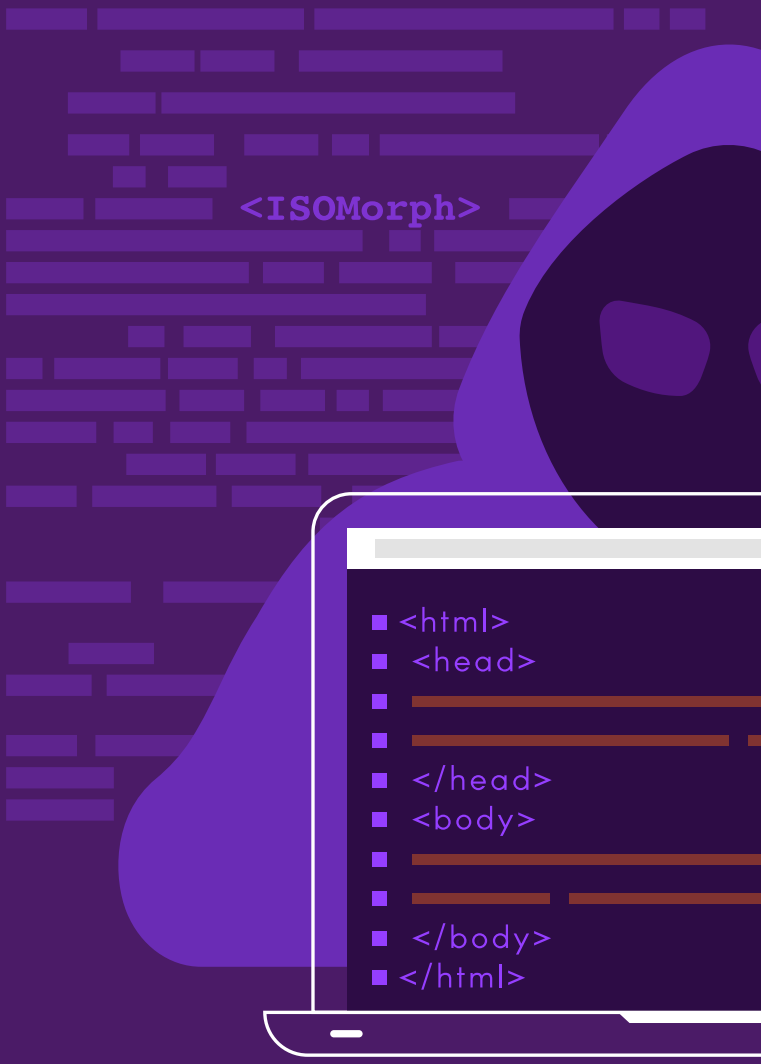
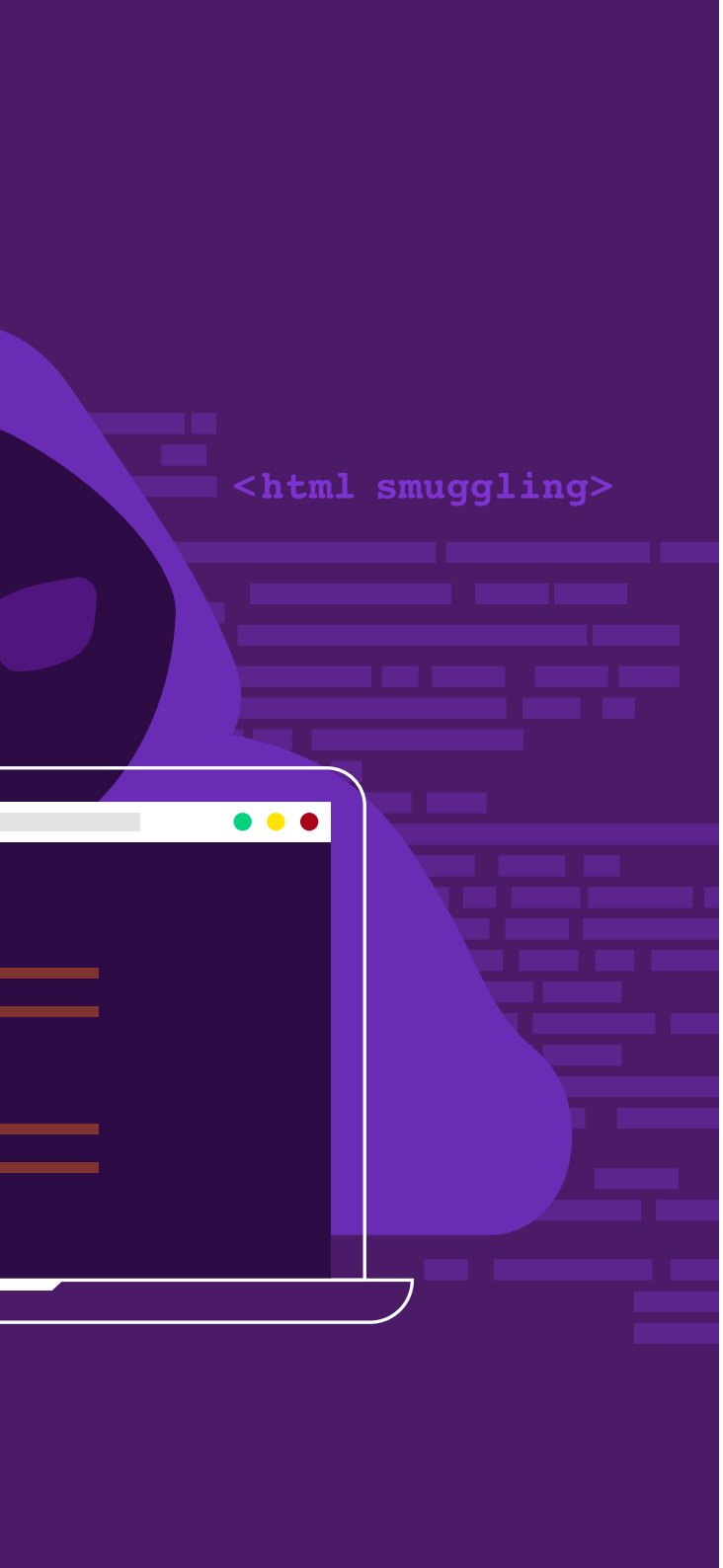
MENLO SECURITY

