슈퍼 하이웨이 공격

악성 DNS 트래픽 심층 분석

Akamai

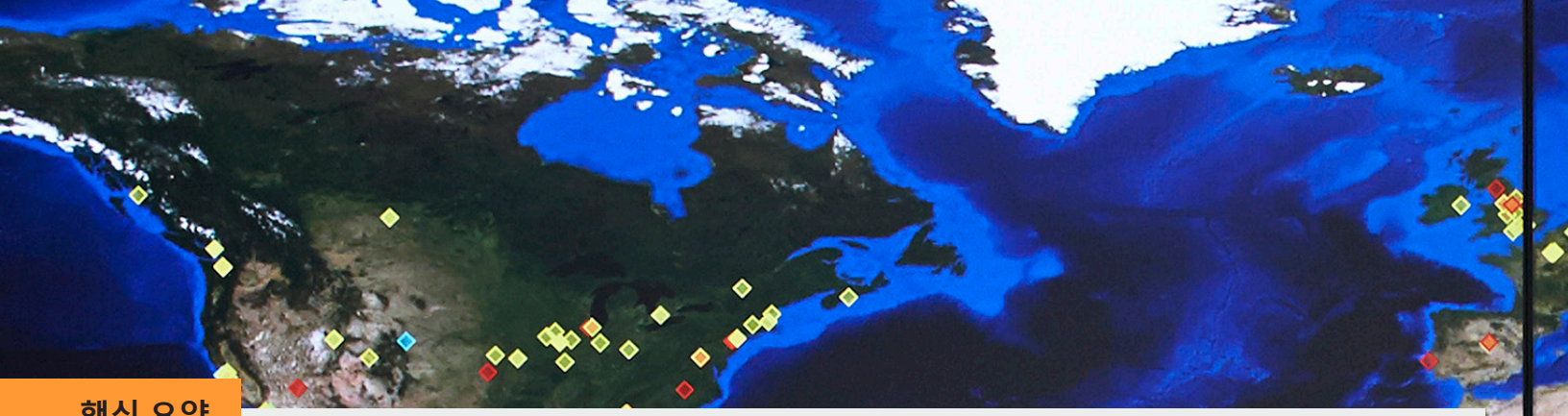
목차

도메인 네임 서버 - 공격 트래픽 하이웨이

DNS(도메인 네임 시스템)는 초창기부터 인터넷 인프라에서 중요한 부분을 차지해 왔습니다. 가정 또는 직장에서 인터넷을 사용할 때 대부분 WWW(월드 와이드 웹)에서 목적지로 정확하게 이동하려면 DNS를 통한 지원을 받아야 합니다. 따라서 공격자가 명령 및 제어(C2) 서버에 접속해 명령을 기다리는 위협 활동이나 도메인에 도달해 악성 파일을 머신에 다운로드하는 원격 코드 실행 등의 공격에 DNS 인프라를 활용한다는 사실은 놀랍지 않습니다. DNS는 많이 사용되는 특성 때문에 공격 인프라의 중요한 부분으로 자리 잡았습니다.

Akamai는 보안 기업으로서 시스템 감염 및 정보 도난으로 이어질 수 있는 악성 DNS 트래픽으로부터 기업뿐만 아니라 개인 사용자도 분석하고 보호할 수 있는 위치에 있습니다. 이 보고서에서는 전 세계 개인 사용자 및 기업을 표적으로 하는 악성 트래픽에 대한 분석을 제공합니다. 공격자 그룹 또는 툴과의 상관관계를 포함해 악성 DNS 트래픽을 철저히 분석하면 가장 빈번하게 발생하는 위협에 대한 중요한 정보를 기업에 제공할 수 있습니다. 따라서 이러한 정보는 보안 실무자가 방어 체계를 평가하고 DNS 악용에 대응하는 기술과 방법을 획득하기 위해 격차 평가를 진행하는 데 도움이 될 수 있습니다. 그렇게 하지 않으면 대외비 데이터 유출, 금전적 손실, 컴플라이언스 위반으로 인한 벌금 부과 등의 피해를 입을 수 있습니다. 2025년까지 사이버 범죄 비용이 매년 10조 5천억 달러에 이를 것으로 예상되는 상황에서 기업은 공격이 발생하기 전에 대비해야 합니다.

Akamai는 기업 및 개인 사용자의 악성 DNS 트래픽을 분석했고, 국가 간 이동하는 Android 기반 멀웨어인 FluBot의 확산, 기업을 표적으로 삼는 다양한 사이버 범죄 그룹의 유행 등 여러 악성 활동 및 캠페인을 포착할 수 있었습니다. 이를 가장 잘 보여주는 사례는 IAB(초기 접속 브로커, Initial Access Broker)와 관련된 C2 트래픽이 상당량 존재한다는 것이었습니다. IAB는 RaaS(Ransomware as a Service) 그룹처럼 기업 네트워크에 침투해 접속 권한을 다른 사람들에게 판매함으로써 수익을 거둡니다. Akamai는 이러한 활동을 정보의 고속도로라고 할 수 있는 DNS에서 관측할 수 있었으며, 독자 여러분을 위해 이를 공유하고자 합니다.



핵심 요약

당사 데이터에 따르면, 모든 분기에 10%~16%의 기업이 네트워크에서 C2 트래픽을 관측했습니다. C2 트래픽이 존재한다는 것은 공격 또는 유출이 진행 중이라는 것을 의미하며 정보를 훔치는 봇넷부터 IAB까지 다양한 위협이 있습니다.

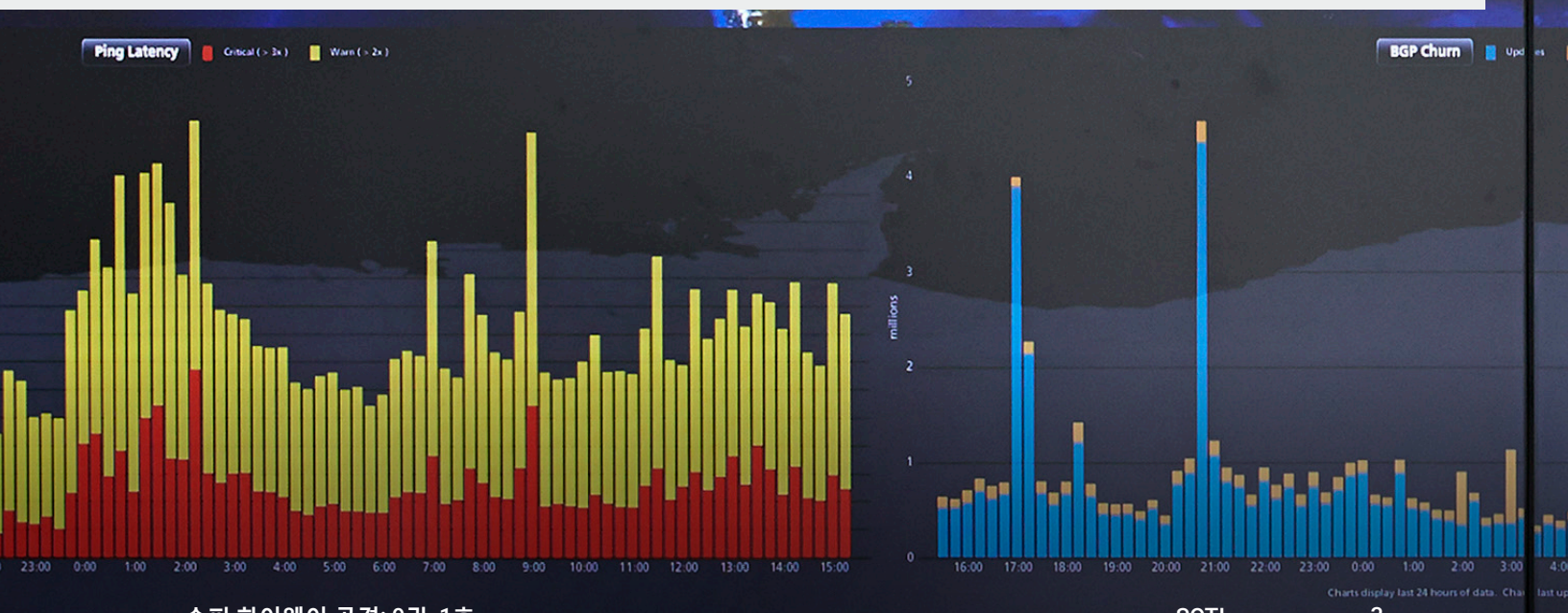
감염된 디바이스 중 26%가 Emotet 및 QakBot 관련 도메인을 포함해 알려진 IAB C2 도메인에 접속했습니다. IAB는 최초 유출을 일으키고 랜섬웨어 그룹 및 기타 사이버 범죄 그룹에 접속권을 판매하기 때문에 기업에 상당한 리스크를 초래합니다.

NAS(Network-Attached Storage) 디바이스는 패치될 가능성은 작고 가치 있는 데이터를 보유하고 있을 가능성은 높기 때문에 악용되기 쉽습니다. Akamai의 데이터에 따르면, 공격자가 QSnatch를 통해 NAS 디바이스를 악용하고 있으며, 기업 네트워크에서 감염된 디바이스 중 36%가 이 위협과 관련된 C2 도메인에 접속하는 것으로 나타났습니다.

감염된 기업의 30%가 제조업계에 속해 있으며, 이는 두 번째로 많이 감염된 업계보다 2배 높은 수치입니다. 여기에서 공급망 문제, 일상생활 중단과 같은 사이버 공격이 실제로 미치는 영향이 확연하게 드러납니다. Network and Information Security 2 (NIS2)와 같은 규정은 제조업과 같은 필수 업종 또는 중요 인프라에 대한 공격을 억제하는 데 도움이 될 수 있습니다.

공격자는 컴퓨터 같은 기존의 디바이스뿐만 아니라 휴대 전화와 IoT(Internet of Things) 디바이스도 악용하려고 합니다. 상당한 양의 공격 트래픽이 모바일 멀웨어 및 IoT 봇넷과 관련되어 있습니다.

DNS 데이터 분석을 통해 유럽, 중동, 아프리카(EMEA), 라틴 아메리카(LATAM), 아시아 태평양 및 일본(APJ)에서 FluBot 멀웨어가 급증하는 것을 확인했습니다. 멀웨어의 소셜 엔지니어링 기법 및 여러 EU(유럽 연합) 언어 사용은 감염 증가의 원인이 될 수 있습니다.



Akamai DNS 트래픽 분석 용어

Akamai Edge DNS 및 DNS Infrastructure에서는 매일 최대 7조 건의 DNS 요청을 관측합니다. Akamai는 사용자와 기업을 보호하기 위해 정보를 훔칠 수 있는 멀웨어 또는 사이트를 제공하는 도메인으로 연결되는 요청을 차단합니다. 또한 악성 DNS 트랜잭션을 조사함으로써 이런 도메인을 멀웨어, 피싱 사이트, C2의 세 가지 범주로 분류하고 기업 및 개인 사용자에 대한 오늘날의 가장 큰 위협을 파악하기 위해 심층 조사를 진행합니다.

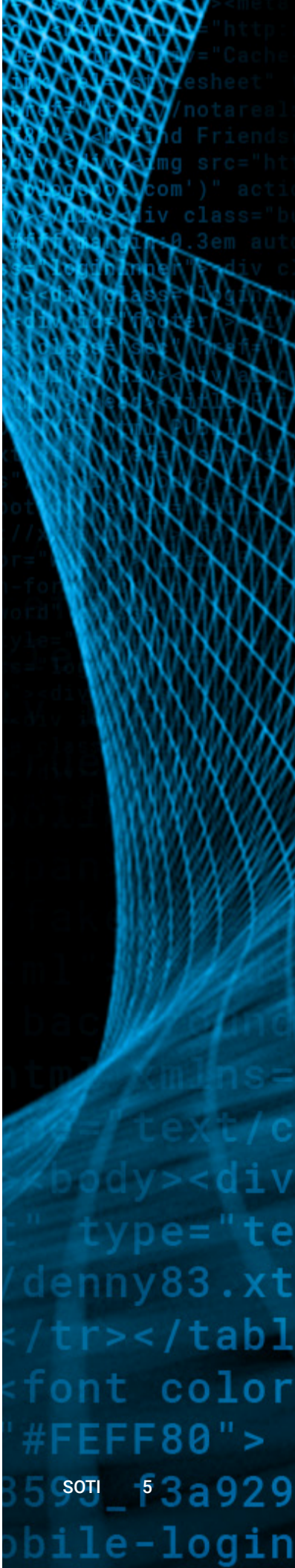
악성 DNS 트래픽 데이터를 신중하게 샘플링함으로써 가장 빈번하게 발생하는 위협에 대해 중요한 결론을 내릴 수 있습니다. Akamai는 2개의 집단을 보호합니다. 첫 번째는 기업입니다. Akamai는 기업 네트워크를 보호합니다. 두 번째는 개인 사용자입니다. Akamai는 개인 네트워크를 통해 인터넷에 접속하는 가정 내 인터넷 사용자를 보호합니다. 이들은 암호화폐 채굴을 통한 금전적 이득과 같은 악의적인 목적으로 디바이스에 침투하려고 하는 봇넷과 같은 위협에 노출되어 있습니다.

먼저 '피싱 사이트', '멀웨어', 'C2'라는 용어를 정의하고 이 용어를 이 보고서에서 어떻게 사용하는지 설명하겠습니다.

피싱 사이트는 사용자가 인증정보 및 개인 식별 정보(PII)와 같은 정보를 유출하도록 유도하기 위해 리테일 기업, 은행, 하이테크 기업 등의 외관이나 느낌을 모방하고 복제하는 피싱 키트에 연결된 도메인입니다. Akamai는 DNS를 통해 이런 트래픽을 관측하고 기업 및 가정 내 사용자를 ID 도용 및 정보 유출로부터 보호합니다.

멀웨어는 악성 파일을 제공하거나 포함하는 악성 도메인입니다. 이 카테고리에는 악성 자바스크립트를 호스팅하는 사이트 및 원치 않는 광고를 제공하거나 이러한 광고가 포함된 페이지로 사용자를 리디렉션하는 감염된 웹 사이트도 포함됩니다. 대부분의 최신 공격은 초기 페이로드를 위해 외부 소스에서 디바이스로 악성 파일을 다운로드하거나 진행 중인 공격의 다음 단계를 다운로드해야 합니다. 이 트래픽을 관측하고 차단하면 초기 감염 또는 진행 중인 공격으로부터 기업을 보호할 수 있습니다.

C2는 DNS 트래픽 분석 측면에서 감염된 디바이스와 통신해 명령을 보낸 다음 디바이스를 제어하는 데 사용되는 도메인입니다. 공격자는 초기 감염 후 감염된 시스템과 공격자가 제어하는 서버 간에 C2 통신을 설정해 다른 멀웨어의 다운로드 및 확산, 데이터 유출, 시스템 종료 및 재부팅 등의 추가 명령을 보내며, 이에 따라 시스템 또는 네트워크의 보안을 추가적으로 침해합니다. C2 트래픽을 탐지하는 것은 매우 중요합니다. 아직 방어할 수 있는 진행 중인 공격을 파악할 수 있기 때문입니다. 또한 C2 서버와 연결된 도메인을 차단하면 C2 통신이 만들어지지 않으며 멀웨어가 추가 안내사항이나 명령을 다운로드하지 못하게 되기 때문에 공격자가 네트워크에서 악성 활동을 진행할 가능성이 줄어듭니다.



