TẠP CHÍ ĐIỆN TỬ
THƯƠNG HIỆU & CÔNG LUẬN

Mã độc đánh cắp tài khoản ngân hàng, chứng khoán: Mức độ nguy hiểm "chưa từng có tiền lệ"

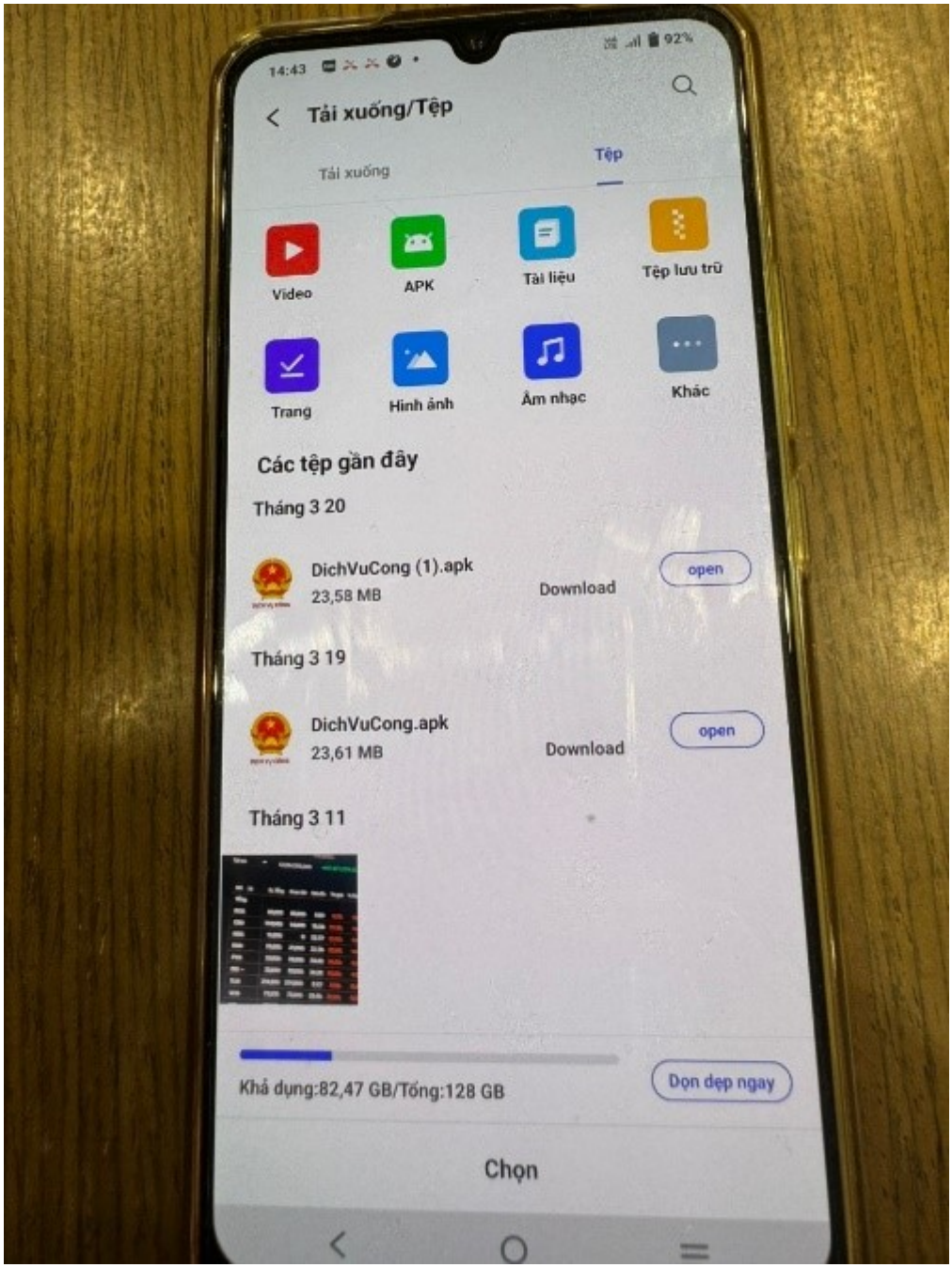
10:54 15/04/2024

Liên tục trong thời gian qua, nhiều người bị sập bẫy các kẻ lừa đảo trên mạng, bị chiếm quyền quản lý tài khoản ngân hàng cũng như chứng khoán, và rút hết tiền trong các tài khoản. Giới chuyên gia nhìn nhận, những vụ lừa đảo mất tiền trong tài khoản ngân hàng diễn ra ngày càng tinh vi, chiếm đoạt số tiền càng lớn, trong đó nhiều nạn nhân mất từ hàng trăm triệu đến hàng chục tỷ đồng.

