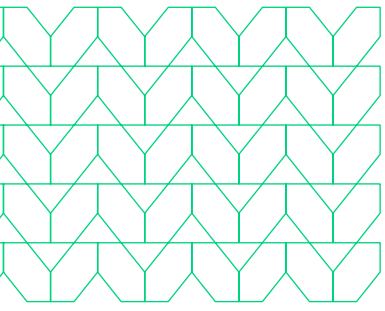
MENLO SECURITY

고도의 회피하는 위협이 발생함에 따라 기존 엔터프라이즈 보안은 위협에 노출 되고있습니다.

브라우저가 존재하는 한, 회피적인 위협은 악성 행위자들이 사용자의 시스템이나 조직의 네트워크에 초기 접근을 성공적으로 얻기 위해 성과를 향상시키기 위해 끊임없이 지속됩니다. 기업 보안 제어에 지속적인 발전이 있음에도 불구하고, 위협 행위자들은 회피적이고 새로운 기술을 사용하여 엔드포인트에 침투하고 피싱 및 랜섬웨어를 전달하는 데 노력합니다.

매년 지속적으로 사이버보안에 예산 투자를 해도 여전히 위협이 성공하여 사용자들이 공격에 영향을 받습니다. 만약 보안 솔루션이 100%의 피싱 위협을 제거할 수 있다면, 보안 인식 훈련은 오늘날 존재할 필요가 없을 것입니다.



브라우저를 기반으로 하는 업무의 증가로 인해 브라우저 기반의 공격과 기기 침해가 증가하고 있습니다. 실제로, 공격 중 50%는 브라우저 내에서 분류/신뢰되는 웹사이트에서 발생하는 회피적인 위협입니다.

웹 브라우저는 기업에서 가장 많이 배포된 응용 프로그램이지만, 가장 보안이 취약한 응용 프로그램이기도 합니다. 기업 사용자들은 웹, 기업 클라우드 및 SaaS 애플리케이션, 심지어 이메일에 접근하는 데 사용하는 여러 기기에서 여러 브라우저를 사용할 가능성이 높습니다. 이로 인해 브라우저는 피싱 및 악성 소프트웨어 공격을 시도하는 가장 인기 있는 대상 중 하나가 되었습니다. 불행하게도, 기존의 보안 제어 기술인 SWG, EDR, 방화벽은 이러한 공격을 막기에는 부족합니다. 위협 요소들이 높은 수준으로 이러한 보안 솔루션의 작동 원리를 이해하고 이를 회피하기 때문입니다. 따라서 기업들이 보안 스택에 투자를 늘리고 있음에도 불구하고, 사용자들은 예전보다 더 취약해진 상태입니다.

사용자들은 생산성, 효율성 및 협업에 중요한 역할을 하는 클라우드, SaaS 기반 애플리케이션 및 기타 웹 기반 도구에 접근하기 위해 근무 시간의 75%를 브라우저에서 사용합니다.

현재 기업 보안 스택에서 새로운 강력하고 효과적인 위협이 잠입할 수 있는 공백이 존재합니다. 고도로 회피적이고 적응적인 위협이라고 불리는 이들은 다이내믹한 행동, 파일리스 공격, 지연 실행과 같은 정교한 기술들을 사용하여 탐지를 피하고 기존의 보안 조치를 우회하는 사이버 보안 위협 유형입니다. 이러한 위협들은 방화벽, SWG 및 EDR의 블라인드 스팟을 공격하도록 설계되어 보안 전문가들이 식별하고 완화하기 특히 어렵습니다. 고도로 회피적이고 적응적인 위협은 특히 웹 브라우저를 공격 벡터로 사용하여 일반적으로 배치된 보안을 우회하는 다양한 기술을 활용합니다. 따라서 이러한 고도로 회피적이고 적응적인 위협은 악성 코드를 전달하고 사용자 시스템을 침해하며 민감한 데이터를 도용하는 데 사용됩니다.

