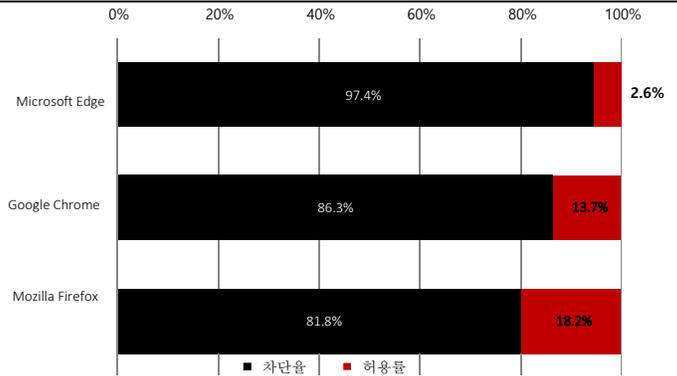


2021년 2분기 웹 브라우저의 맬웨어 방지 기능

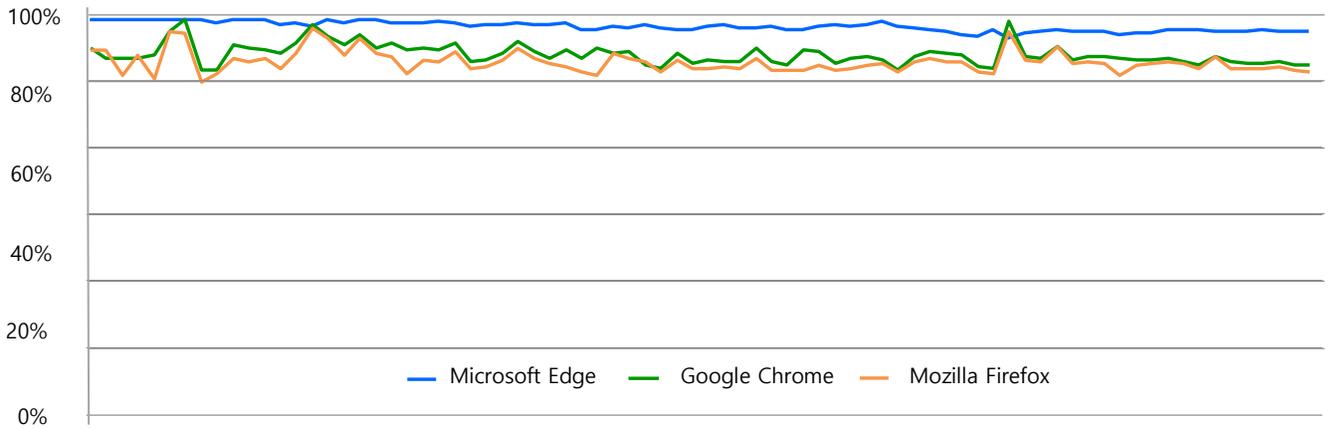
개요

CyberRatings.org에서는 2021년 2분기에 웹 브라우저에서 제공되는 맬웨어 방지 기능 관련 독립 테스트를 진행했습니다. 이 독립 테스트에서는 20일 동안 개별 테스트 80회가 실행되었습니다. Microsoft Edge에서는 맬웨어 방지를 위해 Microsoft Defender SmartScreen을 사용하며, Google Chrome과 Mozilla Firefox에서는 Google 세이프 브라우징 API를 사용합니다. 테스트 결과 최고의 맬웨어 방지 기능을 제공하는 브라우저는 Microsoft Edge로 나타났습니다. Edge는 맬웨어 97.4%를 차단했으며, 제로 아워 방지율도 97.7%로 가장 높았습니다. Google Chrome이 2위(평균 차단율 86.3%), Mozilla Firefox가 3위(81.8%)를 차지했습니다.



