C15: "HUY "REMY" LÀ THỦ PHẠM TẤN CÔNG CHODIENTU.COM!"

<font face="Times New Roman"

Đại diện Phòng chống tội phạm công nghệ cao thuộc C15 Bộ công an cho biết: Tất cả các chứng cứ đều chứng minh rõ ràng Nguyễn Quang Huy là thủ phạm tấn công Chodientu.com.
Tại hội thảo chiều nay 9/11 về các hành vi vi phạm, tội phạm trong Thương mại điện tử (TMĐT) do Vụ TMĐT - Bộ Thương Mại phối hợp cùng các cơ quan chức năng về lĩnh vực tội phạm công nghệ cao tổ chức, giới báo chí đã đặc biệt chú ý tới bài trình bày của Đại diện phòng chống tội phạm công nghệ cao, thuộc C15 Bộ Công An về một vụ việc nổi bật trong lĩnh vực an ninh mạng thời gian qua - website Chodientu.com - trang TMĐT của công ty phần mềm Hòa Bình bị hacker tấn công.
VietNamNet đã có cuộc trao đổi nhanh với ông Trần Văn Hòa - Trưởng phòng chống tội phạm công nghệ cao C15 về vấn đề nhiều bạn đọc đang quan tâm này:

9h15p ngày 8/9/2006, Huy "remy" bước vào trụ sở Bộ Công An (40A Hàng Bài) để trả lời về các vấn đề của cơ quan điều tra đưa ra.

"Nguyễn Quang Huy, tức Huy "Remy" có đúng là thủ phạm tấn công Chodientu.com không - thưa ông?"

"Một trăm phần trăm!"
"Nhưng Huy vẫn không thừa nhận hành vi này?"
"Chúng tôi (Gồm C15 và đại diện Bộ Bưu chính Viễn thông, Thanh tra Bộ BCVT, Thanh tra Bộ VHTT - NV) gồm nhiều chuyên gia về CNTT và Pháp lý đều kết luận những chứng cứ thu thập được đã hoàn toàn chỉ rõ Huy là thủ phạm tấn công vào tên miền Chodientu.com."

"Điều đó cũng giống như một kẻ đã bước lên đoạn đầu đài vẫn không chịu công nhận tội trạng?"
"Đúng vậy! Vấn đề là chứng minh được anh ta đã phạm tội."
Trong buổi hội thảo, ông Hòa đã có bài trình bày về vấn đề khung pháp lý cho hành vi vi phạm và tội phạm trong lĩnh vực TMĐT, sau đó đại diện Phòng chống tội phạm công nghệ cao đã trình bày toàn bộ quá trình xảy ra vụ tấn công tên miền Chodientu.com của công ty Peacesoft, cũng như đưa ra các bằng chứng mà họ cho rằng hoàn toàn có thể chứng minh Huy Remy chính là thủ phạm tiến hành cuộc tấn công.

ông Trần Văn Hòa trình bày về vấn đề khung pháp lý cho hành vi vi phạm và tội phạm trong lĩnh vực TMĐT tại hội thảo chiều 9/11.

Các dấu vết của cơ quan điều tra (CQĐT) mà đại diện phòng chống tội phạm công nghệ cao - thuộc C15 đưa ra, về vấn đề chodientu.com, gồm có:
Thứ nhất, việc Huy chiếm đoạt acount BINHNH trên register.com để kiểm soát các tên miền, thay đổi mail liên hệ: anaconda@anacondasoft.com, quangcao_online_01@yahoo.com, hn_4011@yahoo.com, vbot2006@yahoo.com và Assigned user (chuyển nhượng) sang email vbot2006 athingcn@yahoo.com (hòm thư Yahoo Mail và cũng là nick chat YM của Huy remy) để cũng có quyền kiểm soát các tên miền.
Thứ hai, C15 đưa ra các dấu vết xâm nhập máy chủ của Công ty PM Hòa Bình đặt tại nhà cung cấp dịch vụ VNGT qua user MSSQL, địa chỉ IP truy cập remote máy chủ này vào sáng 23/9/2006 là 58.187.122.76, 58.187.122.204 với tên máy tính truy cập là TEEN_CORP2; log của Apache ghi nhận: Hồi 5 giờ 50 phút ngày 23/9/2006, máy tính có địa chỉ IP 58.187.122.204 đã download file backup dữ liệu của chodientu.com, tên file là "data_backup_all_1809.rar".
Kẻ xâm nhập cũng thêm một user mới vào máy chủ này, đồng thời cài 5 file backdoor: a.php, conf_global.php, chabietdaura.php, ver1.php, vicky.asp vào máy chủ này tại peacesoft.net/data/...
Dấu vết do cơ quan điều tra thu thập được trên máy chủ của Công ty PM Hòa Bình đặt tại VNGT là từ Security Log, Apache Log File a.php và File "conf_global.php".
Thứ ba, CQĐT đưa ra các dấu vết chiếm đoạt account PEACESOFT trên EveryDNS.com của Công ty PM Hòa Bình. Đối tượng đã sử dụng máy chủ đặt tại nhà cung cấp dịch vụ VNGT để truy cập vào EveryDNS - thay đổi, trỏ tất cả tên miền của Công ty PM Hòa Bình tới địa chỉ 69.37.63.80. Đổi mail liên hệ của account này thành anaconda@anacondasoft.com, bao_moi_bao_moi_day@yahoo.com. Các dấu vết sau được CQĐT tìm thấy trên máy chủ của Công ty PM Hòa Bình đặt tại VNGT.