고도로 회피적인 위협은 규모와 정교성 모든 부분에서 발달

지금까지 사이버 범죄자들은 웹 브라우저를 주요한 타깃으로 별로 중요하게 여기지 않았습니다. 그들은 주로 PC, 데스크톱 및 운영 체제의 취약점을 악용하는 데 초점을 맞추었습니다. 현재 사용되고 있는 보안 방법은 방화벽, 안전한 웹 게이트웨이, 샌드박스 분석, URL 평판 및 피싱 탐지 솔루션을 포함하여 기존의 공격 벡터에 집중한 것을 보여줍니다.

그러나 기존 보안의 개념은 특히 점점 확장되는 공격 표면과 주요 기업 애플리케이션으로서의 웹 브라우저 채택에 있어서는 한계가 있습니다. 기업에서 가장 널리 사용되는 응용 프로그램인 웹 브라우저는 네트워크 및 엔드포인트 보안으로부터 충분한 보호를 받지 못하고 더욱 뚜렷한 보안 간극이 발생합니다.

이러한 상황은 IT 및 보안 팀이 기존의 악성 코드 서명만 식별하고 웹 브라우저를 특정 대상으로 하는 회피적인 위협을 효과적으로 차단하지 못하는 감지 기반 접근 방식에 의존해야 하는 것을 강요하고 있습니다. 결과적으로 웹 브라우저 내부의 위협으로부터의 가시성, 통제 및 보호의 필요성이 명확해지고 있습니다. 기업이 완전히 웹 브라우저 보안을 채택하기 전까지, 위협 주체들은 최근의 공격에서 확인된 대로 매우 회피적이고 적응력 있는 위협을 사용하여 기업 네트워크에 침투하게 될 것입니다.

Highly Evasive Threat 예시 1

옥타 해커들이 성공적인 다중 인증(MFA) 우회 기술로 130개 이상의 조직을 공격했습니다.

최근 Twilio와 Cloudflare를 공격한 위협 주체는 136개 기관을 대상으로 한 대규모 피싱 캠페인과 연관되어 있으며, 이로 인해 9,931개의 계정이 MFA 우회를 통해 침해되었습니다. 이러한 공격은 주로 미국, 인도, 캐나다, 프랑스, 스웨덴 및 오스트레일리아에 기반을 둔 대상 기관의 직원들로부터 Okta 신원 자격 증명과 이중 인증(2FA) 코드를 획득하기 위해 시행되었습니다. 사용된 피싱 킷은 이전에 기록된 적이 없는 것으로 나타났습니다. 이러한 캠페인의 동기는 아직 불분명하지만, 정찰 및 금전적 이익을 목적으로 하며, 위협 주체에게 기밀 데이터, 지적 재산, 기업 이메일, 자금에 접근 권한을 부여합니다.

Highly Evasive Threat 예시 2

러시아 국가 지정 위협 요소들은 우크라이나 지원을 명분으로 국가의 외교기관들을 침투하고 있습니다.

러시아 정보기관인 특히 해커 그룹 obeliumAT29 은 유럽 연합과 아프리카를 대상으로 한 외교부 및 ATO 회원국의 외교관 등을 겨냥한 새로운 스파이 캠페인에 관여하고 있습니다. 이 캠페인은 러시아와 관련된 것으로 여겨지는 캐나다 인프라에 대한 공격과 함께 발생하였습니다.

Nobelium/APT29은 이번 공격을 솔라윈즈 공급망 공격으로 잘 알려진 그룹으로, 정교하게 작성된 스피어 피싱 이메일로 공격을 시작하며, 악성 페이로드를 전달하기 위해 HTML 스머글링이라는 매우 회피적인 기술을 사용하여 탐지를 회피합니다. 아직까지는 심각한 피해는 보고되지 않았지만, 캐나다 당국은 중요한 시스템을 보호하고 완화 조치를 적용하는 중요성을 강조하고 있습니다.