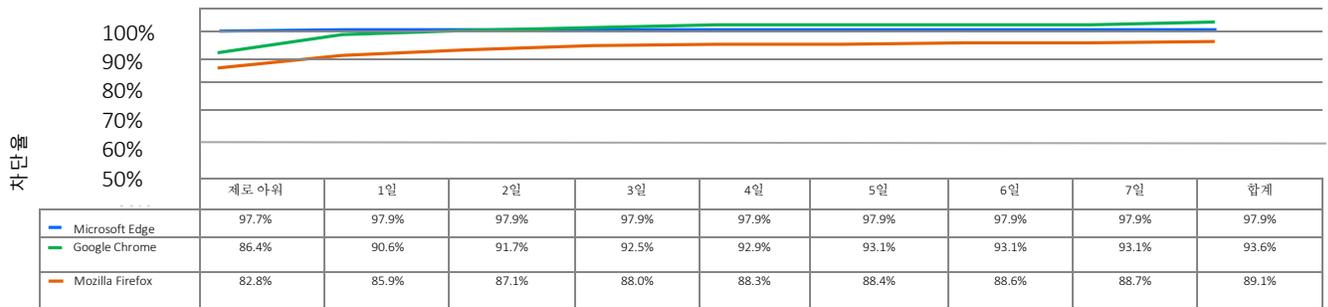
악성 웹 사이트를 방문하려는 잠재적 피해자에게 경고를 제공할 수 있는 웹 사이트는 맬웨어를 효율적으로 차단할 수 있습니다. 소셜 엔지니어링 기법을 통해 사용자가 맬웨어를 다운로드하도록 유도하는 웹 사이트는 사용 시간이 짧은 편이므로, 해당 사이트를 최대한 빨리 검색하여 신뢰도 시스템에 추가해야 합니다. 즉, 효율적인 신뢰도 시스템은 맬웨어를 정확하고 빠르게 찾아내는 "확인률"이 높은 시스템이라 할 수 있습니다.

장기적인 맬웨어 방지 비율



테스트 과정에서는 새 맬웨어가 계속 추가되었습니다. 더 이상 연결할 수 없거나 맬웨어를 호스트하지 않는 URL은 제거되었습니다. 특정 시점에 기록된 측정값에서 각 데이터 포인트가 계산되었습니다. 초기에 맬웨어가 차단된 경우 브라우저의 장기적인 맬웨어 방지 점수가 상향 조정되었습니다. 반면 맬웨어를 차단하지 못한 브라우저의 경우에는 해당 점수가 하향 조정되었습니다.

장기적 맬웨어 차단율



결과 요약

테스트 주기에 샘플이 추가된 시점부터 각 브라우저가 맬웨어를 차단할 때까지 걸린 시간이 위 그림에 나와 있습니다. Microsoft Edge 내의 핵심 맬웨어 방지 기술인 SmartScreen은 클라우드 기반 통합 URL 신뢰도 서비스를 통해 URL 기반 공격 방지 기능을 제공하는 동시에, 애플리케이션 신뢰도를 확인하여 악성 파일을 차단합니다. Google Chrome과 Mozilla Firefox는 Google 세이프 브라우징 API를 사용하여 URL 신뢰도를 확인하고 사용자에게 특정 파일 형식 다운로드 관련 경고를 표시하거나 해당 파일 형식을 차단합니다.

맬웨어 공격

SEM(소셜 엔지니어링 맬웨어) 공격에서는 사용자를 속여 맬웨어 다운로드를 유도합니다. 하이재킹된 이메일과 소셜 미디어 계정은 연락처 간의 암시적 신뢰 관계를 이용합니다. 그러면 피해자는 악성 파일 링크를 신뢰할 수 있는 링크로 오인하게 됩니다. 그리고 Adobe Flash Player와 같은 애플리케이션을 설치해야 한다는 알림, 사용자 컴퓨터가 감염되었거나 업데이트가 필요하다는 경고 등이 표시되는 팝업 메시지 등의 수법도 사용됩니다.

맬웨어가 설치되면 자격 증명 탈취, 신원 도용, 은행 계좌 손상 등의 피해를 입기 쉽습니다.

웹 브라우저의 맬웨어 방지 기능

클라우드 기반 신뢰도 시스템은 맬웨어 방지를 위해 인터넷에서 악성 웹 사이트를 찾아 해당 콘텐츠를 적절하게 분류합니다. 웹 브라우저는 클라우드 기반 신뢰도 시스템에 특정 URL, 파일 또는 애플리케이션의 신뢰도를 요청합니다. 요청 대상 항목에 맬웨어가 있는 것으로 확인되면 웹 브라우저는 해당 URL, 파일 또는 애플리케이션이 악성임을 설명하는 경고 메시지로 사용자를 리디렉션합니다. 추가 교육 콘텐츠를 제공하는 신뢰도 시스템도 있습니다.

