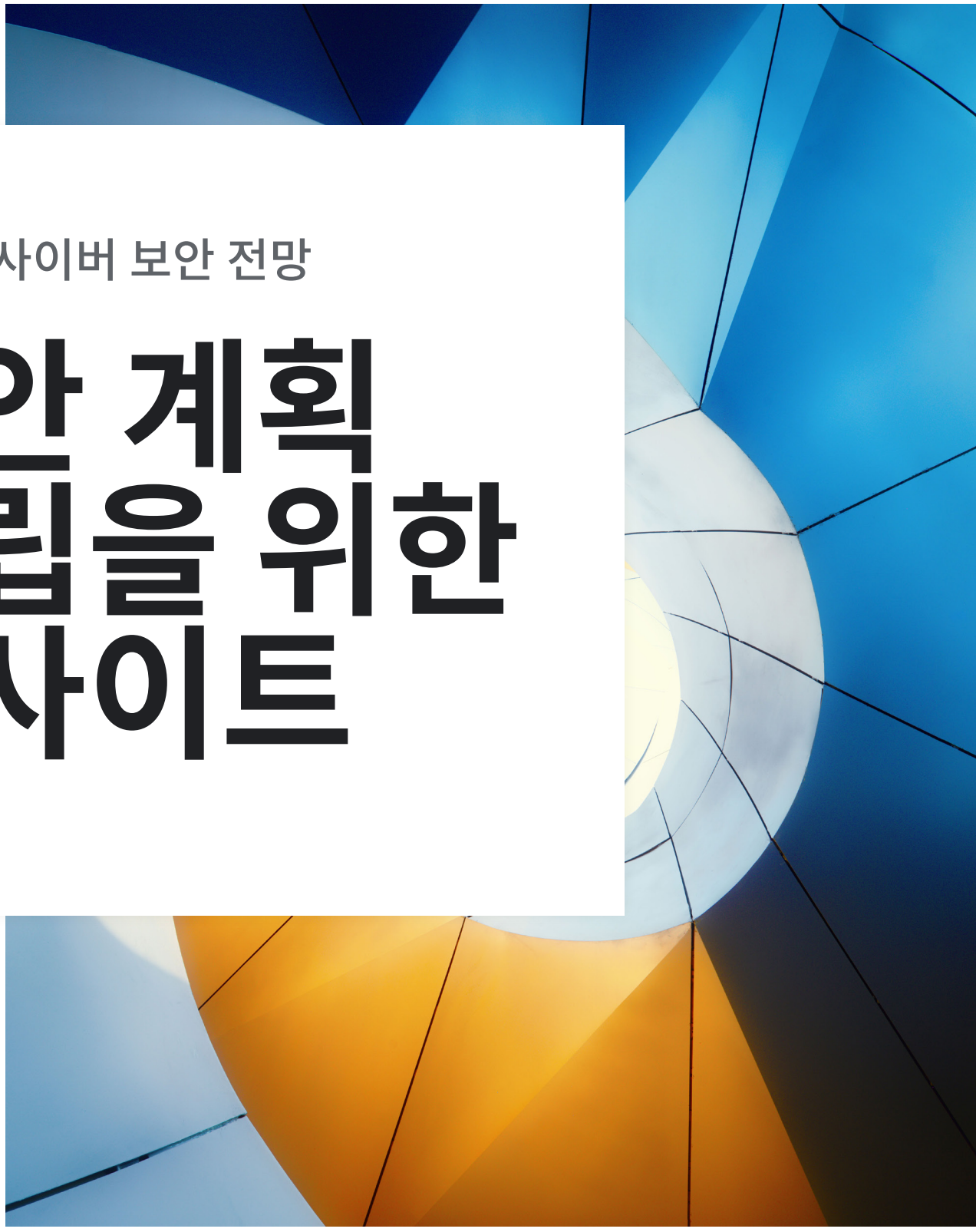
Google Cloud



2024년 사이버 보안 전망

보안 계획 수립을 위한 인사이트

소개

다가올 한 해를 내다보는 것을 '예측(prediction)'한다고 표현하는 경우도 있지만, 2024년 사이버 보안 환경에 대한 Google Cloud의 관점은 이미 관측되는 트렌드에 기반한다는 점에서 '전망(forecast)'이라는 단어에 담는 것이 더 적합하다고 생각됩니다.

Google Cloud의 2024년 사이버 보안 전망 보고서에는 Google Cloud의 여러 보안 책임자와 Mandiant Intelligence, Mandiant Consulting, Chronicle Security Operations, Google Cloud CISO실, VirusTotal 등 여러 보안팀 소속 전문가 수십 명이 공유한 미래지향적인 생각이 가득 담겨 있습니다. 이들 전문가는 최근에 이루어진 대규모 공격에 맞서 최전선에배치된 경험이 풍부한 만큼 조직과 보안팀이 2024년에 어떤 점을 염두에 두어야 하는지를 잘 알고 있습니다.

