X-Force

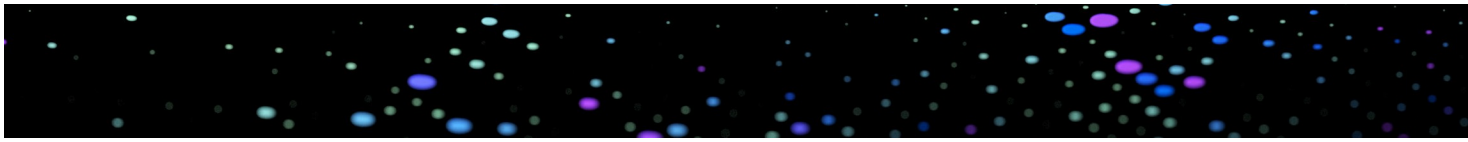
클라우드 보안 위협 동향 보고서 2020

IBM Security X-Force® Incident Response and Intelligence Services(IRIS)

2020년 2분기 특별 인텔리전스 보고서

IBM Security

목차



서론

확장 및 운영의 가속화를 위해 클라우드를 사용하는 조직이 점차 늘고 있습니다. 이러한 상황에서 클라우드에 특화된 사이버 위협의 특성을 이해하는 일은 필수적입니다. 이 분야의 주요 위협을 알아보기 위해 IBM은 글로벌 운영과 클라우드 인시던트 대응 능력을 활용하여 지난 일년간 IBM 이 대응했던 클라우드 관련 사이버 보안 인시던트를 심층적으로 분석했습니다. 본 보고서에서는 IBM Security가 클라우드 보안 운영의 최전선에서 경험한 것들을 다루며, 다음의 주제들로 구성되어 있습니다.

- 누가 클라우드 시스템을 노리는가
- 클라우드 환경에 대한 공격자의 접근을 IBM이 포착하는 방법
- 공격자가 클라우드 환경에 액세스 한 후 나타나는 위협 행위들은 무엇인가
- 자주 접하는 클라우드 보안 문제
- 조직의 클라우드 보안 태세를 강화하기 위한 권장사항

주요 결과

2019년부터 수집된 IBM Security 인시던트 대응 데이터에 따르면 클라우드 환경을 노리는 공격자의 가장 일반적인 동기는 금전적 이득인 것으로 나타났습니다.[1]

45%

클라우드 애플리케이션에 대한 무차별 대입 및 익스플로잇 공격은 이 보고서에서 살펴본 사례의 45%를 차지하여 가장 일반적으로 사용되는 두 가지 침입 경로였습니다.

사이버 범죄자들이 일단 클라우드 환경에 침투하면 개인 식별 정보(Personally Identifiable Information, PII) 도용과 같은 데이터 절도 행위를 주로 하는 것으로 나타났습니다.

10억 개 이상

클라우드 환경을 잘못 구성하여 2019년에 10억 개가 넘는 레코드가 유출되었습니다.

랜섬웨어는 침입을 당한 클라우드 환경에 가장 많이 배포된 멀웨어로, 2위와 3위를 차지한 크립토마이닝(암호 화폐 채굴) 및 봇넷 멀웨어보다 발생 건수가 3배나 더 많았습니다.

주요 결과

클라우드 플랫폼을 악의적 용도를 위한 인프라로 활용하는 것은 노련한 공격자들이 즐겨 시도하는 방법으로, 단 한번의 침해 행위로 연산 작업을 증가시킬 수 있습니다. 이 방법은 공격 대상에게 비용을 발생시킴으로써 공격자 자신의 비용은 최소화할 수 있으며 적법한 소스에서 비롯된 것처럼 보인다는 장점이 있습니다.

시간당 5만 달러 이상의 비용 손실

클라우드에서 실행되는 애플리케이션 유형에 따라, 침입은 짧은 시간 내에 엄청난 대가를 초래할 수 있습니다.

자산을 재배포할 것, 자산을 리이미징하지 말 것: 공격을 받은 클라우드 환경을 리이미징(reimaging)하기 보다 자산을 재배포하는 조직이 더 효과적인 포렌식 수사를 수행할 수 있어서 후속 피해를 방지할 수 있습니다.

심층 방어가 필수: 클라우드 사용이 증가하고 있다는 사실을 아는 멀웨어 개발자들이 많은 일반적인 클라우드 보안 제품을 무력화하는 멀웨어를 만들기 시작했으며, 이로 인해 많은 기업이 부지불식간에 취약한 상태가 되고 있습니다.

클라우드 컴퓨팅: 보안의 이점과 리스크의 공존

클라우드 컴퓨팅은 사용량 기반 지불 방식으로 인터넷을 통해 온디맨드 컴퓨팅 리소스를 전달하므로 컴퓨팅 역량을 전사적으로 확대하려는 조직에게 많은 보안상의 이점을 제공합니다. 대다수의 기업이 현재 약 20% 정도 클라우드로 전환 작업을 진행했습니다. 이러한 기업들은 핵심 IT 인프라를 계속 현대화하고 미션 크리티컬 데이터와 앱을 클라우드로 이전하는 한편, 이러한 새로운 하이브리드 멀티클라우드 환경으로 인해 초래되는 고유한 사이버 보안 과제와 기회에 적응해야 합니다.

클라우드 기반 자산 보호와 관련하여 자주 등장하는 용어들이 있으므로, 클라우드 보안에 대해 논의할 때 주요 용어에 대한 정의를 명확히 할 필요가 있습니다.

퍼블릭 클라우드
조직 외부에 호스팅된 클라우드 환경.

