Akamai

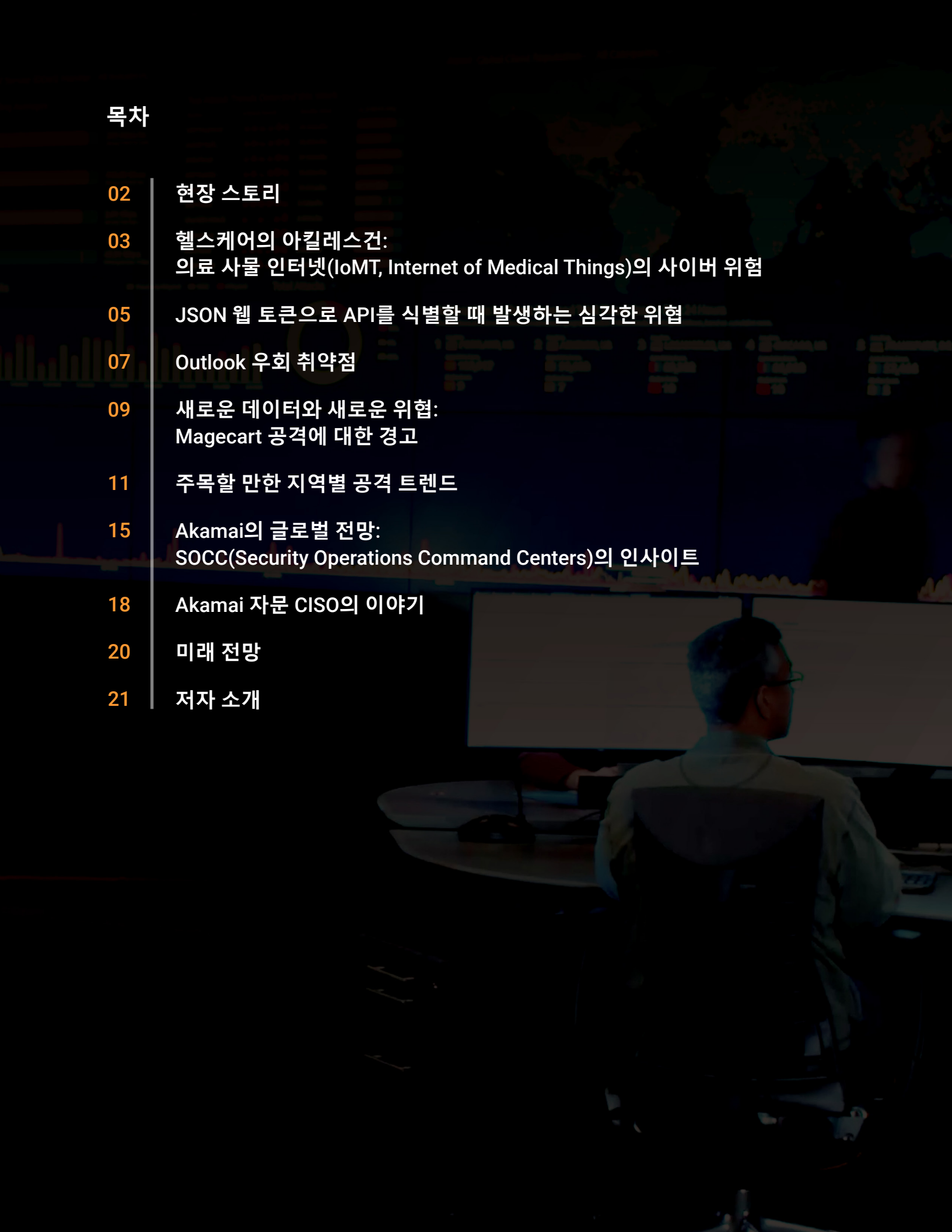
인터넷 현황 보고서

9권 | 6호

연간 리뷰:

2023년의 사이버 보안트렌드와 향후 전망

목차



현장 스토리

이 SOTI(State of the Internet) 보고서에서는 일반적으로 보고서에서 검토하는 연말 리뷰에서 벗어나 올해 가장 흥미로웠던 보안 사례에 대해 중점적으로 다룹니다. 이를 위해 Akamai SIG(Security Intelligence Group) 작성자와 데이터 과학자에게 지난 10개월 동안 다루었던 내용에 대한 연말 평가를 부탁했습니다. 2023년에 보안 리서치 블로그와 SOTI에 발표된 여러 가지 중요한 내용과 새롭게 발견된 사항들 중에서 하나만 고르기는 쉽지 않았을 것입니다. 또한 자문 CISO와 SOCC(Security Operations Command Centers) 부사장에게 올해의 공격 트렌드와 함께 2024년에 유념해야 할 주요 교훈이 무엇인지 요청했습니다.

올해는 보안 분야 뿐만 아니라 Akamai 보안 리서치에 많은 일이 있었습니다. Akamai 보안 전문가의 리서치는 커뮤니티에서 매우 중요한 역할을 합니다. 보안 전문가들은 Akamai의 전용 허브를 통해 인사이트, 방어 전략, 공격 트렌드 등 신뢰할 수 있는 리소스에 쉽게 접속해 기업을 방어할 수 있습니다. 또한 RPC Toolkit 등의 무료 툴과 무료 오픈 소스 자문 에뮬레이션 플랫폼인 Infection Monkey도 이용할 수 있습니다. Infection Monkey는 멀웨어와 마찬가지로, 비트를 뒤집어 접속할 수 있는 파일을 전파 및 암호화해 공격자가 해당 환경에서 어떻게 이동할 수 있는지 또는 없는지에 대한 현실적인 관점을 제공합니다. 위협은 빠르게 진화하고 있기 때문에 이에 대한 지속적인 테스트가 필요합니다. 실무자는 지난번 모의 침투 테스트가 진행되던 당시에 네트워크 상태가 아니라, 지금 이 순간 네트워크의 상태를 파악해야 합니다.

2023년을 한 단어로 요약하자면 전환이라고 말할 수 있습니다. 공격자들은 보안 조치를 우회하기 위해 기법을 바꾸고 새로운 공격표면과 드러나지 않은 표적을 찾아 규모와 업계에 관계없이 모든 기업을 공격했습니다. 마찬가지로 보안팀 직원은 공격을 방어하고 기업을 더 잘 보호하기 위한 새로운 방법을 지속적으로 재조정하고 학습했습니다. Akamai는 동일한 보안 위협을 방어하기 위해 싸우는 보안 실무자들에게 유용한 정보와 방어 전략을 제공하기 위해 솔루션, 리서치, 툴을 조정합니다.

이제 보고서를 확인해보세요!

헬스케어의 아킬레스건: 의료 사물 인터넷(IoMT, Internet of Medical Things)의 사이버 위험

안녕하세요, 저는 바데트 트리비(Badette Tribbey)라고 합니다. SOTI 보고서를 작성하는 스토리 작가로, 보안 전문가 및 데이터 과학자와 협력해 기술적인 결과와 데이터를 의미 있는 인사이트로 전환하고 있습니다. 저는 수학을 싫어하지만, 숫자를 통해 강력한 공격 트렌드를 찾아내는 작업을 좋아합니다.

올해 다루었던 가장 중요한 한 가지 주제는 의료 사물 인터넷(IoMT)의 리스크 증가입니다. 보안 격차의 허점과 멈추지 않는 랜섬웨어에서도 헬스케어 및 생명 과학 분야의 리스크 환경과 해당 업계가 공격에 취약한 이유를 조사했습니다. 가장 놀라웠던 것은 MRI 장비, 인슐린 펌프, 웨어러블과 같은 IoMT 자산이 환자에게는 매우 유익하지만, 헬스케어 공급업체의 리스크를 크게 높이고 있다는 점입니다. 이런 기업들은 이미 헬스케어 생태계 전반의 복잡성, 취약한 레거시 기술, IT 및 사이버 보안 인력 문제 때문에 경계를 보호해야 하는 도전과제에 직면해 있었습니다. 또한 여러 벤더사가 각각의 시스템 또는 애플리케이션에 대한 업데이트를 제공하기 때문에 이런 환경에서 적시에 패치 작업을 수행하는 것은 거의 불가능하며 추적하기도 어렵습니다.

패치되지 않은 IoMT 디바이스는 모든 업계에서 가장 취약한 자산이며 랜섬웨어와 같은 보다 악의적인 위협으로 이어질 수 있습니다. IoMT가 기하급수적으로 증가하고 API 사용도 증가하면서 확대된 취약점은 공격자가 표적에 침투할 발판을 마련하거나 이를 악용해 데이터 유출로 이어지는 경로가 될 수 있습니다(그림 1). Cynerio와 Ponemon Institute가 미국의 여러 병원 및 헬스케어 시스템을 대상으로 실시한 공동 보고서에 따르면, IoMT 디바이스의 보안 격차로 인해 절반 이상이 사이버 공격을 경험했습니다.