기술 발달과 함께 위협이 진화하고 공격자의 TTP(전술, 기술, 절차)도 변화하기 때문에 방어자 역시 뒤처지지 않도록 꾸준히 노력해야 합니다. Google Cloud의 2024년 사이버 보안 전망 보고서는 사이버 보안 업계가 2024년에 전개될 사이버 공격에 맞서 싸울 수 있도록 지원하기 위해 마련되었습니다.

Google Cloud

AI

피싱의 발전, 전문화, 규모 확대

피싱, SMS, 기타 소셜 엔지니어링 작업에 생성형 AI와 대규모 언어 모델(LLM)을 활용하면 음성과 동영상을 비롯한 콘텐츠와 자료가 더욱 합법적인 것처럼 보이게 됩니다. 피싱 이메일과 메시지에서 철자법이나 문법 오류, 문화적 맥락에 맞지 않는 경우를 발견하기가 더 어려워집니다. LLM이 번역을 하거나 이를 교정할 수도 있기 때문에 사용자가 문구 자체만으로는 피싱을 가려내기가 훨씬 더 어려워집니다. 공격자는 LLM을 통해 그럴듯해 보이는 콘텐츠를 가져와 스타일, 흐름, 문장이 원본과 비슷하면서 공격자의 목표에 맞게 조작된 버전을 생성할 수 있습니다.

생성형 AI를 사용하는 공격자는 이러한 캠페인을 대규모로 수행할 수 있습니다. 공격자가 이름, 조직, 직책, 부서, 심지어 건강 데이터에 접근할 수 있게 되면 매우 개인적이고 설득력 있는 맞춤형 이메일로 수많은 대중을 공격할 수 있습니다. 가령 생성형 AI를 사용해 청구서 알림 초안을 작성하는 경우, 그 자체에는 악의적인 내용이 없기 때문에 이러한 이메일을 생성하는 데 악성 LLM을 사용할 필요조차 없을 수 있습니다.

확장 가능한 정보 작전

공격자는 영리한 생성형 AI 프롬프트만 있으면 가짜 뉴스, 수신자와 활발하게 소통할 수 있는 허위 전화, AI가 생성한 가짜 콘텐츠를 기반으로 한 딥페이크 사진과 동영상을 얼마든지 만들 수 있습니다. 이러한 정보 작전은 점차 주류 뉴스로 침투하게 되고, 특유의 확장성으로 인해 뉴스와 온라인상의 정보에 대한 대중의 신뢰도가 떨어져 결국 모든 사람이 자신이 접하는 정보를 회의적으로 바라보거나 더 이상 신뢰하지 않게 될 수 있습니다. 그러면 가까운 미래에 비즈니스와 정부가 대중과 소통하기가 더욱 어려워질 것입니다.

Google Cloud는 이러한 생성형 AI 기술이 미래에 정보 작전은 물론 침입과 같은 활동의 역량을 크게 강화하여 Metasploit 또는 Cobalt Strike와 같은 취약점을 공격하는 프레임워크와 유사한 리소스와 역량이 제한된 공격자의 활동을 지원할 가능성이 있다고 봅니다. 공격자는 이미 생성형 AI를 실험하고 있으며 시간이 지남에 따라 이러한 도구를 더 많이 사용할 것으로 예상됩니다.

공격용 서비스로 사용되는 생성형 AI 및 LLM

LLM과 다른 생성형 AI 도구가 공격자의 타겟 공격을 지원하는 서비스로 개발되고 제공되는 경우가 늘어날 것입니다. 이러한 서비스는 유료 서비스로 언더그라운드 포럼에서 제공되고 피싱 캠페인과 허위 정보 확산 등 다양한 목적으로 사용될 것입니다. 이미 사이버 범죄에 사용되고 있는 랜섬웨어를 비롯해 다른 언더그라운드 서비스를 제품 형태로 성공적으로 제공한 사례가 확인되었습니다.

데이터 해석, 위협 이해, 보안 강화

사이버 방어팀은 생성형 AI 및 관련 기술을 사용하여 공격자에 대한 감지, 대응, 추적을 대규모로 강화하고 분석 및 리버스 엔지니어링과 같이 시간이 많이 드는 기타 작업의 속도를 높일 수 있습니다. 특히 조직이 대량의 데이터를 합성하고 위협 인텔리전스에서 이를 컨텍스트화하여 실행 가능한 감지 또는 기타 분석을 산출하는 방식을 추진하는 데 AI가 요긴하게 사용될 것입니다. 2024년에는 이 노력이 결실을 맺어 AI와 생성형 AI가 이러한 대규모 데이터 세트를 토대로 취해야 할 조치를 분석하고 추론하는 인간의 역량을 강화하는 역할을 하리라 예상합니다. 고도의 기밀성을 유지하면서 고객별 데이터를 오버레이하는 새로운 방식이 등장하여 조직이 영향력 있는 조치를 대규모로 신속하게 전개할 수 있게 될 것입니다. 이것은 보안 목적으로 AI를 활용하는 조직에서 향후 몇 년 안에 이룰 수 있는 혁신의 일부에 불과하며 궁극적으로는 반복 업무 감소, 위협 과부하 해결, 확대되는 인재 격차 해소에 도움이 될 것입니다.