프라이빗 클라우드
조직이 전용으로 사용하기 위해 해당 조직 내부에서 호스팅 및 관리하는 클라우드 환경.

하이브리드 클라우드
온프레미스와 오프프레미스, 그리고 여러 클라우드에 걸쳐 통합되어 있고 전체적으로 관리되는 클라우드 환경.

컨테이너화
컨테이너는 애플리케이션 코드를 라이브러리 및 종속성과 함께 공통의 방식으로 패키징된, 실행 가능한 소프트웨어 유닛으로, 데스크탑, 기존 IT 또는 클라우드 등 어디에서나 실행할 수 있음.

기업들은 클라우드의 요소들을 간편하고 일관성 있으며 통합된 방식으로 하이브리드 멀티클라우드 인프라를 관리해야 하므로 기업 IT 환경은 갈수록 복잡해지고 있습니다. 아키텍처가 끝이 아닙니다. 데이터와 연산이 클라우드로 이동함에 따라, 클라우드의 초연결성에 내재된 보안 위협을 평가하고 해결해야 합니다. 클라우드 보안 위협 환경을 이해하면 조직이 스스로에 대한 보안을 강화하고 잠재적인 보안사고에 대비하는 데 도움이 될 수 있습니다.

리스크에 대한 고려

기업들의 전사적 클라우드 통합이 늘면서 클라우드 간 상호작용으로 인해 잠재적 감염이 온프레미스 공격의 경우보다 훨씬 더 빨리 확산될 수 있습니다. 또한 클라우드에서 실행되는 데이터의 양이 엄청나게 많아짐에 따라 공격자가 훔칠 수 있는 데이터의 양도 늘었습니다. 침해된 레코드 수는 데이터 침해 비용과 밀접한 관련이 있기 때문에 클라우드 보안 인시던트는 많은 비용을 발생시킬 수 있습니다. 비용을 순식간에 끌어올릴 수 있는 또 다른 요인은 클라우드 자산에 대한 무단 액세스입니다. 침해된 작업의 유형에 따라 이러한 무단 액세스로 인해 한 시간 안에 5만 달러(약 6천만원) 이상의 손실이 쉽게 발생할 수 있습니다.

클라우드 자산에 대한 무단 액세스가 초래할 수 있는 손실:

1시간 안에 5만 달러 이상의 손실 발생

클라우드는 많은 조직에게 새롭고 획기적인 사건입니다. 클라우드 보안을 유지하고 데이터 프라이버시에 대한 우려 및 규제 준수 문제를 해결하려면 기존의 IT 보안 관리 방식과는 다른 베스트 프랙티스를 제시하는 새롭고 변화된 접근법이 필요합니다.

누가 클라우드 시스템을 노리는가

IBM Security는 IBM X-Force IRIS(Incident Response and Intelligence Services) 인시던트 대응 팀을 통해 다양한 유형의 그룹이 클라우드 시스템을 공격의 표적으로 삼고 있다는 것을 확인했으며, DarkOwl과의 협력을 통해 딥 웹과 다크 웹에서 활동하는 흥미로운 집단들에 대해서도 알게 되었습니다. IBM Security의 조사 결과에 따르면 금전적 동기를 가진 범죄자가 가장 큰 위협인 것으로 나타났지만, 국가 주도형 공격자(nation state actor) 역시 지속적인 위험 요소에 해당합니다.

클라우드 시스템을 노리는 위협 그룹 중에는 금전적 동기를 가진 범죄자가 가장 많지만 국가 주도형 공격자 역시 지속적 위험 요소에 해당합니다.

클라우드를 노리는 범죄자

X-Force IRIS 인시던트 대응 데이터에 따르면 클라우드 환경을 노리는 그룹 중 가장 자주 관찰된 공격자 카테고리는 사이버 범죄자였습니다. 금전적 동기를 가진 공격자는 특정 그룹이나 조직과 관련된 경우는 드물었으며, 기회주의적인 공격을 통해 클라우드 자산에 액세스하려고 시도하고 성공 확률을 높이기 위해 범죄 시도를 자동화하는 경우가 많았습니다. 다크넷 데이터 인텔리전스 기업인 DarkOwl과의 협력을 통해 추가 연구를 실시한 결과, 지하 세계 포럼 및 시장에서 클라우드를 겨냥한 서비스와 계정을 거래하는 시장이 번성하고 있는 것으로 나타났습니다.

지하 생태계에서 주로 거래되는 것의 예로는 인하된 가격의 클라우드 서비스 계정이 있습니다. 일례로, 러시아어로 운영되는 한 포럼에서는 벤더의 일반 판매 가격보다 저렴하게 대규모 퍼블릭 클라우드 서비스를 매월 무제한으로 이용할 수 있는 권한을 판매하고 있었습니다. 또한 다른 사례에서는 또 다른 그룹이 15달러(약 18,000원)라는 싼 가격으로 다른 대규모 퍼블릭 클라우드에 대한 액세스 키를 판매하고 있었습니다. 이러한 유형의 서비스를 통해 공격자들은 합법적으로 보이는 계정으로 악의적 활동을 위해 클라우드 인프라를 이용할 수 있습니다.