> “여러 벤더사가 각각의 시스템 또는 애플리케이션에 대한 업데이트를 제공하기 때문에 [헬스케어] 환경에서 적시에 패치 작업을 수행하는 것은 거의 불가능하며 추적하기도 어렵습니다.
>
> **– 바데트 트리비(Badette Tribbey) 수석 기술 작가, Akamai**

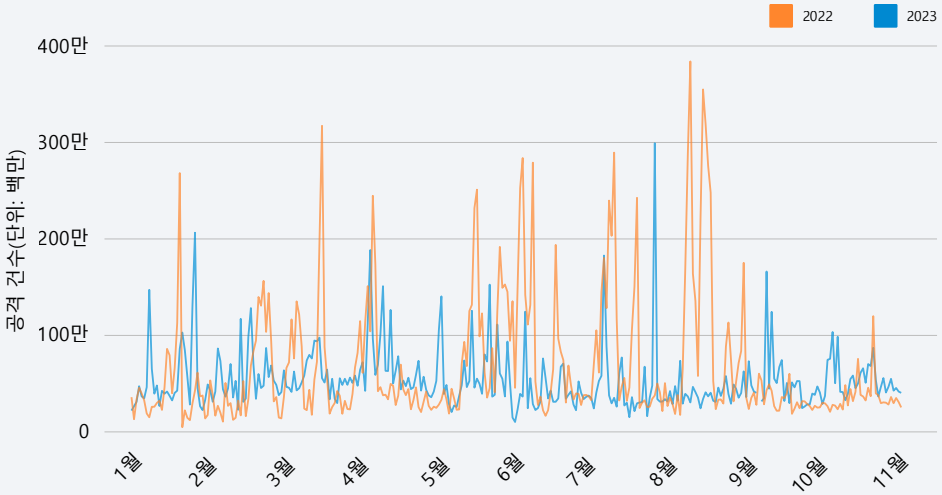


그림 1: 헬스케어 및 제약 업계에 대한 웹 애플리케이션 및 API 공격은 2022년과 2023년 사이에 산발적으로 급증하면서 꾸준한 활동을 보이고 있습니다. 전년 대비 공격은 21% 감소했지만 2023년의 일별 공격 건수 중간값은 2022년보다 높습니다.

헬스케어의 미래

헬스케어 업계에서 IoMT를 확장함에 따라 API는 의료 서비스(원격 진료 및 원격 환자 모니터링 등)의 접근성을 지원하는 중요한 역할을 계속 담당하며 임상 결과와 재정적 결과를 개선할 것입니다. 다크 웹 상에서 의료 기록 및 환자 데이터의 가치는 높기 때문에 헬스케어 서비스에 대한 공격은 줄어들지 않을 것입니다.

현재 트렌드에서 향후 전망으로 관점을 이동해 보면 공격자들은 지속적으로 혁신하고 공격의 규모와 복잡성이 증가할 것입니다. 제로데이 취약점을 이용하는 기술 공격도 계속 증가할 것으로 예상됩니다. 규제 환경(2022년 사이버 헬스케어 보호 및 혁신 [PATCH] 법안을 포함하되 이에 국한되지 않음)이 변하고 있기 때문에 Akamai 솔루션도 임박한 개인정보 보호, 보고, 결제, 데이터 주권, 안정성에 관한 수많은 법을 준수할 수 있도록 대비해야 합니다. 마지막으로, 벤더사를 통합함으로써 벤더 수를 줄이고 내부에 침투한 해커의 체류 시간을 최소화하는 솔루션을 사용하도록 CISO가 예산을 전환하면 더 많은 공격을 방어할 수 있을 것으로 예상합니다.

JSON 웹 토큰으로 API를 식별할 때 발생하는 심각한 위협

안녕하세요! 저는 랜스 로즈(Lance Rhodes)입니다. 2023년 3월부터 Akamai SIG 팀에서 사이버 보안 작가로 일하고 있습니다. 저는 주로 Akamai 보고서와 블로그 간 '결합 조직' 역할을 합니다. 블로그 게시물 및 섹션 리서치를 게시하고 작성하며 SOTI 보고서에서 콘텐츠와 마케팅 자료를 작성합니다. 이 모든 업무는 월간 내부 및 외부 뉴스레터와 보안 컨퍼런스 제출 자료를 위한 협업과 관련되어 있습니다.

지금은 제가 작업했던 흥미로운 블로그 게시물 중 JSON 웹 토큰(JWT) 게시물에 대해 이야기하고자 합니다. 이 게시물은 앱 및 API SOTI 보고서(보안 격차의 허점)와 직접적인 연관성이 있습니다. 이 보고서에서는 API를 식별하는 표준 방법 중 하나인 JWT의 잘못된 인증에 대해 보다 자세히 다룹니다. JWT에 대한 이해도를 높일 수 있는 흥미로운 시간이었습니다.

올해 초 앱 및 API SOTI 보고서를 작성한 후 닛잔 나메르(Nitzan Namer)와 함께 JWT 게시물을 쓰기 시작했습니다. 이 게시물에서는 Open Web Application Security Project (OWASP) API 보안 상위 10대에 오른 JWT를 손상된 사용자 인증에 대한 공격 기법으로 중점적으로 다루었습니다. SOTI 보고서의 한 섹션에서 JWT만 집중적으로 다루었지만, 블로그 게시물에서는 JWT 구조와 권한 상승, 데이터 유출, 계정 탈취 등 가장 큰 위협을 방어하는 모범 사례를 자세히 살펴보았습니다.

닛잔과 이야기를 나누며 이 게시물이 보안 연구원, 기술 실무자, JWT 사용자 및 관리자에게 지속적으로 도움이 되는 리소스로 사용되기를 바란다고 언급했습니다. 이 게시물은 지속적인 리소스가 되기에 적합한 구조와 내용을 갖추었습니다. 먼저 JWT의 기본적인 내용을 언급하고 일반적인 위협의 사례를 제시하며 각각에 대한 모범 사례를 설명하는 6가지 사례 시나리오가 나옵니다. 기본 내용에서는 JWT가 JSON 오브젝트로 공유할 정보가 포함된 토큰을 발행함으로써 API를 보호하는 방법을 설명합니다. 각 토큰은 암호화되지는 않지만 인코딩되며, 헤더, 페이로드, 확인 서명(서버가 토큰을 조작한 이후 데이터가 변경되지 않았음을 인증)으로 구성됩니다.

> “블로그 게시물에서는 JWT 구조와 권한 상승, 데이터 유출, 계정 탈취 등 가장 큰 위협을 방어하는 모범 사례를 자세히 살펴보았습니다.
>
> **– 랜스 로즈(Lance Rhodes), 사이버 보안 작가, Akamai**

6가지 시나리오는 다음과 같습니다.

1. 서버에서 검증 없이 토큰을 사용하도록 허용
2. 서로 다른 애플리케이션에 동일한 비공개 키 사용
3. 취약한 서명 알고리즘 사용
4. 짧거나 낮은 엔트로피 프라이빗 키 선택
5. JWT의 페이로드에 민감한 데이터 보관
6. 키 혼동

JWT는 가장 일반적인 검증 포맷 중 하나입니다. 이 포맷은 실수가 발생할 여지가 많은 대규모 공격표면을 제공하기 때문에 적절한 보안 조치가 매우 중요합니다. 이러한 시나리오는 JWT에 대한 가장 일반적인 위협 중 일부만 보여줍니다. 실제로는 여전히 더 많은 위협이 존재하며 공격 기술도 지속적으로 발전하고 있습니다.

JWT는 암호화되지 않았으며 보안을 염두에 두고 구축되지 않았습니다.

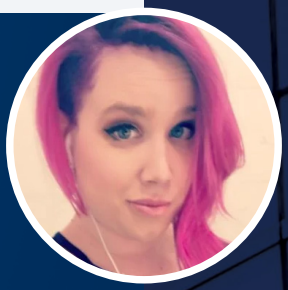
블로그 게시물에서 강조했던 한 가지 핵심 내용은 바로 JWT가 암호화되지 않았으며 보안을 염두에 두고 구축되지 않는다는 점입니다. 보통 이렇게 널리 사용되는 인증 토큰이 이렇게 취약할 것이라 생각하기 어렵습니다. JWT의 매력은 자주 로그인하지 않고도 다양한 웹 애플리케이션 및 API를 사용할 수 있다는 점입니다. SOTI 보고서와 JWT 블로그 게시물에서 Akamai 트래픽의 JWT 알고리즘을 분석한 결과, 이론적으로는 안전성이 떨어지고 비대칭 알고리즘만큼 방어 태세를 갖추지 못했지만 대칭 알고리즘이 가장 일반적으로 사용되고 있다는 결론을 내릴 수 있었습니다. 예를 들어, 두 게시물에서 모두 Akamai 고객 중 54.8%가 대칭인 HS256 알고리즘을 사용하고 있었습니다.