빅4 국가

중국

중국의 활동은 내부 체제 안정과 영토 보전과 같은 장기적인 우선순위가 계속 주도할 것입니다. 타이완 관련 문제, 중국의 지역 패권과 영향력, 주요 시장에 대한 경제적 영향력도 여기에 포함됩니다. 중국의 사이버 첩보원은 계속해서 은밀하게 활동하면서 탐지 기회를 줄이며 추적을 피할 것입니다. 이들 첩보원은 제로데이 취약점 악용, 네트워크 엣지 시스템 표적화, 공급망 침해는 물론, 침해한 네트워크 내부의 트래픽 및 공격자와 피해자 간 트래픽을 모두 위장하도록 설계된 봇넷과 프록시 네트워크의 활용 같은 전술을 계속 사용할 것으로 예상됩니다.

아울러 중국은 혼란을 일으키는 와해성 작전을 개시하고 국내 정치 및 군사적 목적의 캠페인을 전개할 수 있는 군사 및 민간 병력을 육성할 것으로 예상됩니다. 갈등이 고조되는 시기를 틈타 중국의 공격자가 혼란을 일으키는 와해성 작전을 펼칠 가능성이 있다는 사실은 전 세계 조직에 위협이 되며 일상에서 이루어지는 필수 활동, 핵심 인프라, 안전에 영향을 줄 수 있습니다.

러시아

러시아의 사이버 위협 활동은 2024년 이후에도 주로 우크라이나를 대상으로 정보 수집, 혼란을 일으키는 와해성 공격, 정보 작전의 빈도 증가와 같은 형태로 나타나리라 예상됩니다. 또한 우크라이나 밖에서도 정부, 국방, 시민 사회, 비영리, 에너지 관련 기구를 표적으로 하는 등 오랜 우선순위에 따라 러시아의 사이버 첩보 작전(전략 정보 수집 임무일 가능성이 높음)이 지속적으로 전개되는 모습을 보게 될 것입니다.

러시아에 대한 제재 조치는 러시아의 기술 및 군사 혁신에 계속 타격을 줄 것입니다. 러시아는 자국의 전문성 부재를 메우기 위해 지식 재산을 더 많이 훔칠 가능성이 있습니다. 이 같은 행동은 지난 몇 년에 걸쳐 발생한 중국의 지식 재산 도용을 모델로 삼은 것입니다.

북한

북한에 기반을 둔 사이버 위협 활동은 금전적 목적의 작전 비중이 점점 더 커지고 있으며 특히 암호화폐 산업과 기타 블록체인 관련 플랫폼을 표적으로 삼는 양상을 뚜렷하게 보입니다. 2024년에는 무기와 핵 프로그램은 물론 사이버 작전과 인프라 확보를 위한 자금을 마련하기 위해 암호화폐 및 NFT를 갈취하는 데 더욱 집중할 것으로 예상됩니다.

특히 북한은 중앙 정부의 재정 부담을 줄이기 위해 국가 주도로 자급자족 방식 작전을 펼치는 것으로 확인되었습니다. 이 자금 조달 방식은 공동 번영을 위한 자력갱생이라는 북한 정권의 주체 사상에 부합하는 것이기도 합니다. 최근 몇 년간 첩보 작전에 자금을 조달하기 위한 사이버 범죄 캠페인이 상대적으로 증가하는 모습을 보였으며 이러한 추세는 계속 이어질 것으로 보입니다. 또한 북한은 공급망 침해를 더욱 늘릴 수 있는 기회를 활용하리라 예상됩니다.

이란

향후 이란에서 일어나는 국가 차원의 사이버 위협 활동은 이란의 지정학적 야망, 경제 발전의 필요성, 인근 지역 라이벌 국가인 사우디아라비아 및 이스라엘과의 경쟁, 정권 안정 및 존속에 대한 위협, 이란인 디아스포라와 반대 세력에 대한 감시가 주요 목적이 될 것으로 보입니다.

2023년 10월 7일 이스라엘 중남부 지방의 민간인과 군인을 대상으로 다각도로 이루어진 하마스의 무력 공격 이후 이스라엘은 이란, 팔레스타인, 레바논 공격자와 연결된 사이버 첩보원을 더 큰 위협으로 받아들이고 있습니다. 이란의 공격자는 정보 수집, 정보 작전, 해킹 및 유출 혼합 작전 또는 그 밖에 혼란을 일으키는 와해성 공격을 수행할 것으로 예상됩니다.