악성 코드의 42%는 압축 파일로 전달됩니다. 압축 파일은 이제 주변 보안 제어를 우회하는 공격자들에 의해 악성 코드를 전달하는 가장 일반적인 파일 유형입니다.

Highly Evasive Threat 예시 3

악성 소프트웨어 캠페인이 의료 기관들을 대상으로 하여 데이터 수집과 원격 제어를 목적으로 합니다.

금융 및 의료 부문을 대상으로 한 공격적인 위협 행위자가 매우 은폐적인 악성 코드 변형과 검색 엔진 결과 조작을 위해 흔히 알려진 URL 회피 기술인 Legacy URL Reputation Evasion (LURE)을 사용하여 전통적인 보안 조치를 우회하고 있습니다.

이 공격적인 캠페인은 다층적으로 은폐 기법, 특권 상승 및 데이터 수집을 포함하고 있습니다. 성공적인 감염은 위협 행위자가 희생자의 장치를 원격으로 제어하고 민감한 정보를 수집하며 원격 제어를 유지할 수 있게 합니다. 공격의 심각성과 지속적인 특성으로 인해 특히 의료 부문의 조직들은 높은 경계를 유지하고 시스템을 보호하기 위한 적절한 조치를 취하는 것이 권고됩니다.

Highly Evasive Threat 예시 4

미디어 거대기업을 대상으로 데이터 유출 및 계정 침해를 위해 구글의 오픈소스 GC2 도구를 사용합니다.

중국의 국가 위협 그룹은 Barium은 Google의 오픈 소스 Command and Control (GC2) 도구와 LURE 회피 기술을 이용하여 대만의 언론 기업을 대상으로 했습니다. 이 공격 캠페인은 중요한 두 가지 트렌드를 강조합니다: 중국의 위협 그룹들이 GC2와 같은 공개적으로 사용 가능한 도구를 점 increasingly 이용하고, 공격자들이 검출을 피하기 위해 신뢰받는 클라우드 서비스를 사용하고 있다는 것입니다. 검증된 클라우드 서비스와의 연결은 경보를 울리지 않습니다.

Google은 클라우드 서비스가 사이버 범죄자와 국가 지원 공격자에게 수익성 있는 목표가 되고 있으며, 악성 소프트웨어를 호스팅하는 데 또는 명령 및 제어 (C2) 작업의 인프라로 사용됩니다. 여러 가지 악성 소프트웨어가 피싱 캠페인에서 ZIP 아카이브 파일로서 Google Drive에 저장되어 있습니다. 클라우드서비스를 공격 벡터로 계속 사용함으로써 계정을 신원 정보 탈취로부터 보호하기 위해 견고한 보안 조치가 필요함을 강조합니다.

Highly Evasive Threat 예시 5

새로운 Phishing-as-a-Service 키트가 Microsoft O365 피싱 공격을 간편하게 만들어줍니다.

Greatness hishing-as-a-Service (haaS) 플랫폼은 미국, 캐나다, 영국, 호주 및 남아프리카 공화국에서 Microsoft 365을 사용하는 기관을 대상으로 한 활동의 증가를 경험했습니다. 이 플랫폼은 사이버 범죄자들에게 성공적인 피싱 캠페인을 수행하기 위해 필요한 모든 도구를 제공하며, Microsoft O365 페이지를 성공적으로 모방하고 사용자 자격 증명 및 세션 쿠키를 도용하기 위해 필요한 인프라와 난독화된 JavaScript와 이미지를 포함합니다.

공격자가 세션 쿠키를 획득하면 희생자의 이메일, 파일 및 Microsoft 365 서비스의 데이터에 접근할 수 있습니다. 도용된 자격 증명은 종종 기업 네트워크 침투에 사용되어 랜섬웨어 배포와 같은 더 위험한 공격으로 이어질 수 있습니다.

매 분마다 유명한 브랜드를 사칭하는 새로운 피싱 사이트가 출시됩니다.