회피적인 보안 위협 방식 분석내용: 위협 행위자가 보안 스택을 통과하는 4가지 공격 방법

eBook

페이지
내용





재택 근무자를 노리는 HEAT **공격이 더욱 증폭된 방법**

지난 몇 년 동안 우리의 작업 방식은 크게 변화했지만 보안은 그렇지 않았습니다. 과거 보안 시스템은 사용자가 사무실 안에서 일할 때를 고려하여 구축되었지만, 오늘날의 하이브리드 업무 환경에서는 언제 어디서나 비즈니스 크리티컬한 클라우드 애플리케이션과 데이터에 대한 접근이 필요합니다. 많은 조직이 의존하는 전통적인 탐지 및 대응 접근 방식은 현대적인 업무 요구에 부응하지 못하고 있으며, 특히 랜섬웨어와 같은 공격에 대한 대처에 실패하면서, 지난 10년 동안 가장 크고 치명적인 침해의 원인이 되고 있습니다.

랜섬웨어와 같은 위협을 탐지하려면, 과거의 보안 도구는 네트워크 상의 모든 트래픽을 분석하고 악성코드인지 아닌지를 결정해야 합니다. 이러한 도구들은 대규모 트래픽으로 인해 비용이 많이 들며 시간이 많이 소요되며, 그 결과 옳지 않은 양성과 음성이 발생할 수 있습니다. 침해를 막으려면 보안이 항상 옳아야 하지만, 위협 주체는 한 번만 누락되면 됩니다. 위협이 감지될 때에는 이미 피해가 발생하여 시스템이 침해되었을 가능성이 높습니다.

공격자들은 이러한 사실을 잘 알고 있으며, 웹 브라우저를 공격 벡터로 활용하여 네트워크에 초기 접근 권한을 얻고 자격 증명을 훔치거나 악성 코드를 배포하여 종종 완전한 랜섬웨어 공격으로 끝납니다. 사이버 보안 업계에서 대부분 무명하고 방어되지 않은 이러한 고도 회피 적응형 위협(HEAT)은 전통적인 보안 도구의 결함을 이용하도록 구축되었으며, 그것이 바로 그들이 계속해서 수행하는 것입니다. HEAT 공격에 대응하려는 보안 시도는 따라잡기 어려운 과정을 거쳐야 할 것입니다. 사이버 보안이 고양이와 쥐 게임에서 적들의 손에 흐트러진 상황이 되고 있음을 알 수 있습니다.

이 전자책에서는, 우리는 공격자들이 어떻게 HEAT 특성 각각을 활용하여 전통적인 보안 도구를 우회하고 네트워크 상에서 감지되지 않고 자유롭게 움직이는지에 대해 자세히 살펴볼 것입니다.

HEAT 공격은 현재 사용되고 있는 다음과 같은 전통적인 보안 기능과 기술을 회피할 수 있습니다.