글로벌 전망

제로데이 취약점 및 엣지 기기 악용 지속

2012년 이후로 제로데이 취약점을 악용하는 공격이 전반적으로 증가해 왔으며 이 추세대로라면 2023년이 2021년 기록을 넘어설 것으로 보입니다. 2024년에는 국가 차원의 공격자뿐 아니라 사이버 범죄 집단에서도 제로데이 취약점을 더 많이 악용할 것으로 예상됩니다. 그 이유 중 하나는 공격자가 환경에 대한 액세스를 최대한 오래 유지하길 원한다는 점입니다. 제로데이 취약점과 엣지 기기를 악용하면 피싱 이메일을 보내고 멀웨어를 배포하는 등의 임무를 수행할 때보다 훨씬 더 오랫동안 환경에 대한 액세스를 유지할 수 있습니다. 보안팀과 솔루션을 통해 악성 피싱 이메일과 멀웨어를 식별하는 능력이 개선된 만큼 공격자는 감지를 피해 다른 길로 우회할 것입니다. 특히 엣지 기기와 가상화 소프트웨어는 모니터링하기가 까다롭기 때문에 공격자에게 매력적인 표적이 됩니다. 사이버 범죄자들은 제로데이 취약점을 사용하면 피해자 수, 그리고 최근 발생한 대규모 갈취 사건을 고려할 때 랜섬웨어나 갈취 요구에 높은 대가를 지불할 조직 수를 늘릴 수 있다는 사실을 알고 있습니다.

미국 선거를 표적으로 한 사이버 활동

미국 대선이 있는 해로 접어들면서 정부 후원을 받는 공격 집단을 포함한 여러 공격자가 다양한 사이버 활동을 펼칠 것으로 보입니다. 이러한 활동은 선거 시스템을 표적으로 한 첩보 및 영향력 작전, 후보자를 사칭하는 소셜 미디어 활동, 유권자를 대상으로 한 정보 작전 등의 형태가 될 수 있습니다. 선거 후에도 이러한 활동은 수그러들지 않을 전망입니다. 잠재적으로는 행정부 교체 시기에 의사 결정의 우위를 차지하기 위해 미국 정부를 대상으로 한 국가 차원의(특히 중국, 러시아, 이란) 스피어피싱과 기타 공격이 늘어날 것으로 보고 있습니다. 규모와 작전 속도를 높이는 데 생성형 AI 도구가 활용됨에 따라 2024년에는 이러한 캠페인이 더욱 만연할 수 있습니다.

혼란을 일으키는 핵티비즘의 증가

2022년과 2023년에는 러시아의 침공이 계속되는 가운데 러시아나 우크라이나에 대한 지지를 표명하는 공격자와 관련한 핵티비스트 활동이 다시금 증가했습니다. 마찬가지로 최근 발발한 하마스와 이스라엘 간 분쟁과 함께 핵티비스트 활동이 급증했습니다. 이러한 활동으로는 DDoS 공격, 데이터 유출, 변조 등이 있습니다. 특히 Mandiant Intelligence는 두 가지 맥락에서 표면상으로는 핵티비스트 집단이지만 지지를 표명한 국가의 내러티브와 목표에 상당히 부합하고 평균 이상의 역량을 보이는 집단을 추적하고 있습니다. 현재로서는 배후에 있는 특정 국가와의 연관성을 확인할 수 없지만 과거에 러시아와 이란 소속 단체들이 핵티비스트를 가장해 활동한 전력이 있다는 점에 주목하고 있습니다. 배후설을 부인하면서도 이러한 작전을 성공리에 전개할 수 있음을 인지한 국가에서 민간 및 군대를 대상으로 이러한 사이버 공격을 감행할 가능성이 높다는 것이 Mandiant Intelligence의 판단이며, 이러한 전술의 사용이 결국 물리적 피해로까지 확대될 수 있다고 추정하고 있습니다.

모든 국가에서 사이버 무기의 표준 기능이 된 와이퍼

2022년 러시아가 우크라이나를 침공하기 전에 러시아의 APT(Advanced Persistent Threat, 지능형 지속 공격) 그룹은 우크라이나 표적에 액세스하여 무력 작전에 맞춰 동시에 혼란을 일으키는 공격을 개시했습니다. 다른 나라에서도 사이버 무기에 와이퍼 멀웨어를 추가하여 이 기법을 모방할 것입니다. 2024년에는 타이완 해협의 긴장을 비롯한 글로벌 안보 위협 문제가 지속되는 만큼 전략적으로 중요한 표적에 혼란을 일으키는 와이퍼 멀웨어를 사전에 배치해 액세스하는 모습을 보일 것입니다.