미래의 위협: 기업에 만연한 악성 트래픽

Akamai의 DNS 트래픽 분석 결과를 바탕으로 31%의 디바이스가 2022년 4분기에 멀웨어와 연결된 도메인에 1회 이상 접속을 시도한 것을 확인했습니다(그림 1). 또한 6%의 디바이스는 피싱과 관련된 도메인과 통신했습니다. 본 보고서에서 중점적으로 살펴볼 C2 부분은 1년 내내 증가 트렌드가 이어졌으며, 4분기에는 소폭 감소했습니다.

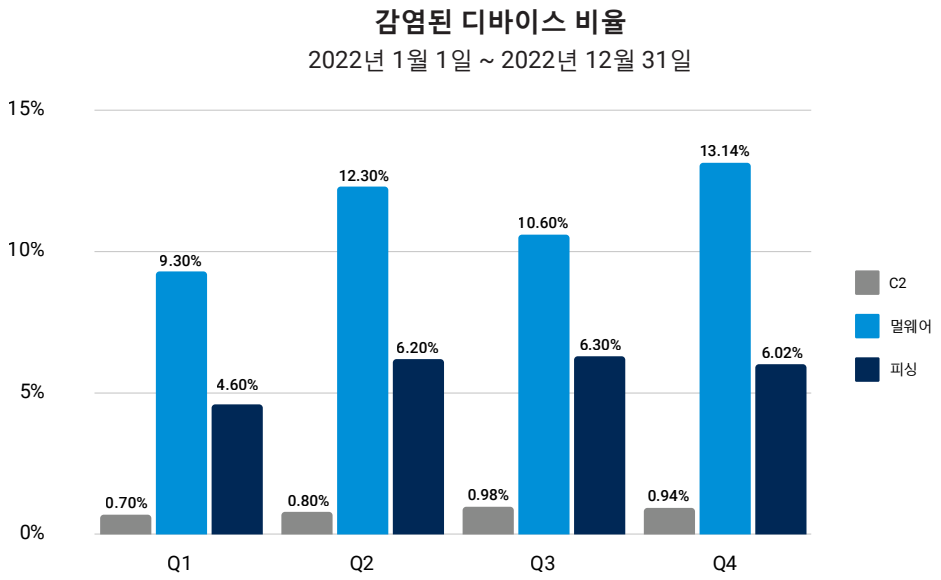


그림 1: 악의적인 목적지로 접속하려는 보안 디바이스가 점차 증가하고 있습니다.

그림 1은 악성 도메인과 통신을 시도한 개별 디바이스만 보여줍니다. 멀웨어에 도달하는 디바이스와 C2 도메인에 도달하는 디바이스의 차이점을 지적하는 것이 중요합니다. 전자는 멀웨어를 다운로드하는 공격자가 사용할 수 있고, 후자는 진행 중인 공격 중에 공격자와 멀웨어 간의 통신을 지원하기 위해 일반적으로 사용되고 공격 주기를 늘리기 위해 추가 멀웨어를 다운로드하는 데 사용될 수 있습니다. 이러한 차이는 머신에 멀웨어를 처음 다운로드할 때 차단될 수 있는 네트워크 침투 시도와 Akamai 데이터에 따르면 DNS를 통해 이동하지 않았을 수 있는 성공적인 침투 또는 진행 중인 공격(C2 도메인에 도달하여 공격 수행)과의 차이를 나타낼 수 있습니다.

이 보고서는 주로 공격자가 디바이스에 성공적으로 침투한 인스턴스의 잠재적인 지표가 될 수 있는 C2 트래픽을 집중적으로 살펴봅니다. 이러한 공격이 얼마나 만연해 있는지 파악하려면 데이터를 다른 시각으로 살펴봐야 합니다. 개별 디바이스를 살펴보는 대신 기업별로 데이터를 집계해 데이터 세트 내에서 진행 중인 공격(C2 트래픽의 존재로 파악)이 얼마나 자주 나타나는지 조사할 수 있습니다.

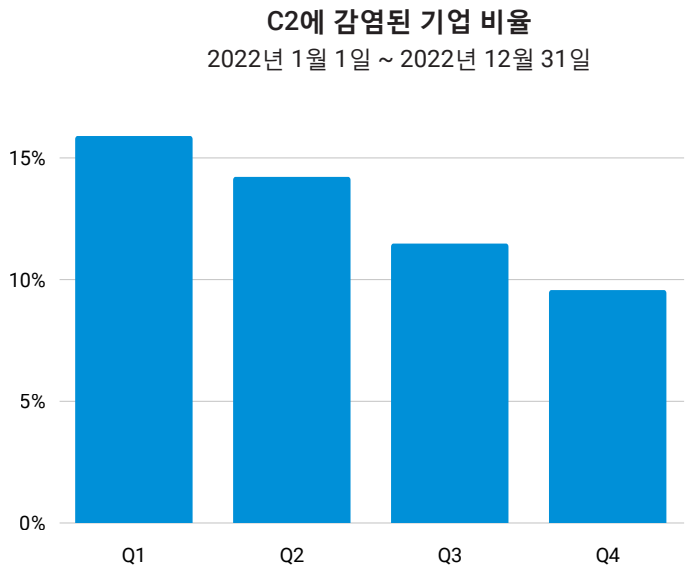


그림 2: 악성 C2 트래픽을 분석한 결과, 1년 동안 최소 한 대 이상의 디바이스가 C2 도메인에 도달한 기업의 비율을 파악할 수 있었습니다.

> **DNS 데이터에 따르면 10%~16%의 기업이 모든 분기에 네트워크를 빠져나올 때 C2 트래픽이 관측되는 인스턴스를 최소 1회 이상 경험했습니다.**

DNS 데이터에 따르면 10%~16%의 기업이 모든 분기에 네트워크를 빠져나올 때 C2 트래픽이 관측되는 인스턴스를 최소 1회 이상 경험했습니다(그림 2). 이는 운영자와 통신을 시도하는 멀웨어를 의미할 수 있으며 잠재적으로 유출의 신호일 수 있습니다. 이 C2 트래픽은 Akamai의 솔루션 덕분에 목적지에 도달하지 못하도록 차단되었지만, 공격이 성공했다면 데이터 탈취, 랜섬웨어 공격 등이 발생했을 수도 있습니다. 2022년 상반기 현재 23억 종의 멀웨어 변종이 탐지되었는데 매일 평균 1501종이 발견된 셈입니다. Akamai 리서치에서는 네트워크에서 멀웨어가 공격을 진행하거나 피해를 일으키지 않도록 방지하기 위해 DNS를 활용할 때의 효과를 중점적으로 다룹니다.

기업에 폭넓은 위협을 일으키는 IAB

오늘날 공격 환경에서는 다단계 공격이 거의 항상 나타납니다(그림 3). 공격자들은 서로 협력하거나 다른 공격자를 고용할 때, 아니면 단일 공격에 다양한 툴을 결합할 수 있을 때 높은 공격 성공률을 기록하고 있습니다. C2는 이러한 공격 성공에 중추적인 역할을 합니다. C2는 통신뿐만 아니라, 페이로드와 다음 단계 멀웨어를 다운로드하도록 지원해 공격을 발전시켜 나가는 데 사용될 수 있습니다. 이는 최근 몇 년 동안 관찰된 Emotet, TrickBot, Ryuk 랜섬웨어 공격 체인에서 가장 잘 드러납니다. Emotet은 먼저 피해자 네트워크에 침투한 후 초기 접속이 완료되면 도메인에 도달해 TrickBot 페이로드를 다운로드함으로써 개인 데이터, 인증정보 등 다양한 정보를 얻습니다. 피해자가 공격자에게 중요한 표적으로 간주되면 멀웨어는 C2 서버에 도달해 최종 페이로드인 RYUK 랜섬웨어를 다운로드합니다.

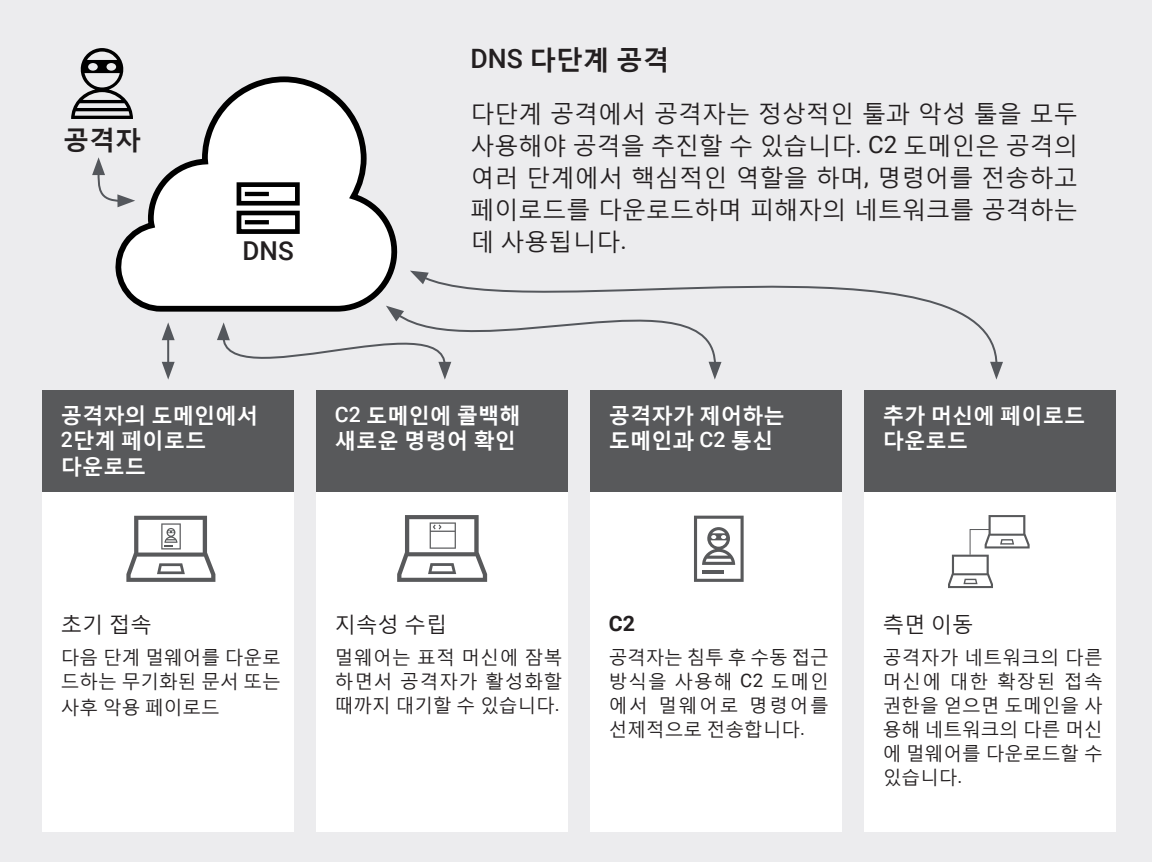


그림 3: 공격의 각 단계에서 C2의 역할

이러한 일련의 이벤트는 이 보고서의 정보를 평가할 때 고려해야 할 중요한 사항입니다. C2 통신은 공격의 다양한 단계에서 발생할 수 있습니다. Conti 그룹과 같은 최신 랜섬웨어 그룹의 방법론을 분석한 결과, 정교한 공격자들은 신속하고 효율적으로 공격을 진행하기 위해 운영자에게 '직접 수동 공격'을 지시하는 경우가 많았습니다. C2 트래픽을 확인하고 차단하는 기능은 지속적인 공격을 차단하는 데 핵심적입니다.

Akamai에서 관측한 C2 도메인은 특정 위협군 또는 공격자 그룹에 속하는 도메인과 그렇지 않은 도메인으로 분류할 수 있습니다. 이 섹션에서는 위협 종류와 연결된 C2 도메인을 심층적으로 살펴보는 동시에 각 그룹의 역량 및 방법에 따라 독자가 리스크 수준을 평가할 수 있도록 지원합니다. 이러한 멀웨어 변종 군 중 일부는 공격자들이 공격 중에 어떻게 사용하는지에 따라 여러 사용 사례에 적합할 수 있습니다.

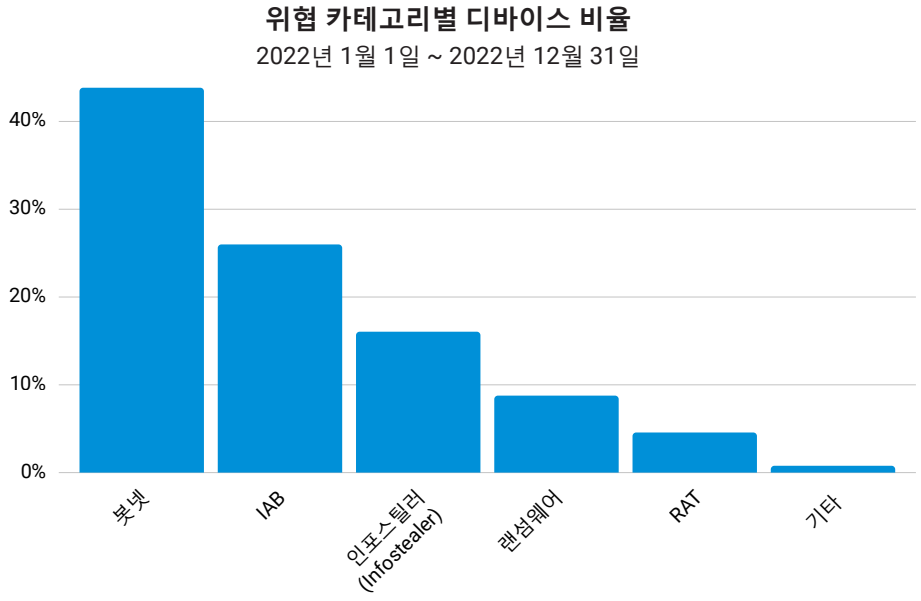


Fig.4: 기업을 표적으로 삼는 위협의 대부분은 봇넷이며 IAB, 인포스틸러(정보 도용자×Infostealer)가 그 뒤를 따릅니다.

그림 4에서 공격자 그룹은 IAB, 봇넷, RaaS 그룹으로 분류됩니다. Akamai 데이터에 따르면 IAB는 기업 네트워크에 가장 큰 위협 중 하나이며, 데이터 탈취를 노리는 봇넷만큼 위협적입니다.

IAB

IAB(초기 접속 브로커×Initial Access Broker)는 주로 랜섬웨어 그룹을 비롯한 다른 사이버 범죄자들이 기업 네트워크의 발판을 마련하기 위해 초기 진입점을 제공하는 데 주력합니다. 지속성, 침입 후 원격 페이로드 실행, 데이터 유출.

RaaS 그룹

RaaS(Ransomware as a Runring Service) 그룹은 기술적 전문 지식이 없는 다른 공격자가 돈을 지불하면 랜섬웨어 소프트웨어를 사용할 수 있도록 허용합니다.

봇넷

공격자는 암호화폐 채굴 및 DDoS 공격에서 데이터 유출, 멀웨어 배포, 측면 이동에 이르기까지 다양한 용도로 봇넷을 사용할 수 있습니다.

정보 도용자

인포스틸러(정보 도용자, Infostealer)는 사용자 이름, 비밀번호, 시스템 정보, 은행 인증정보, 쿠키 등과 같은 다양한 종류의 데이터를 수집합니다.

