Khi hacker tấn công hacker

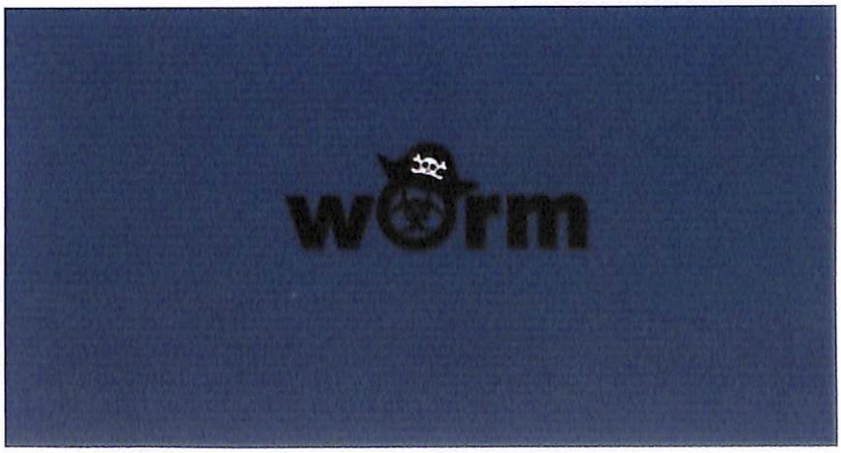
Cuộc chiến thế giới mạng không đơn thuần là của chuyên gia bảo mật chống hacker mà còn là những vụ đụng độ của những băng đảng tin tặc.

Trong khi hầu hết bọn tội phạm mạng có xu hướng đặt tầm nhìn của mình vào việc thu thập dữ liệu có giá trị từ các doanh nghiệp bảo mật yếu kém, và không có giới hạn đối với mục tiêu mà chúng tìm kiếm. Không có danh dự giữa các tên trộm, vì vậy không có gì đáng ngạc nhiên khi với động cơ lợi ích, các hacker mũ đen và cả hacker mũ xám còn tấn công lẫn nhau.

Đôi khi các cuộc tấn công hoàn toàn theo hình thức lính đánh thuê: những đối thủ biết rằng họ có thể đạt được số tiền bẩn rất nhanh nếu tìm được cách truy cập các kho dữ liệu đã được kiểm tra bị đánh cắp danh tính hoặc thông tin tài chính. Tương tự như vậy, một số cuộc chiến không gian mạng được bắt đầu để nhằm loại những đối thủ cạnh tranh ra khỏi thị trường chợ đen trên mạng. Và cùng với đó có những cuộc tấn công mang tính chất cá nhân hơn: để vạch trần một ai đó, giải quyết vấn đề ẩn giấu trên không gian mạng, hoặc thể hiện quan điểm chính trị của mình.

Trộm cắp không có độc quyền

Kẻ trộm là mục tiêu tốt nhất để



nhắm vào cho các hành vi trộm cắp, bởi vì chúng chỉ có thể khiếu nại chính những đồng nghiệp của mình. Một nhóm hacker khá hung hăng có biệt danh là w0rm đã sử dụng nguyên tắc này để tấn công cơ sở dữ liệu người dùng của một diễn đàn của thế giới ngầm có tên gọi là Monopoly, đây là trang web của những tin tặc dùng để trao đổi thông tin về việc chạy botnet phục vụ cho các hành vi lừa đảo và gian lận thẻ tín dụng. Giống như bất kỳ cuộc tấn công vào cơ sở dữ liệu nào khác, w0rm đã rao bán những thông tin của Monopoly với giá 50 USD. Sự khác biệt đối với các cuộc tấn công khác có chăng là các chuyên gia bảo mật có thể cười trên sự đau khổ của những nạn nhân vốn trước đây là đối thủ của mình.