우주 기반 인프라를 대상으로 한 공격

우크라이나의 경우에는 분쟁 중에 우주 기반 기술(예: Starlink, 기타 인공위성 및 통신 네트워크)에 크게 의존하는 모습을 볼 수 있었습니다. 2024년에는 국가 차원의 후원을 받는 고도화된 사이버 공격자가 첩보 활동과 함께 우주 기반 인프라 및 관련 지상 지원 인프라와 통신 채널을 공격해 적을 차단, 방해, 거부, 약화, 파괴 또는 기만하고 첩보 활동을 수행하기 위한 전방위적인 컴퓨터 네트워크 취약점 공격 능력을 갖췄다는 증거가 드러날 것으로 예상합니다.

하이브리드 및 멀티 클라우드 환경을 표적으로 하는 공격의 발전과 영향력 증대

2023년에 Mandiant는 VMware와 협업하여 게스트 가상 머신(VM)에서 공격자가 코드를 실행할 수 있도록 허용하는 제로데이 취약점을 완화했습니다. 이 취약점의 영향은 단일 하이퍼바이저로 제한되었지만 공격자가 클라우드 환경을 표적으로 삼아 지속성을 확보하고 횡 방향으로 이동하는 방법을 찾고 있었다는 사실이 입증되었습니다. 2024년에는 이러한 기술이 클라우드 환경의 경계를 넘어 더욱 발전할 것으로 보고 있습니다. 공격자는 잘못된 설정과 ID 문제의 취약점을 공격하여 다양한 클라우드 환경 내부에서 횡 방향으로의 이동을 시도할 것입니다.

클라우드의 서버리스 서비스를 더 적극적으로 사용하는 공격자

2023년에는 서버리스 인프라에서 크립토마이너의 배포 횟수가 증가하는 현상을 확인했습니다. 2024년에는 사이버 범죄자와 국가 기반 사이버 공격자들이 클라우드 내 서버리스 기술을 더 적극적으로 활용할 것으로 예측됩니다. 공격자가 서버리스로 전환하는 이유는 개발자가 서버리스를 채택하는 이유와 동일합니다. 바로 확장성과 유연성이 높고 자동화된 도구로 배포할 수 있다는 장점 때문입니다.

지속되는 갈취 작전

전 세계 기업과 사회에 가장 큰 영향을 끼치는 사이버 범죄는 여전히 갈취 작전이 될 가능성이 높습니다. 2022년에는 성장세가 주춤했지만 도난 데이터에 대한 광고와 갈취 수익 추정치를 고려할 때 2023년에도 이러한 공격이 증가하고 있으며 시장 전반에 큰 변동 없이 2024년에도 이러한 성장세가 지속될 것으로 보입니다.

첩보 활동 및 슬리퍼 봇넷'

사이버 첩보 작전은 계속해서 공격을 확장하는 더 많은 방법을 찾는 동시에 작전을 위한 추가적인 작전보안(Operations Security, OPSEC)을 수립할 것입니다. 첩보 집단은 기존 및 신규 취약점 공격을 조합하여 취약한 사물 인터넷, SOHO(소규모 사무실 및 홈 오피스), 지원 종료 기기 및 라우터로 슬리퍼 봇넷'을 만들 것입니다. 이러한 슬리퍼 봇넷'은 필요에 따라 사용되다가 적발되거나 더 이상 필요 없으면 폐기되므로 활동을 추적하고 책임 소재를 파악하는 작업이 어려워집니다. 이러한 슬리퍼 봇넷'은 DDoS 공격처럼 공격을 증폭시키는 데 많은 기기가 동원되는 기존 봇넷과는 다를 것입니다.

구식 기술의 부활

공격자들이 감지를 피하기 위해 새로운 기술을 통합하는 가운데 널리 알려지지 않은 구식 기술을 부활시키는 공격자도 있으리라 예상합니다. 예를 들어 2013년에 연구자들은 문서화된 Windows API의 암호화 함수 대신 문서화되지 않은 SystemFunctionXXX 함수를 사용하는 것에 대해 블로그 게시물을 작성한 일이 있습니다. 이 기법은 2022년 4분기가 되어서야 여러 보안 연구자들이 이 기법에 대해 논의하고 자신의 블로그와 GitHub에 코드 스니펫을 공개하기 시작하면서 대중화되기 시작했습니다. 그 시점부터 이 기법을 구현하는 멀웨어 샘플이 VirusTotal에서 더 많이 나타나기 시작했습니다. 또한 2012년 멀웨어 분석 보고서 기술되어 있는 안티 가상 머신(안티 VM) 기법이 최근에 사용된 사례도 확인되었습니다. 많은 국가에서 하이퍼바이저를 두루 사용하는 것은 아니기 때문에 이 기법은 탐지 규칙에 포함되어 있지 않습니다.