또한, 범죄자들은 클라우드에 호스팅된 특정 계정에 침투하는 것을 도와주겠다고 제안하기도 합니다. 영어와 러시아어를 사용하는 해커를 연결하는 한 플랫폼에서는 어떤 사용자가 대규모 퍼블릭 클라우드 플랫폼에서 개인 계정에 액세스하기 위한 우회 유틸리티 링크를 게시한 것도 볼 수 있었습니다. 또한 퍼블릭 클라우드 서비스 ID를 악용하는 방법에 대한 상세한 설명과 이 해커가 포럼에서 판매하려는 스크립트를 포함한 또 다른 게시글도 있었습니다. 다크 웹과 딥 웹 장소에서 볼 수 있는 또 다른 게시글에서는 클라우드 컴퓨팅 리소스를 판매하려고 했습니다. 예컨대, 피싱 사이트를 호스팅하려는 사람에게 클라우드 제공업체에 대한 액세스 권한이 판매되고 있었습니다. 한 해킹 포럼 회원이 클라우드 제공업체가 제공하는 제품을 모방하는 피싱 페이지를 퍼블릭 클라우드 환경에 호스팅하려는 계획을 설명한 사례도 관찰되었습니다.

합법적인 온라인 학습 강좌와 비슷하게, 널리 사용되는 클라우드 서비스에서 클라우드 컴퓨팅 크레딧 또는 훔친 신용카드 정보를 사용하여 계정을 연 다음 악의적 목적에 사용하는 방법을 알려주는 튜토리얼도 많이 발견됩니다.

국가 주도형 공격

국가 주도형(nation state) 공격자들은 금전적 이득과 스파이 활동 목적으로 클라우드 환경을 겨냥하는 것으로 알려져 있습니다. 위협 그룹은 연결된 제3자 시스템에 액세스하기 위해 광범위한 클라우드 환경을 노리는 경우가 많습니다.

민감한 데이터가 클라우드 환경으로 더 많이 이동하면서 스파이 활동에 중점을 두는 위협 그룹이 전략적 인텔리전스 목표를 달성하기 위해 클라우드 환경을 계속해서 표적으로 삼을 것으로 IBM은 예측합니다.

공격자는 어떻게 클라우드 환경을 침해하는가

어느 네트워크나 그렇듯이 클라우드 환경도 다양한 방법으로 공격을 받을 수 있습니다. 그 중 일부는 클라우드에 국한되지만 많은 경우 시스템 전반에 영향을 주기도 합니다.

IBM Security 위협 인텔리전스 팀은 X-Force IRIS의 인시던트 대응 데이터를 활용하여 공격자들이 클라우드 환경을 겨냥하는 가장 일반적인 방법을 알아냈습니다. 많은 경우, 공격자는 동일한 클라우드 내부, 그리고 연결되어 있을 가능성이 있는 클라우드에서 다음 중 하나 이상의 방식을 사용하여 액세스 권한을 획득, 관리, 확산 및 승격합니다.

클라우드 애플리케이션 익스플로잇

2019년 1월부터 2020년 5월까지 클라우드 환경에서 관찰된 가장 일반적인 감염 경로는 클라우드 애플리케이션에 대한 원격 익스플로잇으로, 조사한 클라우드 관련 사이버 보안 이벤트의 45%를 차지했습니다. 클라우드 애플리케이션은 민첩하고 확장 가능하다는 이점이 있지만 공격자에게 넓은 길을 열어줄 위험이 있습니다. 이러한 애플리케이션들은 비즈니스 운영상 꼭 필요한 경우가 많기 때문에 위협 활동의 주요 표적이 됩니다.

45% 클라우드 환경에 대한 원격 익스플로잇은 가장 흔하게 관찰된 감염 경로로, 조사한 클라우드 관련 사이버 보안 이벤트의 45%를 차지했습니다.

지난 2년 동안 IBM Security는 보안에 취약한 애플리케이션이 조직 내에 존재했지만 탐지되지는 않았던 경우를 여러 차례 경험했습니다. 이러한 인시던트는 클라우드의 보안이 성숙하지 않아서 발생하기도 했지만 "섀도우 IT" 때문에 발생하는 경우가 많았습니다. "섀도우 IT"란 직원이 클라우드 기능을 사용하기 위해 승인된 채널 밖에서 보안에 취약한 클라우드 애플리케이션을 사용함으로써 IT 전체 환경을 위험에 빠뜨리는 경우를 말합니다.

클라우드 환경에서 원격 취약점을 해결하는 일은 어려웠습니다. 그 이유 중 하나는 발견된 문제에 대한 공개 카탈로그가 없다는 것이었습니다. 2020년까지 클라우드 제품의 취약성은 기존 CVE 범위 밖에 있었습니다. 이는 클라우드 인프라와 관련된 취약성이 거의 공개적으로 밝혀지지 않았거나 일정 기간 동안 기록되지 않았음을 의미합니다. 그래서 클라우드 환경은 다양한 해결되지 않은 문제를 품은 채 이전에 생각했던 것보다 더 취약한 상태에 놓여있었을 수도 있습니다.

잘못된 구성에 대한 익스플로잇

IBM의 2020 X-Force 위협 인텔리전스 인덱스 데이터에 따르면, 공격자는 2019년 10억 개가 넘는 레코드를 빼돌리는 데 잘못 구성된 클라우드 서버를 활용했습니다. 클라우드 환경의 잘못된 구성과 그 후 발생하는 데이터 유출은 전반적으로 레코드 손실의 가장 큰 원인 중 하나이며 공격자는 이를 통해 조직의 민감한 정보에 액세스하고 이를 훔칠 수 있습니다. 이와 같은 실수는 클라우드 내의 자산에도 영향을 미칠 수 있습니다.

10억 개 이상의 레코드 도난

잘못 구성된 클라우드 서버로 인해 공격자는 2019년에 클라우드 환경에서 10억 개가 넘는 레코드를 빼돌렸습니다.