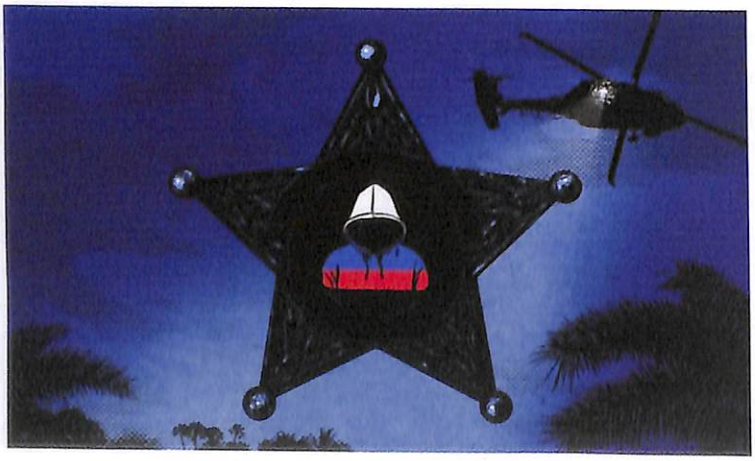
Peace tấn công w0rm

Là một hacker nổi danh trên thị trường chợ đen, tội phạm mạng với biệt danh Peace_of_Mind đã cảm thấy chán ngán và coi những cuộc tấn công của w0rm là những trò hề. Rõ ràng là cuộc tấn công vào Monopoly đã vượt ra khỏi hành vi chọc phá, cuộc tấn công này được xem là có chủ đích và gây xôn xao khắp cộng đồng tin tặc. Peace_of_Mind đã cáo buộc rằng w0rm đã thu thập nhiều thông tin về lỗ hổng zero-day của các trang web từ nhiều diễn đàn khác nhau và về đăng trên trang cá nhân như thể đó là thành tích của mình.

Ngoài ra, Peace_of_Mind còn cho biết chính bản thân mình từng là nạn nhân của w0rm khi tin tặc này tận dụng những lỗ hổng bảo mật trên trang cá nhân của ông rồi chiếm quyền truy cập và thực hiện lừa đảo. Trong cáo buộc này, Peace_of_Mind cũng cho biết rằng mình cũng đã tham gia vào việc sử dụng chương trình phá hoại được gọi là binh sơn kĩ thuật số để tấn công ngược lại trang web w0rm để đưa ra các bằng chứng và những lần truy cập dữ liệu trái phép, các cuộc tấn công đã thực hiện đối với những mục tiêu điển hình như Wall Street Journal, Vice, và CNET.

w0rm

Nhóm tin tặc người Nga nổi tiếng với việc đánh cắp cơ sở dữ liệu tên người dùng, email, và mật khẩu được mã hóa từ các máy chủ của CNET hồi tháng 7/2014 . W0rm cũng thừa nhận, nhóm đã hack thành công trang web của hãng BBC vào cuối năm 2013, trước đó còn tấn công các trang web của Adobe Systems và một số ngân hàng của Mỹ. Với việc tấn công nhắm vào các trang web cao cấp, nhóm hacker Nga này cho biết, họ đã làm một việc có thể nâng cao nhận thức của công chúng về lỗ hổng bảo mật.

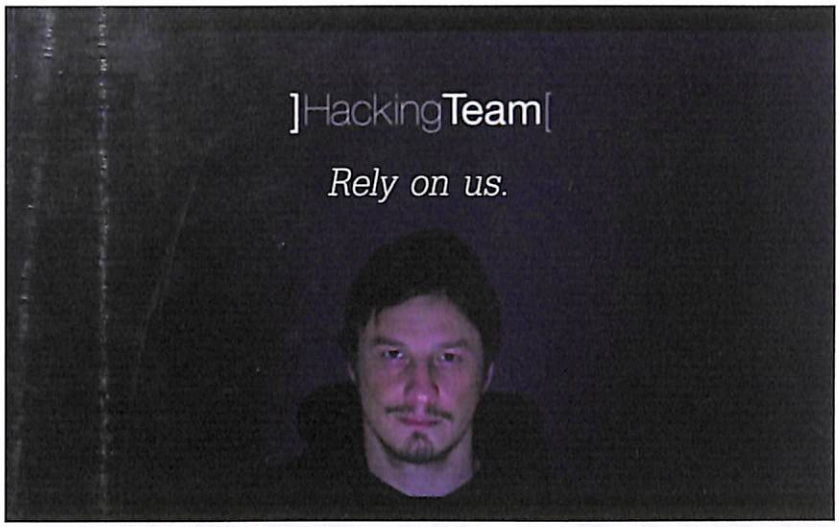


Cuộc tấn công của d33ds

Cuộc chiến của các băng đảng tin tặc khá phổ biến và đã có những trận chiến được ghi vào lịch sử thế giới ngầm. Đáng chú ý nhất là trận chiến năm 2011 của một nhóm hacker có tên gọi d33ds tấn công vào chợ đen của đối thủ Srblche. Nhóm Srblche nổi danh với việc bán quyền truy cập admin của các trường quân sự và các lỗ hổng của nhiều trang web chính phủ Mỹ.

Các thành viên của cộng đồng tin tặc đã cáo buộc rằng trong quá khứ Srblche đã đánh cắp các công cụ của người khác từ các diễn đàn ngầm và cố gắng thu lợi từ chúng. Điều này có thể giải thích lý do tại sao d33ds nhắm mục tiêu vào nhóm Srblche. d33ds đã công bố thông tin về máy chủ, các mật khẩu của khách hàng của Srblche và thậm chí cả mã truy cập quản trị của tin tặc trong văn bản gốc.