Một trong hàng chục bức ảnh chụp màn hình cơ quan điều tra dùng làm căn cứ khi thu thập từ các ổ cứng máy tính của Huy "remy".

Từ các dấu vết này, cơ quan điều tra đồng thời đưa ra các căn cứ: Thứ nhất, công ty FPT xác nhận địa chỉ IP cơ quan điều tra tìm thấy trong Security Log trên máy chủ của Công ty PM Hòa Bình trùng với địa chỉ IP được cấp phát cho thuê bao ADSL của Nguyễn Quang Huy tại thời điểm hành động tấn công được thực hiện.
Thứ hai, ba chiếc máy tính mà Nguyễn Quang Huy sử dụng có tên là TEEN_CORP1, TEEN_CORP2, TEEN_CORP3. Trong đó TEEN_CORP2 trùng với tên máy tính mà đối tượng sử dụng để xâm nhập vào máy chủ của Công ty PM Hòa Bình.
Sau đó, C15 cũng đưa ra hàng chục bức ảnh chụp màn hình mà cơ quan điều tra thu thập được trên hai ổ cứng máy tính của Nguyễn Quang Huy. Cho thấy Huy sở hữu các địa chỉ email kiểm soát tên miền chodientu.com, các file backdoor, user lạ được xác lập trên máy chủ của Công ty Hòa Bình...vv.
Phần sau, C15 đưa ra các thông tin cho thấy nội dung không lành mạnh của trang web gmetal.net. Và chứng minh chủ sở hữu trang web này là Nguyễn Quang Huy với các thông tin: Ngyễn Quang Huy đăng ký gmetal.net ngày 9/1/2006 với địa chỉ mail là huyremy@gmail.com. Đến ngày 24/6/2006 thay đổi mail liên hệ thành huy@teen.net.vn và ngày 7/10/2006 thay đổi mail liên hệ thành vbot2006@yahoo.com.

Bằng chứng thu được trên ổ cứng máy tính của Nguyễn Quang Huy cho thấy đây chính là công cụ thực hiện việc tấn công tên miền chodientu.com và phát tán nội dung đồi truỵ trên website gmetal.net. (Ảnh: Trình bày của C15 tại hội thảo 9/11).

Đại diện C15 cho rằng, với những căn cứ mà C15 đưa ra, hoàn toàn có thể khẳng định Huy là đối tượng đã tấn công tên miền Chodientu.com, cũng như phải chịu trách nhiệm về hoạt động

truyền bá các văn hoá phẩm đồi truỵ của website gmetal.net.

Theo một đại diện cơ quan điều tra cho VietNamNet biết, "Chúng tôi sẽ chuyển các hồ sơ các hành vi phạm tội mang tính dân sự mà Huy đã ký nhận (phát tán virus, tấn công server cài backdoor, lập trang tin không xin phép, dùng phần mềm vi phạm bản quyền - NV) cho bên Thanh tra Bộ BCVT và Thanh tra Bộ VHTT xử phạt. Các mức phạt tổng cộng có thể sẽ lên tới 50 triệu, theo khung từ 10 đến 20 triệu đồng với mỗi hành vi phạm pháp".

"Trước mắt, cơ quan chức năng sẽ vận động đương sự thừa nhận hành vi tấn công tên miền chodientu.com, dựa vào các tình tiết phạm tội và hậu quả gây ra để cân nhắc việc xử phạt hành chính. Trong trường hợp đối tượng bất chấp các bằng chứng, không chịu thừa nhận, chúng tôi sẽ phối hợp với Viện Kiểm sát đánh giá các chứng cứ để lập hồ sơ khởi tố xử lý hình sự theo pháp luật."