Enterprise Strategy Group | Getting to the bigger truth.™

ESG 백서

HEAT(Highly Evasive Adaptive Threat) 공격 증가가 미치는 위협 환경 변화

작성자: John Grady(ESG 시니어 애널리스트)

2022 년 1 월

목차

개요

지난 10 년 간 업무 환경과 기업 환경의 특성이 크게 달라진 반면 사이버보안 실태, 도구 및 전략은 거의 변하지 않고 있습니다. 유감스럽게도 공격자들은 방어 체계를 무력화하기 위해 적극적으로 노력하는 동시에 계속해서 진화하고 있습니다. 공격자들은 전통적인 사이버보안 방식을 그 한계까지 정확하게 이해하고 있으며 공격을 성공할 수 있는 명확한 청사진을 다른 해커들에게 제공하고 있습니다.

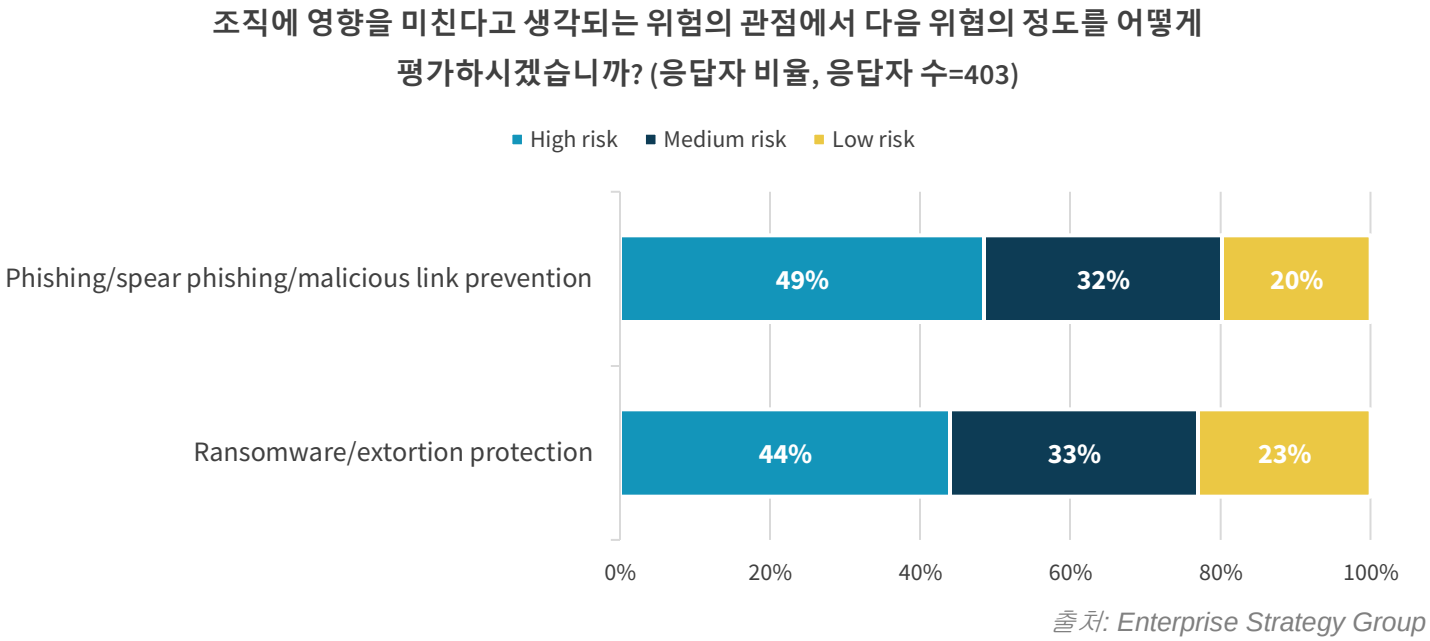
Menlo Security 는 공격자들이 랜섬웨어 및 피싱 공격을 성공적으로 실행하기 위해 사용하는 다양한 기술을 연구했으며 그 결과물로 "HEAT(highly evasive adaptive threats)"라는 용어를 규정했습니다. HEAT 공격은 기존 보안 스택에 통합된 모든 기술을 파악하고 감지를 회피할 수 있는 전달 메커니즘을 빌드함으로써 기존 보안 방어 체계를 무력화합니다. HEAT 공격에 대처하려면 조직은 침해 후 감지 사고 방식에서 위협이 단말에 도달하기 전에 위협을 차단하는 데 집중하는 예방적 사고 방식으로 전환해야 합니다.

