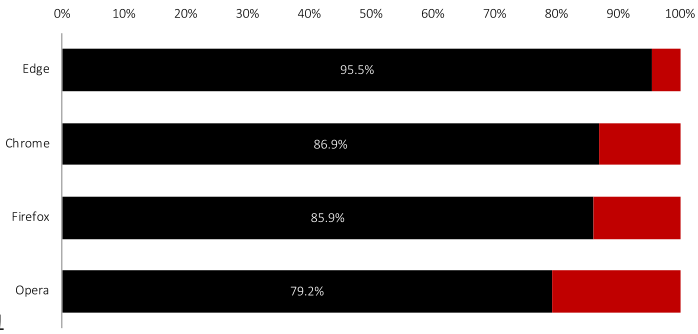
Q2 2020 비교 테스트 보고서

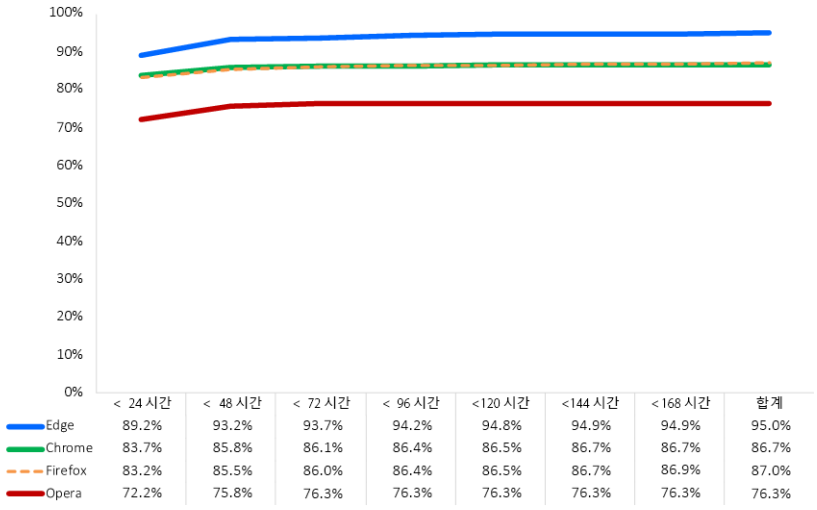
개요

2020 년 2 분기 동안 NSS Labs 는 웹 브라우저에서 제공하는 피싱 방지에 대한 독립적인 테스트를 수행했습니다. 18 일 동안 2,443 개의 고유 피싱 URL 을 사용하여 웹 브라우저당 47,274 개의 개별 테스트가 수행되었습니다. Microsoft Edge 는 피싱으로부터 보호하기 위해 Microsoft Defender SmartScreen 을 사용합니다. Google Chrome 및 Mozilla Firefox 는 Google Safe Browser API 를 활용하고, Opera 는 타사 차단 목록의 조합을 사용합니다.

Microsoft Edge 는 95.5%의 피싱 URL 을 차단하는 동시에 가장 높은 제로 시간 보호율(89.2%)을 제공함으로써 보호 기능이 가장 뛰어났습니다. Google Chrome 이 평균 86.9%를 차단함으로써 두 번째로 높은 보호 기능을 제공했으며, Mozilla Firefox 가 85.9%로 그 뒤를 이었습니다. Opera 는 79.2%를 차단했습니다.