Cảnh báo liên tục... vẫn bị lừa cài ứng dụng giả mạo

Theo các chuyên gia công nghệ, ngoài những thủ đoạn lừa đảo như cuộc gọi video deepfake; giả danh cơ quan thuế, công an, viện kiểm sát, tòa án, lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao; giả mạo biên lai chuyển tiền bán hàng giả hàng nhái trên sàn thương mại điện tử..., gần đây nở rộ hình thức lừa đảo chiếm quyền trợ năng (Accessibility) trên điện thoại sử dụng hệ điều hành Android.

Theo ông Đức Anh, chuyên gia tập đoàn công nghệ hàng đầu thế giới Group-IB, GoldDigger là một mã độc Android Banking Trojan cổ điển, lạm dụng tính năng Accessibility Service trên nền tảng Android và cấp cho tội phạm mạng quyền kiểm soát thiết bị. Khi nạn nhân phát hiện mọi chuyện thì có thể đã quá muộn, vì tiền đã bị rút ra khỏi các tài khoản ngân hàng, chứng khoán được cài đặt trên điện thoại.



Cùng với việc cài phần mềm có chứa mã độc “DichVuCong.apk”, nạn nhân đã vô tình cho phép kẻ lừa đảo được chiếm toàn bộ quyền quản lý, điều khiển như nhắn tin, gọi điện, nghe điện thoại trên chính điện thoại

Hồi tháng Ba, ông M.C sử dụng điện thoại nền tảng Android, đã cài link độc do kẻ giả mạo công an hướng dẫn, từ đó bị chiếm quyền điện thoại và các tài khoản giao dịch chứng khoán và ngân hàng cài trên thiết bị di động này. Theo chia sẻ của nạn nhân, kẻ giả mạo tự xưng là bên công an đã gọi điện đến số điện thoại của ông là 091xxxxx82, yêu cầu xác thực định danh thông tin cá nhân.

Do đã lớn tuổi, không quen với công nghệ và tin vào kẻ mạo danh, nạn nhân đã chuyển điện thoại cho người thứ ba để nhờ người này làm theo hướng dẫn của kẻ lừa đảo, từ đó tải và cài ứng dụng có mã độc “dichvucong.apk” trên điện thoại của ông.

Cùng với việc cài phần mềm có chứa mã độc “DichVuCong.apk”, nạn nhân đã vô tình cho phép kẻ lừa đảo được chiếm toàn bộ quyền quản lý, điều khiển như nhắn tin, gọi điện, nghe điện thoại trên chính điện thoại khách hàng, và sử dụng các thông tin bảo mật được ngân hàng và công ty chứng khoán cung cấp dành riêng cho khách hàng cho các giao dịch trên tài khoản ngân hàng điện tử và tài khoản chứng khoán (bao gồm: Tên truy cập, mật khẩu truy cập tài khoản, các mã xác thực SMS OTP kích hoạt tài khoản và tính năng giao dịch, kích hoạt Smart OTP và xác thực giao dịch tài chính...). Từ đó, đối tượng lừa đảo đã thực hiện các hành vi bán cổ phiếu trên tài khoản chứng khoán, chuyển tiền sang tài khoản ngân hàng và rút tiền, chiếm đoạt tài sản của nạn nhân.

Cũng trong tháng Ba, dư luận bất ngờ khi chuyên gia tài chính N.T.H lên tiếng chia sẻ về việc ông bị “rút ruột” 500 triệu đồng trong tài khoản. Theo đại diện ngân hàng, đây là một vụ việc có dấu hiệu lừa đảo tội phạm công nghệ cao, nên đã tố cáo ra cơ quan công an để xác minh, điều tra.