IBM X-Force 위협 인텔리전스 인덱스

클라우드 간 침해

공격자가 한 클라우드 환경을 감염시킨 뒤 신뢰할 수 있는 연결을 사용하여 다른 클라우드로 측면 이동한 후 추가로 환경을 감염시키는 방법으로 클라우드 환경을 침해하는 경우도 있습니다.

클라우드 환경, 특히 대규모 퍼블릭 클라우드는 많은 양의 통신이 이루어지므로 이러한 유형의 감염을 탐지하기가 훨씬 어려울 수 있기 때문에 클라우드 간 침해는 특히 은밀하게 진행될 수 있습니다.

한 X-Force IRIS 인시던트 대응 사례에서는 각기 다른 지역에 지정된 클라우드 간에 평소보다 많은 양의 데이터가 전송되는 것이 관찰되어 공격자를 탐지할 수 있었습니다. 이러한 유형의 공격을 통해 공격자는 여러 탐지 메커니즘을 피하고 자신의 활동을 일반적인 운영 활동인 것처럼 숨기면서 대규모 데이터 저장소 사이를 재빠르게 이동하여 대상 기업 전반에 해를 끼칠 수 있었습니다.

스위밍 업스트림

또 다른 유형의 감염 경로 중에, 기저 하드웨어로 가서 클라우드 저장소에 대한 특권 액세스 권한을 얻으려고 하는 공격자가 관찰되었습니다.

이 스위밍 업스트림(“swimming upstream”) 기법을 사용하는 경우 공격자는 클라우드 환경에 대한 최초 액세스 권한을 확보한 다음 기저 호스트에 액세스하고 그 후 관리 시스템으로 가서 클라우드 환경 사이를 이동합니다. 스위밍 업스트림은 공격자의 활동을 정상적인 관리 활동으로 은폐할 수 있습니다. 관리 활동 수행 시 인스턴스 사이에서 데이터를 옮겨야 하는 경우가 많기 때문입니다. 따라서 이 두 가지 활동을 구분하는 일은 복잡합니다. 이 기법은 2020년에 심각한 Perfect 10.0 취약점이 발견되었을 때 공개되었습니다. 이 결함을 통해 공격자는 클라우드 환경에서 하드웨어 기반 격리를 해제하여 코드를 가로채고 프로그램을 조작하여 동일한 하드웨어에 호스팅된 사용자 활동에 영향을 줄 수 있었습니다. 이 결함은 그 이후 수정되었습니다.

공격자는 해를 끼치기 위해 어떻게 클라우드를 이용하는가

클라우드 환경에서 해를 끼칠 수 있는 이론적 기법은 많이 있지만, IBM Security가 조사한 바에 따르면 공격자는 다양한 전통적 공격 전술을 구사하여 이 새로운 기술로부터 이득을 얻는 것으로 나타났습니다.

클라우드를 활용하여 조직에 해를 끼치는 수단으로는 랜섬웨어, 데이터 도난, 크립토마이닝(암호 화폐 채굴)이 상위를 차지했습니다. 그러나, 클라우드 환경에서 멀웨어 및 스캠 사이트를 호스팅하거나 액세스 권한을 활용하여 다른 클라우드로 파고드는 방법으로 공격자들은 조직의 범위 밖까지 더 광범위한 피해를 주면서 연결된 환경에 대한 잠재적 위험을 높였습니다.

랜섬웨어

2019년과 2020년 사이에 분석된 X-Force IRIS 인시던트 대응 사례에서 랜섬웨어는 클라우드에서 배포되는 가장 일반적인 유형의 멀웨어로 나타났으며, 다른 멀웨어보다 인시던트 수가 세 배 더 많았습니다.

랜섬웨어 사용 3배 증가

IBM 인시던트 대응 사례에 다르면 클라우드에 배포된 다른 멀웨어보다 랜섬웨어가 세 배 더 많이 사용되었습니다.

네트워크로 연결된 기존의 엔드포인트에 대한 랜섬웨어 공격과 달리 클라우드에서 랜섬웨어는 더욱 파괴적인 영향을 끼치고 더 큰 데이터 손실을 초래할 수 있습니다. 그 이유는 클라우드 환경이 지원하는 운영의 범위가 훨씬 더 넓고, 중요한 애플리케이션에 잠재적으로 영향을 미치는 데다, 날마다 클라우드를 통해 이동하는 데이터의 양이 엄청나게 많기 때문일 수 있습니다.

X-Force IRIS가 대응한 한 랜섬웨어 인시던트의 경우, 인프라 제공업체와 고객이 맡은 클라우드 관리 책임에 공백이 있었기 때문에 감염이 발생했습니다. 이러한 공백 때문에 조직에 비용을 증가시키는 침해 사실을 오랫동안 탐지하지 못했을 수 있습니다. 이 사례는 클라우드 제공업체와 고객이 수행해야 할 클라우드 보안 역할을 정의하는 것이 중요하다는 점을 보여줍니다.

데이터 절도

클라우드 환경은 대량의 정보를 보관하는데, 이러한 데이터를 공격자가 훔쳐서 암시장에서 판매할 수 있습니다. IBM X-Force IRIS가 처리한 인시던트를 통해 도난당한 데이터의 유형이 다양하다는 사실을 알 수 있었습니다. 예를 들면, 공격자가 클라우드 데이터 침해를 통해 신용카드 번호와 같은 민감한 PII를 훔친 사례가 있었습니다. 또 다른 인시던트에서는 공격자가 침해된 클라우드에서 고객 관련 이메일을 훔치려고 했었습니다.

데이터 절도는 2019년에 침해된 클라우드 환경에서 두 번째로 가장 흔하게 발생한 위협 활동이었습니다.