대칭 알고리즘은 사용자가 하나의 키만 있으면 되고 비대칭 알고리즘은 더 많은 양의 계산 리소스를 필요로 하기 때문에 대칭 알고리즘이 더 자주 사용될 수밖에 없습니다. JWT의 암호화된 버전인 JSON 웹 암호화 역시 널리 사용되지 않습니다. 대부분의 회사는 JWT를 사용하고 계산에 소모되는 전력을 절약하는 방법을 선택합니다.

중요한 사실은 편의성, 비용, 속도가 보안보다 자주 우선시된다는 점입니다. 이러한 사실은 보안 연구원 및 작가인 우리의 직업이 왜 중요한지를 반증합니다. 효율성과 안전 사이의 균형을 이루기 위해서는 바람직한 보안 리서치와 관행이 필요합니다.

> 보통 이렇게 널리 사용되는 인증 토큰이 이렇게 취약할 것이라 생각하기 어렵습니다.
>
> **– 랜스 로즈(Lance Rhodes), 사이버 보안 작가, Akamai**

Outlook 우회 취약점



안녕하세요? 오늘 하루도 즐거우셨나요? 저는 트리시아 하워드(Tricia Howard)이고, SIG에서 블로그를 담당하고 있습니다. 저는 기술 문서 작성이라는 중요한 업무를 맡고 있으며, Akamai의 연구원, 기업 커뮤니케이션 팀, 특히 법무팀과 협력해 적시에 효과적인 방식으로 자료를 작성합니다. 제 업무에서 제일 좋은 점은 멋진 업무를 하는 연구원을 대신해 자랑할 수 있다는 게 아닐까 합니다.

올해 제가 쓴 여러 주제 중에서 이번 주제가 가장 까다롭다고 생각합니다. 지난 12개월 동안 우리 팀이 진행한 여러 멋진 업무 중에서 하나만 고르는 것은 정말 어렵습니다. 하지만 굳이 한 가지를 꼽아야 한다면 벤 바네아(Ben Barnea)의 유명하면서도 악명 높은 Outlook 우회 취약점입니다. 벤은 제가 알고 있는 가장 뛰어난 연구원이기도 하고 슬래시 한 개만으로도 전체 패치를 무너뜨리는 방법을 찾기도 했습니다. 터무니없고 불가능한 이야기처럼 들리겠지만 벤은 그 일을 가능하게 만들었습니다.

Outlook에서는 원래 취약점으로 인해 권한이 없는 공격자가 사용자 지정 알림 소리와 함께 Outlook 초대를 보낼 수 있었습니다. 이 소리로 인해 공격자의 서버에 연결해 NTLM 인증정보를 제공하는 공격 경로가 두 배로 증가했습니다. 이러한 공격은 정말 악랄한 기법으로, 이 경로를 통해 공격자는 인증정보를 무차별 대입하거나 릴레이 공격을 감행할 수 있습니다. 물론 이 모든 상황이 권한 상승으로 이어질 수 있으며, 그렇게 되면 어떤 일이 벌어질지 우리 모두 알고 있습니다. 최악의 상황은 이 취약점이 제로 클릭이라는 점입니다. 즉, 사용자가 이 공격을 실행하기 위해 아무런 조치를 취하지 않아도 된다는 뜻입니다. 이 취약점은 매우 강력하고 위험한 상황을 초래할 수 있습니다. 특히 실제로 이 공격이 러시아에서 시작돼 확산하면서 여러 유럽 정부 기관에 침투하기도 했습니다.

이에 대한 패치는 3월에 발표되었습니다. 이 패치는 공격자가 공격자의 서버로 연결되는 경로를 지정하기 위해 사용되는 PidLidReminderFileParameter를 사용하지 못하도록 만들었습니다. 패치에서는 대신 MapURLtoZone 기능을 사용해 해당 경로가 인터넷에 연결하려고 시도하는지 여부를 확인했습니다. 연결을 시도하려고 하면 기존 알림 소리가 재생되어 사용자 지정 알림에 대한 파일 경로 옵션이 제거됩니다. 이렇게 하면 이론적으로 원격 공격자가 이 취약점을 악용할 수 있는 방법이 제거됩니다. 공격자와 피해자가 서로 연결되려면 결국 인터넷에 연결되어야 합니다.

> 보안팀 직원은 새로운 제로 클릭 권한 상승 취약점을 걱정하지 않고 많은 일상적인 업무를 바쁘게 진행합니다.
>
> **– 트리시아 하워드(Tricia Howard)**
> **수석 기술 작가,**
> **Akamai**

무용지물이 된 패치

흥미로운 부분은 이제부터입니다. 그리고 꽤 재미있기도 합니다. 다른 훌륭한 연구원과 마찬가지로 벤은 취약점이 실제로 더 이상 악용될 수 없는지 확인하고 싶었습니다. 정말 간단하게 말하자면, MapURLtoZone에는 기본적으로 허용과 거부, 두 가지 옵션이 있습니다. 인터넷이 필요할까요, 필요하지 않을까요? 대부분의 경우 패치는 의도한 대로 작동했습니다. 그런데 MapURLtoZone은 로컬 경로인 것처럼 보여도 인터넷에 도달하려는 의도가 있다고 인식하고 경로를 차단했습니다.

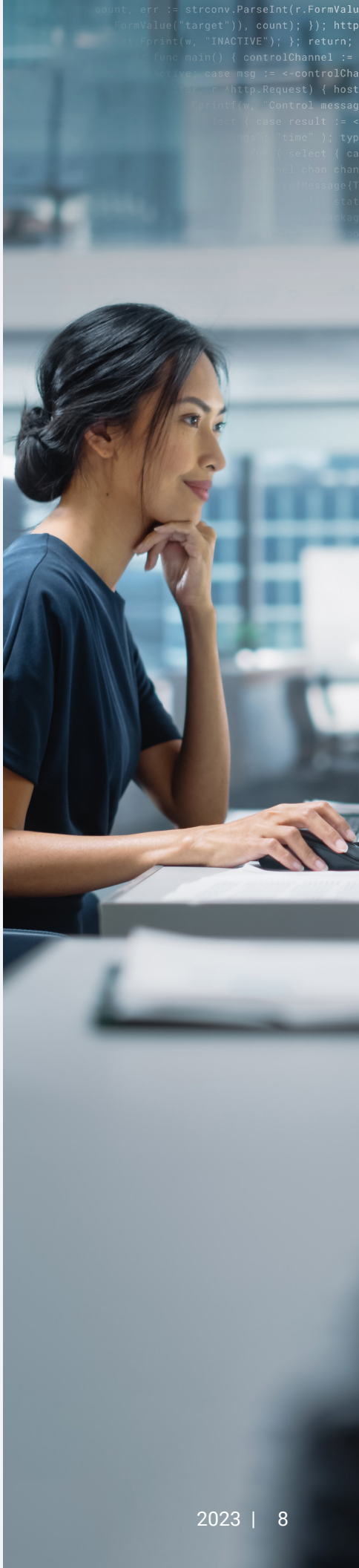
벤은 경로 이름 끝에 '/'를 추가해 테스트해보기로 했습니다. MapURLtoZone이 예상하지 못한 것을 제공해도 허용 또는 거부 여부를 결정해야 합니다. 이때 해당 매개변수는 추가 슬래시를 인식하지 못하고 0을 반환했습니다. 이는 함수가 신뢰할 수 있는 로컬 경로로 읽었음을 의미합니다. 이후 나머지 취약점은 사용자 지정 경로에 CreateFile을 활용함으로써 의도한 그대로 실행할 수 있었습니다.

그것 뿐이었습니다! 슬래시 하나만 추가했을 뿐인데 **치명적인** 취약점에 대한 전체 패치가 갑자기 무용지물이 된 것입니다. 사이버 보안 전문가는 이 위협을 없애기 위해 몇 일, 몇 주 또는 몇 달 동안의 시간과 에너지를 쏟아 이 패치를 만들었을 것입니다. 그런데 모든 노력이 하나의 슬래시만으로 좌절되었습니다.

원래 공격의 정교함은 무너뜨리는 순간, 착란을 일으킵니다. 공격자는 이제 망누스 칼센(Magnus Carlsen)(세계 체스 챔피언) 수준의 장기적 게임에 돌입했습니다. 슬래시만으로 패치를 무용지물로 만들었다면 공격자도 결국 스스로 우회할 수 있는 방법을 알아냈을 것입니다. 벤이 기발한 생각을 통해 이 버그를 발견한 것은 정말 대단한 일입니다.