Vụ tấn công d33ds dường như



mang tính dàn mặt đối thủ nhiều hơn là phân chia địa bàn chợ đen tin tặc. Nhưng qua đó, nhiều nhà nghiên cứu về an ninh mạng cũng chỉ ra rằng các băng đảng tin tặc đang tìm cách hạ bệ những đối thủ cạnh tranh để dành thị trường. Những thị trường này bao gồm việc bán các lỗ hổng bảo mật, gian lận thẻ tín dụng, đánh thuê tin tặc. Srblche cũng chính là nhóm chuyên cung cấp các dịch vụ bao gồm việc tấn công các máy chủ đặc biệt theo yêu cầu của khách hàng.

Cơ quan phòng chống ma túy Hoa Kỳ (DEA) đã tìm cách để tích hợp Remote Control System của Hacking Team với một công cụ gián điệp cho phép họ nhận được "tất cả các lưu lượng truy cập Internet của các ISP ở Columbia". Đã có một cuộc gặp mặt giữa một đại diện của Hacking Team và một người đàn ông của DEA tại Bogota.
Một tài liệu của Hacking Team đã liệt kê những mối đe dọa với hoạt động kinh doanh của họ bao gồm các tổ chức nổi tiếng như: Human Rights Watch, Privacy International, và Citizen Lab. Các nhà hoạt động của nhóm Anonymous cũng được liệt vào danh sách các mối đe dọa với Hacking Team.

Hacking Team bị tấn công

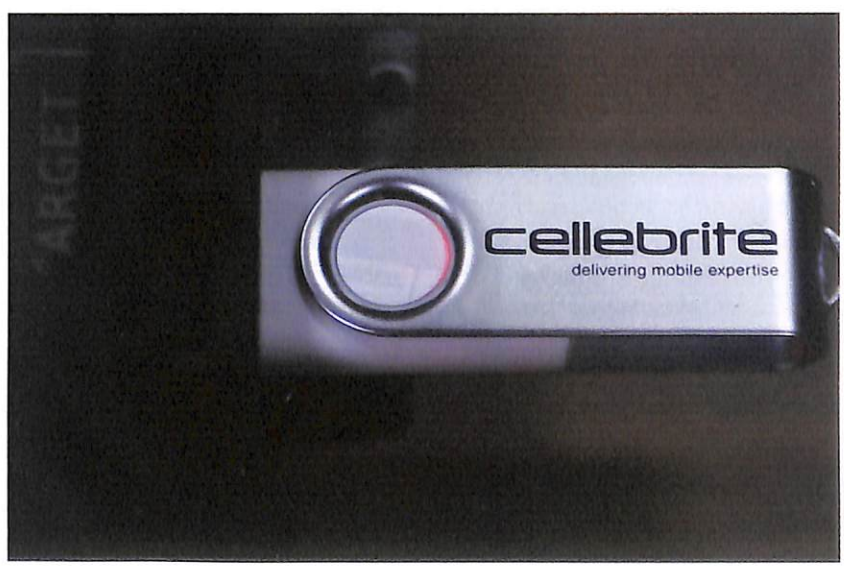
Một trong những cuộc tấn công hacker-on-hacker nổi tiếng nhất trong 2 năm qua chính là việc Hacking Team, công ty phần mềm gián điệp Ý chuyên bán phần mềm gián điệp cho các cơ quan thực thi pháp luật trên toàn thế giới bị xâm nhập. Đây là cuộc tấn công nhằm thể hiện tinh thần hacker đích thực.

Công ty phần mềm gián điệp Ý đã bị một hacker vô danh đánh sập trang web vào hồi tháng 6/2015 và sau tám tháng gần như hoàn toàn im lặng, người "cảnh binh kỹ thuật số" đứng đằng sau vụ hack đã xuất hiện. Gã xuất bản một bài viết chi tiết về cách gã đột nhập vào hệ thống của Hacking Team và vạch trần những bí mật công việc mà Hacking Team đang thực hiện.

Trong bài viết của mình, hacker tự xưng là Phineas Fisher tiết lộ việc đánh cắp hơn 400GB dữ liệu nhạy cảm. Phineas Fisher cho rằng tấn công mạng nhằm vào những vụ tham nhũng và lạm dụng quyền lực mới thực sự là hack có đạo đức, còn tư vấn bảo mật cho các công ty thường là mục tiêu xứng đáng bị tấn công.

Hacking Team tuyên bố rằng phần mềm gián điệp của hãng rất có hiệu quả và các công cụ hack do công ty phát triển thực sự do các cơ quan thực thi pháp luật yêu cầu để chống lại bọn tội phạm và khủng bố. Tuy nhiên, qua nhiều năm, các nhà nghiên cứu ghi nhận một số trường hợp công cụ của Hacking Team được sử dụng để chống lại các nhà báo, người bất đồng chính kiến hoặc các nhà hoạt động. Vụ tấn công của Phineas Fisher đã vạch trần toàn bộ bí mật của công ty hack, bao gồm cả danh sách khách hàng vốn được bảo mật cực kỳ chặt chẽ.

