Device ID+를 이용한 로그 분석 향상 방안

F5 Device ID+로 새로운 컨텍스트와 통찰력 강화

F5 Device ID+ 소개

F5 Device ID+는 기업의 웹 또는 모바일 웹 애플리케이션에 접속하는 물리적 디바이스를 쉽게 식별하는 고유한 가명 처리 식별자 (pseudonymized identifier) 입니다. 삭제와 조작에 취약한 디바이스에 저장되는 쿠키 등 기존 디바이스 식별자와 달리, F5 Device ID+는 제거하거나 조작이 어려운 JavaScript 기반 신호를 사용해 계산되기 때문에 훨씬 더 지속적이고 안정적입니다.

비율을 통한 컨텍스트 지원—로그 분석은 금융 분석과 마찬가지로 미가공 수치보다는 비율이 중요합니다. 비율은 컨텍스트에 수치를 부여합니다. 예를 들어, 유동 부채의 가치는 컨텍스트에서 볼 때 숫자만으로는 아무것도 알려주지 않지만, 유동 자산 대 유동 부채로 계산되는 유동 비율은 회사의 유동성에 관해 많은 것을 알려줍니다.

재무 분석가들과 마찬가지로 보안 분석가들은 특정 변화가 문제를 나타낸다는 사실을 인식한 상태에서 여러 비율을 주시하고, 각 비율에 대한 적절한 범위를 파악하며, 시간 경과에 따른 비율의 추세를 추적합니다.

SIEM 시스템의 추가 데이터 필드인 F5 Device ID+는 미가공 수치, 즉 일정 기간 동안 로그에 나타나는 Device ID의 수가 아니라, 주요 보안 값을 추가합니다. 이는 많은 유용한 비율로 환산되기 때문이며, 본 백서에서 이 내용을 다룰 예정입니다. 뿐만 아니라, 이들 비율은 실용적입니다. F5 Device ID+를 사용해 추가적으로 분석 및 조사가 필요한 네트워크 요청 트래픽을 식별할 수 있습니다.

귀사 및 보유 애플리케이션의 맥락에서 이들 각 비율은 유동적인 고유의 값 범위(아마도 상당히 좁은 범위)를 갖습니다. 본질적으로, 우리는 기업 사이트에서 합법적으로 비즈니스를 수행하는 실제 사용자를 나타내는 정상적인 네트워크 트래픽에 주목합니다. 이들 비율의 변화, 특히 몇 시간 또는 며칠에 걸친 갑작스러운 변화는 경보를 발생시키며 추가 조사를 실시해야 합니다.

Device ID당 IP 주소(IP/DID)

Device ID당 IP 주소 비율은 데스크톱 컴퓨터는 낮고, 노트북은 높으며 모바일 단말인 경우 가장 높을 것으로 예상됩니다. 전반적으로 모든 사용자 디바이스의 비율은 시간이 지남에 따라 크게 달라지지 않으며, 특히 갑작스럽게 변하지는 않습니다. 한 시간 또는 하루와 같이 짧은 기간 동안의 갑작스러운 변화는 일부 사용자가 프록시 네트워크를 사용해 의도적으로 IP 주소를 변경하고 있음을 나타낼 수 있으며, 이는 공격의 신호일 가능성이 높습니다. 이를 발견하면 IP 주소가 많은 Device ID의 네트워크 요청을 조사하십시오.

사용자당 Device ID(DID/User)

많은 사용자들이 한 대보다는 많은 디바이스에서 사이트에 접속할 것으로 예상합니다. Device ID당 IP의 비율과 마찬가지로, 사용자당 Device ID의 비율은 상당히 안정적으로 유지될 것으로 예상됩니다. 마찬가지로 갑작스러운 변화는 적신호입니다. 갑자기 예상보다 많은 디바이스에서 사용자 계정에 접속한다면 이는 공격일 수 있습니다. 대부분의 경우, 이러한 디바이스에서의 접속은 실제 사용자에 의한 접속이 아닙니다.

Device ID당 사용자(Users/DID)

사용자당 Device ID의 역수, 특히 Device ID당 사용자 또한 중요한 비율입니다. 여러 가족 구성원들이 동일한 디바이스를 공유하는 것은 드문 일이 아닙니다. 디바이스를 공유하는 것은 특정 회사나 도서관과 같은 공공장소에서도 발생합니다. 하지만 이 수치는 시간 경과에 따라 일정하게 유지될 것으로 예상합니다. 평균 가족 수는 이번 주 동안에는 더 증가하지 않을 것입니다. 이 비율이 증가하면 공격자가 여러 계정에 액세스하기 위해 단일 디바이스나 제어 디바이스 세트를 사용하고 있음을 나타냅니다. 보다 자세히 알아보려면, Device ID당 사용자 수가 비정상적으로 많은 요청을 살펴보십시오.