절도 대상 데이터의 유형은 공격자의 동기와 숙련도에 따라 다를 수 있지만, 클라우드 환경에서는 사용 가능한 데이터의 양이 훨씬 많으므로 침해의 잠재적 영향 때문에 조직에게 훨씬 더 큰 피해를 초래할 수 있습니다.

크립토마이닝(암호 화폐 채굴)

불법적인 크립토마이닝(암호 화폐 채굴) 위협의 경우, 특히 클라우드와 같은 확장된 인프라를 활용하는 위협의 경우, IBM X-Force IRIS는 지난 1년 동안 공격자가 클라우드 환경을 사용하여 암호화폐를 얻기 위해 마이닝하는 사례를 여러 건 볼 수 있었습니다.

2019년 한 사례에서 X-Force IRIS는 크립토마이너가 클라우드를 감염시킨 뒤 연결된 시스템으로 감염을 측면으로 확산하려고 시도한 인시던트에 대응했습니다. 이러한 종류의 침해는 몇 가지 영향을 줄 수 있습니다. 온프레미스 클라우드 환경의 경우 조직에 전력 비용이 증가할 수 있으며 하드웨어 구성요소의 질이 더 빨리 저하될 수 있고 성능에도 영향이 있을 수 있습니다. 성능 저하는 금융 부문 등의 산업 분야에 중대한 문제를 초래할 수 있습니다.

외부/퍼블릭 클라우드를 사용하는 조직은 데이터 사용량이 증가하여 비용이 증가되거나 처리 성능이 저하되어 대응 시간이 느려질 수 있습니다. 모든 경우, 크립토마이닝(암호 화폐 채굴)은 조직의 리소스를 고갈시켜 비즈니스 운영을 방해할 수 있습니다.

멀웨어 또는 악의적 사이트 호스팅

공격자들은 감염된 클라우드 환경을 활용하여 다른 환경으로 확산될 수 있는 멀웨어를 호스팅할 수 있습니다. 예를 들면, 2019년 후반에 범죄자들이 클라우드 플랫폼에 호스팅하고 있던 결제 카드 스키머가 표적으로 삼은 시스템에 다운로드된 적이 있습니다. 또 다른 사례에서는 공격자가 한 클라우드 인스턴스에서 200개 이상의 기술 지원 사기 사이트를 호스팅하여 사용자를 이 사이트로 유인하였고 클라우드 환경을 사용하여 공격이 정상적인 활동인 것처럼 보이게 했습니다.

클라우드 환경에 멀웨어 또는 악의적 사이트를 호스팅하면 공격자는 정당한 인프라에 대한 콜아웃처럼 위장하여 네트워크 차단을 피할 수 있습니다. 또한, 클라우드 호스팅을 사용하면 공격자가 추상화 계층을 활용할 수 있으므로 공격 활동을 추적하기가 더 어려워집니다. 조직이 클라우드에 멀웨어를 호스팅하고 있다는 사실을 특히 오랜 기간 동안 모르고 지내면 데이터를 잃는 것뿐만 아니라 이러한 공격 활동이 지속되도록 방치했다는 비난까지 받을 수 있으므로 직접적인 피해 외에 평판도 훼손될 수 있습니다.

DNS 침해

IBM X-Force IRIS는 공격자가 직원을 다른 사이트로 유도하기 위해 클라우드에 호스팅된 DNS 서비스를 침해한 여러 사례를 발견했습니다.

DNS 캐시 포이즌 개념을 활용하는 이 은밀한 공격 방법은 기존 클라우드 액세스를 활용하여 조직에 추가적인 해를 끼치며 사용자가 탐지하기 어려울 수 있습니다. 이러한 유형의 침해는 브라우저를 악용하여 악성 페이로드를 엔드포인트 시스템에 심으려고 하는 사이트로 사용자를 유도하거나 네트워크 자격증명(credential)을 훔치기 위한 피싱 사이트로 유도할 수 있습니다. 또는, 범죄자의 주머니를 불려 주기 위해 설정된 광고 또는 클릭 사기로 사용자를 유도할 수도 있습니다.

DNS 침해는 새로운 공격 방식은 아니지만 이러한 서비스가 외부 클라우드 제공업체로 계속 이동되고 있으므로 공격자는 침해를 위한 새로운 통로를 찾을 수 있고 그 영향이 조직 전체로 퍼질 수 있습니다.

측면 확산

공격자는 최초 감염을 클라우드 환경의 다른 부분 또는 클라우드 리소스에 액세스하는 엔드포인트 박스로 확장하기 위해 다양한 방법을 사용합니다. 2019년, IBM X-Force IRIS는 클라우드 환경에 배포된 멀웨어가 SSH 무차별 대입 공격(bruteforcing)을 통해 다른 시스템으로 이동하여 클라우드에 액세스하는 외부 로컬 시스템에 영향을 주려고 한 인시던트에 대응한 적이 있습니다.

또한, 2019년에는 Exim 서버를 통해 확산되는 Linux 웜인 Exim 웜이 CVE 2019-10149를 원격 익스플로잇 공격을 통해 자동으로 감염을 확산시키는 것으로 보고되었습니다. 이 웜은 크립토재킹 멀웨어를 서버에 심으려는 목적으로 서버를 공격합니다.

이러한 유형의 측면 확산은 클라우드 감염 피해를 악화시키고 조직의 내부 네트워크 공간도 감염시킬 수 있습니다.