HEAT(highly evasive adaptive threat) 공격은 기존 보안 스택에 통합된 모든 기술을 파악하고 감지를 회피할 수 있는 전달 메커니즘을 빌드함으로써 기존 보안 방어 체계를 무력화합니다.

보안 위협 환경의 지속적인 진화

지난 수년 간 사이버보안은 많은 조직에 있어 IT 중심 이슈에서 비즈니스 우선 요소로 발전했습니다. 클라우드 채택이나 디지털 변환과 같은 보다 광범위한 이니셔티브 지원에 있어 사이버보안 역할이 이러한 변화에 어느 정도 일조했지만 위협 환경의 진화와 공격 성공에 따른 부정적인 비즈니스 영향도 큰 역할을 했습니다. 사이버 공격이 잠재적으로 중대한 비즈니스 중단을 일으킬 수 있는 상황에서 심각한 결과를 초래할 수 있는 랜섬웨어, 사이버 강탈(extortion) 및 피싱 공격이 많은 조직의 우선 과제로 부상했습니다. ESG 연구 결과에 따르면 실제로 설문 응답자 조직의 약 50%에서 피싱과 랜섬웨어 공격을 조직의 큰 위험으로 인식하고 있습니다 (그림 1 참조).[1]

그림 1. 피싱 및 랜섬웨어 공격 위험에 대한 인식



출처: Enterprise Strategy Group

[1] 출처: ESG Research Report, *Trends in Email Security*, August 2020.

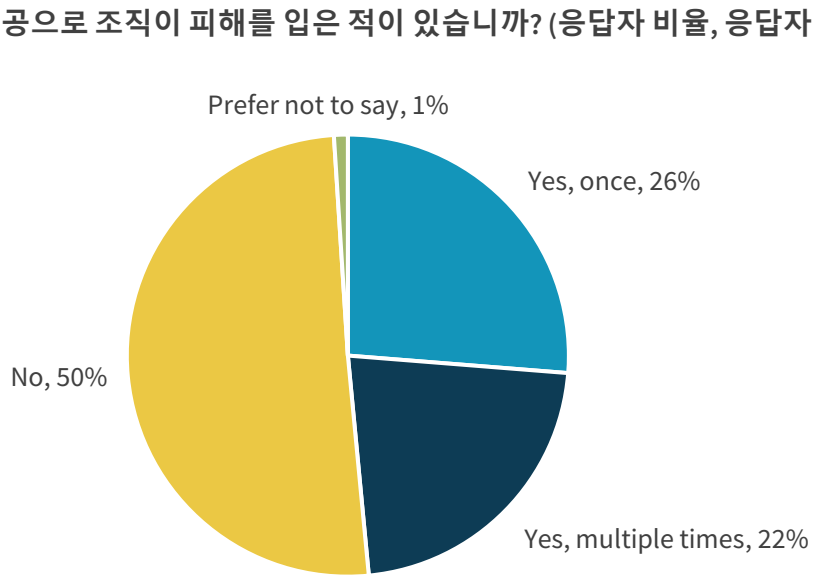
정확하게 말하면 설문 응답자의 22%에서 랜섬웨어 대응이 가장 중요한 비즈니스 우선 과제라고 생각하고 있으며 46%는 5 대 비즈니스 우선 과제 중 하나로 인식하고 있습니다.[2] 잘 알려진 중요 인프라(예: Colonial Pipeline) 및 IT 공급자(예: Acer, Kaseya) 공격 사례는 대중과 기업 경영진에게 이 문제의 중요성을 일깨우는 데 일조했습니다.

설문 응답자의 22%에서 랜섬웨어 대응이 가장 중요한 비즈니스 우선 과제라고 생각하고 있으며 46%는 5 대 비즈니스 우선 과제 중 하나로 인식하고 있습니다.

