BỘ CÔNG AN
CÔNG AN TP. HỒ CHÍ MINH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 1914/CATP-PV05 *Thành phố Hồ Chí Minh, ngày 24 tháng 5 năm 2021*

V/v Thông báo tình hình tội phạm sử dụng công nghệ cao tại Hiệp hội các Quốc gia Đông Nam Á (viết tắt khu vực ASEAN)

Kính gửi:

- Ban Thường trực Ủy ban Mặt trận Tổ quốc Việt Nam TP;
- Lãnh đạo các tổ chức chính trị - xã hội trên địa bàn TP;
- Thủ trưởng các Sở, ban, ngành trực thuộc TP;
- Chủ tịch hội đồng thành viên, Tổng giám đốc, Giám đốc các doanh nghiệp trực thuộc thành phố;
- Chủ tịch UBND 21 quận, huyện và TP Thủ Đức;
- Trưởng Công an 21 quận, huyện và TP Thủ Đức.

Thời gian qua, tình hình tội phạm sử dụng công nghệ cao tại khu vực ASEAN có nhiều diễn biến phức tạp, tội phạm mạng đã trở thành một ngành công nghiệp trị giá hàng tỷ đô la và từ những khoản lợi siêu lợi nhuận đó đã khiến các tổ chức tội phạm truyền thống chuyển sang đa dạng hóa các hoạt động tội phạm bằng cách liên lạc, trao đổi thông tin, giao dịch tài chính và thực hiện các hoạt động phạm tội trên không gian mạng. Thực trạng trên là một trong những nguyên nhân gây mất an ninh trật tự, ảnh hưởng rất lớn đến đời sống Nhân dân trên địa bàn Thành phố.

Nhằm góp phần phát hiện, phòng ngừa, đấu tranh với hoạt động vi phạm pháp luật xảy ra liên quan tội phạm sử dụng công nghệ cao. Công an thành phố gửi Thông báo một số phương thức, thủ đoạn của tội phạm trên ***(gửi kèm Thông báo)***, để các đồng chí lãnh, chỉ đạo bộ phận chức năng tổ chức tuyên truyền, phổ biến sâu rộng đến cán bộ, đoàn viên, hội viên, công nhân viên chức, người lao động, học sinh, sinh viên và Nhân dân nhận biết để phòng ngừa, phát hiện, tích cực tham gia tố giác và đấu tranh với các thủ đoạn hoạt động của loại tội phạm này, đảm bảo giữ vững an ninh chính trị, trật tự an toàn xã hội, góp phần đẩy mạnh công tác xây dựng phong trào toàn dân bảo vệ ANTQ trên địa bàn Thành phố.

Rất mong sự quan tâm phối hợp của các đồng chí./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CATP;
- Các đ/c Phó Giám đốc CATP;
- Phòng PV01, PA 03, 04, 05;
- Công an TP. Thủ Đức, 21 quận, huyện;
- Lưu: VT, PV05.

Độ mật: thường. Đ Chinh 85b.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TP. HỒ CHÍ MINH

Đại tá Nguyễn Thanh Hướng

PHÒNG XÂY DỰNG PHONG TRÀO
BẢO VỆ AN NINH TỔ QUỐC

THÔNG BÁO

Tình hình tội phạm sử dụng công nghệ cao tại Hiệp hội các Quốc gia Đông Nam Á (viết tắt ASEAN)

Thời gian qua, tội phạm mạng đã trở thành một ngành công nghiệp trị giá hàng tỷ đô la và lợi nhuận đó đã khiến các tổ chức tội phạm truyền thống chuyển sang đa dạng hóa các hoạt động tội phạm bằng cách liên lạc, trao đổi thông tin, giao dịch tài chính và thực hiện các hoạt động phạm tội trên không gian mạng. Trong tình hình đại dịch Covid-19 không chỉ đẩy nhanh quá trình chuyển đổi kĩ thuật số của các quốc gia mà còn làm gia tăng tội phạm sử dụng công nghệ cao, đặc biệt dưới hình thức: lừa đảo qua thư điện tử doanh nghiệp; tấn công giả mạo; mã độc tống tiền; đánh cắp dữ liệu thương mại điện tử; viết và bán các công cụ độc hại và lừa đảo trực tuyến. Với một số phương thức, thủ đoạn, như sau:

1. Lừa đảo qua thư điện tử doanh nghiệp (BEC):

Lừa đảo qua thư điện tử doanh nghiệp (BEC) là một ví dụ điển hình của tội phạm sử dụng công nghệ cao mà không yêu cầu có bất kỳ kỹ thuật phức tạp nào để có thể chiếm đoạt một số tiền lớn của nạn nhân.

Phương thức thủ đoạn: Các đối tượng thường sử dụng mã độc tấn công và chiếm đoạt tài khoản thư điện tử của cá nhân có vị trí cao trong một công ty, hay từ một khách hàng hoặc nhà cung cấp dịch vụ, sau đó gửi thư cho nhân viên của công ty yêu cầu chuyển khoản đến một tài khoản ngân hàng nhất định.

