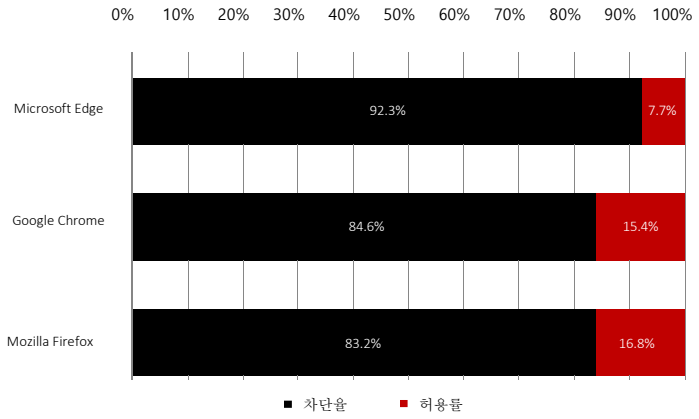
2021년 2분기 웹 브라우저의 피싱 방지 기능

개요

CyberRatings.org에서는 2021년 2분기에 웹 브라우저에서 제공되는 피싱 방지 기능 관련 독립 테스트를 진행했습니다. 이 독립 테스트에서는 20일 동안 개별 테스트 80회가 실행되었습니다. Microsoft Edge에서는 피싱 방지를 위해 Microsoft Defender SmartScreen을 사용하며, Google Chrome과 Mozilla Firefox에서는 Google 세이프 브라우징 API를 사용합니다.

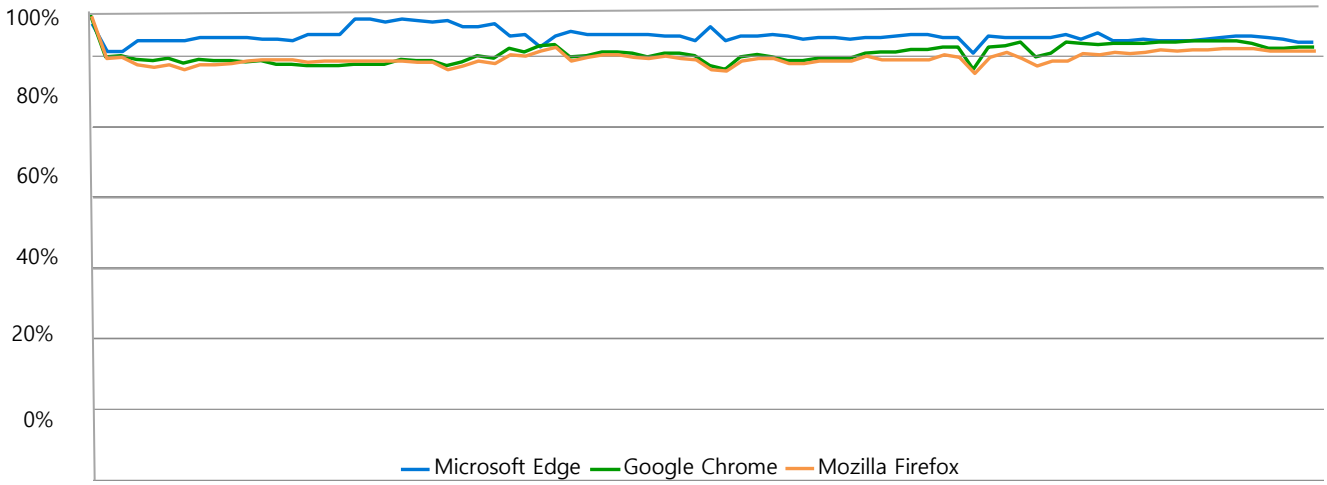
테스트 결과 최고의 피싱 방지 기능을 제공하는 브라우저는 Microsoft Edge로 나타났습니다. Edge는 피싱 URL 92.3%를 차단했으며, 제로 아워 방지율도 93.5%로 가장 높았습니다. Google Chrome이 2위(평균 차단율 84.6%), Mozilla Firefox가 3위(83.2%)를 차지했습니다.



