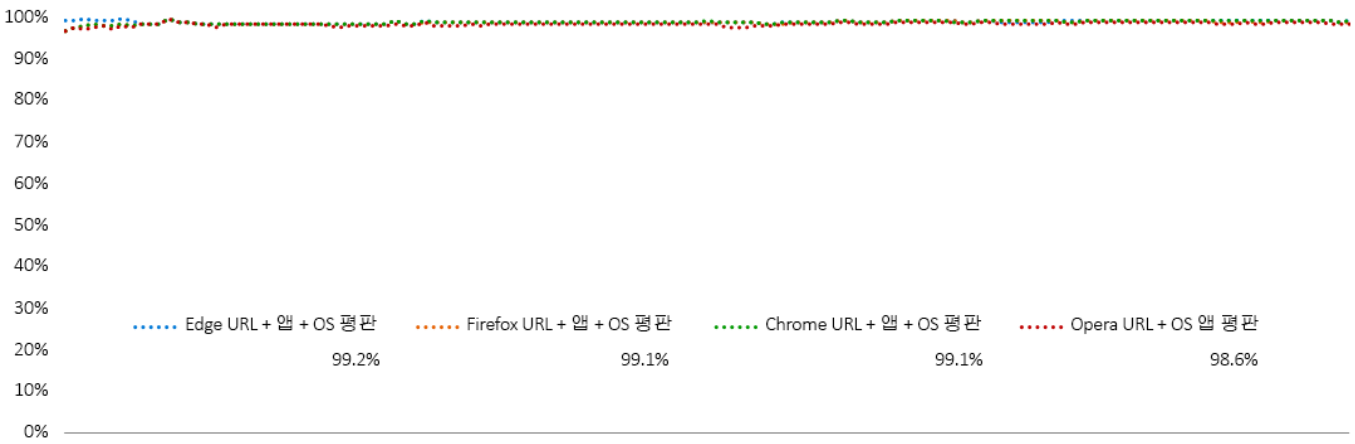
테스트 결과, 다음과 같은 세 가지 보호 계층이 발견되었습니다. URL 평판, 브라우저에서의 응용 프로그램 평판, OS 응용 프로그램 평판입니다. URL 평판은 상당히 우수한 보호 기능을 제공했습니다.



여기에 응용 프로그램 평판까지 더해지면 보호 기능이 강화되었습니다.



운영 체제 평판은 또 다른 추가적인 보호 기능을 제공했습니다. 웹 브라우저가 맬웨어를 차단하여 운영 체제에 도달하지 못하게 하는 것이 이상적입니다. 어쨌든 테스트 결과, 운영 체제 평판은 매우 효과적인 것으로 나타났습니다.



테스트 환경

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

테스트한 제품

- Google Chrome: 버전 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: 버전 83.0.478.10 – 84.0.516.1
- Mozilla Firefox: 버전 75.0 – 76.0.1
- Opera: 버전: 67.0.3575.137 – 68.0.3618.125

작성자

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

테스트 방법론

NSS Labs WBS(Web Browser Security) Test Methodology v4.0 을 www.nsslabs.com 에서 확인할 수 있습니다.

연락처 정보

NSS Labs, Inc.

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

info@nsslabs.com

www.nsslabs.com