Các nhà cung cấp dịch vụ lưu trữ "Chống bị gỡ bỏ": Những yếu điểm trong hệ thống bảo vệ của hạ tầng cơ sở tội phạm mạng

Tội phạm mạng thành công thường sử dụng hạ cơ sở tầng an toàn, không bị phát hiện và có khả năng chống chịu cao. Đằng sau mọi vụ xâm nhập mạng, đánh cắp thông tin đăng nhập, mã độc tống tiền, hay đánh cắp dữ liệu và rao bán trên các diễn đàn bất hợp pháp, luôn hiện hữu một hạ tầng cơ sở an toàn giúp tội phạm mạng hoạt động và ẩn mình.

Tuy nhiên, đối với tội phạm mạng, việc duy trì trạng thái không bị phát hiện và khó truy vết ngày càng trở thành một thách thức. Sự hợp tác toàn cầu giữa các chính phủ, cơ quan thực thi pháp luật, và lãnh vực tư nhân đang khiến việc ẩn danh trên mạng của chúng trở nên khó khăn hơn. Hơn nữa, rất ít tội phạm mạng có đủ kỹ năng và chuyên môn cần thiết để tự mình quản lý và duy trì hạ tầng cơ sở an toàn. Do đó, chúng tìm đến các nhà cung cấp hạ tầng cơ sở bất hợp pháp có thể cung cấp dịch vụ này thay cho chúng, để chúng có thể dồn hết nỗ lực nhắm vào nạn nhân và thu lợi nhuận.

Tội phạm mạng dưới dạng dịch vụ'(Cybercrime-as-a-service) đề cập đến thị trường ngầm đã phát triển nhằm hỗ trợ nhiều đối tượng tội phạm mạng độc hại. Thị trường ngầm này bao gồm một loạt công cụ, dịch vụ, và thông tin ngày càng gia tăng và phát triển, có thể mua được, hỗ trợ tội phạm mạng trong việc tấn công các mục tiêu trực tuyến. Những kẻ muốn trở thành tội phạm mạng có thể mua quyền truy cập vào các mạng, mua công cụ để hỗ trợ trong việc lọt qua các biện pháp bảo mật, cũng như mua phần mềm độc hại để tấn công nạn nhân và đánh cắp thông tin cá nhân. Các nhà cung cấp dịch vụ lưu trữ chống bị gỡ bỏ(Bulletproof hosting - BPH) là một phần của hệ sinh thái này và cung cấp hạ tầng cơ sở an toàn cho tội phạm mạng. Điều rất quan trọng là một nhà cung cấp BPH có thể trực tiếp hỗ trợ hàng trăm tội phạm mạng tấn công các nạn nhân trên toàn thế giới.

Các nhà cung cấp dịch vụ lưu trữ "Chống bị gỡ bỏ"(BPH) là gì?

Nói một cách đơn giản, các nhà cung cấp BPH cho tội phạm mạng thuê một hạ tầng cơ sở ảo và/hoặc hữu hình để hoạt động. Các nhà cung cấp dịch vụ lưu trữ chống bị gỡ bỏ(BPH) là một dạng dịch vụ hạ tầng internet đặc thù cho phép các đối tượng độc hại (bao gồm cả tội phạm mạng) lưu trữ nội dung phi pháp và tiến hành các hoạt động trên internet.

Thuật ngữ "Chống bị gỡ bỏ" chỉ đơn thuần là một chiêu trò tiếp thị mà thôi. Trên thực tế, các dịch vụ này cũng dễ bị vô hiệu hóa như các nhà cung cấp hạ tầng cơ sở khác. Thay vào đó, các nhà cung cấp BPH từ chối tuân thủ các yêu cầu từ cơ quan thực thi pháp luật và các yêu cầu gỡ bỏ nội dung khác, đồng thời phớt lờ các khiếu nại từ các nạn nhân về sự lạm dụng cũng như thông báo yêu cầu từ của chủ thuê bao. Điều này có nghĩa là tội phạm mạng có thể liên lạc, điều hành các diễn đàn và các trang mạng bất hợp pháp, đưa ra phần mềm độc hại và các chiến dịch lừa đảo, cũng như rửa tiền mà không sợ nhà cung cấp sẽ chấm dứt hợp đồng thuê theo yêu cầu của cơ quan thực thi pháp luật hoặc các yêu cầu khác.