결과 요약

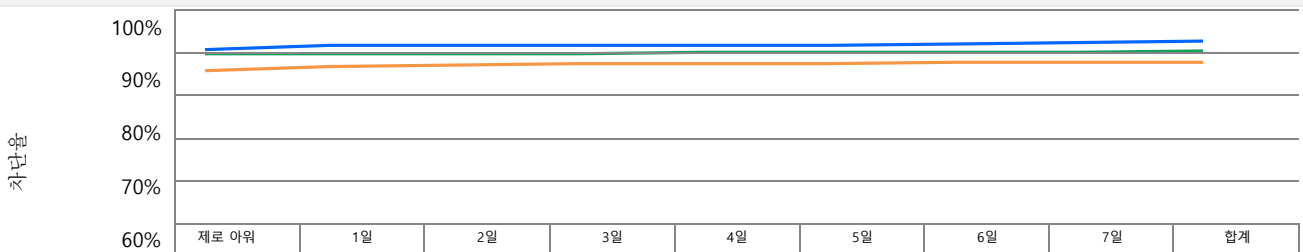
URL 신뢰도 시스템을 활용하면 공격자가 공격 목표를 달성해야 하는 제한 시간을 단축할 수 있습니다. 특정 URL이 알려진 피싱 사이트임을 사용자에게 경고하고 해당 URL 방문을 차단할 수 있기 때문입니다. 하지만 사용자는 매우 다양한 웹 사이트를 방문하며 대다수 웹 사이트는 처음 방문하는 곳이므로, URL 신뢰도 시스템에서 단순히 모든 신규 URL을 차단할 수는 없습니다. 공격자들도 이러한 약점을 간파하고 있으므로 피싱 캠페인도 계속해서 바뀌고 있으며, 공격 시작 시점으로부터 처음 몇 시간 내에 대량의 신규 공격이 진행됩니다.

장기적인 피싱 방지 비율



테스트 과정에서는 새 피싱 URL이 매일 추가되었으며, 더 이상 연결할 수 없거나 피싱 공격이 진행되지 않은 URL은 제거되었습니다. 각 데이터 포인트는 특정 시점의 피싱 방지 상태에 해당됩니다. 초기에 URL이 차단된 경우 브라우저의 장기적인 피싱 방지 일관성 점수가 상향 조정되었습니다. 반면 URL을 차단하지 못한 브라우저의 경우에는 해당 점수가 하향 조정되었습니다.

장기적 차단율



	제로 아워	1일	2일	3일	4일	5일	6일	7일	합계
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%

이 테스트에서는 인터넷에서 발견된 악성 URL을 브라우저가 최대한 빨리 차단하는 능력을 측정했습니다. 6시간 단위로 측정을 계속 진행하여 각 브라우저 제조업체가 피싱 방지 기능을 추가하는 데 걸리는 시간을 확인했습니다. 테스트 주기에 피싱 위협이 추가시점부터 각 브라우저가 피싱 사이트를 차단할 때까지의 대응 시간이 위 그림에 나와 있습니다.

피싱 공격

피싱은 피해자가 공격자에게 중요한 개인 정보를 제공하도록 유도하는 일종의 소셜 엔지니어링 공격입니다. 중요한 정보의 예로는 신용 카드 번호, 사회 보장 번호, 은행 계좌용 로그인 및 암호 등이 있습니다. 이메일, 인스턴트 메시지, SMS 메시지, 소셜 네트워킹 사이트의 링크 등은 모두 피싱 공격의 벡터라 할 수 있습니다. 피싱 웹 사이트의 방문 페이지에서는 방문자 컴퓨터를 몰래 악용하여 소위 "드라이브 바이 익스플로잇(drive-by exploit)"이라는 악성 소프트웨어를 설치하는 경우가 많습니다.

개인과 회사의 중요한 정보를 입수하거나 손상시키겠다고 위협하는 방식으로 진행되는 피싱 공격은 개인은 물론 조직 전체에도 매우 위험합니다. APWG(Anti-Phishing Working Group)의 보고에 따르면, 2020년 4분기에만 확인된 고유 이메일 피싱 캠페인은 총 396,688건에 달합니다.1

웹 브라우저의 피싱 방지 기능

웹 브라우저의 애플리케이션을 통해 제공되는 피싱 방지 기능은 클라우드 서비스에서 URL의 신뢰도를 요청합니다. 이 서비스는 인터넷에서 피싱 웹 사이트를 찾아 차단 목록에 추가합니다. 따라서 웹 브라우저가 URL 방문을 시도하면 세이프 브라우징, SmartScreen 등 해당 브라우저의 피싱 방지 기능이 해당 URL은 악성 사이트임을 설명하는 경고 메시지로 사용자를 리디렉션합니다. 추가 교육 콘텐츠를 제공하는 신뢰도 시스템도 있습니다. 반면 웹 사이트가 "정상"으로 확인되면 웹 브라우저는 아무 조치도 취하지 않습니다.