그러나 몇몇 세계적인 대기업을 대상으로 하는 이러한 유명 사건에만 집중한다면 유형, 규모 및 보안 성숙도에 관계없이 모든 조직이 이러한 문제에 지속적으로 노출될 수 있다는 사실을 간과할 수 있습니다. 특히 ESG 연구에서는 설문 응답자의 36%에서 매일, 매주 또는 매월 랜섬웨어 공격 시도를 경험했으며 이외 27%에서는 지난 12 개월 동안 간헐적으로 랜섬웨어 공격을 받은 것으로 밝혀졌습니다.[3]

유감스럽게도 이러한 공격이 자주 성공합니다. ESG 설문 응답자 중 1/4 이 넘는 26%에서 랜섬웨어 공격 한 번으로 피해를 입었으며 여러 번 공격당한 경우도 22%에 달했습니다(그림 2 참조).[4] 보안 팀은 이러한 문제를 잘 알고 있으며 보안 벤더는 이러한 공격을 방어하기 위해 관련 제품을 업데이트하고 있습니다. 그러나 랜섬웨어를 비롯하여 기타 금전적 목적을 가진 공격의 영향을 조직이 많은 상황에서 "공격자가 어떻게 방어 체계를 계속 우회할 수 있는가?"라는 의문을 갖게 됩니다.

그림 2. 랜섬웨어 공격 성공



출처: Enterprise Strategy Group

[2] 출처: ESG Complete Survey Results, 2022 Technology Spending Intentions Survey, November 2021.
[3] Ibid.
[4] Ibid.

HEAT 정의

Menlo Security 는 최근 공격자들이 전통적인 보안 도구를 통한 감지를 회피하기 위해 점점 더 많이 사용하고 있는 일련의 기술을 발견했습니다. Menlo Security 는 이러한 공격을 "HEAT(Highly Evasive Adaptive Threat)"라고 정의했습니다. 이 용어는 랜섬웨어를 포함하여 사용자, 단말 또는 애플리케이션을 표적으로 삼는 모든 유형의 공격에 사용될 수 있습니다(그림 2 참조). 특히 이러한 공격은 다음 4 가지 주요 특징 중 하나 이상을 갖고 있습니다.