진화하는 클라우드 네이티브 멀웨어

다수의 클라우드 기반 시스템들이 온프레미스 시스템과 동일한 운영 체제와 애플리케이션을 실행합니다. 따라서, 클라우드 환경에서 실행되는 많은 멀웨어는 클라우드 밖의 멀웨어와 동일합니다. 그러나, 클라우드 시스템을 겨냥하거나 활용하도록 특별히 설계된 멀웨어에 관한 사례도 있습니다.

> 이러한 멀웨어의 종류는 세 가지로 분류할 수 있습니다.
>
> — 클라우드를 사용하여 확장하는 멀웨어
>
> — 클라우드 환경에 맞게 적응하는 멀웨어
>
> — 운영 인프라로 클라우드 환경을 이용하는 멀웨어

클라우드를 사용하여 확장하는 멀웨어

멀웨어 운영자는 특정 클라우드 애플리케이션 또는 플랫폼을 겨냥하여 한 번의 침해만으로 빠르게 연산 작업을 늘려 상당한 이익을 얻을 수 있습니다. 새로운 클라우드 환경에 적응하는 멀웨어의 한 예는 2018년 10월에 보고된 Linux 기반 봇인 DemonBot입니다. DemonBot은 Hadoop을 실행하는 클라우드 서버를 겨냥하며 Hadoop의 리소스 관리 툴을 통해 이러한 서버를 감염시킵니다.

X-Force IRIS는 피해를 입은 조직이 공공 요금과 리소스 사용량이 급증한 것을 의심하다가 클라우드 환경에서 DemonBot을 찾아낸 사례를 조사한 적이 있습니다. 이 경우 DemonBot 바이너리의 주요 기능은 분산 서비스 거부 공격(distributed denial of service, DDoS)을 봇넷의 일부로서 실행하는 것입니다. 클라우드 타게팅 기능이 추가되면서 멀웨어 오퍼레이터는 클라우드 리소스를 사용하여 이러한 공격을 증폭시킬 수 있습니다.

조직의 클라우드 채택을 악용한 것으로 밝혀진 또 다른 멀웨어는 2019년 10월 발견된 크립토마이닝(암호 화폐 채굴) 웜인 Graboid입니다. 이 멀웨어는 보안이 적용되지 않은 Docker 호스트를 겨냥하여 침해했고 이 호스트에 악성 Docker 컨테이너를 다운로드했습니다. 이 악성 컨테이너는 크립토마이닝(암호 화폐 채굴)을 수행하고 이 멀웨어를 다른 호스트로 확산시켰습니다.

2019년 6월에는 연구자들이 잘못 구성된 Docker(도커) 호스트를 침입하기 위해 이를 겨냥한 공격 캠페인에 대해 보고했습니다. 이 사례에서 잘못된 API 구성을 악용하여 취약한 컨테이너에 멀웨어를 배포한 것은 AESDDoS라고 알려진 Linux 봇넷 멀웨어였습니다. 그 다음, 이 멀웨어는 명령 제어 서버로부터 명령을 받아서 다양한 DDoS 공격을 실행할 수 있었습니다.

클라우드 환경에 맞게 적응하는 멀웨어

지난 2년 동안 Intezer의 연구자들은 주로 클라우드 환경에서 Linux 서버를 겨냥하는 사이버 공격이 상당히 증가했음을 알게 되었습니다. Linux 운영 체제는 모든 클라우드 서버의 거의 90%에서 사용됩니다.

클라우드를 겨냥하기 위해 멀웨어를 사용하는 공격자의 한 예는 중국계 Pacha Group입니다. 이 그룹은 이전에 탐지된 적이 없는 새로운 Linux.GreedyAntd 멀웨어 변종으로 클라우드 기반 인프라를 표적으로 삼아왔습니다. 이 멀웨어 변종은 이전 변종과 상당량의 코드를 공유합니다. 클라우드 환경에서 Linux 기반 파일 스토리지 시스템(NAS 서버)을 겨냥하는 또 다른 멀웨어는 QNAPCrypt 랜섬웨어입니다. 이러한 종류의 위협은 매우 넓은 사용자층에 영향을 주고 클라우드에 호스팅된 엄청난 양의 데이터에 피해를 줄 수 있습니다.

클라우드 환경의 인기가 계속 증가함에 따라 Linux 중심 멀웨어도 계속 증가할 것으로 보입니다.

운영 인프라로 클라우드 환경을 이용하는 멀웨어

조직이 운영을 확장하는 만큼 멀웨어 배포자, 특히 조직 범죄 및 국가 주도형 공격과 관련된 멀웨어 배포자도 운영을 확장할 수 있습니다. X-Force IRIS의 조사에 따르면 공격자들은 다양한 방법으로 멀웨어 운영을 위해 클라우드 환경을 활용하는 것으로 나타났습니다.

한국의 피해자를 겨냥한, ITG10(AKA APT 37, Scarcruft)의 원격 액세스 툴(Remote Access Tool, RAT)인 RokRat에 대한 한 조사에 따르면 이 툴은 페이로드와 C2(커맨드 앤 컨트롤) 통신 호스팅을 위해 적법한 상용 클라우드 스토리지 서비스를 이용한 것으로 확인되었습니다. 조직의 네트워크에서는 정상적인 운영 활동의 일환으로 상당한 클라우드 통신이 이루어지고 적법한 화이트리스트 제공업체를 이용할 수 있으므로 인프라를 위해 이와 같은 방식으로 클라우드 서비스를 사용하면 탐지하기가 어려울 수 있습니다. 이러한 종류의 클라우드 환경에서 멀웨어를 호스팅하면 악성 페이로드 다운로드를 탐지하는 일도 더욱 어려워질 수 있습니다.