Device ID당 우편번호(Postal/DID)

디바이스 기반 지리적 위치 데이터는 각 HTTP 요청을 특정 우편번호와 연결할 수 있습니다. Device ID당 우편번호는 부분적으로 사용자의 이동성을 측정하는 것입니다. 즉, 사용자가 일정 기간 동안 여러 우편번호에서 디바이스를 실행한 빈도를 나타내며 그 자체로는 보안에 영향을 주지 않습니다. 하지만 설명할 수 없는 이 비율의 증가는 공격자가 실제 위치를 숨기기 위해 프록시 팜을 통해 공격하고 있음을 나타낼 수 있습니다. 프록시 팜을 사용하면 한 디바이스를 단시간 내 여러 위치에서 나타나도록 할 수 있습니다. 조사하려면 우편번호 수가 가장 많은 Device ID를 조사하십시오.

Device ID당 ASN(ASN/DID)

Device ID당 ASN 비율은 1보다 크지만 Device ID당 IP 주소의 비율보다 낮을 수 있습니다. Device ID와 연결된 ASN은 사용자가 한 ASN에서 다른 ASN으로 디바이스를 이동할 때만 변경되기 때문인데, 아마 직장에서 집으로 퇴근하거나, 카페를 들르거나, 일반적으로 이동할 때입니다. Device ID당 우편번호 비율과 마찬가지로 Device ID당 ASN이 갑자기 증가하면 공격자가 프록시 팜을 통해 네트워크 위치를 숨길 수 있음을 나타냅니다.

Device ID당 사용자 에이전트(UA/DID)

특정 브라우저 버전이 제거된 사용자 에이전트 문자열은 Device ID에 따라 변경되어서는 안됩니다. 이 비율이 1보다 큰 숫자를 표시하면, 공격자가 사용자 에이전트를 스푸핑하고 자신이 아닌 다른 사람인 것처럼 변장한다는 신호일 수 있습니다. Device ID를 기반으로 분석해보면, Device ID당 사용자 에이전트 수가 아주 많은 Device ID에 속하는 요청들을 찾을 수 있습니다. 이러한 요청은 일종의 공격일 수 있습니다.

Device ID당 로그인 성공률

로그인 성공률은 총 로그인 시도 중 성공한 로그인 비율을 나타냅니다. 이 메트릭을 파악하지 못하고 있었다면, 이제는 해야 합니다. 로그인을 제공하는 애플리케이션은 이 메트릭을 추적할 수 있습니다. 이것이 불가능한 경우, 요청 경로와 응답 상태 코드, 헤더를 확인하는 웹 로그를 통해 실패 대비 성공률을 파악할 수 있습니다. 로그인 성공률은 그 자체로 매우 중요합니다. 모든 애플리케이션에는 고유의 비율이 있습니다. 이 비율이 감소하면 공격, 크리덴셜 스터핑, Brute Force 공격 또는 로그인 마찰 증가를 나타냅니다.

Device ID당 로그인 성공률을 분석하는 것이 훨씬 더 유용합니다. 로그인 성공률이 유달리 낮은 Device ID의 요청을 분석하면 악의적인 공격시도를 파악할 수 있습니다. 즉, 성공률 자체는 공격이 있는지 여부를 알려주는 반면, Device ID는 공격 소스를 찾는 데 도움이 됩니다.

세션 식별자당 Device ID

웹 사이트는 종종 제한된 시간 동안 세션 식별자를 사용해 세션을 정의합니다. 세션 식별자는 일반적으로 20분 또는 몇 시간 내에 만료됩니다. 이 시간 내에 Device ID가 변경될 가능성은 거의 없기 때문에, 세션 식별자 당 Device ID 비율이 1보다 크면 특히 심각한 보안 위반인 세션 가로채기(hijacking) 시도로 의심할 수 있습니다. 이 경우 Device ID 수가 1보다 큰 세션 식별자를 자세히 조사하십시오.

결론

Device ID+는 공격을 경고하고 의심스러운 활동을 추적할 수 있도록 합니다. 이 백서에서는 Device ID와 관련한 몇 가지 유용한 비율을 검토했지만, 모두 다룬 것은 아닙니다. 애플리케이션의 세부 사항, 비즈니스 모델, 보안 우려 사항 등에 따라 더 큰 가치가 있는 다른 비율을 찾을 수 있습니다.

로그 분석에서 주요 Device ID+ 비율을 추적해 얻을 수 있는 보안상의 이점이나 F5 Device ID+의 기타 사용 사례를 알아보려면 지금 Shape Security 또는 F5 영업 담당자에게 문의하십시오.

자세한 내용은 Shape Security 또는 F5 담당자에게 문의하거나, shapesecurity.com 또는 f5.com를 방문하십시오.

ⓒ2020 F5, Inc. All rights reserved. F5 및 F5 로고는 미국 및 기타 특정 국가에서 F5, Inc.의 상표입니다. 기타 F5 상표는 f5.com에서 확인할 수 있습니다.
본 자료에 언급된 기타 모든 제품, 서비스 또는 회사 이름은 각 소유권자의 상표이며, F5, Inc.의 그 어떠한 명시적 또는 암묵적 보증이나 제휴도 부인합니다.
DC0420 | JOB-CODE-123456789