이것이 바로 이 버그를 찾아낸 연구원이 보안 커뮤니티의 진정한 생명선인 이유입니다. 보안팀 직원은 새로운 제로 클릭 권한 상승 취약점을 걱정하지 않고 많은 일상적인 업무를 바쁘게 진행합니다. 일상 생활에서 기술과 인터넷에 대한 의존도가 높아지면서 보안 연구원들은 이 세상에 진정한 변화를 만들어내고 있습니다.

저는 이 놀라운 팀의 일원이 되어 이 지구에서 가장 뛰어난 사람들과 함께 일하게 되어 매우 자랑스럽습니다. Akamai의 블로그, 트윗, SOTI를 읽어 주시는 모든 분들께 감사의 말을 전합니다. Akamai SIG 내부 및 외부의 연구원 모두에게도 여러분이 하는 모든 일과 찾아낸 모든 성과에 감사드립니다. 내년에 어떤 일이 우리를 기다리고 있을지 함께 알아볼까요?



새로운 데이터와 새로운 위협: Magecart 공격에 대한 경고

안녕하세요. 저는 첼시 터틀(Chelsea Tuttle)이고, Akamai에서 약 8년 간 근무했습니다. 지난 4년은 SOTI에 나오는 데이터를 책임지는 데이터 과학자로서, 데이터를 정리하고 탐색하며 분석하고 시각화하는 데 대부분의 시간을 보냈습니다. 데이터를 보지 않을 때는 SOTI 작가들과 긴밀하게 협력하여 데이터가 우리에게 알려주는 이야기를 전달했습니다. 빅 데이터의 복잡성과 과거 데이터에 기반한 보고의 이점 때문에 새 데이터 세트를 자주 추가하는 편은 아니지만, 올해는 저희도 추가했습니다! 2023년을 돌아보면, 이 새로운 데이터 세트에 대해 게시한 이야기가 제일 마음에 들었습니다. 이러한 노력에 수반되는 학습 기회를 좋아하기 때문입니다.

실제로 네트워크에서 관찰되는 공격 시도 횟수를 보고하는 데 주력하면서 잠재적인 취약점 보호 및 공격 방지와 관련된 데이터를 보고할 중요한 기회를 놓치는 경우가 꽤 자주 있습니다. 올해 SOTI 보고서에 추가한 데이터 세트 중 하나는 공격 규모에 초점을 맞추는 대신, 특별히 잠재적인 취약점 영역을 강조한다는 점에서 눈에 띕니다. 이 데이터 세트는 Akamai Client-Side Protection & Compliance가 매일 수십억 개의 웹 페이지 스크립트를 날카롭게 분석한 관측 결과에서 파생되었습니다. 우리가 주목한 한 가지 잠재적 취약점 영역은 바로 웹사이트 전반에 걸쳐 사용되는 퍼스트파티 및 써드파티 스크립트의 수입니다. 퍼스트파티 스크립트를 사용한다고 해서 보안이 보장되는 것도 아니고 써드파티 스크립트를 사용한다고 해서 반드시 취약점이 생기는 것도 아니지만, 웹페이지 스크립트를 호스팅하는 데 써드파티를 신뢰하는 것처럼 써드파티를 더 많이 신뢰하게 되면 보안 프로필에 많은 리스크가 가중됩니다. Akamai는 모든 업계에서 써드파티 스크립트의 사용이 증가함에 따라 나타나는 보안 격차와 편의성 사이의 간극을 해소하기 위해 노력하고 있습니다.

2023년 6월에 공개한 기프트샵을 통한 침투: 커머스 업계의 위협 SOTI 보고서에서와 같이 올해 Akamai 리서치가 중점을 둔 한 가지 분야는 바로 최근 Magecart 스타일의 웹 스키밍 공격이었습니다. 특히 Magecart 공격이 디지털 커머스 업계를 계속 공략하는 현상을 관측했습니다. 이러한 종류의 공격은 악성 자바스크립트 코드 인젝션을 사용해 디지털 커머스 웹사이트의 장바구니에서 신용카드 정보와 같은 민감한 사용자 인증정보를 훔치려고 시도합니다. 이러한 종류의 공격은 공격자 측에서는 쉽게 시도할 수 있지만, 탐지가 점점 어려워지면서 소비자에게는 큰 리스크를 초래할 수 있습니다. Magecart, 즉 웹 스키밍 공격은 웹사이트 사용자나 소유자가 인식하지 못하는 사이에 자주 발생하며, 공격자는 일반적으로 취약하거나 오래된 소프트웨어를 사용하는 디지털 커머스 웹사이트를 선택합니다.

> “Akamai는 모든 업계에서 써드파티 스크립트의 사용이 증가함에 따라 나타나는 보안 격차와 편의성 사이의 간극을 해소하기 위해 노력하고 있습니다.
>
> **– 첼시 터틀(Chelsea Tuttle), 수석 데이터 과학자, Akamai**

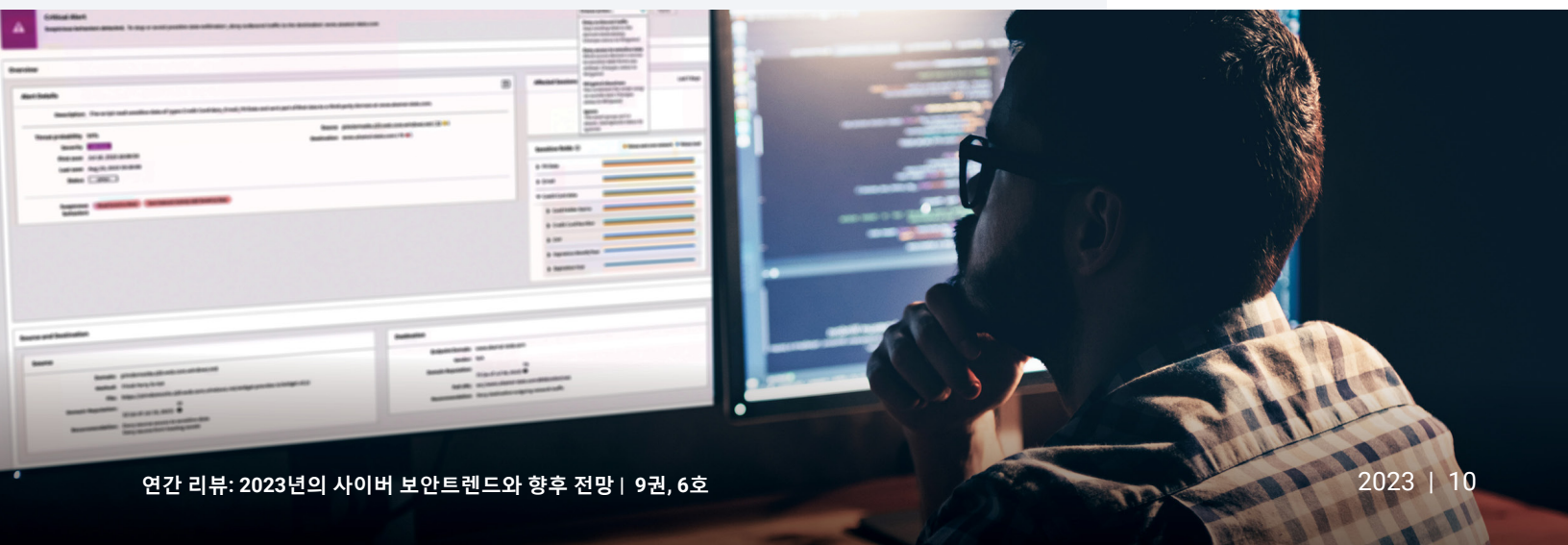
Magecart의 최근 변형

Akamai 연구원이 탐구한 최근 Magecart 캠페인에서는 다양한 Magecart 변형이 관측되었습니다. 2023년 6월 SOTI 보고서에서는, Magecart의 클라이언트 측 공격에 초점을 맞춰 오픈 소스 라이브러리의 써드파티 스크립트에서 발견된 취약점 악용으로 인해 공급망 공격이 발생할 수 있음을 지적했습니다. SOTI 보고서를 작성한 직후 Akamai 연구원은 정상적인 웹사이트를 악용해 타인을 공격하는 새로운 Magecart 스타일의 캠페인을 어떻게 발견했는지에 관한 블로그 게시물을 발표했습니다. 이 캠페인에서 피해를 입은 웹사이트는 기본적으로 두 종류입니다. 호스팅을 위해 탈취되어 공격자가 제어하는 서버 역할을 하는 정상적인 사이트와 클라이언트 측 웹 스키밍으로 공격을 받은 취약한 커머스 사이트가 이에 해당합니다. 8월에는 Akamai 연구원이 디지털 커머스 사이트를 악용해 피해자의 결제 통계를 수집하는 숨겨진 서버 측 템플릿 인젝션 기능을 갖춘 또 다른 새로운 Magento 캠페인을 발견한 사례에 관해 두 번째 블로그 게시물을 발표했습니다.