URL 필터링

이메일 보안 도구

파일 기반 검사

HTTP 콘텐츠/페이지 검사

공격방법 1 :
URL 필터링 회피

정의

직원들이 원하는 웹사이트로 자유롭게 이동할 수 있게 두면, 위협 요소들이 매일 만드는 악성 도메인의 수를 고려하면 재앙의 요인이 됩니다. 도메인의 연령, 평판, 인기 등을 기반으로 웹사이트를 신뢰할 수 있는 것으로 분류하거나 그렇지 않은 것으로 분류하는 것이 이 문제를 해결하는 전통적인 방식입니다. 하지만 위협 요소들은 이 방법에 대해 잘 알고 있기 때문에, 신뢰할 수 있는 웹사이트를 생성하거나 통제를 획득한 다음 악성 컨텐츠를 전달하는 방식으로 쉽게 이를 우회하고 있습니다.

공격 방식

위협 요소들은 URL 필터링 기술을 다음과 같은 기술로 회피하고 있습니다.

악성 웹사이트로 인한 손상

위협 요소들이 URL 필터링 기술을 회피하는 한 가지 방법은, 웹 분류 엔진에 의해 신뢰할 수 있는 것으로 분류된 이미 약한 보안을 가진 웹사이트를 침해하는 것입니다. 신뢰할 수 있는 사이트가 획득되면, 악성코드를 전파하거나 사용자의 로그인 자격 증명을 탈취하기만 하면 됩니다. 공격자들은 종종 악성 컨텐츠를 올리자마자 빠르게 제거하여 공격을 감지하기 어렵게 만듭니다.

CAPTCHA 뒤에 악성 콘텐츠 숨기기

API 봇을 대비하고 오직 사람만 해당 사이트에 접속하도록 보호하기 위해 많은 적법한 웹사이트들이 CAPTCHA를 사용합니다. 그러나 이것은 또한 웹 분류 크롤러가 CAPTCHA를 작성하지 못하므로, 공격자가 악성 콘텐츠를 감추기 위해 벽을 세우는 것과 같습니다. 사용자들은 CAPTCHA를 보면 해당 사이트가 안전하다고 생각할 수 있지만, 항상 그런 것은 아닙니다.

임시 악성 사이트 구축

신뢰할 수 있는 웹사이트를 통제하는 대신, 위협 요소들은 도메인을 직접 등록하고 그들의 신뢰도를 높이기 위해 노력합니다. 그들은 나중에 악성 캠페인에서 사용할 통제된 신뢰할 수 있는 사이트의 저장소를 구축할 수도 있습니다. 공격이 완료되면, 위협 요소들은 심지어 사이트를 원래의 신뢰할 수 있는 상태로 되돌리고 다른 공격에 사용할 수도 있습니다.

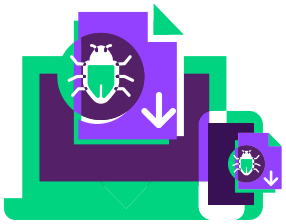
URL 필터링 기술을 회피하는 추가 HEAT 공격 기술

- 제로데이 브라우저 익스플로잇
- 역방향 터널 및 URL 단축기
- 공유 사이트에 호스팅된 악성/무기화된 파일
- 동적으로 생성된 자격 증명 수집 URL을 사용하여
- 도난된 자격 증명을 전송/게시합니다.

공격 과정

01. 위협 배우자가 신뢰할 수 있는 분류된 웹사이트를 장악하거나 스스로 웹사이트를 구축합니다.

02. 신뢰할 수 있는 사이트에 악성 코드가 설치됩니다. SEO는 종종 침해된 사이트의 페이지 순위를 높여 검색 엔진에서 사용자가 이러한 사이트를 쉽게 찾아서 탐색할 수 있습니다.



03. 피해자가 보통의 웹사이트를 방문하고 악성 코드를 다운로드하거나 로그인 정보를 훔쳐갑니다.

이를 피하는 기술 방식:

- 웹 분류
- 기술
- URL 평판 엔진

공격 방법 2:
이메일 보안 도구 회피

정의

만약 작업자가 악성 링크를 클릭하지 않으면 사기성 공격에 노출되지 않을 것입니다. 또한, 악성 링크가 접근하지 못하도록 막는다면 작업자는 해당 링크를 클릭할 수 없습니다. 이것이 안전한 이메일 게이트웨이 (SEG)와 같은 이메일 보안 도구가 활용하는 악성 링크 분석 기술의 논리입니다. 그러나 사기성 공격을 이메일 이외의 채널에서 작동하여 작업자를 대상으로 하는 경우 이러한 논리는 부적합합니다.