최신 프로그래밍 언어로 계속 마이그레이션하는 해커들

해커들은 Go, Rust, Swift 같은 프로그래밍 언어로 계속해서 더 많은 소프트웨어를 개발할 것입니다. 이러한 언어가 우수한 개발 환경과 낮은 진입 장벽, 대규모 표준 라이브러리, 서드 파티 패키지와의 손쉬운 통합을 제공하기 때문입니다. 이러한 언어와 생태계를 기반으로 하면 복잡한 멀웨어를 신속하게 개발하여 새로운 멀웨어를 더 저렴하게 작성하고 탐지를 피할 수 있습니다. 즉, 공격자가 사용하는 도구 세트가 변화할 것이며 이에 따른 새로운 탐지 서명이 필요하다는 뜻입니다. 불행히도 이러한 최신 언어는 대규모 런타임(Go) 또는 최신 컴파일러 기법(Rust)을 사용하여 리버스 엔지니어링 작업을 더 어렵게 만드는 경우가 많습니다. 프로텍터를 사용하지 않고 패킹과 난독화를 사용하여 얻는 이점이라고 할 수 있습니다.

소프트웨어 패키지 관리자를 통해 공급망 공격의 표적이 되는 개발자

최근 몇 년간 IconBurst와 같이 NPM(Node.js 패키지 관리자)을 대상으로 하는 공급망 공격은 공격자가 소프트웨어 개발자를 어떻게 표적으로 삼는지를 보여주었습니다. 특히 우려되는 시나리오는 악성 패키지를 설치하여 공격을 받은 개발자의 소스 코드에 공격자가 액세스하여 백도어를 추가할 수 있게 되는 상황입니다. 이는 적은 비용으로 큰 영향을 끼치는 공격 방식입니다. 결과적으로, 특히 공격자가 PyPI(Python) 및 crates.io(Rust)와 같이 비교적 경계가 느슨한 다른 패키지 관리자로 전환하면서 이러한 종류의 공격은 더욱 보편화될 것으로 예상됩니다. 경계심을 늦추지 않고 이러한 소프트웨어 라이브러리 소스를 모니터링해야 합니다.

모바일 사이버 범죄의 증가

2024년에는 사이버 범죄자 또는 사기범이 가짜 소셜 미디어 계정을 통해 가사 도우미나 마사지와 같은 편의 서비스 홍보를 하고, 은행 또는 정부 기관을 사칭해 메시지를 보내거나, 피해자가 휴대기기에 악성 애플리케이션을 설치하도록 속이는 스푸핑 팝업 알림과 같은 신종 소셜 엔지니어링 전술을 계속 사용할 것으로 예상합니다.

사이버 보험료의 안정화

보험 시장에는 변동이 많다는 특징이 있습니다. 하드 마켓이란 보험료가 상승하고 보장 범위는 제한되는 현상을 가리키고 소프트 마켓이란 보험료는 낮아지고 보장 범위는 넓어지는 현상을 가리킵니다. 지난 몇 년간 보험료가 상승하고 보장 범위가 제한되는 특성을 보였던 사이버 보험 시장이 큰 조정을 겪은 후 이제 소프트 마켓으로 변하기 시작했습니다. 시장에 진입하는 경쟁업체가 늘고 보험사마다 사이버 성장 목표를 야심 차게 추진하면서 치열해진 경쟁 구도 덕분에 그간 업계에서 상승 국면에 있던 보험료가 드디어 안정세를 찾을 것으로 예상됩니다. 시스템 관련 위험에 대한 보장 범위는 계속 제한되는 방향으로 전반적인 트렌드가 흘러갈 것으로 보이지만 보험사가 이 새로운 환경에서 다른 방식으로 경쟁하기 위해 보장을 확대할 가능성도 있습니다.

보안운영 중심의 통합

2024년에는 보안 작업 솔루션에서 통합형 위험 및 위협 인텔리전스를 요구하는 고객이 점점 많아지면서 보안운영(Security Operations, SecOps) 내에 더 많은 통합 기능이 생길 것으로 예상합니다. 고객은 클라우드, 멀티 클라우드, 온프레미스, 하이브리드 환경으로 구성된 전체 네트워크 환경을 아우르는 통합 생태계를 요구하고 보안 프로그램을 즉시 사용할 수 있도록 공급업체가 확실한 워크플로와 지침, 콘텐츠를 제공하기를 기대할 것입니다.

일본 및 아시아 태평양(JAPAC) 전망

선거를 둘러싼 사이버 활동

2024년에 선거를 치르는 나라로는 타이완, 대한민국, 인도, 인도네시아 등이 있습니다. 과거 관찰된 바에 따르면 사이버 첩보, 사이버 범죄, 핵티비즘, 정보 작전 공격자는 이러한 전환점이 되는 주요 이벤트에 관심을 보이곤 했습니다. 선거가 사기는 물론 정보 수집을 위한 미끼로 활용되는 사례가 관찰될 것입니다. 중국에서 새롭게 발표한 지도는 인도와 인도네시아의 선거 과정에서 논쟁을 불러일으킬 수 있습니다.