Thời gian gần đây, các đối tượng bắt đầu chuyển từ sử dụng mã độc sang sử dụng các công cụ quản lý từ xa (RATs). RATs cho phép các đối tượng xác định các tập tin lưu trong thiết bị, thu thập thông tin đăng nhập nhạy cảm và các thông tin cá nhân khác. Các đối tượng cũng có thể sử dụng đường truyền để tải virus có thể tự động lây lan sang các thiết bị khác. Một RATs thường đi kèm một công cụ đánh cắp dữ liệu như phần mềm theo dõi thao tác bàn phím (keylogger) để giúp các đối tượng thu thập nhanh chóng các thông tin đăng nhập nhạy cảm như mật khẩu của tài khoản ngân hàng hay thẻ tín dụng. Những mã độc thường được sử dụng để đánh cắp thông tin trong hoạt động lừa đảo qua thư điện tử doanh nghiệp (BEC) bao gồm: AgentTesla, AzoRult, KeyBase, LokiBot, Pony, PredatorPain và Zeus. Các công cụ quản lý từ xa (RATs) sử dụng trong hình thức BEC thường là: Netwire, DarkComet, LuminosityLink, Remcos, ImminentMonitor, NJRat, Quasar, Adwind và Hworm.

2. Tấn công giả mạo (Phishing):

Xu hướng tấn công giả mạo ở khu vực ASEAN không có dấu hiệu suy giảm. Tại khu vực ASEAN trong thời gian vừa qua, hầu hết các lượt tấn công giả mạo mà Kaspersky ngăn chặn được là nhắm tới các công ty kinh doanh vừa và nhỏ tại Indonesia, Malaysia, Việt Nam.

Phương thức thủ đoạn: Nổi lên tình trạng tội phạm tung những thông tin liên quan đến Covid-19 để lừa đảo những người cả tin. Mã độc, phần mềm gián điệp và virus ăn

cắp thông tin được cài vào trong các bản đồ và trang Web tương tác về Covid-19. Có sự gia tăng số lượng các thư điện tử gửi hàng loạt trong đó lừa người dùng nhấp vào đường dẫn mà từ đó tải về và cài đặt phần mềm gián điệp vào máy tính hoặc thiết bị di động.

Hiện nay, các đối tượng có thể mua một bộ công cụ tấn công giả mạo với giá 20 đô la Mỹ trên các chợ đen trực tuyến kèm hướng dẫn sử dụng trực tuyến. Những đối tượng bán các bộ công cụ cũng có hoạt động hỗ trợ sau khi bán để đảm bảo các thư tấn công giả mạo không bị phát hiện bởi các giải pháp bảo mật có trên thị trường.

3. Mã độc tống tiền (Ransomware):

Theo thống kê của Kaspersky, có khoảng 2,7 triệu mã độc tống tiền ở ASEAN trong quý I, II, III năm 2020, trong đó Indonesia là quốc gia bị tấn công nhiều nhất 1,3 triệu lượt. Các lĩnh vực công nghiệp thường bị tấn công bằng mã độc tống tiền bao gồm: lĩnh vực sản xuất, bán lẻ, cơ quan Chính phủ, dịch vụ y tế và xây dựng. Đặc biệt trong bối cảnh đại dịch Covid-19, các đối tượng có xu hướng tăng cường tấn công các bệnh viện, trung tâm chăm sóc sức khỏe và các cơ quan hành chính.

Phương thức thủ đoạn: Có nhiều hình thức tấn công nhưng các đối tượng sử dụng hai chiến thuật tấn công bằng mã độc tống tiền chính. Một là Chiến thuật thả-và-gom là chiến thuật phát tán mã độc sử dụng thư điện tử rác hoặc các thư quảng cáo mạo danh chứa mã độc. Các loại thư này được gửi cho tất cả mọi người và nếu ai không may sẽ trở thành nạn nhân. Hai là chiến thuật tấn công có mục tiêu. Các đối tượng lựa chọn mục tiêu, sau đó tìm cách can thiệp vào mạng lưới các quan hệ của mục tiêu, từ đó bắt đầu mã hóa các dữ liệu. Chiến thuật thứ hai mất nhiều thời gian và nguồn lực hơn nhưng khoản tiền chuộc cho các dữ liệu bị mã hóa là cao hơn. Các yêu cầu tiền chuộc do dữ liệu bị mã độc tống tiền tấn công thường được các đối tượng cân nhắc kỹ lưỡng, đặc biệt mang tính khả thi về chi phí và là một phần rất nhỏ so với những thiệt hại về sao lưu dữ liệu hay tổn hại về danh tiếng của công ty.

4. Đánh cắp dữ liệu thương mại điện tử:

Dịch bệnh Covid-19 đã thúc đẩy sự phát triển của thương mại điện tử không chỉ ở khu vực ASEAN mà còn trên toàn thế giới, tạo ra cơ hội lớn cho tội phạm mạng thực hiện hành vi lấy cắp thông tin thẻ tín dụng từ các trang Web thương mại điện tử.