결과 요약

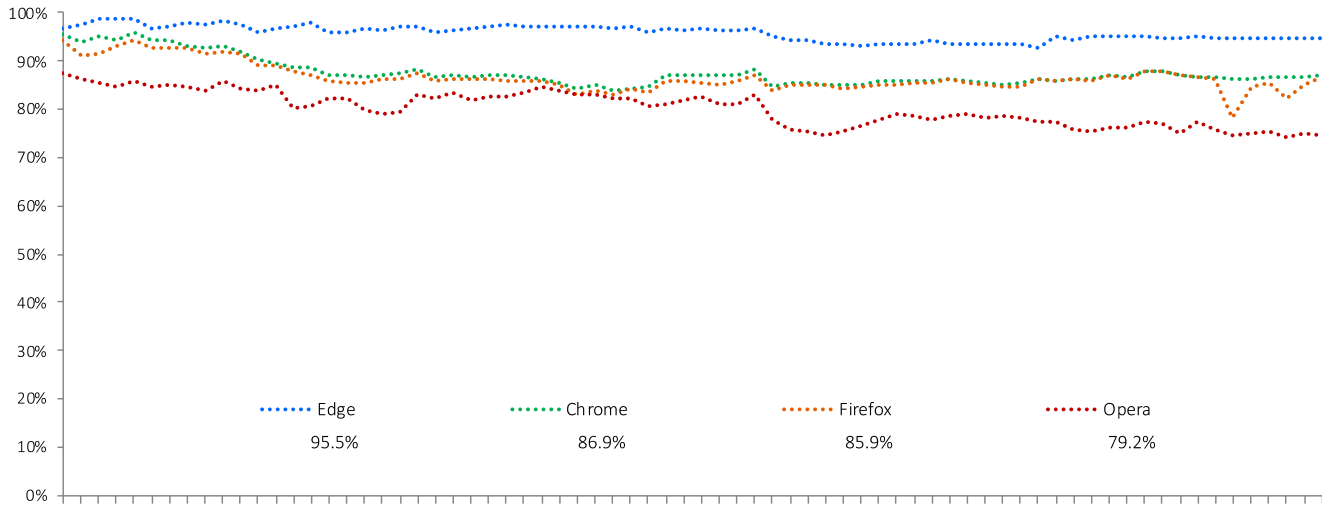


	< 24 시간	< 48 시간	< 72 시간	< 96 시간	<120 시간	<144 시간	< 168 시간	합계
Edge	89.2%	93.2%	93.7%	94.2%	94.8%	94.9%	94.9%	95.0%
Chrome	83.7%	85.8%	86.1%	86.4%	86.5%	86.7%	86.7%	86.7%
Firefox	83.2%	85.5%	86.0%	86.4%	86.5%	86.7%	86.9%	87.0%
Opera	72.2%	75.8%	76.3%	76.3%	76.3%	76.3%	76.3%	76.3%

URL 평판 시스템은 URL 을 방지하거나 URL 이 알려진 피싱 사이트라는 것을 사용자에게 경고함으로써 공격자에게 주어지는 시간을 줄입니다. 하지만 사용자들은 수많은 웹 사이트를 방문하고 그중에 다수가 새로운 웹 사이트이기 때문에 URL 평판 시스템이 새로운 URL 을 다 차단할 수는 없습니다. 이를 알고 있는 공격자의 피싱 캠페인은 끊임없이 변화하고 있으며, 대부분의 새로운 공격은 공격 시작 후 처음 몇 시간 안에 발생합니다.

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

시간 경과에 따른 피싱 방지



테스트 내내 새로운 피싱 URL 이 매일 추가되었으며, 더 이상 연결할 수 없거나 더 이상 피싱 공격을 제공하지 않는 URL 은 제거되었습니다. 각 데이터 점은 특정 시점의 보호를 나타냅니다. URL 이 조기에 차단되면 브라우저의 시간 경과에 따른 보호 일관성 점수가 향상됩니다. 반면에 브라우저가 URL 을 차단하지 못하면 점수가 떨어집니다.

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

배경 정보

피싱은 공격자에게 중요한 개인 정보를 제공하도록 피해자를 속이는 소셜 엔지니어링 공격의 한 종류입니다. 중요한 정보의 예로는 신용카드 번호, 주민등록번호, 은행 계좌의 로그인 정보 및 암호를 들 수 있습니다. 이메일, 인스턴트 메시지, SMS 메시지, 소셜 네트워킹 사이트 링크 모두가 피싱 공격의 매개체가 됩니다. 피싱 웹 사이트의 방문 페이지에서 방문자의 컴퓨터를 몰래 악용하고 악성 소프트웨어를 설치하려고 시도하는 경우도 많습니다(일명 드라이브-바이 익스플로잇).

피싱 공격은 중요한 개인 및 기업 정보를 손상시키거나 훔칠 수 있으므로 개인과 조직 모두에게 상당한 위험을 초래합니다. APWG(Anti-Phishing Working Group)는 2020 년 1 분기에 총 165,772 건의 고유 이메일 피싱 캠페인을 보고했습니다.[1] 피싱 공격이 점점 더 복잡해지고 정교해짐에 따라 이를 탐지하고 방지하기가 더 어려워지고 있습니다.