Các nhà cung cấp BPH cố ý tham gia vào hệ sinh thái tội phạm mạng và tạo điều kiện thuận lợi cho các hành vi phạm tội nghiêm trọng vì động cơ tài chính. Các vấn đề An ninh Mạng nghiêm trọng ảnh hưởng đến các tổ chức của Úc và khách hàng của họ, những điều này đã xảy ra do tội phạm mạng lợi dụng các nhà cung cấp BPH. Hậu quả của những vấn đề này bao gồm các cuộc tấn công bằng mã độc tống tiền gây gián đoạn, tống tiền dữ liệu và đánh cắp thông tin nhạy cảm.

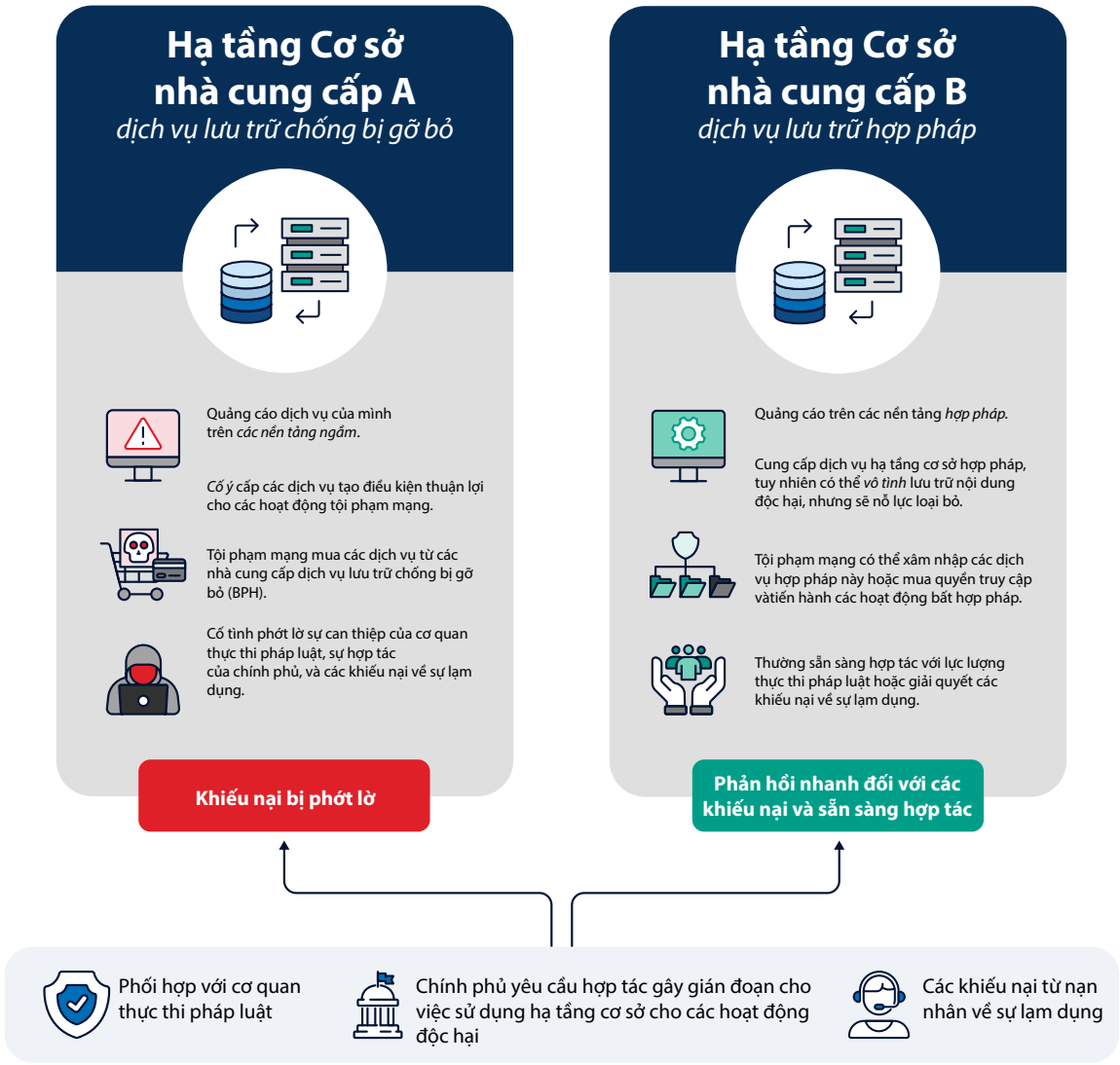
Một mẫu quảng cáo của nhà cung cấp dịch vụ lưu trữ "Chống bị gỡ bỏ" trên các diễn đàn ngầm như sau:

Các nhà cung cấp dịch vụ BPH hoạt động như thế nào?