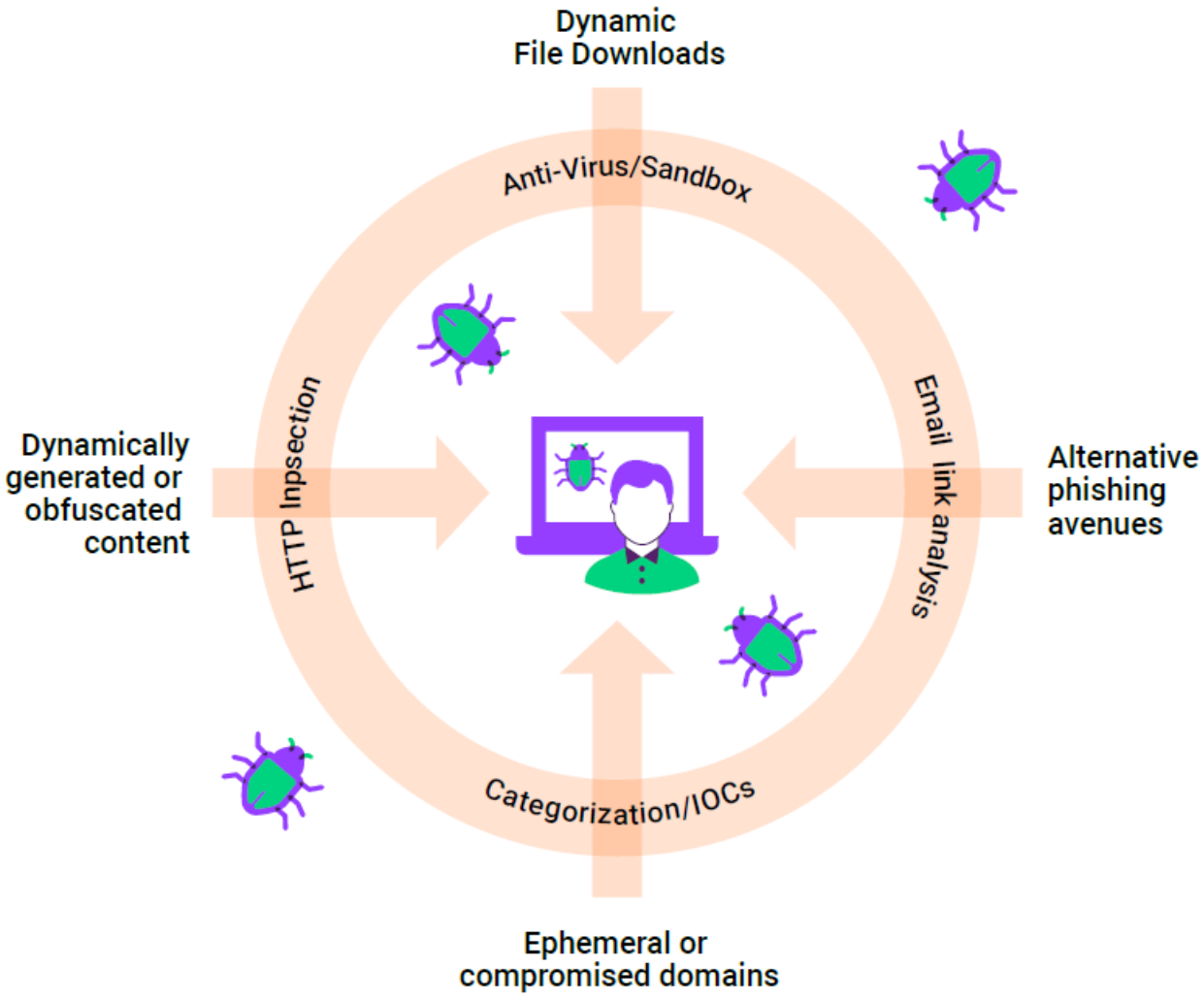
1. **동적 파일 다운로드.** HEAT 공격은 HTML 스머글링(smuggling)을 사용하여 서명 및 코드 분석 기반 감지 방법을 모두 우회합니다. 이 기술은 적법한 HTML5 및 JavaScript 기능을 사용하여 단말로 은밀하게 다운로드를 실행합니다. 공격자는 암호화된 JavaScript blob 을 만들며 사용자가 감염된 링크를 클릭하면 브라우저에서 스크립트를 디코딩하고 디바이스에서 악성 페이로드를 어셈블합니다. 멀웨어가 장치에서 구성되므로 전통적인 검사 메커니즘을 통해 파일이 전달되지 않습니다. JavaScript 를 사용하지 않으면 공격을 완화시킬 수 있지만 합법적인 웹 페이지에 미치는 영향으로 인해 일반적으로 수행할 수 있는 방법이 아닙니다. 이러한 전술이 새로운 것은 아니지만 점점 많이 사용되고 있습니다. SolarWinds 침해 사건을 비롯하여 잘 알려진 여러 공격의 주범인 Nobelium 에서 이 기술을 사용하고 있으며 Menlo Labs 는 HTML 스머글링을 잘 활용하는 Duri 및 ISOMorph 캠페인을 모니터링하고 있습니다.

2. **새로운 피싱 대안.** 피싱 공격은 전통적으로 이메일 벡터에 집중되고 있습니다. 그러나 사용자가 교육을 통해 의심스러운 이메일에 주의를 기울이게 되면서 또한 이메일 보안 도구의 피싱 링크 감지 기능이 향상되면서 HEAT 공격 대상이 다른 채널로 이동했습니다. 최근에는 LinkedIn 및 기타 소셜 미디어 사이트에 대한 스피어 피싱 공격이 피싱 방지 도구를 회피하기 위한 전술로 널리 사용되고 있습니다. 공격자는 연결 초대장, 콘텐츠 게시물 또는 구인 광고를 사용하여 직접적으로 또는 악성 URL 을 통해 멀웨어 페이로드를 전달합니다. 마찬가지로 SMS 메시지도 공격자들이 의심 하지 않는 수신자에게 악성 링크를 보내는 데 많이 사용되고 있습니다. 채널에 관계없이 결과는 동일합니다. 즉 보안 팀에서 문제를 인지하기도 전에 자격 증명이나 다른 민감한 정보가 도용됩니다.