피싱에 대한 웹 브라우저 보호

피싱 방지는 클라우드의 평판 서버에 URL 의 평판을 요청하는 웹 브라우저 내의 응용 프로그램에 의해 제공됩니다. 평판 서버는 인터넷을 샅샅이 살펴봐서 피싱 웹 사이트를 찾은 다음 각 URL 에 점수를 할당하고 차단 목록에 추가합니다. 이렇게 하면 웹 브라우저가 URL 을 방문할 때 브라우저의 피싱 방지 기능(Safe Browsing, SmartScreen 등)이 클라우드 기반 평판 서버에 URL 의 평판을 요청하고, 웹 사이트 결과가 "불량"으로 표시될 경우에는 URL 이 악성이라는 것을 설명하는 경고 메시지를 사용자에게 리디렉션합니다. 일부 평판 시스템에는 추가적인 교육 콘텐츠도 포함되어 있습니다. 반대로, 웹 사이트가 "양호"한 것으로 확인될 경우 웹 브라우저는 아무런 조치도 취하지 않으며 사용자는 방금 브라우저가 보안 검사를 수행했다는 사실조차 알지 못합니다.

테스트 구성 요소 – 피싱 URL

이 보고서의 데이터는 2020 년 4 월 21 일부터 2020 년 5 월 8 일 금요일까지 18 일의 테스트 기간에 걸쳐 있습니다. 모든 테스트는 텍사스주 오스틴에 위치한 NSS 테스트 시설에서 수행되었습니다. 테스트하는 동안 NSS 엔지니어는 테스트 대상 브라우저가 피싱 URL 그리고 클라우드의 브라우저 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 사이트가 평가되었습니다. 새로운 URL 이 지속적으로 테스트에 추가되고, 사용하지 않는 사이트는 제거되었기 때문입니다.

테스트한 전체 악성 URL 수

총 4,020 개의 검증되지 않은 원시 URL 이 각 웹 브라우저에서 여러 번 테스트되었으며, 총 222,527 개의 개별 테스트가 430 시간(18 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 2,443 개의 고유하고 유효한 피싱 URL 이 189,096 개의 유효한 개별 피싱 테스트(웹 브라우저당 47,274 개)에 포함되었으며 신뢰 수준은 95%로 2% 미만(<2%)의 오차 한계를 보였습니다.

하루에 추가된 평균 악성 URL 수

하루 평균 136 개의 새 검증된 URL 이 테스트 세트에 추가되었습니다. 범죄 활동량이 차이를 보임에 따라 이 숫자는 날짜별로 편차가 있었습니다.

피싱 URL 차단

NSS 는 인터넷에서 악성 URL 을 발견하는 차단할 수 있는 브라우저의 능력을 평가했습니다. 엔지니어들은 6 시간마다 이 테스트를 반복하여 공급업체가 보호 기능을 추가하는 데 걸리는 시간을 파악했습니다.

새로운 Microsoft Edge 는 Chromium 을 기반으로 하며 2020 년 1 월 15 일에 공개되었습니다. Windows 및 macOS 의 모든 지원되는 버전과 호환됩니다. 이 브라우저를 다운로드하면 Windows 10 PC 에서 기존 버전의 Microsoft Edge 가 대체됩니다.

