“방탄” 호스팅 제공업체: 사이버 범죄 인프라에 드러난 허점들

사이버 범죄자들은 범행에 성공하기 위해 안정적이고 추적이 불가하며, 복원력이 있는 인프라에 의존합니다. 모든 네트워크 결함, 신용 도용, 랜섬웨어, 데이터 도난 또는 불법 포럼 내에서의 판매 뒤엔, 사이버 범죄자들이 정체를 들키지 않고 범죄를 저지를 수 있는 안정적인 인프라가 존재합니다.

하지만 사이버 범죄자들에게는 발각되지 않고 추적을 피하는 것이 점점 더 어려운 과제가 되고 있습니다. 전 세계 정부, 법 집행 기관, 그리고 민간 부문 간의 협력이 강화되면서, 그들이 온라인에서 익명성을 유지하는 것이 더욱 힘들어지고 있습니다. 이와 더불어, 사이버 범죄자들의 극 소수만이 안정적인 인프라를 자체적으로 유지할 수 있는 능력과 지식을 갖췄습니다. 그렇기 때문에 사이버 범죄자들은 자신들이 피해자와 이익에 집중할 수 있도록 자신들을 대신해 이러한 서비스를 제공할 수 있는 불법 인프라 제공업체들을 찾아 나섭니다.

‘서비스형 사이버 범죄(Cybercrime-as-a-service)’는 다양한 악의적 사이버 행위를 지원하기 위해 생성된 암시장을 의미합니다. 이 암시장에서 사이버 범죄자들이 온라인상의 타겟을 희생시키도록 지원하는 다양한 도구, 서비스 및 정보가 구매 가능하며, 이는 끊임없이 증가하고 진화하고 있습니다. 잠재적 사이버 범죄자들은 네트워크에 대한 접근 권한, 보안 장치를 우회하는 데 도움이 되는 도구, 그리고 피해자의 개인 정보를 훔치는 데 사용되는 악성 소프트웨어를 구매할 수 있습니다. 방탄 호스팅(Bulletproof Hosting, BPH) 제공업체는 해당 생태계의 일원으로 사이버 범죄자들에게 안정적인 인프라를 제공합니다. 가장 핵심은, 하나의 BPH 제공업체가 몇 백명의 사이버 범죄자를 전세계적으로 피해자들을 표적으로 삼을 수 있도록 직접적으로 도울 수 있다는 점입니다.

“방탄” 호스팅(BPH) 제공업체는 무엇인가요?

단순하게 설명 드리면, BPH 제공업체는 사이버 범죄자들이 운영할 수 있는 가상 그리고/또는 물리적 인프라를 임대합니다. BPH 제공업체는 악의적인 사이버 행위자(사이버 범죄자를 포함한)가 불법 콘텐츠를 호스팅하고 인터넷에서 활동을 운영할 수 있도록 해주는 특정한 종류의 인터넷 인프라 서비스입니다.

“방탄”이란 단어는 마케팅 전략에 불과합니다. 현실에서 이러한 서비스도 다른 인프라 제공업체와 마찬가지로 중단될 가능성이 있습니다. 대신 BPH 제공업체들은 법 집행 기관의 요청이나 기타 콘텐츠 삭제 요청을 따르지 않으며, 피해자들의 악용 신고나 구독자의 요청 통지도 무시합니다. 이는 사이버 범죄자들이 법 집행 기관이나 기타 요청에 의해 운영자가 인프라 임대를 종료할 것이라는 우려 없이 의사소통하고 불법 포럼 및 웹사이트를 운영하며, 악성코드 및 피싱 캠페인을 전파하고, 자금을 세탁할 수 있다는 것을 의미합니다.

BPH 제공업체들은 고의적으로 사이버 범죄 생태계에 참여하며 금전 탈취가 목적인 심각한 사이버 범죄가 가능하도록 합니다. 범죄자들이 BPH 제공업체를 이용함으로써 호주 기관들과 그 고객들에게 영향을 미친 대규모 사이버 보안 사고들이 발생했습니다. 이러한 사고의 결과로는 파괴적인 랜섬웨어 공격, 데이터 갈취 및 민감 정보 도난 등이 포함됩니다.