Google과 Firefox는 Google 세이프 브라우징 API를 사용하여 URL 신뢰도를 확인하고 사용자에게 특정 파일 형식 다운로드 관련 경고를 표시합니다. Microsoft Edge는 Microsoft Defender SmartScreen을 사용합니다. SmartScreen은 클라우드 기반 통합 URL 신뢰도 서비스를 통해 URL 기반 공격 방지 기능을 제공하는 동시에, 애플리케이션 신뢰도를 확인하여 악성 파일을 차단합니다.

매일 추가된 평균 악성 URL 수

이 테스트에서는 유효성이 검사된 신규 URL 평균 50개가 매일 테스트 집합에 추가되었습니다. 범죄 활동 수준이 매일 바뀜에 따라 실제로 추가된 정확한 URL의 수는 매일 달랐습니다.

테스트에서 확인된 총 악성 URL 수

각 웹 브라우저에서는 총 테스트 주기 80회 동안 유효성이 검사되지 않은 원시 URL 26,976개를 반복 테스트했습니다. 20일(480시간) 동안 6시간 단위로 중단 없이 테스트가 진행되었습니다. CyberRatings의 엔지니어들이 익스플로잇에 감염된 샘플(테스트 대상에서 제외됨)을 비롯하여 유효성 검사 기준을 통과하지 못한 샘플을 제거했습니다. 이에 따라 최종적으로는 개별 유효 피싱 테스트 61,605회에서 고유한 유효 피싱 URL 996개를 테스트했습니다(웹 브라우저당 테스트 20,535회 실행). 테스트 오차 범위는 3.1%, 신뢰도는 95%였습니다.

테스트 내용 - 피싱 URL

이 보고서에는 테스트 기간 2021년 5월 11일~5월 31일(20일)에 진행된 테스트의 데이터가 포함되어 있습니다. 테스트 기간 동안에는 CyberRatings의 엔지니어들이 연결을 모니터링하여 테스트 대상 브라우저가 피싱 URL 및 클라우드의 브라우저 신뢰도 서비스에 액세스할 수 있는지 확인했습니다.

그리고 각 브라우저가 새로운 피싱 공격을 차단할 수 있는지를 확인하기 위해 새 URL이 테스트에 계속 추가되었으며 연결 불가 상태가 된 사이트는 제거되었습니다.

결과 평가 방식

CyberRatings에서는 인터넷에서 발견된 악성 URL을 각 브라우저가 최대한 빨리 차단하는 능력을 측정했습니다. 엔지니어들은 6시간 단위로 이러한 테스트를 반복 진행하여 각 브라우저 제조업체가 피싱 방지 기능을 추가하는 데 걸리는 시간(해당 기능을 추가한 경우)을 확인했습니다.

테스트에서는 브라우저의 성능을 지속적으로 측정했으며, 브라우저에서 테스트한 모든 URL의 전반적 차단율을 기록했습니다. 악성 URL 차단 성공 횟수를 총 테스트 사례 수로 나누어 각 브라우저의 전반적 차단율을 계산했습니다. 가령 6시간마다 진행된 테스트에서 48시간 동안 온라인 상태였던 URL을 8회 테스트했다면 전체 테스트 실행 8회에서 해당 URL을 6회 차단한 브라우저의 차단율은 75%입니다.

테스트 환경

- Microsoft Windows 10 Pro, 21H1

테스트 대상 제품

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

1 APWG 피싱 활동 추세 보고서

저자

Thomas Skybakmoen, Vikram Phatak

테스트 방법론

CyberRatings 웹 브라우저 보안 테스트 방법론 v1.0은 www.cyberratings.org에서 제공됩니다.

문의처 정보

CyberRatings.org

2303 Ranch Road 620 South

Suite 160, #501

Austin, TX 78734

info@cyberratings.org

www.cyberratings.org