Akamai SIG의 최신 Magecart 블로그 게시물에서는 공격자가 악성 코드를 숨기기 위해 웹사이트의 기본 404 오류 페이지를 조작하는 새로운 난독화 기법을 소개합니다. 여기서 Akamai 연구원은 이 새로운 캠페인이 두 가지 고급 은폐 기법으로 구성되었으며, 공격자가 공격 체인을 늘리고 탐지를 피하기 위해 새로운 기법을 사용한다는 점을 알아냈습니다.

2023년이 끝나가는 시점에 새로운 데이터와 새로운 위협과 관련된 모든 리서치 및 보고 기회를 되짚어 보면서 2024년에도 새로운 데이터와 학습 기회를 기대해봅니다.

Akamai 연구원들은 합법적인 웹사이트를 악용해 다른 웹사이트를 공격하는 새로운 Magecart 스타일의 캠페인을 발견했습니다



주목할 만한 지역별 공격 트렌드

안녕하세요. 저는 샬럿 펠리치아(Charlotte Pelliccia)입니다. 2023년에 아시아 태평양 및 일본(APJ), 유럽, 중동 및 아프리카(EMEA) 지역의 사례를 소개하고자 SOTI 팀에 합류했습니다. APJ 및 EMEA의 스냅샷은 글로벌 SOTI 보고서와 함께 제공됩니다. 이 자리에서는 2023년에 다룬 가장 중요한 공격 트렌드 중 몇 가지를 다시 살펴보고 올해 초에 게시했던 스냅샷의 데이터를 업데이트하고자 합니다.

웹 애플리케이션 및 API 공격 - 두 업계의 이야기

Akamai의 최신 금융 서비스 및 커머스 SOTI 보고서에서와 마찬가지로, 금융 서비스는 APJ 지역에서 웹 애플리케이션 및 API 공격이 가장 많이 발생한 업계이며 커머스가 그 뒤를 이었습니다. 2023년 6월 보고서 이후, 금융 서비스에 대한 공격은 45억 건(37억 건에서 22% 증가)을 넘어섰습니다. 2023년 3월 보고서 이후 커머스 업계에 대한 공격은 12억 건에서 19억 건으로 58% 증가했습니다. 하위 업계 사이의 비율은 비교적 일관되게 유지되었습니다(그림 2).

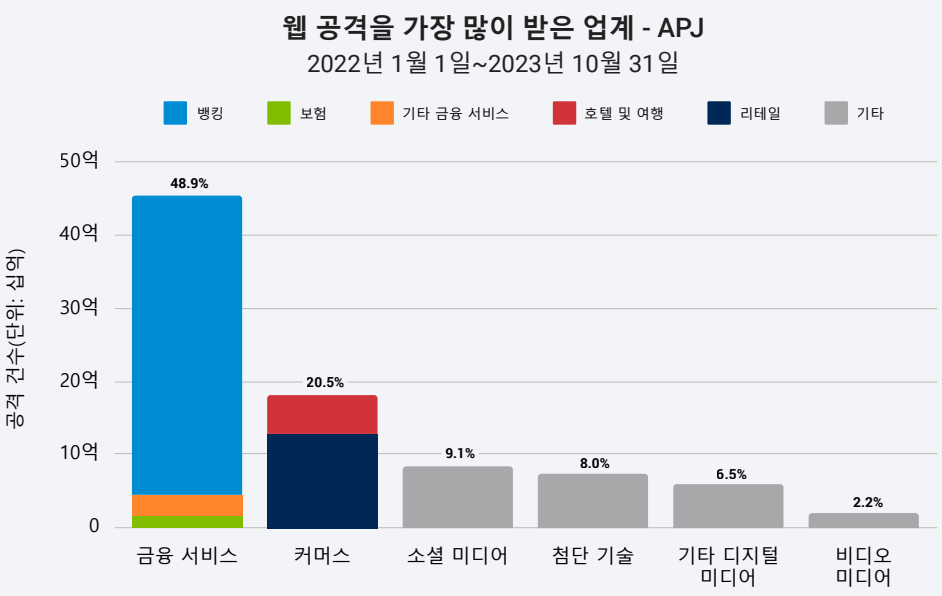


그림 2: 2023년 10월까지 APJ 지역 내 업계에서 발생한 웹 공격

> 기업이 리스크를 더 잘 이해하고 툴과 모범 사례를 미세 조정하려면 지역별 공격 트렌드에 대한 가시성이 반드시 필요합니다.
>
> **– 샬럿 펠리치아(Charlotte Pelliccia), 사이버 보안 작가, Akamai**

한편 EMEA에서는 커머스 업계에서 여전히 웹 애플리케이션 및 API 공격이 가장 많이 발생했고, 2023년 3월 보고서 이후 공격이 46억 건에서 41% 증가한 65억 건을 넘어섰습니다. 제조업이 금융 서비스를 제치고 4위에서 3위로 올라섰지만, 금융 서비스에 대한 공격은 2023년 6월 이후 70% 증가해 10억 건에서 17억 건으로 증가했습니다. 여기에서도 하위 업계 사이의 비율은 비교적 일관되게 유지됩니다(그림 3).

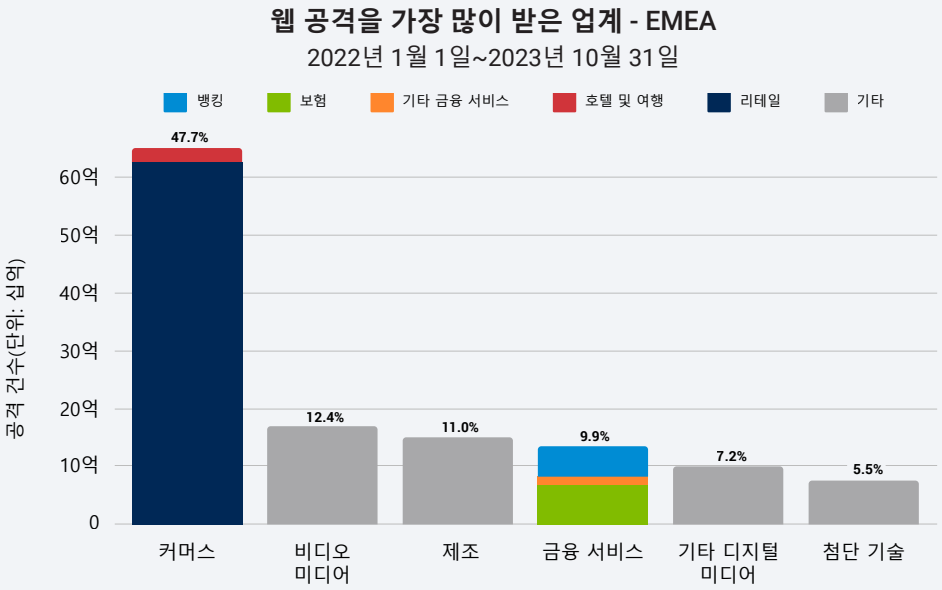


그림 3: 2023년 10월까지 EMEA 지역 내 업계에서 발생한 웹 공격

가장 많이 사용된 악성 봇

이전 보고서에서 확인한 바와 같이, APJ는 악성 봇 활동 부문에서 북미에 이어 2위를 차지했습니다. 2022년 1월부터 2023년 10월까지 APJ 지역에서 가장 많은 공격을 받은 업계는 커머스(27.4%), 비디오 미디어(15.0%), 금융 서비스(14.3%)로 나타났습니다. EMEA에서는 악성 봇 활동의 약 절반(50.1%)이 커머스를 표적으로 삼았으며, 기타 디지털 미디어(15.3%), 비디오 미디어(12.2%)가 그 뒤를 이었습니다(그림 4).