또한, 랜섬웨어, 원격 접속 툴(RAT), 인포스틸러 등이 혼합된 사례를 관측했으며, 이들은 다양한 공격 단계에서 모두 중요한 역할을 합니다. 그리고 초보 공격자와 경험이 많은 사이버 범죄자 모두 첫 침투 기회를 확보하고 네트워크에 숨어 공격을 감행하는 데 사용할 수 있는 툴을 지하 시장에서 손쉽게 구할 수 있기 때문에 기업은 그 어느 때보다 사이버 범죄에 더욱 취약해졌습니다. Akamai는 이와 같이 위협을 분류하는 과정에서 그룹이 운영하는 교차점과 기업에 미치는 잠재적 영향 및 그 의미에 대해 살펴볼 것입니다.

IAB 그룹

'IAB(초기 접속 브로커×Initial Access Broker)'라고 불리는 사이버 범죄자는 주로 다른 사이버 범죄자와 공격자가 기업의 네트워크에 최초로 진입할 수 있는 발판을 마련하는 데 집중합니다. RDP 및 VPN 관련 취약점 악용, 무차별 대입 공격, 인증정보 덤프 수집, 멀웨어로 연결되는 피싱 이메일 실행 등 여러 사이버 범죄 그룹이 유사한 유출 방법을 사용합니다. IAB는 전체 공격을 진행하는 대신 감염된 시스템에 대한 접속 권한을 획득하고 다른 공격자 그룹에게 접속 권한을 판매하는 방향으로 전문화되어 있습니다. LockBit, DarkSide, Conti, BlackByte의 배후에 있는 랜섬웨어 그룹은 IAB를 운영의 일부로 활용한 것으로 알려졌습니다. 2023년 리서치 결과에 따르면 최초 접속의 평균 판매 가격은 미화로 약 2800달러입니다.

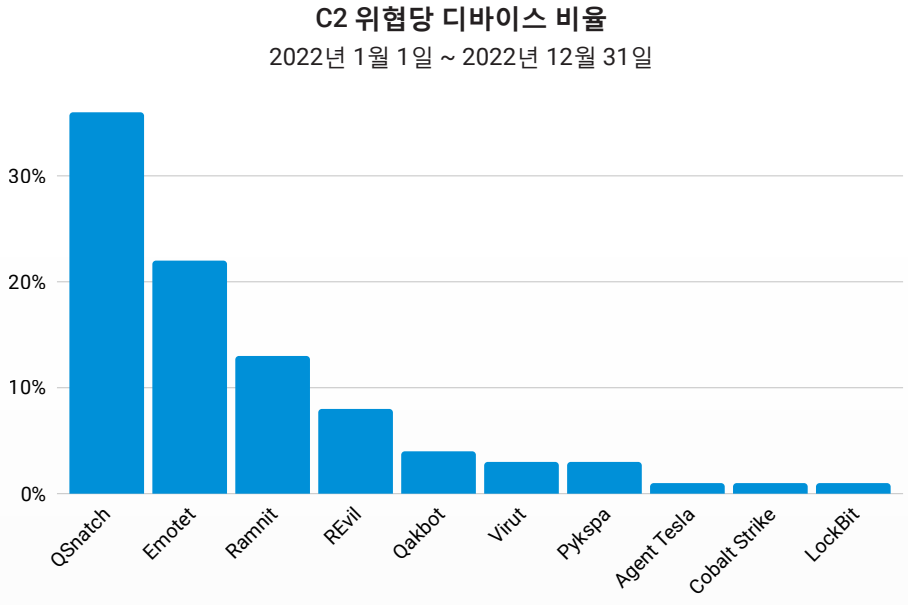
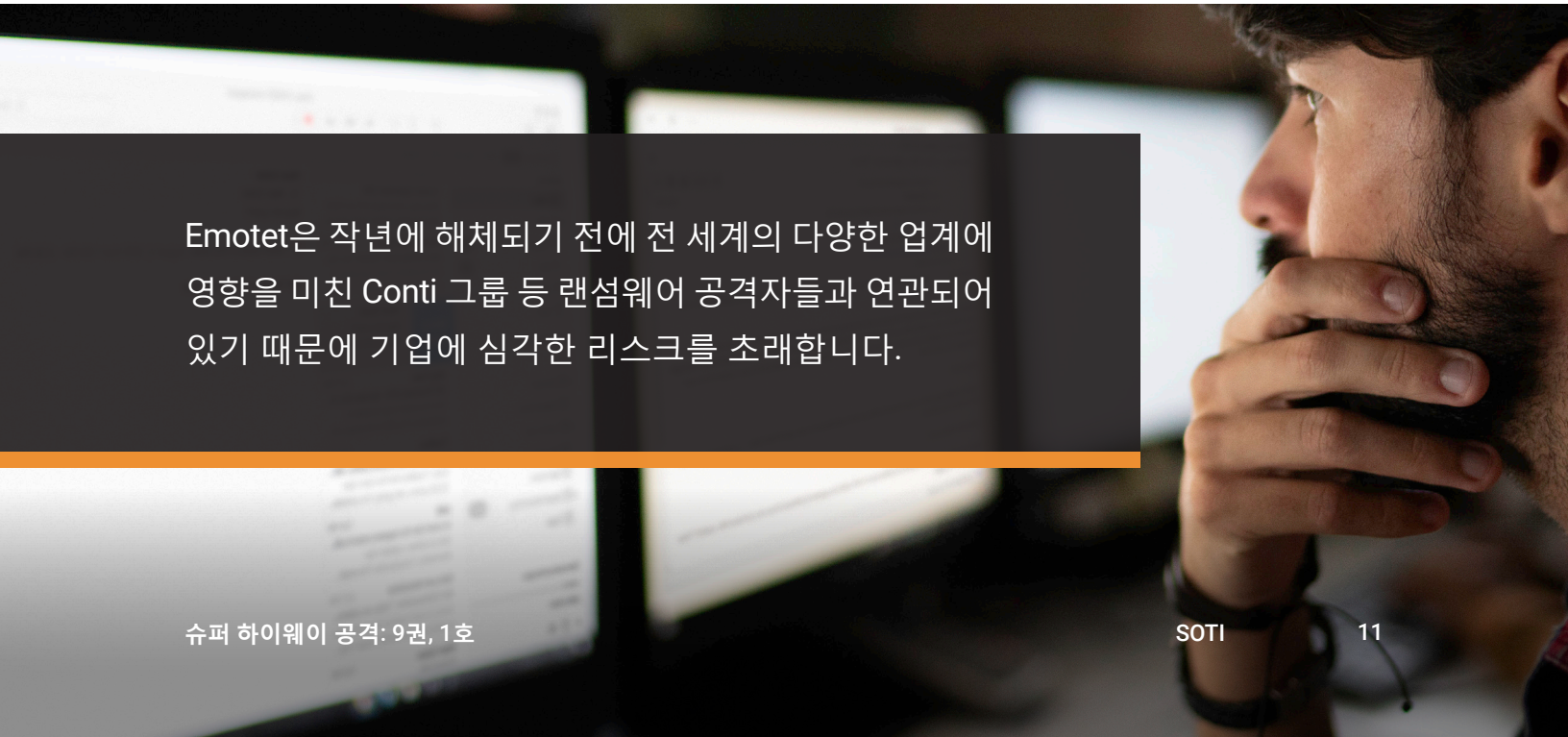


그림 5: QSnatch, Emotet, Ramnit은 기업 네트워크 트래픽에서 가장 많이 관측된 C2 위협입니다.

DNS 데이터(그림 5)에 따르면 감염된 디바이스의 26%가 Qakbot(감염된 디바이스의 4%) 및 Emotet(감염된 디바이스의 22%) 등 IAB 관련 도메인에 접속했습니다. IAB는 RaaS 비즈니스 모델과 사이버 범죄 환경에서 중요한 역할을 합니다. 랜섬웨어 공격자와 사이버 범죄자가 피해자의 네트워크에 침투할 뿐만 아니라 측면 이동, 지속성 수립, 접속 권한 획득 등 다양한 활동을 펼치려면 원격 접속과 인증정보가 필요합니다. 공격자들은 IAB를 활용해 정찰, 잠재적 표적 스캔, 초기 감염 등 많은 시간이 소모되는 작업을 수행합니다. 접속 권한을 암시장에서 쉽게 판매할 수 있기 때문에 이러한 단계를 건너뛸 수 있으며, 공격자가 공격을 시작하는 데 필요한 전문 지식 또는 시간도 줄어듭니다. 따라서 공격하고자 하는 기업에 대한 수많은 잠재적 공격이 발생하면서 랜섬웨어, 대외비 및 민감한 정보 도난, 스파이 행위, 데이터 유출이 발생합니다.

Emotet은 Akamai 데이터 내에서 가장 중요한 IAB 중 하나로 부상하고 있습니다. Emotet은 작년에 해체되기 전에 전 세계의 다양한 업계에 영향을 미친 Conti 그룹 등 랜섬웨어 공격자들과 연관되어 있기 때문에 기업에 심각한 리스크를 초래합니다. 수년 동안 Emotet은 DDoS (Distributed Denial of Service) 및 이메일 도난 기능과 같은 모듈을 추가하고 표적을 확대했습니다. 다양한 기능을 갖춘 뱅킹 트로이 목마 및 봇넷에서 Emotet은 MaaS(Malware as a Service)로 멀웨어를 전환해 IcedID 뱅킹 트로이 목마, TrickBot, UmbreCrypt 랜섬웨어 등의 위협을 배포했습니다. 또한 TrickBot 그룹은 Ryuk, ProLock, Conti 등 여러 랜섬웨어 변종을 배포하기 위해 Emotet을 사용하는 것으로 관측되었습니다. Emotet에서 사용하는 기술에 대한 자세한 내용은 MITRE ATT&CK 프레임워크에서 확인할 수 있습니다.

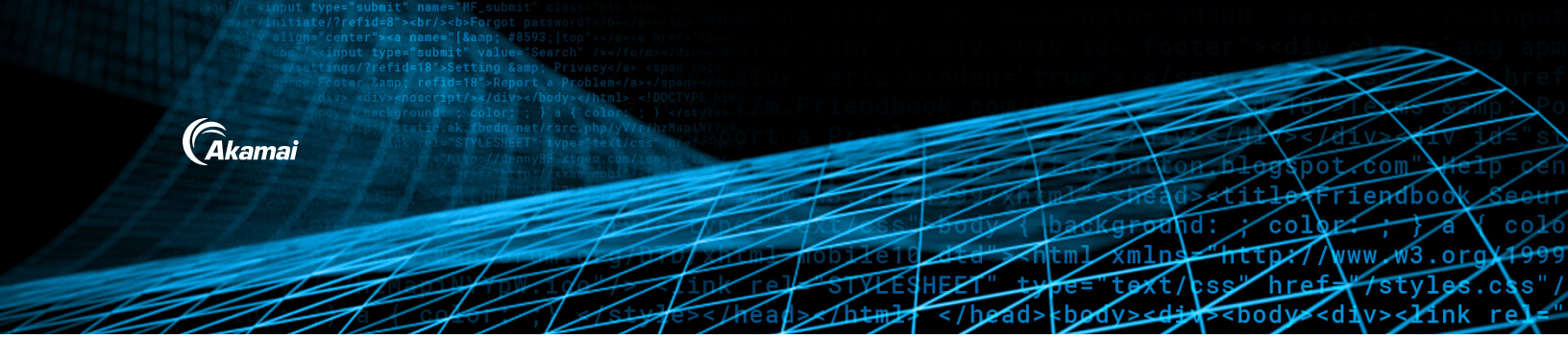


데이터에서 두 번째로 눈에 띄는 IAB는 Qakbot입니다. 이 그룹은 전 세계 50여 곳의 기업에 영향을 미친 것으로 알려진 Black Basta 랜섬웨어 그룹과 협력한 것으로 알려져 있습니다. Qakbot 팀은 정보 도용 기능과 시스템 보안을 더욱 심각하게 감염시키는 2단계 멀웨어를 제공하는 것으로 알려져 있습니다. 리서치에 따르면, Qakbot은 Cobalt Strike를 활용합니다. Cobalt Strike는 공격자가 사용하고 악용하는 정상적인 침투 툴로, 침입 후 일련의 악성 활동을 진행하며 피해자의 환경으로 백도어를 용이하게 합니다. 이 기술은 최근 IAB에서 점점 더 많이 사용되고 있습니다. MITRE ATT&CK 프레임워크는 공격 중에 Qakbot이 활용하는 기술과 관련된 정보를 추가적으로 제공할 수 있습니다.

봇넷 그룹

Akamai의 분석에서 봇넷은 C2 트래픽의 44%를 차지하며 가장 큰 규모의 위협 종류입니다. 이 그룹에는 다양한 공격자들이 포함되어 있으며, 모든 봇넷이 동일하지 않다는 점을 기억해야 합니다. 무해한 변종이 암호화폐 채굴기를 심거나 피해자의 머신을 이용해 DDoS 공격을 일으킬 수 있습니다. 봇넷 자체가 비용을 유발하지만, Akamai가 기업 내에서 발견한 봇넷은 데이터 유출 및 다단계 공격에 사용될 수 있으며, 이는 더욱 심각한 리스크를 초래할 수 있습니다. 봇넷은 네트워크 측면으로 확산될 수 있고 TrickBot의 경우처럼 랜섬웨어를 배포하는 데 사용될 수 있으며, 정보 도용 및 인증정보 수집에 특히 집중하기도 합니다.

Akamai는 기업 환경에서 가장 큰 봇넷인 QSnatch가 네트워크 연결 디바이스에서 확실하게 데이터를 유출하는 것을 발견했습니다. 당사 데이터에 따르면 QSnatch는 36%의 감염된 디바이스에 영향을 주었습니다. 이 멀웨어는 기업에서 백업 또는 파일 스토리지에 사용되는 NAS 디바이스 종류인 QNAP를 표적으로 공략합니다. 감염 방법은 아직 알려지지 않았지만, 연구자들은 QSnatch가 펌웨어 취약점을 악용하거나 기본 사용자 이름 및 비밀번호로 무차별 대입 공격을 단행해 디바이스를 감염시킬 수 있다고 추측합니다. QNAP를 사용하는 기업은 펌웨어를 최신 상태로 유지하고(감염되면 QSnatch는 패치 설치를 방지하고 보안 제품을 비활성화함) 기본 암호를 즉시 변경하는 것이 좋습니다. 공격자들은 인증정보 스크레이핑, 비밀번호 로깅, 원격 접속, 데이터 유출 등을 위해 QSnatch를 사용합니다. 공격자들은 중요한 정보를 많이 갖고 있는 스토리지 디바이스를 공격 표적으로 삼을 수 있으며, 이러한 디바이스가 감염되면 기업은 랜섬웨어 공격이 발생했을 때 대비한 백업이 없습니다. 기법과 대책에 대한 자세한 내용은 CISA 알림에서 자세히 다룹니다.