지속적인 문제가 될 '돼지 도살' 사기

사이버 범죄와 인신매매의 요소를 모두 지닌 돼지 도살 사기는 2024년에 JAPAC 국가의 법 집행 기관에서 계속 문제가 될 것입니다. 돼지 도살 사기는 사기범이 피해자의 신뢰를 얻기 위해 장기간에 걸쳐 잠재적인 연애 상대인 척 하는 일종의 온라인 사기입니다. 사기범은 피해자의 신뢰를 얻으면 여러 금융 사기에 투자하도록 설득하기 시작합니다. 2023년 8월 유엔 보고서는 이러한 사기범 중 상당수가 사실은 피해자이며 인신매매를 당해 사기 작전에 강제로 동원되고 있다고 설명합니다. 2023년 7월 필리핀에서는 사이버 범죄 노동에 강제로 동원됐던 2,700명을 구출했습니다. 해당 보고서에 따르면 상황은 여전히 유동적이며, 필리핀 안팎에서 온라인 범죄에 강제 동원되는 사람이 수십만 명에 이릅니다.

전술, 기술, 절차의 변화

JAPAC 지역에서 엔드포인트 감지 및 대응 솔루션이 더욱 보편적으로 사용되고 있으며 전반적으로 조직의 보안이 더 성숙해지고 있습니다. 결과적으로 리소스가 풍부한 공격자는 감지 가능성을 최소화하기 위해 의도된 전술을 점점 더 적극적으로 활용할 것입니다. 이러한 현상이 전 세계적으로 목격되고 있습니다. 이 지역의 방어팀은 보안, 네트워킹, 가상화 소프트웨어에서의 제로데이 취약점 악용, 라우터 및 기타 엣지 기기에 대한 표적 공격, 피해자 네트워크 안팎에서 공격자 트래픽을 왜곡하고 숨기기 위한 다른 방법의 사용에 대비해야 합니다.

유럽, 중동, 아프리카 (EMEA) 전망

표적이 될 가능성이 있는 유럽의회 선거

6월에 열릴 유럽의회 선거는 사이버 첩보와 정보 작전을 모두 수행하는 공격자에게 매력적인 표적이 될 것입니다. 러시아는 유럽 전역에서 활동 수준이 매우 높다는 점에서 가장 명백한 위협이 되고 있습니다. 우크라이나 침공 이후 APT29가 대륙 전역의 정부 기관을 표적으로 활발하게 활동하고 있고 동시에 유럽에서 분열을 일으키려는 친러시아 정보 작전도 전개되었습니다. 이러한 노력은 선거를 앞두고 더욱 격화될 가능성이 있습니다. 러시아는 사이버 첩보 캠페인에서 훔친 정보를 퍼뜨리기 위해 정보 작전을 펼친 이력이 있습니다. 따라서 유럽 정부는 정보 작전과 네트워크 침입 사이의 다양한 연결 고리를 이해하는 것이 필수적입니다.

유럽 선거는 러시아 외에도 더 광범위한 위협에 직면할 수 있습니다. 최근 몇 년간 벨라루스와 연계된 공격자의 활동이 크게 늘면서 동부 유럽에서 발생하는 정보 작전을 위한 기술 지원도 증가하고 있습니다. 친 중국 정보 작전은 여러 유럽 국가에서 캠페인의 범위와 규모를 크게 늘렸습니다. 유럽 정부는 선제적이고 복원력 있는 방어 체계를 구축하기 위해 정보 작전에 채택된 다양한 기법을 이해해야 합니다.

아프리카에서의 허위 정보 캠페인

디지털 시대에는 허위 정보가 지정학적 영향력을 넓히는 강력한 도구가 되었습니다. 러시아와 중국은 아프리카 국가를 표적으로 삼아 잘못된 정보를 퍼뜨리고, 갈등을 조장하고, 민주주의 기관을 약화시키는 사이버 캠페인을 전개하고 있으며 2024년에도 그 기세는 수그러들지 않을 것으로 보입니다. 예상컨대 중국과 러시아 단체는 스마트폰, 컴퓨터, 전기자동차와 같은 많은 최첨단 제품의 필수 원료인 희토류 산업을 표적으로 삼을 것으로 보입니다. 이러한 자원에 대해 통제권을 확보함으로써 러시아와 중국이 아프리카에서 경제적, 전략적 입지를 강화할 수 있기 때문입니다.