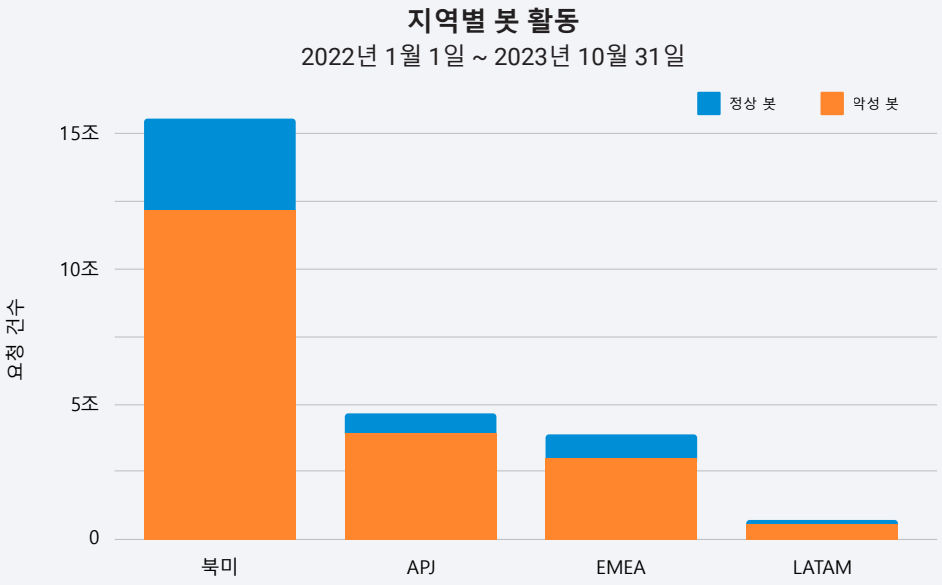


그림 4: 모든 지역에서 악성 봇의 사용은 빈번하게 발생하며 정상 봇의 사용량을 크게 능가함

봇과 DDoS 공격의 변화에 관한 SOCC의 인사이트를 보려면 다음 에세이를 참조하세요.

DDoS 공격과 관련해 지역적 변화에서 표적이 된 EMEA

Akamai의 2023 보고서에서는 공격자가 부분적으로 현재의 지정학적 변화에 기인해 EMEA를 정면으로 겨냥하고 있다는 점이 명백히 드러났습니다. 대표적인 예로, EMEA의 금융 서비스, 도박 및 제조 부문에서 발생한 DDoS(Distributed Denial-of-Service) 공격 건수는 다른 모든 지역의 건수를 합한 것보다 많습니다(그림 5).

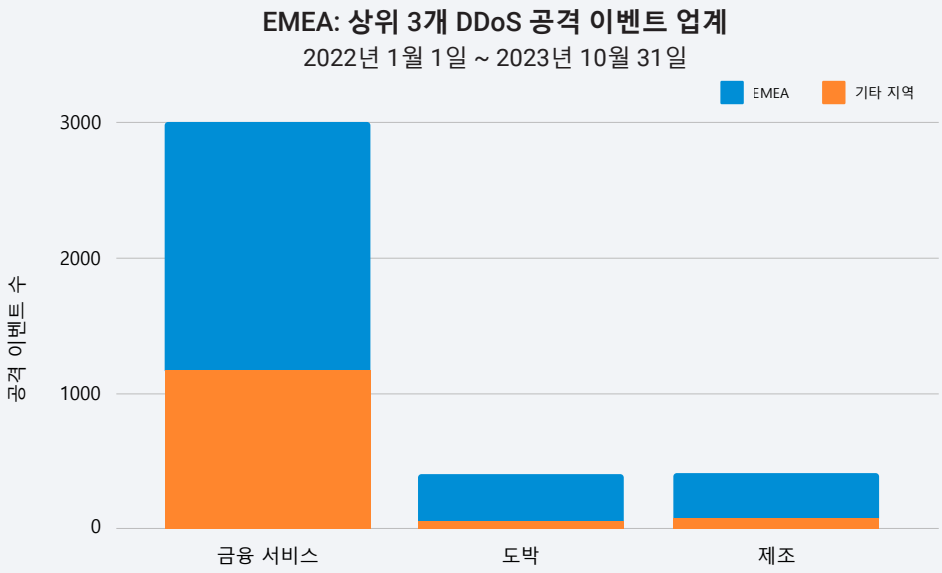


그림 5: EMEA에서 발생한 DDoS 공격 이벤트 수가 다른 모든 지역의 해당 업계에서 발생한 공격 건수를 합산한 것보다 더 많음

향후 전망

공격자가 웹, 봇, DDoS 공격으로 성공을 거두는 한, 이러한 공격은 계속 많이 사용될 것으로 예상됩니다. 실제로 이 세가지 공격 기법은 기세를 유지하거나 강화하기 위해 이미 발전하고 있습니다. 웹 애플리케이션 제로데이 악용 기법은 CL0P와 같은 랜섬웨어 그룹에 의해 랜섬웨어 기법과 연계되고 있으며, DDoS 공격을 포함한 삼중 협박 기법을 이용하고 있습니다. 봇을 이용한 웹 스크레이핑은 거의 모든 주요 항공사 이벤트 또는 티켓 판매에서 새로운 공격 표준이 되었습니다. API의 비즈니스 로직을 노린 API 공격도 새롭게 등장했습니다.

이에 대응해 전 세계 업계 전반에서 규제 감독 및 보고 의무가 지속적으로 증가하고 있으며, 어떤 지역이나 부문도 공격으로부터 안전하지 않습니다. 진화하는 위협 환경에 맞춰 사이버 보안 법률을 최신 상태로 유지하는 것이 목표입니다. 기업은 보고 요구사항을 준수하기 위해 경계를 늦추지 말아야 하며, 멀티레이어 방어를 통해 리스크를 방어할 준비를 갖추어야 합니다.

Akamai의 글로벌 전망: SOCC(Security Operations Command Centers)의 인사이트

안녕하세요. 저는 글로벌 보안 운영 담당 부사장인 로저 바랑코(Roger Barranco)입니다. Akamai에서 거의 10년 동안 근무하면서 Akamai의 매니지드 보안 운영을 책임지고 있습니다. Akamai는 전 세계에 위치한 6개의 SOCC를 통해 유능한 팀이 서비스를 제공하고 있습니다. 저는 사이버 보안 분야에서 처음 커리어를 시작했습니다. 끊임없이 변화하는 흥미로운 시장이었는데 2023년이 그 대표적인 예입니다.

Akamai SOCC는 그 어느 때보다 바쁜 한 해를 보냈습니다. 작년에 비하면 2023년 말까지 처리할 보안 관련 티켓이 약 30% 더 많을 것으로 예상됩니다. 다음으로, Akamai의 Managed Security Service 고객과의 협력을 통해 얻은 핵심 인사이트를 소개하고자 합니다. 기업이 2024년 염두에 두어야 할 사항입니다.

DDoS 공격의 지속적인 변화

공격을 받은 고객 수는 매년 증가하고 있지만 그 '방법'은 오늘날과 다릅니다. 첫째, 공격을 받은 고객 자산의 종류와 규모가 달라졌습니다. 예를 들어, 동일하거나 유사한 엔드포인트에 대한 공격이 예전에 10건이었다면 지금은 고객의 네트워크 공간에서 서로 다른 IP를 겨냥한 공격이 100건에 달합니다. 이러한 공격은 레이어 3뿐만 아니라 레이어 7도 동시에 표적으로 삼습니다. 또한 DNS에 대한 공격이 급격히 증가했고, 고객의 DNS 인프라를 쉽게 피로하게 만드는 유효한 쿼리 공격이 대량으로 발생하고 있습니다. 불과 몇 메가비트의 원치 않는 DNS 트래픽 때문에 기업은 상당한 부담을 겪을 수밖에 없습니다. 또한 사물 인터넷의 힘을 악용해 대규모 혼란을 일으키면서 악명을 떨친 Mirai 활동이 부활할 조짐도 보이기 시작했습니다.

오늘날 위협 환경에서는 변화하는 공격에 대비하기 위해 엣지에 강력한 장비를 구축하는 것만으로는 충분하지 않습니다. 이런 워크로드를 처리할 강력한 클라우드 수준의 보안 서비스가 필요합니다. 이를 통해 현 상태를 유지하면서 각각의 엔드포인트에 맞는 보안 기능을 구축할 수 있습니다. Akamai는 플랫폼과 서비스 측면에서 탁월한 성능을 발휘합니다. 다양한 보안 레이어를 적용해 모든 종류의 사이버 공격을 방어할 수 있습니다. 또한 Akamai의 실무 전문가는 각 고객의 미묘한 특징과 트렌드를 조사함으로써 문제를 차단하고 정상 트래픽은 허용하는 매우 구체적인 방식으로 모니터링하고 방어합니다.

> “Akamai SOCC는 그 어느 때보다 바쁜 한 해를 보냈습니다. 작년에 비하면 2023년 말까지 처리할 보안 관련 티켓이 약 30% 더 많을 것으로 예상됩니다.
>
> – **로저 바랑코(Roger Barranco), 글로벌 보안 운영 담당 부사장, Akamai**

무차별 악성 봇

원치 않는 트래픽과 원하는 트래픽을 구분하는 것이 어렵기 때문에 인증정보 도용은 굉장히 까다로운 공격입니다. 또한 고객의 백엔드에 따라 매우 다른 방어 전략이 필요할 수 있습니다. 인증정보 도용이 가장 쉬운 수익화 방법이기 때문에 인증정보 도용을 시도하는 공격자는 가장 노련하고 경계심이 강합니다. 이러한 봇 공격은 피해가 크고 비용이 많이 든다는 특성 때문에 인증정보 도용 예방 솔루션을 갖추는 것이 매우 중요합니다. 특히 악성 봇 사용량이 계속 증가하고 있는 금융 서비스와 커머스 업계에서는 더욱 그렇습니다.