RaaS 그룹

DNS 트래픽을 분석한 결과, C2에 감염된 디바이스 중 9%가 RaaS(Ransomware as a Runring Service) 그룹과 관련된 도메인에 접속한 것으로 나타났습니다. RaaS 그룹은 기술적 전문 지식이 없는 다른 공격자가 돈을 지불하면 랜섬웨어 소프트웨어를 사용할 수 있도록 허용합니다. 랜섬웨어 공격을 당한 기업은 회사 대외비 데이터 손실뿐만 아니라 수많은 대가를 치러야 합니다. 기업은 문제 해결 및 복구 비용, 법적 수수료, 벌금, 생산성 저하로 인한 다운타임, 브랜드 및 평판 타격 등에 잠재적으로 대처해야 합니다. Cybersecurity Ventures는 2031년까지 랜섬웨어 공격으로 인한 비용이 연간 약 2650억 달러에 달할 것이라고 발표했습니다. 또한 Akamai의 글로벌 랜섬웨어 보고서에서는 랜섬웨어의 치명적인 영향력이 단순히 재정적 피해를 넘어서 공급망 중단, 그리고 심지어는 죽고 사는 문제로 이어질 수 있다는 점을 자세히 설명합니다.

가장 규모가 큰 RaaS 그룹 중 한 곳은 REvil 그룹입니다. 이 그룹은 1500여 곳의 매니지드 서비스 공급업체에 영향을 준 공급망 공격에서 IT 관리 벤더사를 표적으로 삼은 것으로 악명 높습니다. REvil의 활동은 러시아 정부에서 여러 그룹원을 체포하면서 중단되었습니다. 하지만, 그룹이 해체되고 몇 개월 후에 보안 연구자들은 REvil의 유출 사이트가 미국의 일부 대학 등 최근 피해자들의 정보를 악용하면서 다시 활발하게 활동하고 있음을 관측했습니다. 연구자들은 이 캠페인을 진행 중인 REvil 그룹이 이전과 다른 그룹일 수도 있다고 추측하고 이들이 자취를 은폐하기 위해 스스로를 REvil 그룹이라고 주장하는 국가들에 대해 경고했습니다. 기법 측면에서 REvil은 공격 대상에 따라 공격 흐름을 맞춤화하는 것으로 알려져 있으며, 이를 통해 REvil이 공격 대상에 대해 갖고 있는 지식의 수준을 유추할 수 있습니다. REvil과 관련된 전술, 기법, 절차에 대해 자세히 알아보려면 MITRE의 게시물을 확인하시기 바랍니다.

> **공격자들은 중요한 정보를 많이 갖고 있는 스토리지 디바이스를 공격 표적으로 삼을 수 있으며, 이러한 디바이스가 감염되면 기업은 랜섬웨어 공격이 발생했을 때 대비한 백업이 없습니다.**

DNS 트래픽을 분석하면서 발견한 또 다른 RaaS 그룹은 LockBit입니다. Conti가 사라지면서 LockBit 그룹은 가장 활동적인 RaaS 공급업체 중 하나가 되었습니다. 이 보고서에 따르면, 2019년 11월~2022년 3월에는 Lockbit가 Conti 다음으로 가장 많은 기업에 피해를 끼쳤습니다.

LockBit 그룹은 다른 RaaS 그룹보다 더 빠른 암호화 메커니즘을 보유했다고 자부하며, LockBit 2.0을 통해 1만2000여 곳의 기업에 영향을 미쳤다고 주장합니다. 2022년 6월, 이 그룹은 버그 바운티 프로그램 등 추가 기능과 함께 LockBit 3.0을 출시했습니다. 또한 Log4j 취약점을 이용함으로써 표적에 대한 초기 접속을 확보하고 있으며, 이는 패치의 중요성을 강조합니다. 이런 보안 취약점을 해결하지 않은 기업은 LockBit에 감염될 리스크가 증가하게 됩니다. LockBit은 끊임없이 자체적으로 발전하고 있습니다. 최근에는 파일을 암호화하고, 유출 사이트에 게시하고, 피해자가 랜섬(몸값, ransom) 지급을 거부하면 DDoS 공격을 일으키는 삼중 강탈 기법까지 활용하는 것으로 나타났습니다.

주요 툴

이 섹션에 나와 있는 툴은 시스템 유출, 정보 획득, 권한 확대 등 공격에서 특정한 역할을 담당합니다. 다양한 공격자 그룹에서 목격한 무기를 정보 도용자 및 RAT처럼 운영하려면 통신이 필요한 경우가 많습니다. 이러한 툴과 공격자 그룹이 사용하는 기법을 이해하면 보안 실무자가 공격이 어떻게 발생하는지를 이해하고 그에 따라 계획을 수립하는 데 도움이 됩니다.

인포스틸러

사용자 이름, 비밀번호, 시스템 정보, 은행 인증정보, 쿠키 등 다양한 종류의 데이터를 획득할 목적으로 설계된 인포스틸러(정보 도용자, Infostealer)는 여전히 공격에 자주 사용되는 MaaS 중 하나입니다. 전문 지식 또는 기술이 없는 공격자들은 인포스틸러를 비교적 저렴한 비용으로 확보해 공격을 일으킬 수 있습니다.

C2 멀웨어 목록에서 알려진 C2 특성에 접속한 디바이스의 16%가 인포스틸러에 접속한 것을 확인했습니다. Ramnit(감염된 디바이스의 13%)은 단순한 정보 도용자가 아닙니다. Ramnit의 장점은 모듈화 수준이 높다는 것입니다. 공격자는 다른 중요한 데이터를 훔치고 다른 멀웨어를 다운로드 및 배포해 최종 목표를 달성하거나 공격을 진전시키는 등 다양한 기능을 활용할 수 있습니다. 2021년, Ramnit는 최고의 뱅킹 트로이 목마로 자리 잡았으며, 최근 뉴스에서는 또 다른 멀웨어가 Ramnit과 유사한 코드를 공유한다는 점을 언급했습니다.

네트워크에 인포스틸러가 존재하면 사용자의 인증정보가 리스크에 처할 수 있다는 것을 의미합니다. 수집된 도난당한 정보는 암시장에서 판매되어 다른 공격자들이 초기에 접속하는 데 악용될 수 있습니다. 랜섬웨어 그룹은 피싱이나 봇넷을 통해 인포스틸러를 배포해 유효한 인증정보를 획득하고, MaaS를 제공하는 지하 시장에서 인포스틸러에 대한 접속 라이선스를 대여하거나, IAB를 통해 네트워크 접속 권한을 구매할 수 있습니다. 인포스틸러 운영자가 IAB가 되어 매우 정교한 공격을 시작할 수 있는 가장 높은 입찰자 또는 기타 공격자에게 가치가 높은 인증정보(VPN 또는 RDP 접속 등)를 판매하는 경우도 있습니다.

원격 접속 툴

여러 공격 그룹들은 Cobalt Strike를 운영의 일부로 사용해 왔습니다. 공격자는 정찰, 권한 확대, 네트워크를 통한 측면 이동, 지속성 수립, 침입 후 원격 페이로드 실행(랜섬웨어 등), 데이터 유출 등 여러 가지 방법으로 강력한 RAT인 Cobalt Strike를 활용해 왔습니다. 이 툴은 주로 침해 후에 측면 이동과 유출을 위해 사용하지만 스피어 피싱 모듈을 갖고 있기 때문에 초기 접속 기법으로 사용될 수도 있습니다. 이 툴을 사용하는 것으로 알려진 그룹에는 Conti, Qakbot, TrickBot, Emotet 등이 있습니다. 환경에서 Cobalt Strike를 탐지할 수 있도록 이 YARA 룰 세트를 만들어 툴의 악의적인 사용을 확인했습니다.

당사의 데이터는 Agent Tesla C2 트래픽의 존재 여부도 보여줍니다. 이 RAT는 암시장에서 판매되고 있으며, 가격이 저렴하고 사용하기 쉬워 사이버 범죄자들이 선호합니다. 공격자는 이 툴을 사용해 다양한 브라우저에서 인증정보를 수집하고 키 입력과 스크린샷을 캡처하며 키로깅을 수행할 수 있습니다. 주목할 만한 한 가지 기법은 폼 그래빙(form grabbing)인데, 이를 통해 공격자는 PII 및 기타 민감한 정보를 수집할 수 있습니다. 이러한 도난 정보는 신원 도용 또는 사기에 사용될 수 있습니다. PCrisk는 Agent Tesla의 기술과 이 기술이 사용자에게 미치는 영향에 관한 자세한 내용을 게시했습니다.

연중 멀웨어 캠페인이 간헐적으로 발생한 활동 환경

1년 동안 C2 멀웨어 활동의 변동이 상당히 컸습니다(그림 6). 대표적인 사례로 Emotet은 2021년 11월 재유행한 이후 2022년 1월과 2월에 특히 활발하게 활동하고 있습니다. 이러한 활동 증가는 수개월 동안 활동이 없다가 입지를 회복하는 데 도움이 되는 강력한 캠페인을 보여줍니다. Emotet은 복귀 후 몇 달 동안 Visual Basic for Applications 매크로를 사용하지 않도록 설정하려는 Microsoft의 움직임을 회피하는 방법을 포함해 기법을 강화했습니다. 일부 보고서에 따르면 Emotet은 2022년 7월부터 11월 사이에 활동이 다시 중단된 것으로 나타났습니다. 당사의 데이터 조사 결과, Emotet 도메인에 접속한 감염된 디바이스의 비율이 감소한 것처럼 7월에 C2 트래픽이 감소한 것으로 나타났습니다. 이는 Emotet이 1년 동안 활성 상태를 유지했거나 설치된 멀웨어가 여전히 오래된 인프라와 통신하고 있음을 나타낼 수 있습니다. 2023년에 관측한 내용은 Emotet 그룹이 실제로 휴면 상태에 있었는지 결정하는 데 도움이 될 수 있었습니다.

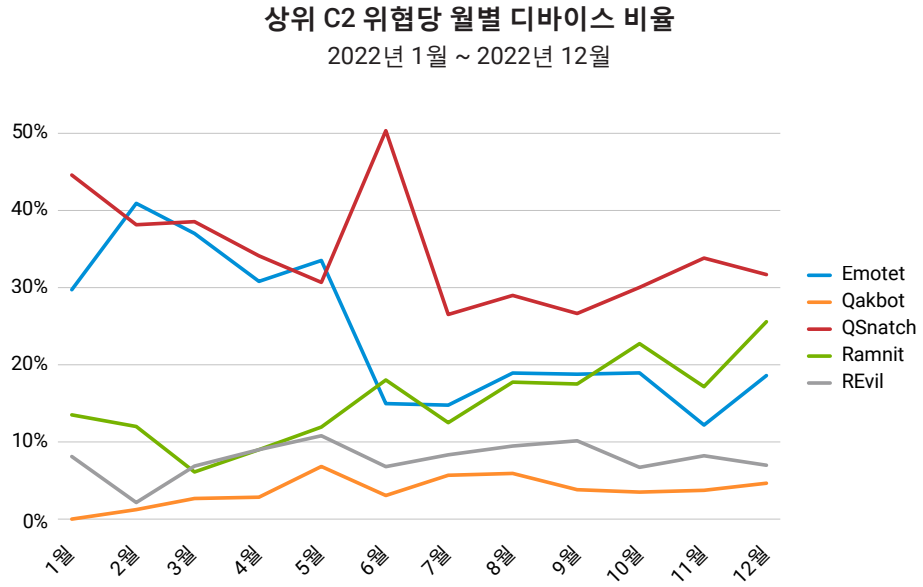


그림 6: 월별 트렌드 그래프를 보면 QSnatch가
2022년 내내 지속적으로 활동했음을 알 수 있습니다.

> **Emotet은 2021년 11월 재유행한 이후 2022년 1월과 2월에 특히 활발하게 활동하고 있습니다. 이러한 활동 증가는 수개월 동안 활동이 없다가 입지를 회복하는 데 도움이 되는 강력한 캠페인을 보여줍니다.**

QSnatch는 1년 내내 지속적으로 활동하면서 6월에 활동량이 정점을 찍었으며, 여기에서 이 위협이 얼마나 만연해 있는지를 확인할 수 있습니다. NAS 서버는 다음과 같은 여러 가지 이유로 공격자의 표적이 될 수 있습니다. 첫째, 중요한 데이터를 포함하고, 둘째, NAS 서버가 패치될 가능성이 낮으며, 셋째, 이러한 디바이스는 기업 네트워크에서 더 쉽게 접속할 수 있으며 측면 이동을 위한 허브 역할을 할 수 있습니다. 지난 몇 년 동안 빌트인 보안 솔루션이 추가되는 등의 변화가 있었지만, 사이버 범죄자들은 설치된 보안 제품을 비활성화하거나 디바이스가 업데이트되어 수정되는 것을 방지해 이러한 변화를 회피했습니다. 따라서 이런 디바이스는 QSnatch의 새로운 변종에 취약합니다.

또한 8월부터 12월까지 기업 네트워크에서 Ramnit의 숫자가 증가하고 있습니다. Ramnit은 공격자가 나중에 다른 공격자에게 판매할 수 있는 광범위한 민감한 정보를 훔쳐 향후 공격으로 이어질 수 있기 때문에 우려할 만한 일입니다.

QSnatch 및 Emotet: 모든 지역에서 공통적으로 많이 발생한 위협

지역별로 빈번하게 발생하는 위협을 확인하기 위해 각 지역의 디바이스가 C2 도메인에 도달하는 비율을 조사했습니다(그림 7). 각 비율은 지역별로 감염된 디바이스 수에 비례하며 지역에 따라 차이가 있습니다. 흥미롭게도, 모든 지역에서 유사한 공격 트렌드가 관측되고 있으며 예외적인 경우는 거의 없습니다. 따라서 지역별로 '결론 및 권장사항' 섹션 또는 위 섹션의 각 멀웨어 그룹에 제공된 권장사항을 따르는 것이 좋습니다.

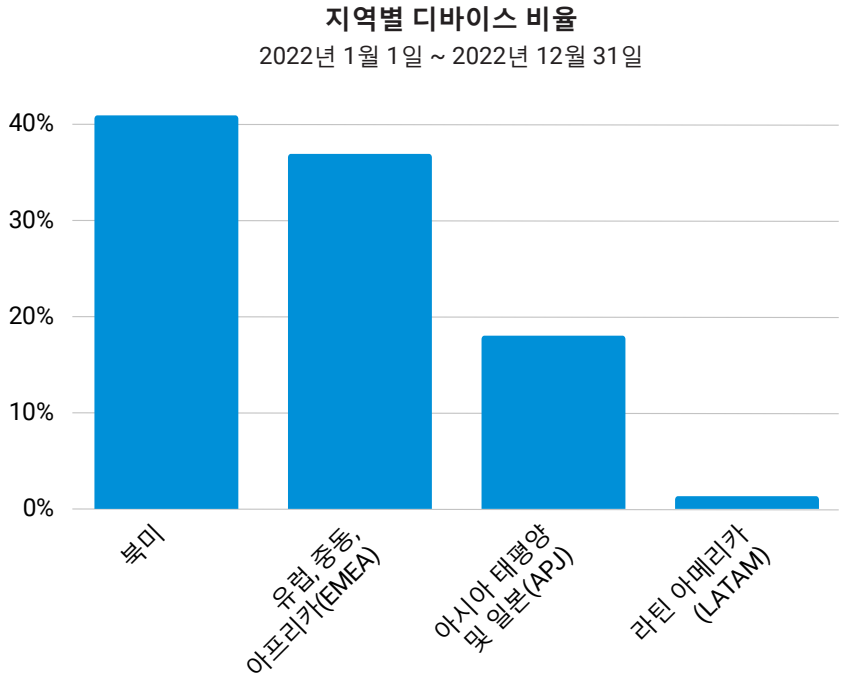


그림 7: 감염된 디바이스 수를 지역별로 분석한 결과 북미 지역이 41%로 선두를 차지했고 EMEA(37%), APJ(18%)가 뒤를 이었습니다.