Mỗi nhà cung cấp BPH lại có mô hình kinh doanh khác nhau. Phương pháp thường gặp nhất là cho khách hàng tội phạm mạng thuê địa chỉ IP (Một chuỗi ký tự duy nhất dùng để nhận dạng mỗi máy tính sử dụng Giao thức Internet (IP) để giao tiếp qua mạng) và sử dụng các phương pháp chuyển mạch mạng phức tạp để giúp che giấu vị trí, danh tính và hoạt động của họ. Trong nhiều trường hợp, các nhà cung cấp BPH bán hoặc cho thuê lại địa chỉ IP và máy chủ từ các nhà cung cấp dịch vụ lưu trữ hợp pháp khác, trung tâm dữ liệu hoặc các Nhà Cung cấp Dịch vụ Internet (Internet Service Providers - ISP). Các nhà cung cấp 'thượng nguồn' này có thể không biết rằng họ đang cung cấp hạ tầng cơ sở cho các nhà cung cấp BPH, những người sau đó cung cấp dịch vụ 'hạ nguồn' các cho tội phạm mạng.

Các nhà cung cấp BPH cấu hình mạng lưới và kiến trúc hệ thống của họ nhằm làm cho việc xác định khách hàng của họ trở nên khó khăn hơn. Ví dụ, họ thường xuyên thay đổi các định danh trên internet liên quan đến hoạt động của khách hàng — chẳng hạn như địa chỉ IP (Một chuỗi ký tự duy nhất dùng để nhận dạng mỗi máy tính sử dụng Giao thức Internet (IP) để giao tiếp qua mạng) được cấp phát và tên miền (Địa chỉ của một trang web hoặc email trên Internet). Các kỹ thuật này gây khó khăn cho lực lượng phòng thủ và các nhà điều tra, vì điều này khiến cho việc liên kết giữa một vấn đề và một địa chỉ IP mà một tác nhân hoặc khách hàng đang sử dụng vào một thời điểm nhất định, trở nên khó khăn hơn. Ngoài ra, các nhà cung cấp BPH thường sử dụng hạ tầng cơ sở tại các quốc gia có cách thức quản lý mạng lỏng lẻo, nơi mà các biện pháp chính thức để điều tra và ngăn chặn hoạt động mạng độc hại hầu như không tồn tại hoặc rất lỏng lẻo.

Các nhà cung cấp dịch vụ lưu trữ BPH (chống bị gỡ bỏ) khác thế nào so với các nhà cung cấp hạ tầng cơ sở hợp pháp?



Việc triệt phá các nhà cung cấp BPH ảnh hưởng như thế nào đối với mối đe dọa từ tội phạm mạng

Các nhà cung cấp BPH là cơ hội quý giá để gián đoạn hoạt động của hàng trăm đến hàng ngàn tội phạm mạng cùng một lúc. Nhiều loại tội phạm mạng và các tác nhân mạng độc hại khác sử dụng dịch vụ này để dễ dàng thực hiện hành vi phạm tội — tin tưởng rằng hoạt động của họ sẽ được che giấu và tiếp tục hoạt động bất chấp các yêu cầu gỡ bỏ hay khiếu nại về sự lạm dụng.

Tuy nhiên, cơ quan thực thi pháp luật, các cơ quan Chính phủ, và lãnh vực tư nhân đang hợp tác nhằm nhắm vào và gián đoạn các nhà cung cấp hạ tầng cơ sở bất hợp pháp này, bao gồm cả các biện pháp Phòng thủ như Chủ động chặn lưu lượng truy cập internet từ các nhà cung cấp BPH đã biết. Những hoạt động này giúp giảm lưu lượng tội phạm mạng tương tác với các mạng lưới của Úc và các đồng minh, đồng thời bao gồm cả các nhà cung cấp hạ tầng cơ sở 'thượng nguồn' hợp pháp và các nhà cung cấp dịch vụ Internet (ISP), những người có thể vô tình tạo điều kiện thuận lợi cho các nhà cung cấp BPH truy cập internet và cung cấp hạ tầng cơ sở an toàn cho tội phạm mạng.

Các nhà cung cấp BPH không phải là thể loại duy nhất trong số các nhà cung cấp hạ tầng cơ sở trong hệ sinh thái tội phạm mạng dưới dạng dịch vụ (cybercrime-as-a-service). Những dịch vụ này duy trì và tạo điều kiện thuận lợi cho mối đe dọa về tội phạm mạng đối với Úc bằng cách tích cực hỗ trợ các chiến dịch tội phạm mạng và cố ý cản trở các cuộc điều tra và đối phó hợp pháp. Việc thực hiện các biện pháp đối phó với các nhà cung cấp BPH làm nổi bật các yếu điểm của các dịch vụ này và những tác nhân mạng độc hại sử dụng chúng.