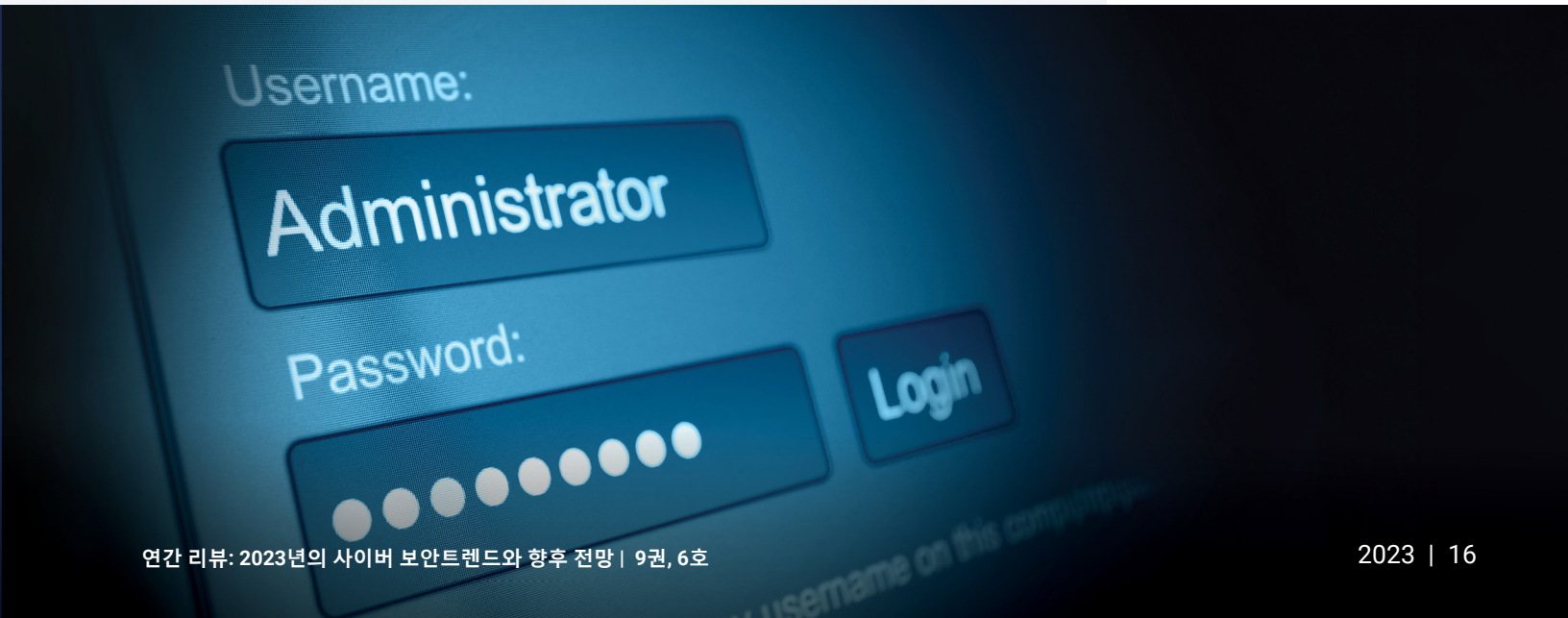
여전히 공격자의 활동 지역이 되고 있는 EMEA

우크라이나 침공 이후 EMEA(특히 유럽)는 다양한 공격 범주(특히 DDoS)와 다양한 업계에서 사이버 공격을 가장 많은 받은 지역으로 미국을 제쳤습니다. 이러한 전환은 많은 공격자가 민족 국가의 국민이거나 민족 국가의 지지자이며 유럽에 대한 관심이 수그러들지 않을 것이란 사실을 강조합니다.

더욱 정교해지는 공격자

스크립트 세대가 일반 툴을 이용해 운이 좋으면 먹히는 공격을 시도하거나 시간당 10달러로 DDoS 봇넷을 빌려 비디오 게임 경쟁업체를 공략하는 것이 주요한 위협으로 존재하던 시대는 지났습니다. 오늘날 공격자는 더욱 정교해졌으며, 구체적인 목표에 집중하고, 전략을 세우며, 때로는 1년 전부터 정찰을 실시해 잠재적인 약점을 활용하기 위한 공격을 고안하는 것으로 보입니다. 공격자가 이러한 기반 작업을 한 결과, 불과 몇 분 정도만 빈번하게 지속되던 지난 몇 년간의 공격 사례와는 달리, 지금은 공격 시간이 더 길어지고 있습니다.

> 공격자가 이러한 기반 작업을 한 결과, 불과 몇 분 정도만 빈번하게 지속되던 지난 몇 년간의 공격 사례와는 달리, 지금은 공격 시간이 더 길어지고 있습니다.
>
> **– 로저 바랑코(Roger Barranco), 글로벌 보안 운영 담당 부사장, Akamai**



사이버 환경과 운영 방식 조정을 위한 모범 사례

이러한 과제에도 불구하고 고객은 Akamai가 고객 사이버 팀의 연장선에서 활동할 수 있도록 지원하는 사이버 환경과 운영 방식 조정을 위한 모범 사례를 준수함으로써 기업을 보호하기 위한 노력의 효율성을 높일 수 있습니다. 첫째, 평상시에 SOCC와 협력해 공격 중에 방어 체계를 구축하는 대신, 선제적으로 방어 체계를 구축해야 합니다. 이러한 방식으로 회피에 성공한 공격을 자세히 기술하는 후속 보고서를 통해 공격이 프로덕션 환경에 영향을 미치지 않고 사전에 공격을 방어할 수 있습니다.

둘째, 운영 준비 및 백업 계획에 대해 선제적으로 준비해야 합니다. 예를 들어, 테스트 중에 서로 다른 플랫폼에서 라우팅을 켜고 끄는 방법을 알고 있는지 확인해야 합니다. 운영상의 문제로 인해 5분의 공격만으로도 고객에게 1시간 동안 피해를 줄 수 있으므로, 사이버 문제에 대응할 준비를 갖추는 것만큼이나 운영 준비를 갖추는 것도 중요합니다.

올해는 사이버 보안이 끊임없이 변화한 해였으며, 앞으로도 이러한 트렌드는 계속될 것으로 예상됩니다. 좋은 소식은 이러한 인사이트를 적용함으로써 2024년에서 고객이 한발 더 앞서 나가 기업을 보호할 수 있다는 점입니다.

Akamai 자문 CISO의 이야기

안녕하세요. 저는 Akamai의 자문 CISO인 스티브 윈터펠드(Steve Winterfeld)입니다. 이전에 Nordstrom Bank의 CISO로, 그리고 Charles Schwab의 인시던트 대응 및 위협 인텔리전스 부문 디렉터로 근무한 바 있습니다. 저는 파트너가 고객을 성공적으로 보호하고 역량을 집중해야 할 영역을 결정하도록 지원하는 업무를 담당하고 있습니다.

올해에는 몇 가지 놀라웠던 트렌드가 몇 가지 있었고, 또 몇 가지는 데이터로 확인돼 향후 Akamai의 전략을 업데이트하는 데 사용될 수 있습니다. 제가 꼽은 올해의 9가지 이야기 중 깨달음을 얻은 순간, 예상했던 소식, 그리고 결코 변하지 않는 것들에 대해 이야기해 보려 합니다.

깨달음을 얻은 순간

- 총 10%~16%의 기업이 분기당 한 번 이상 네트워크의 명령 및 제어(C2) 도메인에 접속했습니다. 또한 감염된 디바이스의 26%가 초기 접속 브로커와 관련된 도메인에 접속했습니다.
- 지난 6개월 동안 제로데이 취약점과 원데이 취약점을 악용한 사례가 크게 증가하면서 랜섬웨어 위협 환경에서 공격 기법이 변화하는 우려스러운 상황이 발생했습니다.
- Akamai 리서치 결과에 따르면, 여러 랜섬웨어 그룹의 피해자는 최초 공격 후 첫 3개월 이내에 후속 공격을 경험할 가능성이 약 6배 더 높습니다.

예상했던 소식

- API의 비즈니스 로직을 노린 API 공격은 탐지하고 방어하기가 복잡합니다. 따라서 개별 요청 수준에서 확인하기가 어렵습니다.
- 기업은 새로운 PCI DSS(Payment Card Industry Data Security Standard) v4.0 요구 사항 및 디지털 운영 안정성 법(DORA) 규정을 준수해야 합니다.