북미

전 세계 대부분의 기업을 괴롭힌 가장 심각한 두 가지 위협은 QSnatch와 Emotet이었습니다. 북미에서는 해당 지역 내에서 감염된 디바이스의 약 29%가 Emotet에 의해 영향을 받지만 33%는 QSnatch에 의해 영향을 받습니다(그림 8). Dark Reading 보고서에 따르면, 인터넷에 연결된 30만 개의 QNAP 디바이스가 있다는 것을 알 수 있었으며, 이 수치는 이 디바이스가 매력적인 공격 대상임을 반영합니다. 또한 QNAP와 같은 NAS 디바이스를 백업으로 사용하고 미디어 또는 파일 서버로 사용할 수 있습니다.

북미에서 주목할 만한 다른 위협으로는 Ramnit, Qakbot, REvil이 있습니다. Emotet과 같은 IAB가 랜섬웨어를 포함한 다양한 감염의 기반이 되었다는 점을 감안하면 이는 상당히 흥미롭습니다.

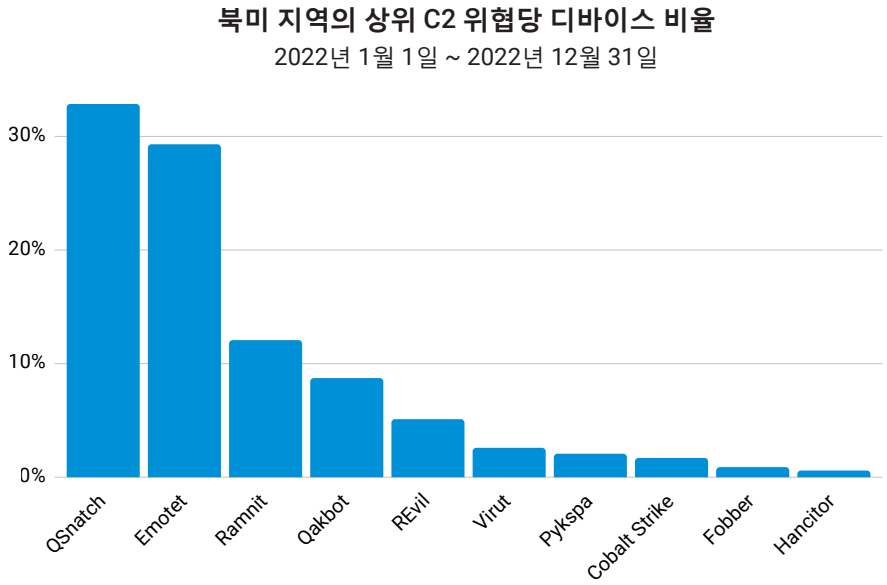


그림 8: 북미 지역 기업들의 경우 감염된 대부분의 디바이스는 QSnatch, Emotet, Ramnit 관련 도메인에 한 번 이상 접속했습니다.

유럽, 중동, 아프리카 지역(EMEA)

EMEA는 북미 다음으로 감염된 디바이스 비율이 가장 높은 지역입니다. 이 지역에서 가장 많이 관측된 위협은 QSnatch(28%)와 Ramnit(21%)이었습니다(그림 9). Ramnit 운영자들이 과거에는 이탈리아, 영국, 프랑스의 은행 및 금융 기관을 표적으로 공격했기 때문에 이 지역에서 Ramnit이 증가하는 것은 놀라운 일이 아닙니다. 반복 공격 중 한 가지 사례에서는 Ramnit의 설정에 EU 지역 국가가 주요 표적으로 포함되었습니다. 실제로 전 세계적으로 Ramnit에 감염된 디바이스 수를 비교하면 EMEA가 Ramnit 감염에서 가장 높은 수치를 차지하고 있습니다. 뿐만 아니라 EMEA에서 Emotet에 감염된 디바이스도 19%로 높았습니다.

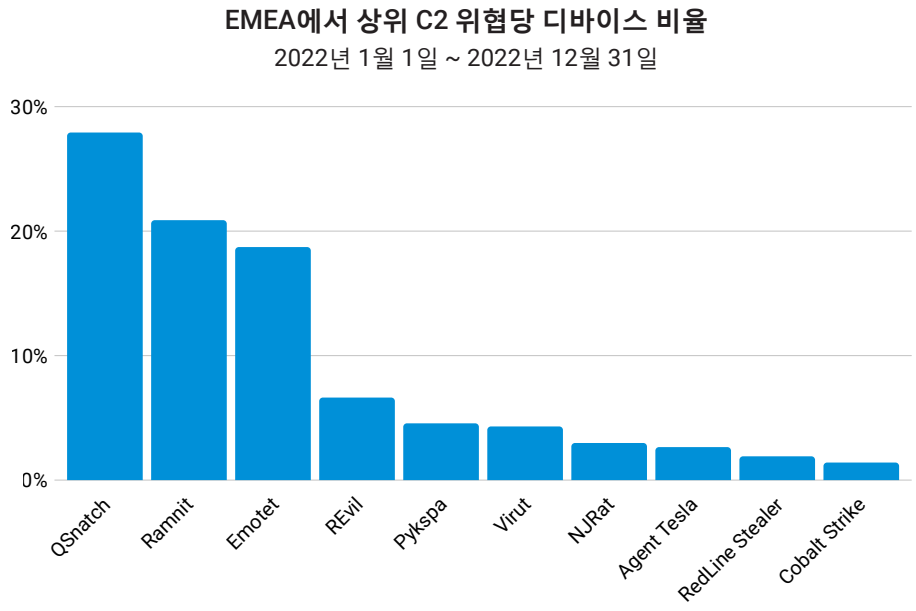


그림 9: 다른 지역보다 EMEA가 Ramnit C2에 접속하는 디바이스가 더 많기 때문에 기업의 리스크가 크게 증가합니다.

아시아 태평양 및 일본

APJ 지역은 QSnatch 감염의 영향을 상당히 크게 받는 것으로 나타났습니다(그림 10). 각 지역의 수치를 비교해 보면 APJ는 QSnatch 감염 디바이스 측면에서 북미 다음으로 2위를 차지했습니다. 반면, APJ 지역은 랜섬웨어 변종인 REvil과 LockBit도 주의해야 합니다. 지역 내 감염된 디바이스에서 관측된 상위 5대 위협에 포함되었기 때문입니다. REvil 그룹의 일원이 작년에 체포되었지만, 이 멀웨어는 몇 달 후 다시 발견되었습니다. 코드에 접속할 수 있는 과거 회원들이 REvil의 재전파를 시도했을 가능성이 있습니다. LockBit 및 REvil과 같은 랜섬웨어 위협(주로 금전적 동기로 발생)이 관측되는 것은 놀라운 일이 아닙니다. 또한 RaaS 운영자들이 Emotet과 같은 IAB를 계속 활용함에 따라 랜섬웨어는 여전히 다양한 업계 및 지역의 비즈니스에 중요한 보안 관련 도전 과제로 남게 될 것입니다.

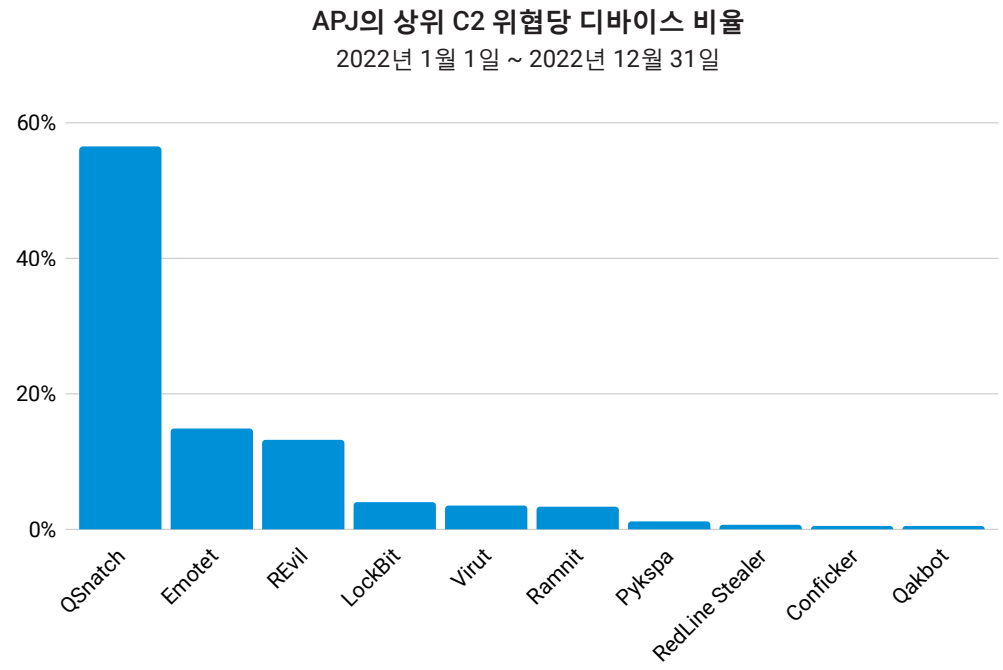


그림 10: Akamai는 이 지역에서 상당한 수의 QSnatch 감염을 관찰했습니다.

라틴 아메리카

이제 LATAM(라틴 아메리카) 지역의 트렌드를 살펴보겠습니다. 이 지역은 감염된 디바이스 수가 가장 적지만 그렇다고 해서 표적 또는 영향을 적게 받는 것은 아닙니다. 글로벌 트렌드와 마찬가지로 이 지역도 QSnatch 및 Emotet의 영향을 받았습니다(그림 11). 이 지역만 개별적으로 조사하면 Tesla, Virut, Ramnit이 가장 두드러집니다.

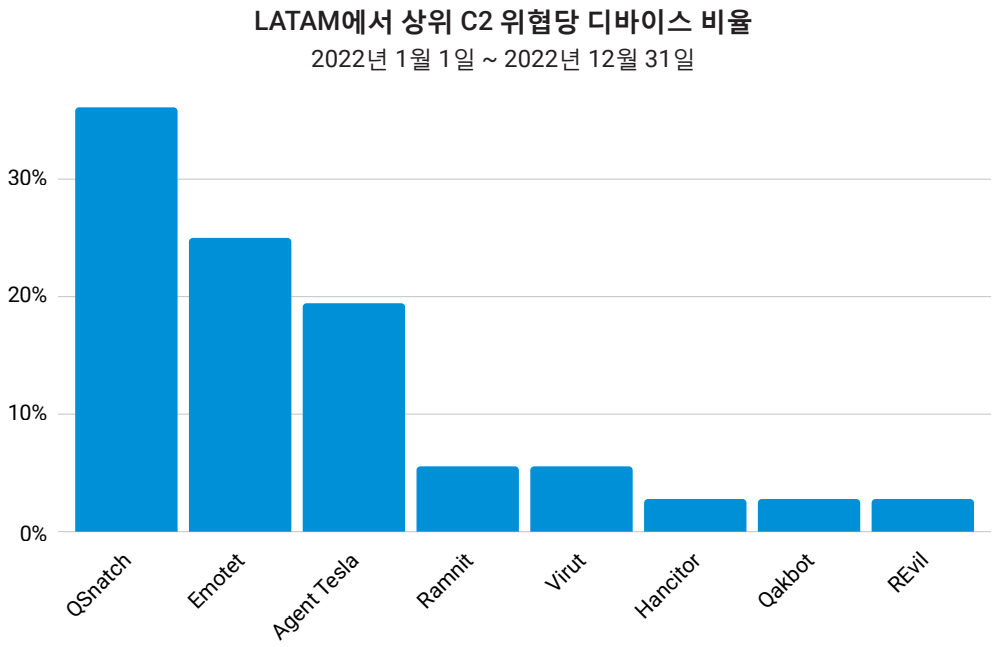


그림 11: 글로벌 트렌드는 LATAM의 위협 환경에서도 유사하게 나타납니다

지역별 세부 분석 내용은 유사성을 확인할 때 뿐만 아니라 지역별로 나타나는 특정 위협을 탐지하는 데도 중요합니다. QSnatch는 항상 상위를 차지하는 위협이지만 그 뒤를 따르는 주요 위협 4가지는 Emotet, REvil, Ramnit, Agent Tesla가 혼합된 형태로 지역별로 다르게 나타납니다. 취약점 관리 및 침투 팀이 중점을 두어야 할 사항을 결정할 때 지역적 위협은 중요한 역할을 합니다.

산업 및 업계 트렌드: IAB 및 봇넷으로 상당한 타격을 입은 제조업

업계 트렌드를 분석하면 각 업계의 리스크 수준과 다른 업계와 비교해 각 업계의 리스크 수준을 확인할 수 있습니다. 감염된 디바이스의 수를 검사하는 대신, 고객별 디바이스를 집계해 각 업계당 타격을 받은 기업 수를 파악했습니다(그림 12). DNS 데이터를 토대로 분석한 결과 악성 C2 트래픽이 발생한 분석 대상 기업 중 30% 이상이 제조업 부문에 속한 것으로 나타났습니다. 또한 비즈니스 서비스(15%), 첨단 기술(14%), 커머스(12%) 업계의 기업들도 영향을 받았습니다. Akamai의 DNS 데이터(제조 및 비즈니스 서비스)에서 상위 2대 업계 역시 글로벌 랜섬웨어 보고서에서 다루었던 Conti 랜섬웨어의 영향을 받은 주요 업계와 일맥상통합니다. 이 보고서에서는 Conti 랜섬웨어의 피해자를 심층적으로 분석하여 업계, 매출, 지역에 따라 프로필을 작성함으로써 이러한 위협의 공격 트렌드를 보여 줍니다.

> **DNS 데이터를 토대로 분석한 결과 악성 C2 트래픽이 발생한 분석 대상 기업 중 30% 이상이 제조업 부문에 속한 것으로 나타났습니다. 또한 비즈니스 서비스(15%), 첨단 기술(14%), 상거래(12%) 업계의 기업도 비슷한 영향을 받았습니다.**

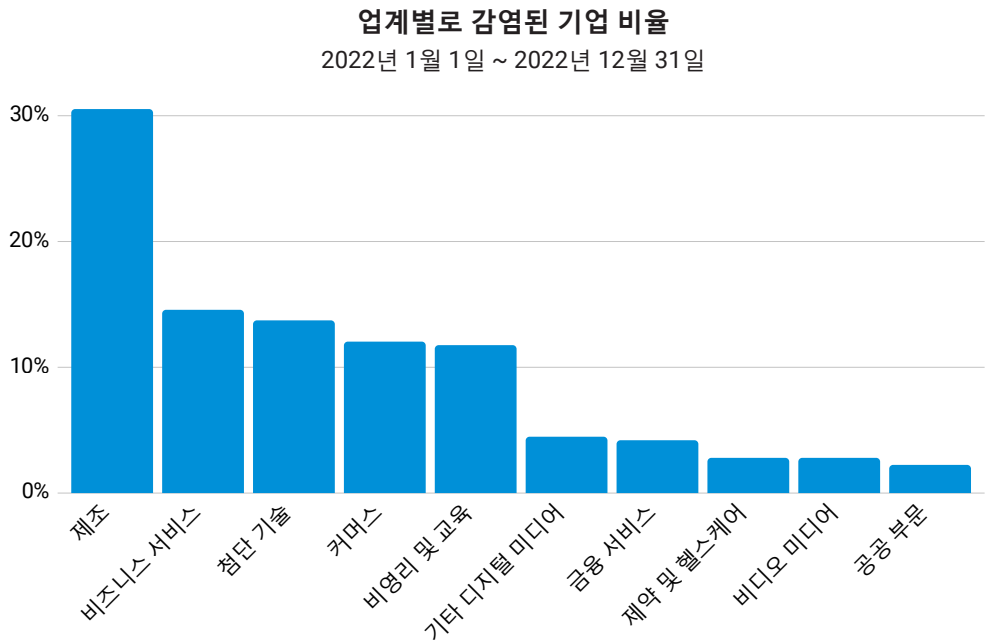


그림 12: 제조, 비즈니스 서비스, 첨단 기술 업계에서 C2 감염이 가장 많이 발견되었습니다.