RokRat과 매우 유사한 Karae도 ITG10의 또 다른 백도어입니다. Karae 역시 C2 통신을 위해 클라우드 스토리지 제공업체를 이용하는 것으로 알려져 있습니다. X-Force IRIS가 분석한 Karae 샘플에서는 공격자가 멀웨어를 호스팅하기 위해 적법한 클라우드 스토리지 서비스 제공업체를 이용했으며 계정 자격증명(credential)은 멀웨어의 바이너리에 하드코딩되어 있는 것으로 밝혀졌습니다. Karae는 피해자의 시스템에 대한 정보를 수집하여 파일에 쓴 후 클라우드에 업로드합니다. 또한, Karae는 이 서비스로부터 추가 바이너리를 다운로드하여 실행을 시도합니다.

이 전술은 정상적이고 적법한 사용자 활동과 섞일 수 있으므로 탐지가 힘듭니다. 이러한 이유로 다양한 동기를 가진 멀웨어 운영자가 이 전술을 사용합니다.

클라우드 보안 향상을 위한 권장사항

클라우드 환경에서 보안 인시던트에 대응하려면 일반적인 인시던트 대응 방법 외에 특별히 고려해야 할 사항이 있습니다. X-Force IRIS가 이 분야에서 쌓은 광범위한 경험을 바탕으로 클라우드 인시던트에 대비하고 대응하면서 얻은 교훈을 몇 가지 모아봤습니다.

더 안전한 클라우드 환경 준비

목적을 염두에 두고 시작

워크로드나 데이터를 클라우드로 옮기는 것을 고려하기 전에 그 목적과 관련된 계획을 세우십시오. 개념 수립 과정에서부터 보안을 염두에 두고 클라우드에서 실행되는 운영 작업의 중요도와 민감도를 고려하십시오. 프로그램을 개발하면서 하이브리드 클라우드 보안의 모든 측면을 파악하고 통제할 수 있도록 포괄적인 보안 서비스를 제공하는 파트너를 이용하는 것을 고려하십시오.

선제적 시뮬레이션 활용

효과적으로 준비를 마쳤는지 확인하기 위해 클라우드 환경 내에서 예측되는 보안 이벤트와 예측하지 못한 보안 이벤트를 모두 시뮬레이션해 보십시오. 이렇게 준비하면 내부 플레이북과 표준 운영 절차를 연습해 볼 수 있는 기회가 생깁니다. 기술적, 운영적 대응 스킬을 테스트하고 향상하는 데 중점을 두면 피해가 발생하거나 확산되기 전에 문제 해결을 위한 조치를 신속하게 취할 수 있습니다. 또한, 이러한 연습은 위협 인텔리전스 기반 대응 시나리오를 지원하기 위해 침해 지표(Indicators of Compromise, IOC)와 같은 전술 정보를 이용하여 강화할 수 있습니다.

정책 "사각지대" 방지

외부 클라우드의 경우 클라우드 환경 보호의 책임은 해당 조직과 클라우드 호스팅 제공업체 모두에게 있는 경우가 많습니다. 클라우드 호스팅은 한 번 설정하면 관리가 필요하지 않은 서비스가 아니므로 클라우드 서비스 제공업체와 서비스를 이용하는 조직 모두가 보안에 신경을 써야 합니다. 계약 내용을 협상할 때 각 당사자의 역할을 상세하게 기술하면 인시던트가 발생하기 전에 책임, 관리 사항, 모니터링, 잠재적 법적 책임을 정의하는 데 도움이 될 수 있습니다. 이렇게 하면 정책 공백으로 인한 인시던트를 예방하는 동시에 더 효율적으로 인시던트를 탐지하고 대응할 수 있습니다.

클라우드 보안에 베스트 프랙티스 적용

클라우드 보안의 경우 나름의 접근법이 있기는 하나, 어떤 측면에서는 그 접근법이 다른 네트워크의 보안 접근법과 유사합니다. 클라우드도 침해의 대상이 될 수 있으므로 조직은 클라우드 환경에 보안 베스트 프랙티스를 적용해야 합니다. 무단 액세스 위협을 완화하기 위해서는 다단계 인증을 사용하면 도난당한 자격 증명을 사용한 침입을 방지하는 데 도움이 됩니다.

특권 계정 관리(Privileged Account Management, PAM)도 클라우드 보호를 향상하기 위한 중요한 개념입니다. 계정 침해로 인한 피해를 최소화하기 위해 계정에 최소 권한만을 허용하고 제로 트러스트 모델의 사용을 고려하십시오. 클라우드 환경에서 이러한 지침을 따르면 인시던트 발생 위험을 완화하거나 발생 가능한 보안 이벤트의 영향을 줄일 수 있습니다.

모니터링 및 기록

클라우드 환경을 모니터링해야 할 이유는 많습니다. 클라우드의 무분별한 확장부터 제3자 액세스 및 예상하지 못한 운영 중단까지, 적절한 모니터링을 통해 멀웨어와 공격의 최초 징후를 탐지할 수 있습니다. 클라우드 사용자는 악의적인 활동에 대한 포렌식 조사를 수행하기 위해 클라우드 환경의 이벤트를 철저히 기록해야 합니다. 정책 사각지대를 방지하기 위해 서비스를 시작하기 전에 해당 조직과 클라우드 호스팅 제공업체는 클라우드 이벤트 모니터링 및 기록에 대한 책임을 규정해야 합니다.