Mức độ nguy hiểm của mã độc là "chưa từng có tiền lệ"

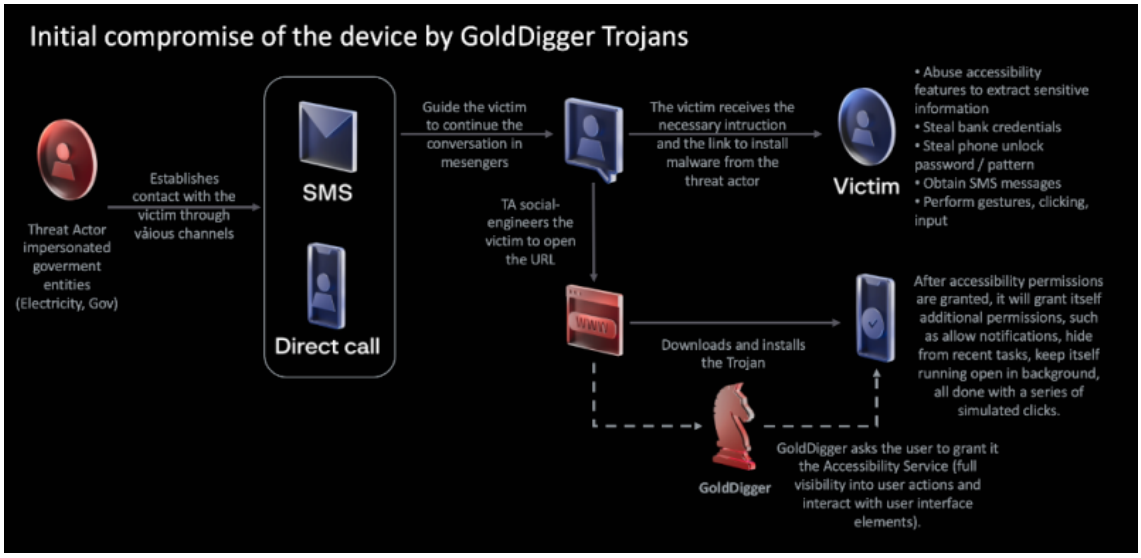
Đầu năm 2024, Group-IB, đã phải gióng lên hồi chuông cảnh báo không chỉ có người dùng điện thoại sử dụng nền tảng Android, mà người dùng iPhone tại Việt Nam đang bị tấn công bởi mã độc ăn cắp tài khoản ngân hàng, với mức độ nguy hiểm "chưa từng có tiền lệ".

Theo ông Đức Anh, chuyên gia từ Group-IB, trước đây, GoldDigger là một mã độc chỉ lạm dụng tính năng Accessibility Service trên nền tảng Android. Hiện nay, nó đã có biến thể nguy hiểm hơn, tấn công trên cả nền tảng iOS để thu thập và lọc thông tin cá nhân từ nạn nhân, cũng như dữ liệu sinh trắc học.

Từ các dữ liệu này, tin tặc sử dụng công cụ AI để tạo ra deepfake bằng cách thay thế khuôn mặt của chúng bằng khuôn mặt của nạn nhân, nhằm để truy cập trái phép vào tài khoản ngân hàng của nạn nhân, hoặc dữ liệu khác được bảo vệ bằng nhận dạng khuôn mặt. Đây có thể là mã độc đầu tiên nhắm vào nền tảng có độ bảo mật cao iOS, với khả năng đánh cắp dữ liệu dạng nhận dạng khuôn mặt, giấy tờ tùy thân, thậm chí cả tin nhắn SMS.

Câu hỏi mà nhiều nạn nhân đặt ra là: Làm cách nào mã độc này có thể giúp kẻ hacker điều khiển từ xa, thực hiện lệnh bán cổ phiếu trên tài khoản chứng

khoán, sau đó chuyển tiền và rút tiền trên tài khoản ngân hàng?



Ông Đức Anh lý giải: Khi vô tình truy cập link /cài đặt ứng dụng giả mạo có mã độc, người dùng sẽ cho phép mã dộc này kích hoạt các quyền của “Accessibility Service - Dịch vụ trợ năng” trên nền tảng Android, vốn ban đầu nhằm mục đích hỗ trợ người dùng khuyết tật vận hành thiết bị của họ (chẳng hạn như đọc màn hình, điều khiển dựa trên cử chỉ, chuyển lời nói thành văn bản và các dịch vụ khác).