3. **사용 후 삭제되거나 손상된 도메인 사용.** 새로운 기술은 아니지만 공격자가 악성 사이트를 손쉽게 스핀업(spin up)할 수 있으면 HEAT 공격이 그 어느 때보다 분류 엔진을 쉽게 우회할 수 있습니다. 오프라인 웹 크롤러가 악의적인 행동을 관찰하기 전에 공격자가 사이트를 폐쇄하고 다른 위치에 만들 수 있습니다. 공격자는 사용 후 삭제된 사이트와 도메인을 사용할 뿐만 아니라 단일 사이트나 여러 사이트를 빌드하고 악의적인 활동에 사용하기 전에 며칠, 몇 주, 심지어 몇 개월 동안 끈기 있게 기다리는 방식을 사용할 수 있습니다. 두 가지 경우 모두 CAPTCHA 를 사용하여 해당 사이트가 피해자에게 더욱 합법적인 사이트로 보이게 하거나 오프라인 웹 크롤러를 회피하거나 악의적인 콘텐츠 자체를 전달할 수 있습니다. 마지막으로 공격자들은 방어 능력이 낮은 합법적인 사이트를 계속 손상시켜 멀웨어를 전달하는 데 사용하므로 분류 기반 방어 체계의 효과가 훨씬 더 낮아집니다.

4. **동적 생성되거나 숨어 있는 콘텐츠 사용.** 또한 HEAT 공격은 JavaScript 의 Eval() 함수 사용 등 브라우저에서 익스플로잇 코드를 생성하여 웹 페이지의 소스 코드를 검사하는 서명을 통한 감지를 회피할 수 있습니다. 또한 공격자는 JavaScript 를 난독 처리하여 보안 연구원과 감지 엔진 모두에서 읽을 수 없게 만들 수 있습니다. 마지막으로 공격자는 JavaScript 를 통한 웹사이트 코드 조작 방식을 사용하여 피싱 공격을 가장 많이 받는 브랜드의 실제 로고(예: Office365)를 가져와 육안 탐지 기반 엔진을 우회합니다.

그림 3. HEAT



출처: Menlo Security

보안 팀에서 HEAT 공격을 주시해야 하는 이유

대부분의 IT 전문가가 사이버 보안이 점점 더 어렵고 복잡해지고 있음에 동의합니다. ESG 연구 결과에 따르면 응답자의 64%에서 에지에서의 네트워크 보안이 2 년 전에 비해 더 어려워졌다고 말했습니다. 이러한 복잡성의 주된 원인은 바로 보안 위협 환경 진화로, 응답자의 41%에서 에지에서의 네트워크 보안을 더욱 어렵게 만드는 요인 중 하나라고 언급했습니다.[5] 이러한 상황으로 보아 특히 HEAT 공격에 특별히 주의해야 하는 이유는 무엇일까요?

가장 큰 이유는 HEAT 기법을 사용하는 공격과 공격자의 유형입니다. Microsoft 는 2021 년 5 월 Nobelium 그룹이 정교한 스피어 피싱 캠페인에 HTML 스머글링을 사용한 사실을 발견했습니다.[6] 마찬가지로, 랜섬웨어를 적극적으로 사용하고 있는 Trickbot 역시 HEAT 기법을 사용해 공격의 초기 페이로드를 전달했습니다. 이러한 두 위협 공격자의 접근만으로도 규모와 유형에 관계없이 모든 조직이 영향을 받을 수 있으며 이러한 전술이 현장에서 확인되었다는 사실은 HEAT 공격이 이미 전면적으로 확산되고 있음을 의미합니다.

[5] 출처: ESG Survey Results, *Transitioning Network Security Controls to the Cloud*, July 2020.
[6] 출처: Microsoft Threat Intelligence Center (MSTIC), *New sophisticated email-based attack from Nobelium*, May 2021.

이러한 공격 환경 증가의 직접적인 원인은 전통적인 도구와 전략이 효과를 발휘하지 못한다는 사실입니다. 멀웨어 감지 기술이 샌드박싱과 분석에 더 의존하는 서명 기반 방식에서 진화된 것은 사실이지만 개선 작업은 점진적으로만 진행되었습니다. 이러한 방법은 여전히 악성 코드 식별에 의존하므로 결과적으로 공격자에게 방어 체계를 회피할 수 있는 기회를 제공합니다.

네트워크 중심 또는 단말 중심 여부에 관계없이 전통적인 보안 모델에서는 궁극적으로 어딘가에 최초 피해자가 나타나야만 서명이나 분석 엔진을 그에 따라 업데이트합니다.