암시장 포럼에 게시된 BPH 제공업체 광고 예시:

BPH 제공업체들은 어떤 방식으로 운영되나요?

각 BPH 제공업체의 사업 모델에는 차이가 있습니다. 가장 일반적인 방법은 사이버 범죄자 고객에게 IP 주소를 임대하고, 복잡한 네트워크 전환 기법을 사용해 그들의 위치, 신원 및 활동을 숨겨주는 것입니다. 많은 경우에 BPH 제공업체들은 다른 합법적인 호스팅 제공업체, 데이터 센터 또는 인터넷 서비스 제공업체(ISP)로부터 IP 주소와 서버를 재판매하거나 임대합니다. 이러한 ‘업스트림’ 제공업체들은 자신들이 BPH 제공업체에 인프라를 제공하고 있다는 사실과, 이들이 다시 사이버 범죄자들에게 ‘다운스트림’ 서비스를 제공하고 있다는 사실을 인지하지 못할 수도 있습니다.

BPH 제공업체들은 자신들의 고객을 식별하는 것이 더욱 어렵도록 네트워크와 시스템 구성을 설계합니다. 예를 들어, 이들은 고객의 활동과 관련된 인터넷 식별 요소(예: 할당된 IP 주소나 도메인 이름)를 자주 변경합니다. 이러한 기법은 특정 시점에 범죄자나 고객이 사용한 IP 주소와 사건을 연관 짓기 어렵게 만들어 대응자와 수사관들에게 큰 어려움을 줍니다. 또한, BPH 제공업체들은 종종, 악성 사이버 활동에 대한 공식적인 조사 및 방지 조치가 없거나 느슨하고 사이버 규제가 관대한 국가의 인프라를 활용합니다.

BPH 제공업체는 합법적인 인프라 제공업체와 어떤 차이가 있나요?

BPH 제공업체에 대한 조치가 사이버 범죄 위험에 미치는 영향

BPH 제공업체들에 대한 조치는 수백에서 수천 명에 이르는 사이버 범죄자들을 한 번에 차단할 수 있는 귀중한 기회를 제공합니다. 다양한 사이버 범죄자들과 악의적인 사이버 행위자들은 이러한 서비스를 이용해 범죄를 더 쉽게 저지르면서, 자신들의 활동이 삭제 요청이나 악용 신고에도 불구하고 계속 숨겨지고 유지될 것이라고 믿고 있습니다.

그러나 법 집행 기관, 정부 기관, 그리고 민간 부문은 이러한 불법 인프라 제공업체들에 대항해 협력 대응하고 있으며 이에는 이미 정체가 알려진 BPH 제공업체에서 발생하는 인터넷 트래픽을 선제적으로 차단하는 등의 방어 조치가 포함됩니다. 이러한 활동은 호주 및 파트너 네트워크와 상호작용하는 사이버 범죄의 양을 줄이는 데 도움이 됩니다. 이들 네트워크에는 BPH 제공업체가 인터넷에 접속해 사이버 범죄자들에게 안전한 인프라를 제공할 수 있도록 의도치 않게 인프라를 내주고 있는 합법적인 '업스트림' 인프라 제공업체와 ISP가 포함됩니다.

BPH 제공업체는 서비스형 사이버 범죄(cybercrime-as-a-service) 생태계 내에서 유일한 인프라 제공업체 카테고리는 아닙니다. 이러한 서비스들은 사이버 범죄 캠페인을 적극적으로 지원하고, 합법적인 조사와 대응을 고의적으로 방해함으로써 호주에 대한 사이버 범죄 위협을 지속 가능케합니다. BPH 제공업체에 대한 조치는 이러한 서비스와 이를 사용하는 악의적인 사이버 행위자들의 취약점을 부각시킵니다.