Google Chrome과 Mozilla Firefox는 Google 세이프 브라우징 API를 사용하여 URL 및 애플리케이션 신뢰도를 확인해 악성 파일을 차단합니다. Microsoft Edge는 Microsoft Defender SmartScreen을 사용합니다. SmartScreen은 클라우드 기반 신뢰도 서비스를 통해 URL 신뢰도를 확인하여 공격을 방지하는 동시에, 애플리케이션 신뢰도를 확인하여 악성 파일을 차단합니다.

매일 추가된 평균 악성 맬웨어 샘플 수

이 테스트에서는 유효성이 검사된 신규 맬웨어 샘플 평균 49개가 매일 테스트 집합에 추가되었습니다. 범죄 활동 수준이 매일 바뀜에 따라 실제로 추가된 정확한 URL의 수는 매일 달랐습니다.

테스트 환경

- Microsoft Windows 10 Pro, 21H1

테스트에서 확인된 총 악성 샘플 수

각 웹 브라우저에서는 총 테스트 주기 78회 동안 유효성이 검사되지 않은 원시 샘플 18,621개를 반복 테스트했습니다. 20일(468시간) 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 맬웨어 테스트 48,672회에서 고유한 유효 맬웨어 샘플 950개를 테스트했습니다(웹 브라우저당 테스트 16,224회 실행). 테스트 오차 범위는 3.2% 미만, 신뢰도는 95%였습니다.

테스트 방법 - 맬웨어 샘플

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 맬웨어 및 클라우드의 신뢰도 서비스에 액세스할 수 있는지 확인했습니다.

그리고 각 브라우저가 새로운 맬웨어 공격을 차단할 수 있는지를 확인하기 위해 새 샘플이 테스트에 계속 추가되었으며 연결 불가 상태가 된 샘플은 제거되었습니다.

결과 평가 방식

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

테스트에서는 브라우저의 성능을 지속적으로 측정했으며, 브라우저에서 테스트한 모든 맬웨어 샘플의 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 맬웨어 샘플을 8회 테스트했다면 전체 테스트 실행 8회에서 해당 샘플을 6회 차단한 브라우저의 차단율은 75%입니다.

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

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

© 2021 CyberRatings.org. All rights reserved. 이 발행물의 어떤 부분도 CyberRatings.org("당사")의 명시적 서면 동의 없이 복제, 복사/스캔, 검색 시스템에 저장, 이메일로 전송하거나 기타 방식으로 배포 또는 전송할 수 없습니다.

1. 당사는 이 보고서의 정보를 통보 없이 변경할 수 있으며 해당 정보의 업데이트 의무를 부인합니다.
2. 이 보고서의 정보는 보고서 발행 시점에 당사가 정확하며 신뢰할 수 있다고 간주하는 내용입니다. 그러나 당사가 해당 정보의 정확성과 신뢰성을 보장하지는 않습니다. 이 보고서를 사용하고 해당 정보를 신뢰할 때 발생하는 위험은 전적으로 사용자의 책임입니다. 당사는 이 보고서 내 정보의 오류나 누락으로 인해 발생하는 모든 유형의 피해, 손실 또는 비용에 대해서도 책임을 지지 않습니다.
3. 당사는 명시적이거나 암시적인 어떠한 보증도 제공하지 않습니다. 당사는 상업성, 특정 목적 적합성, 비침해에 대한 암시적 보증을 비롯한 모든 암시적 보증을 부인 및 제외합니다. 당사는 해당 가능성을 통보 받은 경우를 비롯하여 어떠한 경우에도 직접적, 결과적, 부수적, 징벌적, 간접적 손해 또는 이익, 수익, 데이터, 컴퓨터 프로그램 또는 기타 자산의 손실에 대해 책임을 지지 않습니다.
4. 이 보고서는 테스트 대상 제품(하드웨어 또는 소프트웨어)이나 해당 제품을 테스트하는 데 사용된 하드웨어 및/또는 소프트웨어의 품질을 보증, 권장 또는 보장하지 않습니다. 테스트 결과는 제품에 오류 또는 결함이 없거나, 제품이 사용자의 기대치, 요구 사항, 요구 또는 사양을 충족하거나 중단 없이 작동함을 보장하지 않습니다.
5. 이 보고서는 보고서 내에 언급된 조직의 보증, 후원, 제휴, 확인을 받아 작성된 것이 아닙니다.
6. 이 보고서에 사용된 모든 상표, 서비스 표시 및 상호는 해당 소유자의 상표, 서비스 표시 및 상호입니다.