예를 들어 샌드박스는 잘 알려지지 않은 파일 형식이나 특정 크기의 파일을 처리하지 못할 수 있습니다. 또한 샌드박스에서 멀웨어를 인식할 수 있으므로 조직은 전달 후 분석 방식을 사용할지 또는 사용자 생산성이 잠재적인 영향을 받더라도 파일을 보류할지 여부를 결정해야 합니다. 단말 제품의 경우 장치 자체에 상주하는 데 따른 이점이 있는 것처럼 보일 수 있지만 이러한 도구는 관리되지 않는 장치에 배포되기가 어렵고 공격의 첫 번째 단계에서 해커에 의해 비활성화되는 경우가 많습니다. 네트워크 중심 또는 단말 중심 여부에 관계없이 이러한 모델에서는 궁극적으로 어딘가에 최초 피해자가 나타나야만 서명이나 분석 엔진을 그에 따라 업데이트합니다.

현재 직원들의 업무 환경의 변화가 일어났습니다. 대부분 직원들은 상당 시간 웹 브라우저를 활용합니다. 웹에서 실행되는 비공개 애플리케이션인 기업 SaaS 애플리케이션에 액세스하거나 웹에서 조사 작업을 수행하거나 심지어 이메일에 액세스하는지 여부에 관계없이 많은 직원의 일상 업무에서 브라우저가 핵심을 담당하고 있습니다. 이처럼 브라우저가 새로운 사무실 역할을 하고 있게 되면서 인터넷이 네트워크로 사용되고 애플리케이션과 데이터가 장소에 구애 없게 됨에 따라 가시성과 제어 기능이 저하되고 공격자들은 이를 기회로 활용하고 있습니다.

마지막으로 기술 부족 문제도 계속 커지고 있습니다. 보안 비용 지출이 전반적으로 증가하고 대기업의 경우 보안 역량이 향상된 것은 사실이지만 아직도 많은 조직은 보안 팀에 필요한 비용과 인력 확충에 어려움을 겪고 있습니다. ESG 는 조사 결과, 다른 어떠한 기술 영역보다 사이버보안 지출 증가 계획을 갖고 있는 조직이 많다(69%)는 사실을 알게 되었습니다. 그러나 동시에 약 절반에 해당하는 조직(48%)에서 다른 어떠한 기술 영역보다도 기존 보안 기술이 부족하다는 문제도 제시했습니다.[7] 대기업조차도 전담 보안 팀을 소수의 인력으로만 운용하고 있는 경우도 있습니다. 성능이 낮은 보안 도구는 정확도와 컨텍스트가 부족한 경고를 과도하게 생성하는 경우가 많으며 이로 인해 인력이 부족한 상황이라면 팀의 효율성을 기대하기란 어렵습니다. 결국 보안 팀은 한 문제를 해결하지 못하고 다음 문제를 처리해야 하며 이는 궁극적으로 보안 효과에 영향을 미치는 것은 물론 공격자에게 이로운 기회를 제공하게 됩니다.

HEAT 공격 차단을 위한 주요 고려 사항

앞으로도 공격자는 방어 체계를 우회하기 위한 전술을 계속 개발할 것입니다. 이는 일반적인 공격은 물론 구체적으로 HEAT 공격 모두에 . 그러나 조직에서 이러한 유형의 공격에 대한 민감성을 억제하려면 세 가지 중요 원칙에 집중해야 합니다. 즉 감지에서 예방적 사고 방식으로 전환하고 위협이 단말에 도달하기 전에 미리 차단하며 고급 피싱 방지와 격리 기능을 통합해야 합니다.

조직에서 이러한 유형의 공격에 대한 민감성을 억제하려면 세 가지 중요 원칙에 집중해야 합니다. 즉 감지에서 예방적 사고 방식으로 전환하고 위협이 단말에 도달하기 전에 미리 차단하며 고급 피싱 방지와 격리 기능을 통합해야 합니다.

[7] 출처: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.