공격 방식

위협 행위자들은 다음을 통해 이메일 보안 도구를 피하고 있습니다.
해당 기술:

협업 플랫폼을 통해 가세되는 공격

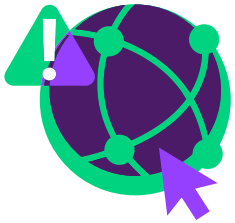
우리는 사기성 공격이 우리의 이메일에 들어올 것으로 예상하고, 보통 위치와는 달리 이메일 외의 텍스트 메시지, 소셜 미디어, Slack과 같은 협업 플랫폼을 통해 그것들을 받을 것으로 기대하지 않습니다. 따라서 우리는 이러한 연락처를 더 신뢰합니다. 이러한 암시적인 신뢰를 이용하여 공격자는 당신의 연락처 중 하나의 역할을 위장하거나 그 계정을 손상시키고, 이미 브라우저를 통과하여 악성 콘텐츠를 보내며, 악의적인 링크 분석의 범위를 벗어납니다.

악성 링크가 포함된 악성 Office 문서 및 PDF

SEG는 전자 메일 본문에 있는 링크만 분석합니다. 파일이나 PDF 안에 있는 링크를 찾지 않으므로, 파일 안에 링크가 숨겨져 있으면 발견할 수 없습니다. 사용자는 Office 문서와 PDF를 신뢰하고, 이러한 파일을 클릭하고 악성 코드를 무심코 다운로드할 가능성이 높습니다.

공격 과정

01. 공격자는 이메일 이외의 채널을 통해 신뢰할 수 있는 연락처를 위장하여 악성 콘텐츠를 보냅니다.



02. 사용자가 악성 링크를 클릭합니다.

03. 악성 콘텐츠가 엔드포인트에 다운로드됩니다.

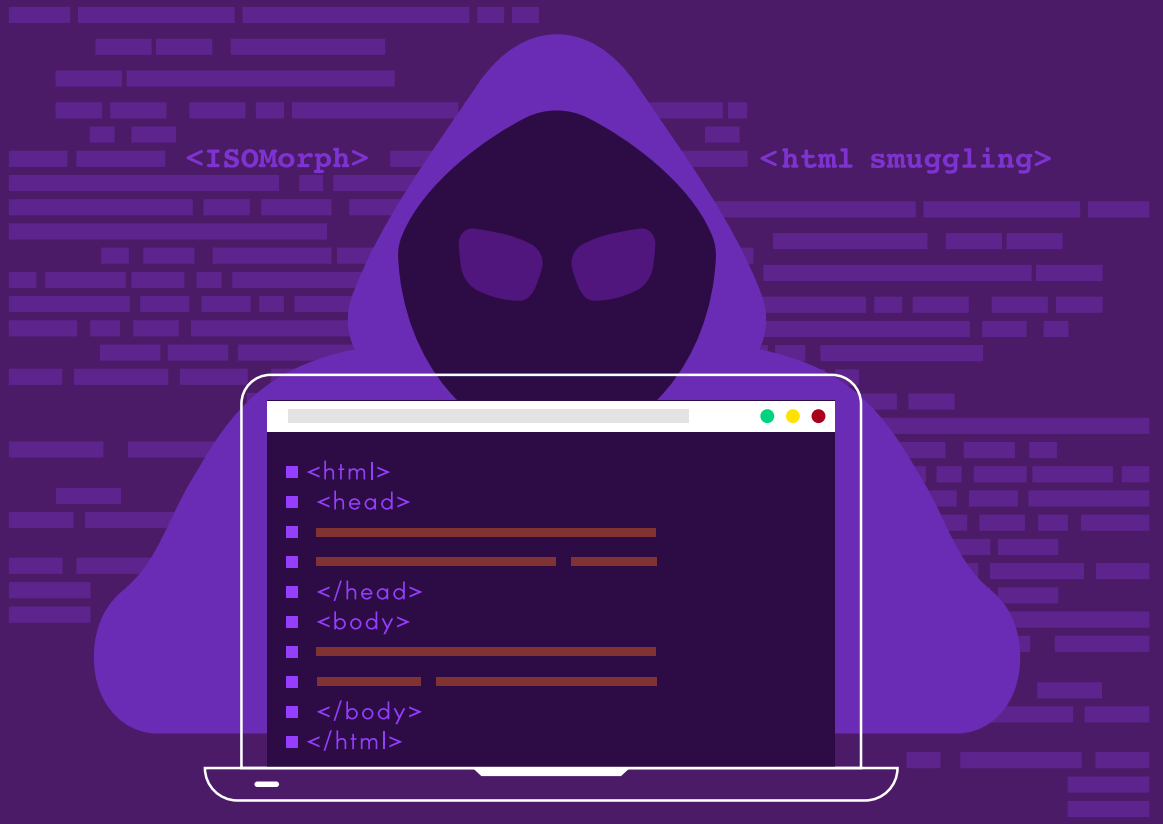
이를 피하는 기술 방식:

- 보안 이메일 게이트웨이(SEGs)
- 악성 이메일 링크 분석 엔진

공격 방법 3:
파일 기반 검사 회피

정의

위협 주체는 합법적인 웹 브라우저를 활용하여, 악성 콘텐츠를 분석할 수 없도록 설계된 공격을 실행하고 있다. 이들은 유산된 보안 기술이 모든 파일이 안전한지 완벽하게 보장하지 못한다는 것을 알고 있으며, 검사 엔진에서 제외된 파일의 예외 사항을 이용하고 있다.