다양한 C2 공격으로 인해 제조업계가 심각한 타격을 받고 있다는 점은 우려스럽습니다. 공격 대상이 매우 중요한 인프라일 뿐만 아니라 제조업계에 대한 공격이 성공하면 공급망 중단과 같은 실질적인 영향을 미칠 수 있기 때문입니다. 이 데이터는 제조업계가 가장 심각하게 감염된 이유에 대한 구체적인 이유를 보여주지는 않지만, 제조업계의 위협 종류에 대한 심층 조사는 일부 실마리를 제공합니다.

규제를 통해 제조업계와 같은 중요 부문의 보안을 강화하는 국가들도 있습니다. NIS2라 불리는 EU 법안은 리스크 분석 및 정보 시스템 보안 정책, 공급망 보안, 필수 법인(예: 에너지, 운송, 은행, 건강, 안전 등)에 대한 인시던트 처리 등 사이버 보안 표준 및 보안 요구 사항을 강화했습니다. 또한 감염된 업계의 범위도 확장되었습니다.

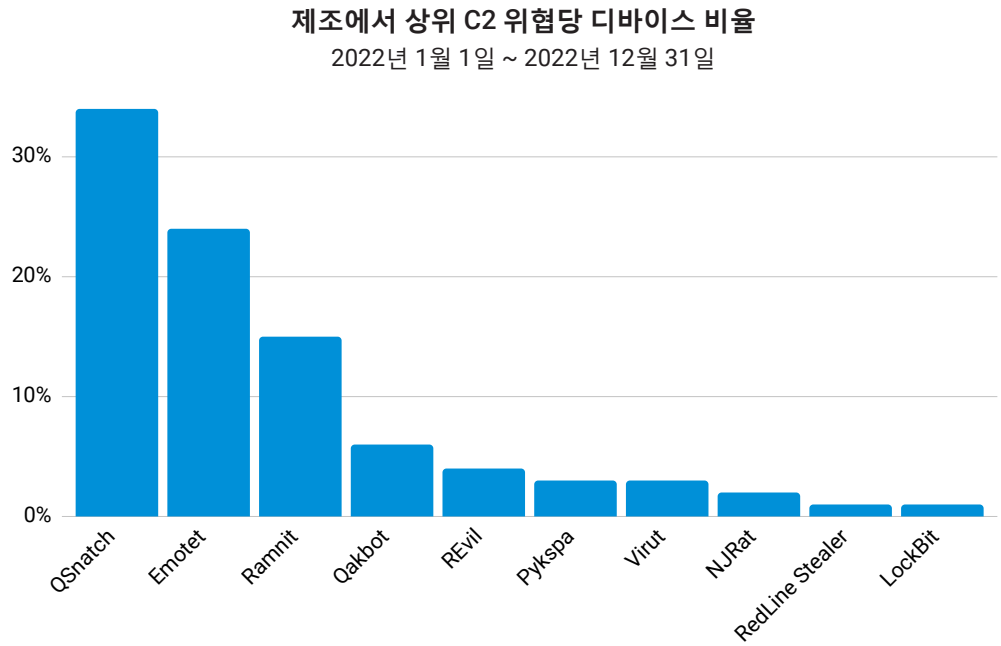


그림 13: 제조업계에서 발견된 상위 C2 위협에는 QSnatch, Emotet, Ramnit이 있습니다.

제조업계를 심층적으로 살펴보면 QSnatch, IAB, Ramnit이 제조업계의 기업들이 접속한 상위 C2 관련 도메인에 해당합니다(그림 13). Akamai 네트워크에 IAB가 존재한다는 것은 공격자들이 잠재 표적에 대한 정보를 수집하고 있다는 것을 의미할 수 있으며, 일단 감염된 머신에 접속하면 공격자는 해당 데이터를 RaaS 그룹 같은 다른 사이버 범죄자에게 판매할 수 있습니다. 또한, 제조업계를 위협하는 C2 멀웨어의 목록에는 인포스틸러도 포함되어 있습니다. 주의해야 할 위협 중 하나는 인증정보나 신용 카드 세부 정보 같은 브라우저 정보를 수집하는 기능을 가진 RedLine Stealer이며, 현재 US $100–150의 월 이용료를 받고 MaaS로 판매되고 있습니다. Group-IB의 리서치에 따르면 이 인포스틸러는 2021년 하반기에서 2022년 상반기 사이에 단일 로그인 계정을 포함하는 로그 3558만5412개를 수집했습니다. 또한, 이 인포스틸러와 관련된 C2 도메인은 2022년 3분기에만 409% 급증했습니다.

업계 트렌드를 추적하면 항상 흥미로운 점을 발견할 수 있습니다. 사이버 범죄자들이 모든 업계를 대상으로 활동을 진행하고 있기 때문에 한 업계에서 일어나는 일은 디딤돌에 해당하는 경우가 많습니다. 공격자들은 종종 업계에서 주목을 받는 기술에 집중합니다. 반면 이들은 랜섬을 지불할 가능성이 가장 높거나, 가장 많은 랜섬을 지불할 가능성이 높은 기업을 노릴 때도 있습니다. 또한 기존의 사이버 보안에 많이 투자하지 않는 업계를 공격하기도 합니다. 다른 기업에서 문제가 발생하는 것이 보인다면 기업 내부 방어 시스템을 확인하는 것이 중요합니다.

공격 받는 가정 내 사용자

공격자들은 기업 네트워크에 성공적으로 침투하면 더 큰 수익을 거두기 때문에 기업을 공격합니다. 이들은 광범위한 툴과 기법을 사용해 기업 경계에 침투하고, 지속성을 수립하고, 대외비 정보를 유출시킵니다. 따라서 이전 섹션에서 설명한 것처럼 기업 네트워크에서 인포스틸러 및 IAB와 같은 위협을 볼 수 있습니다. 그러나 홈 네트워크에서는 어떤 위협이 존재하며 어떤 목적을 위해 사용되고 있는지는 시나리오가 다릅니다.

개인 사용자는 기업 환경만큼 보안이 철저하지 않습니다. 하지만 개인 사용자를 공격했을 때 기업을 공격했을 때와 동일한 금전적 이득을 얻지는 못합니다. 공격자들도 이러한 사실을 알고 있기 때문에 홈 디바이스를 보다 쉽게 감염시켜 수익화할 수 있는 방법을 찾습니다. 예를 들어, 공격자들은 가능한 많은 디바이스를 감염시키기 위해 일단 광범위하게 공격하고 희생자가 걸리길 기다리는 기법으로 대규모 캠페인을 실행하는 반면 기업을 공격할 때는 보다 정교하게 타게팅합니다. 일단 홈 디바이스가 대규모 봇넷의 일부가 되면 공격자는 이런 좀비 디바이스를 동원해 기업을 표적으로 한 스팸 및 DDoS 공격 등 사용자가 알지 못하는 무수한 사이버 범죄 활동을 진행할 수 있습니다. 봇넷이 성공하거나 사이버 범죄자가 봇넷을 대여하려면 가능한 많은 디바이스를 감염시켜야 합니다. 공격자가 개인 사용자를 통해 금전적 이득을 얻는 또 다른 방법은 감염된 디바이스의 컴퓨팅 리소스를 암호화폐 채굴을 위해 사용하는 것입니다.

> **일단 좀비 디바이스가 대규모 봇넷의 일부가 되면 공격자는 이런 디바이스를 동원해 기업을 표적으로 한 스팸 및 DDoS 공격 등 사용자가 알지 못하는 무수한 사이버 범죄 활동을 일으킬 수 있습니다.**

봇넷에 의한 트래픽이 많이 발생하는 홈 네트워크

Akamai는 개인 사용자의 보안에 집중하면서 지난 6개월 동안 수백만 건에 달하는 익명화된 악성 플래그 쿼리 샘플을 분석해 홈 네트워크의 악성 DNS 트래픽을 조사하고 사용자가 우려해야 하는 위협을 보여주고자 합니다. 주요 위협은 봇넷과 관련이 있으며, 공격자들이 다양한 목적으로 IoT 디바이스를 활용하는 방법을 보여줍니다. 이에 관해서는 다음 섹션에서 자세히 살펴보겠습니다.

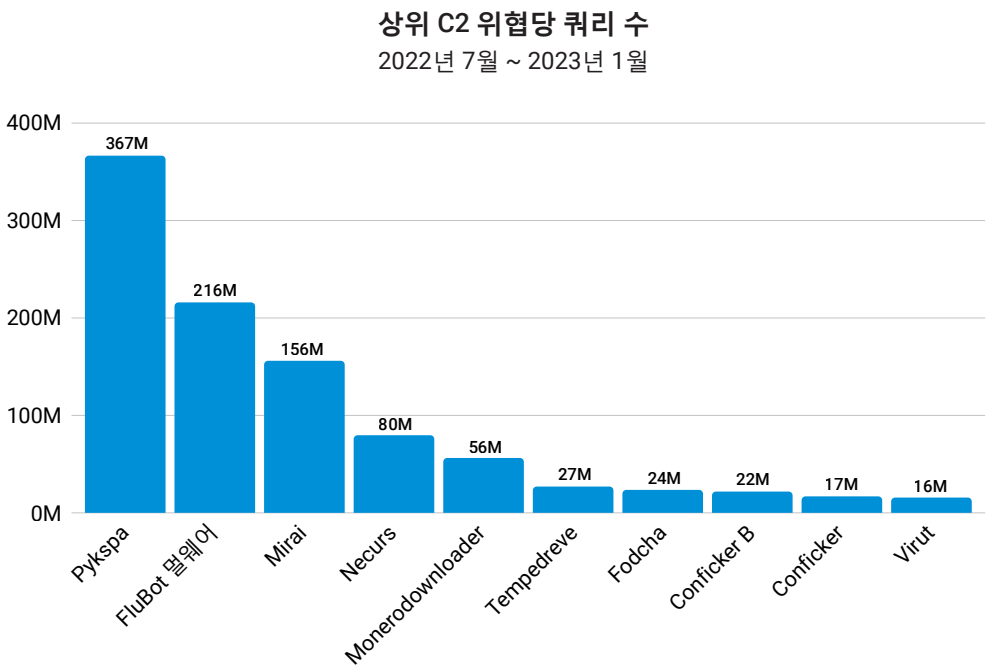


그림 14: 홈 네트워크의 DNS 트래픽에서 가장 많이 관찰되는 상위 3대 봇넷은 Pykspa, FluBot 멀웨어, Mirai입니다.

Pykspa: 소셜 미디어를 통한 전파

Pykspa는 데이터 조사 결과, 전 세계적으로 3억6700만 건의 DNS 쿼리를 기록했습니다(그림 14). Pykspa는 감염된 사용자의 연락처로 악성 링크를 전송하고 Skype를 통해 확산합니다. 브라우저의 탭에서 Twitter를 열면 멀웨어로 연결되는 다운로드 링크가 포함된 트윗도 생성됩니다. 또한 DGA(Domain Generation Algorithm)를 사용해 C2 통신을 설정합니다. 과거에는 v2에서 DGA의 하위 집합을 사용해 탐지되지 않도록 하고 더 오랜 기간 동안 네트워크 내에 머물도록 했습니다.

공격자는 백도어 기능을 사용해 원격 시스템에 접속하고, 파일 다운로드, 프로세스 종료, 다양한 방법을 통해 전파(매핑된 드라이브, 네트워크 공유 등)하는 등 명령어를 임의로 실행합니다. 또한 Pykspa는 감염된 사용자에 대한 개인 정보를 수집하기 위해 Skype 설정을 쿼리합니다. 또한 안티 멀웨어 솔루션과 관련된 특정 문자열이 포함된 웹사이트의 경우 사용자가 해당 웹사이트에 접속하지 못하도록 차단합니다. 흥미로운 점은 Pykspa는 감염된 사용자의 Skype에서 언어 인터페이스를 확인하고, 영어, 독일어, 프랑스어, 스페인어, 이탈리아어 등 이들이 모니터링하는 다양한 언어에 속하는 경우 멀웨어가 Skype 스팸 메시지를 적절히 수정합니다.

FluBot: Android 멀웨어 봇넷

FluBot 멀웨어는 Pykspa 다음으로 가장 많이 사용되는 C2 멀웨어입니다. 주로 문자 메시지를 통해 사용자가 악성 링크를 클릭하도록 유도하여 Android 휴대전화를 감염시키며, 이는 멀웨어 다운로드로 이어집니다. 전파 기법의 일환으로 FluBot 멀웨어는 C2 서버에 감염된 사용자의 연락처 목록을 업로드하고 동일한 소셜 엔지니어링적 유도 수법으로 피해자의 연락처를 전송합니다. 이 멀웨어에는 사용자가 정상적인 은행 앱에 접속할 때 가짜 페이지를 위에 덮어쓰는 기능이 있기 때문에 사용자가 FluBot을 디바이스에 설치하면 은행 및 금융 정보가 리스크에 노출됩니다. 따라서 이러한 인증정보는 ID 도용 또는 사기 거래에 사용될 수 있습니다.

Flubot 멀웨어는 다양한 소셜 엔지니어링 미끼를 사용합니다. 예를 들어, 사용자는 택배 배송 상태를 확인하기 위해 링크를 클릭하도록 제안할 수 있습니다. 또한 사용자에게 음성 메일 메시지가 있다고 알려 가짜 음성 메일 앱을 다운로드하도록 속일 수도 있습니다. 또한 보안 업데이트인 것처럼 가장해 사용자가 링크를 클릭하도록 유도할 수도 있습니다. 사용자가 링크를 클릭하면 앱을 다운로드하라고 안내합니다. 이 앱은 차례로 대화 상대 목록에 접속하고 전화를 걸 수 있는 권한을 요청합니다. 이 위협이 매우 위험한 이유는 접근하기 쉬운 서비스에 대한 권한도 요청해 공격자가 화면 탭을 제어할 수 있도록 함으로써 잠재적으로 더 많은 앱을 설치하게 되기 때문입니다. 사용자가 이 멀웨어를 제거하려면 디바이스를 데이터 초기화하는 것이 좋습니다.

Mirai: IoT의 힘을 빌려 대규모 중단 야기

Mirai는 이번 리서치에서 1억5600만 건의 DNS 쿼리를 기록하며, FluBot 멀웨어 뒤를 바짝 따라가고 있었습니다. 오픈 텔넷 포트를 통해 IoT 디바이스를 표적으로 삼는 것으로 알려져 있으며 가장 큰 DNS 사업자 중 한 곳에 대한 DDoS 공격으로 유명해졌습니다. Mirai는 스스로 전파되는 웜으로 기본 사용자 이름과 비밀번호 조합을 사용하는 취약한 디바이스를 찾습니다. 한때는 공격자들이 무려 10만여 개의 좀비 디바이스를 모아서 유명한 기업을 대상으로 DDoS 공격을 일으켰습니다. Mirai는 공격 초기에 14만5000개의 디바이스를 이용해 기술 기업을 공격했습니다. 이는 사이버 공격을 일으키고 기업에 광범위한 혼란을 야기하기 위해 안전하지 않은 디바이스를 무기로 만드는 방법을 보여주는 한 가지 사례입니다.