> 이러한 인사이트는 보안 프로그램의 실전 태세를 갖추고 중복된 툴이나 공백이 있는 부분을 파악하는 데 도움이 되는 훌륭한 가이드입니다.
>
> **– 스티브 윈터펠드(Steve Winterfeld), 자문 CISO, Akamai**

결코 변하지 않는 것

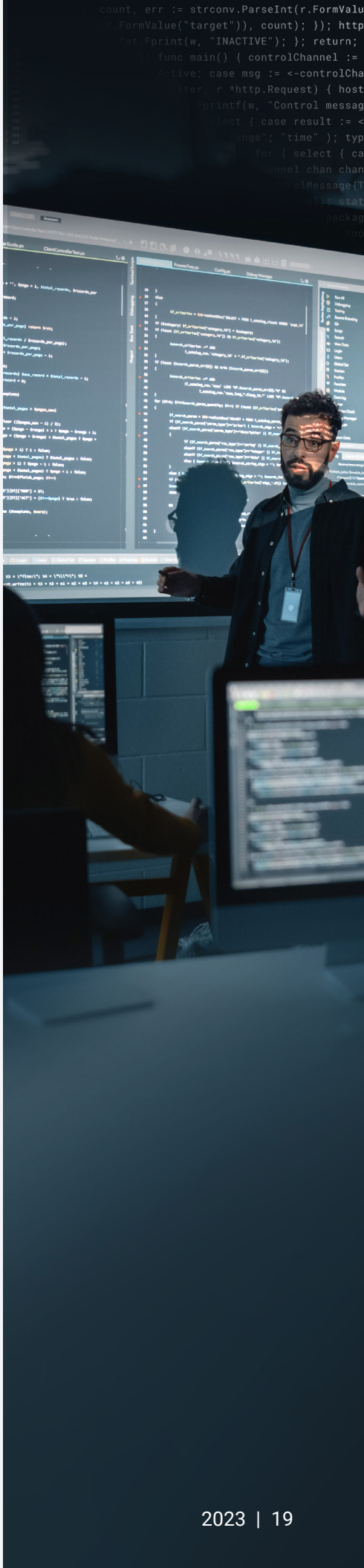
- 봇과 API 공격 수는 계속 증가하고 있으며 DDoS 공격의 경우 신기록이 경신되고 있습니다.
- 가장 공격을 많이 받은 업계는 금융 서비스, 하이테크 및 커머스입니다.
- 가장 많이 활용되는 공격 기법은 로컬 파일 인클루전(LFI)입니다.
- DDoS 공격이 가장 많이 발생한 지역은 북미에서 유럽으로 계속 이동하고 있습니다.

눈에 띄었던 한 가지 중요한 전환은 C2 통신에서 확인된 감염 징후였습니다. 특히 최초 탐지 시점이 멀웨어가 이미 시스템을 감염시키고 통신을 설정한 이후인 경우가 매우 많았다는 점은 우려스러웠습니다. 따라서 공격의 영향을 최소화하려면 예방 조치와 신속한 탐지가 균형을 이루는 것이 매우 중요합니다.

소셜 엔지니어링을 통해 사용자를 공격하는 것에서 제로데이 공격으로 이동했다는 점이 놀라웠습니다. 지난 몇 년 동안, 저는 우리의 기술적 방어가 더 강력해지고 있으며 교육과 모니터링을 통해 직원의 역량을 강화해야 한다고 생각했습니다. 하지만 올해 제로데이로 트렌드가 전환되면서 내년에는 리소스를 어디에 배치할지 더 면밀하게 검토해야 합니다.

가장 불공정한 공격은 기업이 이미 랜섬웨어 공격을 해결하고 있거나 복구하는 중에 발생하는 공격입니다. 자칫하면 위기에 과도하게 집중하고 지속적인 방어 모니터링에 리소스를 소진하기 쉽습니다. 이 리서치는 항시 방어 태세를 갖추어야 함을 강조하는 강력한 근거가 되었습니다!

이러한 인사이트는 보안 프로그램의 실전 태세를 갖추고 중복된 툴이나 공백이 있는 부분을 파악하는 데 도움이 되는 훌륭한 가이드입니다. 플레이북과 프로세스 업데이트, 교육 내용 조정, 모의 침투 계획 강화, 리스크 포트폴리오 검토를 지원하는 노력을 뒷받침할 수 있습니다. 사이버 보안은 팀 스포츠이기 때문에 이러한 인사이트는 내부 파트너(법률 또는 IT 팀 등) 및 벤더사와의 논의를 진행하는 데에도 유용합니다. 항상 그렇듯이 NIST(National Institute of Standards and Technology), MITRE ATT&CK 기술 자료 및 OWASP 상위 10대 리스크와 같은 참고 자료 및 툴은 훌륭한 리소스로 활용할 수 있습니다.



미래 전망

미래를 예측하기란 불가능하지만, 2024년에는 DDoS 및 API 공격이 지배적일 것으로 예상할 수 있습니다. 대규모 봇넷 군대를 구축하고 새로운 기술을 개발하려는 지속적인 노력과 국가 차원의 영향력이 서로 결합하여 DDoS는 계속 확대될 것입니다. 랜섬웨어의 진화와 함께 이런 요인은 법의 도입으로 이어질 것입니다.

전환은 대부분의 업계에서 API 구축의 원동력이 되고 있습니다. 이러한 급격한 성장은 의도치 않게 공격표면과 취약점, 섀도우 API, 좀비 API, API 악용으로 이어질 수 있습니다. 웹 애플리케이션 및 API에 대한 공격도 크게 증가할 것으로 예상됩니다. LFI와 같은 표준 공격과 서버 측 요청 위조(SSRF) 및 서버 측 템플릿 인젝션(SSTI)과 같은 새로운 기술에서 비롯되며, 이에 따라 측면 이동을 탐지하고 영향을 방어할 수 있는 툴이 필요합니다.

마지막으로, 일부 업계와 지역별 트렌드를 제외하고 숙련된 사이버 보안 전문가가 전반적으로 부족할 것으로 예상됩니다. 머신러닝과 대규모 언어 모델 인공지능이 일부 도움이 될 수는 있지만 전반적으로 기업이 필요로 하는 인재를 찾고 유지하기 매우 어려울 것입니다. 이러한 상황에서 중요도가 낮은 기능을 위해 매니지드 서비스를 이용하거나 온디맨드 인력 파견을 위해 벤더사와 파트너십을 체결할 수 있습니다.

Akamai SIG는 빈번하게 발생하는 위협과 새로운 보안 리스크에 대한 경고의 목소리를 계속 낼 것입니다. 위협 인텔리전스에 관한 노력을 강화하기 위해 Akamai 플랫폼과 채널을 통해 보안 커뮤니티와 협력할 것입니다. 그리고 2024년은 SOTI 보고서를 발행한지 10주년이 되는 해입니다. 보안 전문가가 계속 기업을 보호하기 위해 노력할 수 있도록 새로운 데이터 세트, 시각 보조 기능 및 주요 인사이트를 도입함으로써 Akamai 보고서를 지속적으로 개선할 수 있게 되어 매우 기쁩니다.

내년에도 더 많은 리서치 인사이트를 공유할 수 있기를 기대합니다. 그 때까지 안전하게 지내세요!

저자 소개

편집 및 작성

로저 바랑코(Roger Barranco)
트리시아 하워드(Tricia Howard)
샬럿 펠리치아(Charlotte Pelliccia)
랜스 로즈(Lance Rhodes)
바데트 트리비(Badette Tribbey)
첼시 터틀(Chelsea Tuttle)
스티브 윈터펠드(Steve Winterfeld)

검토 및 주제별 기여

킴벌리 고메즈(Kimberly Gomez)
루벤 코(Reuben Koh)
에밀리 라이온스(Emily Lyons)
리차드 메우스(Richard Meeus)
칼리 소넬(Carley Thornell)

데이터 분석

첼시 터틀(Chelsea Tuttle)

마케팅 및 출판

조지나 모랄레스 햄프(Georgina Morales Hampe)
에밀리 스핑크스(Emily Spinks)

인터넷/보안 현황 보고서

지난 보고서를 읽고 Akamai의 다음 인터넷 보안 현황 보고서를 확인하세요. **akamai.com/soti**

Akamai 위협 연구팀 자세히 살펴보기

akamai.com/security-research에서 최신 위협 인텔리전스 분석, 보안 보고서, 사이버 보안 연구 내용을 확인하세요.

이 보고서의 데이터 확인

이 보고서에 참조로 사용된 그래프와 차트의 고품질 버전을 확인하세요. Akamai가 제공한 소스라는 점이 정식으로 인정되고 Akamai 로고가 보존되는 경우 이러한 이미지를 무료로 사용 및 참조할 수 있습니다. **akamai.com/sotidata**

Akamai 솔루션 자세히 알아보기

위협에 대한 Akamai 솔루션을 자세히 살펴보려면 **보안 솔루션** 페이지를 참조하세요.