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

[1] APWG 피싱 활동 경향 보고서

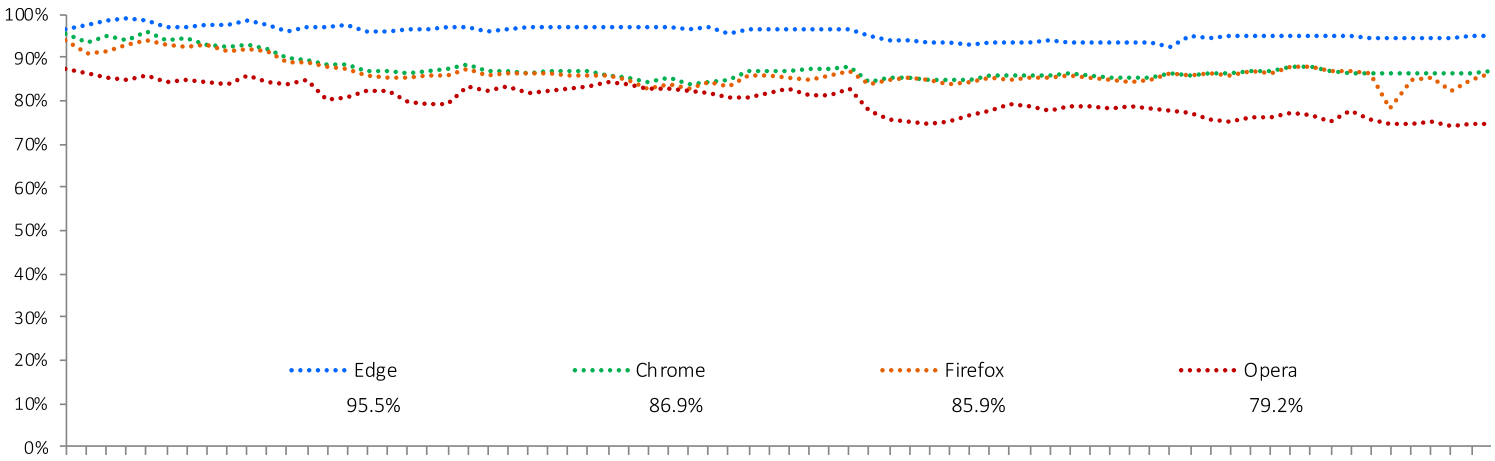
피싱 차단율

Google Chrome 과 Mozilla Firefox 는 Google 의 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[2], PhishTank[3], Metamask[4]의 차단 목록과 Yandex[5]의 맬웨어 차단 목록을 함께 사용합니다.

악성 웹 사이트에 들어가려 한다는 것을 잠재적 피해자에게 경고하는 기능을 갖춘 웹 브라우저는 피싱 및 기타 범죄 활동과의 싸움에서 유리한 위치를 차지하게 됩니다. 피싱 사이트는 수명이 짧기 때문에 사이트를 최대한 빨리 검색, 검증, 분류하여 평판 시스템에 추가하는 것이 중요합니다. 평균 차단 시간과 탐지율의 상관관계에서 그러한 점이 바로 드러납니다. 우수한 평판 시스템은 높은 탐지율을 실현하기 위해 정확하고 빨라야 합니다. 브라우저 개발자는 이러한 관계를 명확하게 이해하고 있으며, 발견 후 24 시간 이내에 차단되는 피싱 사이트가 그 이후 차단되는 맬웨어보다 훨씬 많습니다.

각 브라우저의 개별 차단 성능을 지속적으로 측정했으며, 브라우저에서 테스트한 모든 URL 의 전체 차단율을 기록했습니다. 브라우저의 전체 차단율은 성공한 차단 수를 전체 테스트 사례 수로 나눠서 계산합니다. 예를 들어 6 시간마다 테스트를 수행하면 48 시간 동안 온라인 상태였던 URL 이 8 회 테스트되는 것입니다. 최대 8 회 중 6 회 차단하는 브라우저의 차단율은 75%가 됩니다.

시간 경과에 따른 보호 일관성



테스트 내내 새로운 피싱 URL 이 매일 추가되었으며, 더 이상 연결할 수 없거나 더 이상 피싱 URL 을 제공하지 않는 URL 은 제거되었습니다. 각 데이터 점은 특정 시점의 보호를 나타냅니다. URL 이 조기에 차단되면 브라우저의 시간 경과에 따른 보호 일관성 점수가 향상됩니다. 반면에 브라우저가 URL 을 차단하지 못하면 점수가 떨어집니다.

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

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

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

[5] https://yandex.com

피싱 방지 히스토그램

새로운 피싱 URL 에 대한 즉각적인 보호가 중요합니다. 피싱 사이트는 발견 후 비교적 짧은 시간 안에 제거되는 경우가 많습니다. 적시에 보호를 추가하지 못하는 제품은 위협에 대응하기에 너무 늦을 수 있습니다. 아래의 히스토그램은 위협 요소가 테스트 주기에 들어온 후 각 브라우저가 피싱 사이트를 차단하는 데 걸린 시간을 보여줍니다. 7 일 기간 동안 위협이 차단될 때까지 매일 누적 보호율이 계산됩니다.

테스트 중에 Microsoft Edge 는 피싱 공격에 대한 초기 보호율이 89.2%로 나타났습니다. Google Chrome 과 Mozilla Firefox 는 각각 83.7%, 83.2%의 초기 보호율을 달성했습니다. Opera 의 초기 보호율은 72.2%였습니다. 테스트 7 일째가 끝나는 시점에서 모든 웹 브라우저는 보호율이 상승했습니다. Microsoft Edge 는 5.7% 상승하여 94.9%가 되었습니다. Mozilla Firefox 는 3.7% 상승한 86.9%, Google Chrome 은 3% 상승한 86.7%였습니다. Opera 는 4.1% 상승하여 76.3%가 되었습니다.

	< 24 시간	< 48 시간	< 72 시간	< 96 시간	<120 시간	<144 시간	<168 시간	합계
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%

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 – 84.0.502.0
- 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