공격 방식

다음 기술을 통해 파일 기반 검사 엔진을 우회하고 있다:

큰 사이즈 파일

완벽하게 안전한 샌드박스는 사용자에게 들어오는 모든 파일을 검사해야 한다. 생산성 관점에서 보면 끔찍한 전망이다. 따라서 샌드박스는 특정 크기 이상의 파일을 검사하지 않고, 거부되는 파일과 사용자에게 바로 전달되는 파일이 있다. 여기서 위협은 검사의 첫 번째 방어 계층을 우회하여 검사 없이 무시되고 들어올 수 있다.

암호로 보호된 아카이브

유사한 전술에서 악성 콘텐츠는 샌드박스와 같은 기존 보안 기술로는 검사할 수 없는 암호로 보호된 문서 뒤에 숨겨져 있습니다. PCI(결제 카드 정보) 데이터 및 개인 식별 정보와 같은 민감한 정보를 보호하기 위해 정보(PII), 샌드박스 검사 대상에서 제외됩니다. 불행하게도 공격자는 민감한 정보가 포함된 것으로 보이는 문서에 악성 콘텐츠를 숨김으로써 이 보안 조치를 쉽게 악용할 수 있습니다.

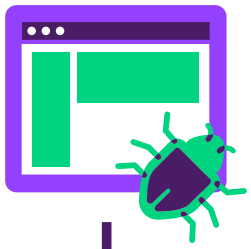
HTML smuggling

위협 주체는 HTML5 및 JavaScript와 같은 합법적인 웹 브라우저 기능을 활용하여 악성 콘텐츠를 HTML 코드 내에 직접 숨기고 있다. 악성 콘텐츠는 JavaScript BLOB(바이너리 큰 객체)에 숨겨지며, 사용자 디바이스에서 웹 페이지 내에서 동적으로 재조립된다. 악성 콘텐츠는 방화벽, 안티 바이러스(AV) 기술 또는 샌드박스를 이미 우회한 후에 엔드포인트에서 구축되어 이전에 어떤 검출 기술에서도 발견되지 않게 된다.

내용 검사를 회피하는 추가적인 HEAT 공격 기술

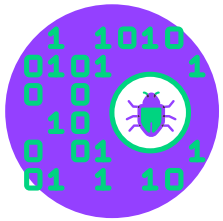
- MSI 설치 프로그램, 아카이브 등에 내장된 스크립트
- 파일 다운로드 이벤트로 이어지는 여러 리디렉션

공격 과정



01. 악성 파일이 브라우저에서 검사되지 않고 구성된다.

02. 악성 파일은 방화벽, 샌드박스 및 바이러스 백신 엔진과 같은 레거시 보안 기술을 우회합니다.



03. 일반적으로 보안 웹 게이트웨이(SWG)에 의해 차단되는 파일 유형은 사용자와의 상호작용 없이 여전히 엔드포인트를 손상시킵니다.

이를 피하는 기술 방식:

- 바이러스 백신 기술
- 샌드박스

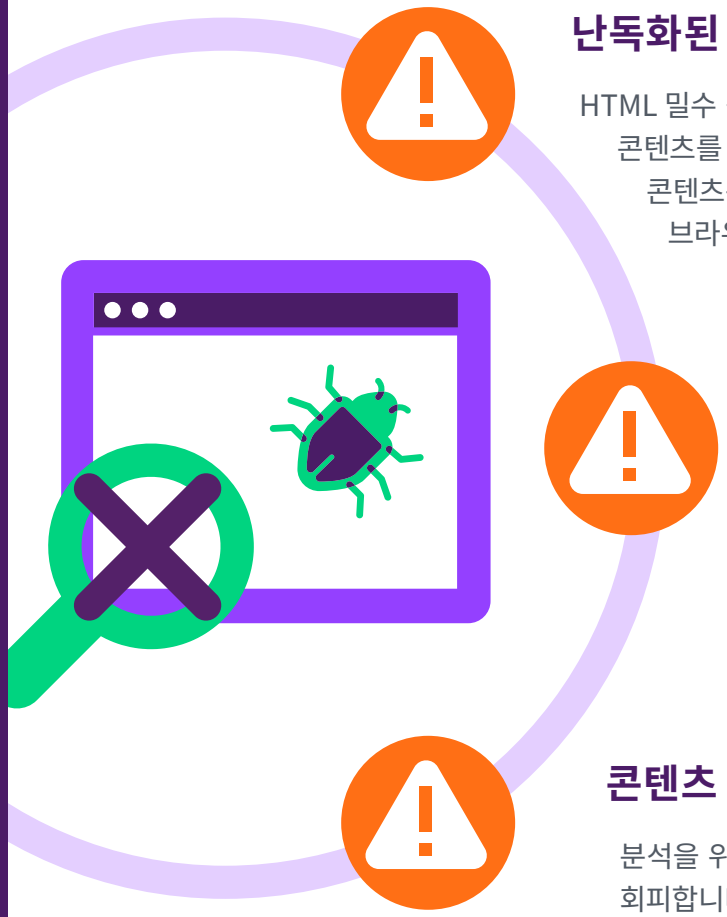
공격 방법 4:
HTTP 콘텐츠/페이지 검사 회피

정의

공격자가 웹 사이트에서 악성 콘텐츠를 숨기려고 시도하는 방법에 관계없이 궁극적으로 페이지의 소스 코드 어딘가에 존재해야 합니다. HTTP 콘텐츠 및 페이지 검사 엔진은 이 소스 코드 전체에서 악성 콘텐츠를 검색합니다. 하지만 물론 악성 콘텐츠를 스캔한다고 해서 모든 것을 발견할 수 있는 것은 아닙니다. 위협 행위자는 합법적인 웹 사이트가 민감한 코드를 난독화할 수 있도록 하는 기능을 활용하여 이 보안 기술을 우회하는 방법을 알아냈습니다.

공격 방식

위협 행위자는 다음 기술을 통해 HTTP 콘텐츠 및 페이지 검사 엔진을 우회하고 있습니다.



난독화된 악성 자바스크립트

HTML 밀수 공격이 작동하는 방식과 유사한 방식으로 위협 행위자는 JavaScript 코드에 악성 콘텐츠를 숨긴 다음 HTTP 트래픽 검사를 통과한 후 엔드포인트에서 자체적으로 재조립합니다. 악성 콘텐츠는 형식으로 존재하지 않기 때문에 탐지할 수 있는 악성 콘텐츠가 없습니다. 최종 사용자의 브라우저에서 생성될 때까지 손상을 입힐 수 있습니다.

동적으로 생성된 피싱 로고

공격자는 악성 피싱 로고를 난독화하기 위해 웹 페이지 소스 코드를 조작하고 있습니다. 종종 정교한 피싱 페이지로 시작하는 이러한 공격은 창의적인 CCS 속임수를 사용하여 겉보기에 무해해 보이는 이미지 아래 알려진 피싱 로고를 숨겨 시각적 감지를 피합니다. 피싱 로고는 끝에 나타납니다. HTTP 트래픽 검사 엔진에 의해 전혀 분석되지 않고 사용자의 장치.

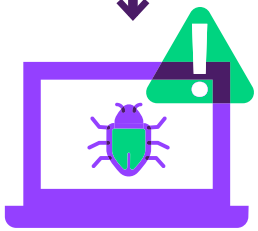
콘텐츠 검사를 회피하는 추가 HEAT 기술

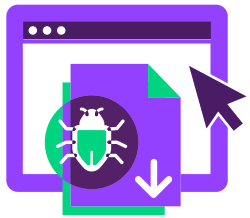
분석을 위한 페이지 리소스 추출을 더 어렵게 만드는 개별 기능을 인코딩하거나 활용하여 피싱 키트를 회피합니다.

공격 과정

01. 공격자는 JavaScript 또는 CCS를 통해 악성 콘텐츠를 난독화합니다.

02. 엔드포인트에 악성 콘텐츠가 재조립됩니다.





03. 피해자가 피싱 로고를 클릭하거나 악성코드를 다운로드한다.

이를 피하는 기술 방식:

- HTTP 콘텐츠 검사 기술
- 레거시 SWG

HEAT 공격 방어

기존의 보안 도구는 단순히 HEAT 공격을 막기 위해 만들어지지 않았습니다. 사이버 보안 예산이 증가함에도 불구하고 이러한 최신 위협에 직면하여 지속적으로 실패하는 것은 놀라운 일이 아닙니다. 탐지에 대한 의존도는 위협에 대한 시야를 그들이 위협하는 것으로 좁힙니다. 네트워크에서 탐지되었습니다. 이것은 공격자에게 명확한 청사진을 제공합니다: 초기 탐지를 피하고 당신이 있는 것입니다. 무료로 얻는 데 필요한 전부입니다. 네트워크를 지배하여 측면으로 이동하거나 데이터를 훔치거나 중요한 시스템을 손상시킵니다.