Độ nóng của vụ tấn công này chưa dừng tại đó khi Phineas Fisher tiết lộ rằng chính mình là người hack Gamma International, đối thủ cạnh tranh với Hacking Team hồi năm 2014. Được biết đến với công nghệ phần mềm gián điệp FinFisher, Gamma trước đây đã bị hiệp hội Phóng viên không biên giới đặt cho cái tên là "kẻ thù của Internet" giống như các chính phủ ở Thổ Nhĩ Kỳ, Ai Cập và Oman.



Cuộc chiến tiếp diễn

Đã có rất nhiều hacker tiếp nối con đường mà Phineas Fisher đã đi. Hồi tháng 1/2017, công ty chuyên về bẻ khóa của Israel là Cellebrite - nổi tiếng sau vụ hack iPhone 5C cho FBI, bị một nhóm hacker lấy đi 900 GB dữ liệu và dọa sẽ công khai bản sao những thông tin đó. Lượng thông tin bị bẻ khóa đó bao gồm: thông tin khách hàng, dữ liệu cơ sở và nhiều tài liệu kỹ thuật quan trọng miêu tả sản phẩm của công ty.

Trong trường hợp này, kẻ tấn công không công khai danh tính, nhưng đã trao đổi thông tin trong phòng chat IRC và với giới truyền thông. Tương tự như các công ty hacker khác, Cellebrite bị cáo buộc có mối quan hệ với nhiều chính phủ và vi phạm nhân quyền một cách trắng trợn.

Một cuộc chiến mang đậm màu sắc chính trị là của 2 băng đảng, Anonymous và Lizard Squad

Có vẻ như sau khá nhiều những chiến tích và vụ tấn công mạng nổi tiếng, nhóm hacker Hồi giáo tự xưng Lizard Squad đã phải nếm "trái đắng" sau lần "hỏi thăm" của Anonymous hồi năm 2015.

Các website của nhóm hacker Lizard Squad đã bị đánh sập và các tài khoản Twitter @lizardmafia của nhóm cũng bị ngưng hoạt động. Nhóm đứng ra chịu trách nhiệm cho vụ tấn công này là một nhánh của mạng lưới hacker ẩn danh Anonymous.

Như trong một tuyên bố khá cứng rắn trước đó của Anonymous trên mạng, mạng lưới này cam kết sẽ làm hết sức để triệt tiêu các website và tài khoản truyền thông của nhiều tổ chức Hồi giáo cực đoan gây nguy hại cho nền hòa bình thế giới. Và bây giờ, để tiếp tục thực hiện hóa lời hứa của mình, mạng lưới này đã có loạt hành động mới nhất nhằm trả đũa cho những động thái tiêu cực gần đây của nhóm hacker Lizard Squad.

Nhánh Anonymous Protection khẳng định rằng, họ làm như vậy với mục đích chính là để bảo vệ mọi người trên Internet và họ coi Lizard Squad giống như một mối đe dọa nghiêm trọng mà Anonymous cần phải xử lý.

Nhóm hacker Lizard Squad là "tác giả" của khá nhiều cuộc tấn công mạng nguy hiểm và nghiêm trọng trong thời gian gần đây, đơn cử như vụ tấn công DDoS vào một số website lớn trong đó có Xbox Live và Playstation Network. Tiếp đến là việc mở dịch vụ Lizard Stresser cho phép đặt thuê nhóm "tấn công" các website khác với mức giá rẻ mạt nhằm mục đích khiêu khích, tạo sự hỗn loạn và kiếm lời bất chính từ hoạt động tấn công mạng.

HỒNG ĐĂNG

Cellebrite đối tác quen thuộc của FBI

Trong 7 năm qua, Cellebrite và FBI từng ký với nhau 187 hợp đồng với trị giá không dưới 10.000 USD một lần. Hồ sơ chính phủ Mỹ ghi nhận Cellebrite vừa ký hợp đồng lớn nhất từ trước đến nay với FBI, trị giá 218.000 USD, cùng ngày FBI công bố bẻ khóa thành công chiếc iPhone của nghi phạm khủng bố.

Là một công ty chuyên bẻ khóa điện thoại di động, sản phẩm chính của Cellebrite là một thiết bị có kích thước bằng chiếc laptop thông thường được gọi là Universal Forensic Extraction Device (UFED). Thiết bị này có thể trích xuất dữ liệu từ hàng ngàn phiên bản điện thoại di động khác nhau. Dữ liệu có thể bao gồm các tin nhắn SMS, email, nhật ký cuộc gọi, và nhiều hơn nữa, chừng nào người dùng UFED vẫn đang nắm giữ trong tay chiếc di động mục tiêu.