2016년, Mirai의 배후 그룹은 소스 코드를 공개했습니다. 법 집행 기관이 이 소스 코드를 추적해 원본 작성자를 잡지 못하게 하려는 조치였을 가능성이 있습니다. 이를 통해 다른 그룹들이 Mirai의 코드를 사용하기 시작했으며 시스템을 감염시키는 등 더 많은 기능으로 코드를 수정하고 강화했습니다. 코드를 완전히 공개하면 Okiru, Satori, Masuta, PureMasuta와 같은 새로운 변형이 나타나며, 여기에는 DDoS 공격을 시작하려는 목적도 있습니다. 감염된 디바이스를 재부팅하면 도움이 되지만 멀웨어가 디바이스를 지속적으로 검사하기 때문에 사용자가 비밀번호를 변경하지 않는 한 다시 감염될 가능성이 큽니다.

Necurs: 멀웨어 배포사 및 접속권 판매자

2012년에 처음 발견된 Necurs 봇넷은 지난 6개월 동안 8천만 건의 쿼리를 기록했습니다. Dridex, TrickBot, Locky 등의 기타 멀웨어 페이로드를 전송할 수 있는 기능이 있기 때문에 개인 사용자와 기업 모두에게 심각한 리스크를 초래합니다. 주목할 만한 한 가지 요인은 이 봇넷이 유료 봇넷 상품의 일부로서 감염된 컴퓨터에 대한 접속 권한을 판매하여 다른 그룹에 제공한다는 점입니다 대부분의 봇넷과 마찬가지로 DGA를 사용해 C2 서버와 통신하는 여러 도메인을 만들어내고 도메인이 차단되더라도 계속 운영됩니다.

랜섬웨어 및 뱅킹 트로이 목마 외에도 Necurs는 러시아 데이트 사기, 제약 사기 등과 같은 다양한 스팸 공격을 배포하는 데 사용됩니다. Microsoft는 조사 과정에서 이 봇넷의 활동을 모니터링한 결과 58일 만에 약 380만 건의 스팸 메일 메시지를 발송했다는 사실을 발견했습니다. 2020년에는 법 집행 기관과 보안 커뮤니티가 협력한 결과 Necurs 봇넷의 운영이 중단되었습니다.

Monerodownloader: 채굴 봇넷

공격자가 수익화하는 여러 가지 방법 중 한 가지는 감염된 머신을 암호화에 사용하는 것입니다. 사이버 범죄자 사이에서 가상화폐 Monero의 인기가 높아짐에 따라 특히 이 Monero를 채굴하기 위해 만들어진 봇넷이 점점 증가하고 있습니다. 공격자가 Monero를 선호하는 이유는 체인이 상대적으로 덜 노출되고 익명성이 제공되기 때문에 추적되지 않습니다. Monerodownloader에 대해 알려진 것은 거의 없지만, 이 서버는 정보를 수집하고 실제 페이로드를 위해 C2 서버에 연결하는 등의 기법을 사용합니다.

패치되지 않은 시스템을 방치하면 Monero Cryptominers와 같은 위협에 노출됩니다. 다른 유사한 Monero 코인 채굴기는 취약점을 활용하고, 무료 소프트웨어로 가장해 사용자가 채굴기를 다운로드하도록 유인하며, 네트워크를 측면으로 이동해 다른 디바이스를 감염시키는 기능으로 최대한 많은 수익을 거둘 수 있습니다. 측면 이동에 대한 설명은 개인 사용자보다 기업에 더 적합하지만, 이는 비밀번호 해독기가 감염을 극대화하는 방법에 대한 인사이트를 제공합니다.

지역별 주요 위협: 홈 네트워크를 지속적으로 지배하는 봇넷

지역 데이터를 자세히 살펴보고, 홈 네트워크의 DNS 트래픽을 기반으로 지역별로 빈번하게 발생하는 특정 봇넷을 확인하고, 이러한 트렌드에 영향을 미칠 가능성이 있는 몇 가지 요인을 살펴보겠습니다.

북미

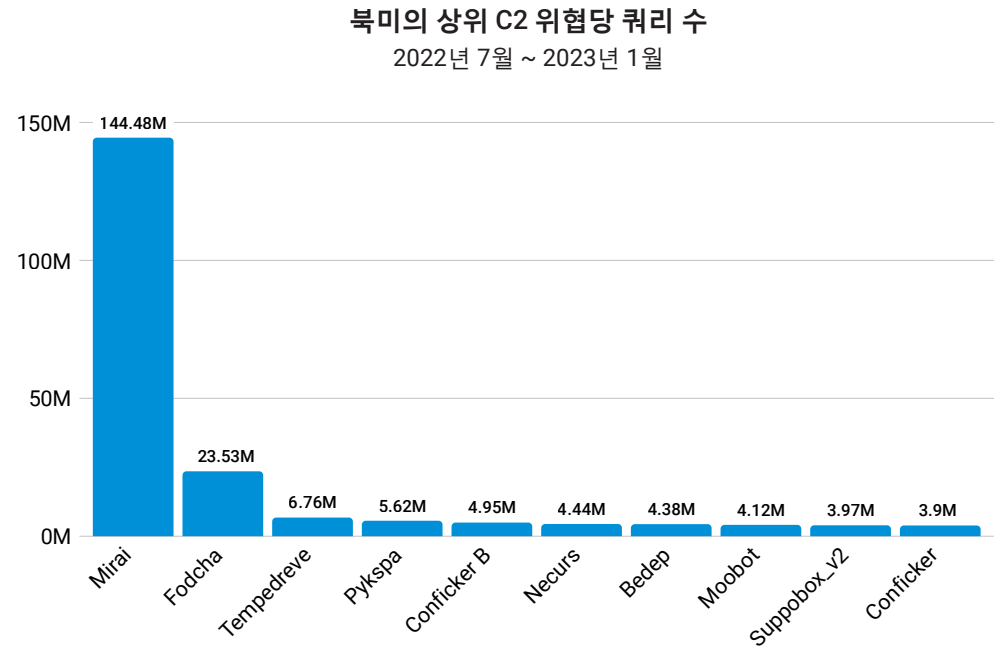


그림 15: Mirai는 안전하지 않은 IoT 디바이스 때문에 북미 지역에서 지속적으로 파장을 일으키고 있습니다.

북미에서는 1억4400만 건의 Mirai 봇넷과 관련된 쿼리가 홈 네트워크에서 발생했습니다(그림 15). 이 봇넷은 여전히 기본 사용자 이름과 비밀번호를 사용하는 취약한 IoT 디바이스를 표적으로 합니다. 이 지역에서 발생하는 대량의 쿼리는 가정에서 IoT 디바이스의 인기 또는 사용량이 많기 때문일 수 있습니다. 2022년 미국 가구의 연결 디바이스는 평균 22개로 전년 동기 25개보다 약간 감소했다고 합니다. 또한 북미 지역에서 IoT 접속이 증가할 것으로 예상됨에 따라(2025년까지 54억 건), Mirai와 같은 위협이나 이와 유사한 변종이 보안이 취약한 IoT 디바이스를 공격할 가능성이 높습니다.

개인 사용자에게 이러한 위협이 미치는 영향은 사이버 범죄자가 모르는 사이에 자신의 디바이스를 악용해 범죄를 저지르게 되는 것입니다. 하지만 기업도 Mirai와 같은 봇넷이 감행하는 DDoS 공격 또는 악성 스팸 캠페인의 영향으로 타격을 받습니다. 공격을 차단하는 가장 좋은 방법은 Mirai 및 기타 유사한 공격으로부터 디바이스를 보호하기 위해 디바이스의 기본 사용자 이름과 비밀번호를 변경하는 것입니다.

유럽, 중동, 아프리카 지역(EMEA)

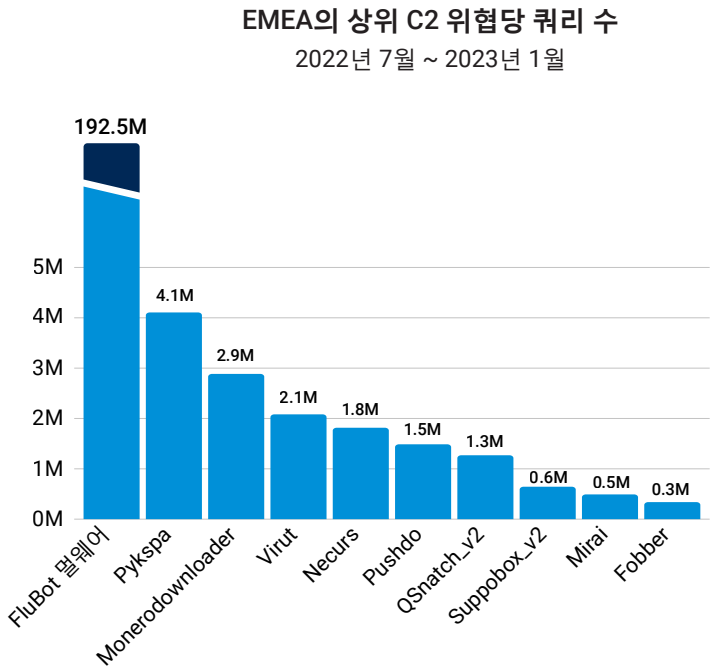


그림 16: FluBot 멀웨어는 전파 기법과 소셜 엔지니어링 미끼의 일환으로 여러 유럽 언어를 사용했기 때문에 EMEA 지역에서 유행했습니다.

EMEA 지역에서 FluBot 멀웨어는 거침 없이 빠른 속도로 확산하고 있습니다. 이 지역에서 관찰된 DNS 쿼리의 엄청난 양(약 1억 9300만 건)은 주목할 만합니다. Akamai는 DNS 트래픽을 조사함으로써 EMEA에서 이러한 감염이 발생하는 것을 확인할 수 있었습니다(그림 16). 한 가지 원인은 공격자가 SMS를 피해자의 연락처 목록으로 보내는 피싱 형태인 스미싱 전파 기법입니다. 이 기법은 사용자를 속여서 실제로는 멀웨어인 패키지 전송 관련 앱 또는 음성 메일 앱을 다운로드하게 유도합니다. 이 외에도 FluBot은 추가 권한을 요청하고 몰래 사용자의 은행 및 금융 인증정보를 기록합니다. 특히 스페인, 독일, 핀란드, 영국 등의 사용자를 표적으로 한 것으로 알려졌습니다. 또한 SMS는 독일어와 헝가리어 등 다수의 유럽 지역 언어로 작성되며, 이는 이 멀웨어가 유럽에서 급증한 여러 가지 원인 중 하나입니다.

라틴 아메리카

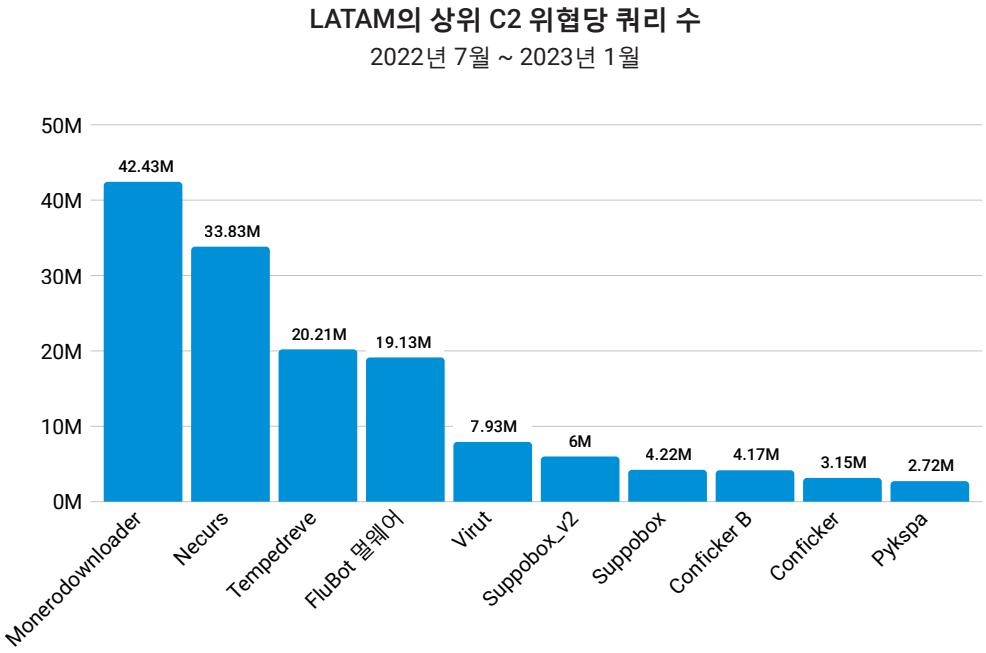


그림 17: 암호화폐 채굴 봇넷 Monerodownloader은 라틴 아메리라 지역에서 암호화폐의 사용이 많았기 때문에 가장 큰 위협이 되었습니다.

북미 및 EMEA와 달리 LATAM 지역은 봇넷의 분포가 더욱 다양하게 나타났습니다(그림 17). 암호화폐 채굴 봇넷인 Monerodownloader는 4200만 건의 쿼리를 기록하며 활성 봇넷 그룹 목록에서 1위를 차지했으며, Necurs(3400만 건)와 Tempedreve(2000만 건)가 그 뒤를 이었습니다. 높은 인플레이션과 송금액에 힘입어 이 지역의 암호화폐 도입율이 높아진 것은 Monerodownloader와 같은 봇넷이 1위를 차지한 이유를 설명합니다. 사용자가 알지 못하는 사이버 범죄자들은 채굴 및 스스로의 금전적 이익을 위해 사용자 디바이스의 리소스를 사용할 수 있습니다. 또한 FluBot은 DNS 트래픽에서 관측되는 큰 위협 중 하나이며, 이는 EMEA 지역 밖에서도 봇넷 트래픽이 매우 높은 것을 보여줍니다.