Phương thức thủ đoạn: Thông thường việc đánh cắp thông tin thẻ tín dụng thường được thực hiện bằng cách đưa phần mềm độc hại Trojans vào máy tính có kết nối với máy quẹt thẻ (máy PoS) để đánh cắp dữ liệu từ bộ nhớ Ram. Tuy nhiên, việc ngày càng nhiều doanh nghiệp chuyển sang sử dụng các nền tảng thương mại điện tử đã tạo thêm cơ hội cho tội phạm mạng ăn cắp được nhiều hơn các thông tin dữ liệu thanh toán, bao gồm thông tin thẻ tín dụng.

Các tổ chức tội phạm mạng sử dụng ngôn ngữ lập trình Javascript (JS) để đánh cắp thông tin thẻ đã dần mở rộng mục tiêu tấn công, không chỉ nhắm đến các cửa hàng sử dụng mã nguồn mở để xây dựng các trang Web và kinh doanh thương mại điện tử như trước đây, mà còn tấn công các nền tảng cửa hàng trực tuyến, bao gồm các giải pháp tự lưu trữ hoặc các nền tảng thương mại trên cơ sở điện toán đám mây. Các đối tượng đánh cắp dữ liệu thanh toán, dữ liệu cá nhân từ các trang web, mã hóa các dữ liệu này để tránh bị phát hiện, sau đó tổ chức các cuộc tấn công vào chính những trang web đó để đòi tiền chuộc.

5. Viết và bán các công cụ độc hại (Crimeware-as-s-Service):

Các phần mềm độc hại, phần mềm đánh cắp dữ liệu và nhiều sản phẩm tương tự đang được bày bán tràn lan trên các trang mạng ngầm, sẵn sàng cung cấp công cụ cho tội phạm thực hiện các cuộc tấn công mạng.

Phương pháp thủ đoạn: Dịch vụ thiết kế và bán phần mềm tấn công giả mạo cung cấp công cụ giúp tội phạm thực hiện hành vi giả mạo để lừa đảo người dùng và thu thập thông tin bảo mật của họ một cách tự động với chi phí thấp và thao tác đơn giản, thậm chí chỉ sau vài cú nhấp chuột.

Dịch vụ thiết kế và bán mã độc tống tiền (RaaS) cung cấp công cụ cho tội phạm thực hiện và quản lý các vụ tấn công thông qua một cổng thông tin điện tử trực tuyến. Giá dịch vụ RaaS tương đối rẻ. Nhiều trường hợp các đối tượng cung cấp dịch vụ đồng ý với mức chia từ 20 - 40% số tiền chuộc lấy được. Một phần mềm độc hại được tạo ra để thực hiện các cuộc tấn công vào hệ thống ngân hàng và thị trường tài chính có tên gọi Vawtrak đã đưa mã độc vào các đường dẫn (Urls) hay được sử dụng để đánh cắp thông tin mà khách hàng nhập trên trang Web của ngân hàng.

6. Đánh cắp tiền ảo (Cryptojacking):

Xu hướng đánh cắp tiền ảo đang gia tăng với các đối tượng tội phạm sử dụng công nghệ cao nhắm vào các nạn nhân tại khu vực ASEAN nơi cơ sở hạ tầng công nghệ thông tin có đường truyền tốt. Thủ tục tham gia giao dịch tiền ảo đơn giản, giá trị tiền ảo đang tăng cao và khả năng tránh sự giám sát của các cơ quan quản lý khiến đánh cắp tiền ảo trở thành mục tiêu lý tưởng của các đối tượng tội phạm sử dụng công nghệ cao.

Phương thức thủ đoạn: Phần mềm độc hại CoinMiner có thể chạy trên máy tính của nạn nhân mà họ không hề hay biết. So sánh với các máy tính được sử dụng với mục đích chuyên biệt, máy tính cá nhân có các tính năng bảo mật dường như ít được cập nhật hơn. Tội phạm sử dụng công nghệ cao đã lợi dụng những lỗ hổng bảo mật đang gia tăng cùng với các chiến thuật phát triển và các phần mềm độc hại tiên tiến để đạt được tối đa lợi nhuận phi pháp.

Từ những phương thức, thủ đoạn của tội phạm sử dụng công nghệ cao để lừa đảo chiếm đoạt tài sản. Công an thành phố (Phòng PV05) đề nghị cán bộ, công nhân viên chức, đoàn viên, hội viên, người lao động, học sinh, sinh viên và Nhân dân nâng cao ý thức cảnh giác phòng ngừa, không cung cấp các thông tin cá nhân hoặc truy cập, sử dụng những đường truyền, trang mạng không rõ nguồn gốc. Nếu phát hiện các phương thức, thủ đoạn hoạt động của loại tội phạm trên phải thông báo ngay cho lực lượng Công an để phối hợp xử lý./.

PHÒNG PV05 - CÔNG AN TP. HỒ CHÍ MINH