Từ đây, mã độc cho phép kẻ lừa đảo chiếm được toàn bộ dữ liệu về hành động của người dùng, và trao quyền cho kẻ lừa đảo tương

tác trên điện thoại như chính người dùng. Điều này có nghĩa, mã độc có thể giúp kẻ gian xem số dư của nạn nhân, lấy cắp thông tin bảo mật, triển khai chức năng ghi nhật ký thao tác bàn phím, cho phép lấy mọi thông tin nhập mã xác thực của nạn nhân. Mã độc sẽ lưu văn bản được hiển thị hoặc viết trên giao diện người dùng, bao gồm cả mật khẩu, khi chúng được nhập.

Techcombank và TCBS nâng mức cảnh báo về ứng dụng giả mạo có mã độc

Đầu tháng Tư, Techcombank tiếp tục nâng cấp cảnh báo về phòng tránh những thủ đoạn lừa đảo cài đặt các ứng dụng giả mạo. Theo Techcombank, hiện nay, các đối tượng lừa đảo đang tận dụng tâm lý thiếu cảnh giác của những người dùng thiết bị di động, để thực hiện các hành vi giả danh cơ quan thực thi pháp luật (Công an, Tòa án,...), cơ quan hành chính nhà nước (Cán bộ thuế/ địa chính/ tài nguyên môi trường,...), nhân viên hỗ trợ (ngân hàng,...),... Mục đích của cùng nhằm mục đích cuối của các thủ đoạn này chính là khiến người dùng tin và cài đặt phần mềm chứa mã độc. Các phần mềm chứa mã độc này sẽ giúp đối tượng lừa đảo vượt qua hầu hết các biện pháp xác thực và bảo vệ của thiết

bị di động, từ đó lấy cắp thông tin cá nhân, thông tin tài khoản ngân hàng để chiếm đoạt tiền và tài sản của nạn nhân.

Để bảo vệ an toàn giao dịch tài khoản, Techcombank và Cty Chứng khoán Kỹ thương đã gửi cảnh báo nâng cao đến tất cả các khách hàng. Theo đó, khuyến nghị các khách hàng NÊN: (i) Cảnh giác và tìm cách kiểm chứng thông tin của bất kỳ đối tượng nào chủ động liên lạc và tự xưng là công an, cán bộ hành chính, cán bộ hỗ trợ dịch vụ công, nhân viên ngân hàng,...bằng cách gọi tới tổng đài hỗ trợ được công bố chính thức của các cơ quan, đơn vị (ii) Chỉ nên cài đặt phần mềm được tìm thấy trực tiếp trên App Store (với thiết bị hệ điều hành iOS)/CH Play (với thiết bị hệ điều hành Android); (iii) Chia sẻ thông tin cảnh giác đến bạn bè, người thân là người cao tuổi hoặc người ít am hiểu về công nghệ.

Theo khuyến nghị này, người dùng tuyệt đối (i) Không cài đặt/ tải trực tiếp bất kỳ ứng dụng nào từ đường link do bất kỳ ai gửi trên tin nhắn SMS, nội dung chat trên các nền tảng xã hội, ứng dụng nhắn tin; hoặc từ các trang web do các đối tượng cung cấp đường link; (ii) Không tin và thực hiện theo hoặc liên hệ với với các đối tượng quảng cáo trên mạng xã hội (Facebook, Zalo, Viber, Telegram,..) về các giải pháp “nhanh” cho bất kỳ dịch vụ công nào.

Từ ngày 1/4/2024, Techcombank chủ động thực hiện thu thập dữ liệu sinh trắc học để triển khai Quyết định 2345 của Ngân hàng Nhà nước, nhằm tăng cường an toàn giao dịch trực tuyến cho khách hàng. Ngân hàng Nhà nước (NHNN) đã ra quy định từ ngày 1/7, khi chuyển tiền qua tài khoản trực tuyến hoặc nạp tiền vào ví điện tử trên 10 triệu đồng phải được xác thực sinh trắc học qua khuôn mặt hoặc vân tay.

Nếu chuyển tiền dưới 10 triệu đồng và tổng số tiền chuyển trong ngày không quá 20 triệu đồng thì xác thực bằng mã OTP, không cần xác thực bằng khuôn mặt, vân tay. Tổng số tiền các giao dịch trên 20 triệu đồng/ngày phải xác thực bằng sinh trắc học (có thể dùng căn cước công dân gắn chip, tài khoản VNeID hoặc dữ liệu sinh trắc học lưu trong cơ sở dữ liệu của ngân hàng). Mục tiêu quan trọng của Quyết định 2345 QĐ/NHNN là để bảo vệ khách hàng trên nền tảng giao dịch số.

Phương Thảo