완전히 새로운 보안 패러다임이 필요하다는 것이 뼈아프게 분명해졌습니다. 그렇다면 HEAT 공격을 막는 가장 좋은 방법은 무엇일까요? HEAT 공격이 처음부터 발생하지 않도록 만드는 것입니다. 격리 기술은 보안에 대한 제로 트러스트 접근 방식을 활성화하여 이를 가능하게 합니다. 모든 웹 콘텐츠 — 악의적이든 아니든 — 나쁜 것으로 취급되며, 클라우드의 추상화된 계층에서 실행됩니다. 작업자가 방문하는 모든 웹 페이지, 클릭하는 링크, 다운로드하는 이메일 첨부 파일은 클라우드의 가상 브라우저에서 발생하므로 맬웨어 및 랜섬웨어와 같은 잠재적 위협이 엔드포인트 근처에 오지 않습니다. 사용자는 위생적이고 안전한 콘텐츠에만 노출되어 공격자가 네트워크에 처음 액세스할 수 있는 기회를 완전히 차단합니다. 위협이 침투할 수 없다면 위협이 아니기 때문입니다.in, it’s not a threat.

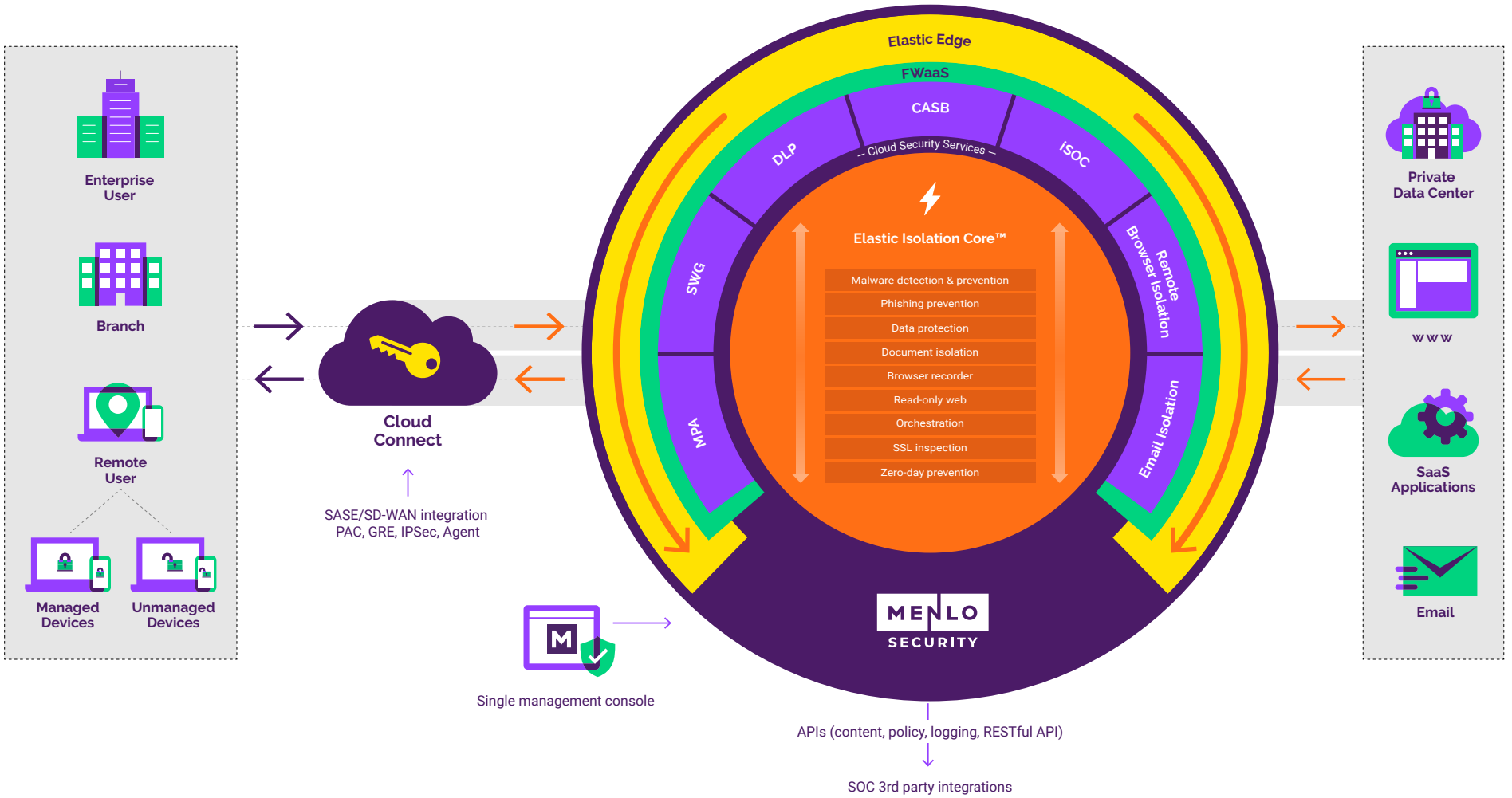
멘로 시큐리티에 대하여

Menlo Security는 웹, 문서 및 이메일에서 맬웨어의 위협을 제거하여 사이버 공격으로부터 조직을 보호합니다. 지식 근로자를 위한 가장 큰 단일 생산성 동인인 웹 브라우저를 보호하는 데 중점을 둡니다. Menlo의 Cloud Security Platform은 위협이 조직에 침투하는 것을 방지하고 단일 글로벌 클라우드 기반 오퍼링에서 데이터 및 애플리케이션 액세스를 보호합니다. 