러시아와 중국에서 허위 정보를 사용해 아프리카에 영향력을 행사하는 또 다른 방법은 권위주의 정권을 지원하는 것입니다. 이러한 정권은 이의 제기를 탄압하고 정보에 대한 접근을 제한하기 때문에 러시아와 중국에서 자신들의 선전을 퍼뜨리고 민주적 가치를 약화시키기가 더욱 수월해집니다. 아프리카에 대한 허위 정보 공세와 집중 공략은 장기전이며 2024년은 이러한 활동이 최고조를 보이는 해가 될 것으로 보입니다.

파리를 넘어 유럽에 대한 공격 표면 확장의 계기가 될 2024년 올림픽

파리에서 개최되는 2024년 하계 올림픽 기간에 입장권 발매 시스템과 상품을 표적으로 한 사이버 범죄가 벌어질 것으로 예상합니다. 특히 금융 정보나 사용자 인증 정보를 요청하는 피싱 캠페인이 급증할 것입니다. 공공 기관과 은행은 경계를 늦춰서는 안 됩니다. 올림픽을 이용해 프랑스를 넘어 유럽 국가들의 정치 체제를 불안정하게 만들고 압박을 가하려는 지정학적 활동이 있을 것으로 보입니다. 또한 올림픽은 직접적이든(입장권 판매 등의 이벤트 관련) 간접적이든(관련 숙소 임대, 대중교통 등) 잘못된 정보와 허위 정보의 표적이 될 가능성이 높습니다.

결론

새로운 기술이 보안팀에 도움이 될 수도 있지만 공격 표면을 확장하는 역할을 할 수도 있습니다. 2024년에는 빠르게 진화하는 생성형 AI의 세상이 공격자에게 설득력 있는 피싱 캠페인과 정보 작전을 대대적으로 전개할 수 있는 새로운 방법을 제공할 것으로 예상됩니다. 하지만 방어자 또한 동일한 기술을 사용하여 공격자에 대한 탐지, 대응, 추적을 강화하고, 더 나아가 반복 업무를 줄이고 위협 과부하를 해결하며 확대되는 기술 격차를 해소할 것입니다.

2024년에도 중국, 러시아, 북한, 이란으로 꼽히는 빅4 국가가 각자의 목표를 달성하기 위해 첩보, 사이버 범죄, 정보 작전, 기타 캠페인을 수행하면서 활동을 이어갈 것으로 예상합니다. 조직의 보안이 발달하면서 이러한 공격의 많은 수가 제로데이 취약점 악용 및 엣지 기기 표적 공격을 비롯해 탐지 피하는 기술을 사용할 것으로 보입니다.

모두가 2024년 한 해 동안 개최될 수많은 주요 이벤트를 중심으로 전개될 전 세계 활동에 대비해야 합니다. 여기에는 미국과 유럽의회, 여러 나라에서 치러지는 선거, 파리 하계 올림픽도 포함됩니다. 아울러 전 세계 주요 갈등이 2024년까지 이어짐에 따라 혼란을 일으키는 핵티비즘의 증가에도 대비해야 합니다.

사이버 보안 환경은 끊임없이 진화합니다. 때로는 예상하지 못한 새로운 방식으로 진화하기도 합니다. 방어팀은 자원이 한정된 경우가 많기에 이를 따라잡는 일이 부담스러울 수밖에 없습니다. Google Cloud의 2024년 사이버 보안 전망 보고서는 보안 전문가가 다가오는 한 해의 확실성과 불확실성 모두에 대비할 수 있도록 돕기 위한 것입니다. Google Cloud가 최전선에서 얻은 이 지식이 대비 과정에 도움이 되길 바랍니다.

참여자

Google Cloud의 2024년 사이버 보안 전망 보고서에 인사이트를 제공한 Google Cloud의 보안 리더를 소개합니다.
Charles Carmakal, CTO of Mandiant Consulting
Sandra Joyce, VP of Mandiant Intelligence
Sunil Potti, GM and VP of Cloud Security
Phil Venables, Chief Information Security Officer

이 밖에도 다음과 같은 많은 Google Cloud 직원이 이 보고서에 참여했습니다.

Willi Ballenthin	Mike Hom	Mike Raggi
Dan Black	Renze Jongman	Alice Revelli
Sarah Bock	Dan Kennedy	Nick Richard
Anton Chuvakin	Cris Kittner	Matt Shelton
Jamie Collier	Karen Kukoda	Monica Shokrai
Vivek Chudgar	Steve Ledzian	Daniel Sislo
Charles deBeck	Yihao Lim	Genevieve Stark
Vicente Diaz	Keith Lunden	Kelli Vanderlee
Eric Doerr	Jens Monrad	Alden Wahlstrom
Renato Fontana	Joseph Pisano	Dominik Weber
David Grout	Fred Plan	Richard Weiss
Scott Henderson	Ofir Rozmann	Jess Xia