기업은 고도로 회피적인 브라우저 기반 위협으로부터 보호할 수 있나요?

고도로 회피적인 위협을 막기 위해 새로운 유형의 솔루션이 필요합니다.
이러한 공격 기법을 격리하고 처음부터 실행을 방지할 수 있는 솔루션이 필요합니다.

기존의 온프레미스 및 클라우드 기반의 네트워크 보안은 악성 위협의 악성 패턴을 의존하거나 네트워크 기반 텔레메트리에서 훈련된 AI를 사용하여 알려지지 않은 피싱 위협이나 회피 기법을 감지하지 못할 수 있습니다. Browser Security와 같은 예방 솔루션은 모든 웹 트래픽에 대한 완전한 가시성을 제공하고 동적 정책 적용을 가능하게 하여 고도로 회피적인 위협이 사용자를 타겟으로 하는 것을 식별하고 막을 수 있습니다.

위협 행위자들이 사용하는 고도로 회피적인 위협으로의 전환을 고려하여, Menlo Security는 브라우저를 대상으로 하는 고도로 회피적인 위협을 감지하고 차단하기 위한 예방 기능들을 도입했습니다. HEAT Visibility는 클라우드 기반 격리 기술을 활용하여 모든 브라우저 세션에 대한 완전한 가시성을 제공하며, 이를 통해 다른 솔루션에서는 보이지 않는 고도로 회피적인 브라우저 기반 위협과 관련된 맥락 풍부하고 실질적인 인텔리전스를 제공하여 사고 대응 속도를 가속화합니다.

컴퓨터 비전, URL 위험 점수 평가 및 웹 페이지 요소 분석과 같은 다양한 AI 기반 기술을 사용하여 Menlo Security의 HEAT Shield는 링크가 사용자 자격 증명을 도용하려는 피싱 사이트인지를 실시간으로 정확하게 판단할 수 있습니다. HEAT Shield는 브라우저를 대상으로 하는 고도로 회피적인 위협과 제로 아워 피싱 공격에 대한 실시간 보호를 제공하여 조직이 필요한 정보를 얻고, 동시에 엔드 유저들에게 원활한 브라우징 환경을 제공합니다.

멘로시큐리티

Menlo Security는 독자적인 격리 기반의 클라우드 보안 플랫폼으로 조직들이 위협을 능가하고 완전히 공격을 차단하며 생산성을 완벽하게 보호할 수 있도록 지원합니다. 이는 클라우드 보안의 약속을 이행하기 위한 유일한 솔루션으로서, 악성 공격을 예방하기 위해 가장 안전한 제로 트러스트 접근 방식을 제공하고, 엔드 유저들이 온라인 작업을 할 때 보안을 눈에 띄지 않게 만들며, 보안 팀에게 운영적 부담을 줄여줍니다. 이제 조직은 안전한 온라인 환경을 제공하여 사용자들이 걱정 없이 작업하고 비즈니스를 전진시킬 수 있습니다.

MENLO SECURITY

자세한 내용을 알아보려면 저희에게 연락주세요:

www. menlosecurity.com/ko-kr/

korea@menlosecurity.com

Menlo Security

Menlo Security는 기업들의 보안 위협을 미리 예측하여 대처하고, 공격을 차단하며, 생산성을 완전히 보호할 수 있도록 하는 독창적인 클라우드 보안 플랫폼을 제공합니다. Menlo Security는 클라우드 보안의 약속을 지키는 유일한 솔루션으로 악성 공격을 방지하는 가장 안전한 Zero Trust 접근 방식을 제공하며, 사용자들이 온라인에서 작업하는 동안 보안을 무시하게 하여 보다 안전한 온라인 경험을 제공하며, 보안 팀에 대한 운영 부담을 줄여줍니다. 이제 기업들은 안전한 온라인 환경을 제공하며 사용자들이 걱정 없이 일할 수 있도록 도와주며, 비즈니스를 원활하게 진행할 수 있습니다.