당사의 Elastic Isolation CoreTM는 보안, 정책 및 가시성이 적용되는 사용자, 콘텐츠 및 애플리케이션을 분리합니다. 위협을 감지하고 대응하는 것이 아니라 위협이 발생하기 전에 방지함으로써 조직은 웹, 이메일, SaaS 애플리케이션 및 개인 애플리케이션 전반에서 HEAT(Highly Evasive Adaptive Threats)를 포함한 모든 위협을 제거합니다.

HEAT 체크

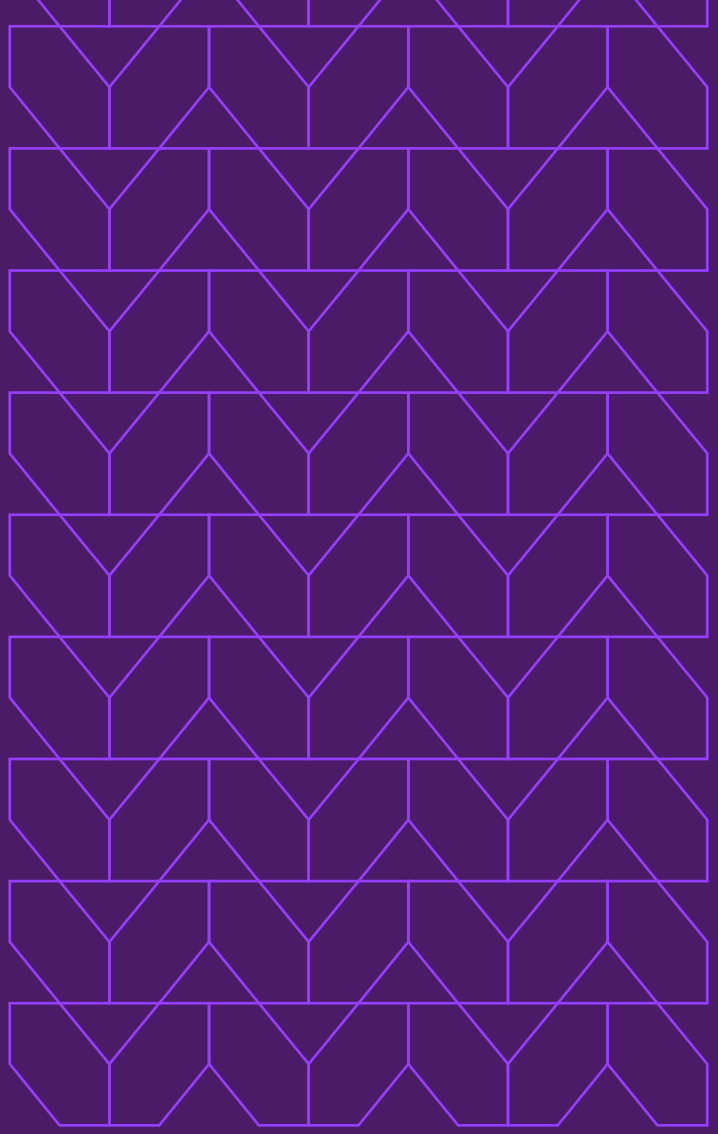
Menlo Security는 조직이 다양한 HEAT 공격에 대한 취약성을 더 잘 이해할 수 있도록 간단한 침투 평가를 제공합니다. 이 평가는 위협 행위자가 현재 사용하고 있는 다양한 실제 HEAT 공격을 활용하여 조직이 안전하게 노출을 추론할 수 있도록 합니다. Menlo의 HEAT 검사 도구는 실제 악성 콘텐츠를 전달합니다.

Menlo's Cloud Security Platform



궁금한 사항이 있으시면
.언제든 연락부탁드립니다

멘로시큐리티에 연락주시면 고객님의 조직이
현재 HEAT 공격에 취약한지를 확인하고 예방하여
처음부터 이러한 공격이 발생하지 않도록 하는 방법을
제안해드리겠습니다.



menlosecurity.com/heatcheck-korea

ask@menlosecurity.com

MENLO SECURITY