아시아 태평양 및 일본

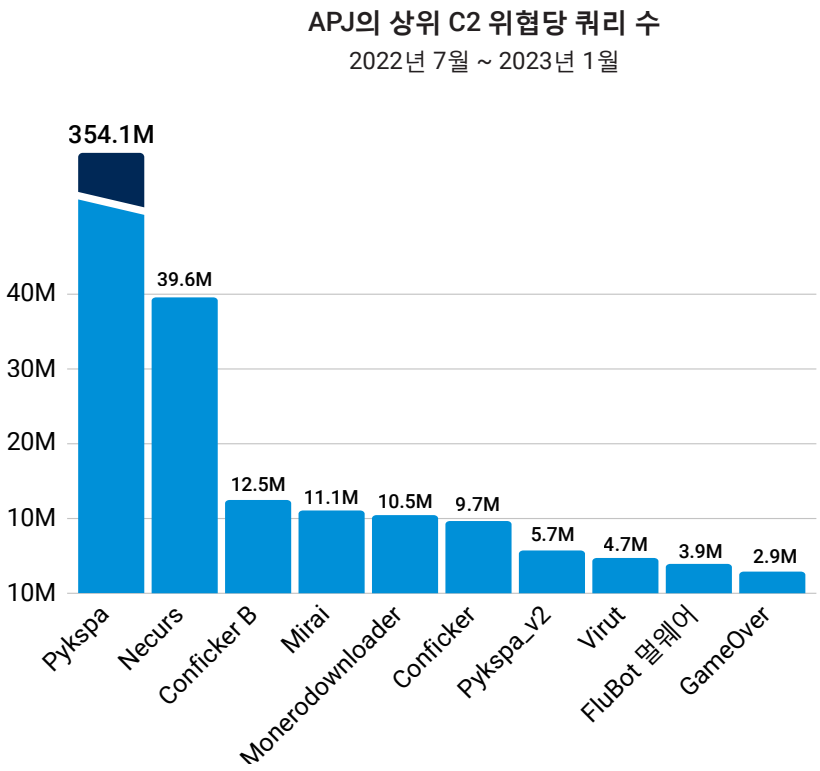


그림 18: APJ 지역의 주요 위협으로는 Pykspa와 Necurs가 있습니다.

APJ에서는 3억5천만 건 이상의 Pykspa 관련 쿼리가 관측되었습니다(그림 18). 2019년 블로그 게시물에서는 Pykspa가 오랜 기간 동안 탐지되지 않기 위해 선택적 DGA 메커니즘을 사용했다고 언급했습니다. 이 보고서에서 강조된 도메인은 대부분 동아시아 지역에서 발견되었습니다. 또한 Necurs 같은 봇넷과 관련된 쿼리도 관측했는데, 이 쿼리는 시스템이 다른 멀웨어에 감염되었음을 나타내는 강력한 지표입니다.

피싱 환경 개요

DNS 트래픽 분석의 마지막 부분에서는 피싱 캠페인의 성공에서 피싱 키트가 차지하는 중요한 역할을 살펴보았습니다. 피싱은 공격자들이 사용하는 기법이 끊임없이 발전하고 있으며 온라인에 제공되는 개인 정보의 양이 증가함에 따라 이전보다 관련성이 훨씬 높아졌습니다. 공격자들은 소셜 엔지니어링을 사용해 피싱 시도가 정상적으로 보이도록 만들고 있으며, 이러한 공격의 성공률이 여전히 높다는 증거가 존재합니다. 연휴 시즌 피싱 사기에 대한 Akamai의 리서치 결과, 공격자들이 계속 공격을 감행하기 위해 사용하는 새로운 기술과 기법을 파악했습니다. 이러한 새로운 기법에는 가짜 사용자의 증언을 사기의 일부로 사용하는 것과 HTML 앵커링을 사용해 유효한 사용자만 사기 웹사이트에 접속하도록 하는 새로 발견된 기술이 포함됩니다.

코로나19 펜데믹 기간에 원격 근무가 증가하면서 피싱 공격의 탐지 및 예방이 더욱 어려워졌고, 이에 따라 개인 및 기업에서는 경계를 늦추지 않고 스스로를 보호하려는 조치를 취하는 일이 더욱 중요해졌습니다. 또한 소셜 미디어가 성장하고 인터넷에 연결된 디바이스가 증가하면서 악의적 사용자는 더 많은 기회를 활용할 수 있게 되었습니다.

금융 서비스를 공격하는 피싱 캠페인

어떤 브랜드가 피싱 사기에 의해 악용되고 모방되고 있는지 조사할 때, 데이터를 수집할 수 있는 여러 가지 방법이 있습니다. 총 캠페인 건수와 피해자 수를 대조했습니다. 이를 통해 특정 캠페인의 성공률을 평가하고 각 업계가 몇 퍼센트를 표적으로 하고 있는지 확인할 수 있습니다.

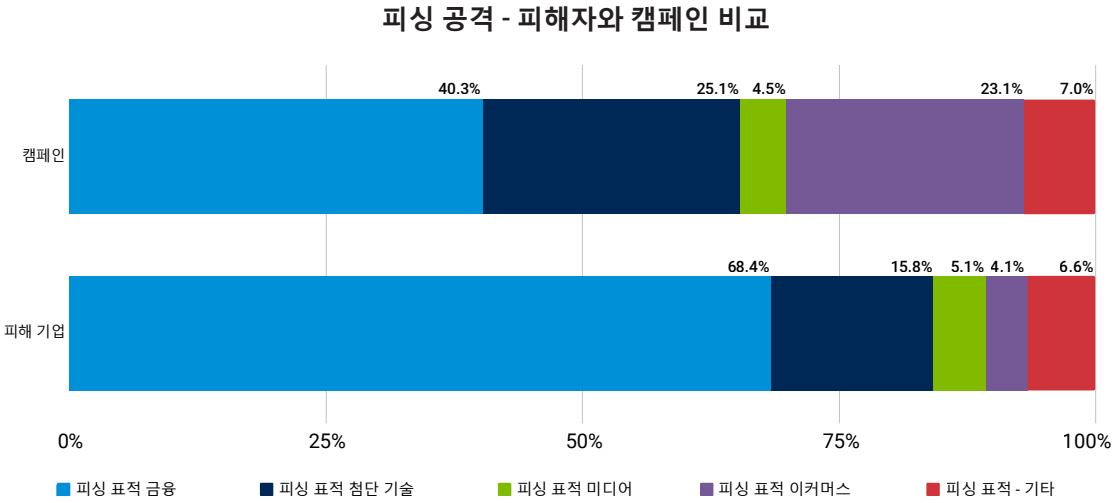


그림 19: 대부분의 피싱 캠페인은 금융 서비스 업계를 표적으로 합니다(2022년 4분기).

리서치 결과, 금융 및 첨단 기술 브랜드가 캠페인과 피해자 수 측면에서 상위를 차지했습니다(그림 19). 또한 금융 서비스 고객에 대한 캠페인의 40.3%가 활성화되어 68.4%의 피해자가 발생한 것으로 나타나 2022년 4분기 금융 서비스에 대한 공격이 매우 효과적임을 알 수 있었습니다. 금융 서비스 보고서 문 앞의 공격자들: 금융 서비스에 대한 공격 분석에서는 피싱 공격이 금전적 동기로 인해 주로 금융 서비스 및 고객을 표적으로 하는 방법을 강조하였습니다. 이러한 공격의 잠재적 영향으로는 브랜드 및 평판 실추, 고객 신뢰 하락 등이 있습니다. 또한 피싱으로 인해 문제를 해결하는 데 기업 리소스가 소모될 수 있습니다.

2022년 4분기에 이커머스에서 피싱 캠페인의 23%가 활성화되었습니다. 실제 피해자보다 더 많은 캠페인을 목격했지만, 사이버 범죄자가 개인 정보나 은행 정보를 알아내면서 공격자들이 이 업계를 표적으로 삼는 것이며 사용자가 경계해야 한다는 점도 주목할 필요가 있습니다.

피싱 사기를 촉진하는 피싱 툴킷

피싱 툴킷의 존재로 인해 압도적인 피싱 환경의 규모와 중요도를 파악할 수 있습니다. 피싱 툴킷은 피싱 웹사이트의 배포 및 유지 관리를 지원해 기술 지식이 없는 사기범도 피싱 환경에 참여해 피싱 사기를 실행하도록 유도할 수 있습니다.

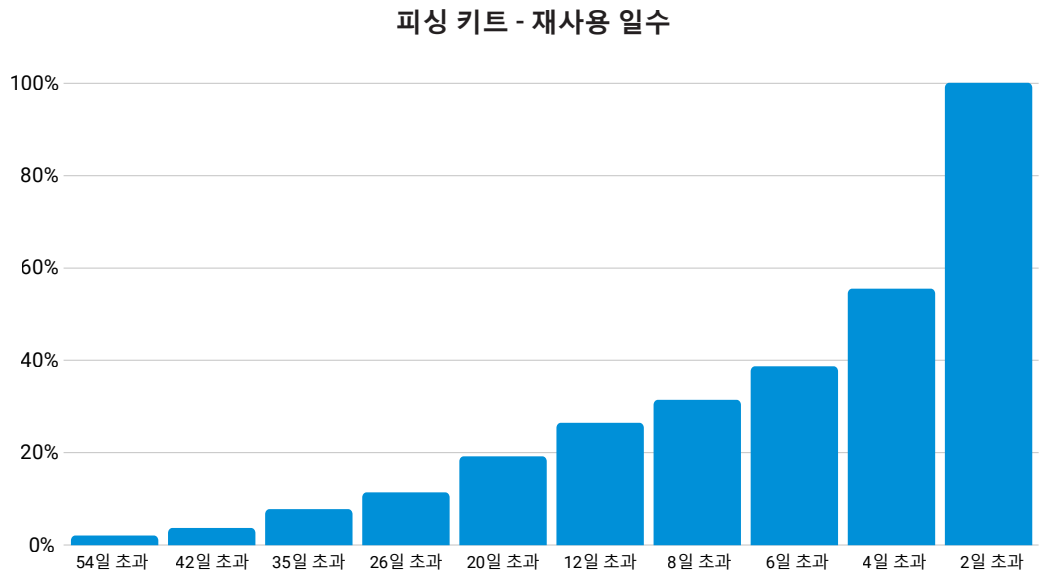


그림 20: 2022년 4분기 재사용 일수별 피싱 툴킷

새로운 공격 캠페인을 시작하기 위해 실제로 사용되는 300개의 서로 다른 피싱 툴킷을 추적한 Akamai 리서치에 따르면 2022년 4분기에 추적된 키트의 2.04%가 54일 이상 재사용되었습니다(그림 20). 또한 55.5%의 키트가 최소 4일 동안 새로운 공격 캠페인을 시작하는 데 재사용되었으며, 추적된 키트의 100%가 2022년 4분기 동안 최소 2일 이상 사용되었습니다.

결론 및 권장사항: 최신 공격에 대비한 선제적 조치

지금까지 위협 그룹, 공격자 방법론을 살펴보았습니다. 이제 이러한 모든 정보를 활용하는 방법을 알아보겠습니다. 먼저 DNS를 내부적으로 관리하거나 써드파티에 아웃소싱하는 방법을 살펴보겠습니다. 규모가 크거나 복잡한 기업의 경우 DNS 관리를 전문으로 하는 공급업체가 사용자를 위해 DNS를 관리하도록 하는 것이 좋습니다. 어느 경우든 DNS의 성능 및 보안을 모니터링해야 합니다. 그런 다음 필요한 여러 가지 제어를 고려합니다. DDoS 방어, 멀웨어 공격, 스크레이핑, 측면 이동, 유출이 주요 방어 영역입니다. 이러한 데이터 여정을 따라 모든 단계에서 막을 수 있는 모든 중요한 취약점을 찾는 것은 사이버 킬체인이라고 하는 사이버 보안 모델입니다.

이 보고서에서 다루는 공격 기법에 대한 플레이북을 만드는 것이 좋습니다. Kakbot 및 Emotet과 같은 IAB, QSnatch와 같은 봇, 실험실 환경에서 LockBit 같은 랜섬웨어, Cobalt Strike와 같은 툴을 사용하고 있는지 알아보려면 침투 팀이나 공격자에게 확인하세요. 보안 제어 디바이스가 이러한 종류의 공격을 효과적으로 경고 및 차단하고, 팀이 이를 해결할 수 있도록 교육하는 것이 중요합니다.

네트워크에서 Cobalt Strike가 탐지되면 즉시 인시던트 보고서를 작성해 조사하는 것이 좋습니다. 이 툴은 공격자가 사용할 수 있지만(이 경우 조사 및 보고되어야 함), 다른 RaaS 공격자 그룹 또는 공격자의 침입을 나타낼 수 있고 아직 방어할 수 있는 진행 중인 공격을 의미하기 때문에 반드시 알려야 합니다.

보안관제센터(SOC)의 운영 방식을 고려하고 IAB 관련 위협이 네트워크에서 정찰 중인 가능성을 나타낼 수 있는 프로세스(비트, Wget 또는 cURL 등)를 추적하는 방법을 결정합니다. 중요한 부분은 다운로드된 항목을 파악하고 아직 실행 중인 경우 중지하는 것입니다. 그런 다음 IAB가 LNK 파일, 매크로 또는 VScript 중 어떤 경우에 트리거되었는지 조사합니다. 그리고 유출이 어떻게 시작되었는지 확인합니다.

Akamai의 보안 리서치 허브에서 최신 리서치 결과를 확인하시기 바랍니다.

방법론

C2 공격 트래픽

이 보고서의 데이터는 Secure Internet Access(SIA) 제품에서 생성되며 C2(Command and Control) 공격 트래픽에 관해 설명합니다. SIA는 클라우드 기반 보안 웹 게이트웨이로, 사용자가 안전한 방식으로 디바이스를 인터넷에 쉽게 연결할 수 있도록 설계되었습니다. 이 보고서 전체에서 사용되는 두 가지 데이터 집합에는 사용자 수가 많은 엔터프라이즈 조직 또는 가정 내 개인 사용자에게 서비스하는 인터넷 공급업체의 보안 알림 데이터가 별도로 반영되었습니다. 이 데이터는 감염된 디바이스 수와 쿼리 수로 각각 측정되었습니다. 감염된 디바이스란 알려진 식별된 C2 도메인에 한 번 이상 연결된 디바이스로 정의합니다. 마찬가지로 C2 쿼리는 알려진 식별된 C2 도메인에 도달하는 쿼리로 정의합니다. 보안팀은 이 데이터를 사내에서 사용해 공격을 조사하고, 악성 행동을 플래깅해 고객에게 알리며, Akamai의 보안 솔루션에 추가 인텔리전스를 제공합니다.

저자 소개

편집 및 작성

오르 카츠(Or Katz)

일리어드 키미(Eliad Kimhy)

바데트 트리비(Badette Tribbey)

검토 및 주제별 기여

타냐 벨루소프
(Tanya Belousov)

스티브 쿱치크
(Stiv Kupchik)

시란 게즈
(Shiran Guez)

그레이스 왕
(Grace Wang)

오피르 하르파즈
(Ophir Harpaz)

스티브 윈터펠트
(Steve Winterfeld)

데이터 분석

로넌 발란틴(Ronan Ballantine)

갈 코흐너(Gal Kochner)

첼시 터틀(Chelsea Tuttle)

마케팅 및 출판

조지나 모랄레스 햄프(Georgina Morales Hampe)

쉬방기 사후(Shivangi Sahu)

인터넷 보안 현황 보고서

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

Akamai 위협 연구

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

이 보고서에서 데이터에 접속

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

기업을 노리는 위협에 대응하는 Akamai 솔루션에 대한 자세한 내용은 Secure Internet Access Enterprise 페이지를 참조하세요. 소비자와 중소기업 시장을 대상으로 하는 서비스 공급업체는 ISP를 위한 보안 인터넷 접속 서비스를 방문하세요.

Akamai는 온라인 라이프를 지원하고 보호합니다. 전 세계 대표적인 기업들은 매일 수십억 명의 사람들의 생활, 업무, 여가를 지원할 디지털 경험을 구축하고, 전송하고, 보호하기 위해 Akamai를 선택합니다. Akamai Connected Cloud는 대규모 분산 엣지 및 클라우드 플랫폼으로 앱과 경험을 사용자와 더 가까운 곳에 배치하고 위협을 멀리서 차단합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 확인하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 3월 발행