감지 기능이 효과를 발휘하려면 조직에 사각 지대가 없는 포괄적인 가시성, 다양한 소스에서 연관성이 높은 데이터, 사고 발생 시 즉각적으로 대응할 수 있는 능력이 있어야 합니다. 거의 모든 복잡한 조직에 있어 이는 무리한 요구입니다. 따라서 사후 대응 방식이 아닌 장치나 시스템이 영향을 받기 전에 최대한 많은 위협을 방지하는 것이 목표가 되어야 합니다. 제로 트러스트에 대한 관심 확대는 이러한 유형의 전략이 검증된 결과입니다. 복잡성과 다양성이 증가함에 따라 확대 범위를 제한하고 환경에서 절대적인 신뢰를 제거해야 하는 필요성이 그 어느 때보다도 중요해지고 있습니다. 보안 팀은 예방적 사고 방식으로 전환하고 제로 트러스트 원칙을 통합함으로써 발생한 문제를 해결하는 데 급급하지 않고 취약점 파악 및 조치, 관련 구성 강화 및 위협 헌팅 등 사전에 조직의 보안 태세를 강화하는 데 집중할 수 있습니다.

이제 다음 문제는 "예방 조치에 있어 어느 부분에 집중해야 하는가?"입니다. 작업자와 리소스가 계속 분산됨에 따라 보호 기능 분산도 중요해지고 있습니다. 동시에 HEAT 공격도 장치에서 멀웨어를 어셈블하고 전달된 제어 기능을 비활성화하는 방식으로 단말 도구를 회피하도록 설계되고 있습니다. 이러한 유형의 공격을 방어하는 데는 클라우드 기반의 웹 중심 보호 방식이 가장 적합해 보이지만 보안 팀은 이러한 도구를 신중하게 평가해야 합니다. 보안 웹 게이트웨이(SWG)는 전통적으로 온프레미스에서 배포되고 제한적 사용 정책을 적용하는 데 집중하고 있으며 서명 기반 위협 방지와 함께 애플리케이션에 대한 가시성이 낮아 HEAT 공격을 방어하는 데 한계가 있었습니다. 보안 팀은 세분화된 애플리케이션 가시성 및 제어 기능, 인라인 콘텐츠 검사 및 HEAT 공격을 사전에 차단할 수 있는 최신 위협 방지 기능을 제공하는 클라우드 기반의 최신 SWG 를 찾아야 합니다.

마지막으로 방지 기능에는 최신 격리 및 피싱 방지 기능이 포함되어야 합니다. 서명과 분석 기능으로도 일부 위협이 엔터프라이즈에 영향을 미치는 것을 방지할 수 있지만 HEAT 공격을 차단하기 위해서는 추가적인 보호 조치가 필요합니다. 격리 기술은 브라우저와 단말의 상호 작용을 방지하므로 HEAT 와 같은 은밀한 위협을 근절시킬 수 있습니다. 마찬가지로, 피싱 방지 범위가 전통적인 이메일 채널 그 이상으로 확장되면서 웹, 소셜 및 SMS 기반 공격에 대한 지속적인 방어도 중요해지고 있습니다.

결론

다른 비즈니스나 산업과 마찬가지로 트렌드와 시장 역동성이 발전함에 따라 사이버 범죄자들도 혁신과 관련성을 유지할 수 있는 방법을 계속 모색하고 있습니다. 원격 및 하이브리드 작업으로의 전환과 클라우드 채택 가속화는 대부분 작업자의 일상 업무 방식을 브라우저 중심으로 완전히 바꾸어 놓았습니다. 공격자 관점에서는 물고기가 많은 곳에 낚싯줄을 던지는 것이 당연한 일입니다.

HEAT 공격은 전통적인 보안 방어 체계의 큰 공백을 악용한다는 점에서 공격자 기술의 중요한 진화라고 할 수 있습니다. 유명한 해커 그룹이 이미 랜섬웨어를 비롯한 다른 최신 공격에 이 방법을 사용하고 있다는 사실은 공격자가 얼마나 민첩하고 보안 팀이 이를 따라잡기 위해 얼마나 빠르게 대처해야 하는지를 명확하게 보여줍니다. 이러한 상황에서 보안 리더는 HEAT 공격을 방어하기 위해 사전 방지, 단말에서 분리된 분산 보호, 최신 피싱 방지 및 격리 기능에 주력해야 합니다.

Enterprise Strategy Group 은 글로벌 IT 커뮤니티에 시장 동향 정보와 실행 가능한 정보를 제공하는 IT 분석, 연구, 검증 및 전략 전문 기업입니다.

www.esg-global.com

contact@esg-global.com

508.482.0188