위협 인텔리전스를 사용한 위협 모니터링

공격자들은 계속 진화하고 있으며 클라우드 환경을 겨냥하기 위한 새로운 기능으로 기존의 무기고를 강화하고 있습니다. 이러한 기능이 계속 발전되고 있으므로 조직은 위협 인텔리전스를 활용하여 타겟 활동의 변화를 모니터링하고 효과적으로 방어해야 합니다.

클라우드 보안 인시던트에 대한 효과적 대응

리이미징보다는 재배포

클라우드 인스턴스를 종료하면 조직은 매우 큰 가치가 있을 수 있는 포렌식 아티팩트를 잃게 됩니다. 이 데이터를 즉시 파괴하는 대신 피해를 입은 시스템을 격리하고 알려진 깨끗한 이미지를 작동시키면 포렌식 조사관이 감염된 인스턴스를 분석하여 문제점과 향후 이를 예방하는 방법을 파악하는 데 도움이 되는 추가적인 단서를 찾을 수도 있습니다.

인시던트의 경우, 조사관이 작업을 수행할 수 있는 워크스테이션을 클라우드에 구축한 다음 침해당한 서버의 이미지를 만들고 휘발성 메모리 데이터를 수집하십시오. 또한, 근본 원인에 대한 포렌식 분석을 수행하면 IT 관리자가 오염된 베이스 이미지를 재배포하지 못하도록 할 수 있습니다.

대역폭 비용 기억하기

오늘날 조직이 직면하는 과제는 클라우드 환경에서 데이터를 이동하는 것과 관련된 높은 대역폭 비용으로 인해 인시던트 발생 후 대용량 서버 이미지를 다운로드하는데 막대한 비용이 발생할 수 있다는 것입니다. 인시던트 발생 전에 관련 정책 또는 요구사항을 마련하면 다운로드 비용을 줄이는 데 도움이 될 수 있습니다. 특히, 감염이 같은 클라우드에 있는 다른 인스턴스에 악영향을 줄 수 있는 경우 그러합니다.

적합한 조사 툴 보유

문제가 발생할 경우 클라우드 보안을 유지하려면 철저한 조사를 수행하기에 적합한 툴이 필요합니다. 일반적인 인시던트 대응 툴과 포렌식 툴은 로컬 환경 또는 온프레미스 호스팅 서버에서만 유용하고 클라우드 환경에는 사용할 수 없는 경우가 많습니다. 그러나, 적합한 툴킷을 마련하면 효과적으로 클라우드를 조사할 수 있습니다.

또한, 조직은 전반적인 인시던트 대응 계획에 클라우드 자산을 포함하고, 조직이 사용하는 모든 클라우드 환경에서 툴이 작동하도록 클라우드 보안 인시던트 대응을 전술적 수준에서 테스트해야 합니다.

인시던트 대응 자동화

클라우드 환경에서 효과적으로 보안을 자동화하면 이벤트에 수동으로 대응하는 대신 탐지 및 대응 능력을 향상할 수 있습니다. 예를 들면, IaC(Infrastructure as Code) 접근법을 따르고 선언적 접근법인 CloudFormation 및 서버리스 이벤트 기반 Lambda 서비스와 같은 툴을 사용하면 침해를 당한 조직은 사전 정의된 템플릿으로 환경을 효율적으로 재구축할 수 있습니다. 이러한 방법을 통해 환경에 대한 랜섬웨어 또는 파괴적 사이버 공격 발생 시 복구 속도를 향상할 수 있습니다.

결론

벤더와 인프라 사용 계약을 맺는 경우, 클라우드 보안은 제공업체와 클라우드 서비스 사용자 모두가 공동의 노력을 기울여 지켜야 합니다. 클라우드를 기반으로 운영되는 조직이 데이터와 서비스의 보안을 적절히 유지하려면 클라우드 환경에 대한 위협을 알고 있어야 합니다.

IBM X-Force 연구에 따르면 공격자들은 클라우드 인프라로 이동하는 조직을 빈틈없이 파악하고 있으며 그에 따라 진화하고 있는 것으로 나타났습니다. 클라우드 침해 비용이 계속 증가하고 있으므로 조직은 클라우드 기반 자산을 보호하기 위해 조치를 취해야 합니다. 선제적으로 대응하고 권장사항을 따르면 클라우드 기반 환경으로 이동하면서도 더욱 효과적으로 스스로를 보호할 수 있습니다.

IBM X-Force 소개

IBM X-Force는 최신 보안 위협을 모니터링하고 연구하면서 고객 및 일반 대중에게 새로운 위협 및 중대한 위협에 대해 알리고 IBM 고객을 보호하기 위한 보안 콘텐츠를 제공합니다. 인프라, 데이터, 애플리케이션 보호는 물론 클라우드 및 보안 관제 서비스까지 제공하는 IBM Security Services는 전문성을 바탕으로 고객의 중요 자산을 지키도록 돕습니다. IBM Security는 세계에서 가장 정교한 네트워크를 보호할 뿐만 아니라 비즈니스 분야를 대표하는 권위자들과 함께합니다.

IBM X-Force IRIS에 대해 알아보기

각주

1. 방법론에 대한 고지: 이 보고서에 언급된 통계는 2018년 6월부터 2020년 3월까지 X-Force IRIS 인시던트 대응 보고서의 일부 내용을 기반으로 합니다. 개인정보 보호 문제를 포함한 다양한 이유 때문에 이러한 제한을 두어야 했습니다. 따라서, 이 보고서에 포함된 통계는 이 기간 동안 관찰된 더 넓은 범위의 클라우드 보안 트렌드를 반영하고 있지만 수집 편향의 영향이 어느 정도 있을 수 있습니다.

IBM Security

Contributed research

Intezer
DarkOwl

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
2020년 5월

IBM